PENTEST BD

Web Application Penetration Testing Report of CC Commerce

Version: 1.0

Prepared By

Rishad Istiak

Pentest BD

Presented To:

Mr. John

CC Commerce

Date: 5 May 2022

PENTEST BD

Table of Contents

PENTEST BD

EXECUTIVE SUMMARY

Pentest BD has conducted a comprehensive penetration test of CC Commerce to identify the vulnerabilities in their web application. The time period of this assessment is from 10 January 2022 to 5 April 2022.

Test Scope

In this engagement, only the main domain of the web application of CC Commerce was in scope for testing. No Denial of Service and Social Engineering attacks were permitted. The assessment was performed manually and also using various industry standard tools like nmap, nessus, burpsuite, metasploit etc.

Testing Summary

Pentest BD has tested in all possible attack vectors for the web application and evaluated the security posture of CC Commerce. Different attacks like Injection, file inclusion, default credential, authentication & authorization issues, misconfiguration, unrestricted file upload etc are tested

Recommendations

Based on the detected vulnerabilities, Pentest BD is providing the following recommendations to enhance the overall security posture of CC Commerce.

- ✓ Ensure user input validation
- ✓ Enforce strong password policy
- ✓ Always apply zero trust policy
- ✓ Enable multi factor authentication for the services
- ✓ Enable auto update feature

PENTEST BD

TESTING APPROACH

Overview

The whole assessment was performed in several phases. The following phases has been used in this penetration testing engagement.

1. **Planning:** Rules of engagement, scopes, goals etc. are defined in this phase.
2. **Discovery:** In this phase, scanning is performed to identify potential vulnerabilities.
3. **Attack:** Try to exploit the vulnerabilities to identify potential vulnerabilities.
4. **Reporting:** All the findings & evidences are properly documented in this phase.

Fig: Penetration Testing Methodology

PENTEST BD

Finding Severity Ratings

The below given table defines levels of security which are used throughout the document to assess the vulnerabilities & risk impact

Severity	Definition
Critical	Exploitation leads to compromising the web server where the attacker can attempt furtherer exploitation and persistence
High	Exploitation can reveal sensitive information and allow the attacker to attempt more attacks that can lead to the web server being compromised.
Medium	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved
Low	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window
Info	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation

Web Application Findings

Scope

For the assessment, the following domain name was in scope.

Target Domain
secretsite.org

PENTEST BD

Vulnerability Summary & Report

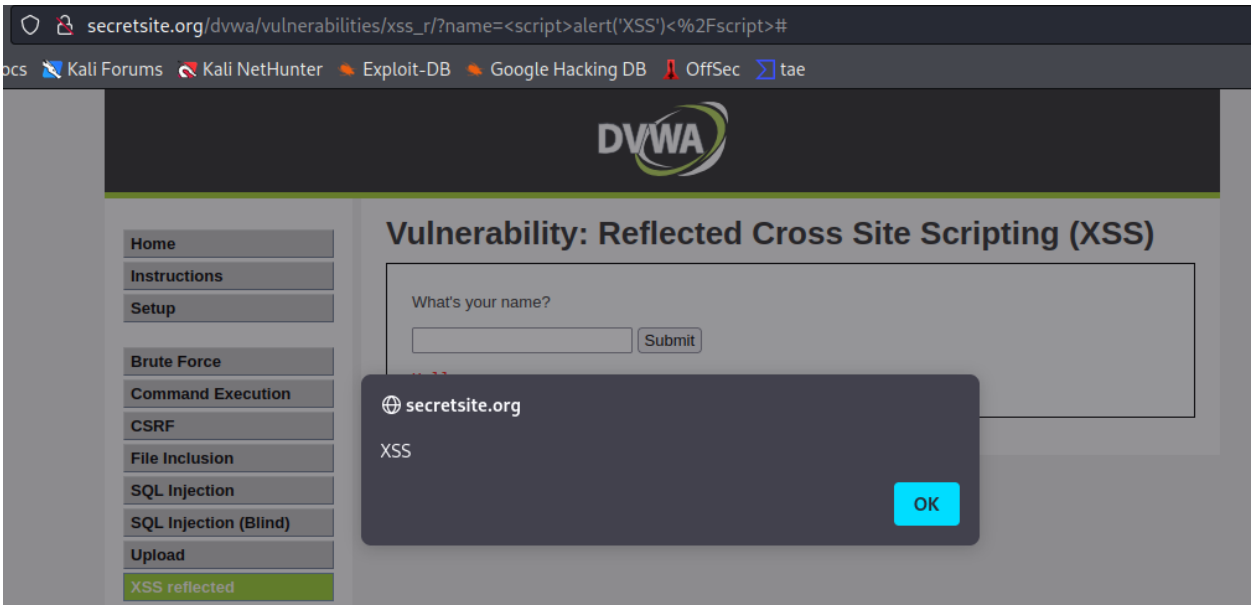
2	1	0	1	0
Critical	High	Medium	Low	Informational

Vulnerability Name	Severity	Recommendation
WPT-01: Reflected Cross Site Scripting	HIGH	Input sanitization & encoding
WPT-02: SQL Injection	CRITICAL	Sanitize user input
WPT-03: Default Credential in Use	CRITICAL	Enforce strong password policy
WPT-04: Cookie Without Same Site Attribute	LOW	Set samesite attribute

Vulnerability Details

WPT-01: Reflected Cross Site Scripting	
Location	http://secretsite.org/dvwa/vulnerabilities/xss_r/
Description	Various URL's were tested & XSS was found due to insufficient user input sanitization
Impact	HIGH
Remediation	To mitigate XSS, you must sanitize your input. Your application code should never output data received as input directly to the browser without checking it for malicious code.

