1 Executive Security Assessment Report

1.1 Introduction

This report presents the findings from a comprehensive security assessment conducted on the domain **iqabotw.ft1.cashedge.com**. The analysis was initiated on **June 18th at 06:45** and concluded in **00h:11m:47s**. The assessment was performed using a **Basic** scan type. The evaluation focused on identifying High and Medium-risk issues that could impact the security posture of the domain.

1.2 Summary of Findings

The security assessment identified a total of **19** issues, categorized as **1** High-risk, **1** Medium-risk, **3** Low-risk, and **14** informational. The most critical finding is the expired SSL certificate, which is overdue by **303** days, posing a significant risk to secure communications and potentially impacting customer trust and compliance. Additionally, the Medium-risk issue involves sensitive subdomain naming, which could expose administrative interfaces to unauthorized access. Low-risk findings include the use of PHP technology, which is prone to vulnerabilities, and a minor DoS vulnerability with a **0.09%** timeout rate. Immediate action is recommended to renew the SSL certificate and review subdomain security to mitigate potential exploitation.

1.3 Key Security Issues

Title	Risk
SSL Certificate Expiration	High
Subdomain Naming Security	Medium
Usage of PHP Technology	Low
SSL/TLS Protocol Security	Low
Denial of Service (DoS) Vulnerability	Low

1.3.1 SSL Certificate Expiration Analysis

Description:
The SSL/TLS certificate for the domain **iqabotw.ft1.cashedge.com** is critically overdue by **303** days, indicating an immediate need for renewal. This lapse poses a significant threat to secure communications and can undermine customer trust and compliance with industry standards.

Affected Assets:
- Domain: **iqabotw.ft1.cashedge.com**

Recommendations:
- Renew the SSL certificate immediately to restore secure communications. - Implement a monitoring system to track certificate expiration dates and ensure timely renewals in the future.

1.3.2 Subdomain Naming Security Assessment

Description:
A sensitive subdomain, **iqabotw.ft1.cashedge.com**, associated with development or staging environments, was detected. Such environments may contain unpatched vulnerabilities or debug information, potentially exposing critical systems and sensitive data to unauthorized access.

Affected Assets:
- Subdomain: **iqabotw.ft1.cashedge.com**

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING

Recommendations:
- Review and secure all development and staging environments. - Implement access controls and ensure that sensitive subdomains are not publicly accessible. - Regularly audit subdomain configurations for security compliance.

1.4 General Recommendations

To enhance the overall security posture, it is recommended to:

- Implement a robust certificate management process to prevent future SSL/TLS expiration issues.
- Conduct regular security audits and vulnerability assessments on all subdomains and associated environments.
- Strengthen access controls and ensure that sensitive environments are isolated from public access.
- Continuously monitor for emerging threats and update security protocols accordingly.

By addressing these critical and Medium-risk issues, the organization can significantly improve its security defenses and protect against potential exploitation.

PUBLIC REPORT - DEMO SCAN - NO INTRUSIVE TESTING