

# Report URI

# Penetration Testing Report

R2281

Application and API Assessment

17/11/2021

Author: Jose Barrera

26a The Downs, Altrincham, Cheshire, WA14 2PU

Tel: +44 (0)161 233 0100

Web: [www.pentest.co.uk](http://www.pentest.co.uk)



## Table of Contents

1	Document Revision History.....	3
2	Introduction .....	4
3	Executive Summary .....	5
4	Recommended Actions.....	9
5	Technical Findings .....	10
5.1	Account Enumeration.....	10
5.2	Excessive Session Timeout .....	14
5.3	Vulnerabilities in Outdated Dependencies Detected .....	16
5.4	HTTP Security Headers Not Enabled .....	18
5.5	Insecure SSL Certificates .....	21
6	Additional Information .....	23

## 1 Document Revision History

Name	Date	Version	Comment
Jose Barrera	16/11/2021	0.1	Initial Document
Mark Rowe	16/11/2021	0.2	QA by senior consultant
Jose Barrera	17/11/2021	1.0	Final Draft

## 2 Introduction

Report URI engaged Pentest Limited to undertake this project. This was to gain independent assurance that security controls are in-line with industry best practices.

Report URI was founded to take the pain out of monitoring security policies like CSP and other modern security features. When you can easily monitor what's happening on your site in real time you react faster and more efficiently, allowing you to rectify issues without your users ever having to tell you. The Report URI platform is constantly evolving to help better protect your users.

Report URI are the best real-time monitoring platform for cutting edge web standards. Their experience, focus and exposure allow them to take the hassle out of collecting, processing, and understanding reports, giving you just the information you need.

Report URI have indicated the need for a security test, of their 'Report URI' application to identify vulnerabilities to attacks that could be launched across a computer network and to provide security assurances regarding their systems. Such a test will allow Report URI to undertake remediation efforts and increase their overall security posture.

### 2.1 Scope & Duration

This assessment included the following phase of work:

- Phase 1 – Web application and API assessment of the Report URI application

The duration included 5 days effort (including reporting). Work commenced on 08/11/2021 and concluded on 12/11/2021.

### 2.2 Scenarios Included

The test was performed from a remote attacker's perspective. Test premium accounts were provided. Additionally, the source-code of the application and production servers IP addresses were also provided to allow for in-depth testing that would be hard to perform otherwise within a limited time window.

### 2.3 Target(s)

- <https://report-uri.com>
- <https://cdn.report-uri.com>

## 3 Executive Summary

Pentest performed a remote security assessment of the Report URI application. The Report URI application performed well during the test and had a strong security posture. The website used Cloudflare web application firewall and followed best security-practices and implemented multiple security controls such as anti-automation protections.

Pentest can conclude that the application handled common web application vulnerabilities in a secure manner. This prevented an authenticated attacker from carrying out attacks that could compromise the server or application such as Cross-Site Scripting and SQL Injection.

No trivial to exploit vulnerabilities were detected which would pose a significant risk to the integrity of the server or the confidentiality of data.

The application was affected only by Low-risk vulnerabilities. The identified issues were not immediately exploitable but concern security best practices.

### 3.1 Next Steps

A complete writeup of every issue is available in the body of this report. It includes required steps to confirm and replicate each issue, along with recommended remedial actions. Pentest recommend taking time to review the findings before arranging a triage meeting to determine the order of priority for remedial work. As a rule of thumb:

- **Critical Risk Items** – Address these immediately.
- **High Risk Items** – Address these as soon as possible after any Critical Risks.
- **Medium Risk Items** – Plan to address these within 3 months of discovery.
- **Low and Info Risk Items** – Track these within a risk register and discuss remediation versus acceptance.

If recommendations within this report are followed Pentest believe that the target's security posture will improve.

## 3.2 Caveats

Pentest provides no warranty that the target(s) are now free from other defects. Security is an ever evolving field and consultancy is based on the opinions of the consultant, their understanding of the goals of Report URI as well as their individual experience.

The findings of this project are based on a time-limited assessment and by necessity can only focus on approved targets which are in scope. An attacker would not be constrained by either time or scope limits and could circumvent controls which are impractical to assess via structured penetration testing.

To appropriately secure assets Pentest encourage a cyclical approach to assessment. Each cycle should include:

- **Comprehensive Assessment** – where a full list of findings is produced with the widest scope possible.
- **Focused Verification Testing** – where solutions to the initial assessment's findings are verified.

Depending on how important the target is to the concerns of Report URI, Pentest recommend repeating the cycle every 6-months or 12-months at least.

### 3.3 Risk Categories & Rationales

Pentest use a simple risk categorisation of each vulnerability to focus the triage process at the risks which truly matter. The Common Vulnerability Scoring System (CVSS) is an industry standard formula. It generates a risk score between 0.0 and 10.0.

