Fortify Security Report Suricata

12/2/24

igen862

Executive Summary

Issues Overview

On Dec 2, 2024, a source code review was performed over the suricata-master code base. 74 files, 1,314 LOC (Executable) were scanned and reviewed for defects that could lead to potential security vulnerabilities. A total of 14 reviewed findings were uncovered during the analysis.

Issues by Fortify Priority Order	
High	10
Low	3
Critical	1

Recommendations and Conclusions

The Issues Category section provides Fortify recommendations for addressing issues at a generic level. The recommendations for specific fixes can be extrapolated from those generic recommendations by the development group.

Project Summary

Code Base Summary

Code location: C:/UPAPPS/DevWorkarea/suricata-master
Number of Files: 74
Lines of Code: 1314
Build Label: <No Build Label>

Scan Information

Scan time: 00:41
SCA Engine version: 22.1.0.0166
Machine Name: STRM-LS161701
Username running scan: igen862

Results Certification

Results Certification Valid

Details:

Results Signature:

SCA Analysis Results has Valid signature

Rules Signature:

There were no custom rules used in this scan

Attack Surface

Attack Surface:
Command Line Arguments:
null.null.null

Environment Variables:
null.null.null
os.null.getenv

File System:
null.null.open
null.file.read
null.file.readlines

Standard Input Stream:
null.null.input
null.null.raw_input

System Information:
null.null.null
null.null.null
os.null.listdir

Filter Set Summary

Current Enabled Filter Set:
Security Auditor View

Filter Set Details:

Folder Filters:
If [fortify priority order] contains critical Then set folder to Critical
If [fortify priority order] contains high Then set folder to High
If [fortify priority order] contains medium Then set folder to Medium
If [fortify priority order] contains low Then set folder to Low
Visibility Filters:

Audit Guide Summary

J2EE Bad Practices

Hide warnings about J2EE bad practices.
Depending on whether your application is a J2EE application, J2EE bad practice warnings may or may not apply. AuditGuide can hide J2EE bad practice warnings.
Enable if J2EE bad practice warnings do not apply to your application because it is not a J2EE application.

Filters:
If category contains j2ee Then hide issue
If category is race condition: static database connection Then hide issue

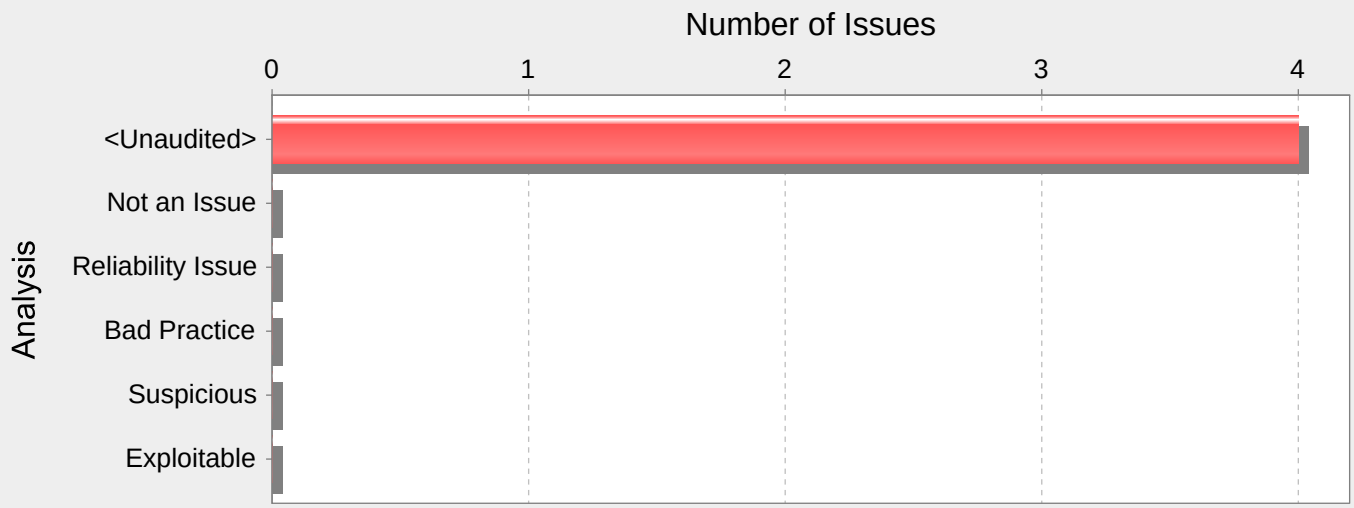
Results Outline

Overall number of results

The scan found 14 issues.

Vulnerability Examples by Category

Category: Credential Management: Hardcoded API Credentials (4 Issues)



Abstract:

Hardcoded API credentials can compromise system security in a way that is not easy to remedy.

Explanation:

Never hardcode credentials, including usernames, passwords, API keys, API secrets, and API Tokens. Not only are hardcoded credentials visible to all of the project developers, they are extremely difficult to update. After the code is in production, the credentials cannot be changed without patching the software. If the credentials are compromised, the organization must choose between security and system availability.

Recommendations:

Make sure that API credentials are either loaded from a configuration file that is only available in the runtime environment or from environment variables.

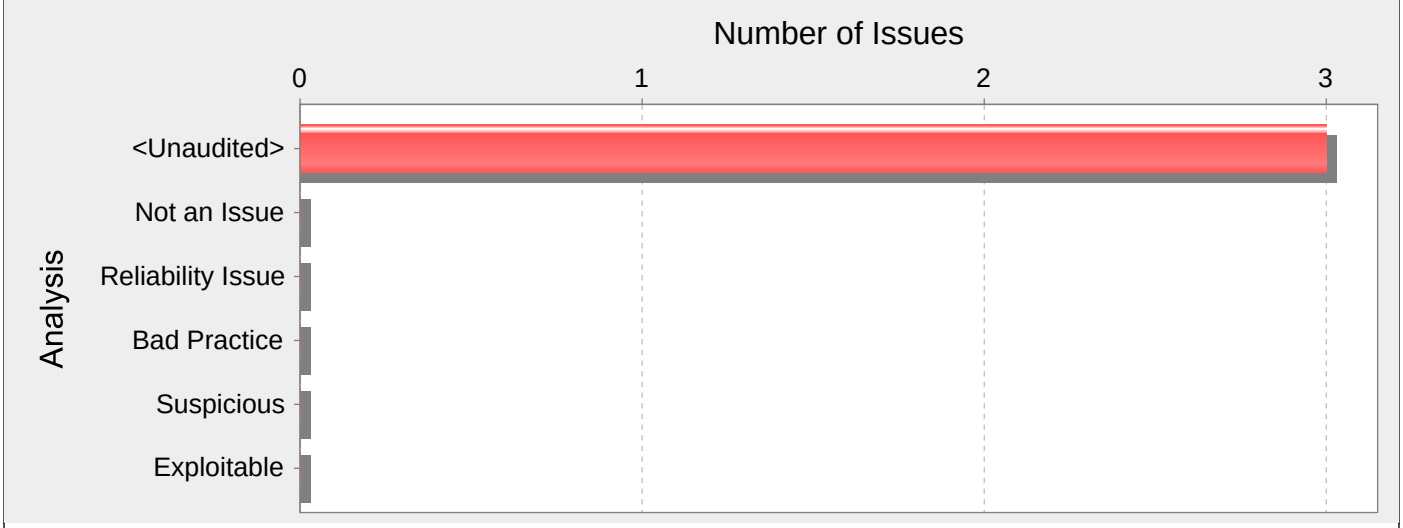
authors-done.yml, line 15 (Credential Management: Hardcoded API Credentials)

Fortify Priority:	High	**Folder**	High
Kingdom:	Security Features		
Abstract:	Hardcoded API credentials can compromise system security in a way that is not easy to remedy.		

Sink: authors-done.yml:15 null()

```
13
14                  - name: Download artifact new authors
15                    uses: actions/github-script@60a0d83039c74a4aee543508d2ffcb1c3799cdea
16                    with:
17                      script: |
```

Category: Path Manipulation (3 Issues)



Abstract:

Attackers can control the file system path argument to open() at convert.py line 31, which allows them to access or modify otherwise protected files.

Explanation:

Path manipulation errors occur when the following two conditions are met:

1. An attacker can specify a path used in an operation on the file system.

2. By specifying the resource, the attacker gains a capability that would not otherwise be permitted.

For example, the program might give the attacker the ability to overwrite the specified file or run with a configuration controlled by the attacker.

Example 1: The following code uses input from an HTTP request to create a file name. The programmer has not considered the possibility that an attacker could provide a file name such as "../../tomcat/conf/server.xml", which causes the application to delete one of its own configuration files.

```
rName = req.field('reportName')
rFile = os.open("/usr/local/apfr/reports/" + rName)
...
os.unlink(rFile);
```

Example 2: The following code uses input from a configuration file to determine which file to open and echo back to the user. If the program runs with adequate privileges and malicious users can change the configuration file, they can use the program to read any file on the system that ends with the extension .txt.

```
...
filename = CONFIG_TXT['sub'] + ".txt";
handle = os.open(filename)
print handle
...
```

Recommendations:

The best way to prevent path manipulation is with a level of indirection: create a list of legitimate values from which the user must select. With this approach, the user-provided input is never used directly to specify the resource name.

In some situations this approach is impractical because the set of legitimate resource names is too large or too hard to maintain. Programmers often resort to implementing a deny list in these situations. A deny list is used to selectively reject or escape potentially dangerous characters before using the input. However, any such list of unsafe characters is likely to be incomplete and will almost certainly become out of date. A better approach is to create a list of characters that are permitted to appear in the resource name and accept input composed exclusively of characters in the approved set.

Tips:

1. If the program performs custom input validation to your satisfaction, use Fortify Custom Rules Editor to create a cleanse rule for the validation routine.

2. Implementation of an effective deny list is notoriously difficult. One should be skeptical if validation logic requires implementing a deny list. Consider different types of input encoding and different sets of metacharacters that might have special meaning when interpreted by different operating systems, databases, or other resources. Determine whether or not the deny list can be updated easily, correctly, and completely if these requirements ever change.

convert.py, line 31 (Path Manipulation)			
Fortify Priority:	High	**Folder**	High
Kingdom:	Input Validation and Representation		
Abstract:	Attackers can control the file system path argument to open() at convert.py line 31, which allows them to access or modify otherwise protected files.		

