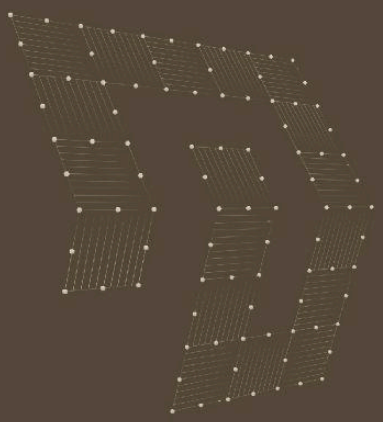
Semgrep

Comparing Pro vs. Community

Anthony Trummer

www.doyensec.com



CONTENT

ABSTRACT

Static Application Security Testing (SAST) is a large component of any modern application security program. Due to SAST's depth of view and the typical setup of modern SDLC pipelines, it has great promise in allowing organizations to completely eradicate common classes of vulnerabilities before they make it to production.

Due in part to its Community Edition's low barrier to entry and ease of use, **Semgrep** has rapidly become a widely-used SAST tool. It has positioned itself in some ways as the middle-ground between a team creating their own scripts to "grep" through a codebase looking for bugs and going all-in with a major investment, in time and/or money, to implement a more robust and/or commercial solution. A team that finds Semgrep's Community Edition useful will likely find itself asking whether they would see a positive ROI on moving up to using Semgrep's commercial version, called Semgrep Code. Our research contrasts the effectiveness of Semgrep's SAST solution to determine if there are meaningful differences between the community & paid versions.

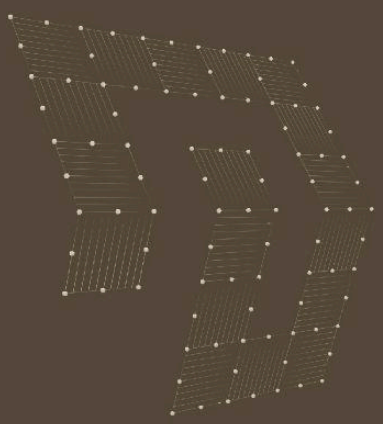
We demonstrate that Semgrep Code identifies more findings than Semgrep Community Edition, in the tested open-source projects. We also see a notable improvement in the true positive rate (TPR) when scanning the projects with Semgrep Code, compared to the Community Edition.

This research was exclusively focused on the usefulness of the rulesets used and the "engine" processing those rules. Doyensec did not evaluate other aspects - such as performance and ease of use.

Keywords

Semgrep, SAST, Static Application Security Testing, Application Security

INTRODUCTION



INTRODUCTION

Static Application Security Testing (SAST) is the process of examining the source code of applications and attempting to locate security vulnerabilities. This is contrasted with Dynamic Application Security Testing (DAST), which tests the code interactively as it is actually running on a computer system. While there are additional forms[1] of testing, diving into them is beyond the scope of this paper.

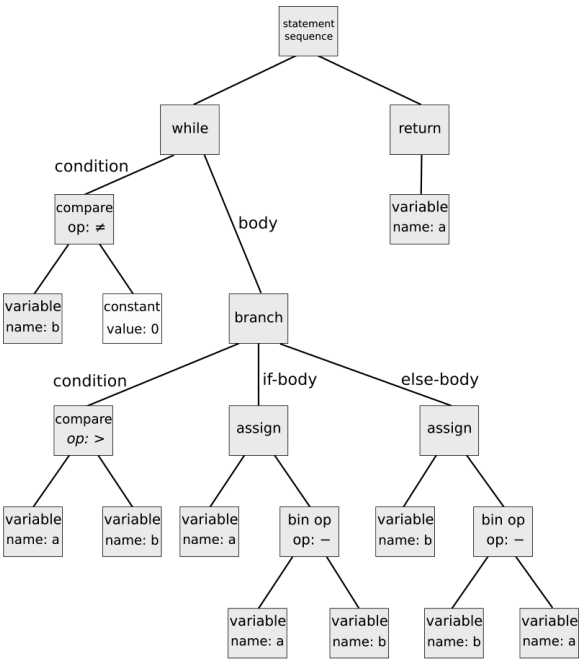
While SAST is considered a valuable tool within the Application Security community, its adoption has long been hampered by, among other things, its lack of context and inability to fully consider the application's environment. What looks like a vulnerability in a banking application is different from an application that focuses on management of computer systems. When deciding whether something constitutes a vulnerability, a tool typically looks at simple cases like whether a certain function is used with a known insecure value (e.g., turning off encryption), or more complex cases involving tracing attacker-controlled data through the application (e.g., SQL injection).

Determining what is "attacker-controlled" is the first step and requires that a SAST tool is capable of understanding all the potential inputs into an application. These could be command line input, data from web requests, local system files and even data the application itself requests from third-party applications. These collectively are generally referred to as "sources".

The next important part of this equation is to determine whether any application functionality exists that is known to be able to result in vulnerabilities. These functionalities are collectively referred to as "sinks". These could be functionalities that execute system commands, database queries, change configuration settings, etc. Basically, they are everything "interesting" an application can do (regardless of its intended use).

Historically, SAST tools have created an intermediate representation of an application in order to be able to follow the code's flow programmatically, but without compiling or interpreting it in the same manner necessary for execution. The classic example of this is the Abstract Syntax Tree (AST)[2]. Once this abstraction is available tools can see how the identified *sources* are used in relation to the identified *sinks*.

[1] https://owasp.org/www-project-devsecops-guideline/latest/02c-Interactive-Application-Security-Testing
[2] https://en.wikipedia.org/wiki/Abstract_syntax_tree



A graphical representation of an example Abstract Syntax Tree
Source: https://upload.wikimedia.org/wikipedia/commons/c/c7/Abstract_syntax_tree_for_Euclidean_algorithm.svg

For instance, the following Java code snippet will result in an equivalent AST format:

```
protected byte[] getProfilePictureAsBase64(String username) {
    var profilePictureDirectory = new File(this.webGoatHomeDirectory, "/PathTraversal/" + username);
    var profileDirectoryFiles = profilePictureDirectory.listFiles();

    if (profileDirectoryFiles != null && profileDirectoryFiles.length > 0) {
      return Arrays.stream(profileDirectoryFiles)
          .filter(file -> FilenameUtils.isExtension(file.getName(), List.of("jpg", "png")))
          .findFirst()
          .map(
              file -> {
                try (var inputStream = new FileInputStream(profileDirectoryFiles[0])) {
```

A Java source code snippet

```
F(
  DefStmt(
    ({
      name=EN(
             Id(("getProfilePictureAsBase64", ()),
               {id_info_id=133; id_flags=Ref(0);
                id_resolved_alternative=Ref([]);
                id_resolved=Ref(None); id_type=Ref(None);
                id_svalue=Ref(None); }));
       attrs=[KeywordAttr((Protected, ()))]; tparams=None; },
      FuncDef(
        {fkind=(Method, ());
         fparams=[Param(
                    {pname=Some(("username", ()));
                     pdefault=None;
                     ptype=Some({t_attrs=[];
                                 t=TyN(
                                     Id(("String", ()),
                                       {id_info_id=134;
                                        id_flags=Ref(0);
                                        id_resolved_alternative=Ref(
                                        []);
                                        id_resolved=Ref(
                                        None);
                                        id_type=Ref(None);
                                        id_svalue=Ref(
                                        None); }));
                                 });
```

A portion of the same Java snippet above in Semgrep's text-based AST format

At a high level, static analysis relies on:

a. Sources - the potentially attacker controlled data
b. Sinks - the potentially exploitable functionality
c. An abstract representation of the application's logic

While technically this is sufficient to find actual vulnerabilities, this modeling is too simplistic and neglects the complexity of real-world applications. One thing that is missing revolves around *sanitizer* functionalities which would render a *source*'s data incapable of successfully exploiting vulnerabilities. An example might be a database input pulled from attacker-controlled data, but which is limited to only the numbers 1-10 by a function that processes the data prior to inclusion in the query.

Another oversight is more subtle and has to do with how the SAST tool builds the intermediate representation of the application. In other words, how broad and thorough is its map? The most simplistic situation would be a map that only identifies *sources* that are explicit request parameter references at the time they are used. Things advance from there when the capability to understand variable assignments is included so any variables tainted with the "attacker-controlled" data are also considered *sources*. Programmers will likely be able to guess one of the limitations that still exist at this level of sophistication, namely scoping.

A variable assignment is only meaningful in its applicable scope, which may change, for example, at a function boundary. More advanced SAST tools need to be able to follow variable assignments as they occur when invoking functions, and when performing operations on them within the function and subsequent functions they invoke.

The *sensitivity* of an SAST tool represents whether it's likely to report more issues with higher false-positive rates (high sensitivity) or less issues with lower false-positive rates (low sensitivity). While a tool's perceived performance is generally taken as a whole, there are several specific facets of the analysis process that can be examined separately as well.

Flow Sensitivity - Does it understand how data is transformed between the source and sink? For example, would the tool flag a vulnerability when a variable is initially tainted, then later overwritten with a safe value, before being used in a sink?

Path/Predicate Sensitivity - Does it take conditionals into account in determining whether there is a reachable path from source to sink?

Context Sensitivity - Can the tool differentiate between multiple invocations of functions, where one produces tainted output (due to tainted input) and the other does not (untainted input)?

Field Sensitivity - Can the tool track which parts of aggregated data types (e.g., arrays) are tainted? For example, if an object has two fields where A is tainted and B is not, can it determine which field is referenced, when it's used in a sink?

