1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **regeneron.fr**. The analysis commenced on **May 17th** at **21:45** and concluded after a duration of **11 minutes and 56 seconds**. The assessment was performed using a basic scan methodology. The scope of the work included evaluating the security posture of the web application and its associated infrastructure, focusing on identifying High and Medium-risk vulnerabilities.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **1 High-risk**, **4 Medium-risk**, and **13 informational**. The most critical finding is the use of deprecated TLS 1.0 and 1.1 protocols across **4 endpoints**, posing significant security risks due to vulnerabilities like the BEAST attack. Immediate remediation is advised to upgrade to TLS 1.2 or 1.3, which are currently acceptable and ideal standards, respectively. Medium-risk issues include shared hosting environments and potentially insecure open ports, such as HTTP on port **80** and **8080**, which require careful review to ensure encryption and security. Additionally, SSL certificate expiration is approaching for one domain, with **72 days** remaining, necessitating timely renewal to avoid service disruptions. These findings underscore the need for prioritized action to mitigate risks and enhance the security posture.

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	Medium

1.3.1 SSL/TLS Protocols Security Assessment

Description:
The assessment revealed that **4 endpoints** are using deprecated TLS 1.0 and 1.1 protocols. 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:
- **4 endpoints** with TLS 1.0 and 1.1 support.

Recommendations:
Immediate action is required to disable TLS 1.0 and 1.1 across all endpoints. It is recommended to upgrade to TLS 1.2 or ideally TLS 1.3 to ensure robust encryption standards are in place.

1.3.2 Shared Hosting Environment Analysis

Description:
The domain **regeneron.fr** is hosted in a shared environment with **66 other domains**, which can increase security risks due to shared resources and potential cross-domain vulnerabilities.

Affected Assets:
- Hostname: **regeneron.fr**

Recommendations:
Consider migrating to a dedicated hosting environment to minimize shared resource risks. Implement strict access controls and monitoring to detect any unauthorized activities.

1.3.3 Nmap Port Scan Results Analysis

Description:
The scan identified **4 open ports**, including potentially insecure ports such as HTTP on ports **80** and **8080**, which lack encryption and may expose the service to web vulnerabilities.
Affected Assets:
- IP Address: **172.64.151.253** - Open Ports: **80/tcp, 443/tcp, 8080/tcp, 8443/tcp**
Recommendations:
Ensure that HTTP services redirect to HTTPS or have HSTS enabled. Regularly review and secure services running on these ports to prevent exploitation.

1.3.4 SSL Certificate Expiration Analysis

Description:
The SSL certificate for the domain **regeneron.fr** is set to expire in **72 days**, categorized under the "Warning" risk level.
Affected Assets:
- Domain: **regeneron.fr**
Recommendations:
Plan for timely renewal of the SSL certificate to avoid service disruptions and maintain secure communications.

1.3.5 Login Form Detection Analysis

Description:
A total of **4 login forms** were detected across the application, indicating a medium interest level due to potential exposure of sensitive user credentials if not properly secured.
Affected Assets:
- URLs associated with detected login forms: - `http://172.64.151.253:80` - `http://172.64.151.253:8080` - `https://regeneron.fr/webruntime/framework/c50b36abe4/prod/lwr_app_bootstrap_hook` - `https://regeneron.fr:8443/webruntime/framework/c50b36abe4/prod/lwr_app_bootstrap_hook`
Recommendations:
Ensure all login forms are served over HTTPS to protect user credentials during transmission. Implement multi-factor authentication where possible to enhance security.

1.4 General Recommendations

To enhance the overall security posture, it is crucial to address High-risk vulnerabilities immediately and plan for Medium-risk issues promptly. Regularly update all systems and protocols to adhere to current security standards, conduct periodic security assessments, and implement robust monitoring solutions to detect and respond to threats in real-time.