# 1 Executive Security Assessment Report

## 1.1 Introduction

The security assessment was conducted on the domain **wc3-cert.fiservapps.com**. The analysis was initiated on **April 1st** at **03:00** and concluded in **00h:09m:57s**. The assessment type was categorized as “Basic”. The evaluation focused on identifying High and Medium-risk vulnerabilities within the web application and infrastructure, utilizing methodologies aligned with OWASP and OSCP standards.

## 1.2 Short Summary of Main Issues

The security assessment identified a total of **20** issues, categorized as **1** High-risk, **4** Medium-risk, **2** Low-risk, and **13** informational. The most critical finding is a Denial of Service (DoS) vulnerability, posing a High risk due to potential service disruptions, with a **0.573%** timeout rate on HTTPS services. Medium-risk issues include the absence of a Web Application Firewall (WAF) on **100%** of analyzed hosts, increasing susceptibility to injection attacks, and SSL certificate expiration within **77** days, necessitating prompt renewal. Additionally, three login forms were detected, requiring security validation to prevent unauthorized access. Immediate actions should focus on mitigating the DoS vulnerability, implementing WAF protection, and addressing SSL certificate renewals to enhance security posture.

## 1.3 Key Security Issues

| Title | Risk |
|---|---|
| Denial of Service (DoS) Assessment | High |
| Absence of WAF | Medium |
| SSL Certificate Expiration Analysis | Medium |
| Nmap Port Scan Results Analysis | Medium |
| Login Form Detection Analysis | Medium |
| Usage of ASP Technology Detected | Low |
| SSL/TLS Protocols Security Assessment | Low |

### 1.3.1 Denial of Service (DoS) Assessment

**Description**

A Denial of Service (DoS) vulnerability was identified, with a **0.573%** timeout rate on HTTPS services. This issue poses a High risk due to potential service disruptions that can affect availability and performance.

**Affected Assets:**

Service ports: **80** (HTTP) and **443** (HTTPS)

**Recommendations:**

- Implement rate limiting and traffic analysis to detect and mitigate DoS attacks. - Optimize server configurations to handle high traffic loads efficiently. - Regularly monitor server performance and response times.

### 1.3.2 Absence of WAF

**Description:**

The absence of a Web Application Firewall (WAF) was noted on **100%** of the analyzed hosts, significantly elevating the risk of successful cyber-attacks, particularly injection-based attacks.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING

**Affected Assets:**
- Host: wc3-cert.fiservapps.com

**Recommendations:**
- Deploy a robust WAF solution to protect against common web application attacks. - Regularly update WAF rules to adapt to emerging threats. - Conduct periodic security assessments to ensure WAF effectiveness.

### 1.3.3 SSL Certificate Expiration Analysis

**Description:**
The SSL certificate for the domain wc3-cert.fiservapps.com is set to expire in **77** days, categorized under the “Warning” risk level, indicating that renewal planning should occur soon.

**Affected Assets:**
- Domain: wc3-cert.fiservapps.com

**Recommendations:**
- Initiate the renewal process for the SSL certificate well before expiration. - Implement automated monitoring for certificate expiration alerts. - Consider using certificates with longer validity periods where appropriate.

### 1.3.4 Nmap Port Scan Results Analysis

**Description:**
Open ports were detected, including port **80** associated with HTTP service, which poses a risk due to lack of encryption. Verification of HTTPS redirection or HSTS implementation is advised.

**Affected Assets:**
- IP: 176.100.165.213 - Ports: **80/tcp** (http), **443/tcp** (ssl/https)

**Recommendations:**
- Ensure all HTTP traffic is redirected to HTTPS. - Implement HSTS to enforce secure connections. - Regularly scan for open ports and close unnecessary ones.

### 1.3.5 Login Form Detection Analysis

**Description:**
Three login forms were detected across the application, requiring security validation to prevent unauthorized access.

**Affected Assets:**
- URLs: - `https://wc3-cert.fiservapps.com:443` - `https://wc3-cert.fiservapps.com/cv/Login.aspx?ac=x&isClassic=True` - `https://wc3-cert.fiservapps.com/CV/setSession.ashx`

**Recommendations:**
- Implement multi-factor authentication for login forms. - Conduct regular security testing on login mechanisms. - Ensure secure transmission of credentials using HTTPS.

## 1.4 General Recommendation

To enhance the overall security posture, it is recommended to prioritize addressing High-risk vulnerabilities immediately while planning for Medium-risk issues. Regular security assessments and updates to security controls should be conducted to adapt to evolving threats. Implementing comprehensive monitoring and alerting systems will aid in early detection and mitigation of potential security incidents.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING