Free Web Application Vulnerability Scan Report

Document Publication Details	
Client	
Penetration Testing Date	6 Nov 2021
Release Date	7 Nov 2021
Classification	CONFIDENTIAL – Not to be disclosed without prior written agreement from Pentestco.

© Pentestco
info@pentestco.com
D07-R924, Dublin, Ireland

CONTENT

1. Executive Summary

1.1. Summary

This is a **FREE** vulnerability scan report which details the results of the web application penetration test carried out by *Pentestco* for and conducted 6 Nov 2021 .A vulnerability scan report is not a penetration testing report. It shows number of security vulnerabilities classified by risk level to give an idea about what is the security level of the scanned web application.

A completed penetration testing report will provide all details about the security findings: description, recommended solution, business impact, attack complexity, precise information to understand what is the vulnerability and how to ammend it and much more.

The following table outlines the breakdown of all findings identified during the assessment and the overall rating given by *Pentestco* based on all findings (threat agents, attack vectors, priority), security weakness and technical and business impacts:

Host	High	Med	Low	Overall Rating
https://enamellearning.co.uk	1	1	7	HIGH

1.2. Objectives

The objective of the engagement was to provide with the following:

- An independent **free** assessment of current strengths and weaknesses of the web application and it's underlying infrastructure.
- Highlight and prioritize any security risks to the organization.
- Compare current security posture with established best practice.

1.3. Conclusion

Based on the results, a total of **1 high, 1 medium and 7 low priority** findings have been identified and *Pentestco* can conclude that there is scope for improvement in a number of areas of the application.

From the findings identified, it may be possible for an attacker or malicious user to perform actions which could damage business activities.

At this stage, it is important for to request a penetration testing report in order to fully identify all findings, implement recommended solutions and if necessary perform another web application penetration test to ensure all risks are reduced to an acceptable level.

1.4. Scope

The scope of the engagement consisted of the following IP address/URL.

- https://enamellearning.co.uk

1.5. Constraints

The methodology used to conduct this vulnerability scan is a two steps process:

- Perform a vulnerability assessment of the server hosting the application.
- Perform a web application penetration test of the application.
- Analyze, interpret, document and present those findings. **Only available on the payment report**

Pentestco uses the OWASP Top 10 as the basis for its web application security testing. The methodology used to test the web application is documented in Appendix B of this report.

2. Overview of Findings: Vulnerability Assessment

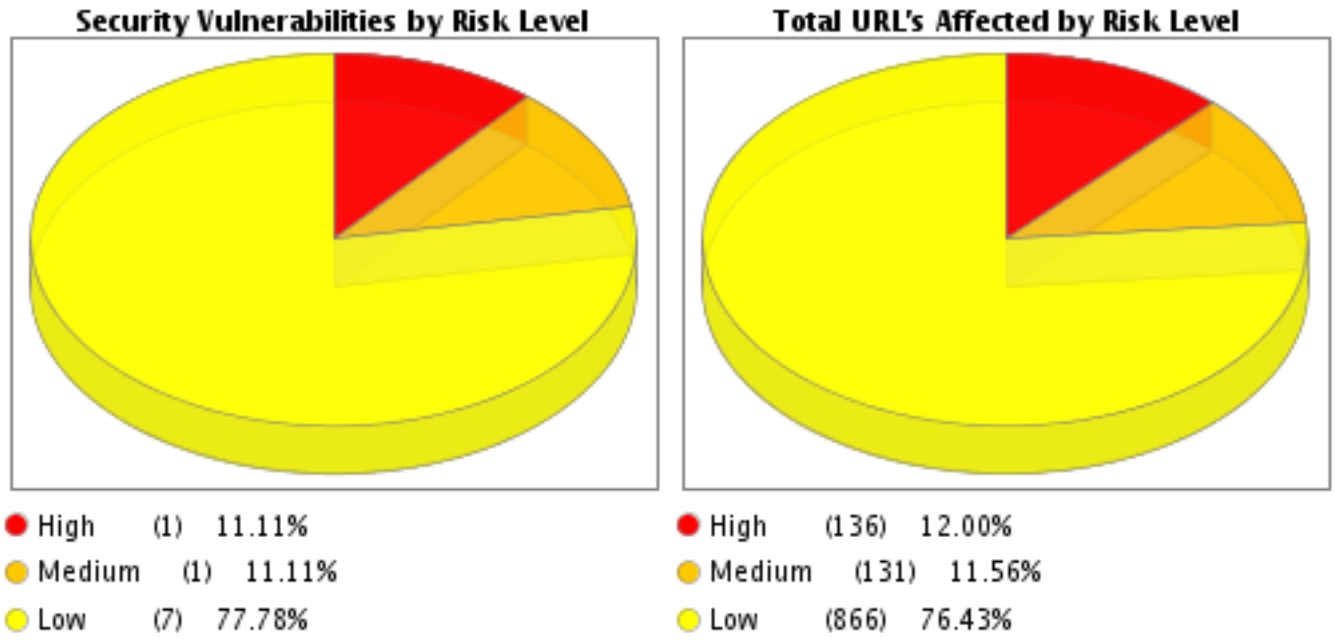
The following section contains a host status table indicating the state of each application and a table with a short description of the vulnerabilities identified, per app. The priority of each vulnerability is determined by the business impact of the resulting exposure if the attack was successful, and the likelihood of the attack taking place is based on attack complexity.

