# Penetration Test of

# https://bookacheckup.co.uk/index.php

# Results and Executive Summary

Table of Contents

## 1. Introduction

*https://bookacheckup.co.uk/index.php* is a healthcare appointment-booking website which has been penetration tested for web application vulnerabilities. The following report will outline and discuss

- standards for cyber and data security
- utilized testing methodologies
- test results and analysis
- standards compliance
- mitigation recommendations

pertaining to the completed test.

## 2. Security Statutes and Application Vulnerability

### 2.1 Healthcare Information Privacy

The following regulations have served as benchmarks in assessing the security of the web application*:*

- GDPR (2018)
  - Health data comprises all information relating to the past, present, and future status of an individual
  - Organizations will implement the appropriate technical measures to ensure all data security
- HIPAA (1996)
  - Only approved bodies can have access to an individual's personal health information

These above requirements will determine if the web application is satisfactorily secured.

## 2.2 Web Application Vulnerabilities

The following components can pose a threat to “misconfigured, unpatched, [and] vulnerable” (Tunggal, 2023)  web application and network configurations:

- Open ports (Schrader, 2022)
- Misconfigured HTML files (ZAP, 2023a)
- Unprotected database servers (Bocetta, 2018)
- User input fields which can be used to exploit the above (Pinto & Stuttard, 2011)

These attack vectors are thus the main foci of the web application penetration test.

## 3. Penetration Test Methodology

To assess the security of *https://bookacheckup.co.uk/index.php*, a remote penetration test was performed with automatic and manual scanning to mirror real-world attack methodologies (Aharoni et al., 2011; Pinto & Stuttard, 2011).

The following tools were utilized during the test:

- Nessus – a vulnerability scanner at the networking layer (Chauhan, 2018)
- Nmap – a port scanner (Kaur & Kaur, 2017)
- Whatweb – a server software scanner (Kali, 2022)
- Zaproxy – a vulnerability scanner at the application/networking layers (Kali, 2023)

The penetration test was separated into two phases: preliminary and main.

The preliminary scan undertook the following:

1. Whatweb: document outdated running software and server types (automatic)
2. Nmap: scan for evidence of a firewall or other protective layer (automatic)

The main scan undertook the following:

3. Nmap: scan for all open ports on the network (automatic)
4. Nessus: parse port vulnerabilitlies and weaknesses (automatic)
5. Zaproxy: isolate vulnerabilitlies at the application layer (manual)

Results of these scans were analysed according to the OWASP (2023) and CAPEC (Mitre, 2023a) frameworks for severity, as well as GDPR and HIPAA for security compliance.

## 4. Penetration Test Results

### 4.1 Preliminary Scan Results

Preliminary scan security concerns are listed in Table 1.

*Table 1: Preliminary Scan Results*

| **Technology** | **Version** | **Updated** | **Vulnerability** |
|---|---|---|---|
| Operating System | Apache, Bootstrap | N/A | Cross-site scripting (Synk, 2023a) |
| Server Software | immunify360-webshield/1.18 | No | Remote code execution (Kovacs, 2021) |
| Server software | JQuery/1.12.4 | No | Cross-site scripting, prototype pollution (Synk, 2023b) |
| Firewall | None | N/A | Unfiltered connection acceptance (Johansen, 2021) |

### 4.2 Main Scan Results

Main scan results produced the following security concerns:

- Open ports (*Table 2*)

- Ranked vulnerabilities (*Table 3*)
- Information vulnerabilities (*Table 4*, see *Appendix I* for full list)

*Table 2: Open Ports*

| Port | Service | State | Vulnerabilities |
|---|---|---|---|
| 21/tcp | FTP | Open | Send and receive sensitive files (Schrader, 2022) |
| 25/tcp | SMTP | Open | Email spoofing and spam (Schrader, 2022) |
| 53/tcp | Domain | Open | Denial of service attacks (Schrader, 2022) |
| 80/tcp | HTTP | Open | Injection and denial of service attacks (Schrader, 2022) |
| 110/tcp | POP3 | Open | Mail command injections (Vulncat, 2023) |
| 143/tcp | IMAP | Open | Bypass multifactor authentication (Cloudflare, 2023) |
| 443/tcp | HTTPS | Open | Injection and denial of service attacks (Schrader, 2022) |
| 465/tcp | SMTPS | Open | Email spoofing and spam (Schrader, 2022) |
| 587/tcp | Submission | Open | Server-side request forgery attacks (Akbar, 2022) |
| 993/tcp | IMAPS | Open | Bypass multifactor authentication (Cloudflare, 2023) |
| 995/tcp | POP3S | Open | Mail command injections (Vulncat, 2023) |
| 2525/tcp | Ms-v-worlds | Open | Remote access trojans (Speedguide, 2023) |
| 3306/tcp | Mysql | Open | Malware, disclose sensitive database information (Schrader, 2022) |
| 5432/tcp | Postgresql | Open | Disclose sensitive database information (HackTricks, 2023) |

