

WEB APPLICATION PENTEST EXECUTIVE SUMMARY

Team 1: Alice Villar, Ian Wolloff, Aidan Curley

TABLE OF CONTENTS

1. Introduction	1
2. Testing Methodology	1
3. Modelling Methodology	1
4. Summary of findings	2
4.1. Information gathering stage	2
4.1.1. Port scanning using Nmap	2
4.1.2. Identified Technologies	3
4.1.3. Subdomain enumeration	3
4.1.4. Looking for sensitive files	4
4.1.5. SQL injection attack experiment	5
4.2. Security vulnerabilities	9
4.2.1. High/medium risk vulnerabilities found	9
4.2.2. Low/informational vulnerabilities found	9
5. Security standard analysis & GDPR compliance	9
5.1. GDPR - personal data	9
5.2 GDPR Controls	10
5.3 GDPR Compliance Tests	10
5.4 GDPR Compliance Tests Details	11
5.4.1. Privacy Policy	11
5.4.2. Website Security	12
5.4.3. Transport Layer Security Encryption	13
5.4.4. Cookie Protection	13
5.4.5. Cookie Disclaimer	13
5.2 WCAG Web Accessibility & Compliance Issues	13
5.3 PCI DSS Compliance Tests	14
6. Pentest Timeline	14
7. Conclusion	15
REFERENCES	15
APPENDIX	16

1. Introduction

A black box security test was conducted on Daedalus-Systems website.. This report details the methodology followed, its limitations, the GDPR requirements for the business, a brief analysis of the vulnerabilities found and a summary of recommendations. We detail the security standards (including the GDPR compliance) and present recommendations for full compliance. Figure 1 details Daedalus-Systems Web Application Penetration Testing.

Business name	Daedalus Systems
Domain	Technology and Electronic ecommerce website
Type of Penetration Testing	External Penetration Testing
Platform	https://www.daedalus-systems.co.uk/
Technique	Web Application Penetration Testing (WAPT)
Scope	Black Box
Testing Methodology	Combination of PTES Penetration Testing Execution Standard and OWASP Web testing framework
Modeling Methodology	STRIDE, DREAD
Version	Executive Summary

Fig 1. WPT Description

2. Testing Methodology

Our security testing methodology combines PTES (Penetration Testing Execution Standard) and the OWASP Web testing framework. PTES provides a structured approach to penetration testing, detailing a seven phase procedure (PTES, 2014). We used a combination of manual and automatic testing as both approaches have their benefits (Stefinko, 2016).

3. Modelling Methodology

We followed the Microsoft Threat Modelling Process to identify and list potential threats, security vulnerabilities and inappropriate defence mechanisms. This process has six steps, as shown in Figure 2.

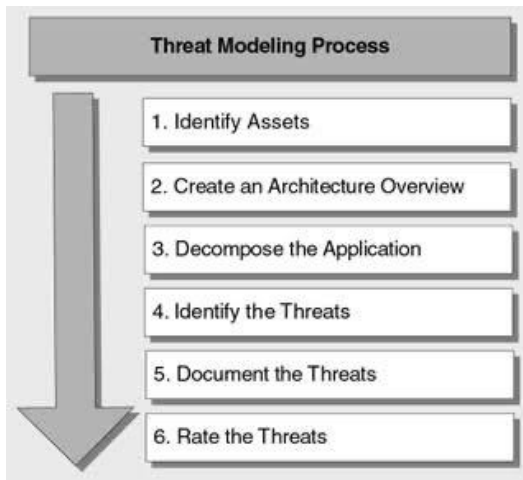


Fig 2. Threat Modelling Process, sourced from Microsoft Docs (2022)

Here is how we did the threat modelling on the targeted application:

- **Step 1:** In the case of Daedalus, the personal data of the clients in the business database is the most valued asset.
- **Step 2:** The technologies required for the application are detailed in Section 4.1.2 (Server software and technology found)
- **Step 3:** The methods to consume the digital asset are documented in Section 4.1.3, where we present all the subdomains of the targeted website.
- **Step 4:** The vulnerabilities we found are in Section 4.2 ("Security Vulnerabilities").
- **Step 5:** We documented the threats in Section 4.2 ("Security Vulnerabilities") with description, target, techniques used and strategy to manage risk
- **Step 6:** We use the DREAD risk analysis model to identify vulnerabilities, and assess their seriousness. (Meier, 2003) This is shown in Section 4.2, Figure 8 and Figure 9.

