Report URI

Penetration Testing Report

3756

Web Application Test

27/11/2024

Author: Jose Barrera

22 Great James Street, London, WC1N 3ES

Tel: +44 (0)161 233 0100

Web: www.pentest.co.uk

Table of Contents

1 Document Revision History

Name	Date	Version	Comment
Jose Barrera	21/11/2024	0.1	Initial Document
Paul Johnston	21/11/2024	0.2	QA by Senior Consultant
Jose Barrera	22/11/2024	1.0	Final Draft
Jose Barrera	27/11/2024	2.0	Final Draft v2

2 Introduction

Report URI was founded to take the pain out of monitoring security policies like CSP and other modern security features. 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 customers just the information they need.

Report URI have indicated the need for a repeat security test of their 'Report URI' application in order 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 assessment of Report URI application

The duration included 5 days effort (including reporting). Work commenced on 11/11/2024 and concluded on 19/11/2024.

2.2 Scenarios Included

- **Black-Box assessment** – testing the web application while unauthenticated without additional information. This simulates a real-world threat posed to all Internet facing services.
- **Rogue-User Scenario** – using credentials provided to simulate the risk as various levels of user account. This simulates the risk of a user either by choice or by being compromised attacking the system.
- **White-box assessment** – using the source code provided.

All the tests were performed against the production environment.

2.3 Target(s)

- https://report-uri.com

3 Executive Summary

Overall, the Report URI application performed well during the assessment. It demonstrated a strong performance throughout the engagement, effectively thwarting attempts by authenticated attackers to exploit vulnerabilities like SQL Injection and Cross-Site Scripting that could potentially compromise the server or application. The application also had proper user access controls in place and showed no signs of an attack surface for authorisation-based attacks.

Only low-severity issues were identified that should be resolved to add additional layers of security to the application and further harden it.

Full details of each issue as well as recommended remedial actions can be found documented in the **Technical Findings** section.

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:

- **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:

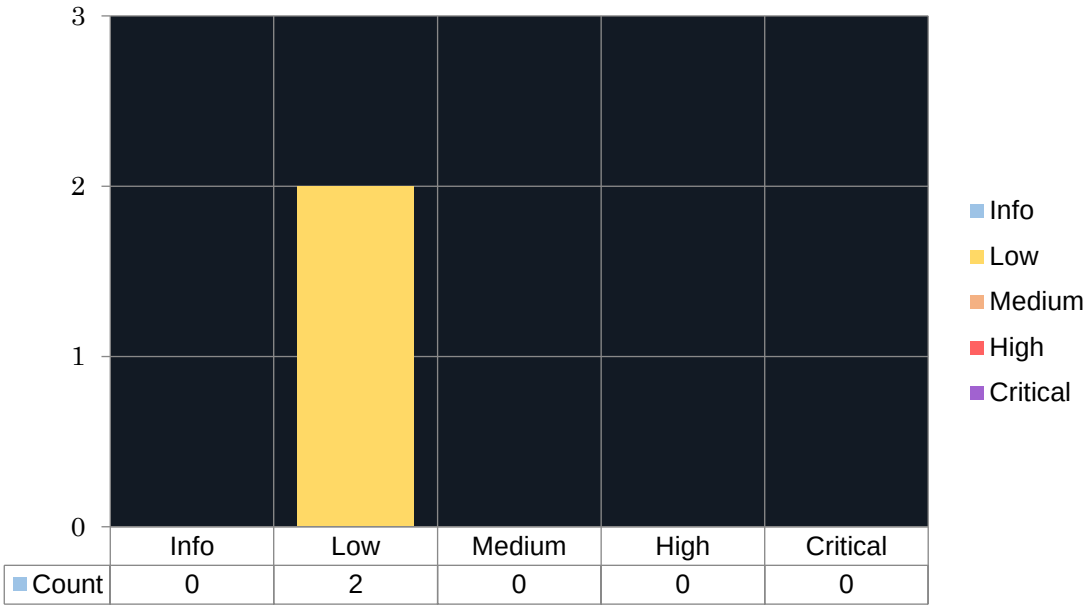
Risk Category	CVSS Score	Rationales
Critical	8.1 – 10.0	Poses a severe risk which is easy to exploit. Begin the process of remediating immediately after the issue has been presented.
High	6.1 – 8.0	Poses a significant risk and can be exploited. Address these as soon as possible after any critical risks have been remediated.
Medium	4.1 – 6.0	Poses an important risk but may be difficult to exploit. Pentest recommends remedial work within 3 months of discovery.
Low	2.1 – 4.0	Poses a minor risk or may be exceedingly difficult to exploit. Address these over the long-term during testing cycles.
Info	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	Pentest Risk Category	CVSS
1	**Vulnerabilities in Outdated Dependencies Detected**	Upgrade the affected libraries to the latest supported version.	Low	**3.1/Low**
2	**No Anti-Automation Protection**	Consider fine tuning CloudFlare Bot protections on vulnerable functions.	Low	**3.1/Low**