*Table 3: Ranked Vulnerabilities*

| Vulerability | | Attack(s) | Risk |
|---|---|---|---|
| 1 | Cloud Metadata Potentially Exposed | Instance Metadata (Vasudevan, 2022) | High |
| 2 | SSL Medium Strength Cipher Suites Supported | SSL SWEET32 (Kiprin, 2021) | High |
| 3 | Absense of Anti-CSRF Tokens | Cross-site request forgery (Mitre, 2023b) | Medium |
| 4 | Content Security Policy Header not Set | Cross-site scripting, clickjacking (Natarajan, n.d.) | Medium |
| 5 | Cross Domain Configuration | Cross-site scripting, cross-site request forgery (Adobe, 2021) | Medium |
| 6 | Hidden File(s) Found | Information leak (ZAP, 2023b) | Medium |
| 7 | TLS Version 1.0 Protocol Detection | Browser exploit against SSL/TLS (Invicti, 2023) | Medium |

| | | | |
|---|---|---|---|
| 8 | TLS Version 1.1 Protocol Deprecated | Man-in-the-middle (Bhattacharya, 2021) | Medium |
| 9 | Vulnerable JS Library | Cross-site scripting, cross-site request forgery, buffer overflow (Beagle, 2021) | Medium |
| 10 | Web Application Potentially Vulnerable to Clickjacking | Clickjacking, UI redress attack (Tenable, 2017) | Medium |
| 11 | Application Error Disclosures | Information leak (IBM, 2021) | Low |
| 12 | Cookie No HttpOnly Flag | Cross-site scripting, cross-site request forgery, man-in-the-middle (Nidecki, n.d.) | Low |
| 13 | Cookie Without Secure Flag | Session sidejacking (Mitre, 2023c) | Low |
| 14 | Cookie without SameSite Attribute | Cross-site request forgery, cross-site scripting, timing attacks (IBM, 2022) | Low |
| 15 | Server Leaks Information via “X-Powered-By” HTTP response Header field(s) | Information leak (IBM, 2023) | Low |
| 16 | Server Leaks Version Information via “Server” HTTP Response Header Field | Information leak (ZAP, 2023c) | Low |
| 17 | SMTP Service Cleartext Login Permitted | Credential/password sniffing (Tenable, 2021a) | Low |
| 18 | Strict-Transport-Security Header Not Set | Man-in-the-middle (Mozilla, 2023a) | Low |
| 19 | Timestamp Disclosure - Unix | Information leak (Ecylabs, 2023) | Low |
| 20 | Web Server Allows Password Autocompletion | Information leak (Tenable, 2021b) | Low |
| 21 | X-Content-Type-Options Header Missing | Content sniffing (Mozilla, 2023b) | Low |

*Table 4: Top Informational Vulnerabilities*

| Vulnerability | Parameter | Instance Count |
|---|---|---|
| Retrieved from cache | HTTP/1.1 | 1612 |
| Cookie poisoning | CSRF token | 128 |
| HTTP | Web servers, CGI abuses | 47 |
| Re-examine cache-control directives | Cache-control | 33 |
| Nessus | Port scanners | 28 |

## 5. Standards Compliance Analysis

The vulnerabilities above have found https://bookacheckup.co.uk/index.php to not be in compliance with either GDPR or HIPAA regulations concerning data privacy and security.

- GDPR violations
  - Technical measures have not been set to assure data security
    - database
      - Mysql/postgresql open ports
      - Hidden files found
    - Application layer
      - Password autocompletion
      - Depricated operating system/server software
      - Information leaks
      - Cross domain configuration
    - Network layer
      - Cookie poisoning
      - TLS/SSL configuration
      - Header settings
      - HTTP cache disclosure
- HIPAA violations
  - Routes exist for unauthorized individuals to access sensitive health information

        - Relevant vulnerabilities
            - Cross-site request forgery and buffer overflow
            - Cross-site scripting and clickjacking
            - Injection and information leaks

It is recommended these security vulnerabilities be mitigated for compliance with GDPR and HIPAA data security statutes.

6. Recommended Mitigations

A number of mitigations are recommended to better secure *https://bookacheckup.co.uk/index.php* against the above vulnerabilities.