The table below explains the risk categories and demonstrates rule-of-thumb equivalency with CVSS scores:

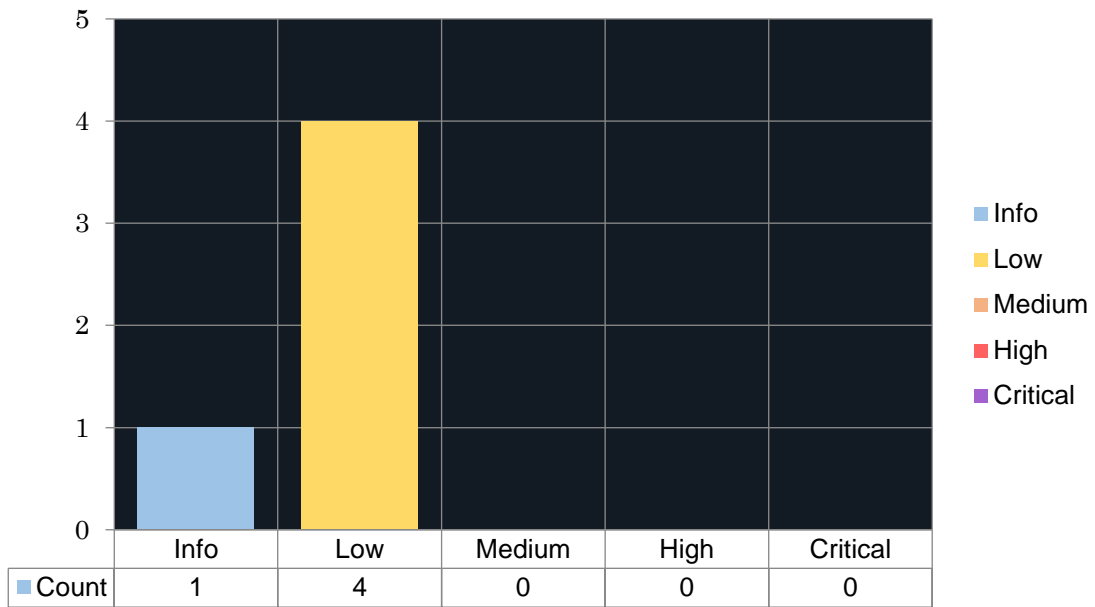
Risk Category	CVSS Score	Rationales
<b>Critical</b>	8.1 – 10.0	Poses a severe risk which is easy to exploit. Begin the process of remediating immediately after the issue has been presented.
<b>High</b>	6.1 – 8.0	Poses a significant risk and can be exploited. Address these as soon as possible after any critical risks have been remediated.
<b>Medium</b>	4.1 – 6.0	Poses an important risk but may be difficult to exploit. Pentest recommends remedial work within 3 months of discovery.
<b>Low</b>	2.1 – 4.0	Poses a minor risk or may be exceedingly difficult to exploit. Address these over the long-term during testing cycles
<b>Info</b>	0.0 – 2.0	Loss of sensitive information, or a discussion point. These are not directly exploitable but may aid an attacker. Remediate these to create a true defence-in-depth security posture,

CVSS is not applicable to all risks. For example, it is incapable of capturing the risk of a “flat network design”. Experience has told us that this is a “high” risk in most cases.

For this reason, the reader may find vulnerabilities which have no CVSS rating in our reports.

We endeavour to provide the reason for omitting the risk score when that is the case, and to provide CVSS by default in all applicable cases.

### 3.4 Visual Summary





## 4 Recommended Actions

ID	Vuln Title	Recommended Action	Risk Category	CVSS
1	<u>Account Enumeration</u>	Return a consistent response time whether the account exists or not	Low	3.4
2	<u>Excessive Session Timeout</u>	Implement a shorter timeout mechanism	Low	1.6
3	<u>Vulnerabilities in Outdated Dependencies Detected</u>	Ensure that components are regularly updated	Low	3.4
4	<u>HTTP Security Headers Not Enabled</u>	Implement available secure header options to elevate the overall security posture of the application	Low	3.1
5	<u>Insecure SSL Certificates</u>	Monitor expiry date of the certificates used by the applications	Info	N/A

## 5 Technical Findings

### 5.1 Account Enumeration

#### 5.1.1 Background

Account Enumeration (also known as User Enumeration) is an issue that allows an unauthenticated/authenticated user to determine a user's account details (such as username or email address) due to information returned by an application.

Oftentimes, it is the discrepancy between responses from applications such as on Forgotten Password pages that allow attackers to determine the validity of user details.

Examples of the types of account enumeration methods are as follows:

- Response discrepancy
- URL redirection
- Forced browsing.

