

AUDITORÍA PARCIAL DEL SITIO

[THEBRIDGE.TECH]

TECNOLOGÍAS QUE USA LA WEB:

Para realizarlo en primera instancia nos basamos en utilizar una herramienta web o extensión de Chrome o Mozilla conocida como **Wappalyzer**, que recoge las tecnologías usadas en la web.

- **Analíticas Web:** En esta web se usa LinkedIn Insight Tag, Facebook Pixel y Google Analytics, para recoger los datos analíticos de todo lo relacionado con la web.
- **Automatización de Marketing:** Se usa HubSpot.
- **Tag Managers:** Se usa Google Tag Manager.
- **Seguridad:** Se usa ClickCease.
- **Page Builder:** Construida o se usa Webflow.
- **Font scripts:** Para las fuentes se usa Google Font API.
- **JavaScript libraries y contenedores:** Las librerías de JS que usan son JQuery 3.5.1, Core-JS 3.19.0 y Preact.
- **Miscelánea:** Usa un protocolo HTTP/2, un Module Federation y Open Graph.
- **Cookie compliance:** Se usa CookieFirst.
- **CDN:** Usa Google Hosted Libraries.
- **A/B testing:** Se usa Google Optimize.

USANDO LA HERRAMIENTA WHATWEB DE KALI LINUX SOBRE EL SITIO

```
(root@cdl-lab)-[/home/cdl]
# whatweb www.thebridge.tech
http://www.thebridge.tech [301 Moved Permanently] Country[UNITED STATES][US],
IP[34.249.200.254], OpenResty, RedirectLocation[https://www.thebridge.tech/]
, Title[301 Moved Permanently]
https://www.thebridge.tech/ [200 OK] Country[UNITED STATES][US], Email[admi
siones@thebridge.tech,hello@thebridge.tech,trabajaconnosotros@thebridgeschool.e
s], Frame, HTML5, IP[34.249.200.254], JQuery, Open-Graph-Protocol[website], S
cript[text/javascript], Title[The Bridge | Digital Talent Accelerator], Uncom
monHeaders[content-security-policy,x-lambda-id,x-served-by,x-cache-hits,x-tim
er,x-cluster-name], X-Frame-Options[SAMEORIGIN]
```

HACIENDO UN DESCUBRIMIENTO DE DIRECTORIOS DEL SITIO WEB

En este caso usaremos la herramienta de Kali Linux dirsearch basada en Python. Usamos el método HTTP con GET. Si le pasamos un comando con una wordlist, podremos ser más específicos pero sino ponemos nada, lo hará por defecto igualmente.

Lo iniciamos...

```
(root@cdl-lab)-[/home/cdl/Documentos/Tools/dirsearch]
# dirsearch -u https://www.thebridge.tech/

dirsearch v0.4.2
Accelerate tu carrera

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size: 10927
```

Target: <https://www.thebridge.tech/>

[18:16:21] Starting:

```
[18:16:28] 406 - 562B - /.exe
[18:16:36] 406 - 562B - /.paket/paket.exe
[18:16:41] 200 - 0B - /.well-known/acme-challenge/dfify
[18:16:41] 200 - 0B - /.well-known/acme-challenge
[18:16:45] 200 - 11KB - /404
[18:16:45] 200 - 6KB - /401
[18:16:53] 406 - 562B - /Symlink.php
[18:16:56] 406 - 562B - /WSO.php
[18:16:57] 400 - 556B - /..\..\..\..\..\..\..\..\..\etc\passwd
[18:16:59] 406 - 562B - /_vti_bin/shtml.exe?_vti_rpc
[18:16:59] 406 - 562B - /_vti_pvt/shtml.exe
[18:17:06] 406 - 562B - /admin.exe
[18:17:33] 406 - 562B - /author.exe
[18:17:35] 406 - 562B - /bin/config.sh
[18:17:35] 406 - 562B - /bin/hostname
[18:17:35] 406 - 562B - /bin/libs
[18:17:35] 406 - 562B - /bin/reset-db-prod.sh
[18:17:35] 406 - 562B - /bin/reset-db.sh
[18:17:35] 406 - 562B - /bin/target
[18:17:35] 406 - 562B - /bin/tmp
[18:17:35] 406 - 562B - /bin/RhoBundle
[18:17:37] 406 - 562B - /c-h.v2.php
[18:17:37] 200 - 51KB - /blog
[18:17:37] 406 - 562B - /c99shell.php
[18:17:37] 406 - 562B - /c99.php
[18:17:37] 406 - 562B - /c100.php
[18:17:39] 406 - 562B - /cfexec.cfm
[18:17:39] 406 - 562B - /cgi-bin/htimage.exe?2,2
[18:17:39] 406 - 562B - /cgi-bin/imagemap.exe?2,2
[18:17:41] 406 - 562B - /cmd-asp-5.1.asp
[18:17:41] 406 - 562B - /cmdjsp.jsp
[18:17:41] 406 - 562B - /cmdasp.asp
```

```

[18:17:41] 406 - 562B - /cmdasp.aspx
[18:17:59] 200 - 16KB - /faqs
[18:18:00] 406 - 562B - /gaza.php
[18:18:05] 406 - 562B - /images/c99.php
[18:18:07] 200 - 60KB - /index.html
[18:18:10] 406 - 562B - /jsp-reverse.jsp
[18:18:16] 406 - 562B - /lol.php
[18:18:17] 200 - 5KB - /manifest.json
[18:18:21] 406 - 562B - /msdac/root.exe?/c+dir
[18:18:26] 406 - 562B - /nst.php
[18:18:26] 406 - 562B - /nstview.php
[18:18:31] 406 - 562B - /perl-reverse-shell.pl
[18:18:31] 406 - 562B - /perlcmd.cgi
[18:18:32] 406 - 562B - /php-backdoor.php
[18:18:32] 406 - 562B - /php-findsock-shell.php
[18:18:32] 406 - 562B - /php-tiny-shell.php
[18:18:32] 406 - 562B - /php-reverse-shell.php
[18:18:40] 406 - 562B - /qsd-php-backdoor.php
[18:18:40] 406 - 562B - /r00t.php
[18:18:40] 406 - 562B - /r57eng.php
[18:18:40] 406 - 562B - /r57shell.php
[18:18:40] 406 - 562B - /r57.php
[18:18:42] 406 - 562B - /remote/fgt_lang?lang=/../..../..//../../../../../../../../bin/sslvpnd
[18:18:43] 200 - 71B - /robots.txt
[18:18:43] 406 - 562B - /rst.php
[18:18:44] 406 - 562B - /scripts/cgimail.exe
[18:18:44] 406 - 562B - /scripts/counter.exe
[18:18:44] 406 - 562B - /scripts/fpcount.exe
[18:18:44] 406 - 562B - /scripts/root.exe?/c+dir
[18:18:44] 406 - 562B - /scripts/samples/search/webhits.exe
[18:18:44] 406 - 562B - /scripts/tools/getdrvs.exe
[18:18:44] 406 - 562B - /scripts/tools/newdsn.exe
[18:18:46] 400 - 556B - /servlet/%C0%AE%C0%AE%C0%AF
[18:18:46] 406 - 562B - /shell.php
[18:18:46] 406 - 562B - /shell.sh
[18:18:48] 406 - 562B - /shtml.exe

```

```

[18:18:48] 406 - 562B - /simple-backdoor.php
[18:18:49] 200 - 128KB - /sitemap.xml
[18:19:07] 406 - 562B - /wp-admin/c99.php
[18:19:08] 406 - 562B - /wp-login.php
[18:19:09] 406 - 562B - /wso.php
[18:19:09] 406 - 562B - /xmlrpc.php
[18:19:10] 406 - 562B - /zehir.php

Task Completed

```

Usando Google Dorks:

El objetivo de usar Google Dorks, es buscar información que esté expuesta del sitio y pueda generar un conflicto por ser información sensible o de carácter privado.



site:thebridge.tech file:pdf



[Q Todo](#)

[Imágenes](#)

[Libros](#)

[Videos](#)

[Shopping](#)

[Más](#)

[Herramientas](#)

Aproximadamente 0 resultados (0,19 segundos)

La búsqueda de **site:thebridge.tech file:pdf** no obtuvo ningún resultado.



site:thebridge.tech file:csv



[Q Todo](#)

[Imágenes](#)

[Noticias](#)

[Videos](#)

[Libros](#)

[Más](#)

[Herramientas](#)

Aproximadamente 0 resultados (0,17 segundos)

La búsqueda de **site:thebridge.tech file:csv** no obtuvo ningún resultado.



site:thebridge.tech file:xls



[Q Todo](#)

[Imágenes](#)

[Shopping](#)

[Videos](#)

[Noticias](#)

[Más](#)

[Herramientas](#)

Aproximadamente 0 resultados (0,17 segundos)

La búsqueda de **site:thebridge.tech file:xls** no obtuvo ningún resultado.



site:thebridge.tech intext:"@thebridge.tech"



[Q Todo](#)

[Imágenes](#)

[Shopping](#)

[Noticias](#)

[Maps](#)

[Más](#)

[Herramientas](#)

Página 2 de aproximadamente 427 resultados (0,19 segundos)

Patrocinado



Codenotch

<https://www.codenotch.com>

Domina análisis de datos - Data Analytics para el Éxito

Descubre el Bootcamp de Data Science más completo y actualizado - 92% de empleabilidad.