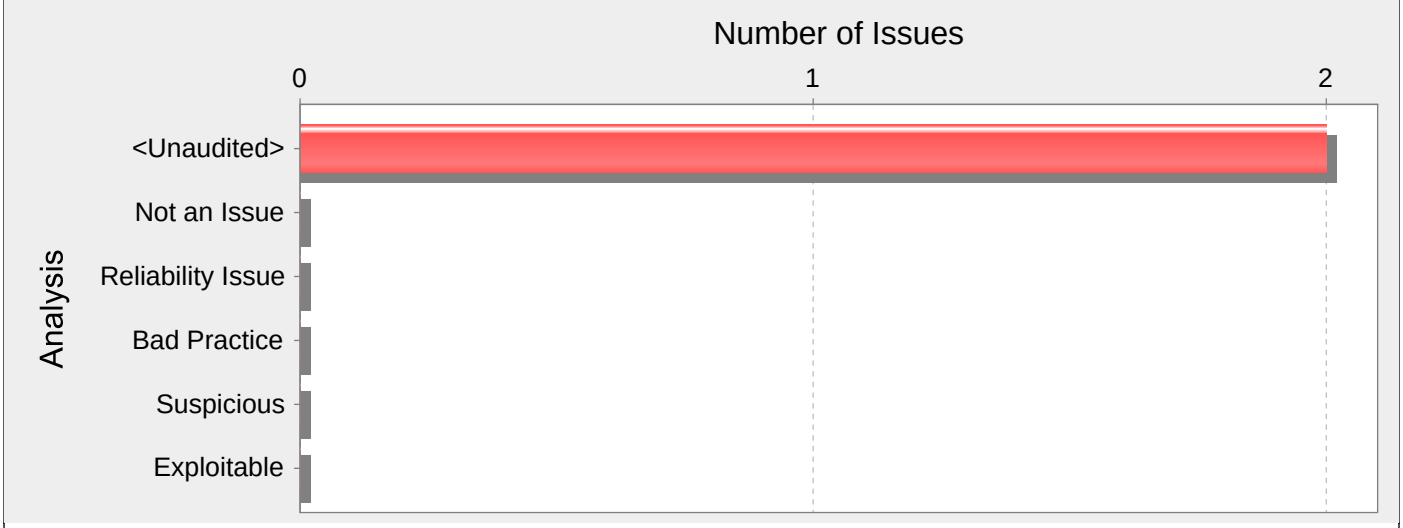
Source: convert.py:38 Read ~PythonGlobalsVar.sys.argv()

```
36
37                  url = sys.argv[1]
38                  output = sys.argv[2]
39
40                  fetch_images(url, output)
```

Sink: convert.py:31 open()

```
29                      print("Fetching image %s." % (image_url))
30
31                      open(os.path.join(dest, filename), "w").write(
32                          urllib.request.urlopen(image_url).read())
```

Category: Dockerfile Misconfiguration: Dependency Confusion (2 Issues)



Abstract:

Retrieving build dependencies using a non-specific version can leave the build system vulnerable to malicious binaries or cause the system to experience unexpected behavior.

Explanation:

Dockerfiles can specify an unbound range of versions for dependencies and base images. If an attacker is able to add malicious versions of dependencies to a repository or trick the build system into downloading dependencies from a repository under the attacker's control, if docker is configured without specific versions of dependencies, then docker will silently download and run the compromised dependency.

This type of weakness would be exploitable as a result of a supply chain attack where attackers can leverage misconfiguration by developers, typosquatting and can add malicious packages to open source repositories. An attack of this type exploits the trust in the published packages to gain access and exfiltrate data.

In docker, the latest tag automatically indicates the version level of an image that doesn't use a digest or unique tag to provide a version for it. Docker automatically assigns the latest tag as mechanism to point to the most recent image manifest file. Because tags are mutable, an attacker can replace an image or layer using a latest (or weak tags such as imagename-lst, imagename-last, myimage).

Example 1: The following configuration instructs Docker to pick the base image using the latest version of ubuntu.

```
FROM ubuntu:Latest
...
```

Docker does not validate whether the repository configured to support the package manager is trustworthy.

Example 2: The following configuration instructs the package manager zypper to retrive the latest version of the given package.

```
...
zypper install package
...
```

In Example 2, if the repository is compromised, an attacker could simply upload a version that meets the dynamic criteria and cause zypper to download a malicious version of the dependency.

Recommendations:

Perform version pinning or simple pinning. Version pinning explicitly specifies the version of images, libraries and support packages an application or system depends on. The primary goal of pinning is to ensure system stability to achieve repeatable deployments. Pinning ensures that end-users, developers, and testers all use the same code base. Pinning can additionally ensure the use of safe dependencies; those which have gone through the rigorous process of application security validation and malware detection.

When you invoke zypper (or other package managers) from docker, use the following formats:

```
RUN zypper install <package_name>=<version> \
RUN gem install <package_name> --version <version>
RUN gem install <package_name> -v <version>
RUN apk add <package_name>=<version>
RUN apt-get update && apt-get install -y  \
<package_name>=<version>  \
<package_name>=<version> \
```

<package_name>=<version> \

&& rm -rf /var/lib/apt/lists/*

Where <package_name> is the name of the dependency to install and <version> is the exact version or release the application should use.

Fortify also recommends:

- Ensure the repositories that the package managers use are trustworthy or that they are properly kept, and there is no install package substitution possible, including the addition of malicious code onto the package.

- Avoid using public or untrusted repositories.

- Scan packages for malware and security vulnerabilities prior to executing any regression tests.

- Use digitally signed images.

- Avoid using image tags such as latest or weak tags such asimagename-lst, imagename-last, myimage for deployments in production environments.

- Stick to more stable tags, like specific version tags, although there is no guarantee that these cannot mutate either.

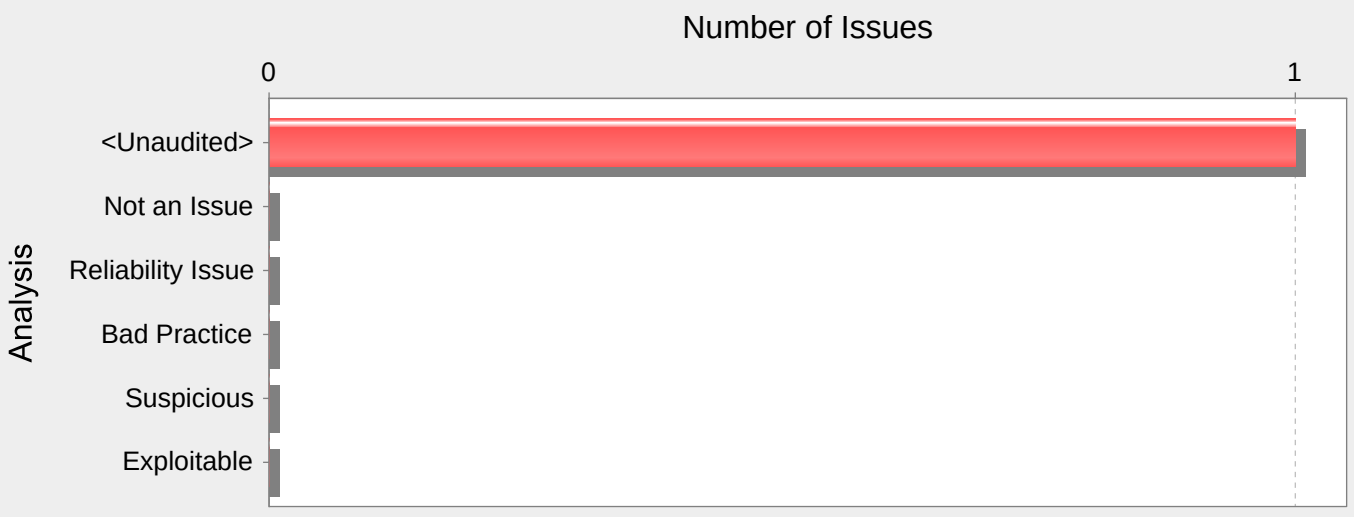
- Do not create mutant tags.

- Implement strict control over the source of images and their layers.

Dockerfile, line 1 (Dockerfile Misconfiguration: Dependency Confusion)

Fortify Priority:	High	**Folder**	High
Kingdom:	Environment		
Abstract:	Retrieving build dependencies using a non-specific version can leave the build system vulnerable to malicious binaries or cause the system to experience unexpected behavior.		
Sink:	Dockerfile:1 FROM()		
-1	`FROM gcr.io/oss-fuzz-base/base-builder-rust`		
0	`RUN apt-get update && apt-get install -y build-essential autoconf automake libtool make pkg-config  python flex bison zlib1g-dev libpcre3-dev cmake tshark`		

Category: Dockerfile Misconfiguration: Default User Privilege (1 Issues)



Abstract:

The Dockerfile does not specify a USER, so it defaults to running with a root user.

Explanation:

When a Dockerfile does not specify a USER, Docker containers run with super user privileges by default. These super user privileges are propagated to the code running inside the container, which is usually more permission than necessary. Running the Docker container with super user privileges broadens the attack surface which might enable attackers to perform more serious forms of exploitation.

Recommendations:

It is good practice to run your containers as a non-root user when possible.

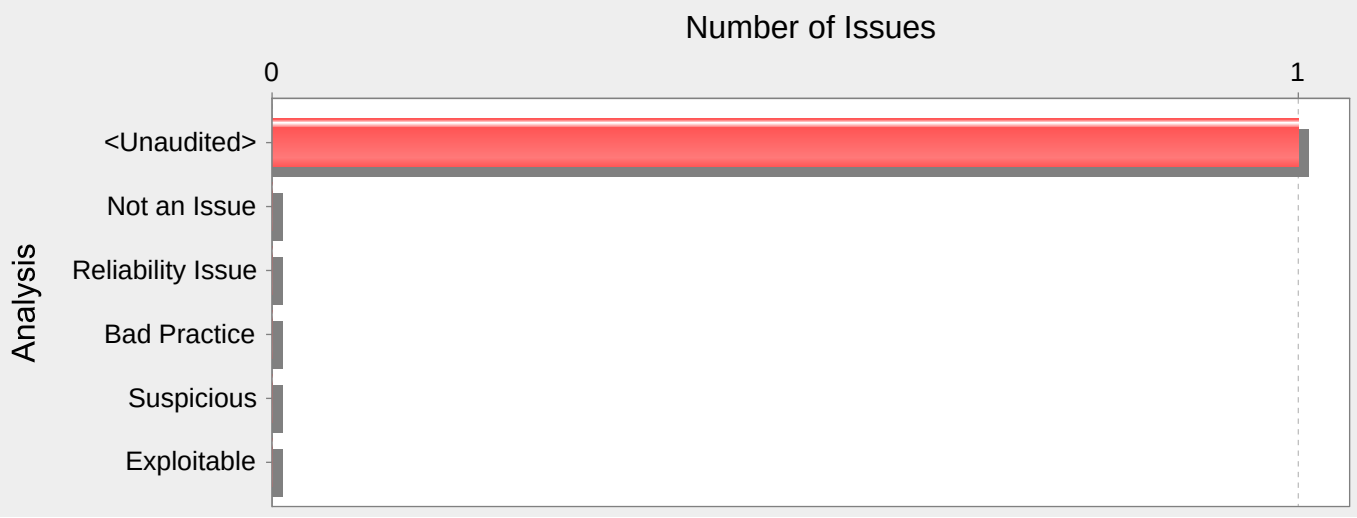
To modify a docker container to use a non-root user, the Dockerfile needs to specify a different user, such as:

```
RUN useradd myLowPrivilegeUser
USER myLowPrivilegeUser
```

Dockerfile, line 1 (Dockerfile Misconfiguration: Default User Privilege)

Fortify Priority:	High	**Folder**	High
Kingdom:	Environment		
Abstract:	The Dockerfile does not specify a USER, so it defaults to running with a root user.		
Sink:	Dockerfile:1 FROM()		
-1	`FROM gcr.io/oss-fuzz-base/base-builder-rust`		
0	`RUN apt-get update && apt-get install -y build-essential autoconf automake libtool make pkg-config  python flex bison zlib1g-dev libpcre3-dev cmake tshark`		

Category: Dynamic Code Evaluation: Code Injection (1 Issues)



Abstract:

Interpreting user-controlled instructions at run-time can allow attackers to execute malicious code.

