Webapp Vulnerability Scan Report

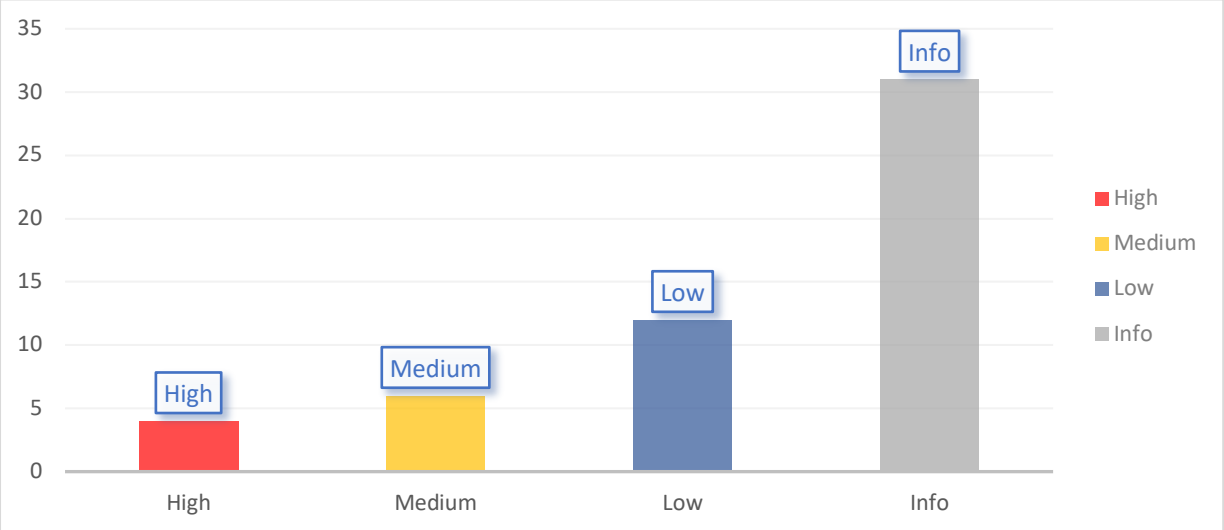
Table of Contents

Scan Information Summary

Target Scanned	http://test.website.com/webapp ✓
Overall Rating	HIGH
Severity Base	CVSS v2.0 Ratings
Start time	2021-06-24 14:49:44 UTC+03
End time	2021-06-24 14:59:44 UTC+03
Scan Duration	57 minutes
Scan Status	FINISHED

Issues Discovered

Total: 53



Tests Performed

Total: 9

Test Type	Name	Performed
Injection	SQL Injection	*YES*
	Command Injection	*YES*
	CRLF	*YES*
	LDAP	*NO*
Broken Authentication	Bypassing access control checks by modifying the URL	*NO*
	Insecure direct object references	*YES*
	Accessing API with missing access controls	*NO*
Fingerprinting	Website Fingerprinting	*YES*
	Libraries	*YES*
Secure Communications	SSL/TLS Check	*YES*
	SSL Vulnerabilities	*NO*
XSS	Stored XSS	*YES*
	Reflected XSS	*NO*

Vulnerabilities

Total: 53

Severity	CVSS	Name	Details
Medium	5.8	HSTS Missing from HTTPS Server (RFC 6789)	View More
High	7.5	Apache version is vulnerable to heap overflow.	View More
Medium	6.2	Communication is not secure	View More
Medium	5.8	Outdated libraries	View More

Risk description:
Vulnerabilities which affect these libraries could be exploited with following exploit: exploit-db.com/exploits/2173
Recommendation:
Upgrade the affected libraries to their lasted versions.

High	9.2	Sensitive Information disclosed	View More
High	8.9	Sensitive files found	View More

Risk description:
These files can contain confidential information such as: application source code, configuration files, SSL certificates, etc. Manual review is
required for the contents of these files.
Recommendation:
We recommend removing these files from the website directory if they are not needed for business purposes.

Low	*N/A*	*Missing Security Header*	View More
Low	N/A	Exposure of Sensitive Information	*View More*

Scanning and Recon

Software Version	*Software Category*
Ubuntu	Operating System
Apache 2.6	Web Serer
jQuery	JavaScript Framework
Symfony	PHP Framework
MySQL	Database

Web Crawler Results

Total URL Crawled: 8

Method	*URL*	*Build Params*
GET	http://test.website.com/webapp	
GET	http://test.website.com/webapp/about.html	
GET	http://test.website.com/webapp/portfolio.html	
GET	http://test.website.com/webapp/services.html	
GET	http://test.website.com/webapp/oneproject.html	
GET	http://test.website.com/webapp/ourteam.html	
GET	http://test.website.com/webapp/assets/img/ourteam.html	
GET	http://test.website.com/webapp/assets/img/css	

SQL Injection

Total SQLi Success: 0
Total SQLi Performed: 1/5
Total SQLi Attempts: 221

✓ In-Band SQLi:

admin") or ("1"="1
admin") or ("1"="1"--
admin") or ("1"="1"#
*admin") or ("1"="1"/**
admin") or "1"="1
admin") or "1"="1"--
admin") or "1"="1"#
*admin") or "1"="1"/**
1234 " AND 1=0 UNION ALL SELECT "admin", "81dc9bdb52d04dc20036dbd8313ed055

✗ Error-based SQLi;
✗ Union-based SQLi;
✗ Inferential SQLi (Blind SQLi);
✗ Boolean-based SQLi;

Cross-Site Scripting

✓ Nothing was found.

Login Interfaces

✓ Nothing was found.

Disclosed Error Messages

✓ Nothing was found.

Operating System Command Injection

✓ Nothing was found.

Directory Traversal

✓ Nothing was found.

Contact Us

Ionut Staniu

ionut.staniu@blackbullet.ro

+40 767890619

www.blackbullet.ro

21 Elena Caragiani Street, Bucharest, Romania