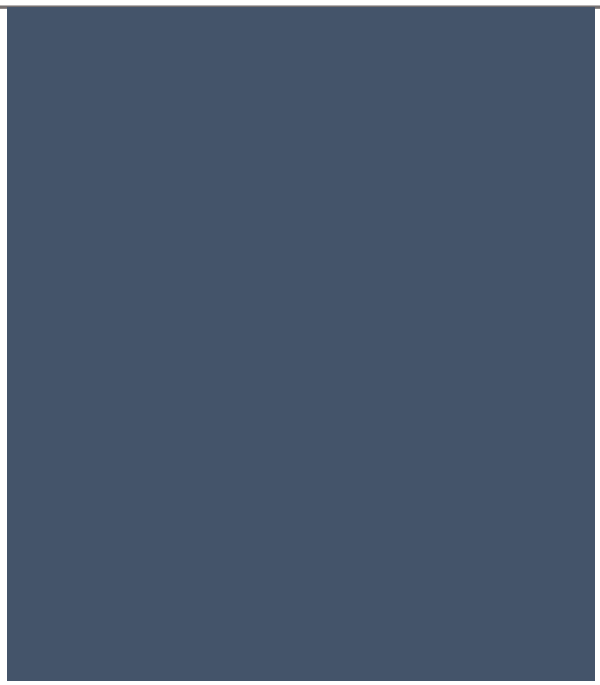


Executive Summary

The Security Squad Group2: Nils Linhoff, Adrian Boscu,Haroun Fujah

Content

Introduction

The Security Squad was tasked with scanning and analysing the Pilates&Yoga e-health website (https://dev8773.d2d6ymu8mykhhu.amplifyapp.com/). In this executive summary we present our findings as well as our recommendations.

Security issues found

The table below presents the tools we have used for the scanning as well as the vulnerabilities found for each tool.

Tool used	Vulnerability
Nmap & Legion	Host is listening on port 80 - unencrypted http traffic (is being redirected later on but any initial request and reply is being sent unencrypted)
DirBuster	The host needs to have appropriate privileges for the directory and files access in order not to permit access to them on the open internet.

Summary scanning analysis

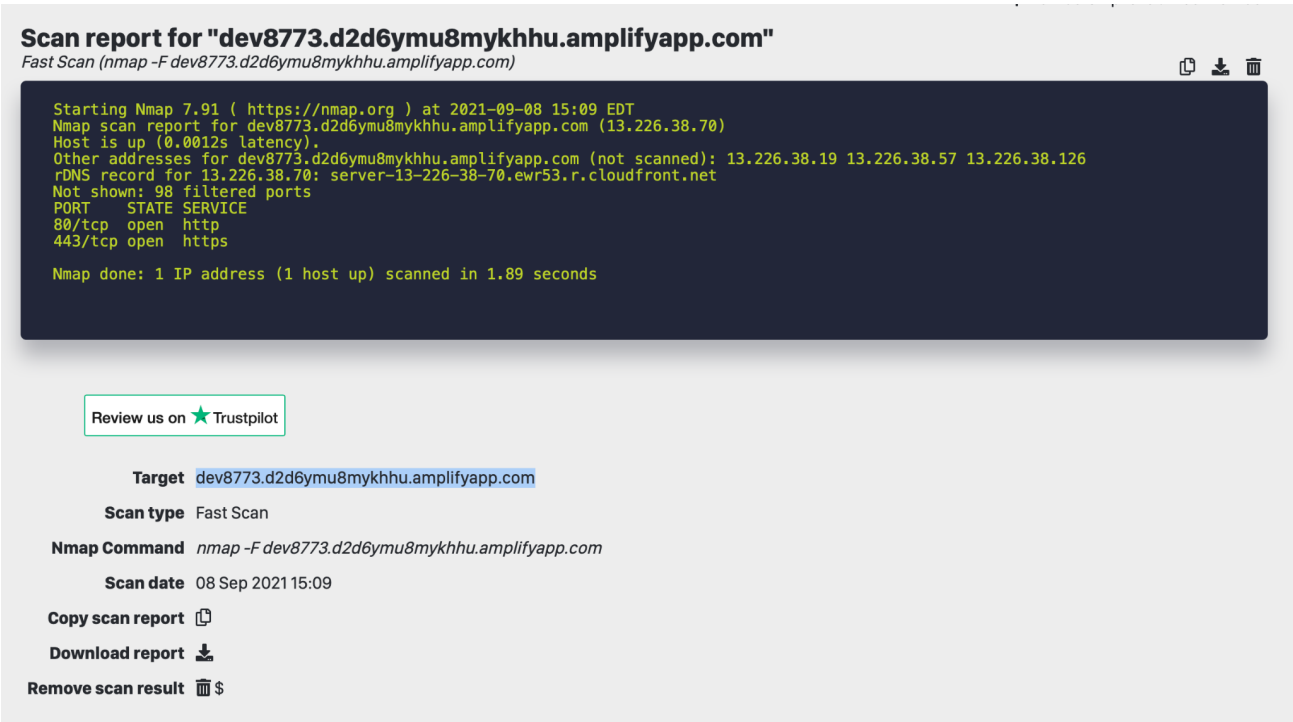
The reason behind selecting the following tools is mainly because they are open source as well as specifically designed for the job as part of the Kali Linux deployment package and they are the industry standards in terms of security and penetration testing according to Allen, Heriyanto and Shakeel Ali, 2014. Each tool is used for a specific purpose which in our case was for port discovery (NMAP and Legion) as well as directory and file search (DirBuster)

