Fortify Audit Workbench

SANS Top 25 2011

js-scan

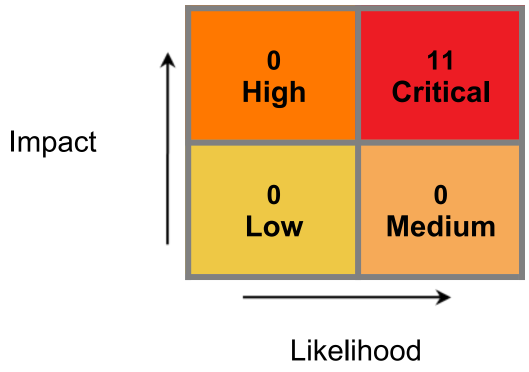
Table of Contents

- Executive Summary
- Project Description
- Issue Breakdown
- Issue Details
  - Risky Resource Management - CWE ID 022
  - Insecure Interaction - CWE ID 078
  - Insecure Interaction - CWE ID 079
  - Insecure Interaction - CWE ID 089
  - Risky Resource Management - CWE ID 120
  - Risky Resource Management - CWE ID 131
  - Risky Resource Management - CWE ID 134
  - Risky Resource Management - CWE ID 190
  - Porous Defenses - CWE ID 250
  - Porous Defenses - CWE ID 306
  - Porous Defenses - CWE ID 307
  - Porous Defenses - CWE ID 311
  - Porous Defenses - CWE ID 327
  - Insecure Interaction - CWE ID 352
  - Insecure Interaction - CWE ID 434
  - Risky Resource Management - CWE ID 494
  - Insecure Interaction - CWE ID 601
  - Risky Resource Management - CWE ID 676
  - Porous Defenses - CWE ID 732
  - Porous Defenses - CWE ID 759
  - Porous Defenses - CWE ID 798
  - Porous Defenses - CWE ID 807
  - Risky Resource Management - CWE ID 829
  - Porous Defenses - CWE ID 862
  - Porous Defenses - CWE ID 863
- Description of Key Terminology
- About Fortify Solutions

Executive Summary

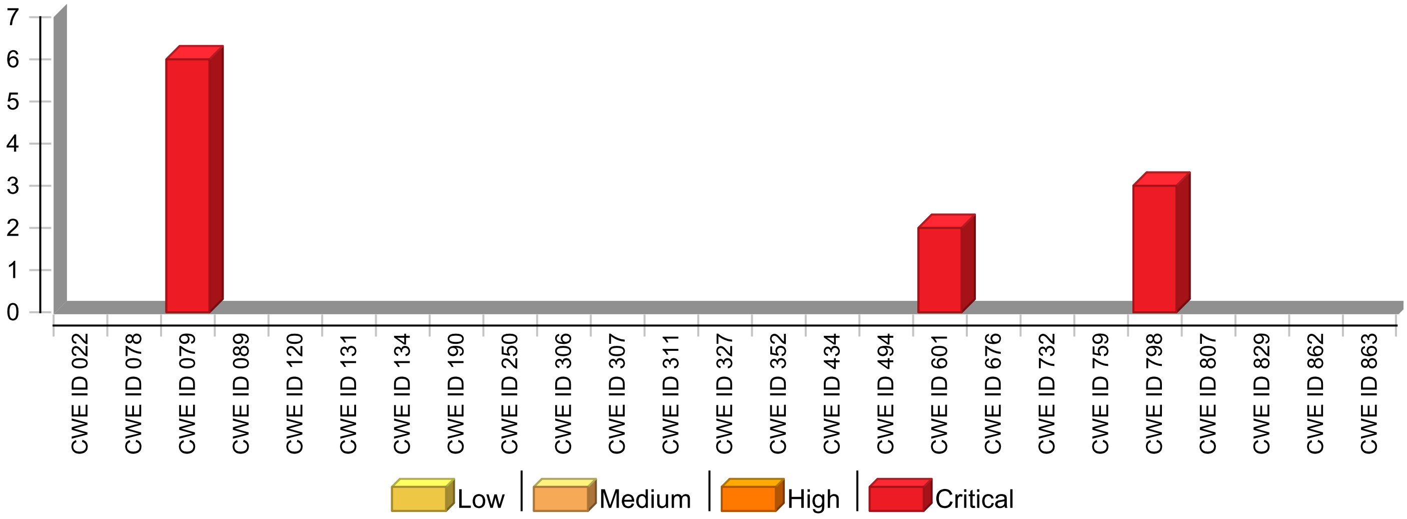
Project Name:	js-scan
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
WebInspect Agent:	Results Not Present
Other:	Results Not Present

Issues by Priority



SANS Top 25 2011 groups	Total	Status
Insecure Interaction	8	**FAIL**
Porous Defenses	3	**FAIL**
Risky Resource Management	0	**PASS**

Issues by SANS Top 25 2011 Categories



* The detailed sections following the Executive Summary contain specifics.