To secure operating systems and server software:

- Regulary update all operating systems and server software to prevent degredation in security
- Implement a firewall to prevent unrestricted access to ports and servers

To secure open port use:

    - A secure virtual private network to create a proxy layer
    - Multi-factor authentication to better secure open service
    - Network segmentation for better access controls
    - Regular port scanning to detect degredation

The above suggestions should also prevent a majority of information vulnerabilities. Mitigation suggestions for ranked vulnerabilities by number ((Mitre, 2023a; Tenable, 2021; ZAP, 2023) are listed in Table 5.

*Table 5: Ranked Vulnerability Mitigations*

| **Vuln.** | **Mitigation** |
|---|---|
| 1 | Monitor NGINX configurations – monitor the use of the ‘Host’ header |
| 2 | Reconfigure the application to avoid using medium strength ciphers |
| 3 | Use an anti-CSRF package – OWASP CSRFGuard |
| 4 | Configure the web/application server to set the CSPH |
| 5 | Perform input/output validation for all content |
| 6 | Disable all non-essential production components |
| 7 | Enable support for TLS 1.2/3, disable TLS 1.0 |
| 8 | Enable support for TLS 1.2/3, disable TLS 1.1 |
| 9 | Ugrade to latest version of ExampleLibrary |
| 10 | Return the X-Frame-Options/Content-Security-Policy HTTP header with the page response |
| 11 | Implement custom error pages |
| 12 | Ensure the HTTPOnly flag is set for all cookies |
| 13 | Use an encrypted channel for transfer for all cookies |
| 14 | Ensure SameSite attribute is set to ‘strict’ |
| 15 | Configure web/application server to suppress ‘X-Powered-By’ headers |
| 16 | Configure web/application server to suppress the ‘Server’ header |
| 17 | Authenticate only over encrypted channels |
| 18 | Configure ‘Strict-Transport-Security’ header on server |
| 19 | Manually confirm the data is not sensitive/cannot be disclosed |
| 20 | Set all autocomplete attributes to ‘off’ |
| 21 | Set X-Content-Type header to ‘nosniff’ |

Implementation of these recommendations should bring the application into compliance with GDPR and HIPAA statutes.

## 7. Conclusion

This report has sought to present and discuss the penetration test results of https://bookacheckup.co.uk/index.php in regards to both GDPR and HIPAA security statutes. The testing process and vulnerabilities unconcovered have been listed, and security compliance with GDPR and HIPAA analysed. Recommendations for technological improvements and vulnerability mitigation for compliance have been recommended.

## 8. Appendices

### 8.1 Appendix I

*Table 3: Full List of Information Vulnerabilities*

| Vulnerability | Parameter | Instance Count |
|---|---|---|
| Retrieved from cache | HTTP/1.1 | 1612 |
| Cookie poisoning | CSRF token | 128 |
| HTTP | Web servers, CGI abuses | 47 |
| Re-examine cache-control directives | Cache-control | 33 |
| Nessus | Port scanners | 28 |
| IETF Md5 | General | 24 |
| Service detection | Service detection | 24 |
| TLS | General, misc. | 16 |
| User agent fuzzer | Header user-agent | 12 |
| Web application cookies are expired | Web servers | 9 |
| Web application cookies not marked secure | Web servers | 9 |
| OpenSSL detection | Service detection | 4 |
| DNS | DNS | 3 |
| CGI generic injectable Parameter | CGI abuses | 3 |
| CGI generic tests load estimation | CGI abuses | 3 |
| CGI Generic tests timeout | CGI abuses | 3 |
| External URLs | Web servers | 3 |
| MantisBT detection | CGI abuses | 3 |
| SMTP server detection | Service detection | 3 |
| Web application potentially sensitive CGI parameter detection | CGI abuses | 3 |
| Web application sitemap | Web servers | 3 |
| Web mirroring | Web servers | 3 |
| ISC Bind | DNS | 2 |
| Apache HTTP server version | Web servers | 2 |
| IMAP service banner retrieval | Service detection | 2 |
| Mailman detection | CGI abuses | 2 |

| | | |
|---|---|---|
| POP server detection | Service detection | 2 |
| Protected web page detection | Web servers | 2 |
| SMTP service STARTTLS command support | SMTP problems | 2 |
| Strict transport security detection | Service detection | 2 |
| Web server detection (HTTP/1.1) | Service detection | 2 |
| Additional DNS hostnames | General | 1 |
| Common platform enumeration | General | 1 |
| Device type | General | 1 |
| FTP server detection | Service detection | 1 |
| FTP service AUTH TLS command support | FTP | 1 |
| Nessus scan information | Settings | 1 |
| Non-compliant strict transport security | Service detection | 1 |
| Open port re-check | General | 1 |
| OS identification | General | 1 |
| PostgreSQL server detection | Service detection | 1 |
| Service detection: 3 ASCII digit code responses | Service detection | 1 |
| SSL certificate chain contains certificates expiring soon | Misc. | 1 |
| Traceroute information | General | 1 |
| WebDAV detection | Web servers | 1 |
| Charset mismatch | HTTP content-type header | 1 |
| Information disclosure – sensitive information | CSRF token | 1 |
| Information disclosure – suspicious comments | Admin | 1 |

