Cyber Security Assessment

A cyber security assessment is a comprehensive evaluation and analysis of an organization's information systems, networks, applications, and overall security posture. The primary objective of this assessment is to identify vulnerabilities, weaknesses, and potential threats that could compromise the confidentiality, integrity, or availability of critical assets and data.

Table of Contents

Scope of Test

The security testing was performed utilizing the vulnerable approach which included:

- Web application vulnerability testing
- Web application penetration testing

The penetration test was performed utilizing the grey box test approach which included:

- Network penetration testing

The following components were in scope of the assessment:

Sr. No	Asset	Domain/FQDN/IP/Subnet
1	Weightworld	www.weightworld.uk

Tools Utilized

We uses a suite of tools during the execution of a security/Functional review. These include in-house developed, commercial and best of breed open-source tools. This avoids reliance on any one class of tool and ensures that results are verified and cross referenced whilst minimizing false positives and negatives. Some of the tools used include (not an exhaustive list):

CLASS OF TOOL	TOOLS USED
Port Scanning / Network Mapping	Nmap
Vulnerability Scanners	Nessus
Penetration Testing Suite	OWASP ZAP Proxy
Info gathering	Whatweb, whois, Harvester
Bruteforce attack	Hydra and Burpsuite

Out of Scope

Due care was taken in order not to damage any property of Weightworld, not to have an impact on live systems or to interfere with the company's daily business. Specifically, the following approaches were not in scope of the assessment, however, situations that would allow such proceedings would have been documented:

- Denial of Service attacks
- Tampering with information integrity

- Email spoofing
- Database attack
- XSS scripting
- Enumeration
- Packet sniffing

Summary

This report reflects the results of the functional (Black box), Penetration (Grey box) and vulnerable test of selected components of Weightworld as highlighted in the scope of test, owned or utilized by Weightworld that are part of the production environment.

Most security controls were tested utilizing a set of automated tools combined with targeted manual tests following a standardized approach. Identified security issues were reviewed to eliminate false positives, prioritized according to business risk, and measures for their remediation have been proposed. The results of the assessment led to the overall impression that the security posture of the environment can be significantly improved. During this testing and the observations that were identified thereafter, multiple critical attack paths were identified and exploited. The overall risk score of the applications in scope was identified as HIGH. Below is a high-level summary of the issues that were identified during the assessment:

1. **Outdated PHP version/PII disclosure -** Currently we are using 7.3 version of PHP which is outdated due to older version some issue generated like:

- **Security Vulnerabilities**
- **Compatibility Issues**
- **Performance Improvements**
- **Lack of Official Support**
- **Maintenance Challenges**
- **Elevated Business Risks**
- **Issues with Third-Party Libraries**

2. Vulnerabilities and Functional issues were identified leading to:

- **Version Disclosures**
- **Exploitable system**
- **Data leakage**

These observations are further detailed in the later section of this document.

Objective

The aim of the assessment was to provide an independent and reliable opinion on the security of application and infrastructure components. The assessment should identify Functional issues, weaknesses, vulnerabilities and quantify their severity so they can be managed, addressed, and therefore help reduce the overall risk to the application.

Success Criteria

The intent of the functional and penetration test was to simulate a real-world attack situation with a goal of identifying how far an attacker may be able to penetrate the environment and able to break the functionality.

Reporting

The client is regularly informed about status and progress of the assessment work. This regular status update consists of a summary of the overall progress and information about any issues interfering with the achievement of the assessment objective. In the case of imminent danger, the client is informed without delay so as to prevent damage. The results of the assessment are documented and delivered in the form of an assessment report. The assessment report contains an executive summary, outlining overall risk posture of the environment as well as key findings, a summary of the environment in scope, a description of the assessment methodology and the assessment work conducted and a detailed list of findings and recommendations.

Overall Security Observations

Info gathered：

Data validation	Nominet was able to match the registrant's name and address against a 3rd party data source on 06-Aug-2019
Registrar	EuroDNS SA [Tag = EURODNS], URL
Relevant dates	Registered on: 20-Aug-2014
	Expiry date: 20-Aug-2024
	Last updated: 31-Jul-2023

