Hewlett Packard
Enterprise

HPE Security Fortify Audit Workbench

NIST SP 800-53 Rev.4

testcms-final-anon

Compliance	Pass	Fail

FORTIFY®

Table of Contents

Executive Summary

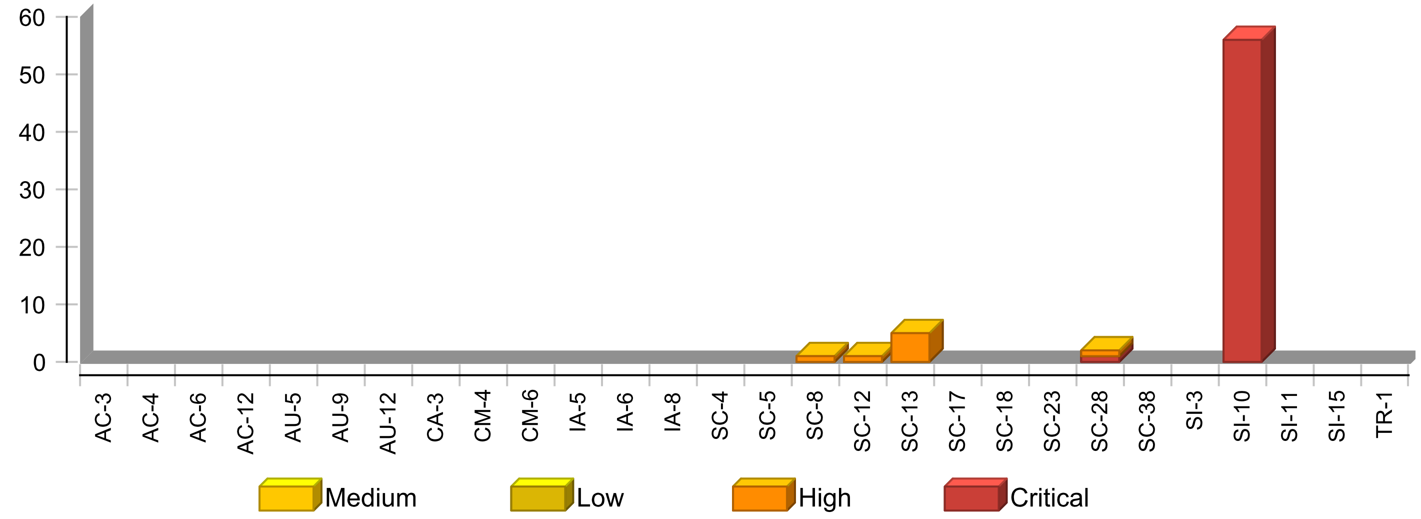
Project Name:	testcms-final-anon
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
SecurityScope:	Results Not Present
Other:	Results Not Present

COMPLIANCE

PASS **FAIL**

NIST SP 800-53 Rev.4 groups	Total	Status
Access Control (AC)	0	**PASS**
Audit and Accountability (AU)	0	**PASS**
Configuration Management (CM)	0	**PASS**
Identification and Authentication (IA)	0	**PASS**
Security Assessment and Authorization (CA)	0	**PASS**
System and Communications Protection (SC)	9	**FAIL**
System and Information Integrity (SI)	56	**FAIL**
Transparency (TR)	0	**PASS**

Issues by NIST SP 800-53 Rev.4 Categories



* The detailed sections following the Executive Summary contain specifics.

Project Description

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

SCA

Date of Last Analysis:	Nov 9, 2016, 1:19 PM	**Engine Version:**	16.10.0095
Host Name:	mrl-PC	**Certification:**	VALID
Number of Files:	92	**Lines of Code:**	3,731

Issue BreakDown

The following table summarizes the number of issues identified across the different NIST SP 800-53 Rev.4 categories and broken down by Fortify Priority Order. The status of a category is considered "In Place" or "PASS" when there are no issues reported for that category.

