Hewlett Packard
Enterprise

HPE Security Fortify Audit Workbench

PCI 3.0

testcms-final-anon

Compliance	In Place	Not In Place

FORTIFY

Table of Contents

Executive Summary

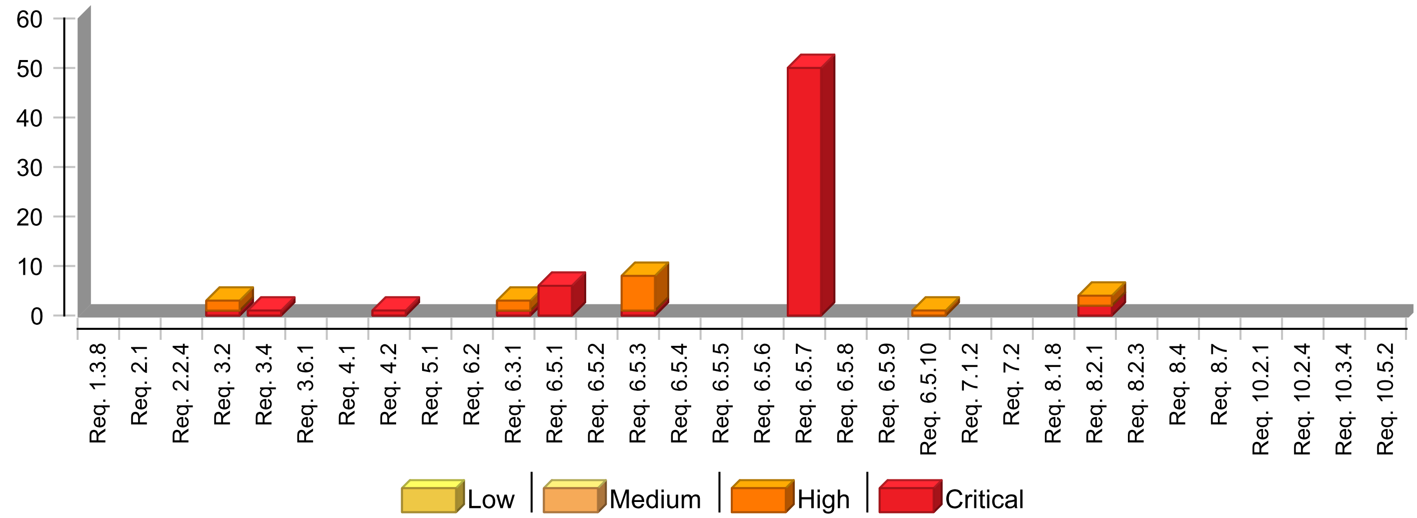
Project Name:	testcms-final-anon
Project Version:	
SCA:	Results Present
WebInspect:	Results Not Present
SecurityScope:	Results Not Present
Other:	Results Not Present

COMPLIANCE

In Place	Not In Place

PCI 3.0 groups	Total	Status
Requirement 1	0	In Place
Requirement 10	0	In Place
Requirement 2	0	In Place
Requirement 3	4	Not In Place
Requirement 4	1	Not In Place
Requirement 5	0	In Place
Requirement 6	68	Not In Place
Requirement 7	0	In Place
Requirement 8	4	Not In Place

Issues by PCI 3.0 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 PCI 3.0 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.