Object Sensitivity - Can the tool track multiple objects of the same class?

To accurately interpret how data is manipulated and used in an application, a SAST tool must also understand the data's type. For example an array's elements can be individually tainted, whereas the entirety of a string is generally used to determine whether it's tainted. In languages like Java, when the variable is declared with its type, this information is readily available to the SAST tool. In a language like

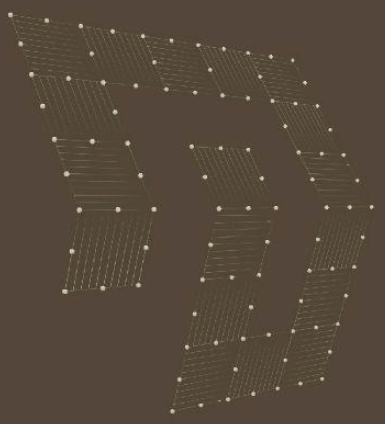
Python, variables are dynamically typed, making this process orders of magnitude more difficult. SAST tools are therefore forced to use a process known as type inference to make educated guesses as to the type of a given data element, using contextual clues. The methods used are quite complex at times and beyond the scope of this research. The takeaway is simply to realize this can have a significant impact on a tool's accuracy.

Adding to the complexity of processing static files for security analysis is the myopic view obtained when only considering a single file at a time. If a SAST tool only builds its map of the code based on a single file at a time, it will encounter countless deadends when trying to follow code paths. For instance, it will be unable to determine how many of the variables it encounters were instantiated, determine all possible usages of any variables instantiated in the single file it's processing (i.e., if they're used in other files) and won't know whether a parameter passed to a *sink* is attacker controlled, unless the entire source-to-sink mapping occurs in the same file.

This study is presented to examine the difference in the performance between two modes of operation for Semgrep, a widely used SAST tool. This comparison was intended to contrast the effectiveness of using the tool in its simplest form, versus making use of some of its additional paid features.

This study endeavored to subjectively determine the total realistic number of vulnerabilities a SAST tool should be able to identify in each project - focusing on the number of **False Positives (FP)** and **True Positives (TP)**.

TARGETS & METHODOLOGY



TARGETS & METHODOLOGY

Our analysis focused on two version of the Semgrep SAST product:

- Semgrep Code
  - Commercial paid version
  - Includes 1500+ additional Pro rules
  - Includes the Pro Engine: advanced code analysis with interfile capabilities and enterprise language support
    - Dataflow analysis to reduce the number of false positives and discover new true positives across files
    - Interprocedural analysis, including dataflow analysis methods such as taint analysis, constant propagation, typed metavariables, taint flowing in and out of callbacks, as well as framework-native analysis

- Community Edition
  - Free and Open source
  - Lightweight static analysis tool for many languages
  - Uses Community rules, available in the Semgrep Registry
  - Single-function analysis

As for targets, two known deliberately insecure applications were used as benchmark:

- OWASP WebGoat
  - WebGoat is a deliberately insecure application developed in Java. It is structured as an interactive teaching environment for web application security
- OWASP Juice Shop
  - Modern deliberately insecure web application written in Node.js, Express and Angular

Using documented writeups and solutions from the Internet, the structures of both Juice Shop and WebGoat were analyzed to get an idea of what to expect. The desire was to focus on the documented vulnerabilities, and avoid having to perform a full code review ourselves. This meant that unexpected vulnerabilities (e.g., an XSS in an SQLi module) or vulnerabilities that were in the application frameworks themselves would be excluded.

However, despite the projects being widely used and numerous solutions being posted online, the task of creating a knowledge base of confirmed vulnerabilities is not trivial. Not all the vulnerabilities presented were actually security bugs, as mockups or tasks to perform without a specific corresponding vulnerability in the code were present. Additionally, several types of issues were recognized that were not something a SAST tool could realistically be expected to identify (e.g., highly contextual). Because of these, there isn't a simple one-to-one relationship between the challenges in the apps and the raw findings from Semgrep, or ultimately what was determined to be in scope.

For the Community version scans, Semgrep was run using this command:

```
semgrep --config p/default --oss-only
```

For the Pro version scans, it was run using this command:

```
semgrep login && semgrep --config p/default --pro
```

For anyone interested in replicating our results, the following targets and tools were used:

- Semgrep version: *1.101.0* [latest at the time of testing]
- OWASP Juice Shop version: v17.1.1-2-ged4aa7cf0 [latest at the time of testing]
  - *Hash: ed4aa7cf05ff722551bf39862732cdba3269d7a2*
- OWASP WebGoat version: v2023.8-115-g02f43c54 [latest at the time of testing]
  - *Hash: 02f43c54d03d7bba5c96d97dc441ca7bc60ba249*

After running the scans, the following steps were performed to reduce the findings to meet the stated objectives above:

1. Marked all the findings that were located in directories and files where no known vulnerabilities were expected to exist as out-of-scope (OOS).
2. Marked all duplicate (DUP) findings (same bug class, same files/lines/functions or same vulnerability chain). This de-deduplication was necessary, in part, to avoid a situation where the scans using the Pro engine were unfairly penalized/credited. This was because both the Community and Pro rules were run during the Pro scans. So, for example, if both a Community rule and Pro rule matched (either TP or FP) it wasn't accurately representative to count it twice.
3. Findings that were application-level settings, such as not enabling CSRF protection, were deliberately included, regardless if they contained any other code/vulnerabilities.
4. It is important to note that because of the way Semgrep works, the findings from the Community rules may vary when run with the Pro engine vs the Community engine. This is in part due to whether sanitizing functions are considered.

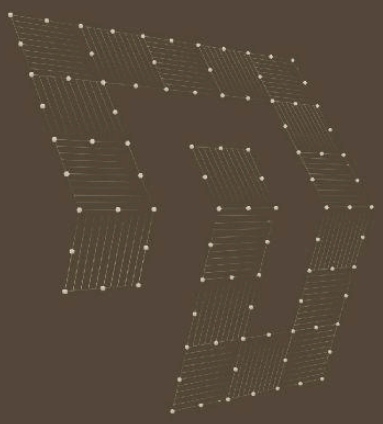
To provide more insight into the de-duplication performed, sharing a common example might clarify the process for the reader. Additionally, it helps illustrate some of the rule pruning one should consider prior to scanning. The table below shows an example of a finding that was observed multiple times.

Rule	Rule Set	Matched Code
java.spring.security.injection.tainted-sql-string.tainted-sql-string	Community	*query = "SELECT * FROM user_data WHERE last_name = '" + accountName + "'";*
java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep	Pro	*ResultSet results = statement.executeQuery(query);*

Both rules matched on the same vulnerability - one on a tainted variable in the SQL query string, closer to the *source* and the other in the query execution (i.e., the *sink*). If an engineer trusts the latter Pro rule, there is no need to run the (effectively) duplicating Community rule, especially if the Pro rule has additional False Positive prevention logic (e.g., if it can detect sanitizing functions, where applicable). In our results, these

cases were considered as *duplicates*, since they ultimately point to the same issue, just from different perspectives.

RESULTS OVERVIEW



OVERVIEW OF OUR RESULTS

Semgrep Pro and Community reported numerous vulnerabilities that were out-of-scope with relation to the training objectives of each target application. Further basic configuration of the tools would easily eliminate these, so they are not taken as negatively reflecting on the tool's performance. In fact, both Semgrep Pro and Community were highly accurate with respect to the vulnerabilities they reported that were deemed in-scope.

Our first set of scanning results, using the Pro engine with the Community rules, show no change from one project and a significant increase in the other, in terms of the number of (valid and in-scope) vulnerabilities detected, prior to de-duplication.

When the results from the scans of Juice Shop were totaled, the Community engine's 24 total vulnerabilities were exactly the same as the results seen from the Pro engine. When examined, the detailed results showed all the findings were identical, with one exception. In the exception, the same vulnerability appeared to be identified in both scans. However, the Community and Pro scan versions used different rules to detect it. This seemed to point to no meaningful difference in comparing the two sets of results.

When the Web Goat results were totaled, the Community engine's 23 total vulnerabilities were significantly less than the 32 returned from the scan using the Pro engine while matching a Community rule. It initially seemed counterintuitive that the raw number of findings would increase for the same rules, since it was believed the Pro engine would be more restrictive on what it considered a TP. Despite being technically beyond what was needed for the comparison, investigating this seemed worthwhile and served as a quality control measure as well.

A rule was identified that resulted in 7 of the additional 9 findings, namely:
java.spring.security.injection.tainted-sql-string.tainted-sql-string

After looking at its definition[3], the rule pointed to a potential explanation.

```
...
 - id: tainted-sql-string
   ...
     interfile: true
...
   options:
...
     interfile: true
   mode: taint
```

[3] https://semgrep.dev/r?q=java.spring.security.injection.tainted-sql-string.tainted-sql-string

Semgrep's *taint mode*[4] settings function differently, based on how the scan is run. In some cases, it can actually cause additional findings to be discovered (as opposed to only reducing false positives). Per the documentation[5]:

> *"Using the CLI option --pro, Semgrep will perform inter-procedural (across functions) as well as inter-file (across files) analysis."*

By deduction, it is likely that at least these 7 additional findings are from strings that were tainted in other files that are only identified due to the inter-file analysis. This suggested that the Pro engine can provide superior results, even when using the Community rules, if the rules are configured to take advantage of the Pro engine's capabilities.

The second set of results, from using the Pro engine with the Pro rules (along with the Community rules), are shown below.