Access Control (AC)	Folder	Issues	Audited	Status
AC-3 Access Enforcement (P1)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
AC-4 Information Flow Enforcement (P1)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
AC-6 Least Privilege (P1)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
AC-12 Session Termination (P2)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
Audit and Accountability (AU)	**Folder**	**Issues**	**Audited**	**Status**
AU-5 Response to Audit Processing Failures (P1)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
AU-9 Protection of Audit Information (P1)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
AU-12 Audit Generation (P1)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
Security Assessment and Authorization (CA)	**Folder**	**Issues**	**Audited**	**Status**
CA-3 System Interconnections (P1)		**0**	**0**	**PASS**
	Critical	0	0	

Security Assessment and Authorization (CA)	**Folder**	**Issues**	**Audited**	**Status**
CA-3 System Interconnections (P1)		**0**	**0**	**PASS**
	High	0	0	
	Medium	0	0	
	Low	0	0	
Configuration Management (CM)	**Folder**	**Issues**	**Audited**	**Status**
CM-4 Security Impact Analysis (P2)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
CM-6 Configuration Settings (P2)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
Identification and Authentication (IA)	**Folder**	**Issues**	**Audited**	**Status**
IA-5 Authenticator Management (P1)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
IA-6 Authenticator Feedback (P2)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
IA-8 Identification and Authentication (Non-Organizational Users) (P1)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
System and Communications Protection (SC)	**Folder**	**Issues**	**Audited**	**Status**
SC-4 Information in Shared Resources (P1)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
SC-5 Denial of Service Protection (P1)		**0**	**0**	**PASS**
	Critical	0	0	

System and Communications Protection (SC)	Folder	Issues	Audited	Status
SC-5 Denial of Service Protection (P1)		0	0	PASS
	High	0	0	
	Medium	0	0	
	Low	0	0	
SC-8 Transmission Confidentiality and Integrity (P1)		1	0	FAIL
	Critical	0	0	
	High	1	0	
	Medium	0	0	
	Low	0	0	
SC-12 Cryptographic Key Establishment and Management (P1)		1	0	FAIL
	Critical	0	0	
	High	1	0	
	Medium	0	0	
	Low	0	0	
SC-13 Cryptographic Protection (P1)		5	0	FAIL
	Critical	0	0	
	High	5	0	
	Medium	0	0	
	Low	0	0	
SC-17 Public Key Infrastructure Certificates (P1)		0	0	PASS
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
SC-18 Mobile Code (P2)		0	0	PASS
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
SC-23 Session Authenticity (P1)		0	0	PASS
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
SC-28 Protection of Information at Rest (P1)		2	0	FAIL
	Critical	1	0	
	High	1	0	
	Medium	0	0	
	Low	0	0	
SC-38 Operations Security (P0)		0	0	PASS
	Critical	0	0	
	High	0	0	

System and Communications Protection (SC)	Folder	Issues	Audited	Status
SC-38 Operations Security (P0)		**0**	**0**	**PASS**
	Medium	0	0	
	Low	0	0	
System and Information Integrity (SI)	**Folder**	**Issues**	**Audited**	**Status**
SI-3 Malicious Code Protection (P1)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
SI-10 Information Input Validation (P1)		**56**	**0**	**FAIL**
	Critical	56	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
SI-11 Error Handling (P2)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
SI-15 Information Output Filtering (P0)		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	
Transparency (TR)	**Folder**	**Issues**	**Audited**	**Status**
TR-1 Privacy Notice		**0**	**0**	**PASS**
	Critical	0	0	
	High	0	0	
	Medium	0	0	
	Low	0	0	

NOTE:
1. Reported issues in the above table may violate more than one NIST SP 800-53 Rev.4 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 Summaries

Below is an enumeration of all issues found in the project. The issues are organized by NIST SP 800-53 Rev. 4, Folder, and vulnerability category. For every vulnerability category, the number of issues is shown.

