1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **historystudycenter.com**. The analysis commenced on **March 17th** at **01:00** and concluded in **00h:11m:05s**. The assessment employed a basic scan type, focusing on identifying High and Medium-risk vulnerabilities within the web application and its infrastructure, following OWASP and OSCP methodologies.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **3 High-risk**, **2 Medium-risk**, and **13 informational**. Critical findings include the presence of deprecated and vulnerable SSL/TLS protocols (TLS 1.0 and 1.1) on **4 endpoints**, posing significant risks of exploitation. Additionally, a High-risk shared hosting environment was detected with over **621 domains** sharing the same IP, potentially impacting data integrity and confidentiality. The analysis also revealed **12 login forms**, indicating a high interest in authentication interfaces that require immediate security validation. Medium-risk issues include insecure open ports (**80** and **8080**) that could expose the system to web service vulnerabilities. Immediate remediation actions should focus on upgrading SSL/TLS protocols, securing shared hosting environments, and reinforcing authentication mechanisms to mitigate these risks effectively.

1.3 Key Security Issues

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

1.3.1 Shared Hosting Environment Analysis

Description:

A High-risk shared hosting environment was detected where **621 domains** share the same IP address. This configuration poses significant risks to data integrity and confidentiality due to potential cross-domain vulnerabilities.

Affected Assets:

- Hostname: **historystudycenter.com**

Recommendations:

- Transition to a dedicated hosting environment to isolate critical assets. - Implement strict access controls and monitoring to detect unauthorized activities. - Regularly audit shared hosting configurations for potential vulnerabilities.

1.3.2 SSL/TLS Protocols Security Assessment

Description:

Deprecated SSL/TLS protocols (TLS 1.0 and 1.1) were identified on **4 endpoints**, exposing them to known vulnerabilities such as the BEAST attack. These protocols are no longer considered secure by modern standards.

Affected Assets:
- Endpoints using TLS 1.0 and TLS 1.1: **4 endpoints**

Recommendations:
- Upgrade all systems to support TLS 1.2 or higher, ideally TLS 1.3. - Disable deprecated protocols in server configurations. - Conduct regular security assessments to ensure compliance with current cryptographic standards.

1.3.3 Login Form Detection Analysis

Description:
The presence of **12 login forms** across various URLs indicates potential security validation issues. These forms may be susceptible to attacks such as credential stuffing or brute force if not properly secured.

Affected Assets:
- URLs with detected login forms include multiple endpoints such as `http://historystudycenter.com:80` and `https://historystudycenter.com:8443`.

Recommendations:
- Implement multi-factor authentication (MFA) for all login interfaces. - Ensure all forms are protected with HTTPS to encrypt data in transit. - Regularly test login forms for vulnerabilities such as SQL injection or cross-site scripting (XSS).

1.3.4 Nmap Port Scan Results Analysis

Description:
Open ports **80** and **8080** were identified as potentially insecure due to lack of encryption and possible exposure to web service vulnerabilities.

Affected Assets:
- IP Address: **172.67.215.145** - Ports: **80/tcp, 8080/tcp**

Recommendations:
- Redirect HTTP traffic on port 80 to HTTPS to ensure encryption. - Evaluate the necessity of services running on port 8080 and secure them with appropriate access controls. - Regularly review open ports and services for potential vulnerabilities.

1.3.5 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for the domain “historystudycenter.com” is set to expire in **50 days**, categorized under “Warning” status, indicating that renewal planning should occur soon.

Affected Assets:
- Domain: **historystudycenter.com**

Recommendations:
- Initiate the renewal process for the SSL/TLS certificate well before expiration. - Implement automated monitoring tools to alert on upcoming certificate expirations. - Ensure all certificates are issued by trusted Certificate Authorities (CAs).

1.4 General Recommendation

To enhance the overall security posture, it is recommended that the organization adopts a proactive approach by implementing continuous monitoring, regular vulnerability assessments, and timely patch management. Additionally, fostering a culture of security awareness among employees will further mitigate risks associated with human factors.