1. Introduction (50 words)
    - bookacheckup.co.uk/index.php = healthcare website pen tested for vulnerabilities
    - this report will discuss:
        - compliance standards
        - meth of pentest
        - results
        - analysis
            - comp to standards
            - mitigations for comp

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
- testing methodologies utilized
- testing results
- vulnerability analysis
- standards compliance
- recommended mitigations

pertaining to the completed test.

2. Lit review (100 words)
    - GDPR
    - HIPAA
    - NIST

3. Methodology (100 words)
    - NMAP
    - NESSUS
    - ZAPROXY

4. Results (600 words)
    - port types
    - Vuln types
    - Info vulns
    - Found vulns

5. Analysis (400 words)
    - standards compare
    - mitigations for compliance
    - info security

6. Conclusion (50 words)

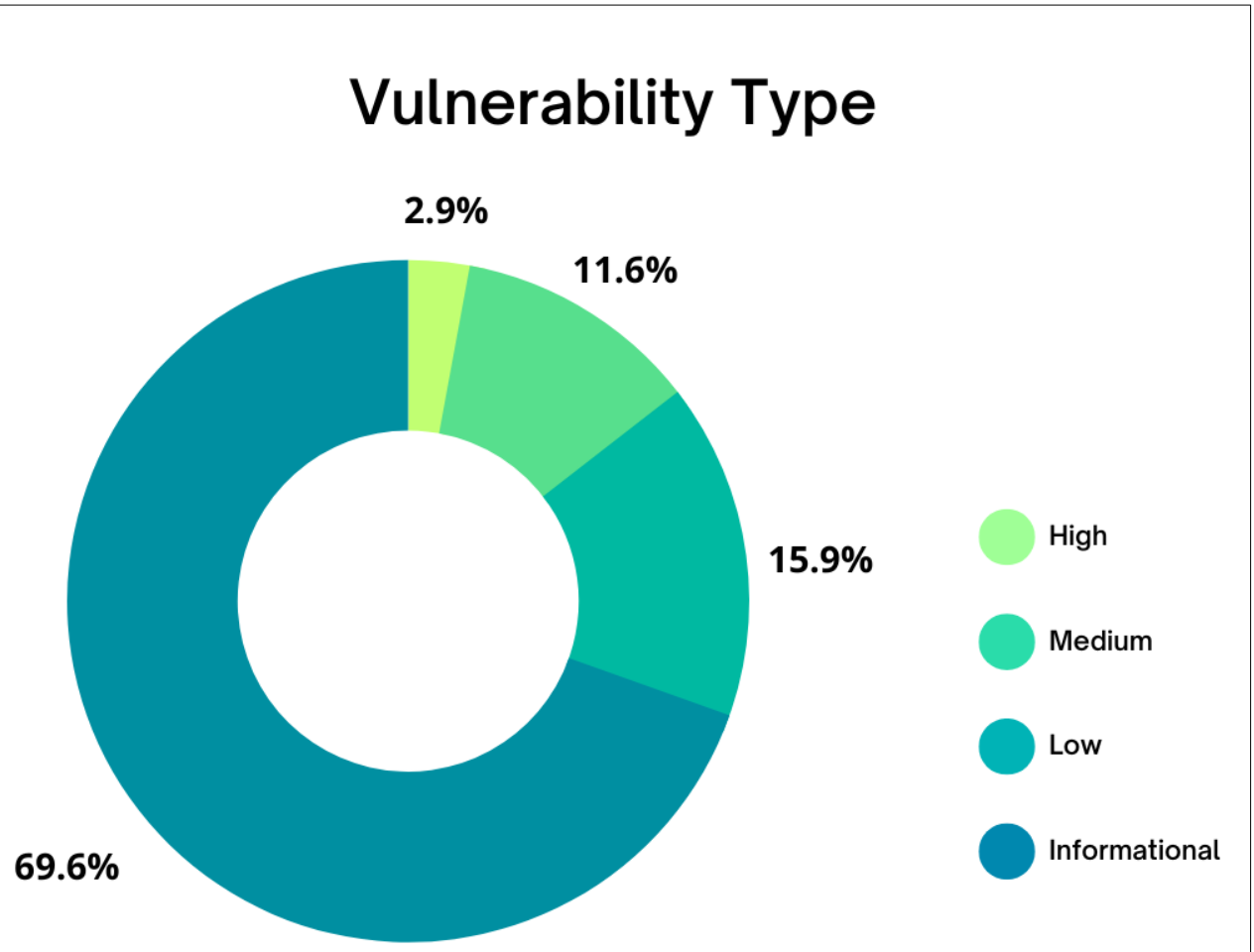

Figure 1: Vulnerability Type Percentage

Table 1: Found Vulnerabilities

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

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

Table 2: Found 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

Table 3: Vulnerable Ports

Port	Service	State
21/tcp	ftp	Open
24/tcp	priv-mail	Filtered
25/tcp	smtp	Open
53/tcp	domain	Open
80/tcp	http	Open
110/tcp	pop3	Open
143/tcp	imap	Open
443/tcp	https	Open
465/tcp	smtps	Open
587/tcp	submission	Open
993/tcp	imaps	Open
995/tcp	pop3s	Open
2525/tcp	ms-v-worlds	Open

3306/tcp	mysql	Open
3389/tcp	ms-wbt-server	Filtered
5432/tcp	postgresql	Open