NMAP scan

Scanning with Nmap provides a detailed list of known ports that the host is actively listening for incoming connections.

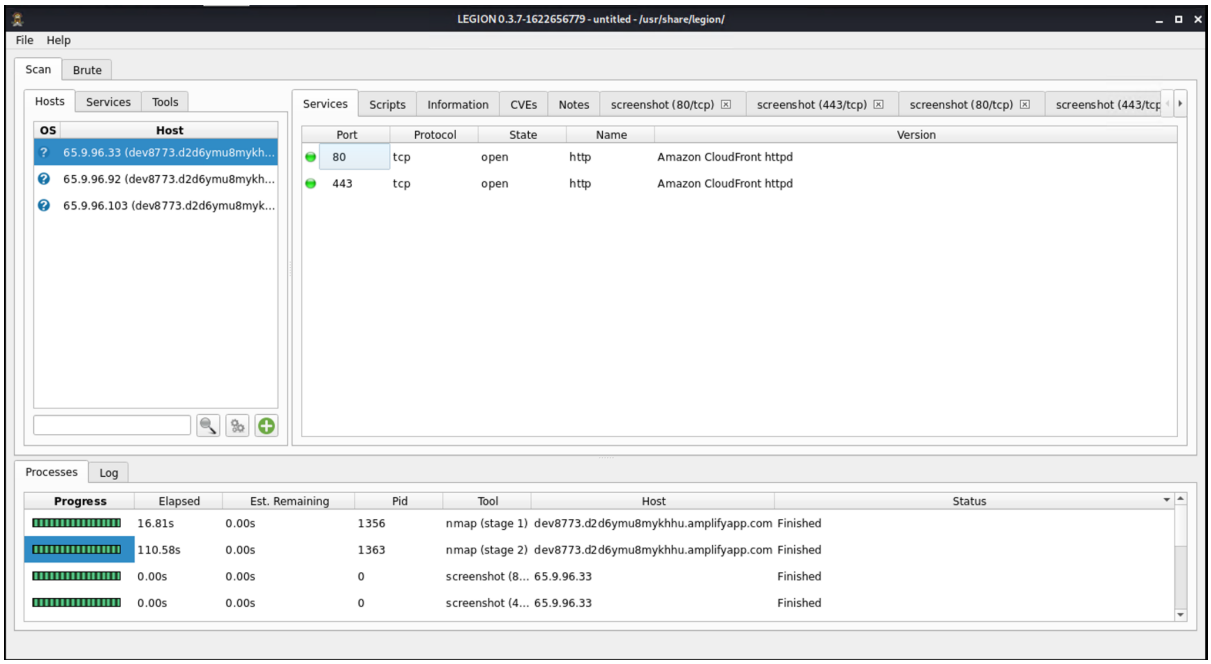
```
Nmap scan report for dev8773.d2d6ymu8mykhhu.amplifyapp.com (65.9.94.2)
Host is up (0.0013s latency).
Other addresses for dev8773.d2d6ymu8mykhhu.amplifyapp.com (not scanned): 65.9.94.66 65.9.94.47 65.9.94.46
Not shown: 998 filtered ports
PORT    STATE SERVICE  VERSION
80/tcp  open  http     Amazon CloudFront httpd
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: CloudFront
|_http-title: Did not follow redirect to https://dev8773.d2d6ymu8mykhhu.amplifyapp.com/
443/tcp open  ssl/http Amazon CloudFront httpd
|_http-generator: Nicepage 3.23.2, nicepage.com
| http-methods:
|_  Supported Methods: GET HEAD OPTIONS
| http-server-header:
|   AmazonS3
|_  CloudFront
|_http-title: Home
| ssl-cert: Subject: commonName=*.d2d6ymu8mykhhu.amplifyapp.com
| Subject Alternative Name: DNS:*.d2d6ymu8mykhhu.amplifyapp.com, DNS:d2d6ymu8mykhhu.amplifyapp.com
| Issuer: commonName=Amazon/organizationName=Amazon/countryName=US
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-08-21T00:00:00
| Not valid after:  2022-09-19T23:59:59
| MD5:   63d3 fe68 2941 b107 567c 5ca0 83ae aa88
|_SHA-1: 167c 35c1 1fd7 3050 38f4 20fd dd38 dc15 abca a9c6

NSE: Script Post-scanning.
Initiating NSE at 06:19
Completed NSE at 06:19, 0.00s elapsed
Initiating NSE at 06:19
Completed NSE at 06:19, 0.00s elapsed
Initiating NSE at 06:19
Completed NSE at 06:19, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 28.08 seconds
```