4. Summary of Findings

The targeted platform is protected with Imunify360 and therefore it was impossible for us to perform further scans without having our IP blocked. To solve this we performed scans using Proxychains and TOR, redirects our network traffic hiding our true IP address. Next, we present the summary of our findings.

4.1. Information gathering stage

We obtained information about the open ports, services, versions of the applications, version of the operating system, etc.

4.1.1. Port scanning using Nmap

We used -sU for UDP and sT for TCP protocol. Fig 3 presents the TCP results. Fig 4 shows the UDP results. In the Appendix, we documented the original prints (Appendix Fig. 2 and Fig 3)

PORT	STATE	SERVICE
21/TCP	OPEN	FTP
25/TCP	OPEN	SMTP
53/TCP	OPEN	DOMAIN
80/TCP	OPEN	HTTP
110/TCP	OPEN	POP3
143/TCP	OPEN	IMAP
443/TCP	OPEN	HTTPS
465/TCP	OPEN	SMTPS
587/TCP	OPEN	SUBMISSION
993/TCP	OPEN	IMAPS
995/TCP	OPEN	POP3S
2525/TCP	OPEN	-
3396/TCP	OPEN	MYSQL
5432/TCP	OPEN	POSTGRES

Fig 3. TCP scan

PORT	STATE	SERVICE
19/UDP	OPEN	CHARGEN
53/UDP	OPEN	DOMAIN
162/UDP	OPEN	SNMPTRAP
1900/UDP	OPEN	UPNP

Fig 4. UDP scan

4.1.2. Server software and technology found

The server software and technology found are shown in the Appendix Fig 1.. The targeted website is protected with Imunify 360, which comes from the host *A2 Hosting* (This can be seen in the Nmap scan print documented in the Appendix Fig 1. Imunify360 protects against malware infections, web attacks, vulnerability exploitation, and other threats. (Imunify360, 2022)

4.1.3 Subdomain enumeration

In Figure 5, we mapped the domain using KnockPy to identify additional targets that could be exploited, by running the following command from a unix/linux terminal:

```
echo | openssl s_client -showcerts -servername daedalus-systems.tech-sourcery.co.uk -connect daedalus-systems.tech-sourcery.co.uk:443
2>/dev/null | openssl x509 -inform pem -noout -text | grep -e DNS
```

Fig 5. Command from a unix/linux terminal

Next, Figure 6 shows all the subdomains found:

IP Address	Sub Domain
68.66.247.187	autodiscover.daedalus-systems.co.uk
68.66.247.187	autoconfig.daedalus-systems.co.uk
68.66.247.187	cpanel.daedalus-systems.co.uk
68.66.247.187	cpcalendars.daedalus-systems.co.uk
68.66.247.187	cpcontacts.daedalus-systems.co.uk
68.66.247.187	ftp.daedalus-systems.co.uk
68.66.247.187	mail.daedalus-systems.co.uk
68.66.247.187	webdisk.daedalus-systems.co.uk
68.66.247.187	webmail.daedalus-systems.co.uk
68.66.247.187	whm.daedalus-systems.co.uk
68.66.247.187	www.daedalus-systems.co.uk

Fig 6. KnockPy Results

4.1.4 Looking for sensitive files

We used DirBuster to brute force directories and file names on the targeted application. We used the default directory-list-2.3-medium.txt. Quite often, what looks like a web server in a state of default installation is actually not, and has pages and applications hidden within. The scan we did with DirBuster didn't identify hidden files and directories.

4.1.5 SQL injection attack experiment

We used SQLMap to identify entry points vulnerable to a SQL injection exploit. Results show no sql injection exploits that can be leveraged. See Figure 7 for details.

```
[15:05:47] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[15:05:54] [WARNING] GET parameter 'route' does not seem to be injectable
[15:05:54] [INFO] testing if GET parameter 'product_id' is dynamic
[15:05:55] [WARNING] GET parameter 'product_id' does not appear to be dynamic
[15:05:55] [WARNING] heuristic (basic) test shows that GET parameter 'product_id' might
not be injectable
[15:05:56] [INFO] testing for SQL injection on GET parameter 'product_id'
```

Fig 7. SQLMap Results

4.2. Security vulnerabilities overview

We used proxychains and TOR to perform scans on the targeted website with VEGA (Appendix Fig. 4), OWASP ZAP (Appendix Fig. 5) and Arachni, three widely used pentesting tools. In total, there were 21 issues found, as is shown in Figure 8.