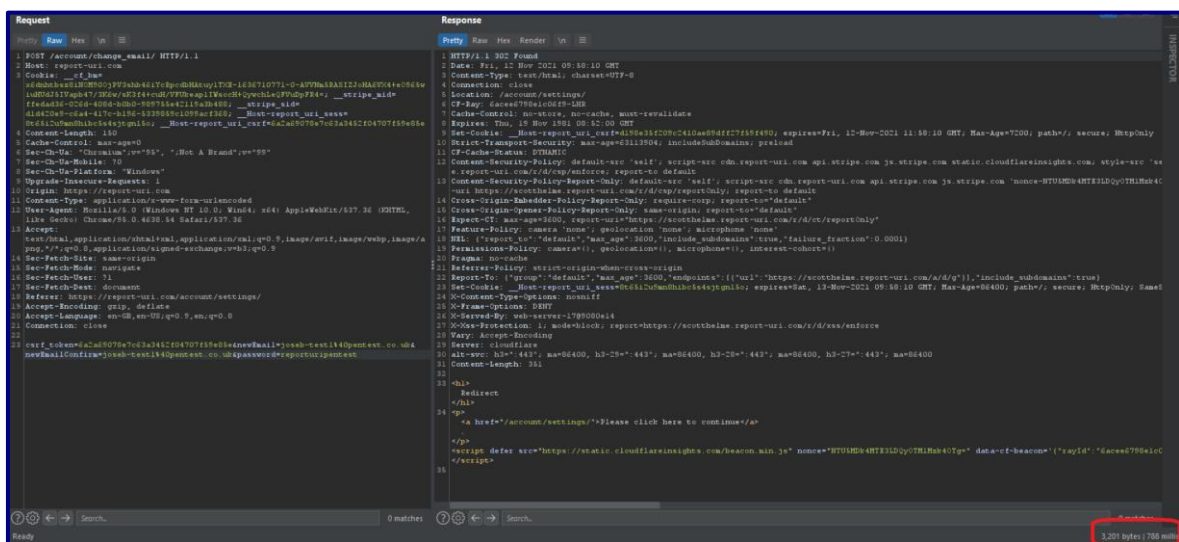
#### 5.1.2 Details

Several methods were identified to check the validity of an account within the system.

##### 5.1.2.1 Change email

The "change email" functionality would return a different response time depending on whether an account existed within the system or not.

The following request was sent to initiate the change email for an existing account (joseb-test1@pentest.co.uk):



```

Request
Raw
Host: report-uri.com
Cookie: __cf_bm=...
Content-Type: application/x-www-form-urlencoded
Accept-Language: en-GB, en-US;q=0.9,en;q=0.8
...

Response
Party
HTTP/1.1 200 OK
Date: Fri, 12 Nov 2021 09:50:10 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 351
...
3,201 bytes / 788 ms
    
```

Figure 15 – Request to change email procedure for a valid account

The response shows the request was successful and took 788 milliseconds to be processed.

Whereas the following request shows an attempt to initiate the process for an account (joseb-test01@pentest.co.uk) which did not exist within the system:

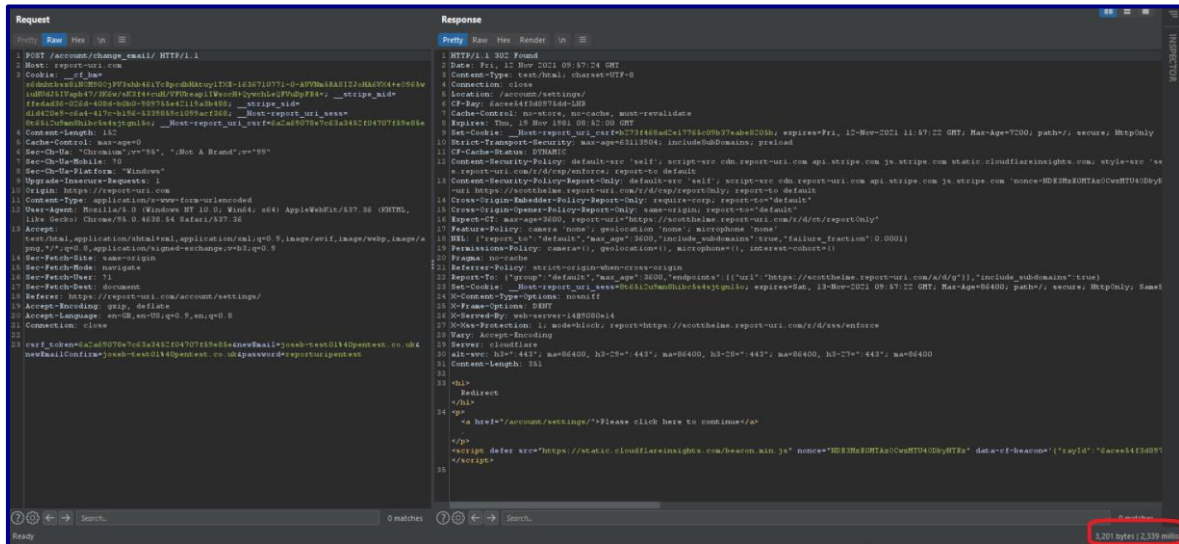


Figure 17 – Request to change email procedure for invalid account

The response shows that the request took 2339 milliseconds to be processed.