Adquiere las habilidades necesarias para triunfar en el sector como analista...



thebridge.tech

<https://thebridge.tech> > becas-cyberskills

Becas Cyberskills_ - The Bridge

Urazurrutia Kalea, 3, 48003 Bilbo, Bizkaia. . Escribenos a: hello@thebridge.tech.

admisiones@thebridge.tech. Llámanos al:.



thebridge.tech

<https://www.thebridge.tech> > financiacion-becas

Financiación y becas - The Bridge

Urazurrutia Kalea, 3, 48003 Bilbo, Bizkaia. . Escribenos a: hello@thebridge.tech.

admisiones@thebridge.tech. Llámanos al:.



site:thebridge.tech intext:"iker arce"



Todo Noticias Imágenes Vídeos Shopping Más Herramientas

Aproximadamente 21 resultados (0,23 segundos)

Imágenes de site:thebridge.tech intext:"iker arce"



Enviar comentarios

Ver todo →



thebridge.tech

https://thebridge.tech › equipo-the-bridge › iker-arce

Iker Arce - The Bridge

Iker Arce. CEO. Icono LinkedIn. ¿Te has quedado con ganas de saber más? No lo dudes y contacta con nosotros, te resolveremos todas las dudas y te ...



BURPSUITE EN EL SITIO WEB:

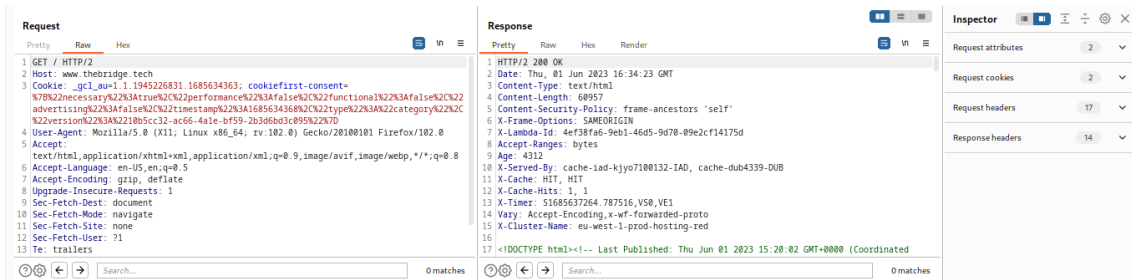
Request to https://www.thebridge.tech:443 [52.17.119.105]

Forward Drop Intercept is on Action Open browser

Pretty Raw Hex

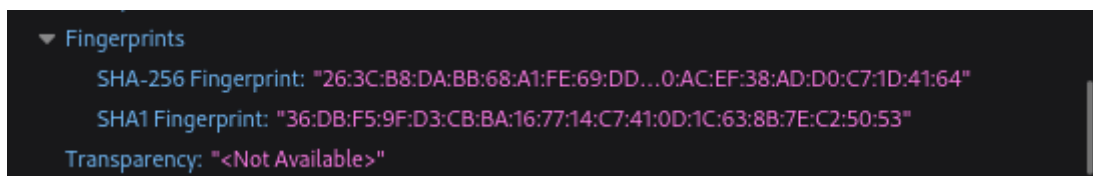
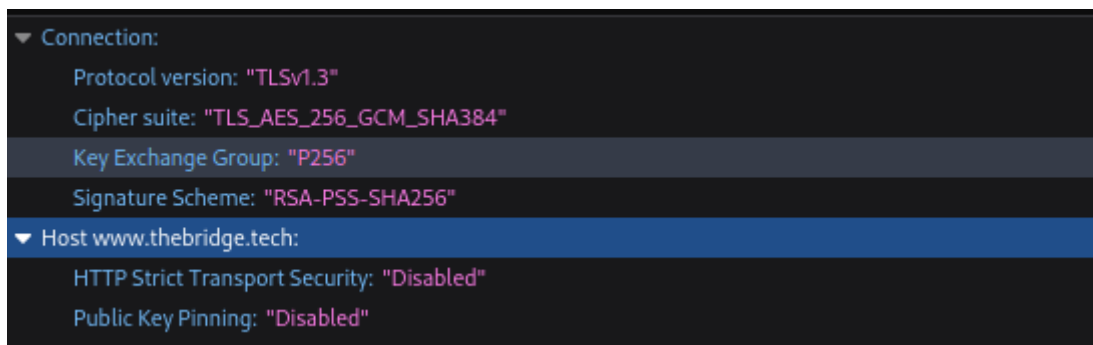
```
1 GET / HTTP/2
2 Host: www.thebridge.tech
3 Cookie: _gcl_au=1.1.1945226831.1685634363; cookiefirst-consent=%7B%22necessary%22%3Atrue%2C%22performance%22%3Afalse%2C%22functional%22%3Afalse%2C%22advertising%22%3Afalse%2C%22timestamp%22%3A1685634368%2C%22type%22%3A%22category%22%2C%22version%22%3A%2210b5cc32-ac66-4a1e-bf59-2b3d6bd3c095%22%7D
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14
15
```

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	https://www.thebridge.tech	GET	/			200	61444	HTML		The Bridge Digital Tale...		✓	52.17.119.105		18:33:08.13...	8080



USAMOS INSPECCIONAR WEB:

En el apartado cifrado/seguridad podemos ver...



Name	Value	D..	Path	Expires / M...	Size	HttpOnly	Secure	SameSite	Partition ...	Priority
cookiefirst-consent	%7B%22necessary%22%3Atrue%2C%22performance%22%3Afals...	w...	/	2024-05-26...	252		✓	Lax		Medium
_gcl_au	1.1.938288172.1685637996	...	/	2023-08-30...	31					Medium

Cookie Value ☐ Show URL-decoded

%7B%22necessary%22%3Atrue%2C%22performance%22%3Afalse%2C%22functional%22%3Afalse%2C%22advertising%22%3Afalse%2C%22timestamp%22%3A1685638000%2C%22type%22%3A%22category%22%2C%22version%22%3A%2210b5cc32-ac66-4a1e-bf59-2b3d6bd3c095%22%7D



General

Detalles

Jerarquía de certificados

▼ ISRG Root X1

▼ R3

www.thebridge.tech

Campos de certificado

▼ www.thebridge.tech

▼ Certificado

Versión

Número de serie

Algoritmo de firma de certificado

Emisor

▼ Validez

Posterior a

Valor de campo

PKCS #1 SHA-256 con cifrado RSA

Exportar...

▼ Extensiones

Uso de claves de certificado

Uso mejorado de clave

Restricciones básicas del certificado

ID de clave de la entidad receptora del certificado

Valor de campo

No crítica

Autenticación de servidor WWW TLS (OID.1.3.6.1.5.5.7.3.1)

Autenticación de cliente WWW TLS (OID.1.3.6.1.5.5.7.3.2)

USAMOS SQLMAP

```
(root@cdl-lab)-[/home/cdl/Documentos/Tools]
# sqlmap -u «http://www.thebridge.tech/?id=1» -passwords -batch
```

Esta línea lo que hará es buscar contraseñas y las intenta crackear, batch indica que no necesita input del usuario.

```
[*] starting @ 18:53:24 /2023-06-01/
[18:53:25] [INFO] testing connection to the target URL
got a 301 redirect to 'https://www.thebridge.tech/?id=1'. Do you want to follow? [Y/n] Y
[18:53:25] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
[18:53:25] [INFO] testing if the target URL content is stable
[18:53:25] [WARNING] GET parameter 'id' does not appear to be dynamic
[18:53:25] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[18:53:25] [INFO] testing for SQL injection on GET parameter 'id'
[18:53:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:53:26] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:53:26] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:53:27] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[18:53:28] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[18:53:28] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[18:53:29] [INFO] testing 'Generic inline queries'
[18:53:29] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:53:29] [WARNING] time-based comparison requires larger statistical model, please wait. (done)
[18:53:30] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:53:30] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:53:31] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:53:32] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[18:53:32] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[18:53:33] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] Y
[18:53:34] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[18:53:35] [WARNING] GET parameter 'id' does not seem to be injectable
[18:53:35] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[18:53:35] [WARNING] HTTP error codes detected during run:
406 (Not Acceptable) - 73 times
[*] ending @ 18:53:35 /2023-06-01/ MACI0N
```

```
(root@cdl-lab)-[/home/cdl/Documentos/Tools]
# sqlmap -u «http://www.thebridge.tech» -dump -T users -D testdb -C name,surname
```

Con esta línea intentamos dumppear la tabla users con las columnas name,surname de la base de datos.

```

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

[*] starting @ 18:55:45 /2023-06-01/

[18:55:45] [INFO] testing connection to the target URL
got a 301 redirect to 'https://www.thebridge.tech/'. Do you want to follow? [Y/n] Y
[18:56:34] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
[18:56:34] [INFO] testing if the target URL contents is stable
[18:56:34] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1')
[18:56:34] [WARNING] HTTP error codes detected during run:
406 (Not Acceptable) - 1 times

[*] ending @ 18:56:34 /2023-06-01/

```

Podemos buscar con `--search` junto con `-T` para tablas y `-C` para columnas para buscar ocurrencias en las diferentes BD.

```

(root@cdl-lab)-[/home/cdl/Documentos/Tools]
# sqlmap -u "http://www.thebridge.tech?id=1" --search --level 3 -C pass