Evidence



References

- https://www.acunetix.com/websitesecurity/cross-site-scripting/
- https://wiki.owasp.org/index.php/PHP_Top_5/

WPT-02: SQL Injection	
Location	http://secretsite.org/dvwa/vulnerabilities/sqli/
Description	Parameter "ID" was vulnerable to SQL Injection which leads to database dump
Impact	HIGH
Remediation	Use parameterized queries when dealing with SQL queries that contain user input. Parameterized queries allow the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection

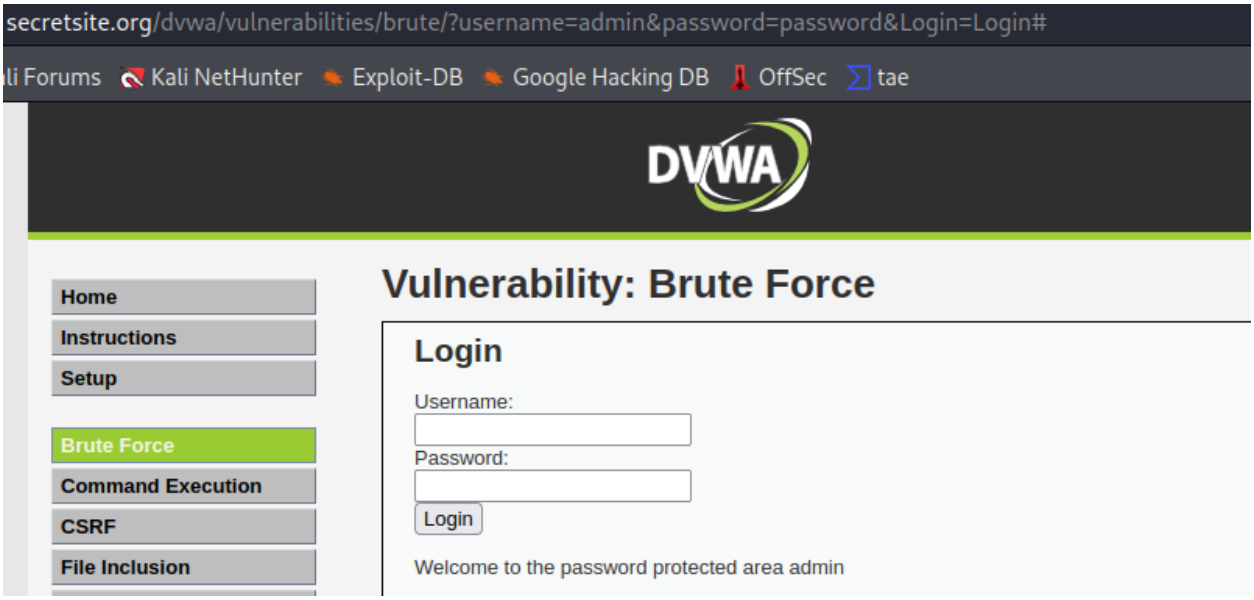
Evidence

References

- https://www.acunetix.com/websitesecurity/sql-injection/
- https://owasp.org/www-community/attacks/SQL_Injection

WPT-03: Default Credential in Use	
Location	http://secretsite.org/dvwa/vulnerabilities/brute/
Description	The target host has File share service enabled. But it doesn't require any authentication mechanism to access the shares.
Impact	CRITICAL
Remediation	Enforce strong password policy in the system

Evidence

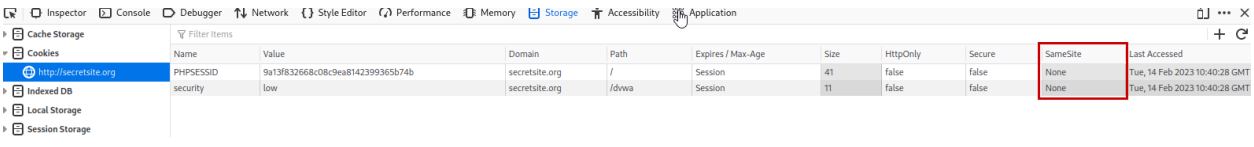


References

- https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/04-Authentication_Testing/02-Testing_for_Default_Credentials
- https://capec.mitre.org/data/definitions/70.html

WPT-04: Cookie Without Same Site Attribute	
Location	http://secretsite.org/dvwa/
Description	PHPSESSIONID does not have the SameSite attribute. Attackers can abuse this in CSRF attacks.
Impact	LOW
Remediation	Set the same site attribute

Evidence



References

- https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite

Conclusion

The main domain is in scope at this time. We have considered it as a black box testing. So we weren't provided any information about the target excluding the domain name. This was the first penetration test of CC Commerce. We have identified several critical & high issues that can be exploited. So we have provided the remediation plan. We have also added all the screenshots, vulnerability scanning report in the drive link. For additional information & documents, please check that drive.

PENTEST BD

THANKS