Explanation:

Many modern programming languages allow dynamic interpretation of source instructions. This capability allows programmers to perform dynamic instructions based on input received from the user. Code injection vulnerabilities occur when the programmer incorrectly assumes that instructions supplied directly from the user will perform only innocent operations, such as performing simple calculations on active user objects or otherwise modifying the user's state. However, without proper validation, a user might specify operations the programmer does not intend.

Example: In this classic code injection example, the application implements a basic calculator that allows the user to specify commands for execution.

```
...
userOps = request.GET['operation']
result = eval(userOps)
...
```

The program behaves correctly when the operation parameter is a benign value, such as "8 + 7 * 2", in which case the result variable is assigned a value of 22. However, if an attacker specifies operations that are both valid and malicious, those operations would be executed with the full privilege of the parent process. Such attacks are even more dangerous when the underlying language provides access to system resources or allows execution of system commands. For example, if an attacker were to specify " os.system('shutdown -h now')" as the value of operation, a shutdown command would be executed on the host system.

Recommendations:

Avoid dynamic code interpretation whenever possible. If your program's functionality requires code to be interpreted dynamically, the likelihood of attack can be minimized by constraining the code your program will execute dynamically as much as possible, limiting it to an application- and context-specific subset of the base programming language.

If dynamic code execution is required, unvalidated user input should never be directly executed and interpreted by the application. Instead, use a level of indirection: create a list of legitimate operations and data objects that users are allowed to specify, and only allow users to select from the list. With this approach, input provided by users is never executed directly.

suricatasc.py, line 259 (Dynamic Code Evaluation: Code Injection)

Fortify Priority:	Critical	**Folder**	Critical
Kingdom:	Input Validation and Representation		
Abstract:	Interpreting user-controlled instructions at run-time can allow attackers to execute malicious code.		

Sink: suricatasc.py:259 FunctionCall: input()

```
257                         command = raw_input(">>> ").strip()
258                     else:
259                         command = input(">>> ").strip()
260                     if command == "quit":
261                         break
```

Detailed Project Summary

Files Scanned

Code base location: C:/UPAPPS/DevWorkarea/suricata-master

Files Scanned:

.clusterfuzzlite/Dockerfile dockerfile 1 KB Nov 29, 2024, 1:37:39 PM

.clusterfuzzlite/build.sh generic 2.7 KB Nov 29, 2024, 1:37:39 PM

.clusterfuzzlite/project.yaml generic Nov 29, 2024, 1:37:39 PM

.github/CODEOWNERS generic Nov 29, 2024, 1:37:39 PM

.github/PULL_REQUEST_TEMPLATE.md generic 1.4 KB Nov 29, 2024, 1:37:39 PM

.github/workflows/authors-done.yml generic 1.9 KB Nov 29, 2024, 1:37:39 PM

.github/workflows/builds.yml generic 115.2 KB Nov 29, 2024, 1:37:39 PM

.github/workflows/codeql.yml generic 1.6 KB Nov 29, 2024, 1:37:39 PM

.github/workflows/commits.yml generic 3.5 KB Nov 29, 2024, 1:37:39 PM

.github/workflows/formatting.yml generic 5.7 KB Nov 29, 2024, 1:37:39 PM

.github/workflows/prepare-deps.yml generic 4.8 KB Nov 29, 2024, 1:37:39 PM

.github/workflows/scorecards-analysis.yml generic 1.8 KB Nov 29, 2024, 1:37:39 PM

configure.ac generic 105 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/capture-hardware/ebpf-xdp.rst generic 22.5 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/capture-hardware/myricom.rst generic 4.1 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/conf.py python 66 Lines 11.2 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/convert.py python 61 Lines 2.5 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/devguide/codebase/code-style.rst generic 17.9 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/devguide/codebase/fuzz-testing.rst generic Nov 29, 2024, 1:37:39 PM

doc/userguide/devguide/codebase/installation-from-git.rst generic 3.4 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/devguide/codebase/testing.rst generic 8.1 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/devguide/contributing/backports-guide.rst generic 5.3 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/devguide/contributing/code-submission-process.rst generic 3.4 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/devguide/extending/app-layer/app-layer-frames.rst generic 11.9 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/devguide/extending/output/index.rst generic 2.7 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/lua/lua-functions.rst generic 18.3 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/output/eve/eve-json-format.rst generic 85.6 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/performance/hyperscan.rst generic 2.6 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/performance/packet-capture.rst generic 4.6 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/performance/statistics.rst generic 6.2 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/rules/differences-from-snort.rst generic 32.1 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/rules/ja-keywords.rst generic 2.3 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/unix-socket.rst generic 9.8 KB Nov 29, 2024, 1:37:39 PM

doc/userguide/upgrade/unified2.rst generic 1.4 KB Nov 29, 2024, 1:37:39 PM

etc/classification.config xml 3.2 KB Nov 29, 2024, 1:37:39 PM

etc/reference.config xml 1.7 KB Nov 29, 2024, 1:37:39 PM

python/suricata/__init__.py python 1 Lines Nov 29, 2024, 1:37:39 PM

python/suricata/config/__init__.py python 1 Lines Nov 29, 2024, 1:37:39 PM

python/suricata/ctl/__init__.py python 1 Lines Nov 29, 2024, 1:37:39 PM

python/suricata/ctl/filestore.py python 83 Lines 4 KB Nov 29, 2024, 1:37:39 PM

python/suricata/ctl/loghandler.py python 43 Lines 2.7 KB Nov 29, 2024, 1:37:39 PM

python/suricata/ctl/main.py python 25 Lines 1.6 KB Nov 29, 2024, 1:37:39 PM

python/suricata/ctl/test_filestore.py python 14 Lines Nov 29, 2024, 1:37:39 PM

python/suricata/sc/__init__.py python 2 Lines Nov 29, 2024, 1:37:39 PM

python/suricata/sc/specs.py python 165 Lines 4.3 KB Nov 29, 2024, 1:37:39 PM

python/suricata/sc/suricatasc.py python 184 Lines 9.8 KB Nov 29, 2024, 1:37:39 PM

python/suricatasc/__init__.py python 2 Lines Nov 29, 2024, 1:37:39 PM
qa/coccinelle/struct-flags.py python 60 Lines 3.1 KB Nov 29, 2024, 1:37:39 PM
qa/sock_to_gzip_file.py python 38 Lines 1.9 KB Nov 29, 2024, 1:37:39 PM
qa/travis.sh generic 1.3 KB Nov 29, 2024, 1:37:39 PM
requirements.txt generic Nov 29, 2024, 1:37:39 PM
rust/.cargo/config.toml.in generic Nov 29, 2024, 1:37:39 PM
rust/Cargo.lock.in generic 30.8 KB Nov 29, 2024, 1:37:39 PM
rust/src/dns/dns.rs generic 56 KB Nov 29, 2024, 1:37:39 PM
rust/src/ja4.rs generic 13.2 KB Nov 29, 2024, 1:37:39 PM
rust/src/lib.rs generic 3.3 KB Nov 29, 2024, 1:37:39 PM
rust/src/log.rs generic 5.5 KB Nov 29, 2024, 1:37:39 PM
rust/src/modbus/detect.rs generic 45.5 KB Nov 29, 2024, 1:37:39 PM
rust/src/pgsql/parser.rs generic 90.5 KB Nov 29, 2024, 1:37:39 PM
rust/src/quic/parser.rs generic 20.8 KB Nov 29, 2024, 1:37:39 PM
rust/src/smb/smb2_records.rs generic 32 KB Nov 29, 2024, 1:37:39 PM
rust/src/websocket/websocket.rs generic 13.3 KB Nov 29, 2024, 1:37:39 PM
scripts/bundle.sh generic 3.2 KB Nov 29, 2024, 1:37:39 PM
scripts/cppclean_check.py python 31 Lines 2 KB Nov 29, 2024, 1:37:39 PM
scripts/dnp3-gen/dnp3-gen.py python 118 Lines 21.8 KB Nov 29, 2024, 1:37:39 PM
scripts/evedoc.py python 134 Lines 6.3 KB Nov 29, 2024, 1:37:39 PM
scripts/git-clang-format-custom generic 21.8 KB Nov 29, 2024, 1:37:39 PM
scripts/setup-app-layer.py python 285 Lines 13.1 KB Nov 29, 2024, 1:37:39 PM
src/app-layer-dnp3.c c 75.7 KB Nov 29, 2024, 1:37:39 PM
src/app-layer-htp.c c 202.9 KB Nov 29, 2024, 1:37:39 PM
src/tests/fuzz/README generic 2.7 KB Nov 29, 2024, 1:37:39 PM
src/util-systemd.c c 2.4 KB Nov 29, 2024, 1:37:39 PM
suricata.yaml.in generic 85.6 KB Nov 29, 2024, 1:37:39 PM
threshold.config xml 1.6 KB Nov 29, 2024, 1:37:39 PM

Reference Elements

Classpath:

No classpath specified during translation

Libdirs:

No libdirs specified during translation

Rulepacks

Valid Rulepacks:

Name: Fortify Secure Coding Rules, Community, Cloud
Version: 2022.3.0.0008
ID: 686C4B2F-0321-4025-B9F4-6E26094B4746
SKU: RUL13242

Name: Fortify Secure Coding Rules, Community, Universal
Version: 2022.3.0.0008
ID: 97b8b0e6-618b-47cf-a7fb-8636faea6b75
SKU: RUL13240

Name: Fortify Secure Coding Rules, Core, Python
Version: 2022.3.0.0008
ID: FD15CBE4-E059-4CBB-914E-546BDCEB422B
SKU: RUL13083

Name: Fortify Secure Coding Rules, Core, Universal
Version: 2022.3.0.0008
ID: 88D39959-D322-499A-87F3-BC9E1193B07A
SKU: RUL13241

Name: Fortify Secure Coding Rules, Extended, Configuration
Version: 2022.3.0.0008
ID: CD6959FC-0C37-45BE-9637-BAA43C3A4D56
SKU: RUL13005

Name: Fortify Secure Coding Rules, Extended, Content
Version: 2022.3.0.0008
ID: 9C48678C-09B6-474D-B86D-97EE94D38F17
SKU: RUL13067

External Metadata:
Version: 2022.1.0.0007

Name: CWE
ID: 3ADB9EE4-5761-4289-8BD3-CBFCC593EBBC
The Common Weakness Enumeration (CWE), co-sponsored and maintained by MITRE, is international in scope and free for public use. CWE provides a unified, measurable set of software weaknesses that is enabling more effective discussion, description, selection, and use of software security tools and services that can find these weaknesses in source code and operational systems as well as better understanding and management of software weaknesses related to architecture and design.

