Hewlett Packard Enterprise

HPE Security Fortify Audit Workbench

OWASP Mobile 2014

testcms-final-anon

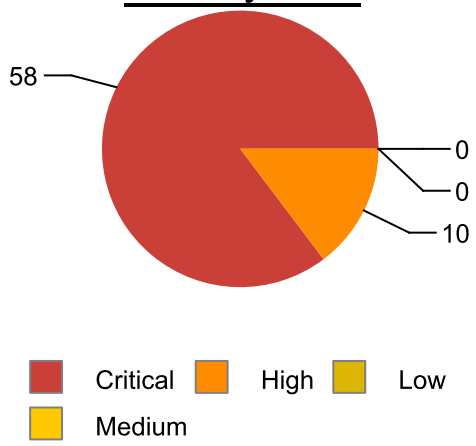
FORTIFY

Table of Contents

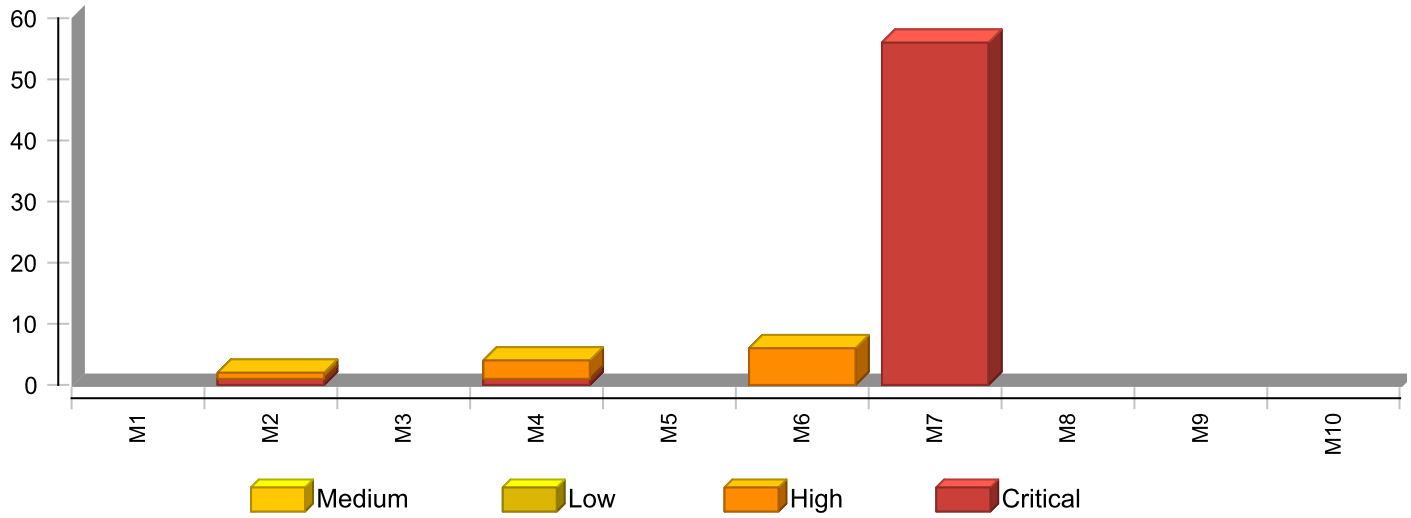
Executive Summary

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

Issues by Folder



Issues by OWASP Mobile 2014 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 OWASP Mobile 2014 categories and broken down by Fortify Priority Order.

