Report for:

Web Application Penetration Testing Reassessment

Broker-MarketPlace

Application: **Broker-MarketPlace – v1.0**

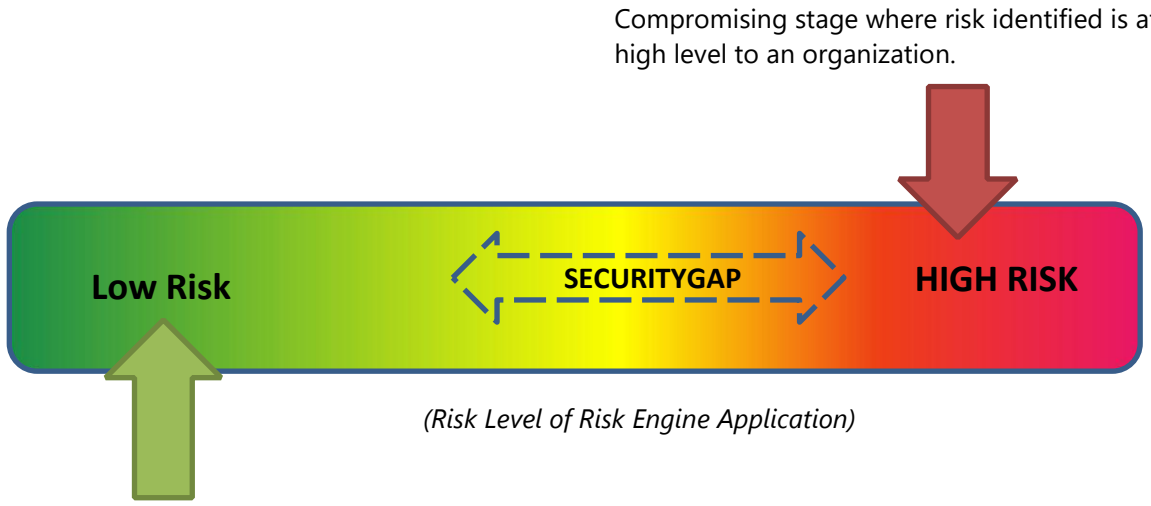
1st August 2026

Table of Contents

Executive Summary

This report presents the outcomes of an external penetration test conducted on behalf of CodeCrimson for Broker-MarketPlace. Authorized by Broker-MarketPlace, the reassessment was conducted on **1st August 2026**. The primary emphasis during this penetration test was on a specific web application, accessible at **https://broker-marketplace.com .**

The application exhibited no several significant security concerns in the retest, an appreciation for the prompt attention from Broker-Marketplace team for fixing of the existing vulnerabilities.



Overview

All activities were conducted in a manner that simulated a malicious actor engaged in a target. The assessment of the application was placed on the identification and exploitation of the security weaknesses. During the reassessment, the vulnerabilities that were found were related to Privilege Escalation via Business Logic Bypass, Broken Access Control on administrative endpoints, Insecure Cross-Origin Resource Sharing (CORS) Configuration, Information Disclosure via robots metafiles, and a Weak Content Security Policy (CSP) are no longer reproducible.

Below table provides severity of the vulnerabilities that were found in the web application.

Phase	Description	Critical	High	Medium	Low	Informational
1	Web Application Penetration Reassessment	0	0	0	0	0
	Total	0	0	0	0	0

Strategic Recommendations

Regardless of the Security Model employed, attackers possess the flexibility to compromise on the application, as they lack specific procedures, unlike ethical hackers who strictly adhere to Rules of Engagement (ROE). To mitigate this risk, users should acquire technical proficiency regarding potential attack vectors, particularly emphasizing threats like phishing. Addressing these vulnerabilities requires proactive training programs to educate users on recognizing phishing emails and identifying potentially risky websites.

On the application front, it is imperative for engineers and developers to enforce secure coding practices. This measure aims to fortify the application, making it challenging for malicious actors to exploit vulnerabilities and compromise data. The incorporation of secure coding practices serves as a robust defense, eliminating numerous exploit opportunities that hinge on insecure code. This proactive approach significantly raises the bar for potential attackers seeking to compromise the application's security.

Using This Report

To facilitate the dissemination of the information within this report throughout your organisation, this document has been divided into the following clearly marked and separable sections.