Project Description

This section provides an overview of the Fortify scan engines used for this project, as well as the project meta-information.

Issue BreakDown

The following table summarizes the number of issues identified across the different SANS Top 25 2011 categories and broken down by Fortify Priority Order.

Insecure Interaction	Fortify Priority				Total Issues
	Critical	High	Medium	Low	
Insecure Interaction - CWE ID 078	0	0	0	0	0
Insecure Interaction - CWE ID 079	6	0	0	0	6
Insecure Interaction - CWE ID 089	0	0	0	0	0
Insecure Interaction - CWE ID 352	0	0	0	0	0
Insecure Interaction - CWE ID 434	0	0	0	0	0
Insecure Interaction - CWE ID 601	2	0	0	0	2

Risky Resource Management	Fortify Priority				Total Issues
	Critical	High	Medium	Low	
Risky Resource Management - CWE ID 022	0	0	0	0	0
Risky Resource Management - CWE ID 120	0	0	0	0	0
Risky Resource Management - CWE ID 131	0	0	0	0	0
Risky Resource Management - CWE ID 134	0	0	0	0	0
Risky Resource Management - CWE ID 190	0	0	0	0	0
Risky Resource Management - CWE ID 494	0	0	0	0	0
Risky Resource Management - CWE ID 676	0	0	0	0	0
Risky Resource Management - CWE ID 829	0	0	0	0	0

Porous Defenses	Fortify Priority				Total Issues
	Critical	High	Medium	Low	
Porous Defenses - CWE ID 250	0	0	0	0	0
Porous Defenses - CWE ID 306	0	0	0	0	0
Porous Defenses - CWE ID 307	0	0	0	0	0
Porous Defenses - CWE ID 311	0	0	0	0	0
Porous Defenses - CWE ID 327	0	0	0	0	0
Porous Defenses - CWE ID 732	0	0	0	0	0
Porous Defenses - CWE ID 759	0	0	0	0	0
Porous Defenses - CWE ID 798	3	0	0	0	3
Porous Defenses - CWE ID 807	0	0	0	0	0
Porous Defenses - CWE ID 862	0	0	0	0	0
Porous Defenses - CWE ID 863	0	0	0	0	0

NOTE:
1. Reported issues in the above table may violate more than one SANS Top 25 2011 category. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Executive Summary table.

Issue Details

Below is an enumeration of all issues found in the project. The issues are organized by SANS Top 25 2011, Fortify Priority Order, and vulnerability category. The issues are then further broken down by the package, namespace, or location in which they occur. Issues reported at the same line number with the same category originate from different taint sources.

Risky Resource Management - CWE ID 022

Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal'). CWE-22 states: "The software uses external input to construct a pathname that is intended to identify a file or directory that is located underneath a restricted parent directory, but the software does not properly neutralize special elements within the pathname that can cause the pathname to resolve to a location that is outside of the restricted directory".

No Issues

Insecure Interaction - CWE ID 078

Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'). CWE-78 states: "The software constructs all or part of an OS command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended OS command when it is sent to a downstream component".

No Issues

Insecure Interaction - CWE ID 079

Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'). CWE-79 states: "The software does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users".