	Total Rules Used (Community/Pro)	Findings From Community Rules (total/in scope)	Findings From Pro Rules (total/in scope)
WebGoat (PRO)	1053/907	207/32	61/35
JuiceShop (PRO)	1053/907	70/24	41/20

When comparing the Pro engine's results from scanning Web Goat, the Pro rules resulted in 35 valid findings compared to 32 from the Community rules.

With respect to the Juice Shop results, there were 20 findings from the Pro rules and 24 from the Community rules. The lower number of Pro findings is not in itself a negative. It could be explained by some combination of the fact that there are a lower number of Pro rules compared to Community rules in our scan, the rules are possibly more precise or the engine does a better job at eliminating superfluous results.

In fact, after the results were de-duplicated and combined, the conclusions are more clear. The net result (24) includes an additional 8 vulnerabilities, representing an increase of 50% for Web Goat. For Juice Shop, the net result (36) points to an improvement of 15 vulnerabilities, representing an increase of 71%. So, for the possible options we're aware of, the best overall results, once they are de-duplicated and combined, appear to come from using both sets of rules with the Pro engine.

[4] https://semgrep.dev/blog/2022/demystifying-taint-mode/
[5] https://semgrep.dev/docs/writing-rules/data-flow/taint-mode

USING THE COMMUNITY AND PRO RULES TOGETHER PROVIDES THE BEST OVERALL RESULTS, ONCE DE-DUPLICATED AND COMBINED. UNFORTUNATELY, THIS IS A MANUAL EFFORT.

Of the reported vulnerabilities that were deemed in-scope, both versions of the tool scored near perfect accuracy (after applying our filtering criteria). In other words, nearly every reported vulnerability that was discovered was expected. Both however flagged one vulnerability incorrectly, resulting in the 1 false positive for each. This set of results creates no distinction between the Community and Pro engines or rules in this investigation, in terms of the accuracy for the vulnerabilities reported.

The chart below breaks down the findings for each tool and against each target:

Tool Mode /Library	Total Findings	True Positives	False Positives	Out-of-Scope	Duplicate True Positives	Duplicate Out-of-Scope
Community/ Web Goat	171	16	1	147	7	0
Pro/ Web Goat	268	24	1	198	43	2
Community/ Juice Shop	66	21	0	38	3	4
Pro/ Juice Shop	111	36	0	59	8	8

Taking this into account, both tools failed to accurately detect numerous vulnerabilities that were deemed as in-scope.

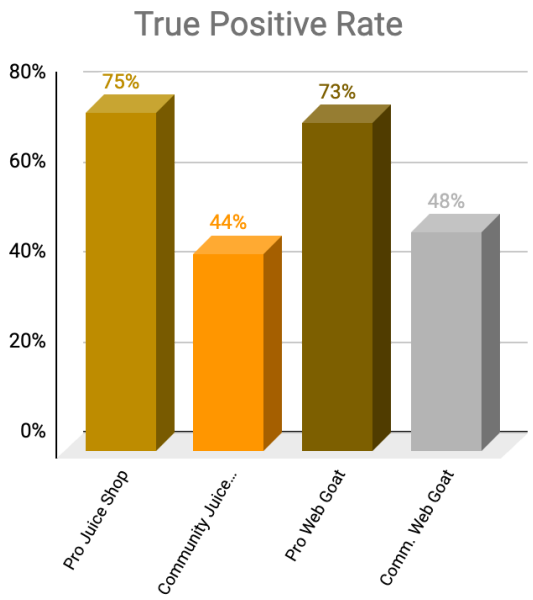
WebGoat has about 185 total sections in the lessons, but it doesn't state the total number of TP and FN one could find. The number believed to be less than one per section and around 33 unique detectable issues exist. This is because many of the lessons are not actual vulnerabilities, either because they are reading exercises, simple questions, mockups of vulnerabilities (e.g., string matching an attacker's input) or things a SAST tool can't be realistically expected to find, either generally or specifically in the modes of operation tested here.

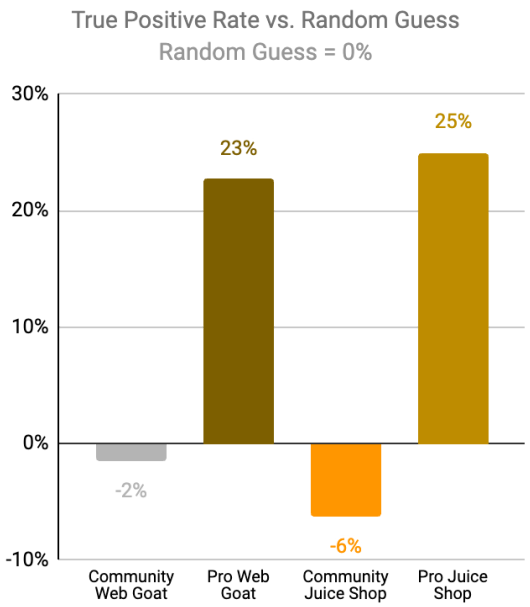
Juice Shop lists 106 challenge solutions. After analyzing the challenges, we determined 48 of those were the types of vulnerabilities that a SAST tool should be capable of detecting, without context-specific customization. We'll use that as the upper bound, which shifts the absolute *true positive rate* (TPR) values. Ultimately, the relative values are what we're looking to compare.

Using the above information as our basis for evaluation, the data presented below describes our results. In short, a 24% improvement in the TPR was observed when scanning the Web Goat project with the Pro mode (engine) with both the Community and Pro rules, compared to the Community version (engine and rules) alone. The results for Juice Shop were similar, resulting in a 31% increase in the TPR from the Pro mode scan.

The summary of these findings is therefore that the TPR shows notable improvement when using the Pro engine with the Pro and Community rules, over just the Community rules with the Community engine.

Tool Mode / Library	TP	DUP TPs	FN (TOTAL-TP)	TPR (TP/(TP+FN)
Community/ Web Goat	16	7	17	16/(16+17)=48%
Pro/ Web Goat	24	43	9	24/(24+9)=72%
Community/ Juice Shop	21	3	27	21/(21+27)=44%
Pro/ Juice Shop	36	8	12	36/(36+12)=75%





THE COMMUNITY RULES AND ENGINE ALONE FAILED TO DETECT A MAJORITY OF THE TOTAL VULNERABILITIES. THE PRO MODE, WHEN USING COMMUNITY AND PRO RULES TOGETHER, RESULTED IN NOTABLY IMPROVED TRUE POSITIVE RATES. YET, A FEW VULNERABILITIES ARE NOT DETECTED BY EITHER OF THOSE ENGINES/RULES.

As this project was focused on comparing these two versions of the Semgrep software and we weren't using contrived test cases (like in the OWASP benchmark), coming up with the list of true

negatives (TN) is effectively impossible without performing a full code review. That said, a relative value could be determined. This would allow for calculating the relative *false positive rate* (FPR = FP/(FP+TN)).

In theory, all test cases which aren't known to contain a vulnerability and are not flagged as having one (incorrectly) are "true negatives" (TN). If the total number of test cases (TT) is known and the TP is known, then TN = TT-TP. Then it is necessary to define a test case, when dealing with software that wasn't constructed specifically for this type of testing.

OWASP's Benchmark tool uses purpose-built test cases, where each file is considered a test case. Therefore, each file is assumed to either contain one vulnerability or none - there is nothing in the middle. However, in the real world, a file could contain multiple vulnerabilities, even in the same function or same line of code, so determining the "unit" of a test case becomes problematic. Additionally, it's necessary to define which files should be included. For example, adding a bunch of additional files where causing a vulnerability is impossible (e.g., a README) would inappropriately skew the FPR.

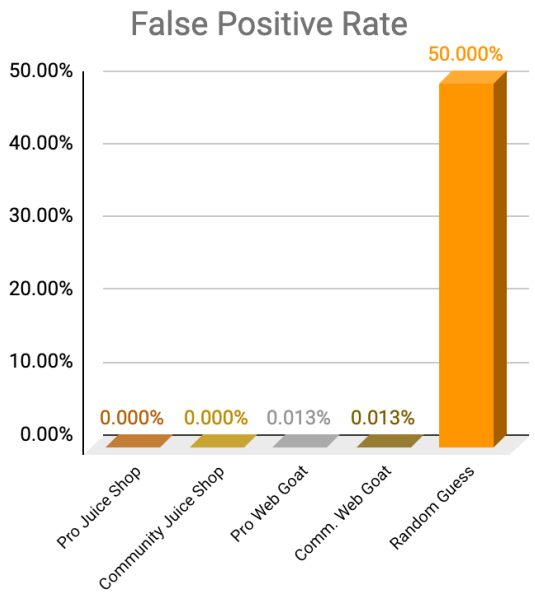
While most commonly vulnerabilities are thought of as being tied to executing a function with user-controlled data, many don't meet this criteria (e.g., insecure configuration, cryptographic issues). The broadest definition would probably be broadly "anything that could potentially create a vulnerability", which creates a nearly infinite number of possibilities. So a choice must be made as to where to draw the line.

