- What Operating System does the web site utilise?
  - ➔ RedHat Enterprise Linux 7 (nmap –A command)

- What web server software is it running?
  - ➔ Web Server: Apache (nmap –A command)

- Is it running a CMS (Wordpress, Drupal, etc?)
  - ➔ Loaded Commerce Community Edition v6.6 by Softaclous (whatweb)

- What protection does it have (CDN, Proxy, Firewall?)
  - ➔ imunify360-webshield/1.18 (whatweb)

- Where is it hosted?
  - ➔ Amsterdam, Netherlands, nl1-ss5.a2hosting.com (nmap –A command)

- Does it have any open ports?
  - ➔

```
─$ nmap 68.66.247.187
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-12 06:11 EST
Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)
Host is up (0.049s latency).
Not shown: 986 filtered tcp ports (no-response)
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  ms-v-worlds
3306/tcp open  mysql
5432/tcp open  postgresql
```

- Does the site have any known vulnerabilities?
  - ➔ CVE-2020-7676, CVE-2020-11023, CVE-2020-11022 (OWASP-ZAP)
  - ➔ ssltrust.com : BREACH; Medium: potentially VULNERABLE, gzip HTTP compression detected - only supplied '/' tested

- What versions of software is it using? Are these patched so that they are up to date?
    - ➔ AngularJS v1.6.9; jquery v.3.4.1
    - ➔ Update version for AngularJS: 1.8.3 (12.10.2020) & jquery: 3.6.0 (2.03.2020)