Requirement 1	Fortify Priority				Total Issues	Status
	Critical	High	Medium	Low		
Requirement 1.3.8	0	0	0	0	0	In Place
Requirement 2	**Fortify Priority**				**Total Issues**	**Status**
	Critical	**High**	**Medium**	**Low**		
Requirement 2.1	0	0	0	0	0	In Place
Requirement 2.2.4	0	0	0	0	0	In Place
Requirement 3	**Fortify Priority**				**Total Issues**	**Status**
	Critical	**High**	**Medium**	**Low**		
Requirement 3.2	1	2	0	0	3	Not In Place
Requirement 3.4	1	0	0	0	1	Not In Place
Requirement 3.6.1	0	0	0	0	0	In Place
Requirement 4	**Fortify Priority**				**Total Issues**	**Status**
	Critical	**High**	**Medium**	**Low**		
Requirement 4.1	0	0	0	0	0	In Place
Requirement 4.2	1	0	0	0	1	Not In Place
Requirement 5	**Fortify Priority**				**Total Issues**	**Status**
	Critical	**High**	**Medium**	**Low**		
Requirement 5.1	0	0	0	0	0	In Place
Requirement 6	**Fortify Priority**				**Total Issues**	**Status**
	Critical	**High**	**Medium**	**Low**		
Requirement 6.2	0	0	0	0	0	In Place
Requirement 6.3.1	1	2	0	0	3	Not In Place
Requirement 6.5.1	6	0	0	0	6	Not In Place
Requirement 6.5.2	0	0	0	0	0	In Place
Requirement 6.5.3	1	7	0	0	8	Not In Place
Requirement 6.5.4	0	0	0	0	0	In Place
Requirement 6.5.5	0	0	0	0	0	In Place
Requirement 6.5.6	0	0	0	0	0	In Place
Requirement 6.5.7	50	0	0	0	50	Not In Place
Requirement 6.5.8	0	0	0	0	0	In Place
Requirement 6.5.9	0	0	0	0	0	In Place
Requirement 6.5.10	0	1	0	0	1	Not In Place
Requirement 7	**Fortify Priority**				**Total Issues**	**Status**
	Critical	**High**	**Medium**	**Low**		
Requirement 7.1.2	0	0	0	0	0	In Place
Requirement 7.2	0	0	0	0	0	In Place
Requirement 8	**Fortify Priority**				**Total Issues**	**Status**
	Critical	**High**	**Medium**	**Low**		
Requirement 8.1.8	0	0	0	0	0	In Place
Requirement 8.2.1	2	2	0	0	4	Not In Place
Requirement 8.2.3	0	0	0	0	0	In Place
Requirement 8.4	0	0	0	0	0	In Place
Requirement 8.7	0	0	0	0	0	In Place

Requirement 10	Fortify Priority				Total Issues	Status
	Critical	High	Medium	Low		
Requirement 10.2.1	0	0	0	0	0	**In Place**
Requirement 10.2.4	0	0	0	0	0	**In Place**
Requirement 10.3.4	0	0	0	0	0	**In Place**
Requirement 10.5.2	0	0	0	0	0	**In Place**

NOTE:
1. Reported issues in the above table may violate more than one PCI 3.0 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 PCI 3.0, Fortify Priority Order, and vulnerability category. For every vulnerability category, the number of issues is shown.

Requirement 1.3.8

Do not disclose private IP addresses and routing information to unauthorized parties.

Requirement 1.3.8 states: "Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet."

HPE Security Fortify considers issues related to the disclosure of internal IP addresses to violate this requirement.

No Issues

Requirement 2.1

Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.

Requirement 2.1 states: "Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed."

HPE Security Fortify considers issues related to the use of default account information to violate this requirement.

No Issues

Requirement 2.2.4

Configure system security parameters to prevent misuse.

Requirement 2.2.4 states: "Examine the system configuration standards to verify that common security parameter settings are included."

HPE Security Fortify considers issues related to application and web server misconfiguration to violate this requirement.

No Issues

Requirement 3.2

Do not store sensitive authentication data after authorization (even if encrypted).

Requirement 3.2 states: "If sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization."

HPE Security Fortify considers issues that leak potentially private data to violate this requirement.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Privacy Violation	0 / 1	0	0	0	0 / 1
Privacy Violation: Autocomplete	0	0 / 2	0	0	0 / 2

Requirement 3.4

Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:

- One-way hashes based on strong cryptography (hash must be of the entire PAN)
- Truncation (hashing cannot be used to replace the truncated segment of PAN)
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures

Requirement 3.4 states: "Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable)."

HPE Security Fortify considers issues that handle authentication data weakly to violate this requirement.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Privacy Violation	0 / 1	0	0	0	0 / 1

Requirement 3.6.1

Generation of strong cryptographic keys:

Requirement 3.6.1 states: "Observe the method for generating keys to verify that strong keys are generated."

HPE Security Fortify considers issues that involve weak cryptography to violate this requirement.

No Issues

Requirement 4.1

Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.

Requirement 4.1 states: "Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to system configurations to verify the use of security protocols and strong cryptography for all locations. Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use."

HPE Security Fortify considers issues that handle security protocols poorly to violate this requirement.

No Issues

Requirement 4.2

Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).

Requirement 4.2 states: "Verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies."

HPE Security Fortify considers issues that expose potentially private data to violate this requirement.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Privacy Violation	0 / 1	0	0	0	0 / 1

Requirement 5.1

Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).

Requirement 5.1 states: "For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists."