High	1
Medium	4
Low	7
Informational	9
Total	21

Fig 8. Vulnerabilities grouped by risk severity

We did not include threats given the cost required to address them. However, we listed them in Section 4.2.1.6 ("Other Vulnerabilities"). If a threat is rated as High, it poses a significant risk to your application and needs to be addressed as soon as possible. Medium threats need to be addressed, but with less urgency. The classification rating is shown in the Figure 9 below:

Rating	High (3)	Medium (2)	Low (1)
D Damage potential	The attacker can subvert the security system	Leaking sensitive information	Leaking trivial information
R Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D Discoverability	The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it.	The bug is obscure, and it is unlikely that users will work out damage potential.

Fig 9. DREAD ratings

4.2.1 High/medium risk vulnerabilities found

1. Page Fingerprint Differential Detected - Possible Local File Include	
Risk Rating	High
Description	A different response fingerprint in relation to a local file include injection attempt was detected. This may indicate the existence of a local file include vulnerability, and could allow attackers to gain unauthorised access to sensitive information.
Target	https://www.daedalus-systems.co.uk/
Request	GET /index.php?route=product/product/write&product_id=../
Solution	Developers should canonicalize the path of any filesystem resource that has a path composed of externally-supplied input and perform an authorization check prior to access.
Resource	/index.php
References	Directory Traversal (Wikipedia), Path Traversal (OWASP), Avoiding Path Traversal (OWASP).

2. Possible HTTP PUT File Upload	
Risk Rating	Medium
Description	The HTTP PUT method allows HTTP clients to store resources on a HTTP server. This means file upload capability. A loss of system integrity could occur if such a request were made, as a server overwrites pre-existing resources located at the URI of a PUT request.
Target	https://www.daedalus-systems.co.uk/
Resource	http://www.daedalus-systems.co.uk/https:/PUT-putfile
Impact	Arbitrary file uploads could affect system integrity if an attacker were to overwrite a pre-existing resource on the server.
Solution	Server settings should be reviewed to identify and disable the misconfiguration. Apache allows for methods such as PUT and DELETE to be restricted using the LIMIT directive.
References	RFC 2616 - HTTP 1.1: Section 9 (IETF) Apache httpd Core Documentation: Limit Directive (Apache) OSVDB 397: Multiple Web Server Dangerous HTTP Method PUT (OSVDB)

3. Insecure cookie setting: missing HttpOnly flag	
Risk Rating	Medium
Description	A cookie has been set without the HttpOnly flag, which means that it can be accessed by the JavaScript code running inside the web page. If an attacker manages to inject malicious JavaScript code on the page (e.g. by using an XSS attack) then the cookie will be accessible and it can be transmitted to another site.
Target	https://www.daedalus-systems.co.uk/
Resource	https://owasp.org/www-community/HttpOnly
Impact	In case of a session cookie, this could lead to session hijacking.
Solution	Ensure that the HttpOnly flag is set for all cookies.
Classification	CWE-1004 OWASP Top 10 - 2013 : A5 - Security Misconfiguration OWASP Top 10 - 2017 : A6 - Security Misconfiguration

4. Insecure cookie setting: missing Secure flag	
Risk Rating	Medium
Description	Since the Secure flag is not set on the cookie, the browser will send it over an unencrypted channel (plain HTTP) if such a request is made. Thus, the risk exists that an attacker will intercept the clear-text communication between the browser and the server and he will steal the cookie of the user.
Target	https://www.daedalus-systems.co.uk/
Resource	OWASP Web Security Testing Guide
Impact	In the worst case scenario, the cookie will be a session cookie and the attacker could gain unauthorised access to the victim's web session.
Solution	Whenever a cookie contains sensitive information or is a session token, then it should always be passed using an encrypted channel. Ensure that the secure flag is set for cookies containing such sensitive information.
Classification	CWE-614 OWASP Top 10 - 2013 : A5 - Security Misconfiguration OWASP Top 10 - 2017 : A6 - Security Misconfiguration