5 Technical Findings

5.1 Vulnerabilities in Outdated Dependencies Detected

5.1.1 Background

Most software products are developed using APIs or libraries provided by third 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 2021 project as category A06 labelled “Vulnerable and Outdated Components” defined at reference [1].

5.1.2 Details

During the assessment a few supporting JavaScript libraries were identified which contained publicly disclosed vulnerabilities such as Cross-Site Scripting.

The table below identifies the location within the application and the related CVE associated with directly related vulnerabilities.

Component version	Location implemented	Vulnerability	CVE
Bootstrap 3.4.1	https://cdn.report-uri.com/libs/twitter-bootstrap/3.4.1/js/bootstrap.min.js	Cross-Site Scripting	CVE-2024-6484
Select 4.2	https://cdn.report-uri.com/libs/select2/3.5.2/select2.min.js	Cross-Site Scripting	CVE-2016-10744

Additionally, Bootstrap version 3.4.1 currently reached EOL (end of life) and no longer receive any updates from the vendor, which exacerbates this issue.

More information about Bootstrap’s version 3 reaching EOL is available in reference [4].

5.1.3 Risk Analysis

Pentest Risk Category	**Low**
CVSS	3.1/Low AV:N/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:L
Explanation	The risk associated with this issue was considered low, as no areas of the application were found to reflect user inputs without appropriate HTML encoding. Moreover, the application implemented a strict CSP. The issue is raised to encourage updating the affected libraries and is not believed to constitute an immediate threat to Report URI or its users.

5.1.4 Recommendation

The immediate recommendation is to download and integrate the latest supported versions of each outdated dependency.

Pentest understands that this would be a significant undertaking for radius, 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, a 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-check” (see reference [2]) which can be integrated into most build processes.

5.1.5 References

[1]	OWASP Top 10: A06_2021 - Vulnerable and Outdated Components
[2]	OWASP: OWASP Dependency Check
[3]	TaringAmberini: Ready to use Java Dependencies Vulnerability Checker
[4]	GitHub – Bootstrap version 4 issue

5.1.6 Affected Item(s)

- https://report-uri.com

5.2 No Anti-Automation Protection

5.2.1 Background

Web applications are subjected to unwanted automated usage. Usually, these events occur due to an improper usage of an existing functionality rather than the exploitation of vulnerabilities. Also, excessive misuse is commonly mistakenly reported as application Denial-of-Service (DoS) like HTTP-flooding, when in fact the DoS is a side-effect instead of the primary intent.

Insufficient anti-automation occurs when a web application permits an attacker to automate a process that was originally designed to be performed only in a manual fashion, i.e. by a human web user

5.2.2 Details

The application did implement anti-automation measures to protect against excessive automated requests. However, as the CloudFlare Bot Management was disabled for the test, remote attackers were able to send many requests to access or generate data.

Although the application used CSRF tokens and validated them properly, it was possible to reuse the CSRF token because a non-standard client (Burp Suite) was used during testing. This client enabled manual manipulation and replay of HTTP requests, bypassing the typical flow of the application and allowing automation.