AC-3 Access Enforcement (P1)

AC-3 Access Enforcement control states: "The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies." HPE Security Fortify considers issues related to (a) abuse of access control settings and (b) untrusted data used to influence criteria keys, paths, and resource locations to violate this control and the following sub-controls: (3) Mandatory Access Control, (5) Security-Relevant Information, and (7) Role-Based Access Control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

AC-4 Information Flow Enforcement (P1)

AC-4 Information Flow Enforcement control states: "The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems based on [Assignment: organization-defined information flow control policies]." HPE Security Fortify considers issues related to (a) improper usage of permissions when sending and receiving messages and (b) overly permissive domain policies to violate this control and the following sub-controls: (20) Approved Solutions and (21) Physical / Logical Separation of Information Flows.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0

Fortify Category	Folder	Issues	Audited
Password Management: Empty Password		**1**	**0**
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

AC-6 Least Privilege (P1)

AC-6 Least Privilege control states: "The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions." HPE Security Fortify considers issues related to overprivilege to violate this control and the following sub-control: (8) Privilege Levels for Code Execution.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

AC-12 Session Termination (P2)

AC-12 Session Termination control states: "The information system automatically terminates a user session after [Assignment: organization-defined conditions or trigger events requiring session disconnect]." HPE Security Fortify considers issues related to excessive session timeouts to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0

Fortify Category	Folder	Issues	Audited
SQL Injection		**6**	**0**
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

AU-5 Response to Audit Processing Failures (P1)

AU-5 Response to Audit Processing Failures control states: "The information system: a. Alerts [Assignment: organization-defined personnel or roles] in the event of an audit processing failure; and b. Takes the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)]." HPE Security Fortify considers issues related to insufficient audit failure handling to violate this control and the following sub-control: (2) Real-Time Alerts.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

AU-9 Protection of Audit Information (P1)

AU-9 Protection of Audit Information control states: "The information system protects audit information and audit tools from unauthorized access, modification, and deletion." HPE Security Fortify considers issues related to log forging to violate this control and the following sub-controls: (4) Access by Subset of Privileged Users and (6) Read-Only Access.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Password Management: Empty Password		1	0
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		1	0
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		1	0
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		2	0
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		6	0
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		5	0
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

AU-12 Audit Generation (P1)

AU-12 Audit Generation control states: "The information system: a. Provides audit record generation capability for the auditable events defined in AU-2 a. at [Assignment: organization-defined information system components]; b. Allows [Assignment: organization-defined personnel or roles] to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3." HPE Security Fortify considers issues related to insufficient logging to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		1	0
	Critical	0	0
	High	1	0

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

CA-3 System Interconnections (P1)

CA-3 System Interconnections control states: "The organization: a. Authorizes connections from the information system to other information systems through the use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency]." HPE Security Fortify considers issues related to open proxy access to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

CM-4 Security Impact Analysis (P2)

CM-4 Security Impact Analysis control states: "The organization analyzes changes to the information system to determine potential security impacts prior to change implementation." HPE Security Fortify considers issues related to cache configuration management to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Privacy Violation		1	0
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		2	0
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		6	0
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		5	0
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

CM-6 Configuration Settings (P2)

CM-6 Configuration Settings control states: "The organization: a. Establishes and documents configuration settings for information technology products employed within the information system using [Assignment: organization-defined security configuration checklists] that reflect the most restrictive mode consistent with operational requirements; b. Implements the configuration settings; c. Identifies, documents, and approves any deviations from established configuration settings for [Assignment: organization-defined information system components] based on [Assignment: organization-defined operational requirements]; and d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures." HPE Security Fortify considers issues related to server misconfiguration to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		1	0
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		50	0
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Key Management: Empty Encryption Key		1	0
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		1	0
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		1	0
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		1	0
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		2	0
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		6	0
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		5	0
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

IA-5 Authenticator Management (P1)

IA-5 Authenticator Management control states: "The organization manages information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators [Assignment: organization-defined time period by authenticator type]; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes." HPE Security Fortify considers issues related to default credentials to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

IA-6 Authenticator Feedback (P2)

IA-6 Authenticator Feedback control states: "The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals." HPE Security Fortify considers issues related to unmasked password fields to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Privacy Violation		1	0
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		2	0
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		6	0
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		5	0
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

IA-8 Identification and Authentication (Non-Organizational Users) (P1)

IA-8 Identification and Authentication (Non-Organizational Users) control states: "The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users)." HPE Security Fortify considers issues related to authentication misconfiguration to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		1	0
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		50	0
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		1	0
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SC-4 Information in Shared Resources (P1)