## 9. References

Adobe. (2021) *Cross Domain Configuration — Acrobat Desktop Application Security Guide*. [online] Available at: https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/xdomain.html [Accessed 6 Mar. 2023].

Aharoni, M., Kearns, D., Kennedy, D., & O'Gorman, F. (2011) Metasploit: The Penetration Tester's Guide. San Francisco: No Starch Press.

Akbar, M.F. (2022) *Server-Side Request Forgery to Internal SMTP Access*. [online] Medium. Available at: https://infosecwriteups.com/server-side-request-forgery-to-internal-smtp-access-dea16fe37ed2 [Accessed 6 Mar. 2023].

Beagle (2021) *Vulnerable Javascript Library*. [online] Available at: https://beaglesecurity.com/blog/vulnerability/vulnerable-javascript-library.html.

Bhattacharya, A. (2021) *Why older TLS protocols are unsafe for your organization?* [online] Encryption Consulting. Available at: https://www.encryptionconsulting.com/why-should-organizations-avoid-older-tls-protocols/.

Bocetta, S. (2018) *6 Simple Ways To Protect Your Website From Attackers*. [online] Available at: https://www.acunetix.com/blog/articles/6-simple-ways-to-protect-your-website-from-attackers/.

Chauhan, A.S. (2018) Practical Network Scanning: Capture Network Vulnerabilities Using Standard Tools Such as Nmap and Nessus. Mumbai, IN: PACKT Publishing Limited.

Cloudflare (2023) *What is IMAP?* [online] cloudflare.com. Available at: https://www.cloudflare.com/learning/email-security/what-is-imap/.

Ecylabs. (2023). *eCyLabs: Website Security Platform*. [online] Available at: https://ecylabs.com/blog/2021/06/21/what-happens-if-timestamp-gets-disclosed/.

GDPR (2018) *General Data Protection Regulation (GDPR)*. [online] General Data Protection Regulation (GDPR). Available at: https://gdpr-info.eu/.

Hacktricks. (2023) *5432, 5433 - Pentesting Postgresql - HackTricks*. [online] Available at: https://book.hacktricks.xyz/network-services-pentesting/pentesting-postgresql [Accessed 6 Mar. 2023].

Health Insurance Portability and Accountability Act of 1996 (1996) govinfo.gov. Government of the United States of America. Available at: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf (Accessed: February 13, 2023).

IBM. (2021) *Information Disclosure Attacks*. [online] Available at: https://www.ibm.com/docs/en/snips/4.6.0?topic=categories-information-disclosure-attacks.

IBM. (2022). *Vulnerability: Cookie without SameSite attribute*. [online] Available at:

https://www.ibm.com/docs/en/cdfsp/7.6.1.x?topic=checklist-vulnerability-cookie-without-samesite-attribute.

IBM. (2023) *Vulnerability: Server leaks information*. [online] Available at: https://www.ibm.com/docs/en/control-desk/7.6.1.x?topic=checklist-vulnerability-server-leaks-information [Accessed 6 Mar. 2023].

Invicti. (2023) *Insecure Transportation Security Protocol Supported (TLS 1.0)*. [online] Available at: https://www.invicti.com/web-vulnerability-scanner/vulnerabilities/insecure-transportation-security-protocol-supported-tls-10/.

Johansen, A. G. (2021) *What is a firewall? Firewalls explained and why you need one*. [online] Available at: https://us.norton.com/blog/emerging-threats/what-is-firewall.

Kali Linux. (2022) *whatweb | Kali Linux Tools*. [online] Available at: https://www.kali.org/tools/whatweb/.

Kali Linux. (2023) *zaproxy | Kali Linux Tools*. [online] Available at: https://www.kali.org/tools/zaproxy/.

Kaur, G. & Kaur, N. (2017) "Penetration Testing – Reconnaissance with NMAP Tool," International Journal of Advanced Research in Computer Science, 8(3): 844–846.

Kiprin, B. (2021) *What is the SWEET32 Attack | Crashtest Security*. [online] Available at: https://crashtest-security.com/prevent-ssl-sweet32/.