Name: CWE Top 25 2019
ID: 7AF935C9-15AA-45B2-8EEC-0EAE4194ACDE
The 2019 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hierarchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like languages and the software under analysis might not be within the C-family of languages - thus, many CWEs would not be in scope.

Name: CWE Top 25 2020
ID: E4C1DC51-45BD-469E-BA5D-BABF690F09F4
The 2020 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team

used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hierarchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like languages and the software under analysis might not be within the C-family of languages - thus, many CWEs would not be in scope.

Name: CWE Top 25 2021
ID: FDA85EBD-56E5-4698-86FD-DD52E2F8F32B
The 2021 CWE Top 25 Most Dangerous Software Errors lists the most widespread and critical weaknesses that can lead to serious vulnerabilities in software (as demonstrated by the National Vulnerability Database). These weaknesses occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently enable attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of heuristic formula that the CWE Team used with a data-driven approach that leveraged the Common Vulnerabilities and Exposure (CVE), National Vulnerability Database (NVD), and Common Vulnerability Scoring System (CVSS). Due to the hierarchical nature of the CWE taxonomy, Fortify considers all CWE IDs which are children of a Top 25 entry, as included within the context of the entry due to the "CHILD-OF" relationship within the hierarchy. Exercise caution if using only this Top 25 list to prioritize auditing efforts because the software under analysis might not align with the assumptions of the heuristic used to define the Top 25. For example, many of these weaknesses are related to C-like languages and the software under analysis might not be within the C-family of languages - thus, many CWEs would not be in scope.

Name: DISA CCI 2
ID: 7F037130-41E5-40F0-B653-7819A4B3E241
The purpose of a Defense Information Systems Agency (DISA) Control Correlation Identifier (CCI) is to provide a standard identifier for policy based requirements which connect high-level policy expressions and low-level technical implementations. Associated with each CCI is a description for each of the singular, actionable, statements compromising an information assurance (IA) control or IA best practice. Using CCI allows high-level policy framework security requirements to be decomposed and explicitly associated with low-level implementations, thus enabling the assessment of related compliance assessment results spanning heterogeneous technologies. The current IA controls and best practices associated with each CCI, that are specified in NIST SP 800-53 Revision 4, can be viewed using the DISA STIG Viewer.
The following table summarizes the number of issues identified across the different CCIs broken down by Fortify Priority Order. The status of a CCI is considered "In Place" when there are no issues reported for a given CCI.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, CCI-003187 is not considered "In Place". Similarly, if the project is missing a Micro Focus Fortify WebInspect scan, or the scan contains any critical findings, CCI-000366 and CCI-000256 are not considered "In Place".

Name: FISMA
ID: B40F9EE0-3824-4879-B9FE-7A789C89307C
The Federal Information Processing Standard (FIPS) 200 document is part of the official series of publications, issued by the National Institute of Standards and Technology (NIST), relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA). Specifically, FIPS Publication 200 specifies the "Minimum Security Requirements for Federal Information and Information Systems."

Name: GDPR
ID: 771C470C-9274-4580-8556-C12F5E4BEC51
The EU General Data Protection Regulation (GDPR) replaces the Data Protection Directive 95/46/EC and was designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens data privacy and to reshape the way organizations across the region approach data privacy. Going into effect on May 25, 2018, GDPR provides a framework for organizations on how to handle personal data. According to GDPR regulation personal data "means any information relating

to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person." GDPR articles that pertain to application security and require businesses to protect personal data during design and development of its product and services are:

- Article 25, Data protection by design and by default - which requires "The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed."
- Article 32, Security of processing - which requires businesses to protect its systems and applications "from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data". This report may be used by organizations as a framework to help identify and protect personal data as it relates to application security.

Name: MISRA C 2012
ID: 555A3A66-A0E1-47AF-910C-3F19A6FB2506
Now in its third edition, the Motor Industry Software Reliability Association (MISRA) C Guidelines describe a subset of the C programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C Guidelines focus upon safety-related software development, a subset of the rules reflects security properties. Fortify interprets the MISRA C Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanisms with the standard rulepacks, however, further support of the MISRA C Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: MISRA C++ 2008
ID: 5D4B75A1-FC91-4B4B-BD4D-C81BBE9604FA
The Motor Industry Software Reliability Association (MISRA) C++ Guidelines describe a subset of the C++ programming language in which there is reduced risk of introducing mistakes in critical systems. While the MISRA C++ Guidelines focus upon safety-related software development, a subset of the rules reflects security properties. Fortify interprets the MISRA C++ Guidelines under the context of security and provides correlation of security vulnerability categories to the rules defined by MISRA. Fortify provides these security focused detection mechanisms with the standard rulepacks, however, further support of the MISRA C++ Guidelines related to safety can be added through the use of custom rules. The results in this report can assist in the creation of a compliance matrix for MISRA.

Name: NIST SP 800-53 Rev.4
ID: 1114583B-EA24-45BE-B7F8-B61201BACDD0
NIST Special Publication 800-53 Revision 4 provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. The following table summarizes the number of issues identified across the different controls and broken down by Fortify Priority Order.

Name: NIST SP 800-53 Rev.5
ID: 32434089-54F3-49F8-93F8-688B6B2FE8ED
NIST Special Publication 800-53 Revision 5 provides a list of security and privacy controls designed to protect federal organizations and information systems from security threats. The following table summarizes the number of issues identified across the different controls and broken down by Fortify Priority Order.

Name: OWASP ASVS 4.0
ID: 28083E33-760F-4A1A-AADA-738CC60082AD
The OWASP Application Security Verification Standard establishes a framework of security requirements and controls that focus on functional and non-functional security controls for the software development lifecycle based upon a community-driven effort. OWASP ASVS identifies several application security verification levels, with each level increasing depth:

<LI>ASVS Level 1 (L1): for low assurance levels and is completely penetration testable.</LI>
<LI>ASVS Level 2 (L2): for applications that contain sensitive data, which requires protection, and is the recommended level for most apps.</LI>
<LI>ASVS Level 3 (L3): for the most critical applications - applications that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust.</LI> </UL>

Name: OWASP Mobile 2014
ID: EEE3F9E7-28D6-4456-8761-3DA56C36F4EE
The OWASP Mobile Top 10 Risks 2014 provides a powerful awareness document for mobile application security. The OWASP Mobile Top 10 represents a broad consensus about what the most critical mobile application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2004
ID: 771C470C-9274-4580-8556-C023E4D3ADB4
The OWASP Top Ten 2004 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2007
ID: 1EB1EC0E-74E6-49A0-BCE5-E6603802987A
The OWASP Top Ten 2007 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2010
ID: FDCECA5E-C2A8-4BE8-BB26-76A8ECD0ED59
The OWASP Top Ten 2010 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2013
ID: 1A2B4C7E-93B0-4502-878A-9BE40D2A25C4
The OWASP Top Ten 2013 provides a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2017
ID: 3C6ECB67-BBD9-4259-A8DB-B49328927248
The OWASP Top Ten 2017 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top Ten represents a broad agreement about what the most critical web application security flaws are with consensus being drawn from data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: OWASP Top 10 2021
ID: 1887A283-3C0D-453C-AD10-0B451EAF096D0
The OWASP Top 10 2021 provides a powerful awareness document for web application security focused on informing the community about the consequences of the most common and most important web application security weaknesses. The OWASP Top 10 represents a broad agreement about what the most critical web application security flaws are with consensus drawn from

data collection and survey results. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

Name: PCI 1.1
ID: CBDB9D4D-FC20-4C04-AD58-575901CAB531
The Payment Card Industry (PCI) Data Security Standard (DSS) 1.1 compliance standard describes 12 requirements which are organized into 6 logically related groups, which are "control objectives". PCI DSS requirements are applicable if Primary Account Number (PAN) is stored, processed, or transmitted by the system.

Name: PCI 1.2
ID: 57940BDB-99F0-48BF-BF2E-CFC42BA035E5
Payment Card Industry Data Security Standard Version 1.2 description

Name: PCI 2.0
ID: 8970556D-7F9F-4EA7-8033-9DF39D68FF3E
The PCI DSS 2.0 compliance standard, particularly sections 6.3, 6.5, and 6.6, references the OWASP Top 10 vulnerability categories as the core categories that must be tested for and remediated. The following table summarizes the number of issues identified across the different PCI DSS requirements and broken down by Fortify Priority Order.

Name: PCI 3.0
ID: E2FB0D38-0192-4F03-8E01-FE2A12680CA3
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.0. Fortify tests for 32 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.1
ID: AC0D18CF-C1DA-47CF-9F1A-E8EC0A4A717E
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2
ID: 4E8431F9-1BA1-41A8-BDBD-087D5826751A
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI 3.2.1
ID: EADE255F-6561-4EFE-AD31-2914F6BFA329
The following is a summary of the application security portions of Payment Card Industry (PCI) Data Security Standard (DSS) v3.2.1. Fortify tests for 31 application security related requirements across sections 1, 2, 3, 4, 6, 7, 8, and 10 of PCI DSS and reports whether each requirement is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is

intended to measure the level of adherence the specific application(s) possess when compared to PCI DSS 3.2.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI SSF 1.0
ID: 0F551543-AF0E-4334-BEDF-1DDCD5F4BF74
The following is a summary of the application security portions of the Secure Software Requirements and Assessment Procedures defined in the Payment Card Industry (PCI) Software Security Framework (SSF) v1.0. Fortify tests for 23 application security related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7, 8, and A.2 of PCI SSF and reports whether each control objective is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI SSF 1.0 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: PCI SSF 1.1
ID: 601EA2F3-5EDC-411C-818C-10DC5B29467D
The following is a summary of the application security portions of the Secure Software Requirements and Assessment Procedures defined in the Payment Card Industry (PCI) Software Security Framework (SSF) v1.1. Fortify tests for 31 application security related control objectives across Control Objective sections 2, 3, 4, 5, 6, 7, 8, A.2, B.2, and B.3 of PCI SSF and reports whether each control objective is In Place or Not In Place to indicate whether requirements are satisfied or not. This report is intended to measure the level of adherence the specific application(s) possess when compared to PCI SSF 1.1 compliance and is not intended to serve as a comprehensive Report on Compliance (ROC). The information contained in this report is targeted at project managers, security auditors, and compliance auditors.

Name: SANS Top 25 2009
ID: 939EF193-507A-44E2-ABB7-C00B2168B6D8
The 2009 CWE/SANS Top 25 Programming Errors lists the most significant programming errors that can lead to serious software vulnerabilities. They occur frequently, are often easy to find, and easy to exploit. They are dangerous because they will frequently allow attackers to completely take over the software, steal data, or prevent the software from working at all. The list is the result of collaboration between the SANS Institute, MITRE, and many top software security experts.