	Folder	Issues	Audited
M1 Weak Server Side Controls		**0**	**0**
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
M2 Insecure Data Storage		**2**	**0**
	Critical	1	0
	High	1	0
	Medium	0	0
	Low	0	0
M3 Insufficient Transport Layer Protection		**0**	**0**
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
M4 Unintended Data Leakage		**4**	**0**
	Critical	1	0
	High	3	0
	Medium	0	0
	Low	0	0
M5 Poor Authorization and Authentication		**0**	**0**
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
M6 Broken Cryptography		**6**	**0**
	Critical	0	0
	High	6	0
	Medium	0	0
	Low	0	0
M7 Client Side Injection		**56**	**0**
	Critical	56	0
	High	0	0
	Medium	0	0
	Low	0	0
M8 Security Decisions Via Untrusted Inputs		**0**	**0**
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0

	Folder	Issues	Audited
M9 Improper Session Handling		**0**	**0**
	Critical	0	0
	High	0	0
	Medium	0	0
	Low	0	0
M10 Lack of Binary Protections		**0**	**0**
	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 OWASP Mobile 2014 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 OWASP Mobile 2014, Folder, and vulnerability category. For every vulnerability category, the number of issues is shown.

M1 Weak Server Side Controls

Weak Server Side Controls category of the OWASP Mobile Top 10 represents all the vulnerabilities that exist on the server side of the mobile ecosystem. When the backend web service or an API call that exposes a mobile interface is implemented using insecure coding practices, a mobile attacker is able to realize the original OWASP Top Ten vulnerability on the server.

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

Fortify Category	Folder	Issues	Audited
Privacy Violation: Autocomplete		2	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

M2 Insecure Data Storage

Insecure Data Storage vulnerabilities occur when sensitive information is stored in an insecure location on the device without any protection. On most mobile devices internal and external storage areas are not encrypted by default, allowing malicious applications and physical attackers unauthorized access to data residing on the device.

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

Fortify Category	Folder	Issues	Audited
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

M3 Insufficient Transport Layer Protection

Insufficient Transport Layer Protection flaws occur whenever data is exchanged between a mobile client and a server in an insecure fashion. Incorrect usage of SSL/TLS protocols and lack of certificate validation are examples of such flaws.

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

M4 Unintended Data Leakage

Unintended Data Leakage occurs when sensitive data is inadvertently placed in an insecure location on the device, usually as a side effect of another operation, such as keyboard caching or application backgrounding.

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

M5 Poor Authorization and Authentication

Poor authentication schemes and privilege management mechanisms allow an attacker to get unauthorized access to resources on the mobile device or execute functionality on the device or the backend server they otherwise would not have access to.

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

Fortify Category	Folder	Issues	Audited
Privacy Violation: Autocomplete		2	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

M6 Broken Cryptography

Many mobile applications use weak encryption algorithms and poor key management processes to protect sensitive data, such as UDID/EMEI, personal data, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes.

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

Fortify Category	Folder	Issues	Audited
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

M7 Client Side Injection

Client Side Injection results in the execution of malicious code on the mobile device. Usually such attacks exercise various injection vulnerabilities, such as SQL Injection, Dangerous File Inclusion, Cross-Site Scripting, and target user data and mobile browsers.

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

M8 Security Decisions Via Untrusted Inputs

In addition to accepting input from the web and other traditional sources, mobile applications also accept input from other mobile applications residing on the device via the Inter-Process Communication (IPC) or the Inter-Component Communication (ICC) mechanisms. Many traditional web vulnerabilities can be triggered by IPC and ICC inputs on the device, which is why all inputs need to be thoroughly validated before being used for any security sensitive operations.

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

M9 Improper Session Handling

Mobile application functionality related to authentication and session management is often implemented in an insecure fashion, allowing attackers to compromise passwords, keys, or session tokens. Other implementation flaws that allow attackers to assume other users' identities include failure to invalidate sessions on the backend and lack of adequate timeout protections.

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

Fortify Category	Folder	Issues	Audited
Privacy Violation: Autocomplete		2	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

M10 Lack of Binary Protections

A lack of binary protections within the mobile application or the use of debug binaries allows attackers to analyze, reverse engineer, and modify the application, potentially turning it into malware.

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

Fortify Category	Folder	Issues	Audited
Password Management: Password in HTML Form		**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