Application Summary

MyBank-Web - 1.0

Hewlett Packard Enterprise

This report provides a complete summary of a single version of an application. This includes a high-level look at the outstanding issues associated with the application as well as detailed information related to the risk profile. Also included is a summary of the user activities that have been performed.

Table of Contents

1. Overview
2. Details
3. Activity Summary
4. Issue Trending
5. Issue Breakdown
    - Issues by Category
    - Issues by OWASP Top Ten 2013
    - Issues by PCI DSS 3.0
    - Issues by CWE
    - Issues by WASC 24
    - Issues by DOD STIG 3.7

Appendix A - Audited Issue Details

Appendix B - Suppressed Issues

Appendix C - New Issue Details

Appendix D - Removed Issue Details

Appendix E - Dependancies

Appendix F - Vulnerability Category Descriptions

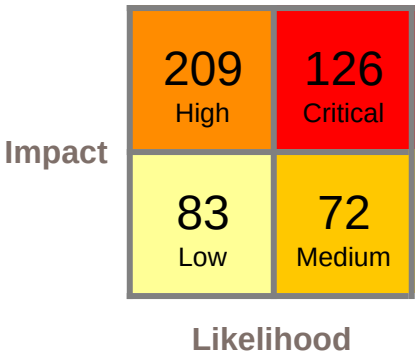
MyBank-Web - 1.0

Overview

Issue Template:	KPMG External
Last Scan LOC:	710,466
Last Scan Files:	3,306
Languages:	

1	High	N/A
Fortify Security Rating	Business Risk	Requirement Progress

Issues by Priority



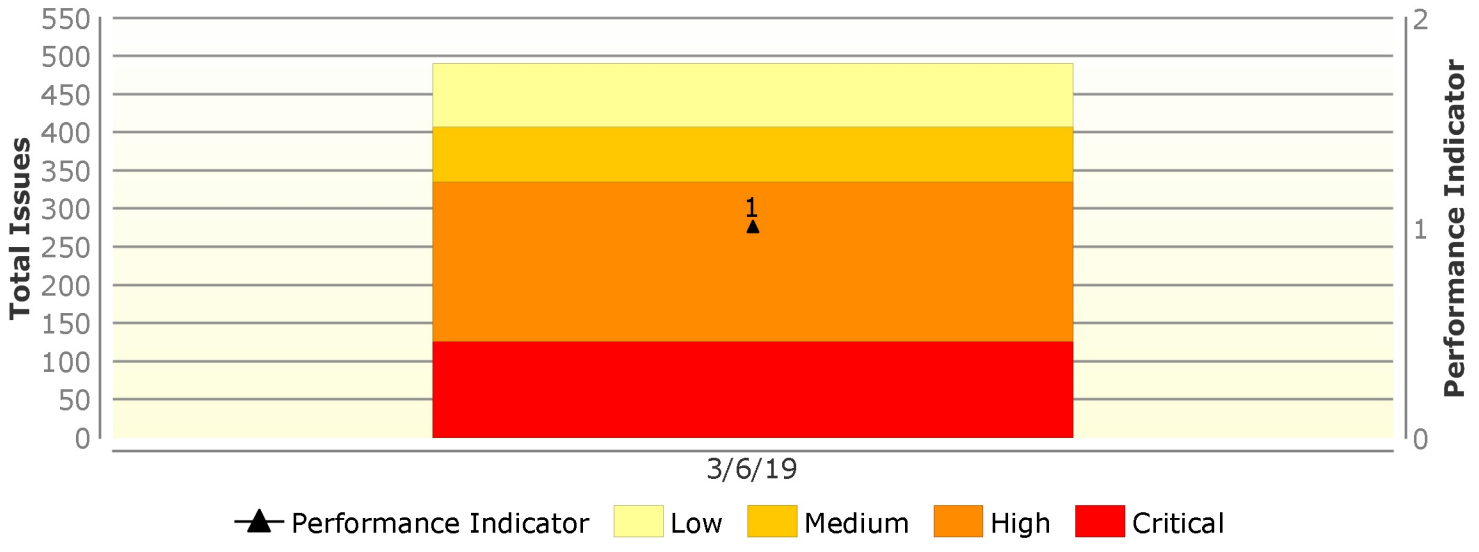
5 Most Prevalant Critical-Priority Issues

Category	Issues
Path Manipulation	**64**
Insecure Transport: Database	**40**
SQL Injection	**14**
Command Injection	**7**
Process Control	**1**

Issues by Attack Vector

Attack Vector	Issues
Database	**34**
Network	0
Web	**281**
Web Service	0
Other	**175**
Total	**490**

Issues and Fortify Security Rating by Date



Issue Trending

Current Performance Indicators

The value in the 'Change' column is the total difference from the first analysis to the current state.

Performance Indicator	Value	Change
Configuration Issues	3 %	-
Critical Exposure Issues	8 %	-
Critical Priority Issues	25 %	-
Critical Priority Issues Audited	97 %	-
Fortify Security Rating	1	-
High Priority Issues	42 %	-
High Priority Issues Audited	97 %	-
Issues That Are Audited	95 %	-
Normalized Vulnerability Score	2.86	-
Remediation Effort - Critical Issues	713	-
Remediation Effort - High Issues	579	-
Remediation Effort - Low Issues	403	-
Remediation Effort - Medium Issues	372	-
Remediation Effort Total	1,743	-
Total Issues	490	-
Vulnerability Density (10KLOC)	6 %	-
Vulnerability Density (KLOC)	0.69	-

Issue Breakdown

Issues by Analysis

Issues by the value an auditor has set for the custom tag 'Analysis.' Once this tag has been set the issue is considered audited.

