1 Executive Security Assessment Report

1.1 Analysis Overview

A comprehensive security assessment was conducted on the domain **feldentertainment.fr**. The analysis was initiated on **April 14th** at **05:45** and completed in **00h:10m:51s**. The assessment employed a basic scan methodology focusing on High and Medium-risk vulnerabilities. The evaluation adhered to OWASP and OSCP methodologies to ensure thoroughness and accuracy.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **1 High-risk**, **3 Medium-risk**, **1 Low-risk**, and **13 informational**. The most critical finding is the use of deprecated and vulnerable SSL/TLS protocols, including TLS 1.0 and TLS 1.1, across **6 endpoints**, posing significant security risks such as susceptibility to the BEAST attack. Additionally, the SSL certificate for feldentertainment.fr is nearing expiration with only **48 days** remaining, requiring prompt renewal to avoid service disruptions. Medium-risk issues include shared hosting environments and insecure open ports (HTTP on port 80 and 8080) that could expose the network to potential threats. Immediate attention to these vulnerabilities is essential to enhance security posture and mitigate potential business impacts.

1.3 Key Security Issues

Title	Risk
SSL/TLS Protocols Security Assessment	High
Shared Hosting Environment Analysis	Medium
Nmap Port Scan Results Analysis	Medium
SSL Certificate Expiration Analysis	Medium
Login Form Detection Analysis	Low

1.3.1 SSL/TLS Protocols Security Assessment

Description:

The assessment revealed the presence of deprecated SSL/TLS protocols, specifically TLS 1.0 and TLS 1.1, across **6 endpoints**. These protocols are vulnerable to attacks such as BEAST and lack modern cryptographic algorithms, posing a critical risk to data integrity and confidentiality.

Affected Assets:

- **6 endpoints** using TLS 1.0
- **6 endpoints** using TLS 1.1

Recommendations:

Immediate deprecation of TLS 1.0 and TLS 1.1 is advised. Transition to TLS 1.2 or ideally TLS 1.3, which offer enhanced security features and performance improvements.

1.3.2 Shared Hosting Environment Analysis

Description:

The domain **feldentertainment.fr** operates within a shared hosting environment with **38 shared domains**, categorized under medium interest. This configuration can lead to resource contention and potential security risks if one of the shared domains is compromised.

Affected Assets:

- Hostname: **feldentertainment.fr**

Recommendations:

Consider migrating to a dedicated hosting environment or implementing strict isolation measures between shared domains to mitigate potential risks.

1.3.3 Nmap Port Scan Results Analysis

Description:

The scan identified **4 open ports**, with ports 80 and 8080 flagged as potentially insecure due to lack of encryption and exposure to web service vulnerabilities.

Affected Assets:

- IP Address: **104.26.2.160**
- Ports: **80/tcp, 443/tcp, 8080/tcp, 8443/tcp**

Recommendations:

Ensure that HTTP services on ports 80 and 8080 are redirected to HTTPS or have HSTS enabled to enforce secure connections.

1.3.4 SSL Certificate Expiration Analysis

Description:

The SSL certificate for **feldentertainment.fr** is set to expire in **48 days**, placing it in the warning category for renewal.

Affected Assets:

- Domain: **feldentertainment.fr**

Recommendations:

Plan for immediate renewal of the SSL certificate to prevent service disruption and maintain secure communications.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to prioritize the remediation of High-risk vulnerabilities, particularly those related to deprecated protocols and certificate management. Regular security assessments should be conducted to identify emerging threats and ensure compliance with industry best practices. Additionally, consider implementing a robust monitoring strategy to detect and respond to potential security incidents promptly.