Document Breakdown	
Executive Summary	Management level, strategic overview of the assessment and the risks posed to the business
Technical Summary	An overview of the assessment from a more technical perspective, including a defined scope and any caveats which may apply
Technical Details	Detailed discussion (including evidence and recommendations) for each individual security issue which was identified
Supplemental Data	Any additional evidence which was too lengthy to include in Section 2
Appendices	This section usually includes the security tools which were used, outlines the assessment methodologies and lists the assessment team members

Document Control

Client Confidentiality

The information that contains in this document is confidential and can only be accessed by authorized people. Such information should not be copied without a written permission.

Proprietary Information

The information in this document is considered proprietary information and should not be disclosed to any third party without prior information. The information written on this document shall only be accessed by the security team and to the client only.

Document Version Control	
Data Classification	Confidential
Client Name	Broker-MarketPlace
Document Title	Web Application Penetration Testing Report
Author	Rehan Mumtaz
Reviewed By	Rehan Mumtaz

Document History			
Issue No.	**Issue Date**	**Issued By**	**Change Description**
0.1	29/07/2026	Rehan Mumtaz	External Pentest Engaged
0.2	1/08/2026	Rehan Mumtaz	Retest & Revised Reports
0.3	1/08/2026	howtopc792	Released to Client

Document Distribution List	
Rehan Mumtaz	Sr. Penetration Tester
Rehan Mumtaz	Sr. Penetration Tester
howtopc792	Founder, Broker MarketPlace

1. Technical Summary

CodeCrimson was contacted by Broker-MarketPlace for External Penetration Testing of their web application within the scope for the identification for possible security issues that could impact the business if such malicious attack would occur.

1.1 Scope

The Penetration Test was carried out on a Web Application. The following is the mentioned URL: -

- https://broker-marketplace.com

1.2 Caveats

Some tests that would disrupt the application were excluded from the scope such as Denial of service or DDOS.

1.3 Post Assessment Clean-up

Revert any changes which were made during the penetration test for the application.

1.4 Risk Ratings

The table below gives a key to the used throughout this report to provide a clear and concise risk scoring system. It should be stressed that quantifying the overall business risk posed by any of the issues found in any test is outside our remit. This means that some risks may be reported as high from a technical perspective but may, because of other controls unknown to us, be considered acceptable.

Risk Rating	CVSSv2 Score	Explanation
Critical	9.0 - 10	A vulnerability was discovered that has been rated as critical. This requires resolution as quickly as possible.
High	7.0 – 8.9	A vulnerability was discovered that has been rated as high. This requires resolution in the short term.
Medium	4.0 – 6.9	A vulnerability was discovered that has been rated as medium. This should be resolved as part of the ongoing security maintenance of the system.
Low	1.0 – 3.9	A vulnerability was discovered that has been rated as low. This should be addressed as part of routine maintenance tasks.
Info	0 – 0.9	A discovery was made that is reported for information. This should be addressed to meet leading practice.

1.5 Exploitability

In the realm of penetration testing, each identified vulnerability uncovered through active assessment is assigned an exploitability rating. This rating assesses the likelihood that an attacker can discover and exploit the vulnerability to cause harm to the application or compromise the protected data.

CodeCrimson recommends leveraging the exploitability rating as a crucial metric for prioritizing the remediation of findings within specific groups that share the same severity and difficulty of fix classification. This focused approach ensures a streamlined effort in addressing vulnerabilities of similar threat levels, specifically within the dynamic landscape of the web application environment. The exploitability ratings include:

Exploitability	Description
Low	Very unlikely to be exploited
Medium	Neither likely nor unlikely to be exploited
High	Very likely to be exploited

Findings Overview

All the issues identified during the assessment are listed below with a brief description and risk rating for each issue. The risk ratings used in this report are defined in Section 1.4 Risk Ratings.

Phase 1 – Penetration Testing Assessment

The below diagram depicts the number of vulnerabilities that are found in the Web Application.

Supplemental Data

There is no supplemental data for this report.

Appendices

Tool List

The following tools were used during the assessment:

Tool Used	Description
Burp Suite	A comprehensive suite of tools for web application security testing.

Tailored Methodologies

External Penetration Testing Assessment

Key Information

An external web application assessment is an in-depth exploration aimed at comprehensively evaluating the security landscape of an organization's web-facing applications. These applications represent critical points of exposure to cyber threats, making this assessment crucial for safeguarding sensitive data, ensuring regulatory compliance, and fortifying the overall cybersecurity posture.