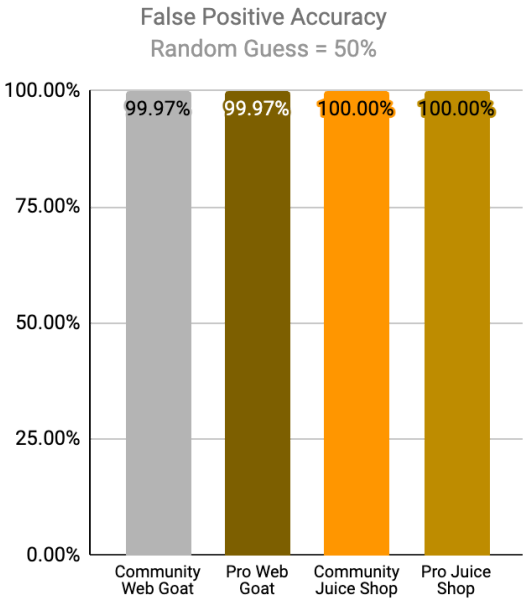
Since both versions of the tool found multiple vulnerabilities in the same file in some cases, but never multiple on the same line, a lined-based count of the total "test cases" (i.e., total lines, subtracting comments and only counting a line once) seemed the most practical choice. The files were limited to those where vulnerabilities were found/expected (i.e., our self-defined scope) and include the following the *src/main/java/org/owasp/webgoat/lessons/* directory and the *src/main/resources/webgoat/static/js/quiz.js* file. These contain 7955 and 47 lines of code respectively, resulting in a total of 8002 lines.

For the Juice Shop tests, there were no FPs, so the FPR is zero. For Web Goat there was one FP, so our formula becomes FPR = FP/(1+FP) = 1/(1+TN) = 1/(1+TT-TP) = 1/(1+8002-TP). For the Community version the FPR is therefore 1/(1+8002-16) = 1/7987 (.013%) and the FPR for the Pro version is 1/(1+8002-24)= 1/7979 (.013%), which is effectively the same (after rounding).

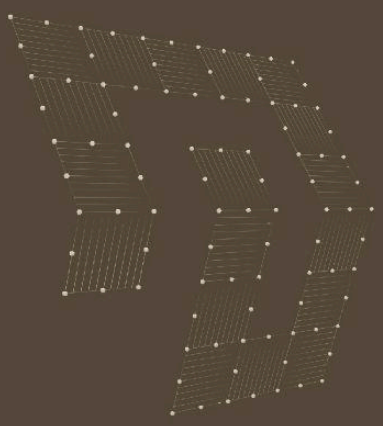
While problematic, as previously discussed, there are 175 files if the file count option is chosen instead. This would have resulted in FPR = 1/(1+175-16) = 1/160 = .63% for the Community version and 1/(1+175-24) = 1/152 = .66% for the Pro version. In summary, the results are the same for most practical purposes, regardless of the approach taken from our available options. We strongly caution that any comparison of these values must be **only** done with analysis using the same approach.

Due to the fact that the FPR measured during our analysis was so low, in the second graph below we are attempting to make this more readable by showing the accuracy of the positives instead, where 100% represents no false positives and 50% would be the odds for a random guess.


False Positive Rate
50.00%
40.00%
30.00%
20.00%
10.00%
0.00%
0.000%
0.000%
0.013%
0.013%
50.000%
Pro Juice Shop
Community Juice Shop
Pro Web Goat
Comm. Web Goat
Random Guess


False Positive Accuracy
Random Guess = 50%
100.00%
75.00%
50.00%
25.00%
0.00%
99.97%
99.97%
100.00%
100.00%
Community Web Goat
Pro Web Goat
Community Juice Shop
Pro Juice Shop

CONCLUSIONS



CONCLUSIONS

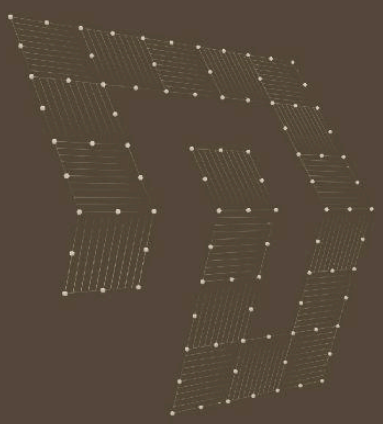
The key takeaway from our examination was that if our results can be replicated when testing real-world applications, an experienced AppSec engineer would benefit from enabling the Pro engine and running the Pro rules alongside the Community rules in Semgrep.

The main benefits observed were:

- Pro mode can increase (valid) findings due to how the inter-file analysis works
- Using Pro mode, with the Community and Pro rules together, provides most actionable findings, once they are de-duplicated and combined
- Using Pro mode, with the Community and Pro rules together provides notable improvements in the True Positive Rates

That said, to save time triaging findings, care should be taken to reduce the directories being scanned and to not use rules that can be considered duplicates, particularly once trusted rules have been identified. The latter aspect could potentially be improved by the vendor maintaining a merged ruleset that would correlate and de-duplicate rules. Additionally, improvements in both engines and rules might help both tools in reducing the number of false negatives.

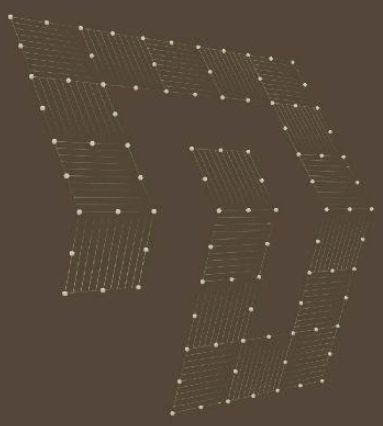
ABOUT THIS RESEARCH



ABOUT THIS RESEARCH

This research is based upon work financially supported by Semgrep. Despite that, Doyensec had complete freedom on the research execution and publication. While Semgrep had the right to decide on whether to publish the effort in its entirety or just citing parts according to our Citation Guideline, under no circumstances has Doyensec adjusted the results represented in this publication or the publication itself.

APPENDIX



APPENDIX

a. Raw scan results
   i. Web Goat Community Scan

File	LoC	Matched Check ID
docs/index.html	7	html.security.audit.missing-integrity.missing-integrity
robot/goat.robot	116	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/java/org/owasp/webgoat/container/service/LabelDebugService.java	64	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/container/service/LabelDebugService.java	77	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/container/service/LessonMenuService.java	73	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/container/service/SessionService.java	24	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/lessons/challenges/challenge1/ImageServlet.java	17	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/challenges/challenge5/Assignment5.java	63	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/challenges/challenge5/Assignment5.java	68	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/cryptography/EncodingAssignment.java	55	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/cryptography/EncodingAssignment.java	57	java.lang.security.audit.tainted-session-from-http-request.tainted-session-from-http-request
src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java	48	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java	55	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java	57	java.lang.security.audit.crypto.use-of-md5.use-of-md5
src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java	67	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java	73	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/cryptography/SigningAssignment.java	55	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/lessons/deserialization/InsecureDeserializationTask.java	60	java.lang.security.audit.object-deserialization.object-deserialization
src/main/java/org/owasp/webgoat/lessons/deserialization/SerializationHelper.java	18	java.lang.security.audit.object-deserialization.object-deserialization
src/main/java/org/owasp/webgoat/lessons/hijacksession/HijackSessionAssignment.java	94	java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/hijacksession/cas/HijackSessionAuthenticationProvider.java	48	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/jwt/JWTSecretKeyEndpoint.java	56	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/jwt/JWTSecretKeyEndpoint.java	61	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	132	java.servlets.security.cookie-issecure-false.cookie-issecure-false
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	133	java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	133	java.lang.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	137	java.servlets.security.cookie-issecure-false.cookie-issecure-false
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	138	java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.j	138	java.lang.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag

File	LoC	Matched Check ID
ava		
src/main/java/org/owasp/webgoat/lessons/jwt/claimmisuse/JWTHeaderJKUEndpoint.java	53	java.spring.security.injection.tainted-url-host.tainted-url-host
src/main/java/org/owasp/webgoat/lessons/pathtraversal/ProfileUploadRetrieval.java	96	java.lang.security.httpservlet-path-traversal.httpservlet-path-traversal
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	83	java.servlets.security.cookie-issecure-false.cookie-issecure-false
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	85	java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	85	java.lang.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	102	java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionChallenge.java	70	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionChallenge.java	72	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionChallenge.java	72	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson10.java	74	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson10.java	74	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson2.java	67	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5a.java	70	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5b.java	87	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	80	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	80	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	160	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	160	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java	83	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java	83	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java	112	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/mitigation/Servers.java	73	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/xxe/SimpleXXE.java	95	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/webwolf/FileServer.java	74	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/webwolf/FileServer.java	97	java.spring.security.injection.tainted-file-path.tainted-file-path
src/main/resources/lessons/authbypass/html/AuthBypass.html	23	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/authbypass/html/AuthBypass.html	43	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge1.html	18	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge1.html	40	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge5.html	69	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge6.html	102	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge7.html	60	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge8.html	234	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/chromedevtools/html/ChromeDevTools.html	25	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/chromedevtools/html/ChromeDevTools	46	python.django.security.django-no-csrf-token.django-no-csrf-token