Below is one request issued by the application to create a team:

```
POST /team/create_team/ HTTP/2
Host: report-uri.com
Cookie: _nss=1; __cf_bm=lYfP1QOpjdweC0p5pHFLAAvVIv1d91kYWSuu5nMGg5M-1731935807-1.0.1.1-
ne_YxFLihgBqNOL5ndq8LwzKFHp5eFI7JSLlzYTJQtjdfQT8KX1YfX8kyMGMlnqzAE8eAKd90S.lm2x0AJ0KlA;
__Host-report_uri_csrf=ec6c3b4d5aa5e5f8ffb26bd9e5f33c83; __Host-
report_uri_sess=c3k0adha2690t2qlqnspbbtr30
[…]
Referer: https://report-uri.com/account/teams/

csrf_token=ec6c3b4d5aa5e5f8ffb26bd9e5f33c83&name=Test%22%3E%3Cscript%3Ealert%281%29%3C%2Fsc
ript
```

The following image shows the teams that were created by the consultant:

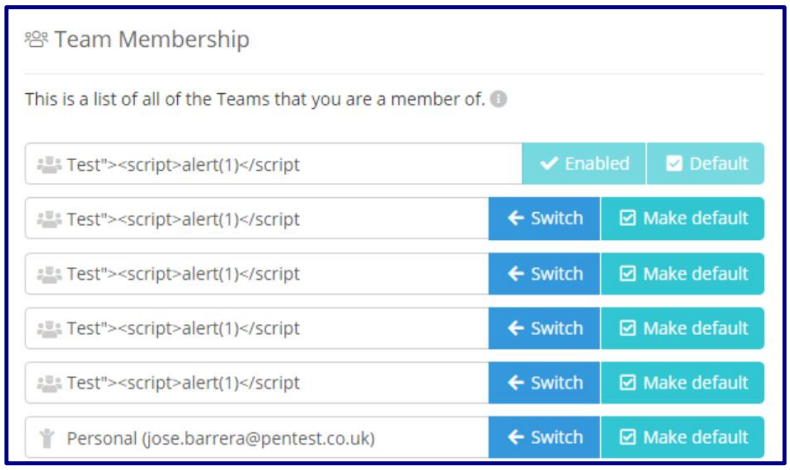


Figure 1 – CSRF token reuse

5.2.3 Risk Analysis

Pentest Risk Category	Low
CVSS	3.1/Low AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:L
Explanation	The risk rating has been set to "Low" since testing was conducted with Cloudflare Bot Management disabled. However, it is unlikely that Cloudflare Bot Management would have prevented this brute-force attempt under normal conditions, as only 6 requests were issued within a short time frame. The limited request volume would likely not trigger typical rate-limiting or anomaly detection mechanisms, making this vulnerability feasible for exploitation in scenarios with similar traffic patterns.

5.2.4 Recommendation

Pentest recommends implementing anti-automation controls on the affected forms. By significantly delaying the success of a password-guessing attack, it provides an effective deterrent to attackers.

Consider the following options to reduce the effectiveness of automated bot attacks:

- **CAPTCHA** can help prevent automated bots by requiring manual interactions from a human. For example, Google's ReCAPTCHA asks the user to identify an object (such as a car or traffic light) from a photo.
- **Rate-Limiting Requests** simply reduces the number of requests an attacker can be made within reasonable time period to the server.