Based on the time responses detailed above, an attacker could enumerate user accounts in this manner.

### 5.1.2.2 Login

The “Login” functionality would return a different response depending on whether an account existed within the system or not.

The following request was sent to initiate the login for an existing account (jose.barrera@pentest.co.uk) with an invalid password:

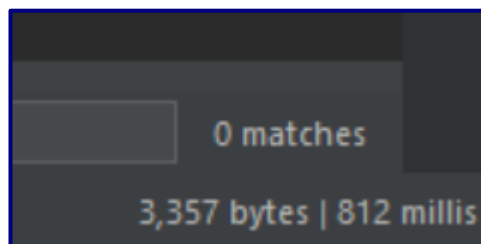


Figure 15 – Request to login procedure for a valid account

The response shows the request took 812 milliseconds to be processed:

Whereas the following request shows an attempt to initiate the process for an account (jose.barrera5555@pentest.co.uk) which did not exist within the system:

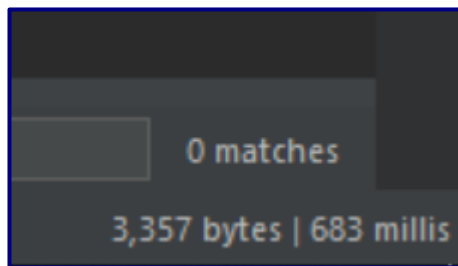


Figure 17 – Request to login procedure for invalid account

The response shows that the account does not exist within the system:

Based on the responses detailed above, an attacker could enumerate user accounts in this manner.

### 5.1.3 Risk Analysis

Risk Category	Low
CVSS	3.4 <a href="#">AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N</a>
Explanation	Whilst being able to determine whether a user exists within the system or not does not directly compromise the application, such behaviour is undesirable. The issue has therefore been rated as low risk.

### 5.1.4 Recommendation

To prevent account enumeration, the application should respond with similar response times to an attacker's enumeration attempts. This prevents an attacker from being able to discern the difference between a valid and invalid account.

### 5.1.5 References

[1]	<a href="#">OWASP: Authentication Cheat Sheet</a>
[2]	<a href="#">Prevent account enumeration on login, reset password and registration pages</a>
[3]	<a href="#">How serious is Username enumeration</a>
[4]	<a href="#">CWE-200: Information Exposure</a>
[5]	<a href="#">CWE-203: Information Exposure Through Discrepancy</a>

### 5.1.6 Affected Item(s)

- <https://report-uri.com>

## 5.2 Excessive Session Timeout

### 5.2.1 Background

Applications should implement timeout functionality and expire active sessions after a period of inactivity. This inactivity period should be related to the sensitivity of the data stored within the application, for example an internet banking application should expire sessions after 5 minutes of inactivity.

This functionality protects the user if they accidentally leave a session logged in on a public device.

### 5.2.2 Details

The application did not implement automatic logout functionality. Once authenticated, the application was still accessible after hours of inactivity. To demonstrate this issue, the consultant requested different resources from the web application using the same session token with a difference of fifteen hours and the session was still valid.

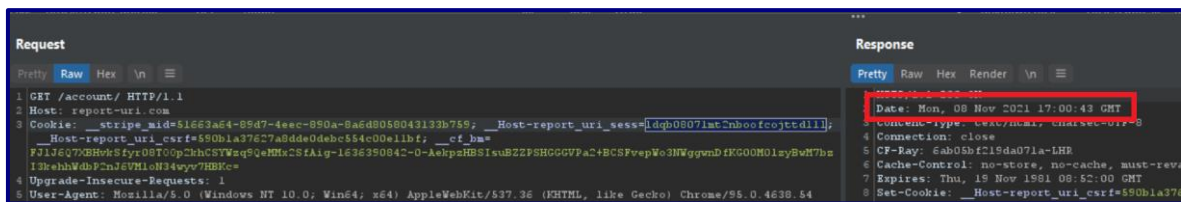


Figure 1 - Excessive session timeout

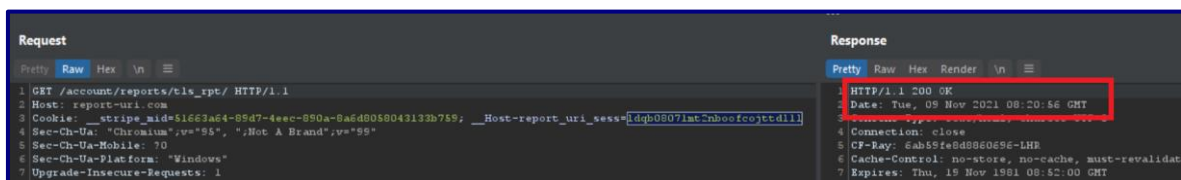


Figure 2 - Excessive session timeout

### 5.2.3 Risk Analysis

Risk Category	Low
CVSS	1.6 <a href="#">AV:P/AC:H/PR:H/UI:N/S:U/C:L/I:N/A:N</a>
Explanation	To exploit this issue, physical access or a well-positioned attacker is required so the risk has been rated as “Low” to reflect that fact.