```

{1.7.2#stable}

<https://sqlmap.org>

```

[*] starting @ 18:58:01 /2023-06-01/

[18:58:01] [INFO] testing connection to the target URL
got a 301 redirect to 'https://www.thebridge.tech/?id=1'. Do you want to follow? [Y/n] Y
[18:58:04] [CRITICAL] previous heuristics detected that the target is protected by some kind of WAF/IPS
[18:58:04] [INFO] testing if the target URL content is stable
[18:58:04] [WARNING] GET parameter 'id' does not appear to be dynamic
[18:58:04] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[18:58:04] [INFO] testing for SQL injection on GET parameter 'id'
[18:58:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[18:58:07] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[18:58:09] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[18:58:10] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[18:58:12] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[18:58:13] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[18:58:16] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[18:58:19] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[18:58:22] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[18:58:25] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[18:58:25] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[18:58:26] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'
[18:58:26] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[18:58:26] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[18:58:26] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[18:58:26] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'

```

```
[18:58:25] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[18:58:26] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'
[18:58:26] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[18:58:26] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[18:58:26] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[18:58:26] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[18:58:26] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[18:58:26] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
[18:58:26] [INFO] testing 'Boolean-based blind - Parameter replace (CASE - original value)'
[18:58:26] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[18:58:27] [INFO] testing 'MySQL >= 5.0 boolean-based blind - ORDER BY, GROUP BY clause (original value)'
[18:58:27] [INFO] testing 'MySQL < 5.0 boolean-based blind - ORDER BY, GROUP BY clause'
[18:58:27] [INFO] testing 'PostgreSQL boolean-based blind - ORDER BY, GROUP BY clause'
[18:58:27] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - ORDER BY clause'
[18:58:27] [INFO] testing 'Oracle boolean-based blind - ORDER BY, GROUP BY clause'
[18:58:28] [INFO] testing 'HAVING boolean-based blind - WHERE, GROUP BY clause'
[18:58:31] [INFO] testing 'PostgreSQL boolean-based blind - Stacked queries'
[18:58:32] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Stacked queries (IF)'
[18:58:34] [INFO] testing 'MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[18:58:37] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[18:58:40] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (UPDATXML)'
[18:58:43] [INFO] testing 'MySQL >= 4.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)'
[18:58:46] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[18:58:49] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[18:58:52] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONVERT)'
[18:58:55] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (CONCAT)'
[18:58:58] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[18:59:01] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (UTL_INADDR.GET_HOST_ADDRESS)'
[18:59:04] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[18:59:07] [INFO] testing 'Firebird AND error-based - WHERE or HAVING clause'
[18:59:10] [INFO] testing 'MonetDB AND error-based - WHERE or HAVING clause'
[18:59:12] [INFO] testing 'Vertica AND error-based - WHERE or HAVING clause'
[18:59:16] [INFO] testing 'IBM DB2 AND error-based - WHERE or HAVING clause'
[18:59:19] [INFO] testing 'MySQL >= 5.1 error-based - PROCEDURE ANALYSE (EXTRACTVALUE)'
[18:59:22] [INFO] testing 'MySQL >= 5.0 error-based - Parameter replace (FLOOR)'
[18:59:22] [INFO] testing 'MySQL >= 5.1 error-based - Parameter replace (EXTRACTVALUE)'
```

```
[18:59:26] [INFO] testing 'Firebird inline queries'
[18:59:26] [INFO] testing 'MySQL >= 5.0.12 stacked queries (comment)'
[18:59:28] [INFO] testing 'MySQL >= 5.0.12 stacked queries'
[18:59:31] [INFO] testing 'MySQL >= 5.0.12 stacked queries (query SLEEP - comment)'
[18:59:33] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[18:59:34] [INFO] testing 'PostgreSQL < 8.2 stacked queries (Glibc - comment)'
[18:59:36] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[18:59:38] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (DECLARE - comment)'
[18:59:39] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[18:59:41] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[18:59:44] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP)'
[18:59:47] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SLEEP - comment)'
[18:59:49] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP - comment)'
[18:59:50] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind'
[18:59:53] [INFO] testing 'MySQL >= 5.0.12 RLIKE time-based blind (query SLEEP)'
[18:59:56] [INFO] testing 'MySQL AND time-based blind (ELT)'
[18:59:59] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[19:00:02] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[19:00:05] [INFO] testing 'Oracle AND time-based blind'
[19:00:08] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace'
[19:00:09] [INFO] testing 'MySQL >= 5.0.12 time-based blind - Parameter replace (subtraction)'
[19:00:09] [INFO] testing 'PostgreSQL > 8.1 time-based blind - Parameter replace'
[19:00:09] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_LOCK.SLEEP)'
[19:00:09] [INFO] testing 'Oracle time-based blind - Parameter replace (DBMS_PIPE.RECEIVE_MESSAGE)'
[19:00:09] [INFO] testing 'MySQL >= 5.0.12 time-based blind - ORDER BY, GROUP BY clause'
[19:00:09] [INFO] testing 'PostgreSQL > 8.1 time-based blind - ORDER BY, GROUP BY clause'
[19:00:10] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_LOCK.SLEEP)'
[19:00:10] [INFO] testing 'Oracle time-based blind - ORDER BY, GROUP BY clause (DBMS_PIPE.RECEIVE_MESSAGE)'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n]
[19:00:22] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[19:00:59] [INFO] testing 'Generic UNION query (random number) - 1 to 10 columns'
```

```
[19:04:19] [INFO] testing 'MySQL UNION query (NULL) - 11 to 20 columns'
[19:04:49] [INFO] testing 'MySQL UNION query (random number) - 11 to 20 columns'
[19:05:20] [INFO] testing 'MySQL UNION query (NULL) - 21 to 30 columns'
[19:05:50] [WARNING] GET parameter 'id' does not seem to be injectable
[19:05:50] [WARNING] parameter 'User-Agent' does not appear to be dynamic
[19:05:50] [WARNING] heuristic (basic) test shows that parameter 'User-Agent' might not be injectable
[19:05:51] [INFO] testing for SQL injection on parameter 'User-Agent'
[19:05:51] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[19:05:54] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (subquery - comment)'
[19:05:55] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (comment)'
[19:05:57] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
[19:05:58] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (Microsoft Access comment)'
[19:06:00] [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
[19:06:03] [INFO] testing 'MySQL AND boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause (MAKE_SET)'
[19:06:06] [INFO] testing 'PostgreSQL AND boolean-based blind - WHERE or HAVING clause (CAST)'
[19:06:09] [INFO] testing 'Oracle AND boolean-based blind - WHERE or HAVING clause (CTXSYS.DRITHSX.SN)'
[19:06:12] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[19:06:12] [INFO] testing 'PostgreSQL boolean-based blind - Parameter replace'
[19:06:12] [INFO] testing 'Microsoft SQL Server/Sybase boolean-based blind - Parameter replace'
[19:06:13] [INFO] testing 'Oracle boolean-based blind - Parameter replace'
[19:06:13] [INFO] testing 'Informix boolean-based blind - Parameter replace'
[19:06:13] [INFO] testing 'Microsoft Access boolean-based blind - Parameter replace'
[19:06:13] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL)'
[19:06:13] [INFO] testing 'Boolean-based blind - Parameter replace (DUAL - original value)'
[19:06:13] [INFO] testing 'Boolean-based blind - Parameter replace (CASE)'
```

VULNERABILIDADES, INFORMES, SCANEOS

Algunas vulnerabilidades o fallos de la web detectados:

Seguridad del sitio:

HTTP Strict Transport Security (HSTS) no se aplica

Sin HSTS aplicado, las personas que navegan por este sitio son más susceptibles a los ataques de intermediarios. El servidor debe configurarse para admitir HSTS.

CSP implementado de manera insegura

Es posible que la Política de seguridad de contenido no restrinja las fuentes de manera adecuada o que contenga 'inseguro en línea' sin el uso de un nonce o hash. Esto aumenta el riesgo de ataques XSS.

X-Content-Type-Options no es falso

Los navegadores pueden interpretar los archivos como un tipo MIME diferente al especificado en el encabezado HTTP de tipo de contenido. Esto puede conducir a ataques de confusión MIME.

CAA no habilitado

El dominio no contiene un registro de autorización de autoridad de certificación (CAA) válido. Un registro CAA indica qué autoridades de certificación (CA) están autorizadas para emitir certificados para un dominio.

No vulnerable a CVE-2015-4000 (Logjam)

El servidor utiliza parámetros fuertes de Diffie-Hellman y no es vulnerable al ataque Logjam.

No vulnerable a CVE-2014-0160 (Heartbleed)

Un error en la implementación de OpenSSL de la extensión TLS heartbeat permite el acceso a partes de la memoria en el host de destino, p. claves criptográficas y contraseñas.

No vulnerable a CVE-2014-3566 (CANICHE)

El servidor no es compatible con SSLv3 y no es vulnerable al ataque POODLE.

Seguridad del email:

Política DMARC no encontrada

No se encontró la política DMARC. Esto facilita que los atacantes envíen correo electrónico desde este dominio. Se debe implementar una política DMARC para este dominio.