5.2.5 References

[1]	OWASP: Automated Threats to Web Applications

5.2.6 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: 2024-03-18T08:02:32Z
   Creation Date: 2011-04-17T11:55:31Z
   Registry Expiry Date: 2025-04-17T11:55:31Z
   Registrar: NameCheap, Inc.
   Registrar IANA ID: 1068
   Registrar Abuse Contact Email: abuse@namecheap.com
   Registrar Abuse Contact Phone: +1.6613102107
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Name Server: CARL.NS.CLOUDFLARE.COM
   Name Server: COCO.NS.CLOUDFLARE.COM
   DNSSEC: signedDelegation
   DNSSEC DS Data: 2371 13 2
B86DC8BE786CAFA5B1D92F52AA23CD9B62AF70DBE9D907AC61A1F9469513B5F6
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-11-21T10:13:42Z <<<
```

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:        2024-09-04
Comment:        All Cloudflare abuse reporting can be done via
https://www.cloudflare.com/abuse
Comment:        Geofeed: https://api.cloudflare.com/local-ip-ranges.csv
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
OrgRoutingHandle: CLOUD146-ARIN
OrgRoutingName:   Cloudflare-NOC
OrgRoutingPhone:  +1-650-319-8930
```

```
OrgRoutingEmail:  noc@cloudflare.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN
OrgTechHandle: ADMIN2521-ARIN
OrgTechName:   Admin
OrgTechPhone:  +1-650-319-8930
OrgTechEmail:  rir@cloudflare.com
OrgTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN
OrgAbuseHandle: ABUSE2916-ARIN
OrgAbuseName:   Abuse
OrgAbusePhone:  +1-650-319-8930
OrgAbuseEmail:  abuse@cloudflare.com
OrgAbuseRef:    https://rdap.arin.net/registry/entity/ABUSE2916-ARIN
OrgNOCHandle: CLOUD146-ARIN
OrgNOCName:   Cloudflare-NOC
OrgNOCPhone:  +1-650-319-8930
OrgNOCEmail:  noc@cloudflare.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/CLOUD146-ARIN
RTechHandle: ADMIN2521-ARIN
RTechName:   Admin
RTechPhone:  +1-650-319-8930
RTechEmail:  rir@cloudflare.com
RTechRef:    https://rdap.arin.net/registry/entity/ADMIN2521-ARIN
RNOCHandle: NOC11962-ARIN
RNOCName:   NOC
RNOCPhone:  +1-650-319-8930
RNOCEmail:  noc@cloudflare.com
RNOCRef:    https://rdap.arin.net/registry/entity/NOC11962-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: 104.17.215.66 – report-uri.com

Port	State	Service	Product	Version	Extra
80/tcp	open	http	cloudflare	Unknown	Unknown
443/tcp	open	https	cloudflare	Unknown	Unknown
2052/tcp	open	clearvisn	Unknown	Unknown	Unknown
2053/tcp	open	http	nginx	Unknown	Unknown
2082/tcp	open	infowave	Unknown	Unknown	Unknown
2083/tcp	open	http	nginx	Unknown	Unknown
2086/tcp	open	gnunet	Unknown	Unknown	Unknown
2087/tcp	open	http	nginx	Unknown	Unknown
2095/tcp	open	nbx-ser	Unknown	Unknown	Unknown
2096/tcp	open	http	nginx	Unknown	Unknown
8080/tcp	open	http-proxy	cloudflare	Unknown	Unknown
8443/tcp	open	https-alt	cloudflare	Unknown	Unknown
8880/tcp	open	cddbp-alt	Unknown	Unknown	Unknown

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 TestSSL.

6.3.1 TestSSL Results for:

```
/testssl.sh --openssl bin/openssl.Linux.x86_64 --quiet --wide --log 104.17.215.66

 Start 2024-11-19 11:20:42        -->> 104.17.215.66:443 (104.17.215.66) <<--

 rDNS (104.17.215.66):   --
 Service detected:       HTTP


 Testing protocols via sockets except NPN+ALPN

 SSLv2      not offered (OK)
 SSLv3      not offered (OK)
 TLS 1      not offered
 TLS 1.1    not offered
 TLS 1.2    offered (OK)
 TLS 1.3    offered (OK): final
 NPN/SPDY   h2, http/1.1 (advertised)
 ALPN/HTTP2 h2, http/1.1 (offered)

 Testing cipher categories

 NULL ciphers (no encryption)                      not offered (OK)
 Anonymous NULL Ciphers (no authentication)        not offered (OK)
 Export ciphers (w/o ADH+NULL)                     not offered (OK)
 LOW: 64 Bit + DES, RC[2,4], MD5 (w/o export)      not offered (OK)
 Triple DES Ciphers / IDEA                         not offered
 Obsoleted CBC ciphers (AES, ARIA etc.)            offered
 Strong encryption (AEAD ciphers) with no FS       offered (OK)
 Forward Secrecy strong encryption (AEAD ciphers)  offered (OK)