SC-4 Information in Shared Resources control states: "The information system prevents unauthorized and unintended information transfer via shared system resources." HPE Security Fortify considers issues related to (a) heap inspection, (b) race conditions, (c) cross-session contamination, and (d) insecure compiler optimization to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SC-5 Denial of Service Protection (P1)

SC-5 Denial of Service Protection control states: "The information system protects against or limits the effects of the following types of denial of service attacks: [Assignment: organization-defined types of denial of service attacks or reference to source for such information] by employing [Assignment: organization-defined security safeguards]." HPE Security Fortify considers issues that can result in a denial of service, such as memory leak, unreleased resource, and use after free, to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0

Fortify Category	Folder	Issues	Audited
SQL Injection		6	0
	Medium	0	0
	Low	0	0
Weak Encryption		5	0
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SC-8 Transmission Confidentiality and Integrity (P1)

SC-8 Transmission Confidentiality and Integrity control states: "The information system protects the [Selection (one or more): confidentiality; integrity] of transmitted information." HPE Security Fortify considers issues related to insecure transport to violate this control and the following sub-controls: (1) Cryptographic or Alternate Physical Protection and (3) Cryptographic Protection for Message Externals.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		1	0
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		50	0
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		1	0
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		1	0
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		1	0
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		1	0
	Critical	1	0

Fortify Category	Folder	Issues	Audited
Privacy Violation		**1**	**0**
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SC-12 Cryptographic Key Establishment and Management (P1)

SC-12 Cryptographic Key Establishment and Management control states: "The organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [Assignment: organization-defined requirements for key generation, distribution, storage, access, and destruction]." HPE Security Fortify considers issues related to (a) cryptographic key management and (b) insufficient key size to violate this control and the following sub-controls: (2) Symmetric Keys and (3) Asymmetric Keys.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0

Fortify Category	Folder	Issues	Audited
Key Management: Empty Encryption Key		**1**	**0**
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SC-13 Cryptographic Protection (P1)

SC-13 Cryptographic Protection control states: "The information system implements [Assignment: organization-defined cryptographic uses and type of cryptography required for each use] in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards." HPE Security Fortify considers issues related to weak (a) encryption, (b) hash functions, and (c) pseudo-random number generators to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0

Fortify Category	Folder	Issues	Audited
Weak Encryption		**5**	**0**
	Low	0	0

SC-17 Public Key Infrastructure Certificates (P1)

SC-17 Public Key Infrastructure Certificates control states: "The organization issues public key certificates under an [Assignment: organization-defined certificate policy] or obtains public key certificates from an approved service provider." HPE Security Fortify considers issues related to (a) weak SSL certificates and (b) inadequate certificate validation to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0

Fortify Category	Folder	Issues	Audited
Privacy Violation: Autocomplete		**2**	**0**
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SC-18 Mobile Code (P2)

SC-18 Mobile Code control states: "The organization: a. Defines acceptable and unacceptable mobile code and mobile code technologies; b. Establishes usage restrictions and implementation guidance for acceptable mobile code and mobile code technologies; and c. Authorizes, monitors, and controls the use of mobile code within the information system." HPE Security Fortify considers issues related to (a) JavaScript hijacking, (b) cross-site flashing, (c) file uploads, (d) using external ant, maven or ivy dependency repositories, and (e) unauthorized includes to violate this control and the following sub-controls: (3) Prevent Downloading / Execution, (4) Prevent Automatic Execution, and (5) Allow Execution Only in Confined Environments.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0

Fortify Category	Folder	Issues	Audited
Password Management: Empty Password		1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		1	0
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		1	0
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		2	0
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		6	0
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		5	0
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SC-23 Session Authenticity (P1)

SC-23 Session Authenticity control states: "The information system protects the authenticity of communications sessions." HPE Security Fortify considers issues related to (a) session fixation, (b) inadequate session identifiers, (c) cross-site request forgery, and (d) the use of persistent cookies to violate this control and the following sub-controls: (1) Invalidate Session Identifiers at Logout and (3) Unique Session Identifiers with Randomization.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		1	0
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SC-28 Protection of Information at Rest (P1)