La política de SPF utiliza todos

El registro del marco de políticas del remitente (SPF) es demasiado indulgente en cuanto a qué dominios pueden enviar correo electrónico en nombre del dominio. Es preferible que este registro no utilice el mecanismo ~all, ya que no indica al receptor del correo que rechace mensajes de fuentes no autorizadas. Cuando no se aplica DMARC, se debe usar -all en el registro SPF.

Network Security:

DNSSEC no habilitado

Los registros DNSSEC evitan que terceros falsifiquen los registros que garantizan la identidad de un dominio. DNSSEC debe configurarse para este dominio.

Brand Protection:

Registrador de dominio o protección de eliminación de registro no habilitada

El dominio no está protegido contra solicitudes de eliminación no solicitadas con el registrador o registro. El dominio debe tener configurado clientDeleteProhibited o serverDeleteProhibited.

Registrador de dominio o protección de actualización de registro no habilitada

El dominio no está protegido contra solicitudes de actualización no solicitadas con el registrador o registro. El dominio debe tener configurado clientUpdateProhibited o serverUpdateProhibited.

Se han detectado algunos fallos en el handshake del sitio web, algunos ejemplos:

IE 11 / Win Phone 8.1 R Server sent fatal alert: handshake_failure

Safari 6 / iOS 6.0.1 Server sent fatal alert: handshake_failure

Safari 7 / iOS 7.1 R Server sent fatal alert: handshake_failure

Safari 7 / OS X 10.9 R Server sent fatal alert: handshake_failure

Safari 8 / iOS 8.4 R Server sent fatal alert: handshake_failure

Safari 8 / OS X 10.10 R Server sent fatal alert: handshake_failure

No hay rastro del malware en el sitio:

Scanned site: https://www.thebridge.tech:443		
<div>SITESCAN PARAMETERS</div> <div>IP address: 52.17.119.105</div> <div>Country: Ireland</div> <div>Server: Unknown</div> <div>CMS: Webflow</div> <div>Scan date: Jun Thu 2023/06/01 19:10</div>	<div>DETECTION DETAILS</div> <div>Malicious files: 0</div> <div>Suspicious files: 0</div> <div>Potentially Suspicious files: 0</div> <div>Clean files: 24</div> <div>External links detected: 167</div> <div>Iframes scanned: 12</div> <div>Referenced domains: 0</div> <div>Blacklisted links detected: 0</div> <div>Blacklisted iframes: 0</div> <div>Referenced blacklisted domains: 1</div>	<div>BLACKLISTING STATUS</div> <div>Quttera Labs Clean</div> <div>ZeusTracker Clean</div> <div>Yandex Safebrowsing Clean</div> <div>MalwareDomainList Clean</div> <div>Phishtank Clean</div> <div>Google Clean</div> <div>StopBadware Clean</div> <div>URLhaus Clean</div>

Algunas peticiones de sandbox asociadas al sitio web:

SANDBOX REQUESTS	
Detected Redirects: 4	
Sandbox Requests	
URL	http://www.thebridge.tech/
Method	GET
HTTP error	301
Target IP	52.17.119.105
Target Country	Ireland
Redirected URL	https://www.thebridge.tech/

URL	https://consent.cookiefirst.com/sites/thebridge.tech-d6002cb0-069d-4c56-8051-fa8608d17e24/consent.js
Method	GET
HTTP error	200
Target IP	169.150.247.36
Target Country	Germany

URL	https://uploads-ssl.webflow.com/60780bff57ddc42a6adc1d7e/css/the-bridge-site.webflow.1793a6f6f.min.css
Method	GET
HTTP error	200
Target IP	18.66.112.109
Target Country	United States

URL	https://fonts.googleapis.com/css?family=Lato:100,100italic,300,300italic,400,400italic,700,700italic,900,900italic%7COpen+Sans:300,300italic,400,400italic,600,600italic,700,700italic,800,800italic%7CExo:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic%7CMontserrat:100,100italic,200,200italic,300,300italic,400,400italic,500,500italic,600,600italic,700,700italic,800,800italic,900,900italic%7CPT+Serif:400,400italic,700,700italic%7CMulish:regular,700,800%7CMulish:regular,700,800%7CRoboto:100,100italic,300,300italic,regular,italic,500,500italic,700,700italic,900,900italic
Method	GET
HTTP error	200
Target IP	142.250.185.106
Target Country	United States

URL	https://consent.cookiefirst.com/sites/thebridge.tech-d6002cb0-069d-4c56-8051-fa8608d17e24/version.json?v=1685639469959
Method	GET
HTTP error	200

URL	https://uploads-ssl.webflow.com/60780bff57ddc42a6adc1d7e/6176993fc0b3373e03669c47_trama-left.png
Method	GET
HTTP error	200
Target IP	18.66.112.109
Target Country	United States

URL	https://uploads-ssl.webflow.com/60780bff57ddc42a6adc1d7e/6478b5e4fe695cac2f94eb6b_TheBridge-logo_RGB_color-neg-trans.svg
Method	GET
HTTP error	200
Target IP	18.66.112.109
Target Country	United States

TECNOLOGÍAS O COMPONENTES OBSOLETOS O EN SU DEFECTO, CON VERSIONES NUEVAS SIN ACTUALIZAR:

Vulnerabilidades y componentes de CMS con huellas dactilares ⓘ	
jQuery 3.5.1	El componente está desactualizado. No se han encontrado vulnerabilidades de seguridad conocidas. Actualice a la versión más reciente 3.7.0 .
Preactuar 10	El componente está desactualizado. No se han encontrado vulnerabilidades de seguridad conocidas. Actualice a la versión más reciente 10.15.1 .

Si el sitio web cae dentro del alcance de CDE (entorno de datos del titular de la tarjeta), se pueden aplicar los siguientes requisitos de [PCI DSS](#):

REQUISITO 6.2

El CMS del sitio web o sus componentes parecen estar desactualizados. Compruebe si hay actualizaciones disponibles.


Configuración incorrecta o debilidad

Faltan algunos encabezados HTTP relacionados con la seguridad y la privacidad o están mal configurados.

Configuración incorrecta o debilidad

FALTAN ENCABEZADOS HTTP REQUERIDOS

Estricta-Transporte-Seguridad 

Opciones de tipo de contenido X 



Prueba de seguridad del software

2 PROBLEMAS ENCONTRADOS



Certificados

**CERT - www.thebridge.tech -
www.thebridge.tech**
2023-03-16 - 2023-06-14 (Valid)

**CERT - thebridge.tech -
www.thebridge.tech**
2022-06-25 - 2023-07-08 (Valid)

Problemas

Critica	subresource-integrity Fecha detectada: jue., 1 de jun. de 2023 19:39	Media	content-security-policy Fecha detectada: jue., 1 de jun. de 2023 19:39	Media	strict-transport-security Fecha detectada: jue., 1 de jun. de 2023 19:39
Baja	x-content-type-options Fecha detectada: jue., 1 de jun. de 2023 19:39	Baja	x-xss-protection Fecha detectada: jue., 1 de jun. de 2023 19:39	Baja	headers-exposed Fecha detectada: jue., 1 de jun. de 2023 19:41

[HTTP Observatory](#)[TLS Observatory](#)[SSH Observatory](#)[Third-party Tests](#)

Scan Summary



Host:	www.thebridge.tech
Scan ID #:	38079070 (unlisted)
Start Time:	June 1, 2023 7:30 PM
Duration:	6 seconds
Score:	0/100
Tests Passed:	6/11

Recommendation

Fantastic work using HTTPS! Did you know that you can ensure users never visit your site over HTTP accidentally?

HTTP Strict Transport Security tells web browsers to only access your site over HTTPS in the future, even if the user attempts to visit over HTTP or clicks an [http://](#) link.

- [Mozilla Web Security Guidelines \(HSTS\)](#)
- [MDN on HTTP Strict Transport Security](#)

Once you've successfully completed your change, click Initiate Rescan for the next piece of advice.

Test Scores

Test	Pass	Score	Reason
Content Security Policy	✗	-20	Content Security Policy (CSP) implemented unsafely. This includes 'unsafe-inline' or data: inside script-src, overly broad sources such as https: inside object-src or script-src, or not restricting the sources for object-src or script-src.
Cookies	—	0	No cookies detected
Cross-origin Resource Sharing	✓	0	Content is not visible via cross-origin resource sharing (CORS) files or headers
HTTP Public Key Pinning	—	0	HTTP Public Key Pinning (HPKP) header not implemented (optional)

Test	Pass	Score	Reason
HTTP Strict Transport Security	✗	-20	HTTP Strict Transport Security (HSTS) header not implemented
Redirection	✓	0	Initial redirection is to HTTPS on same host, final destination is HTTPS
Referrer Policy	—	0	Referrer-Policy header not implemented (optional)
Subresource Integrity	✗	-50	Subresource Integrity (SRI) not implemented, and external scripts are loaded over HTTP or use protocol-relative URLs via <code>src="//..."</code>
X-Content-Type-Options	✗	-5	X-Content-Type-Options header not implemented
X-Frame-Options	✓	+5	X-Frame-Options (XFO) implemented via the CSP <code>frame-ancestors</code> directive

CSP Analysis

Test	Pass
Blocks execution of inline JavaScript by not allowing <code>'unsafe-inline'</code> inside <code>script-src</code>	✗
Blocks execution of JavaScript's <code>eval()</code> function by not allowing <code>'unsafe-eval'</code> inside <code>script-src</code>	✓
Blocks execution of plug-ins, using <code>object-src</code> restrictions	✗
Blocks inline styles by not allowing <code>'unsafe-inline'</code> inside <code>style-src</code>	✗
Blocks loading of active content over HTTP or FTP	✓
Blocks loading of passive content over HTTP or FTP	✓
Clickjacking protection, using <code>frame-ancestors</code>	✓
Deny by default, using <code>default-src 'none'</code>	✗
Restricts use of the <code><base></code> tag by using <code>base-uri 'none'</code> , <code>base-uri 'self'</code> , or specific origins	✗
Restricts where <code><form></code> contents may be submitted by using <code>form-action 'none'</code> , <code>form-action 'self'</code> , or specific URIs	✗
Uses CSP3's <code>'strict-dynamic'</code> directive to allow dynamic script loading (optional)	—

Looking for additional help? Check out Google's CSP Evaluator!