Cross-Site Scripting: DOM		Critical
Package: src.core		
Location	**Analysis Info**	**Analyzer**
src/core/cache-storage.ts:33	**Sink:** Assignment to link.href **Enclosing Method:** getOrigin() **Source:** Read window.location **from** setContext() **In** src/core/cache-storage.ts:44	SCA
src/core/cache-storage.ts:34	**Sink:** Assignment to link.href **Enclosing Method:** getOrigin() **Source:** Read link.href **from** getOrigin() **In** src/core/cache-storage.ts:34	SCA
src/core/cache-storage.ts:34	**Sink:** Assignment to link.href **Enclosing Method:** getOrigin() **Source:** Read window.location **from** setContext() **In** src/core/cache-storage.ts:44	SCA
Package: tests		
Location	**Analysis Info**	**Analyzer**
tests/test.js:9	**Sink:** write() **Enclosing Method:** appendScript() **Source:** Read window.location **from** appendScript() **In** tests/test.js:12	SCA
tests/test.js:9	**Sink:** write() **Enclosing Method:** appendScript() **Source:** Read window.location **from** appendScript() **In** tests/test.js:10	SCA
Package: www.src		
Location	**Analysis Info**	**Analyzer**
www/src/preview.ts:55	**Sink:** Assignment to testLink.href **Enclosing Method:** selectTest() **Source:** Read testSelector.value **from** lambda() **In** www/src/preview.ts:98	SCA

Insecure Interaction - CWE ID 089

Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection'). CWE-89 states: "The software constructs all or part of an SQL command using externally-influenced input from an upstream component, but it does not neutralize or incorrectly neutralizes special elements that could modify the intended SQL command when it is sent to a downstream component".

No Issues

Risky Resource Management - CWE ID 120

Buffer Copy without Checking Size of Input ('Classic Buffer Overflow'). CWE-120 states: "The program copies an input buffer to an output buffer without verifying that the size of the input buffer is less than the size of the output buffer, leading to a buffer overflow".

No Issues

Risky Resource Management - CWE ID 131

Incorrect Calculation of Buffer Size. CWE-131 states: "The software does not correctly calculate the size to be used when allocating a buffer, which could lead to a buffer overflow".

No Issues

Risky Resource Management - CWE ID 134

Uncontrolled Format String. CWE-134 states: "The software uses externally-controlled format strings in printf-style functions, which can lead to buffer overflows or data representation problems".

No Issues

Risky Resource Management - CWE ID 190

Integer Overflow or Wraparound. CWE-190 states: "The software performs a calculation that can produce an integer overflow or wraparound, when the logic assumes that the resulting value will always be larger than the original value. This can introduce other weaknesses when the calculation is used for resource management or execution control".

No Issues

Porous Defenses - CWE ID 250

Execution with Unnecessary Privileges. CWE-250 states: "The software performs an operation at a privilege level that is higher than the minimum level required, which creates new weaknesses or amplifies the consequences of other weaknesses".

No Issues

Porous Defenses - CWE ID 306

Missing Authentication for Critical Function. CWE-306 states: "The software does not perform any authentication for functionality that requires a provable user identity or consumes a significant amount of resources".

No Issues

Porous Defenses - CWE ID 307

Improper Restriction of Excessive Authentication Attempts. CWE-307 states: "The software does not implement sufficient measures to prevent multiple failed authentication attempts within in a short time frame, making it more susceptible to brute force attacks".

No Issues

Porous Defenses - CWE ID 311

Missing Encryption of Sensitive Data. CWE-311 states: "The software does not encrypt sensitive or critical information before storage or transmission".

No Issues

Porous Defenses - CWE ID 327

Use of a Broken or Risky Cryptographic Algorithm. CWE-327 states: "The use of a broken or risky cryptographic algorithm is an unnecessary risk that may result in the exposure of sensitive information".

No Issues

Insecure Interaction - CWE ID 352

Cross-Site Request Forgery (CSRF). CWE-352 states: "The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request".

No Issues

Insecure Interaction - CWE ID 434

Unrestricted Upload of File with Dangerous Type. CWE-434 states: "The software allows the attacker to upload or transfer files of dangerous types that can be automatically processed within the product's environment".

No Issues

Risky Resource Management - CWE ID 494

Download of Code Without Integrity Check. CWE-494 states: "The product downloads source code or an executable from a remote location and executes the code without sufficiently verifying the origin and integrity of the code".

No Issues

Insecure Interaction - CWE ID 601

URL Redirection to Untrusted Site ('Open Redirect'). CWE-601 states: "A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks".