5. Insecure cookie setting: domain too loose	
Risk Rating	Medium
Description	A cookie may be used in multiple subdomains belonging to the same domain.
Target	https://www.daedalus-systems.co.uk/
Resource	OWASP Web Security Testing Guide
Impact	Potentially risky websites under your main domain may access those cookies and use the victim session on the main site.
Solution	The Domain attribute should be set to the origin host to limit the scope to that particular server. For example if the application resides on server app.mysite.com, then it should be set to Domain=app.mysite.com
Classification	CWE-614 OWASP Top 10 - 2013 : A5 - Security Misconfiguration OWASP Top 10 - 2017 : A6 - Security Misconfiguration

6. Vulnerabilities found for server-side software	
Risk Rating	Medium
Description	These vulnerabilities expose the affected applications to the risk of unauthorised access to confidential data and possibly to denial of service attacks.
Target	https://www.daedalus-systems.co.uk/
Resource	OWASP Web Security Testing Guide
Impact	Potentially risky websites under your main domain may access those cookies and use the victim session on the main site.
Solution	We recommend you to upgrade the affected software to the latest version in order to eliminate the risk of these vulnerabilities.
Classification	CWE-1026 OWASP Top 10 - 2013 : A9 - Using Components with Known Vulnerabilities OWASP Top 10 - 2017 : A9 - Using Components with Known Vulnerabilities.

4.2.2. Low/informational vulnerabilities found

Next, Figure 10 shows the Low Risk Vulnerabilities found and Figure 11 presents the Informational Risk Vulnerabilities found.



Fig 10. Low Risk

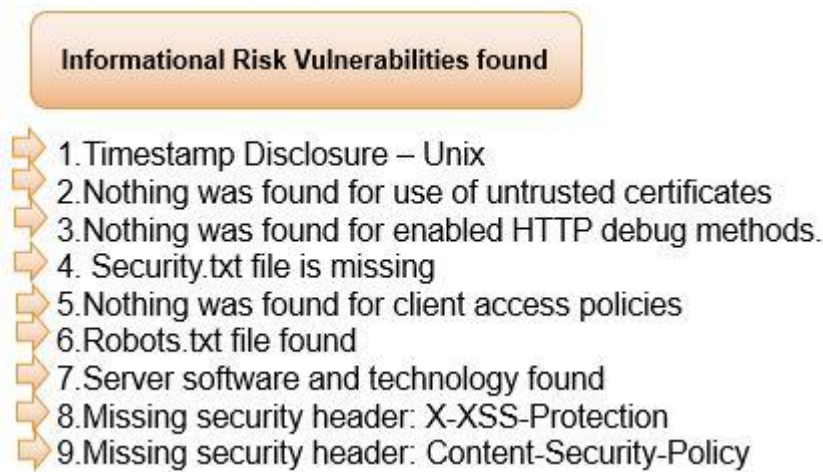


Fig 11. Informational Risk

5. Security standard analysis & GDPR compliance

5.1. GDPR - personal data

The General Data Protection Regulation (GDPR) governs the processing and sharing of personal data, including: Subject Identification Data, Personal Data (any data that can be used to identify an individual), Spatial Data and Cookie identifier. Figure 12 shows our conclusions regarding the data compliance for the targeted website that includes payment facilities.

1.	Visitors	Customers	3 rd Party Data Processors
Identification Data	X	X	X
Personal Data		X	X
Spatial / Geographic Data	X	X	
Cookies	X	X	X

Fig 12. GDPR - Personal Data

5.2 GDPR Controls

Next, Figure 13 presents the minimum controls daedalus site needs:

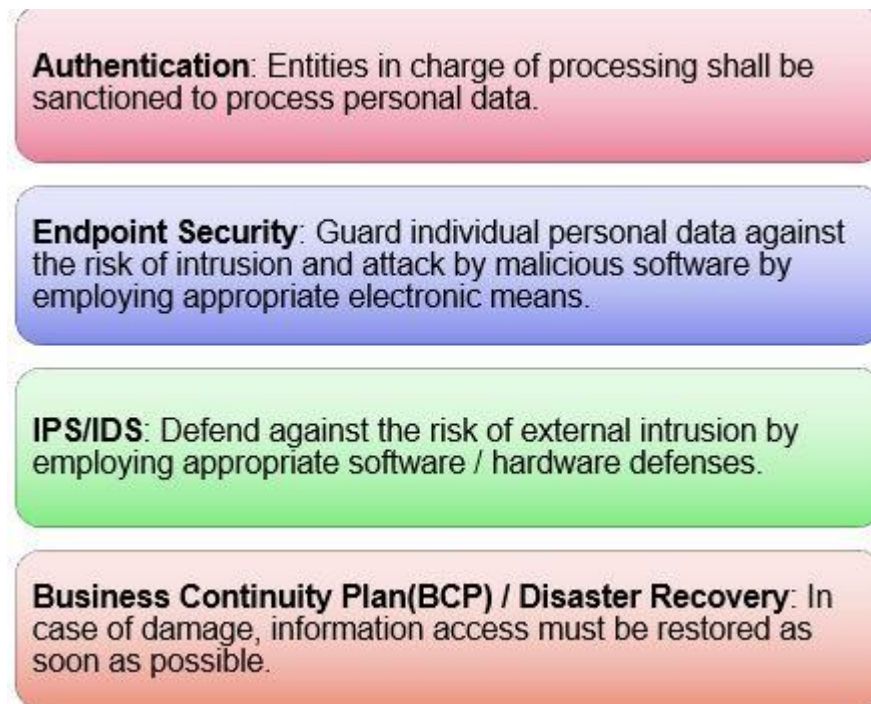


Fig 13. GDPR Controls

5.3 GDPR Compliance Tests

Figure 14 below shows the GDPR compliance tests we performed.

Test	Result	Contravenes
Privacy Policy Test	Privacy Policy with no text	Article 13
Website Security	Outdated Versions with Known CVEs	Article 5(1)(f) Article 24(1) Article 32
TLS Encryption	HTTPS is missing site is available on port 80	Article 5(1)(f) Article 24(1) Article 32
Cookie Protection	Cookies with (personal or tracking information) are sent without the Secure flag.	Article 5(1)(f) Article 24(1) Article 32
Cookie Disclaimer	Third-party cookies including tracking information are sent, no cookie disclaimer text was found on the website.	Article 13

Fig 14. GDPR compliance

5.4 GDPR Compliance Tests Details

This section is aimed to provide the GDPR compliance test details regarding Privacy Policy, Website Security, Transport Layer Security Encryption, Cookie Protection, Cookie Disclaimer.

5.4.1. Privacy Policy

Article 13 of GDPR requires the data controller to provide a notice to data subjects when collecting personal data. However, privacy policy contains no text, as shown in Figure 15.

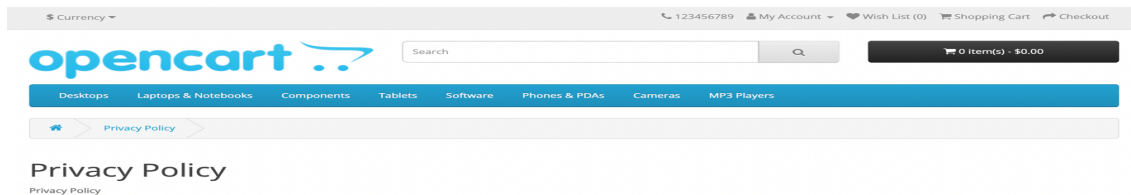


Fig 15. Privacy Policy

5.4.2. Website Security

Article 5(1)(f), Article 24(1) & Article 32 of GDPR necessitate implementation, testing and maintenance of adequate security controls to safeguard personal data. The following was identified as having out of date software.

Software	Version
OpenCart	3.0.3.7
JQuery	2.1.1
BootStrap	3.3.5

Fig 16. Software Version

The Figures 16 and 17 below details the known issues with these versions:

J-Query			
CVSS Score	CVE_ID	Type	URL
5.5 (Medium)	CVE-2020-11022	Cross Site Scripting	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11022
4.8 (Medium)	CVE-2019-11358	Prototype Pollution	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11358
4.1 (Medium)	CVE-2020-11023	Cross Site Scripting	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-11023

Fig 16. J-Query

Bootstrap			
CVSS Score	CVE_ID	Type	URL
5.5 (Medium)	CVE-2016-10735	Cross Site Scripting	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10735
5.5 (Medium)	CVE-2018-14040	Cross Site Scripting	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14040
5.5 (Medium)	CVE-2018-14042	Cross Site Scripting	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14042
5.5 (Medium)	CVE-2018-14041	Cross Site Scripting	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14041
5.3 (Medium)	CVE-2019-8331	Cross Site Scripting	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-8331
5.3 (Medium)	CVE-2018-20677	Cross Site Scripting	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20677
5.3 (Medium)	CVE-2018-20676	Cross Site Scripting	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20676

Fig 17. Bootstrap

5.4.3. Transport Layer Security Encryption

Article 5(1)(f), Article 24(1) and Article 32 of GDPR require “examination and maintenance of adequate security controls to protect personal data” (Anon GDPR). UK NCSC also give supplementary details on best practice that include effective maintenance of the web application software stack including routine website security analysis. Daedalus site is available on both port 80(HTTP) and port 443(HTTPS) access to port 80 should be removed or redirected to the secure port 443.