File	LoC	Matched Check ID
.html		
src/main/resources/lessons/chromedevtools/html/ChromeDevTools.html	67	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/cia/html/CIA.html	30	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/clientsidefiltering/html/ClientSideFiltering.html	96	html.security.plaintext-http-link.plaintext-http-link
src/main/resources/lessons/clientsidefiltering/js/clientSideFiltering.js	6	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/lessons/clientsidefiltering/js/clientSideFiltering.js	38	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/lessons/cryptography/html/Cryptography.html	31	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/cryptography/html/Cryptography.html	48	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/cryptography/html/Cryptography.html	65	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/cryptography/html/Cryptography.html	90	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/cryptography/html/Cryptography.html	113	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/csrf/html/CSRF.html	16	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/csrf/html/CSRF.html	35	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/csrf/html/CSRF.html	93	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/csrf/html/CSRF.html	213	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/csrf/html/CSRF.html	237	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/deserialization/html/InsecureDeserialization.html	26	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/hijacksession/html/HijackSession.html	5	html.security.audit.missing-integrity.missing-integrity
src/main/resources/lessons/hijacksession/templates/hijackform.html	3	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/httpbasics/html/HttpBasics.html	26	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/httpproxies/html/HttpProxies.html	25	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/idor/html/IDOR.html	23	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/idor/html/IDOR.html	81	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/idor/html/IDOR.html	108	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/insecurelogin/html/InsecureLogin.html	18	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/insecurelogin/html/InsecureLogin.html	26	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/jwt/documentation/JWT_decode.adoc	8	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries.adoc	28	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries.adoc	40	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries.adoc	56	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries_assignment.adoc	7	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries_assignment2.adoc	7	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries_solution.adoc	7	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_signing_solution.adoc	35	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_signing_solution.adoc	77	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/html/JWT.html	20	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/jwt/html/JWT.html	125	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/jwt/html/JWT.html	158	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/jwt/html/JWT.html	323	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/html/JWT.html	389	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/images/logs.txt	2	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/lessontemplate/html/LessonTemplate.	48	python.django.security.django-no-csrf-token.django-no-csrf-token

File	LoC	Matched Check ID
html		
src/main/resources/lessons/logging/html/LogSpoofing.html	17	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/logging/html/LogSpoofing.html	39	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/missingac/html/MissingFunctionAC.html	53	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/missingac/html/MissingFunctionAC.html	76	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/missingac/html/MissingFunctionAC.html	98	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/passwordreset/html/PasswordReset.html	144	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/passwordreset/templates/password_reset.html	12	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/pathtraversal/html/PathTraversal.html	192	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/securepasswords/html/SecurePasswords.html	21	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/spoofcookie/html/SpoofCookie.html	5	html.security.audit.missing-integrity.missing-integrity
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	16	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	40	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	64	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	88	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	189	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	217	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	245	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	274	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionAdvanced.html	21	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionAdvanced.html	34	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionAdvanced.html	169	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html	26	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html	45	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html	73	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html	96	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html	176	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/ssrf/html/SSRF.html	13	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/ssrf/html/SSRF.html	35	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/vulnerablecomponents/html/VulnerableComponents.html	5	html.security.audit.missing-integrity.missing-integrity
src/main/resources/lessons/vulnerablecomponents/html/VulnerableComponents.html	104	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/webwolfintroduction/html/WebWolfIntroduction.html	19	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/webwolfintroduction/html/WebWolfIntroduction.html	40	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/webwolfintroduction/html/WebWolfIntroduction.html	77	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScripting.html	13	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScripting.html	134	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScripting.html	149	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScripting.html	169	python.django.security.django-no-csrf-token.django-no-csrf-token

File	LoC	Matched Check ID
src/main/resources/lessons/xss/html/CrossSiteScriptingMitigation.html	24	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScriptingMitigation.html	44	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScriptingStored.html	68	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/webgoat/static/js/libs/backbone-min.js	1	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/mode-java.js	573	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/mode-java.js	576	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.prototype-pollution.prototype-pollution-loop.prototype-pollution-loop
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.prototype-pollution.prototype-pollution-loop.prototype-pollution-loop
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/quiz.js	34	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	843	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	1189	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	1206	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	4011	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	4079	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	4088	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	4354	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	4391	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	5999	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	6202	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	6695	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	7940	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	7962	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	8056	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/templates/login.html	31	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/webwolf/templates/files.html	32	python.django.security.django-no-csrf-token.django-no-csrf-token

ii. Web Goat Pro Scan

File	LoC	Matched Check ID
.mvn/wrapper/MavenWrapperDownloader.java	92	java.lang.security.audit.active-debug-code-printstacktrace.active-debug-code-printstacktrace
robot/goat.robot	116	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/it/java/org/owasp/webgoat/CryptoIntegrationTest.java	32	java.lang.security.audit.active-debug-code-printstacktrace.active-debug-code-printstacktrace

File	LoC	Matched Check ID
src/it/java/org/owasp/webgoat/CryptoIntegrationTest.java	39	java.lang.security.audit.active-debug-code-printstacktrace.active-debug-code-printstacktrace
src/it/java/org/owasp/webgoat/LabelAndHintIntegrationTest.java	170	java.lang.security.audit.active-debug-code-printstacktrace.active-debug-code-printstacktrace
src/main/java/org/owasp/webgoat/container/service/LabelDebugService.java	64	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/container/service/LabelDebugService.java	77	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/container/service/LessonMenuService.java	73	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/container/service/SessionService.java	24	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/container/users/UserService.java	52	java.spring.security.audit.spring-sqli.spring-sqli
src/main/java/org/owasp/webgoat/lessons/challenges/challenge1/ImageServlet.java	17	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/challenges/challenge5/Assignment5.java	63	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/challenges/challenge5/Assignment5.java	68	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/cryptography/EncodingAssignment.java	55	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/cryptography/EncodingAssignment.java	57	java.lang.security.audit.tainted-session-from-http-request.tainted-session-from-http-request
src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java	48	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java	55	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java	57	java.lang.security.audit.crypto.use-of-md5.use-of-md5
src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java	67	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/lessons/cryptography/HashingAssignment.java	73	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/cryptography/SigningAssignment.java	55	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/lessons/deserialization/InsecureDeserializationTask.java	60	java.lang.security.audit.object-deserialization.object-deserialization
src/main/java/org/owasp/webgoat/lessons/deserialization/InsecureDeserializationTask.java	61	java.spring.security.objectinputstream-deserialization-spring.objectinputstream-deserialization-spring
src/main/java/org/owasp/webgoat/lessons/deserialization/SerializationHelper.java	18	java.lang.security.audit.object-deserialization.object-deserialization
src/main/java/org/owasp/webgoat/lessons/hijacksession/HijackSessionAssignment.java	94	java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/hijacksession/HijackSessionAssignment.java	94	java.servlets.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/hijacksession/HijackSessionAssignment.java	94	java.servlets.security.audit.cookie-missing-samesite.cookie-missing-samesite
src/main/java/org/owasp/webgoat/lessons/hijacksession/cas/HijackSessionAuthenticationProvider.java	48	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/jwt/JWTSecretKeyEndpoint.java	56	java.lang.security.audit.crypto.weak-random.weak-random
src/main/java/org/owasp/webgoat/lessons/jwt/JWTSecretKeyEndpoint.java	61	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	132	java.servlets.security.cookie-issecure-false.cookie-issecure-false
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	133	java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	133	java.lang.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	133	java.servlets.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.j	133	java.servlets.security.audit.cookie-missing-samesite.cookie-missing-samesite

File	LoC	Matched Check ID
ava		
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	133	java.servlets.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	137	java.servlets.security.cookie-issecure-false.cookie-issecure-false
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	138	java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	138	java.lang.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	138	java.servlets.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	138	java.servlets.security.audit.cookie-missing-samesite.cookie-missing-samesite
src/main/java/org/owasp/webgoat/lessons/jwt/JWTVotesEndpoint.java	138	java.servlets.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag
src/main/java/org/owasp/webgoat/lessons/jwt/claimmisuse/JWTHeaderJKUEndpoint.java	53	java.spring.security.injection.tainted-url-host.tainted-url-host
src/main/java/org/owasp/webgoat/lessons/passwordreset/SecurityQuestionAssignment.java	105	java.spring.tainted-html-string-responsebody.tainted-html-string-responsebody
src/main/java/org/owasp/webgoat/lessons/pathtraversal/ProfileUploadBase.java	66	java.spring.spring-tainted-path-traversal.spring-tainted-path-traversal
src/main/java/org/owasp/webgoat/lessons/pathtraversal/ProfileUploadBase.java	99	java.spring.spring-tainted-path-traversal.spring-tainted-path-traversal
src/main/java/org/owasp/webgoat/lessons/pathtraversal/ProfileUploadBase.java	108	java.spring.spring-tainted-path-traversal.spring-tainted-path-traversal
src/main/java/org/owasp/webgoat/lessons/pathtraversal/ProfileUploadRetrieval.java	96	java.lang.security.httpservlet-path-traversal.httpservlet-path-traversal
src/main/java/org/owasp/webgoat/lessons/pathtraversal/ProfileUploadRetrieval.java	96	java.servlets.security.httpservlet-path-traversal.httpservlet-path-traversal
src/main/java/org/owasp/webgoat/lessons/pathtraversal/ProfileZipSlip.java	75	java.spring.security.injection.tainted-file-path.tainted-file-path
src/main/java/org/owasp/webgoat/lessons/pathtraversal/ProfileZipSlip.java	75	java.spring.spring-tainted-path-traversal.spring-tainted-path-traversal
src/main/java/org/owasp/webgoat/lessons/pathtraversal/ProfileZipSlip.java	75	java.spring.spring-tainted-path-traversal.spring-tainted-path-traversal
src/main/java/org/owasp/webgoat/lessons/securepasswords/SecurePasswordsAssignment.java	93	java.spring.tainted-html-string-responsebody.tainted-html-string-responsebody
src/main/java/org/owasp/webgoat/lessons/securepasswords/SecurePasswordsAssignment.java	94	java.spring.tainted-html-string-responsebody.tainted-html-string-responsebody
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	83	java.servlets.security.cookie-issecure-false.cookie-issecure-false
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	85	java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	85	java.lang.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	85	java.servlets.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	85	java.servlets.security.audit.cookie-missing-samesite.cookie-missing-samesite
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	85	java.servlets.security.audit.cookie-missing-secure-flag.cookie-missing-secure-flag
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	102	java.lang.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	102	java.servlets.security.audit.cookie-missing-httponly.cookie-missing-httponly
src/main/java/org/owasp/webgoat/lessons/spoofcookie/SpoofCookieAssignment.java	102	java.servlets.security.audit.cookie-missing-samesite.cookie-missing-samesite
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionChallenge.java	70	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionChallenge.java	72	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/S	72	java.lang.security.audit.formatted-sql-string.formatted-sql-string