Name: SANS Top 25 2010
ID: 72688795-4F7B-484C-88A6-D4757A6121CA
SANS Top 25 2010 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: SANS Top 25 2011
ID: 92EB4481-1FD9-4165-8E16-F2DE6CB0BD63
SANS Top 25 2011 Most Dangerous Software Errors provides an enumeration of the most widespread and critical errors, categorized by Common Weakness Enumeration (CWE) identifiers, that lead to serious vulnerabilities in software (http://cwe.mitre.org/). These software errors are often easy to find and exploit. The inherent danger in these errors is that they can allow an attacker to completely take over the software, steal data, or prevent the software from working at all.

Name: STIG 3.1
ID: F2FA57EA-5AAA-4DDE-90A5-480BE65CE7E7
Security Technical Implementation Guide Version 3.1 description

Name: STIG 3.10
ID: 788A87FE-C9F9-4533-9095-0379A9B35B12

Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.4
ID: 58E2C21D-C70F-4314-8994-B859E24CF855
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.5
ID: DD18E81F-3507-41FA-9DFA-2A9A15B5479F
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

Name: STIG 3.6
ID: 000CA760-0FED-4374-8AA2-6FA3968A07B1
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.7
ID: E69C07C0-81D8-4B04-9233-F3E74167C3D2
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG identifies several severities with respect to vulnerabilities:

<LI>CAT I: allow an attacker immediate access into a machine, allow super user access, or bypass a firewall.</LI>
<LI>CAT II: provide information that have a high potential of giving access to an intruder.</LI>
<LI>CAT III: provide information that potentially could lead to compromise.</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 3.9
ID: 1A9D736B-2D4A-49D1-88CA-DF464B40D732
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APP<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APP5080: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APP5100: CAT II is not considered "In Place".

Name: STIG 4.1
ID: 95227C50-A9E4-4C9D-A8AF-FD98ABAE1F3C
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.10
ID: EF1FF442-1673-4CF1-B7C4-920F1A96A8150
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.11
ID: D9F6C005-1ED5-4685-8A69-79A87A1A9431
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.2
ID: 672C15F8-8822-4E05-8C9E-1A4BAAA7A373
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>

<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.3
ID: A0B313F0-29BD-430B-9E34-6D10F1178506
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.4
ID: ECEC5CA2-7ACA-4B70-BF44-3248B9C6F4F8
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.5
ID: E6010E0A-7F71-4388-B8B7-EE9A02143474
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].

DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.6
ID: EFB9B012-44D6-456D-B197-03D2FD7C7AD6
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].
DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.7
ID: B04A1E01-F1C1-48D3-A827-0F70872182D7
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>].
DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.8

ID: E6805D9F-D5B5-4192-962C-46828FF68507
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 4.9
ID: 7B9F7B3B-07FC-4B61-99A1-70E3BB23A6A0
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930: CAT II are not considered "In Place".

Name: STIG 5.1
ID: 1E2530B5-61C5-45D0-B479-79CB82DAFF83
Each requirement or recommendation identified by the Defense Information Systems Agency (DISA) STIG is represented by a STIG identifier (STIGID), which corresponds to a checklist item and a severity code [APSC-DV-<I>ID</I>: CAT <I>SEV</I>]. DISA STIG defines three severities with respect to vulnerabilities where their:

<LI>exploitation leads to direct and immediate loss of Confidentiality, Availability, or Integrity (CAT I).</LI>
<LI>exploitation potentially results in loss of Confidentiality, Availability, or Integrity (CAT II).</LI>
<LI>existence degrades protections against loss of Confidentiality, Availability, or Integrity (CAT III).</LI> </UL>

The following table summarizes the number of issues identified across the different STIGIDs broken down by Fortify Priority Order. The status of a STIGID is considered "In Place" when there are no issues reported for a given STIGID.

If the project is missing a Fortify Static Code Analyzer (SCA) scan, or the scan contains findings that have not been fixed, hidden or suppressed, STIGID APSC-DV-003170: CAT II is not considered "In Place". Similarly, if the project is missing a Fortify WebInspect scan, or the scan contains any critical findings, STIGID APSC-DV-001460: CAT II and STIGID APSC-DV-002930:

CAT II are not considered "In Place".

Name: WASC 2.00
ID: 74f8081d-dd49-49da-880f-6830cebe9777
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site. Version 2.00 of their Threat Classification outlines the attacks and weaknesses that can commonly lead to a website being compromised.

Name: WASC 24 + 2
ID: 9DC61E7F-1A48-4711-BBFD-E9DFF537871F
The Web Application Security Consortium (WASC) was created as a cooperative effort to standardize, clarify, and organize the threats to the security of a web site.

Properties

WinForms.CollectionMutationMonitor.Label=WinFormsDataSource
WinForms.ExtractEventHandlers=true
WinForms.TransformChangeNotificationPattern=true
WinForms.TransformDataBindings=true
WinForms.TransformMessageLoops=true
ast.loading.filter=false
awt.toolkit=sun.awt.windows.WToolkit
com.fortify.AuthenticationKey=C:\Users\IGEN862\AppData\Local/Fortify/config/tools
com.fortify.Core=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\Core
com.fortify.InstallRoot=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0
com.fortify.InstallationUserName=igen862
com.fortify.SCAExecutablePath=C:/Program Files/Fortify/Fortify_SCA_and_Apps_22.1.0/bin/sourceanalyzer.exe
com.fortify.TotalPhysicalMemory=33622642688
com.fortify.VS.RequireASPPrecompilation=true
com.fortify.WorkingDirectory=C:\Users\IGEN862\AppData\Local/Fortify
com.fortify.locale=en
com.fortify.log.console=false
com.fortify.sca.AddImpliedMethods=true
com.fortify.sca.AntCompilerClass=com.fortify.dev.ant.SCACompiler
com.fortify.sca.AppendLogFile=true
com.fortify.sca.BuildID=suricata-master
com.fortify.sca.BuildOptions=-pid-file C:\Windows\TEMP\3\PID1459044908173251012O.tmp -b suricata-master -machine-output C:\UPAPPS\DevWorkarea\suricata-master
com.fortify.sca.BundleControlflowIssues=true
com.fortify.sca.CfmlUndefinedVariablesAreTainted=true
com.fortify.sca.CollectPerformanceData=true
com.fortify.sca.CustomRulesDir=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\Core\config\customrules
com.fortify.sca.DaemonCompilers=com.fortify.sca.util.compilers.GppCompiler,com.fortify.sca.util.compilers.GccCompiler,com.fortify.sca.util.compilers.AppleGppCompiler,com.fortify.sca.util.compilers.AppleGccCompiler,com.fortify.sca.util.compilers.MicrosoftCompiler,com.fortify.sca.util.compilers.MicrosoftLinker,com.fortify.sca.util.compilers.LdCompiler,com.fortify.sca.util.compilers.ArUtil,com.fortify.sca.util.compilers.SunCCompiler,com.fortify.sca.util.compilers.SunCppCompiler,com.fortify.sca.util.compilers.IntelCompiler,com.fortify.sca.util.compilers.ExternalCppAdapter,com.fortify.sca.util.compilers.ClangCompiler
com.fortify.sca.DeadCodeFilter=true
com.fortify.sca.DeadCodeIgnoreTrivialPredicates=true
com.fortify.sca.DefaultAnalyzers=semantic:dataflow:controlflow:nullptr:configuration:content:structural:buffer

com.fortify.sca.DefaultFileTypes=java,rb,jsp,jspx,tag,tagx,tld,sql,cfm,php,phtml,ctp,pks,pkh,pkb,xml,config,settings,properties,dll,exe,inc,asp,vbscript,js,ini,bas,cls,vbs,frm,ctl,html,htm,xsd,wsdd,xmi,py,cfml,cfc,abap,xhtml,cpx,xcfg,jsff,as,mxml,cbl,cscfg,csdef,wadcfg,appxmanifest,wsdl,plist,bsp,ABAP,BSP
com.fortify.sca.DefaultJarsDirs=default_jars
com.fortify.sca.DefaultRulesDir=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\Core\config\rules
com.fortify.sca.DisableCFRules=19EF0414-88CD-4882-82FC-BF3A89865666,4E28CEFE-1B94-4711-BF5A-EDA5D1B3E6BF,A2D33B21-FE55-4C53-86C6-2AB5BF343738,7F4CC818-7525-440B-9C68-02267A80179A,7F80BA1C-82E9-4F2A-BBB4-ADFDFB27B215,E650C773-2BB6-42AA-BC29-370AAF0C53ED
com.fortify.sca.DisableDeadCodeElimination=false
com.fortify.sca.DisableFunctionPointers=false
com.fortify.sca.DisableGlobals=false
com.fortify.sca.DisableInferredConstants=false
com.fortify.sca.DisplayProgress=true
com.fortify.sca.EnableInterproceduralConstantResolution=true
com.fortify.sca.EnableNestedWrappers=true
com.fortify.sca.EnableStructuralMatchCache=true
com.fortify.sca.EnableWrapperDetection=true
com.fortify.sca.FVDLDisableDescriptions=false
com.fortify.sca.FVDLDisableProgramData=false
com.fortify.sca.FVDLDisableSnippets=false
com.fortify.sca.FVDLStylesheet=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\Core/resources/sca/fvdl2html.xsl
com.fortify.sca.IndirectCallGraphBuilders=WinFormsAdHocFunctionBuilder,VirtualCGBuilder,J2EEIndirectCGBuilder,JNICGBuilder,StoredProcedureResolver,JavaWSCGBuilder,StrutsCGBuilder,DotNetWSCGBuilder,SqlServerSPResolver,ASPCGBuilder,ScriptedCGBuilder,NewJspCustomTagCGBuilder,DotNetCABCGBuilder,StateInjectionCGBuilder,SqlServerSPResolver2,PHPLambdaResolver,JavaWebCGBuilder
com.fortify.sca.JVMArgs=-XX:+UseParallelGC -XX:SoftRefLRUPolicyMSPerMB=3000 --illegal-access=permit --add-exports=jdk.management/com.sun.management.internal=ALL-UNNAMED --add-exports=jdk.scripting.nashorn/jdk.nashorn.internal.runtime=ALL-UNNAMED --add-exports=java.base/jdk.internal.misc=ALL-UNNAMED --add-opens=java.base/java.nio=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/sun.nio.ch=ALL-UNNAMED --add-opens=java.base/java.lang.reflect=ALL-UNNAMED --add-opens=java.base/java.util.regex=ALL-UNNAMED --add-opens=java.base/java.net=ALL-UNNAMED --add-opens=java.base/javax.crypto=ALL-UNNAMED --add-opens=java.management/sun.management=ALL-UNNAMED -Xmx28858M -Xss16M
com.fortify.sca.JavaSourcepathSearch=true
com.fortify.sca.JdkVersion=1.8
com.fortify.sca.LogFile=C:\Users\IGEN862\AppData\Local\Fortify\sca22.1\log\sca
com.fortify.sca.LogFileDir=C:\Users\IGEN862\AppData\Local\Fortify\sca22.1\log
com.fortify.sca.LogFileExt=.log
com.fortify.sca.LogFileName=sca.log
com.fortify.sca.LogFileNameNoExt=sca
com.fortify.sca.LogFilePath=C:\Users\IGEN862\AppData\Local\Fortify\sca22.1\log\sca.log
com.fortify.sca.LogLevel=INFO
com.fortify.sca.LowSeverityCutoff=1.0
com.fortify.sca.MachineOutputMode=
com.fortify.sca.NoNestedOutTagOutput=org.apache.taglibs.standard.tag.rt.core.RemoveTag,org.apache.taglibs.standard.tag.rt.core.SetTag
com.fortify.sca.PHPVersion=7.4
com.fortify.sca.PID=18952
com.fortify.sca.Phase0HigherOrder.Languages=python,ruby
com.fortify.sca.Phase0HigherOrder.Level=1