5.4.4. Cookie Protection

Article 5(1)(f), Article 24(1) and Article 32 of GDPR require examination and maintenance of security controls to protect personal data, including effective maintenance of web application software and regular website security analysis. However, each of these cookies is missing the following flags: Secure, HttpOnly, SameSite. This could allow for leakage of sensitive information.

5.4.5. Cookie Disclaimer

Along with Article 13 of GDPR, the EU ePrivacy Directive requires website operators to obtain explicit consent prior to setting any cookies. However, no Cookie Disclaimer is found on the site to opt in to receiving cookies.

5.2 WCAG Web Accessibility & Compliance Issues

Web Content Accessibility Guidelines 2.0, published in December 2008, became an ISO standard, ISO/IEC 40500:2012 in October 2012. WCAG 2.1 became a W3C Recommendation in June 2018. (W3C, 2018) The accessibility of UK websites is covered by the Equality Act 2010. Business owners are required to make ‘reasonable adjustments’ to make their websites accessible to people with disabilities. (Anon UK GOV,Wikipedia)

The WCAG compliance tests discovered the issues presented in Figure 18. The issues identified are addressed to ensure full compliance with the WCAG guidelines.

Page Scan Results

 **76/100** [Share Results](#)

1 critical, 2 serious, 0 moderate, 0 minor

CRITICAL • WCAG 2.0 A • Buttons must have discernible text

Ensures buttons have discernible text. Applicable success criteria: 4.1.2

ELEMENTS **9**

SERIOUS • WCAG 2.0 AA • Elements must have sufficient color contrast

Ensures the contrast between foreground and background colors meets WCAG 2 AA contrast ratio thresholds. Applicable success criteria: 1.4.3

ELEMENTS **20**

SERIOUS • WCAG 2.0 A • Links must have discernible text

Ensures links have discernible text. Applicable success criteria: 4.1.2, 2.4.4

ELEMENTS **1**

Figure 18. WCAG compliance test

5.3 PCI DSS Compliance Tests

In the PCI security standards, Requirement 6 is about developing and maintaining secure systems and applications. Requirement 6.2 is being disrespected because some components are outdated (as shown in Section XX). Besides, Requirement 6.5 is being disrespected because the website contains public CVEs. Figure 19 presents our recommendations.

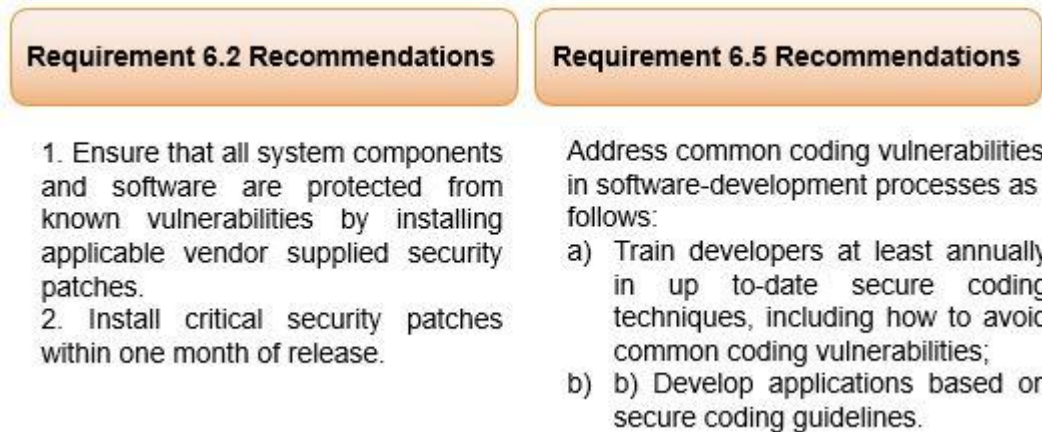


Fig 19. PCI Recommendations

6. Pentest Timeline

Next, Figure 20 shows the project timeline.