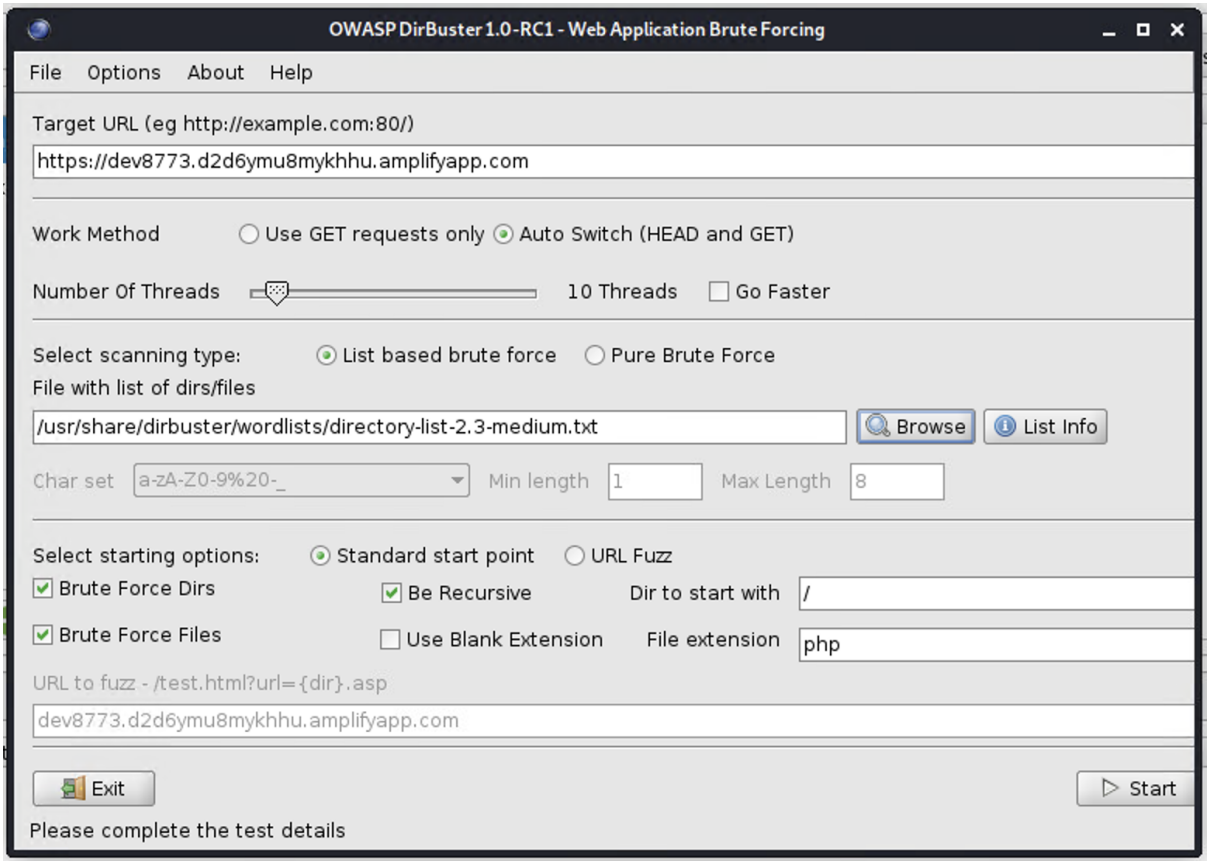
The scan performed shows us that the host is actively listening to the port TCP80 and TCP443 which are equivalent to HTTP and HTTPS respectively. We have performed the same scan from a dedicated host as well as using an online tool both providing the same outcome.