Open Redirect		Critical
Package: src.core		
Location	**Analysis Info**	**Analyzer**
src/core/cache-storage.ts:34	**Sink:** Assignment to link.href **Enclosing Method:** getOrigin() **Source:** Read link.href **from** getOrigin() **In** src/core/cache-storage.ts:34	SCA
Package: www.src		
Location	**Analysis Info**	**Analyzer**
www/src/preview.ts:55	**Sink:** Assignment to testLink.href **Enclosing Method:** selectTest() **Source:** Read testSelector.value **from** lambda() **In** www/src/preview.ts:98	SCA

Risky Resource Management - CWE ID 676

Use of Potentially Dangerous Function. CWE-676 states: "The program invokes a potentially dangerous function that could introduce a vulnerability if it is used incorrectly, but the function can also be used safely".

No Issues

Porous Defenses - CWE ID 732

Incorrect Permission Assignment for Critical Resource. CWE-732 states: "The software specifies permissions for a security-critical resource in a way that allows that resource to be read or modified by unintended actors".

No Issues

Porous Defenses - CWE ID 759

Use of a One-Way Hash without a Salt. CWE-759 states: "The software uses a one-way cryptographic hash against an input that should not be reversible, such as a password, but the software does not also use a salt as part of the input".

No Issues

Porous Defenses - CWE ID 798

Use of Hard-coded Credentials. CWE-798 states: "The software contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data".

Password Management: Hardcoded Password		Critical
Package: src.dom.replaced-elements		
Location	Analysis Info	Analyzer
src/dom/replaced-elements/input-element-container.ts:43	**Sink:** FieldAccess: PASSWORD **Enclosing Method:** ~file_function() **Source:**	SCA
src/dom/replaced-elements/input-element-container.ts:43	**Sink:** VariableAccess: PASSWORD **Enclosing Method:** ~file_function() **Source:**	SCA

Password Management: Password in HTML Form		Critical
Package: tests.reftests		
Location	Analysis Info	Analyzer
tests/reftests/forms.html:37	**Enclosing Method:** () **Source:**	SCA

Porous Defenses - CWE ID 807

Reliance on Untrusted Inputs in a Security Decision. CWE-807 states: "The application uses a protection mechanism that relies on the existence or values of an input, but the input can be modified by an untrusted actor in a way that bypasses the protection mechanism".

No Issues

Risky Resource Management - CWE ID 829

Inclusion of Functionality from Untrusted Control Sphere. CWE-829 states: "The software imports, requires, or includes executable functionality (such as a library) from a source that is outside of the intended control sphere".

No Issues

Porous Defenses - CWE ID 862

Missing Authorization. CWE-862 states: "The software does not perform an authorization check when an actor attempts to access a resource or perform an action".

No Issues

Porous Defenses - CWE ID 863

Incorrect Authorization. CWE-863 states: "The software performs an authorization check when an actor attempts to access a resource or perform an action, but it does not correctly perform the check. This allows attackers to bypass intended access restrictions".

No Issues

Description of Key Terminology

Likelihood and Impact

Likelihood
Likelihood is the probability that a vulnerability will be accurately identified and successfully exploited.

Impact
Impact is the potential damage an attacker could do to assets by successfully exploiting a vulnerability. This damage can be in the form of, but not limited to, financial loss, compliance violation, loss of brand reputation, and negative publicity.

Fortify Priority Order

Critical
Critical-priority issues have high impact and high likelihood. Critical-priority issues are easy to detect and exploit and result in large asset damage. These issues represent the highest security risk to the application. As such, they should be remediated immediately.

SQL Injection is an example of a critical issue.

High
High-priority issues have high impact and low likelihood. High-priority issues are often difficult to detect and exploit, but can result in large asset damage. These issues represent a high security risk to the application. High-priority issues should be remediated in the next scheduled patch release.

Password Management: Hardcoded Password is an example of a high issue.

Medium
Medium-priority issues have low impact and high likelihood. Medium-priority issues are easy to detect and exploit, but typically result in small asset damage. These issues represent a moderate security risk to the application. Medium-priority issues should be remediated in the next scheduled product update.

Path Manipulation is an example of a medium issue.

Low
Low-priority issues have low impact and low likelihood. Low-priority issues can be difficult to detect and exploit and typically result in small asset damage. These issues represent a minor security risk to the application. Low-priority issues should be remediated as time allows.

Dead Code is an example of a low issue.

About Fortify Solutions

Fortify is the leader in end-to-end application security solutions with the flexibility of testing on-premise and on-demand to cover the entire software development lifecycle. Learn more at software.microfocus.com/en-us/solutions/application-security.