com.fortify.sca.PidFile=C:\Windows\TEMP\3\PID6715109170714022454.tmp
com.fortify.sca.PrintPerformanceDataAfterScan=false
com.fortify.sca.ProjectRoot=C:\Users\IGEN862\AppData\Local/Fortify
com.fortify.sca.ProjectRoot=C:\Users\IGEN862\AppData\Local/Fortify
com.fortify.sca.PythonVersion=2
com.fortify.sca.Renderer=fpr
com.fortify.sca.RequireMapKeys=classrule
com.fortify.sca.ResultsFile=C:\UPAPPS\DevWorkarea\suricata-master\fortify-output\suricata-version2.fpr
com.fortify.sca.SolverTimeout=15
com.fortify.sca.SqlLanguage=TSQL
com.fortify.sca.SuppressLowSeverity=true
com.fortify.sca.ThreadCount.NameTableLoading=1
com.fortify.sca.TypeInferenceFunctionTimeout=60
com.fortify.sca.TypeInferenceLanguages=javascript,python,ruby
com.fortify.sca.TypeInferencePhase0Timeout=300
com.fortify.sca.UnicodeInputFile=true
com.fortify.sca.UniversalBlacklist=.*yyparse.*
com.fortify.sca.analyzer.controlflow.EnableLivenessOptimization=false
com.fortify.sca.analyzer.controlflow.EnableMachineFiltering=false
com.fortify.sca.analyzer.controlflow.EnableRefRuleOptimization=false
com.fortify.sca.analyzer.controlflow.EnableTimeOut=true
com.fortify.sca.compilers.ant=com.fortify.sca.util.compilers.AntAdapter
com.fortify.sca.compilers.ar=com.fortify.sca.util.compilers.ArUtil
com.fortify.sca.compilers.armcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.armcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.c++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.c89=com.fortify.sca.util.compilers.C89Compiler
com.fortify.sca.compilers.cc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.cl=com.fortify.sca.util.compilers.MicrosoftCompiler
com.fortify.sca.compilers.clearmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.devenv=com.fortify.sca.util.compilers.DevenvNetAdapter
com.fortify.sca.compilers.fortify=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.compilers.g++=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++-*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++2*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++3*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.g++4*=com.fortify.sca.util.compilers.GppCompiler
com.fortify.sca.compilers.gcc=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc-*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc2*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc3*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gcc4*=com.fortify.sca.util.compilers.GccCompiler
com.fortify.sca.compilers.gmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.icc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.icl=com.fortify.sca.util.compilers.MicrosoftCompiler
com.fortify.sca.compilers.icpc=com.fortify.sca.util.compilers.IntelCompiler
com.fortify.sca.compilers.jam=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.javac=com.fortify.sca.util.compilers.JavacCompiler
com.fortify.sca.compilers.ld=com.fortify.sca.util.compilers.LdCompiler
com.fortify.sca.compilers.link=com.fortify.sca.util.compilers.MicrosoftLinker
com.fortify.sca.compilers.make=com.fortify.sca.util.compilers.TouchlessCompiler

com.fortify.sca.compilers.msbuild=com.fortify.sca.util.compilers.MSBuildAdapter
com.fortify.sca.compilers.msdev=com.fortify.sca.util.compilers.DevenvAdapter
com.fortify.sca.compilers.mvn=com.fortify.sca.util.compilers.MavenAdapter
com.fortify.sca.compilers.nmake=com.fortify.sca.util.compilers.TouchlessCompiler
com.fortify.sca.compilers.tcc=com.fortify.sca.util.compilers.ArmCcCompiler
com.fortify.sca.compilers.tcpp=com.fortify.sca.util.compilers.ArmCppCompiler
com.fortify.sca.compilers.touchless=com.fortify.sca.util.compilers.FortifyCompiler
com.fortify.sca.compilers.xilink=com.fortify.sca.util.compilers.MicrosoftLinker
com.fortify.sca.cpfe.441.command=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\Core/private-bin/sca/cpfe441.rfct
com.fortify.sca.cpfe.command=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\Core/private-bin/sca/cpfe48
com.fortify.sca.cpfe.file.option=--gen_c_file_name
com.fortify.sca.cpfe.options=--remove_unneeded_entities --suppress_vtbl -tused
com.fortify.sca.env.classpath=.;C:\db2\RTC-11~1.01\SQLLIB\java\db2java.zip;C:\db2\RTC-11~1.01\SQLLIB\java\db2jcc4.jar;C:\db2\RTC-11~1.01\SQLLIB\java\db2jcc_license_cu.jar;C:\db2\RTC-11~1.01\SQLLIB\bin
com.fortify.sca.env.exesearchpath=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin;C:/Program Files/Fortify/Fortify_SCA_and_Apps_22.1.0/Core/private-bin/awb/../../../jre/bin/server;C:/Program Files/Fortify/Fortify_SCA_and_Apps_22.1.0/Core/private-bin/awb/../../../jre/bin;C:\Program Files\Eclipse Adoptium\jdk-17.0.1.12-hotspot\bin;C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin;C:\Program Files (x86)\Nice Systems\NICE Player Codec Pack\\;c:\program files\adoptopenjdk\jdk-11.0.10.9-hotspot\bin;c:\oracle\ora-19.03.00.00-32\client_32\bin;c:\oracle\ora-19.03.00.00-64\client_64\bin;c:\program files (x86)\common files\oracle\java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\system32\wbem;C:\Windows\system32\windowspowershell\v1.0\;C:\Windows\system32\openssh\;c:\program files (x86)\java\jdk1.6.0_10\bin;c:\software\phantomjs\bin;c:\oracle\ora-11.02.00.02\bin;C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\ManagementStudio\;C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\;C:\Program Files\Microsoft SQL Server\110\Tools\Binn\;C:\Program Files (x86)\Microsoft Visual Studio 10.0\Common7\IDE\PrivateAssemblies\;C:\Program Files (x86)\Microsoft SQL Server\110\DTS\Binn\;C:\Program Files\SlikSvn\bin;C:\Program Files (x86)\Microsoft SDKs\TypeScript\1.0\;C:\Program Files\Microsoft SQL Server\120\Tools\Binn\;c:\software\maven\3.5.0\bin;C:\Program Files\TortoiseSVN\bin;C:\Program Files (x86)\NICE Systems\NICE Player Release 3\\;%NPM_HOME%;C:\db2\RTC-11~1.01\SQLLIB\BIN;C:\db2\RTC-11~1.01\SQLLIB\FUNCTION;C:\Program Files (x86)\PuTTY\;C:\Program Files\Git\cmd;C:\Program Files\Microsoft VS Code\bin;C:\Program Files (x86)\Microsoft SQL Server\160\DTS\Binn\;C:\Program Files\Azure Data Studio\bin;C:\Program Files\Microsoft SQL Server\130\Tools\Binn\;C:\Program Files (x86)\Microsoft SQL Server\120\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\130\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\140\DTS\Binn\;C:\Program Files\TortoiseGit\bin;C:\software\Ant\1.9.4\bin;C:\Users\IGEN862\AppData\Local\Microsoft\WindowsApps;c:\software\maven\3.5.0\bin;C:\Program Files\Java\jdk1.8.0_121\bin;C:\software\AndroidSDK\sdk\tools;C:\software\AndroidSDK\sdk\platform-tools;C:\software\Gradle\5.2.1\bin;c:\software\scrcpy;C:\Program Files\Git\usr\bin;C:\Program Files\nodejs-12.18.3;C:\Users\IGEN862\AppData\Roaming\npm;C:\software\jboss\EWS\Tomcat-8.0.26-64bit\bin;C:\software\Gradle\5.2.1\bin;C:\UPAPPS\DevWorkarea\axis2-1.8.2;;C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin\..\Core\lib;C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin;
com.fortify.sca.fileextensions.ABAP=ABAP
com.fortify.sca.fileextensions.BSP=ABAP
com.fortify.sca.fileextensions.abap=ABAP
com.fortify.sca.fileextensions.appxmanifest=XML
com.fortify.sca.fileextensions.as=ACTIONSCRIPT
com.fortify.sca.fileextensions.asp=ASP
com.fortify.sca.fileextensions.bas=VB6
com.fortify.sca.fileextensions.bsp=ABAP
com.fortify.sca.fileextensions.cfc=CFML
com.fortify.sca.fileextensions.cfm=CFML
com.fortify.sca.fileextensions.cfml=CFML
com.fortify.sca.fileextensions.cls=VB6
com.fortify.sca.fileextensions.config=XML

com.fortify.sca.fileextensions.cpx=XML
com.fortify.sca.fileextensions.cs=CSHARP
com.fortify.sca.fileextensions.cscfg=XML
com.fortify.sca.fileextensions.csdef=XML
com.fortify.sca.fileextensions.ctl=VB6
com.fortify.sca.fileextensions.ctp=PHP
com.fortify.sca.fileextensions.dll=MSIL
com.fortify.sca.fileextensions.erb=RUBY_ERB
com.fortify.sca.fileextensions.exe=MSIL
com.fortify.sca.fileextensions.faces=JSPX
com.fortify.sca.fileextensions.frm=VB6
com.fortify.sca.fileextensions.htm=HTML
com.fortify.sca.fileextensions.html=HTML
com.fortify.sca.fileextensions.ini=JAVA_PROPERTIES
com.fortify.sca.fileextensions.java=JAVA
com.fortify.sca.fileextensions.js=JAVASCRIPT
com.fortify.sca.fileextensions.jsff=JSPX
com.fortify.sca.fileextensions.jsp=JSP
com.fortify.sca.fileextensions.jspx=JSPX
com.fortify.sca.fileextensions.mdl=MSIL
com.fortify.sca.fileextensions.mod=MSIL
com.fortify.sca.fileextensions.mxml=MXML
com.fortify.sca.fileextensions.php=PHP
com.fortify.sca.fileextensions.phtml=PHP
com.fortify.sca.fileextensions.pkb=PLSQL
com.fortify.sca.fileextensions.pkh=PLSQL
com.fortify.sca.fileextensions.pks=PLSQL
com.fortify.sca.fileextensions.plist=XML
com.fortify.sca.fileextensions.properties=JAVA_PROPERTIES
com.fortify.sca.fileextensions.py=PYTHON
com.fortify.sca.fileextensions.rb=RUBY
com.fortify.sca.fileextensions.settings=XML
com.fortify.sca.fileextensions.sql=SQL
com.fortify.sca.fileextensions.tag=JSP
com.fortify.sca.fileextensions.tagx=JSP
com.fortify.sca.fileextensions.tld=TLD
com.fortify.sca.fileextensions.vb=VB
com.fortify.sca.fileextensions.vbs=VBSCRIPT
com.fortify.sca.fileextensions.vbscript=VBSCRIPT
com.fortify.sca.fileextensions.wadcfg=XML
com.fortify.sca.fileextensions.wsdd=XML
com.fortify.sca.fileextensions.wsdl=XML
com.fortify.sca.fileextensions.xcfg=XML
com.fortify.sca.fileextensions.xhtml=JSPX
com.fortify.sca.fileextensions.xmi=XML
com.fortify.sca.fileextensions.xml=XML
com.fortify.sca.fileextensions.xsd=XML
com.fortify.sca.jsp.UseNativeParser=true
com.fortify.sca.parser.python.ignore.module.1=test.badsyntax_future3
com.fortify.sca.parser.python.ignore.module.2=test.badsyntax_future4
com.fortify.sca.parser.python.ignore.module.3=test.badsyntax_future5