LEGION scan

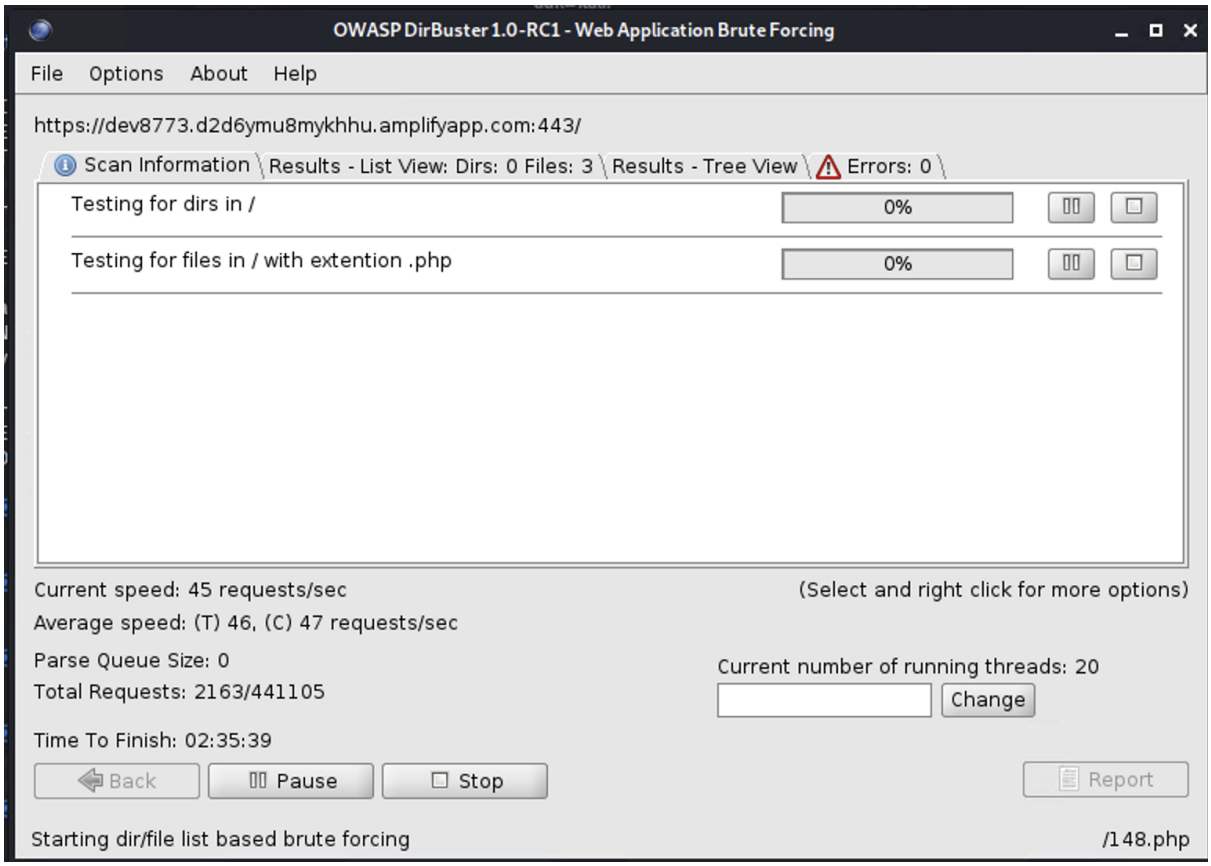


Legion is a similar tool as Nmap that provides details about the ports the host is listening to for incoming connections but in addition it provides a list of possible vulnerabilities that the host is running such as an old ssh server version. In our case because the web service is provided through CloudFront the output of vulnerabilities are not listed.

