Diagram

Description automatically generated with low confidence

WEB APPLICATION

PENETRATION TESTING

REPORT

for

tigertek.org.uk

Prepared by:

Fatima Al-Soqatri

Words count: 604 [Appendices excluded]

February 13, 2023

Executive Summary

This report presents the results of the Black Box penetration testing for the *tigertek.org.uk* web site and external network infrastructure. The recommendations provided in this report are structured to facilitate remediation of the identified security risks. This document serves as a formal letter of attestation for the recent *tigertek.org.uk* web application and external network infrastructure penetration testing.

Evaluation ratings compare information gathered during the engagement to “best in class” criteria for security standards. We believe that the statements made in this document provide an accurate assessment of the *tigertek.org.uk* current security as it relates to the *tigertek.org.uk* data.

We highly recommend reviewing the Summary section of business risks and High-Level Recommendations to better understand risks and discovered security issues.(Appendix B)

Scope of assessment Web Application

Security Level **F**

Grade Inadequate

Assignment Objectives

Our primary goal within this project was to provide the *tigertek.org.uk* with an understanding of the current level of security in the web application and its infrastructure components. We completed the following objectives to accomplish this goal:

● Identifying application-based threats to and vulnerabilities in the application

● Comparing *tigertek.org.uk* current security measures with industry best practices

● Providing recommendations that *tigertek.org.uk* can implement to mitigate threats and vulnerabilities and meet industry best practices

Technical Details

2.2 Security tools used.

● Manual testing: Burp Suite Pro [Commercial Edition]

● Vulnerability scan: Nessus, OpenVAS, Nikto, arachni

● Network scan: Nmap, masscan

● Directory enumeration: gobuster, dirsearch

Summary of Findings

1. Hostnames and IP-addresses

|  |  |
| --- | --- |
| **Scope:** | **Description:** |
| [IP\_ADDRESS] | 68.66.247.187 |
| [DOMAINS] | tigertek.org.uk |

1. Port scan results

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Port number** | **State** | **Service name** | **Service product** | **Service info** |
| 21 | Open | ftp | Pure-FTPd |  |
| 22 | Closed | ssh |  |  |
| 25 | Open | smtp | Exim smtpd  4.95 |  |
| 53 | Open | domain | ISC BIND  9.11.4-P2 | RedHat Enterprise Linux 7 |
| 80 | Open | http | Apache httpd | W3 Total Cache/0.9.4.6.4 |
| 88 | Closed | kerberos-sec |  |  |
| 110 | Open | pop3 | Dovecot pop3d |  |
| 143 | Open | imap | Dovecot imapd |  |
| 443 | Open | https | Apache httpd | W3 Total Cache/0.9.4.6.4 |
| 445 | Closed | microsoft-ds |  |  |
| 587 | Open | smtp | Exim smtpd  4.95 | 587 |
| 993 | Open | imap | Dovecot imapd | 993 |
| 995 | Open | pop3 | Dovecot pop3d | 995 |
| 3306 | Open | mysql | MySQL 5.5.5-10.3.36-MariaDB-cll-lve | 3306 |
| 5432 | Open | postgresql | PostgreSQL DB 9.6.0 or later | 5432 |

1. Subdomains

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Hostname | Ip address | Server | Technology | Web platform |
| tigertek.org.uk | 68.66.247.187 |  | Apache | PHP 7.4.33 |
| mail.tigertek.org.uk | 68.66.247.187 |  | Apache | PHP 7.4.33 |
| autodiscover.tigertek.org.uk | 68.66.247.187 |  | Apache |  |
| ftp.tigertek.org.uk | 68.66.247.187 |  | Apache | PHP |
| webmail.tigertek.org.uk | 68.66.247.187 |  | Apache |  |
| cpanel.tigertek.org.uk | 68.66.247.187 |  | Apache |  |
| www.tigertek.org.uk | 68.66.247.187 |  | Apache | PHP 7.4.33 |
| autoconfig.tigertek.org.uk | 68.66.247.187 |  | Apache |  |

1. Vulnerabilities

Our assessment of the tigertek.org.uk web application revealed the following vulnerabilities:

|  |  |
| --- | --- |
| Vulnerability | Criticality |
|  | High |
| This header can hint to the user agent to protect against some forms of XSS | Medium |
| The site uses SSL and the Strict-Transport-Security HTTP header is not defined. | Medium |
| The site uses SSL and Expect-CT header is not present. | Medium |
| This could allow the user agent to render the content of the site in a different fashion to the MIME type | Medium |

Recommendations

Taking into consideration all issues that have been discovered, we highly recommend to:

* Use an access control matrix to define the access control rules for application users.
* Requests that modify data should be validated through the CSRF token to avoid possible Cross-Site Request Forgery attacks.
* Implement strict access control checks.
* Implement a protection mechanism for the login process. You could use a user lockout mechanism to prevent external actors from guessing users’ passwords.
* Continuously monitor logs for anomalies to detect abnormal behavior and fraud transactions.
* Review security configuration of all additional modules, like text editors.
* Avoid transmitting sensitive data (tokens, etc.) inside the URL of a request.
* Review 2FA configuration on app demo version.
* form a whitelist of permitted domains, and this will reduce your exposure to Host header injection attacks.

Appendix A

**Assessment Methodology**

This Penetration Testing Methodology is grounded on the following guides and standards:

● Penetration Testing Execution Standard (PTES)

● OWASP Top 10 Application Security Risks

● OWASP Web Security Testing Guide

● Open Source Security Testing Methodology Manual (OSSTMM)

**Penetration Testing Execution Standard (PTES)** consists of seven main sections which start from the initial communication and reasoning behind a pentest, through intelligence gathering and threat modeling phases where testers are working behind the scenes to get a better understanding of the tested organization, through vulnerability research, exploitation and post-exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process.

**Open Web Application Security Project (OWASP)** is an industry initiative for web application security. OWASP has identified the 10 most common attacks that succeed against web applications. Besides, OWASP has created Application Security Verification Standard (ASVS) which helps to identify threats, provides a basis for testing web application technical security controls, and can be used to establish a level of confidence in the security of Web applications.

**The Open Source Security Testing Methodology Manual (OSSTMM)** is peer-reviewed and maintained by the Institute for Security and Open Methodologies (ISECOM). It has been primarily developed as a security auditing methodology assessing against regulatory and industry requirements. It is not meant to be used as a standalone methodology but rather to serve as a basis for developing one which is tailored towards the required regulations and frameworks.

Appendix B

Grading Criteria:

|  |  |  |
| --- | --- | --- |
| Grade | Security | Criteria Description |
| **A** | Excellent | The security exceeds “Industry Best Practice” standards. The overall posture was found to be excellent with only a few low-risk findings identified. |
| **B** | Good | The security meets accepted standards for “Industry Best Practice.” The overall posture was found to be strong with only a handful of medium- and low-risk shortcomings identified. |
| **C** | Fair | Current solutions protect some areas of the enterprise from security issues. Moderate changes are required to elevate the discussed areas to “Industry Best Practice” standards |
| **D** | Poor | Significant security deficiencies exist. Immediate attention should be given to the discussed issues to address the exposures identified. Major changes are required to elevate to “Industry Best Practice” standards. |
| **F** | Inadequate | Serious security deficiencies exist. Shortcomings were identified throughout most or even all of the security controls examined. Improving security will require a major allocation of resources. |