Grade History

Date	Score	Grade
June 1, 2023 7:30 PM	0	F

Raw Server Headers

Header	Value
Accept-Ranges:	bytes
Age:	7697
Connection:	keep-alive
Content-Encoding:	gzip
Content-Length:	13265
Content-Security-Policy:	frame-ancestors 'self'
Content-Type:	text/html
Date:	Thu, 01 Jun 2023 17:30:49 GMT
Vary:	Accept-Encoding,x-wf-forwarded-proto
X-Cache:	HIT, HIT
X-Cache-Hits:	31, 1
X-Cluster-Name:	us-west-2-prod-hosting-red
X-Frame-Options:	SAMEORIGIN
X-Lambda-Id:	4ef38fa6-9eb1-46d5-9d70-09e2cf14175d
X-Served-By:	cache-iad-kjyo7100132-IAD, cache-bfi-krnt7300081-BFI
X-Timer:	S1685640649.414668,VS0,VE1

[HTTP Observatory](#)**[TLS Observatory](#)**[SSH Observatory](#)[Third-party Tests](#)

This site uses an **untrusted** or **invalid certificate**. The following results ignore this error.

Scan Summary



Host: www.thebridge.tech (44.238.31.106)

Scan ID #: 55240031

End Time: June 1, 2023 7:30 PM

[Compat. Level:](#) Intermediate

Explainer: [189051446](#)

Certificate

Common name: www.thebridge.tech

Alternative Names: www.thebridge.tech

First Observed: 2023-06-01 (certificate #[189051446](#))

Valid From: 2023-03-16

Valid To: 2023-06-14

Key: RSA 2048 bits

Issuer: R3

Signature Algorithm: SHA256WithRSA

Cipher Suites

Cipher	Code ()	Size	AEAD ()	PFS ()	Protocols
ECDHE-RSA-AES128-GCM-SHA256	0x0C 0x2F	2048 bits	✓	✓	TLS 1.2
ECDHE-RSA-AES256-GCM-SHA384	0x0C 0x30	2048 bits	✓	✓	TLS 1.2
DHE-RSA-AES128-GCM-SHA256	0x00 0x9E	2048 bits	✓	✓	TLS 1.2

Cipher	Code ()	Size	AEAD ()	PFS ()	Protocols
DHE-RSA-AES256-GCM-SHA384	0x00 0x9F	2048 bits	✓	✓	TLS 1.2

Miscellaneous

CAA Record:	No
Cipher Preference:	Server selects preferred cipher
Compatible Clients:	Android 4.4.2, Apple ATS 9, BingPreview Jan 2015, Chrome 31, Edge 12, Firefox 31.3.0 ESR, Googlebot Feb 2015, IE 11, Java 8b132, OpenSSL 1.0.1h, Opera 60, Safari 9, Yahoo Slurp Jun 2014, YandexBot Sep 2014
OCSP Stapling:	No

Suggestions

Looking for improved security and have a user base of only modern clients?

Take a look at the [Mozilla “Modern” TLS configuration](#)! It provides an extremely high level of security and performance and is compatible with all clients released in the last couple years. It is not recommended for general purpose websites that may need to service older clients such as Android 4.x, Internet Explorer 10, or Java 6.x.

[Want the detailed technical nitty-gritty?](#)

Please note that these suggestions may not be appropriate for your particular usage requirements! If they do sound like something you'd like assistance with, then hop on board:

[Teleport me to Mozilla's configuration generator!](#)

Worried about malware or getting blacklisted? Check out our [website monitoring & cleanup](#) subscriptions.

[Create an Account](#)

Disclaimer: SiteGuarding scanner is absolutely free and does not have full access to the website. We do our best, but 100% accuracy is possible only with installed tools on your website. You can try our [Website Antivirus Scanner](#) or request free [Website Security Analyze](#) or contact with our [Support by email or Live Chat](#) to get more details.

Send us request and get free website review and consultation

www.thebridge.tech

Name*

Email*

[GET HELP](#)

General Result

Site

Input: http://thebridge.tech/

Domain: thebridge.tech

Final Url: https://www.thebridge.tech/

Ip

75.2.70.75

99.83.190.102

Redirects To

https://thebridge.tech/

https://www.thebridge.tech/

Links



Frames

Our website uses cookies, which help us to improve our site and enables us to deliver the best possible service and customer

[https://www.googletagmanager.com/ns.html?id=GTM-NX1B1GK](#)
[https://www.googletagmanager.com/ns.html?id=GTM-THMB6J5](#)

[policy](#)

[Accept](#)

LiveChat

https://cdn.embedly.com/widgets/media.html?src=https://www.youtube.com/embed/GXe4SLsRT3o?list=PLRak6Z7xB8Mv2s3wYuiuf4kHm2LUuae4I&display_name=YouTube&url=https://www.youtube.com/watch?v=GXe4SLsRT3o&image=https://i.ytimg.com/vi/GXe4SLsRT3o/hqdefault.jpg&key=96f1f04c5f4143bcb0f2e68c87d65feb&type=text/html&schema=youtube

https://cdn.embedly.com/widgets/media.html?src=https://www.youtube.com/embed/cKQ0zfAJg5U?list=PLRak6Z7xB8Mv2s3wYuiuf4kHm2LUuae4I&display_name=YouTube&url=https://www.youtube.com/watch?v=cKQ0zfAJg5U&image=https://i.ytimg.com/vi/cKQ0zfAJg5U/hqdefault.jpg&key=96f1f04c5f4143bcb0f2e68c87d65feb&type=text/html&schema=youtube

https://cdn.embedly.com/widgets/media.html?src=https://www.youtube.com/embed/q_dSp54pyle?list=PLRak6Z7xB8Mv2s3wYuiuf4kHm2LUuae4I&display_name=YouTube&url=https://www.youtube.com/watch?v=q_dSp54pyle&image=https://i.ytimg.com/vi/q_dSp54pyle/hqdefault.jpg&key=96f1f04c5f4143bcb0f2e68c87d65feb&type=text/html&schema=youtube

Js External

<https://ajax.googleapis.com/ajax/libs/webfont/1.6.26/webfont.js>

<https://consent.cookiefirst.com/sites/thebridge.tech-d6002cb0-069d-4c56-8051-fa8608d17e24/consent.js>

<https://www.googleoptimize.com/optimize.js?id=OPT-T6K86CT>

<https://js.hsforms.net/forms/v2-legacy.js>

<https://js.hsforms.net/forms/v2.js>

[https://d3e54v103j8qbb.cloudfront.net/js/jquery-](https://d3e54v103j8qbb.cloudfront.net/js/jquery-3.5.1.min.dc5e7f18c8.js?site=60780bff57ddc42a6adc1d7e)

[3.5.1.min.dc5e7f18c8.js?site=60780bff57ddc42a6adc1d7e](https://d3e54v103j8qbb.cloudfront.net/js/jquery-3.5.1.min.dc5e7f18c8.js?site=60780bff57ddc42a6adc1d7e)

<https://uploads-ssl.webflow.com/60780bff57ddc42a6adc1d7e/js/webflow.5bcf8f520.js>

Urls

/

/bootcamp/online

/bootcamp/bootcamps-full-time

/bootcamp/bootcamps-part-time

/bootcamps/bootcamp-ciberseguridad

/bootcamps/bootcamp-cloud-devops

/bootcamps/bootcamp-data-science

/bootcamps/bootcamp-fullstack-developer

/bootcamps/bootcamp-marketing-digital

/bootcamps/bootcamp-product-design

/campus/bootcamps-online

/campus/bootcamps-bilbao

/campus/bootcamps-madrid

/campus/bootcamps-valencia

/campus/bootcamps-sevilla

/campus-bootcamps/online

/financiacion-becas/financiacion-becas

/financiacion-becas/income-share-agreement-isa

/empresas-intituciones/soluciones-empresas

/empresas-intituciones/servicios-universidades-instituciones-educativas

/empresas-intituciones/contrata-nuestros-graduados

/empleabilidad



Our website uses cookies, which help us to improve our site and enables us to deliver the best possible service and customer

[policy.](#)