Fig 20. Timeline

7. Conclusion

Following the PTES and the OWASP Web testing framework, along with the Microsoft Threat Modelling Process, our team performed a comprehensive Web Application Security Pentest in the Daedalus-Systems site. Imunify360 is protecting the targeted application so we had to use ProxyChains and TOR to be able to perform scans without being blocked. We identified *high-risk*, *medium-risk*, *low-risk*, and *Informational* issues in the targeted application. When a threat is rated as High, it poses a significant risk to the application and needs to be addressed as soon as possible. Medium threats need to be addressed, but with less urgency. We also examined GDPR compliance and provided several recommendations to ensure that there are no deficiencies in the site in meeting legal guidelines and frameworks. The management team of the web site should ensure that regular security assessments take place at least one every twelve months to identify any weakness in the cyber security defences.

REFERENCES

PTES (2014). PTES Technical guideline. Available from: http://www.pentest-standard.org/index.php/Main_Page

ISO/IEC (2013) Information technology — Security techniques — Information security management systems — Requirements. Available from: <https://www.iso.org/standard/54534.html>

PCI (2008). Payment Card Industry Security Standards. Available from: https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf

Stefinko, Y., Piskozub, A., & Banakh, R. (2016, February). Manual and automated penetration testing. Benefits and drawbacks. Modern tendency. In 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET) (pp. 488-491). IEEE.

Imunify360 (2022). Hosting providers that offer Imunify360. Imunify360. Available from: <https://www.imunify360.com/>

W3C. (2018). *Web Content Accessibility Guidelines (WCAG) 2.1*, 2.1. Available from: <https://www.w3.org/TR/WCAG21>.










Microsoft Docs (2022) Threats and Countermeasures. Available from: [https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648641\(v=pandp.10\)](https://docs.microsoft.com/en-us/previous-versions/msp-n-p/ff648641(v=pandp.10))

Web Content Accessibility Guidelines
https://en.wikipedia.org/wiki/Web_Content_Accessibility_Guidelines

Guide to the General Data Protection Regulation (GDPR).
<https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

Keeping devices and software up to date - NCSC.GOV.UK. Available from: <https://www.ncsc.gov.uk/collection/device-security-guidance/managing-deployed-devices/keeping-devices-and-software-up-to-date>

APPENDIX

Software / Version	Category
 Apache	Web servers
 PHP 7.3.33	Programming languages
 OpenCart	Ecommerce
 Cart Functionalty	Ecommerce
 Swiper Slider	Miscellaneous
 Bootstrap 3.3.5	UI frameworks
 Google Font API	Font scripts
 Font Awesome	Font scripts
 jQuery 2.1.1	JavaScript libraries

Appendix Fig 1. Technologies

```

Nmap Output | Ports / Hosts | Topology | Host Details | Scans
nmap -sV -O daedalus-systems.co.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-02 19:51 E. South America Standard Time
Nmap scan report for daedalus-systems.co.uk (68.66.247.187)
Host is up (0.23s latency).
Not shown: 917 filtered tcp ports (no-response), 70 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Pure-FTPd
53/tcp    open  domain       ISC BIND 9.11.4-P2 (RedHat Enterprise Linux 7)
80/tcp    open  http         Apache httpd (W3 Total Cache/0.9.4.6.4)
110/tcp   open  pop3         Dovecot pop3d
143/tcp   open  imap         Dovecot imapd
443/tcp   open  ssl/http     Apache httpd (W3 Total Cache/0.9.4.6.4)
465/tcp   open  smtps?
587/tcp   open  smtp         Exim smtpd 4.94.2
993/tcp   open  ssl/imap     Dovecot imapd
995/tcp   open  ssl/pop3     Dovecot pop3d
2525/tcp  open  smtp         Exim smtpd 4.94.2
3306/tcp  open  mysql        MySQL 5.5.5-10.3.23-MariaDB-cll-lve
5432/tcp  open  postgresql   PostgreSQL DB 9.6.0 or later
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-
bin/submit.cgi?new-service :
SF-Port5432-TCP:V=7.92%I=7%D=12/2%Time=61A94E18%P=i686-pc-windows-windows%
SE:r(SMBProgNeg,8C,"E\0\0\0\x8b5FATAL\0VFATAL\0C0A000\0Munsupported\x20fro
SE:intend\x20protocol\x20655363\0.19778:\x20server\x20supports\x201\0.\0\x20to\
SE:x203\0\0Fpostmaster\0L2050\0RProcessStartupPacket\0\0");
Aggressive OS guesses: Linux 3.10 - 4.11 (94%), Linux 5.1 (94%), HP P2000 G3 NAS device (90%), Linux 3.18 (90%), Linux 3.2 - 4.9 (90%), Linux
3.13 (89%), Linux 3.13 or 4.2 (89%), Linux 3.16 - 4.6 (89%), Linux 4.1 (89%), Linux 4.10 (89%)
No exact OS matches for host (test conditions non-ideal).
Service Info: Host: n11-ss5.a2hosting.com; OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.30 seconds