Registration status	Registered until expiry date
Name servers	nina.ns.cloudflare.com
	zod.ns.cloudflare.com
ASNS found	AS13335
Interesting URLs found	https://www.weightworld.uk/
Emails found	info@weightworld.uk
Hosts found	1. *.weightworld.uk
	2. m.weightworld.uk
	3. m.weightworld.uk:35.187.176.202
IPs found	1. 104.199.76.114
	2. 104.26.12.219
	3. 104.26.13.219
	4. 172.66.40.216
	5. 172.66.43.40
	6. 172.67.68.191
	7. 23.227.38.65
	8. 2606:4700:3108::ac42:2b41
	9. 2606:4700:3108::ac42:2bad
	10. 35.187.176.202
IP: 172.66.40.216	**Country:** RESERVED, ZZ
Summary	This IP is associated with the weightworld.uk domain. It utilizes HTML5, is served via a cloudflare HTTP server, contains scripts, includes uncommon HTTP headers such as referrer-policy and cf-ray, and employs X-Frame-Options with the value of SAMEORIGIN. Additionally, it specifies IE=Edge compatibility in the X-UA-Compatible header.
Detected Plugins	- HTML5: HTML version 5 is detected.
	- HTTPServer: The HTTP server header indicates cloudflare.
	- Script: Scripts are detected.
	- UncommonHeaders: Uncommon HTTP headers like referrer-policy and cf-ray are detected.
	- X-Frame-Options: The X-Frame-Options header is set to SAMEORIGIN.
	- X-UA-Compatible: The X-UA-Compatible header specifies IE=Edge compatibility.

HTTP Headers	- HTTP/1.1 403 Forbidden
	- Date: Fri, 09 Feb 2024 05:15:49 GMT
	- Content-Type: text/html; charset=UTF-8
	- Transfer-Encoding: chunked
	- Connection: close
	- X-Frame-Options: SAMEORIGIN
	- Referrer-Policy: same-origin
	- Cache-Control: private, max-age=0, no-store, no-cache, must-revalidate, post-check=0, pre-check=0
	- Expires: Thu, 01 Jan 1970 00:00:01 GMT
	- Vary: Accept-Encoding
	- Server: cloudflare
	- CF-RAY: 8529a3006ac3856b-BOM
	- Content-Encoding: gzip

SECURITY OBSERVATIONS	SEVERITY
Outdated Version of PHP	Critical
PII disclosure	High
Absence of Anti-CSRF Tokens	Medium
Content Security Policy (CSP) Header Not Set	Medium
Big Redirect Detected (Potential Sensitive Information Leak)	Low
Cookie No HttpOnly Flag	Low
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low
Cookie without SameSite Attribute	Low

Critical Risk Findings

SECURITY OBSERVATIONS	EFFORT TO FIX
Outdated Version of PHP	Critical

Synopsis

The remote host contains an unsupported version of a web application scripting language

Description

According to its version, the installation of PHP on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.

Corrective Control

Upgrade to a version of PHP that is currently supported.

Currently we are working with the older PHP version so we can fix this issue by upgrading the PHP version in latest version so that it supports the website.

- Identify Current PHP Version
- Check PHP Release Life-cycle
- Review Change-log and Backward Compatibility
- Backup Your Web Application:
- Update Server Software
- Test Locally
- Update PHP
- Modify Configuration

```
Source              : X-Powered-By: PHP/7.3.31
Installed version   : 7.3.31
End of support date : 2021/12/06
Announcement        : http://php.net/supported-versions.php
Supported versions  : 8.0.x / 8.1.x
```

References

http://php.net/eol.php
https://wiki.php.net/rfc/releaseprocess

High Risk Findings

SECURITY OBSERVATIONS	EFFORT TO FIX
PII disclosure	High

Synopsis

The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

Description

This synopsis highlights a critical issue regarding the inclusion of sensitive Personally Identifiable Information (PII) within the response. PII refers to any data that can be used to identify a specific individual, and its disclosure poses significant privacy and security risks. In this case, the response contains highly sensitive PII such as credit card numbers (CC) and social security numbers (SSN), which are commonly targeted by identity thieves and cyber criminals for fraudulent activities. The presence of such information demands immediate attention to ensure its proper handling and protection to prevent unauthorized access or misuse.
URL - https://www.weightworld.uk/muscle-toners.html

Corrective Control

Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

References

N/A

Medium Risk Findings

SECURITY OBSERVATIONS	EFFORT TO FIX
Absence of Anti-CSRF Tokens	Medium

Synopsis

CSRF token is missing.

Description

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

- The victim has an active session on the target site.
- The victim is authenticated via HTTP auth on the target site.
- The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

Corrective Control

Phase: Architecture and Design

Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation

Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design

Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).

Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.

Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.

This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation

Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

References

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

https://cwe.mitre.org/data/definitions/352.html

SECURITY OBSERVATIONS	EFFORT TO FIX
Content Security Policy (CSP) Header Not Set	Medium

Synopsis

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross-Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft, to site defacement, to malware distribution

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

Corrective Control

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.

References

https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy

https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html

https://www.w3.org/TR/CSP/