#### 5.2.4 Recommendation

Pentest recommends that after a period of inactivity, for example, 20 minutes that the session is invalidated, and the user is required to re-authenticate to the application by entering their username and password.

#### 5.2.5 References

[1] [OWASP: Session Management Cheatsheet](#)

#### 5.2.6 Affected Item(s)

- <https://report-uri.com>



## 5.3 Vulnerabilities in Outdated Dependencies Detected

### 5.3.1 Background

Most software products are developed using APIs or libraries provided by 3rd parties. Doing so reduces development time and cost and feeds into the “why re-invent the wheel?” philosophy. Once a component has been integrated into an application it must be upgraded regularly to guard against bugs and remove publicly known vulnerabilities.

Failure to do so can mean that the application itself is at risk of exploitation due to weaknesses that exist in the supporting dependencies. This risk has been captured by the OWASP top 10 2017 project as category A9 labelled “Using Components with known vulnerabilities” defined at reference [\[1\]](#).

### 5.3.2 Details

The Report URI application used an outdated framework that contained publicly disclosed vulnerabilities. The table below details these scripts and their locations within the application:

Software	Version	Location
jQuery UI	1.12.1	<a href="https://cdn.report-uri.com/libs/jqueryui/1.12.1/jquery-ui.min.js">https://cdn.report-uri.com/libs/jqueryui/1.12.1/jquery-ui.min.js</a>
Moment	2.10.3	<a href="https://cdn.report-uri.com/libs/moment.js/2.10.3/moment.min.js">https://cdn.report-uri.com/libs/moment.js/2.10.3/moment.min.js</a>

The following table shows the versions of the affected software and the reported vulnerabilities reference for further reading.

Software	Vulnerabilities
jQuery UI 1.12.1	<a href="#">[3]</a>
Moment 2.10.3	<a href="#">[4]</a>

Several of the known vulnerabilities pertain to injection-related issues such as Cross-Site Scripting (XSS) and Denial of Service (DoS). While the framework versions were vulnerable to XSS, those would be exploitable if specific functions are used by the application.

Due to the time-limited nature of the assessment, all the scripts could not be verified. No exploitable weakness was confirmed. However, using outdated and known vulnerable frameworks is evidence of insecure development practices.



### 5.3.3 Risk Analysis

Risk Category	Low
CVSS	3.4 <a href="#">AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N</a>
Explanation	<p>Several publicly disclosed vulnerabilities could affect the scripts identified above. However, to be exploitable the target site would need to use the vulnerable functionality.</p> <p>Determining if that is the case is time consuming and does not represent value for money for Report URI. This is because there is an official solution available (to patch), and future development of the site may introduce an exploitable vulnerability. Given these factors, Pentest has rated the issue as “Low” severity issue.</p>

### 5.3.4 Recommendation

The immediate recommendation is to download and integrate the latest supported versions of each outdated dependency. Pentest Ltd understands that this would be a significant undertaking due to changes in the underlying APIs and updated versions of the dependencies. As such, to ensure that updated components do not affect the user experience, full User Acceptance Testing (UAT) would need to be carried out.

The advice above would triage the initial problem only and would not prevent the situation from recurring. The long-term solution is to modify the Software Development Life Cycle (SDLC) to ensure that dependencies are regularly updated. OWASP provides a free tool called “dependency-checker” (see reference [2]) which can be integrated into most build processes.

### 5.3.5 References

[1]	<a href="#">OWASP: Top 10 2017 - A9 Using Components with Known Vulnerabilities</a>
[2]	<a href="#">OWASP: OWASP Dependency Check</a>
[3]	<a href="#">jQuery UI 1.12.1 Vulnerabilities</a>
[3]	<a href="#">Moment 2.10.3 Vulnerabilities</a>

### 5.3.6 Affected Item(s)

- <https://cdn.report-uri.com>

## 5.4 HTTP Security Headers Not Enabled

### 5.4.1 Background

Modern web browsers offer several security protections which can be enabled by an application through its HTTP response headers. By default, these options are not enabled making them protections which must be opted into.

The following HTTP security headers are available:

- Strict Transport Security – This header instructs a browser to always visit the site over a secure channel (https).
- Content Security Policy – CSP can be used to restrict where user agents are permitted to source and/or send content from/to. Most commonly used as a protection against all forms of XSS.
- Frame Options – This header helps prevent “click-jacking” attacks.
- X-Content-Type-Options – This header will prevent the browser from interpreting files as something else than declared by the content type in the HTTP headers.