File	LoC	Matched Check ID
qlInjectionChallenge.java		
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionChallenge.java	72	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionChallenge.java	72	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionLesson6a.java	72	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionLesson6a.java	90	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionLesson6a.java	90	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionLesson6a.java	90	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionLesson6b.java	73	java.lang.security.audit.active-debug-code-printstacktrace.active-debug-code-printstacktrace
src/main/java/org/owasp/webgoat/lessons/sqlinjection/advanced/SqlInjectionLesson6b.java	77	java.lang.security.audit.active-debug-code-printstacktrace.active-debug-code-printstacktrace
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson10.java	67	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson10.java	74	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson10.java	74	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson10.java	74	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson10.java	74	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson2.java	67	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson2.java	67	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson2.java	67	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson3.java	65	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson3.java	65	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson4.java	64	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson4.java	64	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5.java	83	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5.java	83	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5a.java	66	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5a.java	70	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5a.java	70	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5a.java	70	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5b.java	63	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5b.java	67	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5b.java	67	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson5b.java	87	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction	68	java.spring.security.injection.tainted-sql-string.tainted-sql-string

File	LoC	Matched Check ID
/SqlInjectionLesson8.java		
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	80	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	80	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	80	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	80	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	156	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	160	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	160	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	160	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson8.java	160	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java	69	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java	83	java.lang.security.audit.formatted-sql-string-deepsemgrep.formatted-sql-string-deepsemgrep
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java	83	java.lang.security.audit.formatted-sql-string.formatted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java	83	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java	83	java.spring.security.java-sql-sqli.java-sql-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/introduction/SqlInjectionLesson9.java	112	java.lang.security.audit.sqli.jdbc-sqli.jdbc-sqli
src/main/java/org/owasp/webgoat/lessons/sqlinjection/mitigation/Servers.java	73	java.spring.security.injection.tainted-sql-string.tainted-sql-string
src/main/java/org/owasp/webgoat/lessons/sqlinjection/mitigation/SqlInjectionLesson10b.java	133	java.lang.security.audit.active-debug-code-printstacktrace.active-debug-code-printstacktrace
src/main/java/org/owasp/webgoat/lessons/ssrf/SSRFTask1.java	65	java.lang.security.audit.active-debug-code-printstacktrace.active-debug-code-printstacktrace
src/main/java/org/owasp/webgoat/lessons/ssrf/SSRFTask2.java	54	java.spring.security.injection.tainted-url-host.tainted-url-host
src/main/java/org/owasp/webgoat/lessons/ssrf/SSRFTask2.java	54	java.spring.security.tainted-ssrf-spring-add.tainted-ssrf-spring-add
src/main/java/org/owasp/webgoat/lessons/xss/CrossSiteScriptingLesson5a.java	97	java.spring.tainted-html-string-responsebody.tainted-html-string-responsebody
src/main/java/org/owasp/webgoat/lessons/xss/CrossSiteScriptingLesson5a.java	102	java.spring.tainted-html-string-responsebody.tainted-html-string-responsebody
src/main/java/org/owasp/webgoat/lessons/xss/CrossSiteScriptingLesson5a.java	107	java.spring.tainted-html-string-responsebody.tainted-html-string-responsebody
src/main/java/org/owasp/webgoat/lessons/xxe/Ping.java	50	java.spring.spring-tainted-path-traversal.spring-tainted-path-traversal
src/main/java/org/owasp/webgoat/lessons/xxe/SimpleXXE.java	95	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/webwolf/FileServer.java	74	java.spring.security.unrestricted-request-mapping.unrestricted-request-mapping
src/main/java/org/owasp/webgoat/webwolf/FileServer.java	97	java.spring.security.injection.tainted-file-path.tainted-file-path
src/main/java/org/owasp/webgoat/webwolf/FileServer.java	97	java.spring.spring-tainted-path-traversal.spring-tainted-path-traversal
src/main/resources/lessons/authbypass/html/AuthBypass.html	23	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/authbypass/html/AuthBypass.html	43	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge1.html	18	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge1.html	40	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge5.html	69	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge6.html	102	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge7.html	60	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/challenges/html/Challenge8.html	234	python.django.security.django-no-csrf-token.django-no-csrf-token

File	LoC	Matched Check ID
src/main/resources/lessons/chromedevtools/html/ChromeDevTools.html	25	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/chromedevtools/html/ChromeDevTools.html	46	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/chromedevtools/html/ChromeDevTools.html	67	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/cia/html/CIA.html	30	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/clientsidefiltering/html/ClientSideFiltering.html	96	html.security.plaintext-http-link.plaintext-http-link
src/main/resources/lessons/clientsidefiltering/js/clientSideFiltering.js	6	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/lessons/clientsidefiltering/js/clientSideFiltering.js	38	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/lessons/cryptography/html/Cryptography.html	31	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/cryptography/html/Cryptography.html	48	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/cryptography/html/Cryptography.html	65	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/cryptography/html/Cryptography.html	90	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/cryptography/html/Cryptography.html	113	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/csrf/html/CSRF.html	16	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/csrf/html/CSRF.html	35	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/csrf/html/CSRF.html	93	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/csrf/html/CSRF.html	213	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/csrf/html/CSRF.html	237	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/deserialization/html/InsecureDeserialization.html	26	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/hijacksession/html/HijackSession.html	5	html.security.audit.missing-integrity.missing-integrity
src/main/resources/lessons/hijacksession/templates/hijackform.html	3	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/httpbasics/html/HttpBasics.html	26	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/httpproxies/html/HttpProxies.html	25	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/idor/html/IDOR.html	23	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/idor/html/IDOR.html	81	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/idor/html/IDOR.html	108	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/insecurelogin/html/InsecureLogin.html	18	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/insecurelogin/html/InsecureLogin.html	26	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/jwt/documentation/JWT_decode.adoc	8	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries.adoc	28	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries.adoc	40	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries.adoc	56	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries_assignment.adoc	7	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries_assignment2.adoc	7	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_libraries_solution.adoc	7	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_signing_solution.adoc	35	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/documentation/JWT_signing_solution.adoc	77	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/html/JWT.html	20	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/jwt/html/JWT.html	125	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/jwt/html/JWT.html	158	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/jwt/html/JWT.html	323	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/jwt/html/JWT.html	389	generic.secrets.security.detected-jwt-token.detected-jwt-token

File	LoC	Matched Check ID
src/main/resources/lessons/jwt/images/logs.txt	2	generic.secrets.security.detected-jwt-token.detected-jwt-token
src/main/resources/lessons/lessontemplate/html/LessonTemplate.html	48	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/logging/html/LogSpoofing.html	17	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/logging/html/LogSpoofing.html	39	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/missingac/html/MissingFunctionAC.html	53	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/missingac/html/MissingFunctionAC.html	76	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/missingac/html/MissingFunctionAC.html	98	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/passwordreset/html/PasswordReset.html	144	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/passwordreset/templates/password_reset.html	12	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/pathtraversal/html/PathTraversal.html	192	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/securepasswords/html/SecurePasswords.html	21	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/spoofcookie/html/SpoofCookie.html	5	html.security.audit.missing-integrity.missing-integrity
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	16	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	40	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	64	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	88	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	189	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	217	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	245	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjection.html	274	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionAdvanced.html	21	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionAdvanced.html	34	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionAdvanced.html	169	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html	26	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html	45	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html	73	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html	96	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/sqlinjection/html/SqlInjectionMitigations.html	176	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/ssrf/html/SSRF.html	13	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/ssrf/html/SSRF.html	35	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/vulnerablecomponents/html/VulnerableComponents.html	5	html.security.audit.missing-integrity.missing-integrity
src/main/resources/lessons/vulnerablecomponents/html/VulnerableComponents.html	104	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/webwolfintroduction/html/WebWolfIntroduction.html	19	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/webwolfintroduction/html/WebWolfIntroduction.html	40	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/webwolfintroduction/html/WebWolfIntroduction.html	77	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScripting.html	13	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScripting.html	134	python.django.security.django-no-csrf-token.django-no-csrf-token