 Testing server's cipher preferences

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Cipher Suite
Name (IANA/RFC)
-----------------------------------------------------------------------------------------
-----------------------------------
SSLv2
 -
SSLv3
 -
TLSv1
 -
TLSv1.1
 -
TLSv1.2 (server order -- server prioritizes ChaCha ciphers when preferred by clients)
 xc02b    ECDHE-ECDSA-AES128-GCM-SHA256     ECDH 253   AESGCM      128
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 xcca9    ECDHE-ECDSA-CHACHA20-POLY1305     ECDH 253   ChaCha20    256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
 xc009    ECDHE-ECDSA-AES128-SHA            ECDH 253   AES         128
TLS ECDHE ECDSA WITH AES 128 CBC SHA
 xc02c    ECDHE-ECDSA-AES256-GCM-SHA384     ECDH 253   AESGCM      256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 xc00a    ECDHE-ECDSA-AES256-SHA            ECDH 253   AES         256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 xc023    ECDHE-ECDSA-AES128-SHA256         ECDH 253   AES         128
TLS ECDHE ECDSA WITH AES 128 CBC SHA256
 xc024    ECDHE-ECDSA-AES256-SHA384         ECDH 253   AES         256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
```

```
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 253   AESGCM      128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xcca8   ECDHE-RSA-CHACHA20-POLY1305       ECDH 253   ChaCha20    256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
 xc013   ECDHE-RSA-AES128-SHA              ECDH 253   AES         128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 x9c     AES128-GCM-SHA256                 RSA        AESGCM      128
TLS_RSA_WITH_AES_128_GCM_SHA256
 x2f     AES128-SHA                        RSA        AES         128
TLS_RSA_WITH_AES_128_CBC_SHA
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH 253   AESGCM      256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc014   ECDHE-RSA-AES256-SHA              ECDH 253   AES         256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 x9d     AES256-GCM-SHA384                 RSA        AESGCM      256
TLS_RSA_WITH_AES_256_GCM_SHA384
 x35     AES256-SHA                        RSA        AES         256
TLS_RSA_WITH_AES_256_CBC_SHA
 xc027   ECDHE-RSA-AES128-SHA256           ECDH 253   AES         128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 x3c     AES128-SHA256                     RSA        AES         128
TLS_RSA_WITH_AES_128_CBC_SHA256
 xc028   ECDHE-RSA-AES256-SHA384           ECDH 253   AES         256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 x3d     AES256-SHA256                     RSA        AES         256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLSv1.3 (no server order, thus listed by strength)
 x1302   TLS_AES_256_GCM_SHA384            ECDH 253   AESGCM      256
TLS_AES_256_GCM_SHA384
 x1303   TLS_CHACHA20_POLY1305_SHA256      ECDH 253   ChaCha20    256
TLS_CHACHA20_POLY1305_SHA256
 x1301   TLS_AES_128_GCM_SHA256            ECDH 253   AESGCM      128
TLS_AES_128_GCM_SHA256

 Has server cipher order?     yes (OK) -- only for < TLS 1.3
 Negotiated protocol          TLSv1.3
 Negotiated cipher            TLS_AES_256_GCM_SHA384, 253 bit ECDH (X25519)

 Testing robust forward secrecy (FS) -- omitting Null Authentication/Encryption, 3DES, RC4

 FS is offered (OK) , ciphers follow (client/browser support is important here)

Hexcode  Cipher Suite Name (OpenSSL)       KeyExch.   Encryption  Bits     Cipher Suite
Name (IANA/RFC)
-----------------------------------------------------------------------------------------
---------------------------------
 x1302   TLS_AES_256_GCM_SHA384            ECDH 253   AESGCM      256
TLS_AES_256_GCM_SHA384
 x1303   TLS_CHACHA20_POLY1305_SHA256      ECDH 253   ChaCha20    256
TLS_CHACHA20_POLY1305_SHA256
 xc030   ECDHE-RSA-AES256-GCM-SHA384       ECDH 256   AESGCM      256
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 xc02c   ECDHE-ECDSA-AES256-GCM-SHA384     ECDH 256   AESGCM      256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 xc028   ECDHE-RSA-AES256-SHA384           ECDH 256   AES         256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 xc024   ECDHE-ECDSA-AES256-SHA384         ECDH 256   AES         256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
 xc014   ECDHE-RSA-AES256-SHA              ECDH 256   AES         256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
 xc00a   ECDHE-ECDSA-AES256-SHA            ECDH 256   AES         256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 xcca9   ECDHE-ECDSA-CHACHA20-POLY1305     ECDH 253   ChaCha20    256
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
 xcca8   ECDHE-RSA-CHACHA20-POLY1305       ECDH 253   ChaCha20    256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
 x1301   TLS_AES_128_GCM_SHA256            ECDH 253   AESGCM      128
TLS_AES_128_GCM_SHA256
 xc02f   ECDHE-RSA-AES128-GCM-SHA256       ECDH 256   AESGCM      128
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 xc02b   ECDHE-ECDSA-AES128-GCM-SHA256     ECDH 256   AESGCM      128
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
```

