1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **helpdesk.campusbrno.cz**. The evaluation was performed using a certified web application and infrastructure penetration testing tool, adhering to OWASP and OSCP methodologies. The analysis commenced on **April 15th at 07:00** and concluded after **10 minutes and 54 seconds**. The assessment was classified as a “Basic” type.

1.2 Short Summary of Main Issues

The security assessment identified a total of **19 issues**, categorized as **0 High**, **2 Medium**, **2 Low**, and **15 informational**. The most critical findings include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, significantly increasing the risk of injection-based attacks and potential data breaches. Additionally, the Nmap port scan revealed open ports, including HTTP on port **80**, which lacks encryption, posing a Medium risk. The SSL/TLS assessment showed compliance with modern standards, with **1 endpoint** supporting TLS 1.3 and TLS 1.2, indicating a Low risk. Immediate actions should focus on implementing WAF protection and ensuring HTTP traffic is redirected to HTTPS to mitigate vulnerabilities.

1.3 Key Security Issues

Title	Risk
Absence of WAF	Medium
Nmap Port Scan Results Analysis	Medium
SSL/TLS Protocols Security	Low
Login Form Detection Analysis	Low

1.3.1 Absence of WAF

Description

The absence of a Web Application Firewall (WAF) was detected on the analyzed host, resulting in a **100% vulnerability rate**. This significantly elevates the risk of successful cyber-attacks, particularly injection-based attacks, potentially leading to unauthorized data access, data breaches, and system compromise.

Affected Assets

- Domain: **helpdesk.campusbrno.cz**

Recommendations

Implement a Web Application Firewall (WAF) to provide an additional layer of security by filtering and monitoring HTTP traffic between the web application and the Internet. This will help mitigate risks associated with injection-based attacks and unauthorized access.

1.3.2 Nmap Port Scan Results Analysis

Description

The Nmap port scan revealed **2 open ports**, including port **80** running HTTP without encryption. This poses a Medium risk unless there is a redirection to HTTPS or HSTS is enabled.

Affected Assets

- IP Address: **164.215.114.30** - Ports: **80/tcp** and **8443/tcp**

Recommendations

Ensure that all HTTP traffic is redirected to HTTPS to protect data in transit. Implement HSTS

(HTTP Strict Transport Security) to enforce secure connections and prevent man-in-the-middle attacks.

1.3.3 SSL/TLS Protocols Security Assessment

Description
The SSL/TLS assessment showed that the endpoint supports TLS 1.3 and TLS 1.2, which are considered secure protocols. No endpoints were found using deprecated or vulnerable protocols such as SSLv3 or TLS 1.0.

Affected Assets
- No vulnerable hosts detected

Recommendations
Continue monitoring and maintaining current SSL/TLS configurations to ensure compliance with best practices. Regularly update cryptographic libraries to protect against emerging threats.

1.3.4 Login Form Detection Analysis

Description
A total of **1 login form** was detected across the application, which requires security validation to ensure it is not susceptible to common vulnerabilities such as brute force attacks or credential stuffing.

Affected Assets
- URLs: - `http://164.215.114.30:8443` - `http://helpdesk.campusbrno.cz:8443`

Recommendations
Implement strong authentication mechanisms such as multi-factor authentication (MFA) and rate limiting on login attempts to enhance security. Regularly review login form security settings to prevent unauthorized access.

1.4 General Recommendation

To enhance the overall security posture, it is recommended to implement a comprehensive security strategy that includes regular vulnerability assessments, timely patch management, and continuous monitoring of network traffic. Additionally, employee training on cybersecurity best practices should be conducted to mitigate human-related risks.