The four-phase methodology employed—profiling, discovery, assessment, and exploitation—is meticulously crafted to systematically uncover vulnerabilities specific to web environments. These vulnerabilities often stem from complex interactions between user inputs, insecure coding practices, and configuration oversights unique to web applications.

Test Highlights

Profiling of the corporate application using non-invasive techniques including:

1. Profiling the Web Application
    - Employ Open-Source Intelligence (OSINT) techniques to gather comprehensive information, encompassing:
    - IP Addresses
    - Host/Port Discovery
2. Foot-printing
    - Methodically gather domain-related intelligence, including:
    - Domain Name Information
    - IP Addresses
    - Execute passive and active scans, employ directory brute forcing, and leverage Whois information.
3. Network Scanning
    - Execute TCP & UDP port scanning.
    - Employ OS fingerprinting techniques to identify target system characteristics.
    - Identify and enumerate services running on accessible ports.
4. Vulnerability Assessment
    - Systematically assess and analyze vulnerabilities present in the web application.
    - Utilize automated tools for thorough Vulnerability Assessment.
5. Penetration Testing & manual assessment
    - Conduct manual testing to identify vulnerabilities, including but not limited to: -

- Brute Force Attacks
- Session Hijacking
- File Upload Vulnerabilities
- SSL Configuration Checks
- No Rate Limiting Checks
- Authentication Mechanism Strength Evaluation
- Injection (e.g., SQL, NoSQL, OS)
- Broken Authentication
- Sensitive Data Exposure
- XML External Entity (XXE)
- Broken Access Control
- Security Misconfigurations
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using Components with Known Vulnerabilities
- Insufficient Logging & Monitoring

6. Authentication Testing
    - Scrutinize the robustness of authentication mechanisms.
    - Test for the presence of weak or default credentials
7. API Security Assessment
    - Assess the security robustness of any exposed APIs.
    - Scrutinize for vulnerabilities such as authorization bypass or injection in API requests.

8 Client-Side Security Assessment
    - Evaluate the security posture of client-side scripts.
    - Identify and address potential security vulnerabilities in JavaScript code.

9. Reporting
    - Deliver a comprehensive report detailing discovered vulnerabilities, their severity, and recommended mitigation strategies.
    - Include a concise summary of findings, risk assessments, and actionable remediation strategies.

CodeCrimson utilizes a diverse set of scanning tools and methodologies tailored for web application penetration testing, strategically evaluating, and leveraging opportunities within the defined rules of engagement and the specified scope. After the completion of automated discovery, manual testing is employed to identify potential attack vectors specific to web applications.

The information gathered is then strategically employed in targeted attacks against exposed web services. These attack scenarios encompass a variety of exploits, including those targeting memory corruption vulnerabilities and web system misconfigurations, subject to client agreement. The execution of all exploitation strictly adheres to pre-established rules of engagement, recognizing that the success of exploitation depends on the prevailing circumstances.

Authentication processes within the web application are methodically tested, utilizing both direct and indirect methods such as brute force and password guessing techniques. Notably, precautions are taken to avoid brute-force attacks in situations where the risk of account lockout exists.

Upon the successful exploitation of vulnerabilities, gained access and privileges are leveraged to pursue the escalation of access rights to the maximum achievable level within the web application. Rigorous record-keeping practices are followed to document all recovered data, with copies securely stored before any modifications are made to files. Each exploit is accompanied by a thorough risk assessment, aiming to mitigate potential disruptions to live web systems.

Assessment Team

The following members of staff were assigned to this assessment.

Name	Job Title	Comments
Rehan Mumtaz	Sr. Penetration Tester	CRT.

This is to acknowledge that

Rehan Mumtaz

OSID: 57216423

has achieved the

OSCP+

(OffSec Certified Professional Plus)