SC-28 Protection of Information at Rest control states: "The information system protects the [Selection (one or more): confidentiality; integrity] of [Assignment: organization-defined information at rest]." HPE Security Fortify considers issues related to (a) password and credential management and (b) insecure storage to violate this control and the following sub-control: (1) Cryptographic Protection.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0

Fortify Category	Folder	Issues	Audited
SQL Injection		**6**	**0**
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SC-38 Operations Security (P0)

SC-38 Operations Security control states: "The organization employs [Assignment: organization-defined operations security safeguards] to protect key organizational information throughout the system development life cycle." HPE Security Fortify considers issues related to insecure deployment to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0

Fortify Category	Folder	Issues	Audited
Privacy Violation		**1**	**0**
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SI-3 Malicious Code Protection (P1)

SI-13 Malicious Code Protection control states: "The organization: a. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code; b. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures; c. Configures malicious code protection mechanisms to: 1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection; and d. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system." HPE Security Fortify considers issues related to malicious application discovery to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0

Fortify Category	Folder	Issues	Audited
Cross-Site Scripting: Reflected		**50**	**0**
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SI-10 Information Input Validation (P1)

SI-10 Information Input Validation control states: "The information system checks the validity of [Assignment: organization-defined information inputs]." HPE Security Fortify considers issues related to (a) inadequate or disabled input validation, including cross-site scripting and path manipulation, and (b) injection flaws to violate this control and the following sub-control: (5) Restrict Input to Trusted Sources and Approved Formats.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0

Fortify Category	Folder	Issues	Audited
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SI-11 Error Handling (P2)

SI-11 Error Handling control states: "The information system: a. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries; and b. Reveals error messages only to [Assignment: organization-defined personnel or roles]." HPE Security Fortify considers issues related to (a) inadequate error handling and (b) revealing debug information to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0

Fortify Category	Folder	Issues	Audited
Privacy Violation		**1**	**0**
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

SI-15 Information Output Filtering (P0)

SI-15 Information Output Filtering control states: "The information system validates information output from [Assignment: organization-defined software programs and/or applications] to ensure that the information is consistent with the expected content." HPE Security Fortify considers issues related to output encoding miconfiguration to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0

Fortify Category	Folder	Issues	Audited
Password Management: Empty Password		**1**	**0**
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0
	Medium	0	0
	Low	0	0

TR-1 Privacy Notice

TR-1 Privacy Notice control states: "The organization: a. Provides effective notice to the public and to individuals regarding: (i) its activities that impact privacy, including its collection, use, sharing, safeguarding, maintenance, and disposal of personally identifiable information (PII); (ii) authority for collecting PII; (iii) the choices, if any, individuals may have regarding how the organization uses PII and the consequences of exercising or not exercising those choices; and (iv) the ability to access and have PII amended or corrected if necessary; b. Describes: (i) the PII the organization collects and the purpose(s) for which it collects that information; (ii) how the organization uses PII internally; (iii) whether the organization shares PII with external entities, the categories of those entities, and the purposes for such sharing; (iv) whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; (v) how individuals may obtain access to PII; and (vi) how the PII will be protected; and c. Revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy, before or as soon as practicable after the change." HPE Security Fortify considers issues related to missing privacy policy to violate this control.

Fortify Category	Folder	Issues	Audited
Cookie Security: HTTPOnly not Set		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Cross-Site Scripting: Reflected		**50**	**0**
	Critical	50	0
	High	0	0
	Medium	0	0
	Low	0	0
Key Management: Empty Encryption Key		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Empty Password		**1**	**0**
	Critical	0	0
	High	1	0
	Medium	0	0
	Low	0	0
Password Management: Password in HTML Form		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation		**1**	**0**
	Critical	1	0
	High	0	0
	Medium	0	0
	Low	0	0
Privacy Violation: Autocomplete		**2**	**0**
	Critical	0	0
	High	2	0
	Medium	0	0
	Low	0	0
SQL Injection		**6**	**0**
	Critical	6	0
	High	0	0
	Medium	0	0
	Low	0	0
Weak Encryption		**5**	**0**
	Critical	0	0
	High	5	0

Fortify Category	Folder	Issues	Audited
Weak Encryption		**5**	**0**
	Medium	0	0
	Low	0	0