File	LoC	Matched Check ID
src/main/resources/lessons/xss/html/CrossSiteScripting.html	149	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScripting.html	169	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScriptingMitigation.html	24	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScriptingMitigation.html	44	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/lessons/xss/html/CrossSiteScriptingStored.html	68	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/webgoat/static/js/libs/ace.js	1740	javascript.browser.security.wildcard-postmessage-configuration.wildcard-postmessage-configuration
src/main/resources/webgoat/static/js/libs/ace.js	3500	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/js/libs/ace.js	4491	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	4491	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	5475	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/js/libs/ace.js	6291	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	6343	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	6429	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	6429	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	6429	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	9471	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	9471	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	9807	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	9859	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	11797	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	11808	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	11808	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/ace.js	17320	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/js/libs/ace.js	17409	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/js/libs/ace.js	21176	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/js/libs/ace.js	21469	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/js/libs/backbone-min.js	1	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/jquery-ui-1.10.4.js	622	javascript.lang.security.audit.prototype-pollution.prototype-pollution-loop.prototype-pollution-loop
src/main/resources/webgoat/static/js/libs/jquery-ui-1.10.4.js	7171	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/jquery-ui-1.10.4.js	7171	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/jquery-ui-1.10.4.js	11639	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/jquery-ui-1.10.4.js	11651	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/mode-java.js	573	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/mode-java.js	576	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.prototype-pollution.prototype-pollution-loop.prototype-pollution-loop
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.prototype-pollution.prototype-pollution-loop.prototype-pollution-loop
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/libs/underscore-min.js	6	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/js/quiz.js	34	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	843	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	1189	javascript.browser.security.insecure-document-method.insecure-document-method

File	LoC	Matched Check ID
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	1206	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	4011	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	4079	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	4088	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	4354	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	4391	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	5999	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	6202	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	6695	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	7940	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	7962	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/static/plugins/bootstrap-wysihtml5/js/wysihtml5-0.3.0.js	8056	javascript.browser.security.insecure-document-method.insecure-document-method
src/main/resources/webgoat/templates/login.html	31	python.django.security.django-no-csrf-token.django-no-csrf-token
src/main/resources/webwolf/templates/files.html	32	python.django.security.django-no-csrf-token.django-no-csrf-token

iii. Juice Shop Community Scan

File	LoC	Matched Check ID
data/static/codefixes/dbSchemaChallenge_1.ts	5	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
data/static/codefixes/dbSchemaChallenge_1.ts	5	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
data/static/codefixes/dbSchemaChallenge_3.ts	11	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
data/static/codefixes/dbSchemaChallenge_3.ts	11	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
data/static/codefixes/restfulXssChallenge_2.ts	59	javascript.audit.detect-replaceall-sanitization.detect-replaceall-sanitization
data/static/codefixes/restfulXssChallenge_2.ts	59	javascript.audit.detect-replaceall-sanitization.detect-replaceall-sanitization
data/static/codefixes/unionSqlInjectionChallenge_1.ts	6	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
data/static/codefixes/unionSqlInjectionChallenge_1.ts	6	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
data/static/codefixes/unionSqlInjectionChallenge_3.ts	10	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
data/static/codefixes/unionSqlInjectionChallenge_3.ts	10	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
data/static/users.yml	150	generic.secrets.security.detected-generic-secret.detected-generic-secret
data/staticData.ts	7	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
frontend/src/app/app.guard.spec.ts	40	generic.secrets.security.detected-jwt-token.detected-jwt-token
frontend/src/app/last-login-ip/last-login-ip.component.spec.ts	50	generic.secrets.security.detected-jwt-token.detected-jwt-token
frontend/src/app/last-login-ip/last-login-ip.component.spec.ts	56	generic.secrets.security.detected-jwt-token.detected-jwt-token
frontend/src/hacking-instructor/helpers/helpers.ts	38	javascript.lang.security.audit.prototype-pollution.prototype-pollution-loop.prototype-pollution-loop
frontend/src/hacking-instructor/index.ts	111	javascript.browser.security.insecure-document-method.insecure-document-method
frontend/src/index.html	14	html.security.audit.missing-integrity.missing-integrity
frontend/src/index.html	15	html.security.audit.missing-integrity.missing-integrity
frontend/src/index.html	16	html.security.audit.missing-integrity.missing-integrity

File	LoC	Matched Check ID
lib/codingChallenges.ts	24	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
lib/codingChallenges.ts	24	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
lib/codingChallenges.ts	76	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
lib/codingChallenges.ts	78	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
lib/insecurity.ts	44	javascript.lang.security.audit.hardcoded-hmac-key.hardcoded-hmac-key
lib/insecurity.ts	56	javascript.jsonwebtoken.security.jwt-hardcode.hardcoded-jwt-secret
lib/insecurity.ts	152	javascript.lang.security.audit.hardcoded-hmac-key.hardcoded-hmac-key
lib/startup/restoreOverwrittenFilesWithOriginals.ts	28	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
lib/startup/validatePreconditions.ts	120	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/b2bOrder.ts	22	javascript.express.security.audit.express-detect-notevil-usage.express-detect-notevil-usage
routes/captcha.ts	23	javascript.browser.security.eval-detected.eval-detected
routes/chatbot.ts	198	javascript.express.security.injection.raw-html-format.raw-html-format
routes/dataErasure.ts	69	javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-traversal
routes/dataErasure.ts	69	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/fileServer.ts	33	javascript.express.security.audit.express-res-sendfile.express-res-sendfile
routes/fileServer.ts	33	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/fileUpload.ts	29	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/fileUpload.ts	39	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/fileUpload.ts	80	javascript.express.security.audit.express-libxml-vm-noent.express-libxml-vm-noent
routes/keyServer.ts	14	javascript.express.security.audit.express-res-sendfile.express-res-sendfile
routes/keyServer.ts	14	javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-traversal
routes/keyServer.ts	14	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/logfileServer.ts	14	javascript.express.security.audit.express-res-sendfile.express-res-sendfile
routes/logfileServer.ts	14	javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-traversal
routes/logfileServer.ts	14	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/login.ts	36	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
routes/login.ts	36	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
routes/order.ts	45	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/profileImageUrlUpload.ts	23	javascript.express.security.audit.express-ssrf.express-ssrf
routes/quarantineServer.ts	14	javascript.express.security.audit.express-res-sendfile.express-res-sendfile
routes/quarantineServer.ts	14	javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-traversal
routes/quarantineServer.ts	14	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/redirect.ts	19	javascript.express.security.audit.express-open-redirect.express-open-redirect
routes/search.ts	23	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
routes/search.ts	23	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
routes/userProfile.ts	36	javascript.browser.security.eval-detected.eval-detected
routes/userProfile.ts	56	javascript.express.security.express-insecure-template-usage.express-insecure-template-usage

File	LoC	Matched Check ID
routes/videoHandler.ts	57	javascript.lang.security.audit.unknown-value-with-script-tag.unknown-value-with-script-tag
routes/videoHandler.ts	69	javascript.lang.security.audit.unknown-value-with-script-tag.unknown-value-with-script-tag
server.ts	105	javascript.express.security.audit.express-check-csurf-middleware-usage.express-check-csurf-middleware-usage
server.ts	148	javascript.lang.security.audit.unsafe-formatstring.unsafe-formatstring
server.ts	260	javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
server.ts	264	javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
server.ts	268	javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
server.ts	272	javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
views/promotionVideo.pug	79	javascript.express.security.audit.xss.pug.explicit-unescape.template-explicit-unescape

iv. Juice Shop Pro Scan

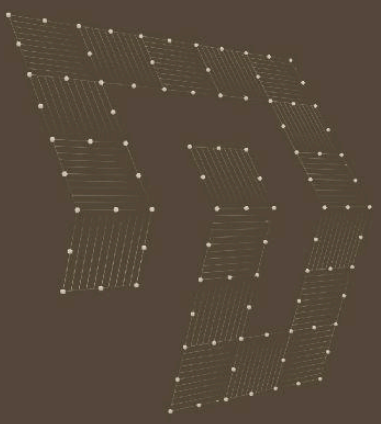
File	LoC	Matched Check ID
data/static/codefixes/dbSchemaChallenge_1.ts	5	javascript.express.db.sequelize-express.sequelize-express
data/static/codefixes/dbSchemaChallenge_1.ts	5	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
data/static/codefixes/dbSchemaChallenge_1.ts	5	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
data/static/codefixes/dbSchemaChallenge_3.ts	11	javascript.express.db.sequelize-express.sequelize-express
data/static/codefixes/dbSchemaChallenge_3.ts	11	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
data/static/codefixes/dbSchemaChallenge_3.ts	11	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
data/static/codefixes/restfulXssChallenge_2.ts	59	javascript.audit.detect-replaceall-sanitization.detect-replaceall-sanitization
data/static/codefixes/restfulXssChallenge_2.ts	59	javascript.audit.detect-replaceall-sanitization.detect-replaceall-sanitization
data/static/codefixes/unionSqlInjectionChallenge_1.ts	6	javascript.express.db.sequelize-express.sequelize-express
data/static/codefixes/unionSqlInjectionChallenge_1.ts	6	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
data/static/codefixes/unionSqlInjectionChallenge_1.ts	6	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
data/static/codefixes/unionSqlInjectionChallenge_3.ts	10	javascript.express.db.sequelize-express.sequelize-express
data/static/codefixes/unionSqlInjectionChallenge_3.ts	10	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
data/static/codefixes/unionSqlInjectionChallenge_3.ts	10	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
data/static/users.yml	150	generic.secrets.security.detected-generic-secret.detected-generic-secret
data/staticData.ts	7	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
frontend/src/app/app.guard.spec.ts	40	generic.secrets.security.detected-jwt-token.detected-jwt-token
frontend/src/app/last-login-ip/last-login-ip.component.spec.ts	50	generic.secrets.security.detected-jwt-token.detected-jwt-token
frontend/src/app/last-login-ip/last-login-ip.component.spec.ts	56	generic.secrets.security.detected-jwt-token.detected-jwt-token
frontend/src/app/search-result/search-result.component.ts	151	typescript.angular.angular-route-bypass-security-trust.angular-route-bypass-security-trust
frontend/src/assets/private/three.js	11375	javascript.browser.security.insecure-document-method.insecure-document-method
frontend/src/hacking-instructor/helpers/helpers.ts	38	javascript.lang.security.audit.prototype-pollution.prototype-pollution-loop.prototype-pollution-loop
frontend/src/hacking-instructor/index.ts	111	javascript.browser.security.insecure-document-method.insecure-document-method
frontend/src/index.html	14	html.security.audit.missing-integrity.missing-integrity
frontend/src/index.html	15	html.security.audit.missing-integrity.missing-integrity
frontend/src/index.html	16	html.security.audit.missing-integrity.missing-integrity
lib/codingChallenges.ts	24	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolv