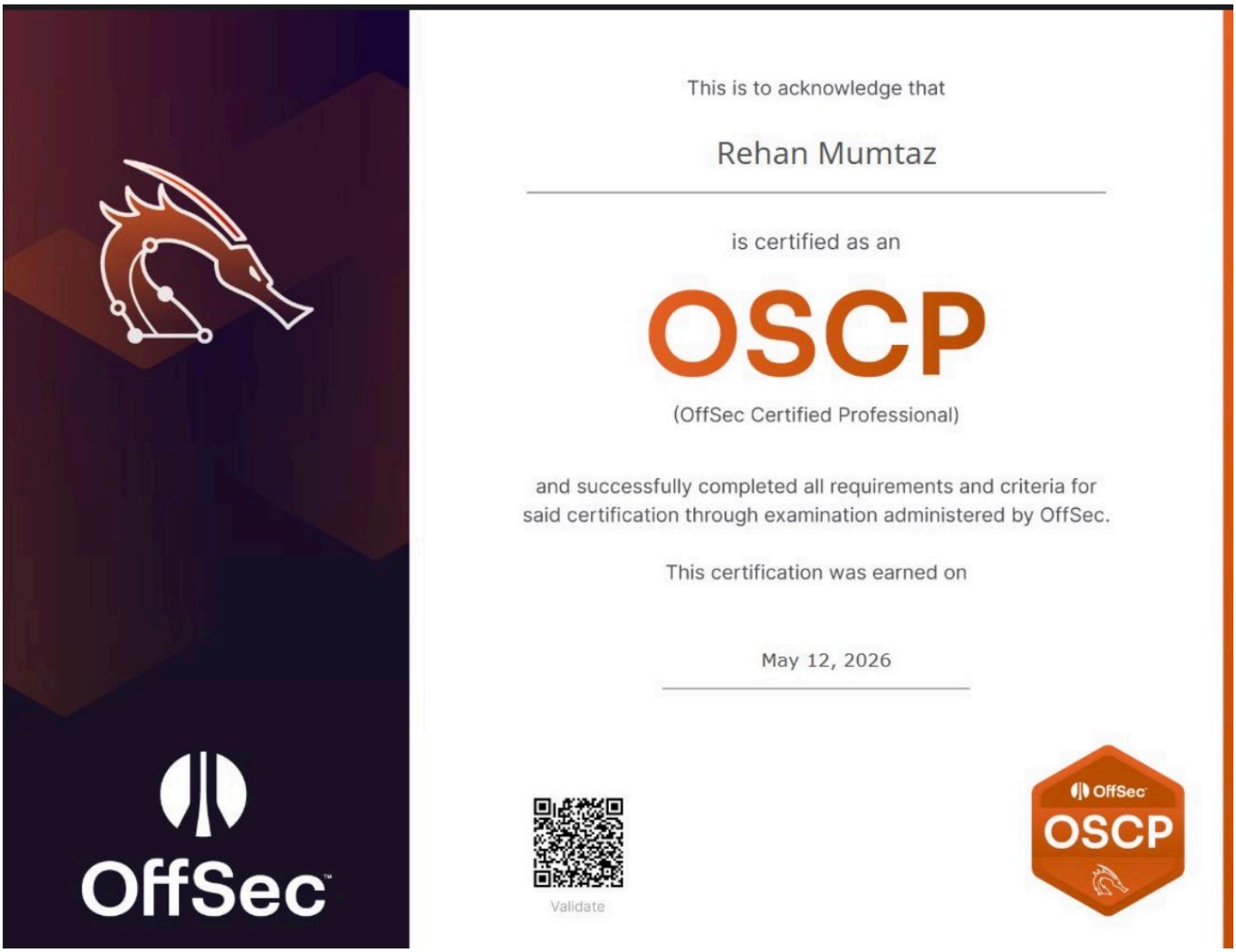
and successfully completed all requirements and criteria for said certification through examination administered by OffSec.

This certification was earned on

May 12, 2026

This certification expires three years after issuance.

Ning Wang, OffSec CEO


This is to acknowledge that
Rehan Mumtaz
is certified as an
OSCP
(OffSec Certified Professional)
and successfully completed all requirements and criteria for said certification through examination administered by OffSec.
This certification was earned on
May 12, 2026
Validate
OffSec
OSCP
OffSec

ALTERED SECURITY

CERTIFIED RED TEAM PROFESSIONAL (CRTP)

This is to certify that

Rehan Mumtaz

has successfully completed all the requirements for the

ACTIVE DIRECTORY ATTACK-DEFENSE LAB

and has passed the certification exam as of **September 4, 2024**

Nikhil Mittal
Founder, Altered Security

Student ID: **ADLID9805**

INE SECURITY

PROUDLY PRESENTED TO

Rehan Mumtaz

eCPPT

Certified Professional Penetration Tester

Tracy Wallace
Director of Content Development

Dara Warn
Chief Executive Officer