1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **endnote.com**. The analysis commenced on **March 17th** at **00:00** and concluded in **23 minutes and 18 seconds**. The assessment was identified with the tracking ID **0477e07f700c** and was categorized as a "Basic" type scan. The evaluation focused on identifying High and Medium-risk vulnerabilities within the web application and its infrastructure, utilizing methodologies aligned with OWASP and OSCP standards.

1.2 Short Summary of Main Issues

The security assessment identified **4** High-risk, **2** Medium-risk, **1** Low-risk, and **13** informational issues. Critical findings include leaked email addresses and passwords on the deep web, posing significant risks of phishing and unauthorized access, and a shared hosting environment with over **31,000** domains, increasing exposure to potential attacks. Additionally, the detection of **8** login forms and a Denial of Service (DoS) vulnerability with a **12.24%** timeout rate on HTTPS services highlight severe vulnerabilities that could disrupt operations and compromise sensitive data. Immediate actions should focus on mitigating these high-risk issues to protect the organization's assets and reputation.

1.3 Key Security Issues

Title	Risk
Email Addresses and/or Passwords Leaked on...	High
Shared Hosting Environment Analysis	High
Login Form Detection Analysis	High
Denial of Service (DoS) Vulnerability Assess...	High
Nmap Port Scan Results Analysis	Medium
SSL Certificate Expiration Analysis	Medium

1.3.1 Email Addresses and/or Passwords Leaked on the Deep Web

Description

A total of **3** leaked credentials were identified, including email addresses and passwords, found on the deep web. This exposure poses critical security risks such as unauthorized access, phishing, social engineering, and further data breaches. The breach sources include multiple databases such as AntiPublic and BreachCompilation.

Affected Assets

- Email addresses: ezra@endnote.com

Recommendations

Immediate password resets for affected accounts are recommended. Implement multi-factor authentication (MFA) across all user accounts to enhance security. Conduct regular security awareness training to educate users about phishing risks.

1.3.2 Shared Hosting Environment Analysis

Description

The domain is hosted in a shared environment with over **31,795** domains, which significantly increases the risk of cross-site contamination and other security threats inherent in shared hosting setups.

Affected Assets
- Hostnames: endnote.com, www.endnote.com

Recommendations
Consider migrating to a dedicated hosting environment to reduce exposure to shared hosting risks. Regularly monitor for unusual activities that may indicate cross-site contamination.

1.3.3 Login Form Detection Analysis

Description
A total of **8** login forms were detected across various URLs, indicating potential security risks due to multiple authentication interfaces that may not be adequately secured.

Affected Assets
- URLs with detected login forms include: `https://endnote.com/apex/`, `http://endnote.com/case/:recordId/:recordName`, etc.

Recommendations
Ensure all login forms are secured using HTTPS. Implement rate limiting to prevent brute force attacks. Regularly test login forms for vulnerabilities such as SQL injection or cross-site scripting (XSS).

1.3.4 Denial of Service (DoS) Vulnerability Assessment

Description
A DoS vulnerability was identified with a **12.24%** timeout rate on HTTPS services, indicating a high severity level that could lead to service disruptions.

Affected Assets
- Service Ports: **80** (HTTP), **443** (HTTPS)

Recommendations
Enhance server capacity and optimize configurations to handle peak loads efficiently. Implement network traffic monitoring to detect and mitigate potential DoS attacks promptly.

1.3.5 Nmap Port Scan Results Analysis

Description
The scan revealed **4** open ports, including port **80** (HTTP), which is potentially insecure due to lack of encryption.

Affected Assets
- IP: **23.185.0.4**

Recommendations
Ensure HTTP traffic is redirected to HTTPS. Enable HSTS to enforce secure connections. Regularly review open ports and services for unnecessary exposure.

1.3.6 SSL Certificate Expiration Analysis

Description
SSL certificates for both domains are set to expire in **31** days, categorized under the “Warning” risk level.

Affected Assets
- Domains: endnote.com, www.endnote.com

Recommendations
Plan for immediate renewal of SSL certificates to avoid service disruptions and maintain secure communications.

1.4 General Recommendations

To enhance overall security posture, it is recommended to implement a comprehensive vulnerability management program that includes regular security assessments, timely patch management, and continuous monitoring of network activities. Additionally, fostering a culture of security awareness among employees will help mitigate risks associated with human factors.