Detailed scan results for loadedwithstuff.co.uk / 68.66.247.187 :

```
nmap 68.66.247.187 -p-

Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-12 04:55 EST

Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)

Host is up (0.033s latency).

Not shown: 65527 filtered tcp ports (no-response), 1 filtered tcp ports (host-unreach)

PORT      STATE SERVICE

80/tcp    open  http

443/tcp   open  https

2077/tcp  open  tsrmagt

2086/tcp  open  gnunet

2525/tcp  open  ms-v-worlds

52223/tcp open  unknown

52224/tcp open  unknown


Nmap done: 1 IP address (1 host up) scanned in 4016.84 seconds


–$ nmap 68.66.247.187

Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-12 06:11 EST

Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)

Host is up (0.049s latency).

Not shown: 986 filtered tcp ports (no-response)

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  ms-v-worlds
3306/tcp open  mysql
5432/tcp open  postgresql
```

```
Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)
Host is up (0.014s latency).
Not shown: 966 filtered tcp ports (no-response)
PORT     STATE  SERVICE        VERSION
21/tcp    open   tcpwrapped
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=*.a2hosting.com/organizationName=A2 Hosting, Inc./stateOrProvinceName=Michigan/countryName=US
| Subject Alternative Name: DNS:*.a2hosting.com, DNS:a2hosting.com
| Not valid before: 2021-05-05T00:00:00
|_Not valid after:  2022-06-05T23:59:59
```

```
25/tcp    open   tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
53/tcp    open   tcpwrapped
| dns-nsid:
|_  bind.version: 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.8
80/tcp    open   tcpwrapped
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache
110/tcp   open   tcpwrapped
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_pop3-capabilities: RESP-CODES PIPELINING UIDL TOP USER CAPA SASL(PLAIN LOGIN) STLS AUTH-RESP-CODE
| ssl-cert: Subject: commonName=*.a2hosting.com/organizationName=A2 Hosting, Inc./stateOrProvinceName=Michigan/countryName=US
| Subject Alternative Name: DNS:*.a2hosting.com, DNS:a2hosting.com
| Not valid before: 2021-05-05T00:00:00
|_Not valid after:  2022-06-05T23:59:59
|_ssl-date: TLS randomness does not represent time
125/tcp   closed locus-map
143/tcp   open   tcpwrapped
| ssl-cert: Subject: commonName=*.a2hosting.com/organizationName=A2 Hosting, Inc./stateOrProvinceName=Michigan/countryName=US
| Subject Alternative Name: DNS:*.a2hosting.com, DNS:a2hosting.com
| Not valid before: 2021-05-05T00:00:00
|_Not valid after:  2022-06-05T23:59:59
|_ssl-date: TLS randomness does not represent time
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_imap-ntlm-info: ERROR: Script execution failed (use -d to debug)
443/tcp   open   ssl/tcpwrapped
```

```
|_http-title: Did not follow redirect to https:///
| ssl-cert: Subject: commonName=tech-sourcery.co.uk
| Subject Alternative Name: DNS:tech-sourcery.co.uk, DNS:autodiscover.tech-sourcery.co.uk, DNS:cpanel.tech-sourcery.co.uk, DNS:cpcalendars.tech-sourcery.co.uk, DNS:cpcontacts.tech-sourcery.co.uk, DNS:mail.tech-sourcery.co.uk, DNS:webdisk.tech-sourcery.co.uk, DNS:webmail.tech-sourcery.co.uk, DNS:www.tech-sourcery.co.uk
| Not valid before: 2021-12-12T00:00:00
|_Not valid after:  2022-03-12T23:59:59
|_ssl-date: TLS randomness does not represent time
|_http-server-header: Apache
465/tcp   open   tcpwrapped
| smtp-commands: nl1-ss5.a2hosting.com Hello ip-95-223-75-227.hsi16.unitymediagroup.de [95.223.75.227], SIZE 78643200, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, HELP
|_ Commands supported: AUTH HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
| ssl-cert: Subject: commonName=*.a2hosting.com/organizationName=A2 Hosting, Inc./stateOrProvinceName=Michigan/countryName=US
| Subject Alternative Name: DNS:*.a2hosting.com, DNS:a2hosting.com
| Not valid before: 2021-05-05T00:00:00
|_Not valid after:  2022-06-05T23:59:59
587/tcp   open   tcpwrapped
| ssl-cert: Subject: commonName=*.a2hosting.com/organizationName=A2 Hosting, Inc./stateOrProvinceName=Michigan/countryName=US
| Subject Alternative Name: DNS:*.a2hosting.com, DNS:a2hosting.com
| Not valid before: 2021-05-05T00:00:00
|_Not valid after:  2022-06-05T23:59:59
| smtp-commands: nl1-ss5.a2hosting.com Hello ip-95-223-75-227.hsi16.unitymediagroup.de [95.223.75.227], SIZE 78643200, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP
|_ Commands supported: AUTH STARTTLS HELO EHLO MAIL RCPT DATA BDAT NOOP QUIT RSET HELP
993/tcp   open   tcpwrapped
|_ssl-date: TLS randomness does not represent time
```

```
| ssl-cert: Subject: commonName=*.a2hosting.com/organizationName=A2 Hosting,
Inc./stateOrProvinceName=Michigan/countryName=US
| Subject Alternative Name: DNS:*.a2hosting.com, DNS:a2hosting.com
| Not valid before: 2021-05-05T00:00:00
|_Not valid after:  2022-06-05T23:59:59
995/tcp   open   tcpwrapped
| ssl-cert: Subject: commonName=*.a2hosting.com/organizationName=A2 Hosting,
Inc./stateOrProvinceName=Michigan/countryName=US
| Subject Alternative Name: DNS:*.a2hosting.com, DNS:a2hosting.com
| Not valid before: 2021-05-05T00:00:00
|_Not valid after:  2022-06-05T23:59:59
|_ssl-date: TLS randomness does not represent time
2525/tcp  open   tcpwrapped
3306/tcp  open   tcpwrapped
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.23-MariaDB-cll-lve
|   Thread ID: 8742714
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, IgnoreSigpipes, Speaks41ProtocolNew, ODBCClient,
LongColumnFlag, SupportsLoadDataLocal, FoundRows, SupportsTransactions, ConnectWithDatabase,
Speaks41ProtocolOld, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis,
SupportsCompression, InteractiveClient, SupportsMultipleStatments, SupportsAuthPlugins,
SupportsMultipleResults
|   Status: Autocommit
|   Salt: a(D^+Y^ONz>bS[LN"[&K
|_  Auth Plugin Name: mysql_native_password
|_sslv2: ERROR: Script execution failed (use -d to debug)
7778/tcp  closed interwise
9876/tcp  closed sd
```

```
32773/tcp closed sometimes-rpc9
32774/tcp closed sometimes-rpc11
32783/tcp closed unknown
32785/tcp closed unknown
38292/tcp closed landesk-cba
41511/tcp closed unknown
42510/tcp closed caerpc
48080/tcp closed unknown
49156/tcp closed unknown
49158/tcp closed unknown
49159/tcp closed unknown
49160/tcp closed unknown
49163/tcp closed unknown
49165/tcp closed unknown
49175/tcp closed unknown
49176/tcp closed unknown
50000/tcp closed ibm-db2
55555/tcp closed unknown
OS fingerprint not ideal because: Didn't receive UDP response. Please try again with -sSU
No OS matches for host
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   11.34 ms 10.0.2.2
2   11.41 ms 68.66.247.187.static.a2webhosting.com (68.66.247.187)
```

```
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 111.15 seconds
```

```
–# nmap 68.66.247.187 -O

Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-16 07:38 EST

Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)

Host is up (0.013s latency).

Not shown: 986 filtered tcp ports (no-response)

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  ms-v-worlds

3306/tcp open  mysql

5432/tcp open  postgresql

Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
```

```
Device type: bridge|general purpose

Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (92%)

OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu

Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (92%)
```

```
–# nmap 68.66.247.187 -A

Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-16 07:40 EST

Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)

Host is up (0.0032s latency).

Not shown: 986 filtered tcp ports (no-response)

PORT     STATE SERVICE    VERSION

21/tcp   open  ftp        Pure-FTPd

25/tcp   open  smtp?

|_smtp-commands: Couldn't establish connection on port 25

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)

|_http-title: Site doesn't have a title (application/octet-stream).

|_http-server-header: imunify360-webshield/1.18

110/tcp  open  pop3       Dovecot pop3d

|_sslv2: ERROR: Script execution failed (use -d to debug)

|_ssl-date: ERROR: Script execution failed (use -d to debug)

|_tls-alpn: ERROR: Script execution failed (use -d to debug)

|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)

|_ssl-cert: ERROR: Script execution failed (use -d to debug)

143/tcp  open  imap       Dovecot imapd
```

```
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_imap-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_imap-capabilities: AUTH=LOGINA0001 IDLE SASL-IR capabilities ID OK AUTH=PLAIN Pre-login listed more have post-login ENABLE LOGIN-REFERRALS LITERAL+ IMAP4rev1 NAMESPACE STARTTLS
