1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **patentum.at**. The analysis commenced on **May 13th** at **15:00** and concluded in **11 minutes and 57 seconds**. The assessment was identified by tracking ID **0d0711f9990f** and utilized a **Basic** scan type. The scope of the work included evaluating the web application and infrastructure for vulnerabilities, focusing on high and medium-risk issues.

1.2 Summary of Key Issues

The security assessment identified a total of **20 issues**, categorized as **2 high-risk**, **4 medium-risk**, **2 low-risk**, and **12 informational**. Critical findings include the presence of unencrypted HTTP traffic and an expired SSL certificate, both posing significant risks of data interception and non-compliance with security standards. The absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts further elevates the risk of cyber-attacks. Medium-risk issues such as shared hosting environments and open HTTP ports without encryption were also noted, potentially exposing sensitive data. Immediate action is recommended to address these vulnerabilities, particularly by implementing HTTPS and renewing SSL certificates to mitigate risks and enhance security posture.

1.3 Key Security Issues

Title	Risk
Unencrypted HTTP Traffic Detected	High
SSL Certificate Expiration Analysis	High
Absence of WAF	Medium
Shared Hosting Environment Analysis	Medium
Nmap Port Scan Results Analysis	Medium
Login Form Detection Analysis	Medium

1.3.1 Unencrypted HTTP Traffic Detected

Description:
Unencrypted HTTP traffic was detected on **2 URLs**, including `http://78.136.38.106:80` and `http://www.patentum.at:80`. This lack of encryption poses significant risks such as data interception, man-in-the-middle attacks, and compromise of sensitive information.
- **Affected Assets:**
-URLs: `http://78.136.38.106:80`, `http://www.patentum.at:80`
- **Recommendations:**
Implement HTTPS for all web traffic to ensure data is encrypted in transit. Utilize certificates from trusted Certificate Authorities and enable HTTP Strict Transport Security (HSTS) to enforce secure connections.

1.3.2 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for `www.patentum.at` is critically expired with **-92 days** remaining, indicating an immediate need for renewal to maintain secure communications.

Affected Assets:
- Domain: `www.patentum.at`

Recommendations:
Renew the SSL/TLS certificate immediately to restore secure communications. Implement a monitoring system to alert when certificates are nearing expiration to prevent future lapses.

1.3.3 Absence of WAF

Description:
The absence of a Web Application Firewall (WAF) was noted on **100%** of analyzed hosts, significantly increasing vulnerability to injection-based attacks and unauthorized data access.

Affected Assets:
- Host: `www.patentum.at`

Recommendations:
Deploy a Web Application Firewall to protect against common web application attacks such as SQL injection and cross-site scripting (XSS). Regularly update WAF rules to adapt to emerging threats.

1.3.4 Shared Hosting Environment Analysis

Description:
The domain `www.patentum.at` operates in a shared hosting environment with **58 shared domains**, categorized as medium interest due to potential security risks from shared infrastructure.

Affected Assets:
- Hostname: `www.patentum.at`

Recommendations:
Consider migrating to a dedicated hosting environment to reduce risk exposure from other tenants. If shared hosting must be used, ensure robust isolation measures are in place.

1.3.5 Nmap Port Scan Results Analysis

Description:
Port 80 (HTTP) was identified as potentially insecure due to lack of encryption on IP `78.136.38.106`. This exposes the service to risks associated with unencrypted traffic.

Affected Assets:
- IP: `78.136.38.106`

Recommendations:
Ensure all services running on port 80 are redirected to HTTPS or have HSTS enabled. Regularly audit open ports and services for compliance with security best practices.

1.3.6 Login Form Detection Analysis

Description:
A total of **4 login forms** were detected across various URLs, indicating potential authentication interfaces that require security validation.

Affected Assets:
- URLs: `https://www.patentum.at/documents/`, `http://78.136.38.106:443`, `http://www.patentum.at:443`
`https://www.patentum.at:443`, `https://78.136.38.106:443`

Recommendations:
Conduct thorough security assessments of all login forms to ensure they are protected against common vulnerabilities such as brute force attacks and credential stuffing. Implement multi-factor authentication where possible.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to implement comprehensive encryption practices, deploy a Web Application Firewall, and regularly monitor and renew SSL/TLS certificates. Additionally, consider transitioning to dedicated hosting environments where feasible and ensure all authentication interfaces are secured against common attack vectors. Regular security audits should be conducted to identify and mitigate emerging threats promptly.