DirBuster scan

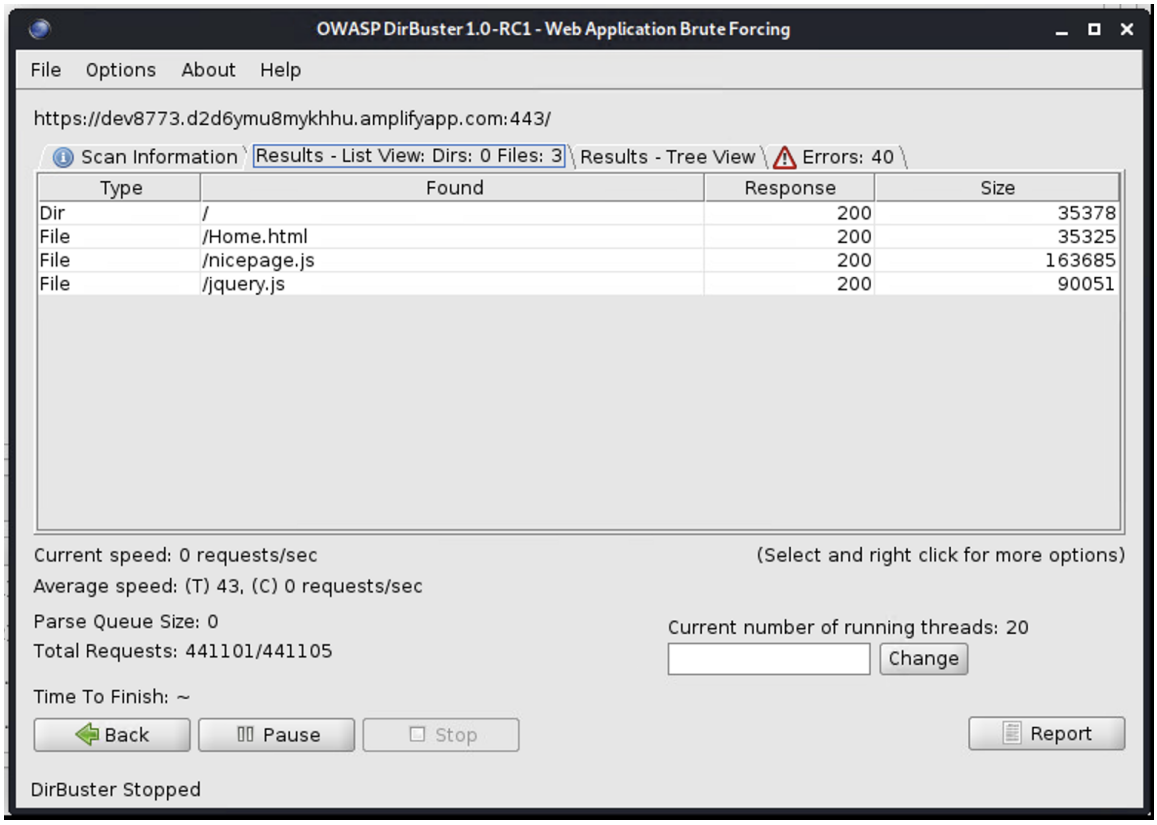


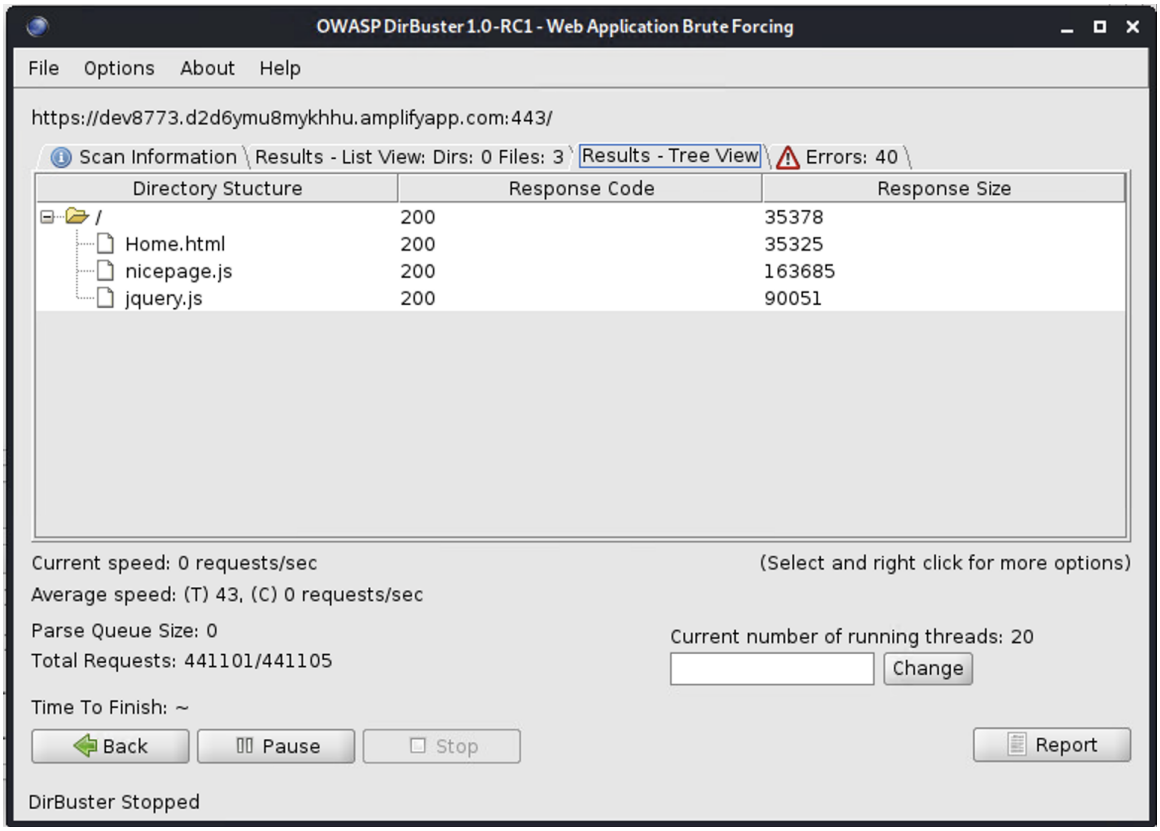
DirBuster is a scanning tool that checks the website subdirectories and files against a predefined word list. This is particularly dangerous while specific files or sub folders are not having appropriate permissions and are exposed to the open internet. In our scan we can see below the number of requests per second as well as total number of requests and progress.



In the above output we can see the scanning information and the requests being sent to the host against the predefined word list.

The below two outputs are showing the files or directories the tool has found, the size of the files and the tree structure.