```
 xc027   ECDHE-RSA-AES128-SHA256           ECDH 256   AES         128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 xc023   ECDHE-ECDSA-AES128-SHA256         ECDH 256   AES         128
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 xc013   ECDHE-RSA-AES128-SHA              ECDH 256   AES         128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
 xc009   ECDHE-ECDSA-AES128-SHA            ECDH 256   AES         128
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA

 Elliptic curves offered:     prime256v1 secp384r1 secp521r1 X25519


 Testing server defaults (Server Hello)

 TLS extensions (standard)    "renegotiation info/#65281" "EC point formats/#11" "session
ticket/#35" "status request/#5"
                              "next protocol/#13172" "signed certificate timestamps/#18"
"key share/#51" "supported versions/#43"
                              "extended master secret/#23" "application layer protocol
negotiation/#16" "compress certificate/#27"
 Session Ticket RFC 5077 hint 64800 seconds, session tickets keys seems to be rotated <
daily
 SSL Session ID support       yes
 Session Resumption           Tickets: yes, ID: no
 TLS clock skew               Random values, no fingerprinting possible
 Certificate Compression      0002/Brotli
 Client Authentication        none

  Server Certificate #1 (in response to request w/o SNI)
   Signature Algorithm          SHA256 with RSA
   Server key size              RSA 2048 bits (exponent is 65537)
   Server key usage             Digital Signature, Key Encipherment
   Server extended key usage    TLS Web Server Authentication, TLS Web Client
Authentication
   Serial                       0366B5349812310CEE06E134DFC27D918DAF (OK: length 18)
   Fingerprints                 SHA1 59EFE1175AC1D020DF5DD7F4EC507F7510F22F50
                                SHA256
C60594A5D59820E4BBA32177F49884AE6AB13B6CF7F680BC84DB9C9458CD8048
   Common Name (CN)             report-uri.com
   subjectAltName (SAN)         *.report-uri.com report-uri.com
   Trust (hostname)             certificate does not match supplied URI
   Chain of trust               Ok
   EV cert (experimental)       no
   Certificate Validity (UTC)   86 >= 30 days (2024-11-16 06:24 --> 2025-02-14 06:24)
   ETS/"eTLS", visibility info  not present
   Certificate Revocation List  --
   OCSP URI                     http://r10.o.lencr.org
   OCSP stapling                offered, not revoked
   OCSP must staple extension   --
   DNS CAA RR (experimental)    not offered
   Certificate Transparency     yes (certificate extension)
   Certificates provided        2
   Issuer                       R10 (Let's Encrypt from US)
   Intermediate cert validity   #1: ok > 40 days (2027-03-12 23:59). R10 <-- ISRG Root X1
   Intermediate Bad OCSP (exp.) Ok

  Server Certificate #2 (in response to request w/o SNI)
   Signature Algorithm          ECDSA with SHA384
   Server key size              EC 256 bits (curve P-256)
   Server key usage             Digital Signature
   Server extended key usage    TLS Web Server Authentication, TLS Web Client
Authentication
   Serial                       04BC413080D4314D9B57B912A354A16D3D3E (OK: length 18)
   Fingerprints                 SHA1 F1FBA4AFC6616F3C00800F8B3277D1334537359A
                                SHA256
C4191F04B29173B1C2895A49DC2F24082B5560FC58F9C3AE5EE51C446139C893
   Common Name (CN)             report-uri.com
   subjectAltName (SAN)         *.report-uri.com report-uri.com
   Trust (hostname)             certificate does not match supplied URI
   Chain of trust               Ok
   EV cert (experimental)       no
   Certificate Validity (UTC)   86 >= 30 days (2024-11-16 06:24 --> 2025-02-14 06:24)
   ETS/"eTLS", visibility info  not present
```

