

Blind Security

BlindSec Portal Application Pentest

## Business Confidential

*Date: March 28th 2025 Project: DC-001 Version 1.0*



## Table of Contents

Περιεχόμενα

[Business Confidential 1](#_Toc170944781)

[Table of Contents 2](#_Toc170944782)

[Confidentiality Statement 3](#_Toc170944783)

[Disclaimer 3](#_Toc170944784)

[Contact Information 3](#_Toc170944785)

[Assessment Overview 4](#_Toc170944786)

[Assessment Components 4](#_Toc170944787)

[Web Application Penetration Test 4](#_Toc170944788)

[Finding Severity Ratings 5](#_Toc170944789)

[Risk Factors 5](#_Toc170944790)

[Likelihood 5](#_Toc170944791)

[Impact 5](#_Toc170944792)

[Scope 6](#_Toc170944793)

[Scope Exclusions 6](#_Toc170944794)

[Client Allowances 6](#_Toc170944795)

[Executive Summary 7](#_Toc170944796)

[Scoping and Time Limitations 7](#_Toc170944797)

[Identified Kill Chain 7](#_Toc170944798)

[Tester Notes and Recommendations 7](#_Toc170944799)

[Vulnerability Summary & Report Card 8](#_Toc170944800)

[Internal Penetration Test Findings 8](#_Toc170944801)

[Technical Findings 9](#_Toc170944802)

[Web Application Penetration Test Findings 9](#_Toc170944803)

[Additional Scans and Reports 10](#_Toc170944804)

# Confidentiality Statement

This document is the exclusive property of Blind Security and CSCGR Pentesting Team. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Blind Security and CSCGR Pentesting Team.

Blind Security may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

# Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. CSCGR Pentesting Team prioritized the assessment to identify the weakest security controls an attacker would exploit. The CSCGR Pentesting Team recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

# Contact Information

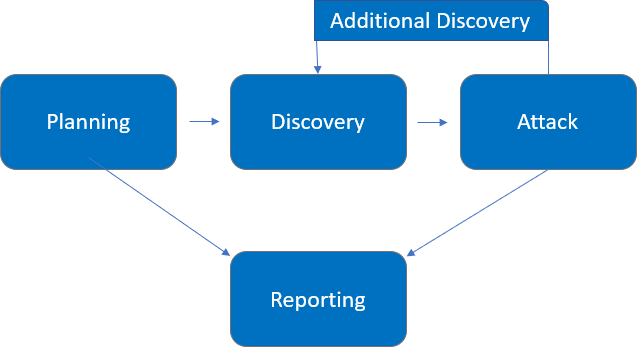
|  |  |  |
| --- | --- | --- |
| **Name** | **Title** | **Contact Information** |
| Blind Security | | |
| Petros Papadopoulos | CSO | Email: petros.papadopoulos@blindsecurity.net |
| CSCGR Pentesting Team | | |
| Your\_Team\_Lead | Senior Consultant | Email: your-team-lead-email |
| Your\_Team\_Member | Consultant | Email: your-team-member -email |
| Your\_Team\_Member | Consultant | Email: your-team-member -email |
| Your\_Team\_Member | Consultant | Email: your-team-member -email |

# Assessment Overview

In March 28th, 2025, CSCGR Pentesting Team engaged Blind Security for 6 hours to evaluate the security posture of its application compared to current industry best practices that included a black-box web application penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

* Planning – Customer goals are gathered and rules of engagement obtained.
* Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
* Attack – Confirm potential vulnerabilities through exploitation.
* Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



# Assessment Components

### Web Application Penetration Test

A web application penetration test simulates an attacker targeting a web application. A pentester will analyze the application to identify potential vulnerabilities and perform common and advanced web attacks, such as SQL injection, cross-site scripting (XSS), remote code execution (RCE), and security misconfigurations. The pentester will attempt to exploit these vulnerabilities to gain unauthorized access, escalate privileges, compromise user and admin accounts, and exfiltrate sensitive data.

# Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

|  |  |  |
| --- | --- | --- |
| **Severity** | **CVSS V3**  **Score Range** | **Definition** |
| Critical | 9.0-10.0 | Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately. |
| High | 7.0-8.9 | Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible. |
| Moderate | 4.0-6.9 | 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 | 0.1-3.9 | 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. |
| Informational | N/A | No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation. |

# Risk Factors

Risk is measured by two factors: Likelihood and Impact:

### Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

### Impact

Impact measures the potential vulnerability’s effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

# Scope

|  |  |
| --- | --- |
| **Assessment** | **Details** |
| BlindSec Portal | https://portal.blindsecurity.net |

### Scope Exclusions

Per client request, CSCGR Pentesting Team did not perform any of the following attacks during testing:

* Denial of Service (DoS)
* Phishing/Social Engineering
* Password Guessing / Bruteforcing Attacks
* Active Scans with tools such as Dirbuster, gobuster, sqlmap, etc.

All other attacks not specified above were permitted by Blind Security

### Client Allowances

Blind Security did not provide CSCGR Pentesting Team any allowances. CSCGR Pentesting Team has treated the assessment as a black box assessment.

# Executive Summary

CSCGR Pentesting Team evaluated Blind Security’s web application “BlindSec Portal” through penetration testing at March 28th, 2025. The following sections provide a high-level overview of vulnerabilities discovered, and the kill chain that can lead to <Major Impact issue>.

### Scoping and Time Limitations

Scoping during the engagement did not permit denial of service, social engineering, active scans or password guessing or bruteforcing attacks across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for six

(6) business hours.

### Identified Kill Chain

Your-Kill-Chain

### Tester Notes and Recommendations

Quick notes on what was discovered. Really high level, remember this section is talking to stakeholders, not devs or IT.

# Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

### Internal Penetration Test Findings

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| X | X | X | X | X |
| Critical | High | Moderate | Low | Informational |

|  |  |  |
| --- | --- | --- |
| **Finding** | **Severity** | **Recommendation** |
| Web Application Penetration Test | | |
| WEBXX: Finding Title | Critical | Recommendation |
| WEBXX: Finding Title | Critical | Recommendation |
| WEBXX: Finding Title | Critical | Recommendation |

|  |  |  |
| --- | --- | --- |
| WEBXX: Finding Title | Moderate | Recommendation |

<Delete this comment before sending> - Three findings are enough, if you’d like to add more, it’s up to you.<Delete this comment before sending>

# Technical Findings

### Web Application Penetration Test Findings

Finding WEBXX: Finding Title (Critical)

|  |  |
| --- | --- |
| Description: | Small description of the issue |
| Risk: | Likelihood: High – What’s the likelihood of it being exploited? Think of terms of ease of exploitation and required privileges.  Impact: High – What’s the impact if exploited? Think of terms of compromise and post compromise. Does it affect one user, or all users, what can an attacker do with it? |
| References: | One reference of the issue is enough, try to find an OWASP link |

Evidence

Can be screenshots

Remediation

What’s your remediation recommendations?

### Additional Scans and Reports

CSCGR Pentesting Team provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by CSCGR Pentesting Team.

The reports identify hygiene issues needing attention but are less likely to lead to a breach, i.e. defense-in-depth opportunities. For more information, please see the documents in your shared drive folder labeled “Additional Scans and Reports”.



Last Page