See Appendix B for additional details on how findings are classified.

2.1 Host https://enamellearning.co.uk

2.1.1 Risk Summary

Host	Port	SSL	High	Med	Low	Overall Rating
https://enamellearning.co.uk	443	yes	1	1	7	HIGH
Total URL's affected by risk level			136	131	866	



2.1.2. Summary of Findings

Only available on the payment report

3. Detailed Findings and Recommendations

3.1 Host https://enamellearning.co.uk

Only available on the payment report

4. Recommended Next Steps

4.1 Host https://enamellearning.co.uk

Only available on the payment report

4.2 SDLC Phases

Pentestco advocates the Secure Software Development Lifecycle (SDLC) approach to application security. The following table documents the phases of a typical SDLC and the security activities that can be conducted at various stages by an organisation

Phase	SDLC	Security Activities
1 & 2	Requirements & Design	Establish baseline Security Requirements Conduct Threat Modelling
3	Implementation	Static Code Analysis Penetration Testing
4	Testing	Dynamic Code Analysis Manual Penetration Testing
5	Deployment / Maintenance	Server Hardening Vulnerability Assessment Logging and Monitoring

There are further security activities that can be conducted throughout the development process to develop a more secure and robust application. *Pentestco* would recommends that review their current development process and integrate additional security activities where possible.

Apendix A: Classification of Findings

Impact	Description
Arbitrary code execution	Results in the ability to execute any commands of the attacker's choice on a target machine or in a target process
Denial of service	Results in the temporary or permanent loss of availability of a computer system, system component or data
Privilege escalation	Results in an attacker gaining elevated access to resources that are normally protected from an application or user
Unauthorised access	Results in an attacker gaining access to data, applications or systems without consent, usually by circumventing any authorisation mechanism that may be in place
Data manipulation	Used when data can be tampered with without necessarily obtaining access to a system or an application
Security bypass	Used when a security control can be circumvented without necessarily obtaining access to a system or an application
Sensitive information exposure	Used when potentially sensitive documents, confidential data or credentials are revealed
System information exposure	Used when excessive system information about the system, application or process is revealed
Unknown	Used when the impact is not known due to insufficient information from the vendor, researchers and the security community

Attack Complexity	Description
High	**Specialised access conditions exist.** In most configurations, the attacking party must already have elevated privileges or spoof additional systems in addition to the attacking system. The attack depends on social engineering methods that would be easily detected by people. The vulnerable configuration is seen very rarely in practice.
Medium	**The access conditions are somewhat specialised.** The attacking party is limited to a group of systems or users at some level of authorisation. Some information must be gathered before a successful attack can be launched. The affected configuration is non-default, and is not commonly configured. The attack requires an amount of social engineering that might occasionally fool cautious users.
Low	**Specialized access conditions or extenuating circumstances do not exist.** The affected product typically requires access to a wide range of systems and users, possibly anonymous and untrusted (e.g., Internet-facing web or mail server). The affected configuration is default or ubiquitous. The attack can be performed manually and requires little skill or additional information gathering.

Solution Status	Description
Vendor patch	A patch is available from the vendor of the vulnerable application or system component
Temporary fix	Used when a patch is being developed but is not yet available and compensating measures can be implemented to circumvent the vulnerability
System configuration	Used when modifying a system configuration setting will compensate or eliminate the issue
Application configuration	Used when modifying an application configuration setting will compensate or eliminate the issue
Manual fix	Used when a manual action is required to fix the issue, such as removing a file, restarting a process or disabling a service
No solution	Used when no patch is available and no compensating measure can currently be implemented to avoid the issue

Priority	Description
HIGH	Significant financial impact, or significant impact on the organisation's strategy or operational activities Extended loss of key systems or cause significant disruption of service to customers Give rise to reputational damage Significant stakeholder concern
MEDIUM	Moderate financial impact, or moderate impact on the organisation's strategy or operational activities Limited loss of key systems, extended loss of a non-key system or poor service to customers group Require a plan of action to resolve Moderate stakeholder concern
LOW	No financial impact Result in low impact on the organisation's strategy or operational activities No reputational damage Low stakeholder concern
INFO	No financial impact Informational items that do not directly relate to security risks Items that may potentially be used to conduct further attacks against the environment under review Automatically gathered information that should be reviewed

Apendix B: Web Application Penetration Test Methodology