Accept

LiveChat

/sobre-nosotros/quienes-somos
/sobre-nosotros/por-que-the-bridge
/sobre-nosotros/equipo-the-bridge
/sobre-nosotros/impacto-social
/sobre-nosotros/career-readiness
/blog
/financiacion-becas/becas-super-talents
/financiacion-becas/becas-4talent-tech
/?8cad1a9e_page=2
/aviso-legal
/politica-cookies
/politica-privacidad

Website Certificate

Cert Expires: 14 Jun 2023

Cert Issuer: Let's Encrypt

Cert Authority: R3

[Get Help & Explanation](#)

[Fix My Website](#)

Detailed Blacklist Analyze

Global Blacklists

- ✔OK Bkav
- ✔OK CMC Threat Intelligence
- ✔OK Snort IP sample list
- ✔OK VX Vault
- ✔OK ViriBack
- ✔OK PhishLabs
- ✔OK K7AntiVirus
- ✔OK CINS Army
- ✔OK Quttera
- ✔OK BlockList
- ✔OK PrecisionSec
- ✔OK OpenPhish
- ✔OK 0xSI_f33d



Our website uses cookies, which help us to improve our site and enables us to deliver the best possible service and customer

✔OK Feodo Tracker

[policy.](#)

[Accept](#)

LiveChat

- ✔OK ArcSight Threat Intelligence
- ✔OK Scantitan
- ✔OK AlienVault
- ✔OK Sophos
- ✔OK Phishtank
- ✔OK Cyan
- ✔OK Spam404
- ✔OK SecureBrain
- ✔OK CRDF
- ✔OK Rising
- ✔OK Fortinet
- ✔OK alphaMountain.ai
- ✔OK Lionic
- ✔OK Cyble
- ✔OK Seclookup
- ✔OK Xcitium Verdict Cloud
- ✔OK Artists Against 419
- ✔OK Google Safebrowsing
- ✔OK SafeToOpen
- ✔OK ADMINUSLabs
- ✔OK ESTsecurity
- ✔OK Juniper Networks
- ✔OK Heimdal Security
- ✔OK AutoShun
- ✔OK Trustwave
- ✔OK AICC (MONITORAPP)
- ✔OK CyRadar
- ✔OK Dr.Web
- ✔OK Emsisoft
- ✔OK Abusix
- ✔OK Webroot
- ✔OK Avira
- ✔OK securolytics



Our website uses cookies, which help us to improve our site and enables us to deliver the best possible service and customer

✔OK Antiy-AVL

[policy.](#)

Accept

LiveChat

- ✔OK AlphaSOC
- ✔OK Acronis
- ✔OK Quick Heal
- ✔OK URLQuery
- ✔OK Viettel Threat Intelligence
- ✔OK DNS8
- ✔OK benkow.cc
- ✔OK EmergingThreats
- ✔OK Chong Lua Dao
- ✔OK Yandex Safebrowsing
- ✔OK Lumu
- ✔OK Kaspersky
- ✔OK Sucuri SiteCheck
- ✔OK desenmascara.me
- ✔OK CrowdSec
- ✔OK Cluster25
- ✔OK URLhaus
- ✔OK PREBYTES
- ✔OK StopForumSpam
- ✔OK Blueliv
- ✔OK Netcraft
- ✔OK ZeroCERT
- ✔OK Phishing Database
- ✔OK MalwarePatrol
- ✔OK Sangfor
- ✔OK IPsum
- ✔OK MalwareD
- ✔OK BitDefender
- ✔OK GreenSnow
- ✔OK G-Data
- ✔OK VIPRE
- ✔OK SCUMWARE.org
- ✔OK PhishFort



Our website uses cookies, which help us to improve our site and enables us to deliver the best possible service and customer

✔OK malwares.com URL checker

[policy.](#)

Accept

LiveChat

- ✔OK Forcepoint ThreatSeeker
- ✔OK Criminal IP
- ✔OK Certego
- ✔OK ESET
- ✔OK Threatsourcing
- ✔OK ThreatHive
- ✔OK Bfore.Ai PreCrime
- ✔OK McAfee
- ✔OK Yandex
- ✔OK Google
- ✔OK Norton

SPAM Blacklists

- ✔OK ivmURI
- ✔OK Nordspam DBL
- ✔OK SEM FRESH
- ✔OK SEM URI
- ✔OK SEM URIRED
- ✔OK SORBS RHSBL BADCONF
- ✔OK SORBS RHSBL NOMAIL
- ✔OK Spamhaus DBL
- ✔OK SURBL multi
- ✔OK OSPAM
- ✔OK Abuse.ro
- ✔OK Abusix Mail Intelligence Blacklist
- ✔OK Abusix Mail Intelligence Domain Blacklist
- ✔OK Abusix Mail Intelligence Exploit list
- ✔OK Anonmails DNSBL
- ✔OK BACKSCATTERER
- ✔OK BARRACUDA
- ✔OK BLOCKLIST.DE



Our website uses cookies, which help us to improve our site and enables us to deliver the best possible service and customer

✔OK CALIVENT

[policy.](#)

Accept

LiveChat

✔OK CYMRU BOGONS

- ✔ OK DAN TOR
- ✔ OK DAN TOREXIT
- ✔ OK DNS SERVICIOS
- ✔ OK DRMX
- ✔ OK DRONE BL
- ✔ OK FABELSOURCES
- ✔ OK HIL
- ✔ OK HIL2
- ✔ OK Hostkarma Black
- ✔ OK IBM DNS Blacklist
- ✔ OK ICMFORBIDDEN
- ✔ OK IMP SPAM
- ✔ OK IMP WORM
- ✔ OK INTERSERVER
- ✔ OK ivmSIP
- ✔ OK ivmSIP24
- ✔ OK JIPPG
- ✔ OK KEMPTBL
- ✔ OK KISA
- ✔ OK Konstant
- ✔ OK LASHBACK
- ✔ OK LNSGBLOCK
- ✔ OK LNSGBULK
- ✔ OK LNSGMULTI
- ✔ OK LNSGOR
- ✔ OK LNSGSRG
- ✔ OK MADAVI
- ✔ OK MAILSPIKE BL
- ✔ OK MAILSPIKE Z
- ✔ OK MSRBL Phishing
- ✔ OK MSRBL Spam
- ✔ OK NETHERRELAYS
- ✔ OK NETHERUNSURE
- ✔ OK NIXSPAM



Our website uses cookies, which help us to improve our site and enables us to deliver the best possible service and customer

[policy](#)

Accept

LiveChat

- ✔OK Nordspam BL
- ✔OK NoSolicitado
- ✔OK ORVEDB
- ✔OK PSBL
- ✔OK RATS Dyna
- ✔OK RATS NoPtr
- ✔OK RATS Spam
- ✔OK RBL JP
- ✔OK RSBL
- ✔OK SCHULTE
- ✔OK SEM BACKSCATTER
- ✔OK SEM BLACK
- ✔OK Sender Score Reputation Network
- ✔OK SERVICESNET
- ✔OK SORBS BLOCK
- ✔OK SORBS DUHL
- ✔OK SORBS HTTP
- ✔OK SORBS MISC
- ✔OK SORBS NEW
- ✔OK SORBS SMTP
- ✔OK SORBS SOCKS
- ✔OK SORBS SPAM
- ✔OK SORBS WEB
- ✔OK SORBS ZOMBIE
- ✔OK SPAMCOP
- ✔OK Spamhaus ZEN
- ✔OK SPFBL DNSBL
- ✔OK Suomispam Reputation
- ✔OK SWINOG
- ✔OK TRIUMF
- ✔OK TRUNCATE
- ✔OK UCEPROTECTL1
- ✔OK UCEPROTECTL2
- ✔OK UCEPROTECTL3



Our website uses cookies, which help us to improve our site and enables us to deliver the best possible service and customer

[policy.](#)

Accept

LiveChat

✔OK Woodys SMTP Blacklist

✔OK WPBL

✔OK ZapBL

[Get Help & Explanation](#)

[Fix My Website](#)

Link Analyze

Your website loads images, javascript, css style files from these domains.

Total Domains: **20**

Total Blacklisted Domains: **0**

Domain URL	Found Links	Blacklist Status
uploads-ssl.webflow.com	74	ok
ajax.googleapis.com	1	ok
consent.cookiefirst.com	1	ok
www.googleoptimize.com	1	ok
js.hsforms.net	1	ok
d3e54v103j8qbb.cloudfront.net	1	ok
fonts.googleapis.com	1	ok
fonts.gstatic.com	1	ok
thebridge.tech	1	ok
www.thebridge.tech	1	ok
www.eventbrite.es	2	ok
www.thebridge.tech	2	ok
twitter.com	1	ok
www.instagram.com	1	ok
www.linkedin.com	1	ok



Our website uses cookies, which help us to improve our site and enables us to deliver the best possible service and customer experience.

[privacy policy](#)

[policy](#)

[Accept](#)

LiveChat

[Launch Event](#)

[Join UpGuard Summit for product releases and security trends](#)

Products & Solutions ▾

[Pricing](#)

[Resources ▾](#)

[Customers](#)

[Login](#)

[Contact sales](#)

[Free trial](#)



UpGuard BreachSight

Instant Cyber Security Rating for thebridge.tech

To get a deeper insight into your entire organization, including surfacing data leaks and identity breaches, as well as your third-party vendors, [book a free demo](#) today.