HPE Security Fortify considers the presence of a malicious application to violate this requirement.

No Issues

Requirement 6.2

Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

Requirement 6.2 states: "Examine policies and procedures related to security-patch installation."

HPE Security Fortify considers the presence of an unpatched application to violate this requirement.

No Issues

Requirement 6.3.1

Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.

Requirement 6.3.1 states: "Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers."

HPE Security Fortify considers the presence of hardcoded account information to violate this requirement.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Key Management: Empty Encryption Key	0	0 / 1	0	0	0 / 1
Password Management: Empty Password	0	0 / 1	0	0	0 / 1
Password Management: Password in HTML Form	0 / 1	0	0	0	0 / 1

Requirement 6.5.1

Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.

Requirement 6.5.1 states: "Verify that injection flaws are addressed by coding techniques that include:
1. Validating input to verify user data cannot modify meaning of commands and queries.
2. Utilizing parameterized queries."

HPE Security Fortify considers issues that mix control commands with user data to violate this requirement.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
SQL Injection	0 / 6	0	0	0	0 / 6

Requirement 6.5.2

Buffer overflow.

Requirement 6.5.2 states: "Verify that buffer overflows are addressed by coding techniques that include:
1. Validating buffer boundaries.
2. Truncating input strings."

HPE Security Fortify considers issues that overflow buffer boundaries to violate this requirement.

No Issues

Requirement 6.5.3

Insecure cryptographic storage.

Requirement 6.5.3 states: "Verify that insecure cryptographic storage is addressed by coding

techniques that:
1. Prevent cryptographic flaws.
2. Use strong cryptographic algorithms and keys."

HPE Security Fortify considers issues that involve weak cryptography to violate this requirement.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Key Management: Empty Encryption Key	0	0 / 1	0	0	0 / 1
Password Management: Empty Password	0	0 / 1	0	0	0 / 1
Password Management: Password in HTML Form	0 / 1	0	0	0	0 / 1
Weak Encryption	0	0 / 5	0	0	0 / 5

Requirement 6.5.4

Insecure communications.

Requirement 6.5.4 states: "Verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications."

HPE Security Fortify considers issues that transfer data using weak cryptography to violate this requirement.

No Issues

Requirement 6.5.5

Improper error handling.

Requirement 6.5.5 states: "Verify that improper error handling is addressed by coding techniques that do not leak information via error messages (for example, by returning generic rather than specific error details)."

HPE Security Fortify considers issues that expose potentially private data to violate this requirement.

No Issues

Requirement 6.5.6

All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).

Requirement 6.5.6 states: "Verify that coding techniques address any "high risk" vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1."
Furthermore, requirement 6.1.b states: "Interview responsible personnel and observe processes to verify that:
1. New security vulnerabilities are identified.
2. A risk ranking is assigned to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities.

3. Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information."

HPE Security Fortify considers issues that are identified outside of the other PCI DSS requirements to violate this requirement. Only those issues, outside of those issues specifically identified by PCI DSS, ranked "Critical" or "High" are reported in this report.

No Issues

Requirement 6.5.7

Cross-site scripting (XSS).

Requirement 6.5.7 states: "Verify that cross-site scripting (XSS) is addressed by coding techniques that include:
1. Validating all parameters before inclusion.
2. Utilizing context-sensitive escaping."

HPE Security Fortify considers issues within the cross-site scripting category to violate this requirement.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Cross-Site Scripting: Reflected	0 / 50	0	0	0	0 / 50

Requirement 6.5.8

Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).

Requirement 6.5.8 states: "Verify that improper access control - such as insecure direct object references, failure to restrict URL access, and directory traversal - is addressed by coding technique that includes:
1. Proper authentication of users. Sanitizing input.
2. Not exposing internal object references to users.
3. User interfaces that do not permit access to unauthorized functions."

HPE Security Fortify considers issues that have any of the following to violate this requirement:
- untrusted data used to influence criteria keys, paths, and resource locations
- allow untrusted data to influence dynamic file inclusion
- handle authentication incorrectly or weakly
- weak or misconfigured access control settings

No Issues

Requirement 6.5.9

Cross-site request forgery (CSRF).

Requirement 6.5.9 states: "Verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers."

HPE Security Fortify considers issues within the cross-site request forgery category to violate this requirement.

No Issues

Requirement 6.5.10

Broken authentication and session management.