com.fortify.sca.parser.python.ignore.module.4=test.badsyntax_future6
com.fortify.sca.parser.python.ignore.module.5=test.badsyntax_future7
com.fortify.sca.parser.python.ignore.module.6=test.badsyntax_future8
com.fortify.sca.parser.python.ignore.module.7=test.badsyntax_future9
com.fortify.sca.parser.python.ignore.module.8=test.badsyntax_nocaret
com.fortify.search.defaultSyntaxVer=2
com.sun.management.jmxremote=true
dotnet.install.dir=C:\Windows\Microsoft.NET\Framework64\
dotnet.sdk.v11.install.dir=
dotnet.sdk.v20.install.dir=
dotnet.sdk.v3x.install.dir=
dotnet.v30.referenceAssemblies=C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\
dotnet.v35.referenceAssemblies=C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.5\
file.encoding=Cp1252
file.separator=\
ide.hide.excluded.files=false
idea.home.path=C:\Windows\TEMP\3\
idea.ignore.disabled.plugins=true
idea.io.use.nio2=true
idea.plugins.compatible.build=201.6668.13
java.awt.graphicsenv=sun.awt.Win32GraphicsEnvironment
java.awt.headless=true
java.awt.printerjob=sun.awt.windows.WPrinterJob
java.class.path=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\Core\lib\exe\sca-exe.jar
java.class.version=55.0
java.home=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\jre
java.io.tmpdir=C:\Windows\TEMP\3\
java.library.path=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin;C:\Windows\Sun\Java\bin;C:\Windows\system32;C:\Windows;C:/Program Files/Fortify/Fortify_SCA_and_Apps_22.1.0/Core/private-bin/awb/../../../jre/bin/server;C:/Program Files/Fortify/Fortify_SCA_and_Apps_22.1.0/Core/private-bin/awb/../../../jre/bin;C:\Program Files\Eclipse Adoptium\jdk-17.0.1.12-hotspot\bin;C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin;C:\Program Files (x86)\Nice Systems\NICE Player Codec Pack\\;c:\program files\adoptopenjdk\jdk-11.0.10.9-hotspot\bin;c:\oracle\ora-19.03.00.00-32\client_32\bin;c:\oracle\ora-19.03.00.00-64\client_64\bin;c:\program files (x86)\common files\oracle\java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\system32\wbem;C:\Windows\system32\windowspowershell\v1.0\;C:\Windows\system32\openssh\;c:\program files (x86)\java\jdk1.6.0_10\bin;c:\software\phantomjs\bin;c:\oracle\ora-11.02.00.02\bin;C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\ManagementStudio\;C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\;C:\Program Files\Microsoft SQL Server\110\Tools\Binn\;C:\Program Files (x86)\Microsoft Visual Studio 10.0\Common7\IDE\PrivateAssemblies\;C:\Program Files (x86)\Microsoft SQL Server\110\DTS\Binn\;C:\Program Files\SlikSvn\bin;C:\Program Files (x86)\Microsoft SDKs\TypeScript\1.0\;C:\Program Files\Microsoft SQL Server\120\Tools\Binn\;c:\software\maven\3.5.0\bin;C:\Program Files\TortoiseSVN\bin;C:\Program Files (x86)\NICE Systems\NICE Player Release 3\\;%NPM_HOME%;C:\db2\RTC-11~1.01\SQLLIB\BIN;C:\db2\RTC-11~1.01\SQLLIB\FUNCTION;C:\Program Files (x86)\PuTTY\;C:\Program Files\Git\cmd;C:\Program Files\Microsoft VS Code\bin;C:\Program Files (x86)\Microsoft SQL Server\160\DTS\Binn\;C:\Program Files\Azure Data Studio\bin;C:\Program Files\Microsoft SQL Server\130\Tools\Binn\;C:\Program Files (x86)\Microsoft SQL Server\120\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\130\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\140\DTS\Binn\;C:\Program Files\TortoiseGit\bin;C:\software\Ant\1.9.4\bin;C:\Users\IGEN862\AppData\Local\Microsoft\WindowsApps;c:\software\maven\3.5.0\bin;C:\Program Files\Java\jdk1.8.0_121\bin;C:\software\AndroidSDK\sdk\tools;C:\software\AndroidSDK\sdk\platform-tools;C:\software\Gradle\5.2.1\bin;c:\software\scrcpy;C:\Program Files\Git\usr\bin;C:\Program Files\nodejs-12.18.3;C:\Users\IGEN862\AppData\Roaming\npm;C:\software\jboss\EWS\Tomcat-8.0.26-64bit\bin;C:\software\Gradle\5.2.1\bin;C:\UPAPPS\DevWorkarea\axis2-1.8.2;;C:\Program

Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin\..\Core\lib;C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin;;.
java.rmi.server.randomIDs=true
java.runtime.name=OpenJDK Runtime Environment
java.runtime.version=11.0.14.1+1-LTS
java.specification.name=Java Platform API Specification
java.specification.vendor=Oracle Corporation
java.specification.version=11
java.vendor=Azul Systems, Inc.
java.vendor.url=http://www.azul.com/
java.vendor.url.bug=http://www.azul.com/support/
java.vendor.version=Zulu11.54+25-CA
java.version=11.0.14.1
java.version.date=2022-02-08
java.vm.compressedOopsMode=Zero based
java.vm.info=mixed mode
java.vm.name=OpenJDK 64-Bit Server VM
java.vm.specification.name=Java Virtual Machine Specification
java.vm.specification.vendor=Oracle Corporation
java.vm.specification.version=11
java.vm.vendor=Azul Systems, Inc.
java.vm.version=11.0.14.1+1-LTS
jdk.debug=release
jdk.vendor.version=Zulu11.54+25-CA
line.separator=

log4j.configurationFile=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\Core\config\log4j2.xml
log4j.isThreadContextMapInheritable=true
max.file.path.length=255
os.arch=amd64
os.name=Windows 10
os.version=10.0
path.separator=;
project.structure.add.tools.jar.to.new.jdk=false
psi.incremental.reparse.depth.limit=1000
psi.track.invalidation=true
stderr.isatty=false
stdout.isatty=false
sun.arch.data.model=64
sun.boot.library.path=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\jre\bin
sun.cpu.endian=little
sun.cpu.isalist=amd64
sun.desktop=windows
sun.io.unicode.encoding=UnicodeLittle
sun.java.command=sourceanalyzer -Djava.awt.headless=true -Dcom.sun.management.jmxremote=true -XX:+UseParallelGC -XX:SoftRefLRUPolicyMSPerMB=3000 --illegal-access=permit --add-exports=jdk.management/com.sun.management.internal=ALL-UNNAMED --add-exports=jdk.scripting.nashorn/jdk.nashorn.internal.runtime=ALL-UNNAMED --add-exports=java.base/jdk.internal.misc=ALL-UNNAMED --add-opens=java.base/java.nio=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/sun.nio.ch=ALL-UNNAMED --add-opens=java.base/java.lang.reflect=ALL-UNNAMED --add-opens=java.base/java.util.regex=ALL-UNNAMED --add-opens=java.base/java.net=ALL-UNNAMED --add-