Summary of threat analysis

Threat modelling enables the Pilates & Yoga E-health business to counteract potential security threats in advance, thereby averting significant cost implications relating to the containment, eradication and business recovery following a data breach (Shevchenko et al., 2018).

STRIDE

STRIDE is an acronym threat analysis method developed by Loren Kohnfelder and Praerit Garg in 1999 and implemented by Microsoft in 2002.

Spoofing (violating authentication)	**Tampering (violating integrity)**	**Repudiation (violating non-repudiation)**	**Information disclosure (violating confidentiality)**	**Denial of Service(violating availability)**	**Elevation of Privilege(violating authorization)**
IP spoofing – 'Man in the middle attack'	Malicious actors modifying the E-health website directory files	The inability to maintain a record of system and network logs.	Compromise of sensitive client information due to poor access control mechanisms.	Denial of service attack on the E-health website.	Unauthorized access of E-health website directory & files
Eavesdropping through unencrypted network	Wireless (Wi-Fi) network tampering	Malicious actor uses someone else's payment instrument on the E-health website without authorization	Malicious actor redirects traffic to permit reading data on the network		
Phishing website claiming the identity of the E-health site.					

Spoofing

IP Spoofing – Man in the Middle Attack

The aforementioned vulnerability scanning exercise with Nmap and Legion tools revealed the susceptibility of unencrypted network traffic on port TCP80 and TCP443. This leaves the E-health yoga & Pilates business exposed to IP spoofing man in the middle attacks.

This violates the ISO27001 and GDPR security standards as consumer trust and data security will be adversely affected which may result in a fall in customer demand for services on the E-health website.

Eavesdropping through unencrypted network

Unencrypted network traffic revealed in the Nmap & Legion vulnerability scanning exercise increases the likelihood of malicious actors eavesdropping over the network.

For cyber criminals, the advantages of implementing an eavesdropping attack on the E-health business can be substantial as customer debit card information or passwords can be siphoned from snooping at unencrypted traffic (Stone, n.d.).

Phishing E-health Website Link

A malicious actor could spoof the identity of the E-health website across the network (Shostack, 2014). Unassuming customers who access the phishing E-health website risk their personal information exposed to unlawful use.

Phishing schemes can be extraordinarily competent in deceiving customers to expose sensitive data such as passwords, credit card information and personal health information (USC EMHA Online. 2021).

Tampering

Malicious actors tampering with E-health website directory files

Malicious Attackers can alter files in a setting where they have appropriate permission. Hence, they can modify E-health confidential business files due to the poorly defined access privileges of the website directory and files revealed by the DirBuster Vulnerability scanning exercise. This erodes customer trust in the E-health and yoga business.

Wireless (Wi-Fi) Network Tampering

(Shostack, 2014) maintains that network tampering arises when a malicious attacker can alter data travelling within the Wi-Fi wireless network and redirect it to their machine. Several network protocols were designed with the requirement of specialist hardware to generate or read random packets. The prerequisite of special hardware safeguards against tampering and spoofing threats.

Repudiation

Malicious actor uses someone else's payment instrument on the E-health website without authorization

Repudiation threats transpire when an individual claims they did not do something or assume no responsibility for a situation. Shostack (2014), caustically adds, repudiation threats occur at the business layer of security vulnerabilities, where the corporate modalities relating to the sale of E-health yoga and fitness information is implemented.

The affected customer could claim not to have initiated the transaction and terminate their account due to the poor authentication mechanism at the point of payment on the E-health yoga and fitness website. This violates ISO27001

The inability to maintain a record of system and network logs

In addition, repudiation threats are related to the logging systems and procedures of the E-health website (Shostack, 2014).

A log is the documentation of occurrences within an establishment's systems and networks which contain log entries of data related to a particular event which has developed within a system or network (Kent & Souppaya, 2006).

As a result, the Security Squad must log vital incidents such as successes and failures of authentication efforts, access attempts, and efforts by customers to access or modify logs. In the absence of retaining or analysing logs, the probability of cyberattacks on the E-health website increases significantly (Shostack, 2014).

Information Disclosure

Compromise of sensitive client information due to poor access control mechanisms.

The DirBuster scanning exercise revealed that the host requires explicit access privileges for the E-health website directory and files, to avert their unlawful compromise.

Further to this, the inability to establish precise access privileges on the website directory and files exposes private client financial and health information on the open internet (Shostack, 2014). As a result, this circumvents the integrity component of the information security triad and ISO 27001 certification as client information is exposed to unlawful disclosure and malicious tampering.

Malicious actor redirects traffic to permit reading data on the network

Shostack (2014), states that data flows are particularly vulnerable to information disclosure attacks when data is travelling within a network. Subsequently, attackers can read the data on the network and transmit it to themselves by spoofing the network control protocol, enabling access to the traffic.

Consequently, this violates confidentiality, integrity and ISO 27001 whereby the operational risk of revealing confidential business information is augmented.