```
   Certificate Revocation List  --
   OCSP URI                     http://e6.o.lencr.org
   OCSP stapling                offered, not revoked
   OCSP must staple extension   --
   DNS CAA RR (experimental)    not offered
   Certificate Transparency     yes (certificate extension)
   Certificates provided        2
   Issuer                       E6 (Let's Encrypt from US)
   Intermediate cert validity   #1: ok > 40 days (2027-03-12 23:59). E6 <-- ISRG Root X1
   Intermediate Bad OCSP (exp.) Ok


 Testing HTTP header response @ "/"

 HTTP Status Code             403 Forbidden
 HTTP clock skew              0 sec from localtime
 Strict Transport Security    not offered
 Public Key Pinning           --
 Server banner                cloudflare
 Application banner           --
 Cookie(s)                    (none issued at "/") -- maybe better try target URL of 30x
 Security headers             --
 Reverse Proxy banner         --


 Testing vulnerabilities

 Heartbleed (CVE-2014-0160)                not vulnerable (OK), no heartbeat extension
 CCS (CVE-2014-0224)                       not vulnerable (OK)
 Ticketbleed (CVE-2016-9244), experiment.  not vulnerable (OK)
 ROBOT                                     not vulnerable (OK)
 Secure Renegotiation (RFC 5746)           supported (OK)
 Secure Client-Initiated Renegotiation     not vulnerable (OK)
 CRIME, TLS (CVE-2012-4929)                not vulnerable (OK)
 BREACH (CVE-2013-3587)                    no gzip/deflate/compress/br HTTP compression
(OK)  - only supplied "/" tested
 POODLE, SSL (CVE-2014-3566)               not vulnerable (OK), no SSLv3 support
 TLS_FALLBACK_SCSV (RFC 7507)              No fallback possible (OK), no protocol below TLS
1.2 offered
 SWEET32 (CVE-2016-2183, CVE-2016-6329)    not vulnerable (OK)
 FREAK (CVE-2015-0204)                     not vulnerable (OK)
 DROWN (CVE-2016-0800, CVE-2016-0703)      not vulnerable on this host and port (OK)
                                           make sure you don't use this certificate
elsewhere with SSLv2 enabled services, see

https://search.censys.io/search?resource=hosts&virtual_hosts=INCLUDE&q=C60594A5D59820E4BBA3
2177F49884AE6AB13B6CF7F680BC84DB9C9458CD8048
 LOGJAM (CVE-2015-4000), experimental      not vulnerable (OK): no DH EXPORT ciphers, no DH
key detected with <= TLS 1.2
 BEAST (CVE-2011-3389)                     not vulnerable (OK), no SSL3 or TLS1
 LUCKY13 (CVE-2013-0169), experimental     potentially VULNERABLE, uses cipher block
chaining (CBC) ciphers with TLS. Check patches
 Winshock (CVE-2014-6321), experimental    not vulnerable (OK)
 RC4 (CVE-2013-2566, CVE-2015-2808)        no RC4 ciphers detected (OK)


 Running client simulations (HTTP) via sockets

 Browser                      Protocol  Cipher Suite Name (OpenSSL)       Forward Secrecy
------------------------------------------------------------------------------------------
-----
 Android 6.0                  TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-
256)
 Android 7.0 (native)         TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     256 bit ECDH (P-
256)
 Android 8.1 (native)         TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256     253 bit ECDH
(X25519)
 Android 9.0 (native)         TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH
(X25519)
 Android 10.0 (native)        TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH
(X25519)
 Android 11 (native)          TLSv1.3   TLS_AES_128_GCM_SHA256            253 bit ECDH
(X25519)
```