Kovacs, E. (2021) *Serious Vulnerability Found in Imunify360 Web Server Security Product*. [online] SecurityWeek. Available at: https://www.securityweek.com/serious-vulnerability-found-imunify360-web-server-security-product/ [Accessed 6 Mar. 2023].

Mitre. (2023a) *CAPEC - Common Attack Pattern Enumeration and Classification (CAPEC$^{TM}$)*. [online] Available at: https://capec.mitre.org/.

Mitre. (2023b) *CWE - CWE-352: Cross-Site Request Forgery (CSRF) (3.4.1)*. [online] Mitre.org. Available at: https://cwe.mitre.org/data/definitions/352.html.

Mitre. (2023c). *CAPEC - CAPEC-102: Session Sidejacking (Version 3.9)*. [online] Available at: https://capec.mitre.org/data/definitions/102.html [Accessed 6 Mar. 2023].

Mozilla. (2023a) *Strict-Transport-Security - HTTP | MDN*. [online] Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security.

Mozilla. (2023b) *X-Content-Type-Options*. [online] Available at: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Content-Type-Options.

Natarajan, V. S. (n.d.) *Content Security Policy Prevents XSS*. [online] MST Solutions. Available at: https://www.mstsolutions.com/technical/preventing-xss-with-%E2%80%8Bcontent-security-policy/.

Nidecki, T. A. (n.d) *Cookie Security Flags | Learn AppSec*. [online] Available at: https://www.invicti.com/learn/cookie-security-flags/ [Accessed 6 Mar. 2023].

OWASP (2023) *OWASP Top Ten*. [online] Owasp.org. Available at: https://owasp.org/www-project-top-ten/.

Pinto, M. & Stuttard, D. (2011) The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. 2nd Ed. Indianapolis, USA: Wiley.

Schrader, D. (2022) *Common Open Port Vulnerabilities List*. [online] https://blog.netwrix.com/. Available at: https://blog.netwrix.com/2022/08/04/open-port-vulnerabilities-list/.

SpeedGuide. (2023) *Port 2525 (tcp/udp)*. [online] Available at: https://www.speedguide.net/port.php?port=2525 [Accessed 6 Mar. 2023].

Synk. (2023a) B*ootstrap 4.0.0 Vulnerabilities | Snyk*. [online] Available at: https://security.snyk.io/package/npm/bootstrap/4.0.0 [Accessed 6 Mar. 2023].

Synk. (2023b) JQ*uery 1.12.4 Vulnerabilities | Snyk*. [online] Available at: https://security.snyk.io/package/npm/jquery/1.12.4.

Tenable. (2017) *Web Application Potentially Vulnerable to Clickjacking*. [online] Available at: https://www.tenable.com/plugins/nessus/85582 [Accessed 6 Mar. 2023].

Tenable. (2021a) *SMTP Service Cleartext Login Permitted*. [online] Available at: https://www.tenable.com/plugins/nessus/54582.

Tenable. (2021b) *Web Server Allows Password Auto-Completion*. [online] Available at: https://www.tenable.com/plugins/nessus/42057 [Accessed 6 Mar. 2023].

Tunggal, A. T. (2023) *What is an Open Port? | Definition & Free Checking Tools for 2022 | UpGuard*. [online] Available at: https://www.upguard.com/blog/open-port#toc-1.

Vasudevan, T. (2022). *How an Attacker Could Use Instance Metadata to Breach Your App in AWS*. [online] Skyhigh Security. Available at: https://www.skyhighsecurity.com/en-us/about/newsroom/blogs/threat-research/how-an-attacker-could-use-instance-metadata-to-breach-aws.html [Accessed 6 Mar. 2023].

Vulncat. (2023) *Software Security | Mail Command Injection: POP3*. [online] Available at: https://vulncat.fortify.com/en/detail?id=desc.dataflow.java.mail_command_injection_pop3 [Accessed 6 Mar. 2023].

ZAP. (2023a) *OWASP ZAP – Active Scan Rules - Beta*. [online] Available at: https://www.zaproxy.org/docs/desktop/addons/active-scan-rules-beta/ [Accessed 6 Mar. 2023].

ZAP. (2023b) *OWASP ZAP – Hidden File Found*. [online] Available at: https://www.zaproxy.org/docs/alerts/40035/ [Accessed 6 Mar. 2023].

ZAP. (2023c) *OWASP ZAP – Server Leaks its Webserver Application via 'Server' HTTP Response Header Field*. [online] Available at: https://www.zaproxy.org/docs/alerts/10036-1/ [Accessed 6 Mar. 2023].