File	LoC	Matched Check ID
		e-traversal
lib/codingChallenges.ts	24	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
lib/codingChallenges.ts	76	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
lib/codingChallenges.ts	76	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
lib/codingChallenges.ts	76	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
lib/codingChallenges.ts	78	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
lib/codingChallenges.ts	78	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
lib/codingChallenges.ts	78	javascript.lang.security.audit.detect-non-literal-regexp.detect-non-literal-regexp
lib/insecurity.ts	23	javascript.lang.hardcoded.strings.detected-private-key.detected-private-key
lib/insecurity.ts	23	javascript.lang.hardcoded.strings.detected-private-key.detected-private-key
lib/insecurity.ts	44	javascript.lang.security.audit.hardcoded-hmac-key.hardcoded-hmac-key
lib/insecurity.ts	56	javascript.jsonwebtoken.security.jwt-hardcode.hardcoded-jwt-secret
lib/insecurity.ts	56	javascript.lang.hardcoded.strings.detected-private-key.detected-private-key
lib/insecurity.ts	152	javascript.lang.security.audit.hardcoded-hmac-key.hardcoded-hmac-key
lib/insecurity.ts	152	javascript.lang.hardcoded.strings.detected-private-key.detected-private-key
lib/insecurity.ts	195	javascript.express.session-fixation.session-fixation
lib/startup/restoreOverwrittenFilesWithOriginals.ts	28	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
lib/startup/validatePreconditions.ts	120	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
lib/utils.ts	90	javascript.jssha.jssha-sha1.jssha-sha1
models/index.ts	29	javascript.sequelize.node-sequelize-hardcoded-secret-argument.node-sequelize-hardcoded-secret-argument
routes/b2bOrder.ts	22	javascript.express.code.vm-express.vm-express
routes/b2bOrder.ts	22	javascript.express.security.audit.express-detect-notevil-usage.express-detect-notevil-usage
routes/captcha.ts	23	javascript.browser.security.eval-detected.eval-detected
routes/dataErasure.ts	69	javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-traversal
routes/dataErasure.ts	69	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/dataExport.ts	61	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli
routes/dataExport.ts	80	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli
routes/fileServer.ts	33	javascript.express.security.audit.express-res-sendfile.express-res-sendfile
routes/fileServer.ts	33	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/fileUpload.ts	29	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/fileUpload.ts	30	javascript.express.file.fs-express.fs-express
routes/fileUpload.ts	35	javascript.express.file.fs-express.fs-express
routes/fileUpload.ts	39	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/fileUpload.ts	80	javascript.express.code.vm-express.vm-express
routes/fileUpload.ts	80	javascript.express.security.audit.express-libxml-vm-noent.express-libxml-vm-noent
routes/keyServer.ts	14	javascript.express.security.audit.express-res-sendfile.express-res-sendfile
routes/keyServer.ts	14	javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-traversal
routes/keyServer.ts	14	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/likeProductReviews.ts	18	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli
routes/likeProductReviews.ts	25	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli
routes/likeProductReviews.ts	31	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli

File	LoC	Matched Check ID
routes/likeProductReviews.ts	42	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli
routes/logfileServer.ts	14	javascript.express.security.audit.express-res-sendfile.express-res-sendfile
routes/logfileServer.ts	14	javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-traversal
routes/logfileServer.ts	14	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/login.ts	36	javascript.express.db.sequelize-express.sequelize-express
routes/login.ts	36	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
routes/login.ts	36	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
routes/order.ts	45	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/orderHistory.ts	17	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli
routes/orderHistory.ts	36	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli
routes/profileImageFileUpload.ts	28	javascript.express.express-fs-filename.express-fs-filename
routes/profileImageFileUpload.ts	28	javascript.express.file.fs-express.fs-express
routes/profileImageUrlUpload.ts	23	javascript.express.request.ssrf-deepsemgrep.ssrf-deepsemgrep
routes/profileImageUrlUpload.ts	23	javascript.express.security.audit.express-ssrf.express-ssrf
routes/profileImageUrlUpload.ts	31	javascript.express.express-fs-filename.express-fs-filename
routes/profileImageUrlUpload.ts	31	javascript.express.file.fs-express.fs-express
routes/quarantineServer.ts	14	javascript.express.security.audit.express-res-sendfile.express-res-sendfile
routes/quarantineServer.ts	14	javascript.express.security.audit.express-path-join-resolve-traversal.express-path-join-resolve-traversal
routes/quarantineServer.ts	14	javascript.lang.security.audit.path-traversal.path-join-resolve-traversal.path-join-resolve-traversal
routes/redirect.ts	19	javascript.express.open-redirect-deepsemgrep.open-redirect-deepsemgrep
routes/redirect.ts	19	javascript.express.security.audit.express-open-redirect.express-open-redirect
routes/search.ts	23	javascript.express.db.sequelize-express.sequelize-express
routes/search.ts	23	javascript.sequelize.security.audit.sequelize-injection-express.express-sequelize-injection
routes/search.ts	23	javascript.express.security.injection.tainted-sql-string.tainted-sql-string
routes/showProductReviews.ts	34	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli
routes/trackOrder.ts	17	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli
routes/updateProductReviews.ts	18	javascript.express.mongodb.express-mongo-nosqli.express-mongo-nosqli
routes/userProfile.ts	36	javascript.browser.security.eval-detected.eval-detected
routes/userProfile.ts	56	javascript.express.security.express-insecure-template-usage.express-insecure-template-usage
routes/videoHandler.ts	57	javascript.lang.security.audit.unknown-value-with-script-tag.unknown-value-with-script-tag
routes/videoHandler.ts	69	javascript.lang.security.audit.unknown-value-with-script-tag.unknown-value-with-script-tag
routes/vulnCodeFixes.ts	79	javascript.express.express-fs-filename.express-fs-filename
routes/vulnCodeFixes.ts	80	javascript.express.express-fs-filename.express-fs-filename
routes/vulnCodeFixes.ts	80	javascript.express.file.fs-express.fs-express
routes/vulnCodeSnippet.ts	93	javascript.express.express-fs-filename.express-fs-filename
routes/vulnCodeSnippet.ts	94	javascript.express.express-fs-filename.express-fs-filename
routes/vulnCodeSnippet.ts	94	javascript.express.file.fs-express.fs-express
server.ts	105	javascript.express.security.audit.express-check-csurf-middleware-usage.express-check-csurf-middleware-usage
server.ts	148	javascript.lang.security.audit.unsafe-formatstring.unsafe-formatstring
server.ts	260	javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
server.ts	264	javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing

File	LoC	Matched Check ID
server.ts	268	javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
server.ts	272	javascript.express.security.audit.express-check-directory-listing.express-check-directory-listing
views/promotionVideo.pug	79	javascript.express.security.audit.xss.pug.explicit-unescape.template-explicit-unescape

RESOURCES



RESOURCES

- OWASP Juice Shop - https://owasp.org/www-project-juice-shop/
- OWASP WebGoat - https://owasp.org/www-project-webgoat/
- Semgrep Community Edition (CE) - https://semgrep.dev/docs/contributing/semgrep-philosophy
- Semgrep AppSec Platform versus Semgrep Community Edition - https://semgrep.dev/docs/semgrep-pro-vs-oss
- Important updates to Semgrep OSS - https://semgrep.dev/blog/2024/important-updates-to-semgrep-oss/
- Semgrep Pro Engine - https://semgrep.dev/products/pro-engine/
- Comparison and Evaluation on Static Application Security
- Testing (SAST) Tools for Java - https://sen-chen.github.io/img_cs/pdf/fse2023-sast.pdf
- Sonar Source list of Web Goat findings - https://github.com/SonarSource/sonar-benchmarks-scores/blob/master/java/security/OWASP-WebGoat/ground-truth.json
- GitLab How to benchmark security tools: a case study using WebGoat - https://about.gitlab.com/blog/2020/08/11/how-to-benchmark-security-tools/
- WebGoat Labs walkthroughs - https://docs.cycubix.com/application-security-series/web-application-security-essentials/solutions
- Juice Shop walkthroughs - https://pwning.owasp-juice.shop/companion-guide/latest/
- Juice Shop challenges list - https://pwning.owasp-juice.shop/companion-guide/latest/part2/README.html
- Juice Shop challenge solutions - https://pwning.owasp-juice.shop/companion-guide/latest/appendix/solutions.html
- Vendor notes regarding Juice Shop - https://pwning.owasp-juice.shop/companion-guide/latest/part4/vendors.html
- Juice Shop Coding Challenges - https://pwning.owasp-juice.shop/companion-guide/latest/part5/code-snippets.html#_vulnerable_code_snippets
- Semgrep CLI reference - https://semgrep.dev/docs/cli-reference