Denial of Service

Denial of service attacks overwhelm a resource that is required to deliver a service (Shostack, 2014).

The occurrence of IP spoofing due to the open network ports aids the probability of a denial-of-service attack. Cyber criminals can utilize spoofed IP addresses to overpower computer servers with packets of data thereby shutting the E-health fitness and yoga website down (What is IP spoofing?, n.d.).This signifies a total compromise of system availability and integrity as the E-health website is shut down and customers are unable to access required services.

Elevation of Privilege

Unauthorized access of E-health website directory & files

Elevation of privilege threats occur when a malicious actor gains access to data and services which they are not legitimately authorized to see (Alhassan et al., 2016). This relates to the ambiguous access privileges for the E-health website directory and files discovered by the DirBuster scanning exercise.

Furthermore, A particular limitation of the stride is that the quantity of threats can grow significantly as a system increases in complexity (Shevchenko et al., 2018).

PASTA

The Process for Attack Simulation and Threat Analysis (P.A.S.T.A) is a risk-centric threat modelling measure introduced in 2012 by Tony UcedaVéleZ outlining the following business requirements adapted from (Shevchenko et al., 2018):

1. **Define Objectives** - Identify security & compliance requirements The business objective was to scan and analyze the Pilates & yoga E-health website for security vulnerabilities.
2. **Define Technical Scope** - Create Boundaries of the Technical Environment The technical scope was to utilize open-source scanning tools such as Nmap, Legion, and Dirbuster to identify the specific weaknesses.
3. **Application Decomposition** - Identify Access Points & Trust Levels The scanning exercises enabled the Security Squad to pinpoint vulnerable access points such as opened network ports and undefined access privileges for the website directory and files.
4. **Threat Analysis** - Probabilistic Attack Scenarios Analysis The STRIDE modelling approach permitted the Security Squad to ascertain probable attack scenarios such as IP spoofing 'man in the middle attacks' and denial of service attacks.
5. **Vulnerability & Weaknesses Analysis –** Queries of vulnerability scanning exercise
6. **Attack Modelling -** Attack Surface Analysis The scanning exercise signified that the system is exposed to numerous threats, which conveys a large attack surface (Shostack, 2018).
7. **Risk & Impact Analysis** - Countermeasure Identification The threats exposed in the scanning exercise signified the absence of business requirements needed to reduce the trust boundaries of the system.

DREAD

By utilizing the DREAD model, risk rating for a threat is portrayed by asking the following questions adapted from (Alhassan et al., 2016):

Damage Potential – How extensive is the damage potential of the attack?

Reproducibility – How easy is it to repeat the attack?

Exploitability – How complicated is it to launch an attack?

Affected Users – How many users are impacted by the attack?

Discoverability – How easy is it to find the threat?

DREAD Risk Rating Scheme

Range of Risk	**Threat Rating**
0-6	Low
7-11	Medium
12-15	High

Threats to the Yoga&Pilates website in relation to DREAD

Threat	D	R	E	A	D	Total	Threat Rating (In Order of Severity)
Phishing website claiming the identity of the E-health site.	3	3	3	2	4	14	High
Compromise of sensitive client information due to poor access control mechanisms.	3	3	3	3	1	13	High
Unauthorized access of E-health website directory & files	3	3	3	3	1	13	High
Malicious actors modifying the E-health website directory files	3	3	3	3	1	13	High
Malicious actor redirects traffic to permit reading data on the network	3	2	3	3	1	12	High
Denial of service attack on the E-health website	3	2	3	3	1	12	High
Eavesdropping through unencrypted network	3	2	2	3	1	11	Medium
IP spoofing ‘Man in the middle attack’.	3	2	2	2	1	10	Medium
Unauthorized access of E-health website directory & files	3	2	1	2	1	10	Medium

Evaluation and recommendation of security standards

Part of the security assessment is to evaluate the current state of the website against recommended and mandatory security standards. The aim is to highlight the areas in which the website needs improvement and to provide further suggestions for future security standards.

Evaluation of "Yoga&Pilates" website against GDPR

The European Data Protection Regulation (GDPR) is a federated security standard that harmonizes data privacy laws across the EU (GDPR – Material scope', no date).

Since the website as well as its services are located in the United States the site does not need to hold up against GDPR standards. However, the Security Squad recommends, in the case of expansion of the business to a GDPR country, to work through the following checklist (GDPR compliance checklist - GDPR.eu, no date). The GDPR comprises different security dimensions: Lawful basis and transparency, data security, accountability, and governance as well as privacy rights.

Lawful basis and transparency

- Information audit: conduct an audit on what information the organisation has and how it processes it.
- legal justification for data processing: provides a legal justification for the processing of private data
- provide a clear privacy policy: inform the customer on how and why their data is processed.