Value	Priority			
	Critical	High	Medium	Low
Suspicious	0	0	0	3
Bad Practice	85	25	23	11
Not an Issue	38	179	47	59
<None>	3	5	2	10
Total	**126**	**209**	**72**	**83**

Issues by Category (Audited / Total)

Category	Priority			
	Critical	High	Medium	Low
Access Control: Database	0	103 / 103	0	0
Command Injection	7 / 7	2 / 2	0	23 / 25
Connection String Parameter Pollution	0	3 / 3	0	0
Dead Code: Unused Field	0	0	0	0 / 1
Dead Code: Unused Method	0	0	0	0 / 1
Insecure Transport: Database	39 / 40	0	0	0
Log Forging	0	12 / 12	0	0
Missing XML Validation	0	0	0	3 / 3
Password Management: Empty Password	0	1 / 1	0	0
Password Management: Hardcoded Password	0	5 / 5	0	0
Path Manipulation	62 / 64	48 / 48	70 / 72	5 / 5
Path Manipulation: Base Path Overwriting	0	2 / 2	0	0
Process Control	1 / 1	0	0	0
Registry Manipulation	0	0	0	16 / 16
Setting Manipulation	0	0	0	4 / 4
SQL Injection	14 / 14	0	0	22 / 28
Unreleased Resource: Streams	0	2 / 2	0	0
Unreleased Resource: Unmanaged Object	0	10 / 15	0	0
Unsafe Native Invoke	0	16 / 16	0	0
Total	**126**	**209**	**72**	**83**

Issues by OWASP Top Ten 2013

OWASP Top Ten 2013 Category	Priority			
	Critical	High	Medium	Low
A1 Injection	21	17	0	56
A2 Broken Authentication and Session Management	0	0	0	0
A3 Cross-Site Scripting (XSS)	0	0	0	0
A4 Insecure Direct Object References	65	153	72	5
A5 Security Misconfiguration	0	0	0	0
A6 Sensitive Data Exposure	40	6	0	0
A7 Missing Function Level Access Control	0	0	0	0
A8 Cross-Site Request Forgery (CSRF)	0	0	0	0
A9 Using Components with Known Vulnerabilities	0	0	0	0
A10 Unvalidated Redirects and Forwards	0	0	0	0
None	0	33	0	22

** Reported issues in the above table may violate more than one OWASP Top Ten 2013 requirement. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Issues by Category table.*

Issues by PCI DSS 3.0

Requirement	Priority			
	Critical	High	Medium	Low
None	0	0	0	18
Requirement 10.5.2	0	12	0	0
Requirement 4.1	40	0	0	0
Requirement 6.3.1	0	6	0	0
Requirement 6.5.1	21	17	0	60
Requirement 6.5.3	0	6	0	0
Requirement 6.5.4	40	0	0	0
Requirement 6.5.6	0	33	0	0
Requirement 6.5.8	65	153	72	5
Requirement 8.2.1	0	6	0	0

** Reported issues in the above table may violate more than one PCI DSS 3.0 requirement. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Issues by Category table.*

Issues by CWE

CWE Category	Priority			
	Critical	High	Medium	Low
CWE ID 111	0	16	0	0
CWE ID 112	0	0	0	3
CWE ID 114	1	0	0	0
CWE ID 117	0	12	0	0
CWE ID 15	0	0	0	20
CWE ID 22	64	50	72	5
CWE ID 235	0	3	0	0
CWE ID 259	0	6	0	0
CWE ID 297	40	0	0	0
CWE ID 404	0	17	0	0
CWE ID 494	1	0	0	0
CWE ID 561	0	0	0	2
CWE ID 566	0	103	0	0
CWE ID 73	64	50	72	5
CWE ID 77	7	2	0	25
CWE ID 78	7	2	0	25
CWE ID 798	0	5	0	0
CWE ID 89	14	0	0	28

** Reported issues in the above table may violate more than one CWE requirement. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Issues by Category table.*

Issues by WASC 24

WASC Category	Priority			
	Critical	High	Medium	Low
Denial of Service	0	17	0	0
Information Leakage	40	0	0	0
Insufficient Authentication	0	6	0	0
Insufficient Authorization	0	103	0	0
None	1	31	0	25
OS Commanding	7	2	0	25
Path Traversal	64	50	72	5
SQL Injection	14	0	0	28

** Reported issues in the above table may violate more than one WASC 24 requirement. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Issues by Category table.*

Issues by DOD STIG 3.7

Category	Priority			
	Critical	High	Medium	Low
APP3050 CAT II	0	0	0	2
APP3210.1 CAT II	0	6	0	0
APP3250.1 CAT I	40	0	0	0
APP3250.2 CAT I	40	0	0	0
APP3250.3 CAT II	40	0	0	0
APP3250.4 CAT II	40	0	0	0
APP3340 CAT I	0	6	0	0
APP3350 CAT I	0	6	0	0
APP3480.1 CAT I	0	103	0	0
APP3510 CAT I	86	83	72	81
APP3540.1 CAT I	14	0	0	28
APP3540.3 CAT II	14	0	0	28
APP3570 CAT I	8	2	0	25
APP3600 CAT II	64	50	72	5
APP3690.2 CAT II	0	12	0	0
APP3690.4 CAT II	0	12	0	0
APP6080 CAT II	0	17	0	0

** Reported issues in the above table may violate more than one DOD STIG 3.7 requirement. As such, the same issue may appear in more than one row. The total number of unique vulnerabilities are reported in the Issues by Category table.*