Requirement 6.5.10 states, "Verify that broken authentication and session management are addressed via coding techniques that commonly include:
1. Flagging session tokens (for example cookies) as "secure."
2. Not exposing session IDs in the URL.
3. Incorporating appropriate time-outs and rotation of session IDs after a successful login."

HPE Security Fortify considers issues that handle authentication incorrectly, or weakly, to violate this requirement.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Cookie Security: HTTPOnly not Set	0	0 / 1	0	0	0 / 1

Requirement 7.1.2

Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.

Requirement 7.1.2 states: "Verify that access to privileged user IDs is:
1. Assigned only to roles that specifically require such privileged access.
2. Restricted to least privileges necessary to perform job responsibilities."

HPE Security Fortify considers issues that do not restrict access rights to the minimum required to violate this requirement.

No Issues

Requirement 7.2

Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.

Requirement 7.2 states: "Verify that an access control system is implemented as follows:
1. Confirm that access control systems are in place on all system components.
2. Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.
3. Confirm that the access control systems have a default "deny-all" setting."

HPE Security Fortify considers issues that do not provide unique authentication to violate this requirement.

No Issues

Requirement 8.1.8

If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal or session.

Requirement 8.1.8 states: "For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less."

HPE Security Fortify considers issues that have missing or excessive session time-out specifications to violate this requirement.

No Issues

Requirement 8.2.1

Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.

Requirement 8.2.1 states: "Many network devices and applications transmit unencrypted, readable passwords across the network and/or store passwords without encryption. A malicious individual can easily intercept unencrypted passwords during transmission using a "sniffer," or directly access unencrypted passwords in files where they are stored, and use this data to gain unauthorized access."

HPE Security Fortify considers issues that transfer data using weak cryptography to violate this requirement.

Category	Fortify Priority (audited/total)				Total Issues
	Critical	High	Medium	Low	
Key Management: Empty Encryption Key	0	0 / 1	0	0	0 / 1
Password Management: Empty Password	0	0 / 1	0	0	0 / 1
Password Management: Password in HTML Form	0 / 1	0	0	0	0 / 1
Privacy Violation	0 / 1	0	0	0	0 / 1

Requirement 8.2.3

Passwords/phrases must meet the following:

- Require a minimum length of at least seven characters.
- Contain both numeric and alphabetic characters.

Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.

Requirement 8.2.3 states: "For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require at least the following strength/complexity:

- Require a minimum length of at least seven characters.

- Contain both numeric and alphabetic characters."

HPE Security Fortify considers issues related to weak password policy to violate this requirement.

No Issues

Requirement 8.4

Document and communicate authentication procedures and policies to all users including:
- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials
- Instructions not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised.

Requirement 8.4 states: "Examine procedures and interview personnel to verify that authentication procedures and policies are distributed to all users. Review authentication procedures and policies that are distributed to users and verify they include:
- Guidance on selecting strong authentication credentials
- Guidance for how users should protect their authentication credentials.
- Instructions for users not to reuse previously used passwords
- Instructions to change passwords if there is any suspicion the password could be compromised.

Interview a sample of users to verify that they are familiar with authentication procedures and policies."

HPE Security Fortify considers issues related to weak password policy to violate this requirement.

No Issues

Requirement 8.7

All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:
- All user access to, user queries of, and user actions on databases are through programmatic methods.
- Only database administrators have the ability to directly access or query databases.
- Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).

Requirement 8.7 states: "Examine database and application configuration settings to verify that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures)."

HPE Security Fortify considers issues related to unrestricted direct database access to violate this requirement.

No Issues

Requirement 10.2.1

All individual accesses to cardholder data.

Requirement 10.2.1 states: "Verify all individual access to cardholder data is logged."

HPE Security Fortify considers issues that involve insufficient logging to violate this requirement.

No Issues

Requirement 10.2.4

Invalid logical access attempts.

Requirement 10.2.4 states: "Verify invalid logical access attempts are logged."

HPE Security Fortify considers issues that involve insufficient logging to violate this requirement.

No Issues

Requirement 10.3.4

Success or failure indication.

Requirement 10.3.4 states: "Verify success or failure indication is included in log entries."

HPE Security Fortify considers issues that involve insufficient logging to violate this requirement.

No Issues

Requirement 10.5.2

Protect audit trail files from unauthorized modifications.

Requirement 10.5.2 states: "Verify that current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation."

HPE Security Fortify considers issues that allow untrusted data to alter system logs to violate this requirement.

No Issues