### 5.4.2 Details

The host “cdn.report-uri.com” did not enable the following security HTTP headers:

- Content-Security-Policy
- X-Frame-Options
- X-Content-Type-Options

For example, the following shows the HTTP server request and response from the host that was gathered during the assessment:

```
GET /img/logo.svg HTTP/1.1
Host: cdn.report-uri.com
```

*Figure 3 - HTTP Security Headers Not Enabled - Request*

```
HTTP/1.1 200 OK
Date: Fri, 12 Nov 2021 11:20:44 GMT
Content-Type: image/svg+xml
Connection: close
CF-Ray: 6acf5f6e2a236695-MAD
Access-Control-Allow-Origin: *
Age: 38276
Cache-Control: public, max-age=31536000
ETag: W/"613216b2-fc1"
Expires: Sat, 12 Nov 2022 11:20:44 GMT
Last-Modified: Fri, 03 Sep 2021 12:36:02 GMT
Strict-Transport-Security: max-age=63113904; includeSubDomains; preload
Vary: Accept-Encoding
CF-Cache-Status: HIT
Cross-Origin-Resource-Policy: cross-origin
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
NEL:
{"report_to":"default","max_age":3600,"include_subdomains":true,"failure_fraction":0.00001}
```

```
Report-To:
{"group":"default","max_age":3600,"endpoints":[{"url":"https://scotthelme.report-
uri.com/a/d/g"}],"include_subdomains":true}
Server: cloudflare
alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443";
ma=86400
Content-Length: 4033
```

Figure 4 - HTTP Security Headers Not Enabled – Reponse

As seen in the response below, the server was missing the “X-Frame-Options”, “Content-Security-Policy” and “X-Content-Type-Options” headers.

### 5.4.3 Risk Analysis

Risk Category	Low
CVSS	3.1 <a href="#">AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N</a>
Explanation	The lack of security HTTP headers does not constitute an actual vulnerability but instead a lack of enforcing existing security features in web browsers and so has been rated as a “Low” severity issue.

### 5.4.4 Recommendation

Consider implementing the response headers above where possible. Further reading can be found in the references.

#### 5.4.4.1 Content-Security-Policy

Pentest recommends that the Content Security Policy (CSP) feature is implemented to improve resistance to Cross-site Scripting attacks by:

- Limiting the use of inline scripts
- Limiting the use of inline styles
- Limiting allowed asset sources to trusted locations.

When configured correctly, CSP can mitigate all but the most sophisticated cross-site scripting attacks.

#### 5.4.4.2 Frame-Options

Unless business requirements require the application to be embedded in a third-party application, the web server should include the following X-Frame-Option HTTP header to prevent the pages from being rendered within an iframe and/or only from specified domains:

```
X-Frame-Options: Deny
X-Frame-Options: Allow-From https://approved.domain.com
```

Alternatively, consider using frame-busting JavaScript to prevent the application from being embedded within another web page.

#### 5.4.4.3 X-Content-Type-Options

The web server should issue the following `X-Content-Type-Options` HTTP header:

```
X-Content-Type-Options: nosniff
```

#### 5.4.5 References

- |     |   |
|-----|---|
| [1] | <a href="#">OWASP: Secure Headers Project</a>     |
| [2] | <a href="#">Content Security Policy Reference</a> |

#### 5.4.6 Affected Item(s)

- <https://cdn.report-uri.com>

## 5.5 Insecure SSL Certificates

### 5.5.1 Background

SSL certificates are a small data file that are used to bind a cryptographic key to an organisation's details and are used to aid in establishing encrypted connections to clients. Typically, this would be used in web applications to secure sensitive transmissions such as credit card transactions, data transfer and logins.

SSL certificates are designed to expire after a set period of time (as determined during the certificates creation). This is designed to help ensure the legitimacy of services and websites to protect users against compromise from malicious websites.

Expired SSL certificates will generate warnings within the browser that requires a user to dismiss the warning. Although there no functional security risk associated with expired certificates, as the encryption ciphers are still functional, the warnings could concern users and may result in users being conditioned to dismiss certificate warnings.

### 5.5.2 Details

The host "report-uri.com" was using an SSL certificate issued which is near expiry:

```
Subject: *.report-uri.com
Altnames: DNS:*.report-uri.com, DNS:report-uri.com
Issuer: R3

Not valid before: Oct 7 00:10:45 2021 GMT
Not valid after: Jan 5 00:10:44 2022 GMT
```

The certificate details can be obtained from the SSL scan in Section [SSL/TLS Assessment](#).

### 5.5.3 Risk Analysis

Risk Category	Info
CVSS	N/A

### 5.5.4 Recommendation

All the certificates near expiry should be monitored to ensure that they are renewed before expiry.

### 5.5.5 References

[1]	<a href="#">SSL/TLS Ciphers and Protocols - Deployment Best Practices</a>
[2]	<a href="#">CWE-327: Use of a Broken or Risky Cryptographic Algorithm</a>
[3]	<a href="#">The Dangers of Self-Signed SSL Certificates</a>
[4]	<a href="#">Dangers of SSL Certificate Expiration</a>
[5]	<a href="#">OWASP: Transport Layer Protection Cheat Sheet</a>
[6]	<a href="#">CWE-295: Improper Certificate Validation</a>

### 5.5.6 Affected Item(s)

- <https://report-uri.com>

## 6 Additional Information

### 6.1 WHOIS Database

The WHOIS database stores information about the individual or organisation who owns and manages a domain or IP address range. Attackers will review WHOIS entries trying to find useful information such as names and contact details for employees.