443/tcp  open  ssl/http   Apache httpd (W3 Total Cache/0.9.4.6.4)
| tls-alpn:
|   h2
|_  http/1.1
|_ssl-date: TLS randomness does not represent time
|_http-server-header: imunify360-webshield/1.18
| tls-nextprotoneg:
|   h2
|_  http/1.1
| ssl-cert: Subject: commonName=tech-sourcery.co.uk
| Subject Alternative Name: DNS:tech-sourcery.co.uk, DNS:autodiscover.tech-sourcery.co.uk, DNS:cpanel.tech-sourcery.co.uk, DNS:cpcalendars.tech-sourcery.co.uk, DNS:cpcontacts.tech-sourcery.co.uk, DNS:mail.tech-sourcery.co.uk, DNS:webdisk.tech-sourcery.co.uk, DNS:webmail.tech-sourcery.co.uk, DNS:www.tech-sourcery.co.uk
| Not valid before: 2021-12-12T00:00:00
|_Not valid after:  2022-03-12T23:59:59
|_http-title: Site doesn't have a title (text/html).
465/tcp  open  ssl/smtp   Exim smtpd 4.94.2
|_smtp-commands: nl1-ss5.a2hosting.com Hello ip-95-223-75-200.hsi16.unitymediagroup.de [95.223.75.200], SIZE 78643200, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, HELP
587/tcp  open  smtp       Exim smtpd 4.94.2
|_smtp-ntlm-info: ERROR: Script execution failed (use -d to debug)
```

```
|_smtp-commands: nl1-ss5.a2hosting.com Hello ip-95-223-75-200.hsi16.unitymediagroup.de [95.223.75.200], SIZE 78643200, 8BITMIME, PIPELINING, PIPE_CONNECT, AUTH PLAIN LOGIN, STARTTLS, HELP

993/tcp  open  ssl/imap   Dovecot imapd

995/tcp  open  ssl/pop3   Dovecot pop3d

|_pop3-capabilities: UIDL PIPELINING AUTH-RESP-CODE TOP SASL(PLAIN LOGIN) USER CAPA RESP-CODES

2525/tcp open  smtp       Exim smtpd 4.94.2

|_smtp-commands: Couldn't establish connection on port 2525

3306/tcp open  mysql      MySQL 5.5.5-10.3.23-MariaDB-cll-lve

|_ssl-cert: ERROR: Script execution failed (use -d to debug)

|_tls-alpn: ERROR: Script execution failed (use -d to debug)

|_ssl-date: ERROR: Script execution failed (use -d to debug)

|_sslv2: ERROR: Script execution failed (use -d to debug)

|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)

5432/tcp open  postgresql PostgreSQL DB 9.6.0 or later

| fingerprint-strings:

|   SMBProgNeg:

|     SFATAL

|     VFATAL

|     C0A000

|     Munsupported frontend protocol 65363.19778: server supports 1.0 to 3.0

|     Fpostmaster.c

|     L2050

|_    RProcessStartupPacket

|_ssl-cert: ERROR: Script execution failed (use -d to debug)

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=1/16%Time=61E4122D%P=x86_64-pc-linux-gnu%r(SM

SF:BProgNeg,8C,"E\0\0\0\x8bSFATAL\0VFATAL\0C0A000\0Munsupported\x20fronten
SF:d\x20protocol\x2065363\.19778:\x20server\x20supports\x201\.0\x20to\x203
SF:\.0\0Fpostmaster\.c\0L2050\0RProcessStartupPacket\0\0");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%), Bay Networks embedded (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: nl1-ss5.a2hosting.com; OS: Linux; CPE: cpe:/o:redhat:enterprise_linux:7

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.11 ms 10.0.2.2
2   0.26 ms 68.66.247.187.static.a2webhosting.com (68.66.247.187)

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 814.64 seconds



# nmap 68.66.247.187 -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-16 07:55 EST
Nmap scan report for 68.66.247.187.static.a2webhosting.com (68.66.247.187)
Host is up (0.0055s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
```

```
80/tcp  open  tcpwrapped

443/tcp open  tcpwrapped


Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 18.43 seconds
```

```
–$ whatweb loadedwithstuff.co.uk

http://loadedwithstuff.co.uk [301 Moved Permanently] Apache, Country[UNITED STATES][US],
HTTPServer[Apache], IP[68.66.247.187], PHP[7.3.33],
RedirectLocation[https://loadedwithstuff.co.uk/], Strict-Transport-Security[max-age=63072000;
includeSubDomains], UncommonHeaders[x-content-type-options,upgrade], X-Frame-
Options[SAMEORIGIN], X-Powered-By[PHP/7.3.33]

https://loadedwithstuff.co.uk/ [403 Forbidden] Apache, Bootstrap, Cookies[lcsid], Country[UNITED
STATES][US], Email[sales@example.com,sales@loadedwithstuff.co.uk], HTML5, HTTPServer[Apache],
IP[68.66.247.187], JQuery[3.4.1], MetaGenerator[Loaded Commerce Community Edition v6.6],
PHP[7.3.33], Script[javascript,text/javascript], Strict-Transport-Security[max-age=63072000;
includeSubDomains], Title[Loaded Commerce 6.6  - Powerful Ecommerce Shopping Cart],
UncommonHeaders[x-content-type-options,upgrade], X-Frame-Options[SAMEORIGIN], X-Powered-
By[PHP/7.3.33]
```