Data security

- secure software development: practice secure software development and processes
- encrypt, anonymize and pseudonime: Use these data protection methods whenever possible
- data security awareness: provide training for the organisation
- data protection impact assessment
- plan for a data breach: have an action plan ready in case of a data breach

Accountability and governance

- Assign GDPR roles: assign the necessary roles in the organisation such as data protection officer
- Data processing agreement: provide a data processing agreement for your customers and any third party

Privacy rights

- Right to enquire personal data: ensure that the customer has an easy way to enquire which data has been stored.

- Right to update and correct personal data: ensure that the customer has an easy way to update and correct their personal data
- Right to delete data: ensure that the customer has an easy way to request that their data is deleted
- Right to request stop processing data: ensure that the customer has an easy war to request to stop processing their data.

This list is just to highlight the most important key factors of the GDPR, it is not exhaustive. But we strongly recommend implementing a data consent form for the processing of cookies regardless of the current place of business. For an in-depth analysis of GDPR compliance we recommend commissioning the Security Squad.

Recommendation for a ISO27001 certifications

The Security Squad recommends a ISO 27001 certification in order to show good data security practice and to stay competitive in the market. The industry standard ISO 27001 for Information security management system might includes requirements for the assessment and treatment of information security risks (The new ISO/IEC 27001:2013 standard, no date). It is the norm for the implementation and operation of an information security management system. This has several benefits:

- minimizing legal and operational risks
- optimizing security processes
- reducing IT-costs
- increasing trust among customers, business partners
- identifying security threats
- protecting data against disclosure, tampering and repudiation

To achieve a ISO 27001 certification a information security management system should be implemented and possible security risks should be identified, evaluated and observed (See Summary of threat analysis/Summary of scanning analysis). The Security Squad strongly recommends an ISO 27001 certification to publicly display that cybersecurity and data security is well managed at this organisation.

Summary of recommendations

Based on our extensive scanning and threat analysis, the Security Squad formulated recommendations and mitigation strategies as laid out in the Summary of threat analysis and Summary of scanning analysis. To highlight

the most important actions to improve cyber security for the Yoga&Pilates website, please refer to the executive action plan:

Executive action plan

Urgency	Action
high	acknowledge DREAD risks
high	implement encryption (data/network)
middle	close TCP80 and TCP443.
middle	implement 2-factor authentification
middle	implement logging and IDP system
middle	timeout single IP requests
middle	implement a GDPR data consent form
middle	implement business continuity measures
middle	Implement data security (GDPR) policies
middle	implement GDPR checklist (as recommended)
middle	employ the Security Squad for further cybersecurity consultation
low	get ISO27001 certified

References

Tang, A., 2014. Network Security - A guide to penetration testing. 8th ed. pp.8-11. ISSN 1353-4858, available at: https://0-doi-org.serlib0.essex.ac.uk/10.1016/S1353-4858(14)70079-0.

Allen, L., Heriyanto, T. and Shakeel Ali, S., 2014. Kali Linux – Assuring Security by Penetration Testing. Published by Packt Publishing.

Alhassan, J., Abba, E., Olaniyi, O. and Waziri, V., 2016. Threat Modeling of Electronic Health Systems and Mitigating Countermeasures. *Information and Communication Technology and its Applications*,.

Shevchenko, N., Chick, T., O'Riordan, P., Scanlon, T. and Woody, C., 2018. *Threat Modeling: A Summary of Available Methods*. [online] Available at: <https://apps.dtic.mil/sti/pdfs/AD1084024.pdf> [Accessed 23 October 2021].

Shostack, A., (2014) *Threat Modeling: Designing for Security*. 1st ed. Indianapolis: John Wiley & Sons.

Stone, M., n.d. *What Are Eavesdropping Attacks & How To Prevent Them*. [online] Verizon Enterprise. Available at: <https://enterprise.verizon.com/resources/articles/s/what-are-eavesdropping-attacks/> [Accessed 23 October 2021]

USC EMHA Online. 2021. Electronic Health Records | Read About Cybersecurity Concerns. [online] Available at: <https://healthadministrationdegree.usc.edu/blog/cybersecurity-in-the-electronic-health-record-era/> [Accessed 23 October 2021].

Kent, K. and Souppaya, M. (2006) Guide to Computer Security Log Management. Available from: https://csrc.nist.gov/publications/detail/sp/800-92/final [Accessed 23 October 2021]

www.kaspersky.com. n.d. *What is IP spoofing?*. [online] Available at: <https://www.kaspersky.com/resource-center/threats/ip-spoofing> [Accessed 23 October 2021].

'Art. 2 GDPR – Material scope' (no date) *General Data Protection Regulation (GDPR)*. Available at: https://gdpr-info.eu/art-2-gdpr/ (Accessed: 29 September 2021).

GDPR compliance checklist - GDPR.eu (no date). Available at: https://gdpr.eu/checklist/ (Accessed: 18 October 2021).

The new ISO/IEC 27001:2013 standard (no date). Available at: https://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/ (Accessed: 8 September 2021).