Best practices state that generic contact details should be used such as “whois@domain.com” rather than providing the name of a member of staff.

#### 6.1.1 Entry for Domain: report-uri.com

```
Domain name: report-uri.com
Registry Domain ID: 1651365076_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com
Updated Date: 2021-03-18T07:27:10.01Z
Creation Date: 2011-04-17T11:55:31.00Z
Registrar Registration Expiration Date: 2022-04-17T11:55:31.00Z
Registrar: NAMECHEAP INC
Registrar IANA ID: 1068
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854014545
Reseller: NAMECHEAP INC
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Registry Registrant ID: Redacted for Privacy Purposes
Registrant Name: Redacted for Privacy Purposes
Registrant Organization: Redacted for Privacy Purposes
Registrant Street: Redacted for Privacy Purposes
Registrant City: Redacted for Privacy Purposes
Registrant State/Province: Lancashire
Registrant Postal Code: Redacted for Privacy Purposes
Registrant Country: GB
Registrant Phone: Redacted for Privacy Purposes
Registrant Phone Ext: Redacted for Privacy Purposes
Registrant Fax: Redacted for Privacy Purposes
Registrant Fax Ext: Redacted for Privacy Purposes
Registrant Email: Select Contact Domain Holder link at
https://www.namecheap.com/domains/whois/result?domain=report-uri.com
Registry Admin ID: Redacted for Privacy Purposes
Admin Name: Redacted for Privacy Purposes
Admin Organization: Redacted for Privacy Purposes
Admin Street: Redacted for Privacy Purposes
Admin City: Redacted for Privacy Purposes
Admin State/Province: Redacted for Privacy Purposes
Admin Postal Code: Redacted for Privacy Purposes
Admin Country: Redacted for Privacy Purposes
Admin Phone: Redacted for Privacy Purposes
Admin Phone Ext: Redacted for Privacy Purposes
Admin Fax: Redacted for Privacy Purposes
Admin Fax Ext: Redacted for Privacy Purposes
Admin Email: Select Contact Domain Holder link at
https://www.namecheap.com/domains/whois/result?domain=report-uri.com
Registry Tech ID: Redacted for Privacy Purposes
Tech Name: Redacted for Privacy Purposes
Tech Organization: Redacted for Privacy Purposes
Tech Street: Redacted for Privacy Purposes
Tech City: Redacted for Privacy Purposes
Tech State/Province: Redacted for Privacy Purposes
Tech Postal Code: Redacted for Privacy Purposes
Tech Country: Redacted for Privacy Purposes
Tech Phone: Redacted for Privacy Purposes
Tech Phone Ext: Redacted for Privacy Purposes
```

```
Tech Fax: Redacted for Privacy Purposes
Tech Fax Ext: Redacted for Privacy Purposes
Tech Email: Select Contact Domain Holder link at
https://www.namecheap.com/domains/whois/result?domain=report-uri.com
Name Server: carl.ns.cloudflare.com
Name Server: coco.ns.cloudflare.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2021-11-15T16:23:35.15Z <<<
```



## 6.1.2 Entry for IP Address Range: 104.16.0.0 - 104.31.255.255

```
NetRange: 104.16.0.0 - 104.31.255.255
CIDR: 104.16.0.0/12
NetName: CLOUDFLARENET
NetHandle: NET-104-16-0-0-1
Parent: NET104 (NET-104-0-0-0-0)
NetType: Direct Allocation
OriginAS: AS13335
Organization: Cloudflare, Inc. (CLOUD14)
RegDate: 2014-03-28
Updated: 2021-05-26
Comment: All Cloudflare abuse reporting can be done via
https://www.cloudflare.com/abuse
Ref: https://rdap.arin.net/registry/ip/104.16.0.0

OrgName: Cloudflare, Inc.
OrgId: CLOUD14
Address: 101 Townsend Street
City: San Francisco
StateProv: CA
PostalCode: 94107
Country: US
RegDate: 2010-07-09
Updated: 2021-07-01
Ref: https://rdap.arin.net/registry/entity/CLOUD14

OrgTechHandle: ADMIN2521-ARIN
OrgTechName: Admin
OrgTechPhone: +1-650-319-8930
OrgTechEmail: rir@cloudflare.com
OrgTechRef: https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

OrgNOCHandle: CLOUD146-ARIN
OrgNOCName: Cloudflare-NOC
OrgNOCPhone: +1-650-319-8930
OrgNOCEmail: noc@cloudflare.com
OrgNOCTRef: https://rdap.arin.net/registry/entity/CLOUD146-ARIN

OrgRoutingHandle: CLOUD146-ARIN
OrgRoutingName: Cloudflare-NOC
OrgRoutingPhone: +1-650-319-8930
OrgRoutingEmail: noc@cloudflare.com
OrgRoutingRef: https://rdap.arin.net/registry/entity/CLOUD146-ARIN

OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName: Abuse
OrgAbusePhone: +1-650-319-8930
OrgAbuseEmail: abuse@cloudflare.com
OrgAbuseRef: https://rdap.arin.net/registry/entity/ABUSE2916-ARIN

RNOCHandle: NOC11962-ARIN
RNOCName: NOC
RNOCPhone: +1-650-319-8930
RNOCEmail: noc@cloudflare.com
RNOCRef: https://rdap.arin.net/registry/entity/NOC11962-ARIN

RTechHandle: ADMIN2521-ARIN
RTechName: Admin
RTechPhone: +1-650-319-8930
RTechEmail: rir@cloudflare.com
RTechRef: https://rdap.arin.net/registry/entity/ADMIN2521-ARIN

RAbuseHandle: ABUSE2916-ARIN
RAbuseName: Abuse
RAbusePhone: +1-650-319-8930
RAbuseEmail: abuse@cloudflare.com
RAbuseRef: https://rdap.arin.net/registry/entity/ABUSE2916-ARIN
```