[Contact sales](#)

[Free trial](#)

UpGuard Security Rating

B 713 / 950

UpGuard's Cyber Security Ratings range from 0 to 950. The higher the score, the better the security practices on the primary domain for thebridge.tech.

Company info

[Website →](#)

Company	thebridge.tech
Employees	
Location	
CEO	



Website Security



HTTP Strict Transport Security (HSTS) not enforced

Without HSTS enforced, people browsing this site are more susceptible to man-in-the-middle attacks. The server should be configured to support HSTS.



CSP implemented unsafely

The Content Security Policy may not restrict sources appropriately, or may contain 'unsafe-inline' without the use of a nonce or hash. This increases the risk of XSS attacks.



X-Content-Type-Options is not nosniff

Browsers may interpret files as a different MIME type than what is specified in the Content-Type HTTP header. This can lead to MIME confusion attacks.



CAA not enabled

The domain does not contain a valid Certification Authority Authorization (CAA) record. A CAA record indicates which Certificate Authorities (CAs) are authorized to issue certificates for a domain.



No insecure SSL/TLS versions available

No insecure SSL/TLS versions are available for this site.



SSL available

SSL is supported for this site.



Not vulnerable to CVE-2015-0204 (FREAK)

The server does not offer RSA_EXPORT cipher suites, so clients are not vulnerable to the FREAK attack.



Not vulnerable to CVE-2015-4000 (Logjam)

The server is using strong Diffie-Hellman parameters and is not vulnerable to the Logjam attack.



Not vulnerable to CVE-2014-0160 (Heartbleed)

A bug in OpenSSL's implementation of the TLS heartbeat extension allows access to portions of memory on the targeted host e.g. cryptographic keys and passwords.

✓ **Not vulnerable to CVE-2014-3566 (POODLE)**

The server does not support SSLv3, and is not vulnerable to the POODLE attack.

✓ **SSL does not expire within 20 days**

SSL certificate does not expire within 20 days.

✓ **SSL expiration period shorter than 398 days**

The SSL certificate presented by the server has an expiration period shorter than 398 days.

✓ **SSL has not expired**

SSL certificate has not expired.

✓ **Strong SSL algorithm**

Industry standard SHA-256 encryption in use.

✓ **Hostname matches SSL certificate**

The site's hostname matches the SSL certificate.

✓ **Certificate not found on our revoked certificate list**

The site's certificate chain was checked against our list of revoked certificates.

✓ **SSL certificate chain present in server response**

A complete SSL certificate chain was presented by the server for this domain.

✓ **SSL chain certificates do not expire within 20 days**

SSL intermediate and root certificates do not expire within 20 days.

✓ **Trusted SSL certificate**

The certificate presented by this domain was issued by a trusted certificate authority.

✓ **HTTP requests are redirected to HTTPS**

All HTTP requests are redirected to HTTPS.

**X-Powered-By header not exposed**

Information about specific technology used on the server is obscured.

**ASP.NET version header not exposed**

Ensuring the ASP.NET version header is not exposed makes it harder for attackers to exploit certain vulnerabilities.

**ASP.NET version header not exposing specific ASP.net version**

Ensuring the ASP.NET version header is not exposing a specific version makes it harder for attackers to exploit certain vulnerabilities.

**Server information header not exposed**

Ensuring the server information header is not exposed reduces the ability of attackers to exploit certain vulnerabilities.

**Referrer Policy is not unsafe-url**

The website's Referrer Policy is not configured to allow unsafe information to be sent in the referrer header.

**Domain index is not a listable directory**

The domain index is not a listable directory.

**No unmaintained page detected**

The page appears to be maintained.

**No open cloud storage service detected**

No cloud storage service configured to allow anonymous file listing was detected.

**CSP implemented without insecure active sources**

The Content Security Policy does not allow any insecure active sources.

**CSP implemented without insecure passive sources**

The Content Security Policy does not allow any insecure passive (img/media) sources.

**CSP implemented without unsafe-eval**

A Content Security Policy is implemented to help protect against XSS and clickjacking attacks.

[See details](#)

Email Security

DMARC policy not found

DMARC policy was not found. This makes it easier for attackers to send email from this domain. A DMARC policy should be deployed for this domain.

SPF policy uses ~all

Sender Policy Framework (SPF) record is too lenient as to which domains are allowed to send email on the domain's behalf. This record should preferably not use the ~all mechanism, as this does not instruct the mail receiver to reject messages from unauthorised sources. When DMARC is not being enforced, -all should be used on the SPF record.

SPF enabled

Sender Policy Framework (SPF) records prevent spammers from sending messages with forged addresses.

SPF syntax correct

Sender Policy Framework (SPF) record passes basic syntax checks.

SPF ptr mechanism not used

Sender Policy Framework (SPF) record does not include the ptr mechanism.

No unregistered MX records detected

No unregistered MX records that could lead to receiving mail on behalf of the target organization were detected.

[See details >](#)



Network Security



DNSSEC not enabled

DNSSEC records prevent third parties from forging the records that guarantee a domain's identity. DNSSEC should be configured for this domain.



No ports are open



Phishing and Malware



Not a suspected phishing page

This site does not appear to be a forgery or imitation of another website.



Not a suspected malware provider

This website does not appear to contain malicious code.



Not suspected of unwanted software

This website does not appear to be attempting to install unwanted software.

[See details >](#)



Brand Protection



Domain registrar or registry deletion protection not enabled

Domain is not protected from unsolicited deletion requests with the registrar or registry. The domain should have clientDeleteProhibited or serverDeleteProhibited set.



Domain registrar or registry update protection not enabled

Domain is not protected from unsolicited update requests with the registrar or registry. The domain should have clientUpdateProhibited or serverUpdateProhibited set.



Domain does not expire soon

Domain does not expire within 30 days.

- ✓ **Domain has not expired**
Domain has not expired.
- ✓ **Domain registrar or registry transfer protection enabled**
Domain is protected from unsolicited transfer requests.
- ✓ **Domain not flagged as inactive**
Domain is not flagged as inactive.
- ✓ **Domain not pending deletion**
Domain is not pending deletion with the registrar.
- ✓ **Domain not pending restoration**
Domain is not pending restoration with the registrar.
- ✓ **Domain free of registry DNS resolution hold**
Domain is not under a DNS resolution hold with the registry itself.
- ✓ **Domain free of registrar DNS resolution hold**
Domain is not under a DNS resolution hold with the registrar.
- ✓ **Domain renewal not prohibited by registry**
Domain is not prohibited from renewal at the registry itself.
- ✓ **No subdomain takeover vulnerability detected**
No domain's DNS records that could lead to subdomain takeover were detected.

Want a deeper scan?

These are just preliminary results for thebridge.tech. UpGuard scans billions of digital assets daily across thousands of vectors. Data leak detection, vulnerability scanning and identity breach detection are just some of the advanced capabilities offered by the UpGuard platform.

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.thebridge.tech](#) > 44.238.105.202

SSL Report: [www.thebridge.tech](#) (44.238.105.202)

Summary

Overall Rating

A

Certificate

Protocol Support

Key Exchange

Cipher Strength

0 20 40 60 80 100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

	www.thebridge.tech
Subject	Fingerprint SHA256: 263cb8dabb68a1fe69ddcdafa90f90a8b09a8edb0034a0acef38add0c71d4164 Pin SHA256: A2PjBtRllzD3u9d3j1PQs31StgsCntejNYuA5lridQs=
Common names	www.thebridge.tech
Alternative names	www.thebridge.tech
Serial Number	036bda238aa7103f7fd8bfa43ae7514df0cd
Valid from	Thu, 16 Mar 2023 03:13:34 UTC
Valid until	Wed, 14 Jun 2023 03:13:33 UTC (expires in 12 days, 9 hours)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	3 (4011 bytes)
Chain issues	None

#2

	R3
Subject	Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSumWb+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 2 years and 3 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1

Additional Certificates (if supplied)

Signature algorithm	SHA256withRSA
#3	
Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcb648f3cd8e1bffa4dc4c2f99b9d47cf7f1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 1 year and 3 months)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA



Certification Paths



[Click here to expand](#)

Configuration



Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No



Cipher Suites

# TLS 1.3 (suites in server-preferred order)			
TLS_AES_256_GCM_SHA384 (0xc1302)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_CHACHA20_POLY1305_SHA256 (0xc1303)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_AES_128_GCM_SHA256 (0xc1301)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
# TLS 1.2 (suites in server-preferred order)			
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc0a8)	ECDH secp256r1 (eq. 3072 bits RSA)	FS	256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0xc09e)	DH 4096 bits	FS	128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0xc09f)	DH 4096 bits	FS	256



Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1	FS
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1	FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1	FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1	FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1	FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1	FS

Handshake Simulation

IE 11 / Win 7 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 4096 FS
IE 11 / Win 8.1 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 4096 FS
IE 11 / Win Phone 8.1 <small>R</small>	Server sent fatal alert: handshake_failure		
IE 11 / Win Phone 8.1 Update <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 4096 FS
IE 11 / Win 10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 16 / Win 10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 18 / Win 10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 13 / Win Phone 10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.1l <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2s <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.0k <small>R</small>	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.1c <small>R</small>	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure		
Safari 7 / iOS 7.1 <small>R</small>	Server sent fatal alert: handshake_failure		
Safari 7 / OS X 10.9 <small>R</small>	Server sent fatal alert: handshake_failure		
Safari 8 / iOS 8.4 <small>R</small>	Server sent fatal alert: handshake_failure		
Safari 8 / OS X 10.10 <small>R</small>	Server sent fatal alert: handshake_failure		
Safari 9 / iOS 9 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / OS X 10.12 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta <small>R</small>	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 12.1.1 / iOS 12.3.1 <small>R</small>	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 <small>R</small>	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)



[Click here to expand](#)

- (1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.
(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.
(R) Denotes a reference browser or client, with which we expect better effective security.
(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).
(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.