```

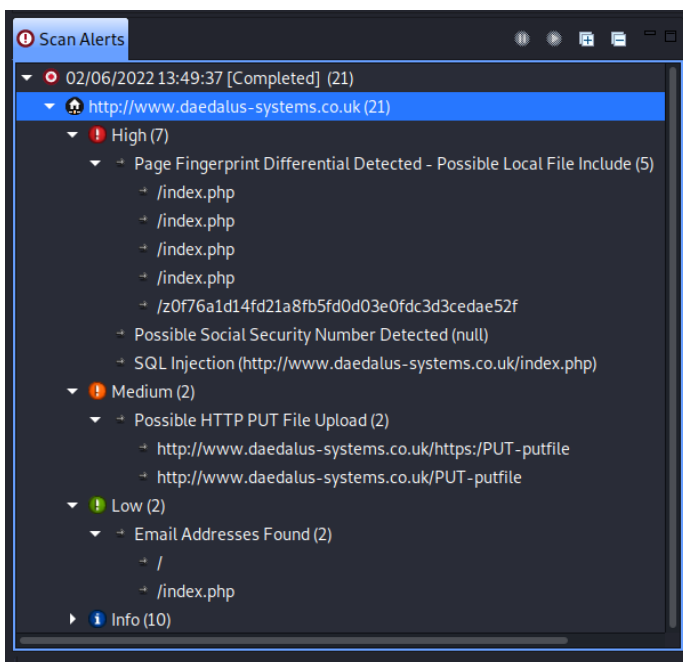
Appendix Fig 2. Original Scan Nmap TCP

```

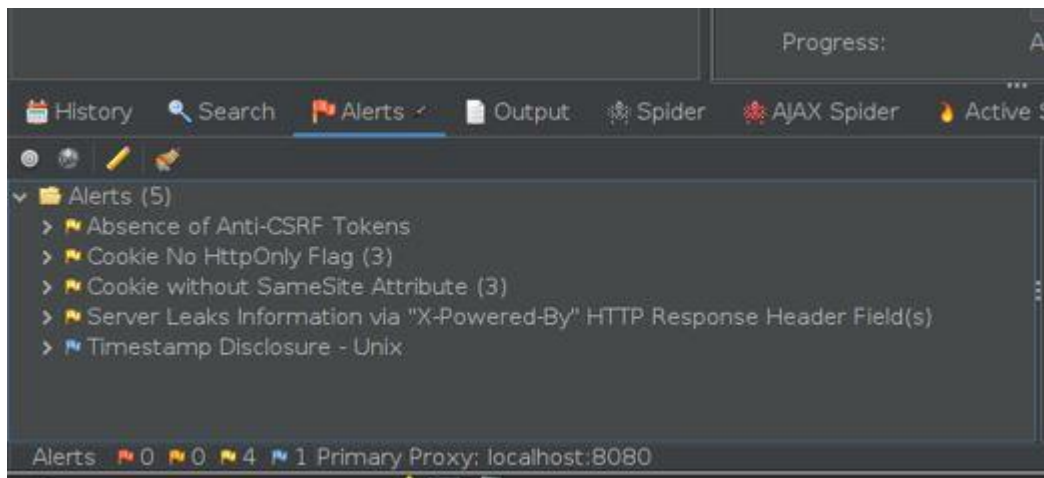
Starting Nmap 7.92 ( https://nmap.org ) at 2021-12-02 09:07 GMT
Nmap scan report for www.daedalus-systems.co.uk (68.66.247.187)
Host is up (0.026s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
Not shown: 996 closed udp ports (port-unreach)
PORT      STATE      SERVICE
19/udp    open|filtered  chargen
53/udp    open        domain
162/udp   open|filtered  snmptrap
1900/udp  open|filtered  upnp

```

Appendix Fig 3. Original Scan Nmap UDP



Appendix Fig 4. VEGA Scan



Appendix Fig 5. OwaspZAP