```
 Android 12 (native)          TLSv1.3   TLS_AES_128_GCM_SHA256           253 bit ECDH
(X25519)
 Chrome 79 (Win 10)           TLSv1.3   TLS_AES_128_GCM_SHA256           253 bit ECDH
(X25519)
 Chrome 101 (Win 10)          TLSv1.3   TLS_AES_128_GCM_SHA256           253 bit ECDH
(X25519)
 Firefox 66 (Win 8.1/10)      TLSv1.3   TLS_AES_128_GCM_SHA256           253 bit ECDH
(X25519)
 Firefox 100 (Win 10)         TLSv1.3   TLS_AES_128_GCM_SHA256           253 bit ECDH
(X25519)
 IE 6 XP                      No connection
 IE 8 Win 7                   No connection
 IE 8 XP                      No connection
 IE 11 Win 7                  TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256    256 bit ECDH (P-
256)
 IE 11 Win 8.1                TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256    256 bit ECDH (P-
256)
 IE 11 Win Phone 8.1          TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256    256 bit ECDH (P-
256)
 IE 11 Win 10                 TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256    256 bit ECDH (P-
256)
 Edge 15 Win 10               TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256    253 bit ECDH
(X25519)
 Edge 101 Win 10 21H2         TLSv1.3   TLS_AES_128_GCM_SHA256           253 bit ECDH
(X25519)
 Safari 12.1 (iOS 12.2)       TLSv1.3   TLS_CHACHA20_POLY1305_SHA256     253 bit ECDH
(X25519)
 Safari 13.0 (macOS 10.14.6)  TLSv1.3   TLS_CHACHA20_POLY1305_SHA256     253 bit ECDH
(X25519)
 Safari 15.4 (macOS 12.3.1)   TLSv1.3   TLS_AES_128_GCM_SHA256           253 bit ECDH
(X25519)
 Java 7u25                    No connection
 Java 8u161                   TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256    256 bit ECDH (P-
256)
 Java 11.0.2 (OpenJDK)        TLSv1.3   TLS_AES_128_GCM_SHA256           256 bit ECDH (P-
256)
 Java 17.0.3 (OpenJDK)        TLSv1.3   TLS_AES_256_GCM_SHA384           253 bit ECDH
(X25519)
 go 1.17.8                    TLSv1.3   TLS_AES_128_GCM_SHA256           253 bit ECDH
(X25519)
 LibreSSL 2.8.3 (Apple)       TLSv1.2   ECDHE-ECDSA-CHACHA20-POLY1305    253 bit ECDH
(X25519)
 OpenSSL 1.0.2e               TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256    256 bit ECDH (P-
256)
 OpenSSL 1.1.0l (Debian)      TLSv1.2   ECDHE-ECDSA-CHACHA20-POLY1305    253 bit ECDH
(X25519)
 OpenSSL 1.1.1d (Debian)      TLSv1.3   TLS_AES_256_GCM_SHA384           253 bit ECDH
(X25519)
 OpenSSL 3.0.3 (git)          TLSv1.3   TLS_AES_256_GCM_SHA384           253 bit ECDH
(X25519)
 Apple Mail (16.0)            TLSv1.2   ECDHE-ECDSA-AES128-GCM-SHA256    256 bit ECDH (P-
256)
 Thunderbird (91.9)           TLSv1.3   TLS_AES_128_GCM_SHA256           253 bit ECDH
(X25519)


 Rating (experimental)

 Rating specs (not complete)  SSL Labs's 'SSL Server Rating Guide' (version 2009q from
2020-01-30)
 Specification documentation  https://github.com/ssllabs/research/wiki/SSL-Server-Rating-
Guide
 Protocol Support (weighted)  0 (0)
 Key Exchange     (weighted)  0 (0)
 Cipher Strength  (weighted)  0 (0)
 Final Score                  0
 Overall Grade                M
 Grade cap reasons            Grade capped to M. Domain name mismatch
                              Grade capped to A. HSTS is not offered

 Done 2024-11-19 11:22:10 [  90s] -->> 104.17.215.66:443 (104.17.215.66) <<--
```

22 Great James Street
Holborn
London
WC1N 3ES

+44 (0)161 233 0100