Protocol Details

Unable to perform this test due to an internal error. (1) For a better understanding of this test, please read this longer explanation (2) Key usage data kindly provided by the Censys network search engine; original DROWN website here (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete INTERNAL ERROR: connect timed out INTERNAL ERROR: connect timed out	
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No

Protocol Details

Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	Unknown
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported Named Groups	secp256r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No



HTTP Requests



1 https://www.thebridge.tech/ (HTTP/1.1 200 OK)



Miscellaneous

Test date	Thu, 01 Jun 2023 17:11:00 UTC
Test duration	102.653 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	ec2-44-238-105-202.us-west-2.compute.amazonaws.com

SSL Report v2.1.10

Copyright © 2009-2023 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)

[Try Qualys for free!](#) Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including [certificate security](#) solutions.

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.thebridge.tech](#) > 44.238.105.202

SSL Report: [www.thebridge.tech](#) (44.238.105.202)

Summary

Overall Rating

A

Certificate

Protocol Support

Key Exchange

Cipher Strength

0 20 40 60 80 100

Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This site works only in browsers with SNI support.

This server supports TLS 1.3.

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	www.thebridge.tech Fingerprint SHA256: 263cb8dabb68a1fe69ddcdafa90f90a8b09a8edb0034a0acef38add0c71d4164 Pin SHA256: A2PjBtRI/zD3u9d3j1PQS31StgsCntejNYuA5lridQs=
Common names	www.thebridge.tech
Alternative names	www.thebridge.tech
Serial Number	036bda238aa7103f7fd8bfa43ae7514df0cd
Valid from	Thu, 16 Mar 2023 03:13:34 UTC
Valid until	Wed, 14 Jun 2023 03:13:33 UTC (expires in 12 days, 10 hours)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	R3 AIA: http://r3.i.lencr.org/
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	OCSP OCSP: http://r3.o.lencr.org
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	3 (4011 bytes)
Chain issues	None

#2

Subject	R3 Fingerprint SHA256: 67add1166b020ae61b8f5fc96813c04c2aa589960796865572a3c7e737613dfd Pin SHA256: jQJTbIh0grw0/1TkHSuMwB+Fs0Ggogr621gT3PvPKG0=
Valid until	Mon, 15 Sep 2025 16:00:00 UTC (expires in 2 years and 3 months)
Key	RSA 2048 bits (e 65537)
Issuer	ISRG Root X1

Additional Certificates (if supplied)

Signature algorithm	SHA256withRSA
#3	
Subject	ISRG Root X1 Fingerprint SHA256: 6d99fb265eb1c5b3744765fcb648f3cd8e1bffa4dc4c2f99b9d47cf7f1c24f Pin SHA256: C5+lpZ7tcVwmwQIMcRtPbsQWLABXhQzejna0wHFr8M=
Valid until	Mon, 30 Sep 2024 18:14:03 UTC (expires in 1 year and 3 months)
Key	RSA 4096 bits (e 65537)
Issuer	DST Root CA X3
Signature algorithm	SHA256withRSA



Certification Paths



Click here to expand

Configuration



Protocols

TLS 1.3	Yes
TLS 1.2	Yes
TLS 1.1	No
TLS 1.0	No
SSL 3	No
SSL 2	No



Cipher Suites

# TLS 1.3 (suites in server-preferred order)			[-]
TLS_AES_256_GCM_SHA384 (0xc1302)	ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_CHACHA20_POLY1305_SHA256 (0xc1303)	ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_AES_128_GCM_SHA256 (0xc1301)	ECDH secp256r1 (eq. 3072 bits RSA) FS		128
# TLS 1.2 (suites in server-preferred order)			[-]
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)	ECDH secp256r1 (eq. 3072 bits RSA) FS		128
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)	ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xc028)	ECDH secp256r1 (eq. 3072 bits RSA) FS		256
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02e)	DH 4096 bits FS		128
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (0xc02f)	DH 4096 bits FS		256



Handshake Simulation

Android 4.4.2	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 5.0.0	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 6.0	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 7.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 8.0	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Android 8.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
Android 9.0	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
BingPreview Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 69 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Chrome 70 / Win 10	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
Chrome 80 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
Firefox 31.3.0 ESR / Win 7	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 47 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 49 / XP SP3	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 62 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS
Firefox 73 / Win 10 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384	ECDH secp256r1 FS
Googlebot Feb 2018	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 FS

Handshake Simulation

IE 11 / Win 7 R	RSA 2048 (SHA256)	TLS 1.2	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 4096 FS
IE 11 / Win 8.1 R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 4096 FS
IE 11 / Win Phone 8.1 R	Server sent fatal alert: handshake_failure		
IE 11 / Win Phone 8.1 Update R	RSA 2048 (SHA256)	TLS 1.2 > http/1.1	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 DH 4096 FS
IE 11 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 15 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 16 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 18 / Win 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Edge 13 / Win Phone 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 8u161	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Java 11.0.3	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
Java 12.0.1	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
OpenSSL 1.0.1j R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.0.2s R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.0k R	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
OpenSSL 1.1.1c R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 6 / iOS 6.0.1	Server sent fatal alert: handshake_failure		
Safari 7 / iOS 7.1 R	Server sent fatal alert: handshake_failure		
Safari 7 / OS X 10.9 R	Server sent fatal alert: handshake_failure		
Safari 8 / iOS 8.4 R	Server sent fatal alert: handshake_failure		
Safari 8 / OS X 10.10 R	Server sent fatal alert: handshake_failure		
Safari 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 9 / OS X 10.11 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / iOS 10 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 10 / OS X 10.12 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Safari 12.1.2 / MacOS 10.14.6 Beta R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
Safari 12.1.1 / iOS 12.3.1 R	-	TLS 1.3	TLS_AES_256_GCM_SHA384 ECDH secp256r1 FS
Apple ATS 9 / iOS 9 R	RSA 2048 (SHA256)	TLS 1.2 > h2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
Yahoo Slurp Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS
YandexBot Jan 2015	RSA 2048 (SHA256)	TLS 1.2	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS

Not simulated clients (Protocol mismatch)



Click here to expand

- (1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.
- (2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.
- (3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.
- (R) Denotes a reference browser or client, with which we expect better effective security.
- (All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).
- (All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.



Protocol Details

Unable to perform this test due to an internal error.	
(1) For a better understanding of this test, please read this longer explanation	
(2) Key usage data kindly provided by the Censys network search engine; original DROWN website here	
(3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete	
INTERNAL ERROR: connect timed out	
INTERNAL ERROR: connect timed out	
Secure Renegotiation	Supported
Secure Client-Initiated Renegotiation	No
Insecure Client-Initiated Renegotiation	No
BEAST attack	Mitigated server-side (more info)
POODLE (SSLv3)	No, SSL 3 not supported (more info)
POODLE (TLS)	No (more info)
Zombie POODLE	No (more info)
GOLDENDOODLE	No (more info)
OpenSSL 0-Length	No (more info)
Sleeping POODLE	No (more info)
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported (more info)
SSL/TLS compression	No
RC4	No
Heartbeat (extension)	No

Protocol Details

Heartbleed (vulnerability)	No (more info)
Ticketbleed (vulnerability)	No (more info)
OpenSSL CCS vuln. (CVE-2014-0224)	No (more info)
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No (more info)
ROBOT (vulnerability)	No (more info)
Forward Secrecy	Yes (with most browsers) ROBUST (more info)
ALPN	Yes h2 http/1.1
NPN	Yes h2 http/1.1
Session resumption (caching)	No (IDs assigned but not accepted)
Session resumption (tickets)	No
OCSP stapling	No
Strict Transport Security (HSTS)	No
HSTS Preloading	Not in: Chrome Edge Firefox IE
Public Key Pinning (HPKP)	No (more info)
Public Key Pinning Report-Only	No
Public Key Pinning (Static)	Unknown
Long handshake intolerance	No
TLS extension intolerance	No
TLS version intolerance	No
Incorrect SNI alerts	No
Uses common DH primes	No
DH public server param (Ys) reuse	No
ECDH public server param reuse	No
Supported Named Groups	secp256r1, secp384r1 (server preferred order)
SSL 2 handshake compatibility	No
0-RTT enabled	No



HTTP Requests



1 https://www.thebridge.tech/ (HTTP/1.1 200 OK)



Miscellaneous

Test date	Thu, 01 Jun 2023 17:11:00 UTC
Test duration	102.653 seconds
HTTP status code	200
HTTP server signature	-
Server hostname	ec2-44-238-105-202.us-west-2.compute.amazonaws.com

SSL Report v2.1.10

Copyright © 2009-2023 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)

[Try Qualys for free!](#) Experience the award-winning [Qualys Cloud Platform](#) and the entire collection of [Qualys Cloud Apps](#), including [certificate security](#) solutions.