## 6.2 Port Scan Results

To offer a service to other computers, a “port” is made available. Each open port creates a communication channel which can pose a security risk that an attacker can enumerate information from, or at worst exploit to compromise the target.

Best practices state that only the minimum number of open ports should be enabled to reduce the attack surface.

### 6.2.1 Target: report-uri.com - 104.17.183.88

Port	State	Service	Product	Version
80	open	http		Cloudflare http proxy
443	open	ssl/http		Cloudflare http proxy
2052	open	http		Cloudflare http proxy
2053	open	ssl/http		nginx
2082	open	http		Cloudflare http proxy
2083	open	ssl/http		nginx
2086	open	http		Cloudflare http proxy
2087	open	ssl/http		nginx
2095	open	http		Cloudflare http proxy
2096	open	ssl/http		nginx
8080	open	http		Cloudflare http proxy
8443	open	ssl/http		Cloudflare http proxy
8880	open	http		Cloudflare http proxy

## 6.3 SSL/TLS Assessment

Transport Layer Security (TLS) is used to ensure the confidentiality and integrity of traffic as it transits a network. It is also used to give certainty of the identity of the client, server, or both. Insecure configurations are common. The following sub-sections show information gathered using SSLScan.

### 6.3.1 SSLScan Results for: report-uri.com - 443

```
Connected to 104.17.184.88

Testing SSL server cdn.report-uri.com on port 443 using SNI name cdn.report-uri.com

SSL/TLS Protocols:
SSLv2      disabled
SSLv3      disabled
TLSv1.0    disabled
TLSv1.1    disabled
TLSv1.2    enabled
TLSv1.3    enabled

  TLS Fallback SCSV:
Server supports TLS Fallback SCSV

  TLS renegotiation:
Session renegotiation not supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLSv1.3 not vulnerable to heartbleed
TLSv1.2 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.3 128 bits TLS_AES_128_GCM_SHA256      Curve 25519 DHE 253
Accepted  TLSv1.3 256 bits TLS_AES_256_GCM_SHA384      Curve 25519 DHE 253
Accepted  TLSv1.3 256 bits TLS_CHACHA20_POLY1305_SHA256 Curve 25519 DHE 253
Preferred TLSv1.2 128 bits ECDHE-ECDSA-AES128-GCM-SHA256 Curve 25519 DHE 253
Accepted  TLSv1.2 256 bits ECDHE-ECDSA-AES256-GCM-SHA384 Curve 25519 DHE 253
Accepted  TLSv1.2 256 bits ECDHE-ECDSA-CHACHA20-POLY1305 Curve 25519 DHE 253

  Server Key Exchange Group(s):
TLSv1.3 128 bits secp256r1 (NIST P-256)
TLSv1.3 192 bits secp384r1 (NIST P-384)
TLSv1.3 260 bits secp521r1 (NIST P-521)
TLSv1.3 128 bits x25519
TLSv1.2 128 bits secp256r1 (NIST P-256)
TLSv1.2 192 bits secp384r1 (NIST P-384)
TLSv1.2 260 bits secp521r1 (NIST P-521)
TLSv1.2 128 bits x25519

  Server Signature Algorithm(s):
TLSv1.3 Server accepts all signature algorithms.

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
ECC Curve Name:      prime256v1
ECC Key Strength:    128

Subject: *.report-uri.com
Altnames: DNS:*.report-uri.com, DNS:report-uri.com
Issuer: R3

Not valid before: Oct  7 00:10:45 2021 GMT
Not valid after:  Jan  5 00:10:44 2022 GMT
```



A Shearwater Group plc  
Company

26a, The Downs  
Altrincham  
Cheshire  
WA14 2PU

+44 (0)161 233 0100