opens=java.base/javax.crypto=ALL-UNNAMED --add-opens=java.management/sun.management=ALL-UNNAMED -Dwin32.LocalAppdata=C:\Users\IGEN862\AppData\Local -Ddotnet.install.dir=C:\Windows\Microsoft.NET\Framework64\ -Ddotnet.sdk.v11.install.dir= -Ddotnet.sdk.v20.install.dir= -Ddotnet.sdk.v3x.install.dir= -Ddotnet.v30.referenceAssemblies=C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.0\ -Ddotnet.v35.referenceAssemblies=C:\Program Files\Reference Assemblies\Microsoft\Framework\v3.5\ -Dvs.140.dotnet.clr.version=v4.0.30319 -Dcom.fortify.sca.env.classpath=.;C:\db2\RTC-11~1.01\SQLLIB\java\db2java.zip;C:\db2\RTC-11~1.01\SQLLIB\java\db2jcc4.jar;C:\db2\RTC-11~1.01\SQLLIB\java\db2jcc_license_cu.jar;C:\db2\RTC-11~1.01\SQLLIB\bin -Dcom.fortify.sca.env.exesearchpath=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin;C:/Program Files/Fortify/Fortify_SCA_and_Apps_22.1.0/Core/private-bin/awb/../../../jre/bin/server;C:/Program Files/Fortify/Fortify_SCA_and_Apps_22.1.0/Core/private-bin/awb/../../../jre/bin;C:\Program Files\Eclipse Adoptium\jdk-17.0.1.12-hotspot\bin;C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin;C:\Program Files (x86)\Nice Systems\NICE Player Codec Pack\\;c:\program files\adoptopenjdk\jdk-11.0.10.9-hotspot\bin;c:\oracle\ora-19.03.00.00-32\client_32\bin;c:\oracle\ora-19.03.00.00-64\client_64\bin;c:\program files (x86)\common files\oracle\java\javapath;C:\Windows\system32;C:\Windows;C:\Windows\system32\wbem;C:\Windows\system32\windowspowershell\v1.0\;C:\Windows\system32\openssh\;c:\program files (x86)\java\jdk1.6.0_10\bin;c:\software\phantomjs\bin;c:\oracle\ora-11.02.00.02\bin;C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\ManagementStudio\;C:\Program Files (x86)\Microsoft SQL Server\110\Tools\Binn\;C:\Program Files\Microsoft SQL Server\110\Tools\Binn\;C:\Program Files (x86)\Microsoft Visual Studio 10.0\Common7\IDE\PrivateAssemblies\;C:\Program Files (x86)\Microsoft SQL Server\110\DTS\Binn\;C:\Program Files\SlikSvn\bin;C:\Program Files (x86)\Microsoft SDKs\TypeScript\1.0\;C:\Program Files\Microsoft SQL Server\120\Tools\Binn\;c:\software\maven\3.5.0\bin;C:\Program Files\TortoiseSVN\bin;C:\Program Files (x86)\NICE Systems\NICE Player Release 3\\;%NPM_HOME%;C:\db2\RTC-11~1.01\SQLLIB\BIN;C:\db2\RTC-11~1.01\SQLLIB\FUNCTION;C:\Program Files (x86)\PuTTY\;C:\Program Files\Git\cmd;C:\Program Files\Microsoft VS Code\bin;C:\Program Files (x86)\Microsoft SQL Server\160\DTS\Binn\;C:\Program Files\Azure Data Studio\bin;C:\Program Files\Microsoft SQL Server\130\Tools\Binn\;C:\Program Files (x86)\Microsoft SQL Server\120\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\130\DTS\Binn\;C:\Program Files (x86)\Microsoft SQL Server\140\DTS\Binn\;C:\Program Files\TortoiseGit\bin;C:\software\Ant\1.9.4\bin;C:\Users\IGEN862\AppData\Local\Microsoft\WindowsApps;c:\software\maven\3.5.0\bin;C:\Program Files\Java\jdk1.8.0_121\bin;C:\software\AndroidSDK\sdk\tools;C:\software\AndroidSDK\sdk\platform-tools;C:\software\Gradle\5.2.1\bin;c:\software\scrcpy;C:\Program Files\Git\usr\bin;C:\Program Files\nodejs-12.18.3;C:\Users\IGEN862\AppData\Roaming\npm;C:\software\jboss\EWS\Tomcat-8.0.26-64bit\bin;C:\software\Gradle\5.2.1\bin;C:\UPAPPS\DevWorkarea\axis2-1.8.2;;C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin\..\Core\lib;C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin; -Dcom.fortify.sca.ProjectRoot=C:\Users\IGEN862\AppData\Local/Fortify -Dstdout.isatty=false -Dstderr.isatty=false -Dcom.fortify.sca.PID=18952 -Xmx28858M -Dcom.fortify.TotalPhysicalMemory=33622642688 -Xss16M -Dcom.fortify.sca.JVMArgs=-XX:+UseParallelGC -XX:SoftRefLRUPolicyMSPerMB=3000 --illegal-access=permit --add-exports=jdk.management/com.sun.management.internal=ALL-UNNAMED --add-exports=jdk.scripting.nashorn/jdk.nashorn.internal.runtime=ALL-UNNAMED --add-exports=java.base/jdk.internal.misc=ALL-UNNAMED --add-opens=java.base/java.nio=ALL-UNNAMED --add-opens=java.base/java.util=ALL-UNNAMED --add-opens=java.base/java.lang=ALL-UNNAMED --add-opens=java.base/java.io=ALL-UNNAMED --add-opens=java.base/sun.nio.ch=ALL-UNNAMED --add-opens=java.base/java.lang.reflect=ALL-UNNAMED --add-opens=java.base/java.util.regex=ALL-UNNAMED --add-opens=java.base/java.net=ALL-UNNAMED --add-opens=java.base/javax.crypto=ALL-UNNAMED --add-opens=java.management/sun.management=ALL-UNNAMED -Xmx28858M -Xss16M -Djava.class.path=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\Core\lib\exe\sca-exe.jar -scan -pid-file C:\Windows\TEMP\3\PID6715109170714022454.tmp @C:\Users\IGEN862\AppData\Local\Fortify\AWB-22.1.0\suricata-master\suricata-masterScan.txt
sun.jnu.encoding=Cp1252
sun.management.compiler=HotSpot 64-Bit Tiered Compilers
sun.os.patch.level=
user.country=US
user.dir=C:\Program Files\Fortify\Fortify_SCA_and_Apps_22.1.0\bin
user.home=C:\Users\IGEN862

user.language=en
user.name=igen862
user.script=
user.timezone=America/Chicago
user.variant=
vs.140.dotnet.clr.version=v4.0.30319
win32.LocalAppdata=C:\Users\IGEN862\AppData\Local

Commandline Arguments

-scan
-pid-file
C:\Windows\TEMP\3\PID6715109170714022454.tmp
-b
suricata-master
-machine-output
-format
fpr
-f
C:\UPAPPS\DevWorkarea\suricata-master\fortify-output\suricata-version2.fpr

Warnings

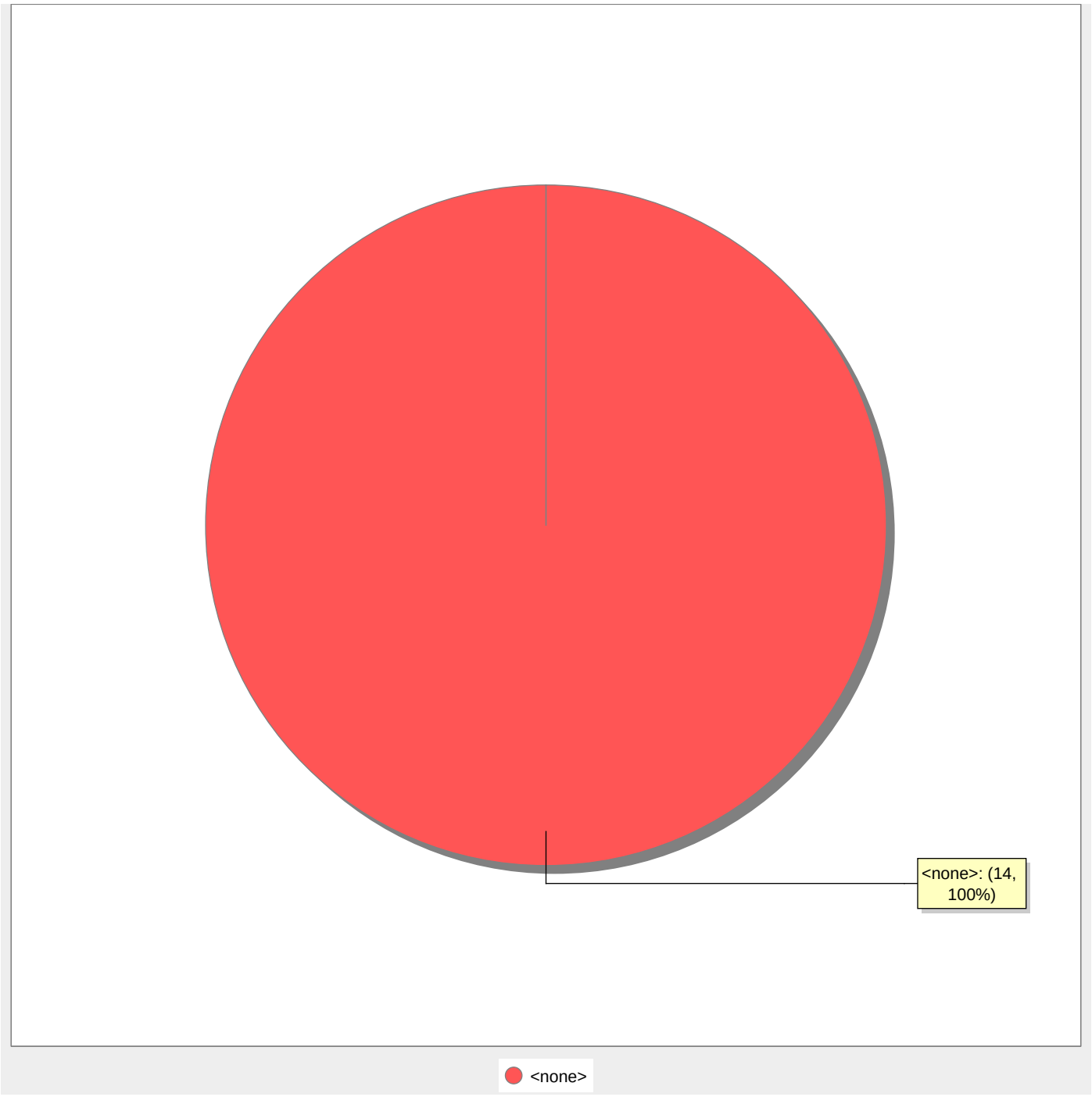
[12004] The Python frontend was unable to resolve the following import:
suricata.sc.suricatasc at C:\UPAPPS\DevWorkarea\suricata-master\python\suricata\sc__init__.py:1.
jinja2 at C:\UPAPPS\DevWorkarea\suricata-master\scripts\dnp3-gen\dnp3-gen.py:28.
io at C:\UPAPPS\DevWorkarea\suricata-master\scripts\setup-app-layer.py:9.
logging at C:\UPAPPS\DevWorkarea\suricata-master\python\suricata\ctl\filestore.py:24.
json at C:\UPAPPS\DevWorkarea\suricata-master\python\suricata\sc\suricatasc.py:19.
unittest at C:\UPAPPS\DevWorkarea\suricata-master\python\suricata\ctl\test_filestore.py:3.
suricata.sc at C:\UPAPPS\DevWorkarea\suricata-master\python\suricatasc__init__.py:1.
gzip at C:\UPAPPS\DevWorkarea\suricata-master\qa\sock_to_gzip_file.py:6.
requests at C:\UPAPPS\DevWorkarea\suricata-master\doc\userguide\convert.py:9.
argparse at C:\UPAPPS\DevWorkarea\suricata-master\python\suricata\ctl\main.py:19.
shlex at C:\UPAPPS\DevWorkarea\suricata-master\doc\userguide\conf.py:17.
yaml at C:\UPAPPS\DevWorkarea\suricata-master\scripts\dnp3-gen\dnp3-gen.py:26.
[12007] You may need to add some arguments to the -python-path argument to SCA.
[12041] The Python frontend was unable to resolve import of the following optional modules :
sphinx_rtd_theme at C:\UPAPPS\DevWorkarea\suricata-master\doc\userguide\conf.py:139.
simplejson at C:\UPAPPS\DevWorkarea\suricata-master\python\suricata\sc\suricatasc.py:17.
[12042] Imports located inside try statements are considered as optional
[242] The property com.fortify.sca.cpfe.441.command is not a valid property.
[242] The property com.fortify.sca.cpfe.file.option is not a valid property.
[242] The property com.fortify.sca.cpfe.options is not a valid property.
[242] The property com.fortify.sca.cpfe.command is not a valid property.
[242] The property com.fortify.sca.DisplayProgress is not a valid property.

Issue Count by Category

Issues by Category	
Credential Management: Hardcoded API Credentials	4
Path Manipulation	3
Dockerfile Misconfiguration: Dependency Confusion	2
System Information Leak: Internal	2
Dockerfile Misconfiguration: Default User Privilege	1
Dynamic Code Evaluation: Code Injection	1
Poor Error Handling: Empty Catch Block	1

Issue Breakdown by Analysis

Issues by Analysis



New Issues

Issues by New Issue

The following issues have been discovered since the last scan.