OWASP-ZAP:

Vulnerable JS Library: /* AngularJS v1.6.9: The identified library angularjs, version 1.6.9 is vulnerable. (CVE-2020-7676; CVE-2020-11023; CVE-2020-11022)

- ➔ Solution: Please upgrade to the latest version of angularjs.

Absence of Anti-CSRF Tokens: No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

* The victim has an active session on the target site.

* The victim is authenticated via HTTP auth on the target site.

* The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

- ➔ Solution:

Phase: Architecture and Design
Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.
For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Implementation
Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.

Phase: Architecture and Design
Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330).
Note that this can be bypassed using XSS.

Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation.
Note that this can be bypassed using XSS.

Use the ESAPI Session Management control.
This control includes a component for CSRF.

Do not use the GET method for any request that triggers a state change.

Phase: Implementation
Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

Application Error Disclosure: This page contains an error/warning message that may disclose sensitive information like the location of the file that produced the unhandled exception. This information can be used to launch further attacks against the web application. The alert could be a false positive if the error message is found inside a documentation page.

- ➔ Solution:

  Review the source code of this page. Implement custom error pages. Consider implementing a mechanism to provide a unique error reference/identifier to the client (browser) while logging the details on the server side and not exposing them to the user.

Cookie No HttpOnly Flag: A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.

- ➔ Solution: Ensure that the HttpOnly flag is set for all cookies.

Cookie Without Secure Flag: A cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

- ➔ 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.

Cookie without SameSite Attribute: A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.

- ➔ Solution:
  Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s): The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

- ➔ Solution:
  Ensure that your web server, application server, load balancer, etc. is configured to suppress "X-Powered-By" headers.

Timestamp Disclosure – Unix: A timestamp was disclosed by the application/web server – Unix

➔ Solution:
Manually confirm that the timestamp data is not sensitive, and that the data cannot be aggregated to disclose exploitable patterns.

Information Disclosure - Sensitive Information in URL: The request appeared to contain sensitive information leaked in the URL. This can violate PCI and most organizational compliance policies. You can configure the list of strings for this check to add or remove values specific to your environment.

➔ Solution: Do not pass sensitive information in URIs.

Information Disclosure - Suspicious Comments: The response appears to contain suspicious comments which may help an attacker. Note: Matches made within script blocks or files are against the entire content not only comments.

➔ Solution: Remove all comments that return information that may help an attacker and fix any underlying problems they refer to.

```
# nmap -sF -F loadedwithstuff.co.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-21 07:07 EST
Nmap scan report for loadedwithstuff.co.uk (68.66.247.187)
Host is up (0.0026s latency).
rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com
All 100 scanned ports on loadedwithstuff.co.uk (68.66.247.187) are in ignored states.
Not shown: 100 closed tcp ports (reset)

Nmap done: 1 IP address (1 host up) scanned in 0.65 seconds
```

```
–# nmap -sU -F loadedwithstuff.co.uk
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-21 07:09 EST
```

```
Nmap scan report for loadedwithstuff.co.uk (68.66.247.187)

Host is up (0.0059s latency).

rDNS record for 68.66.247.187: 68.66.247.187.static.a2webhosting.com

Not shown: 99 open|filtered udp ports (no-response)

PORT   STATE SERVICE

53/udp open  domain


Nmap done: 1 IP address (1 host up) scanned in 18.86 seconds
```

```
$ sqlmap loadedwithstuff.co.uk

        ___

       __H__

 ___ ___[)]_____ ___ ___  {1.5.11#stable}

|_ -| . [(]     | .'| . |

|___|_  [)]_|_|_|__,|  _|

      |_|V...       |_|   https://sqlmap.org


[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is
the end user's responsibility to obey all applicable local, state and federal laws. Developers assume
no liability and are not responsible for any misuse or damage caused by this program


[*] starting @ 07:47:47 /2022-01-21/


[07:47:47] [INFO] testing connection to the target URL

got a 301 redirect to 'https://loadedwithstuff.co.uk/'. Do you want to follow? [Y/n] y

you have not declared cookie(s), while server wants to set its own
('lcsid=5bafe97d2d8...1c34f201a6'). Do you want to use those [Y/n] y

[07:48:32] [INFO] checking if the target is protected by some kind of WAF/IPS
```

```
[07:48:33] [CRITICAL] heuristics detected that the target is protected by some kind of WAF/IPS

are you sure that you want to continue with further target testing? [Y/n] y

[07:48:52] [WARNING] please consider usage of tamper scripts (option '--tamper')

[07:48:52] [INFO] testing if the target URL content is stable

[07:48:53] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are advised to rerun with '--forms --crawl=2'

[07:48:53] [WARNING] HTTP error codes detected during run:

403 (Forbidden) - 2 times


[*] ending @ 07:48:53 /2022-01-21/
```

```
$ searchsploit loadedwithstuff.co.uk

Exploits: No Results

Shellcodes: No Results
```