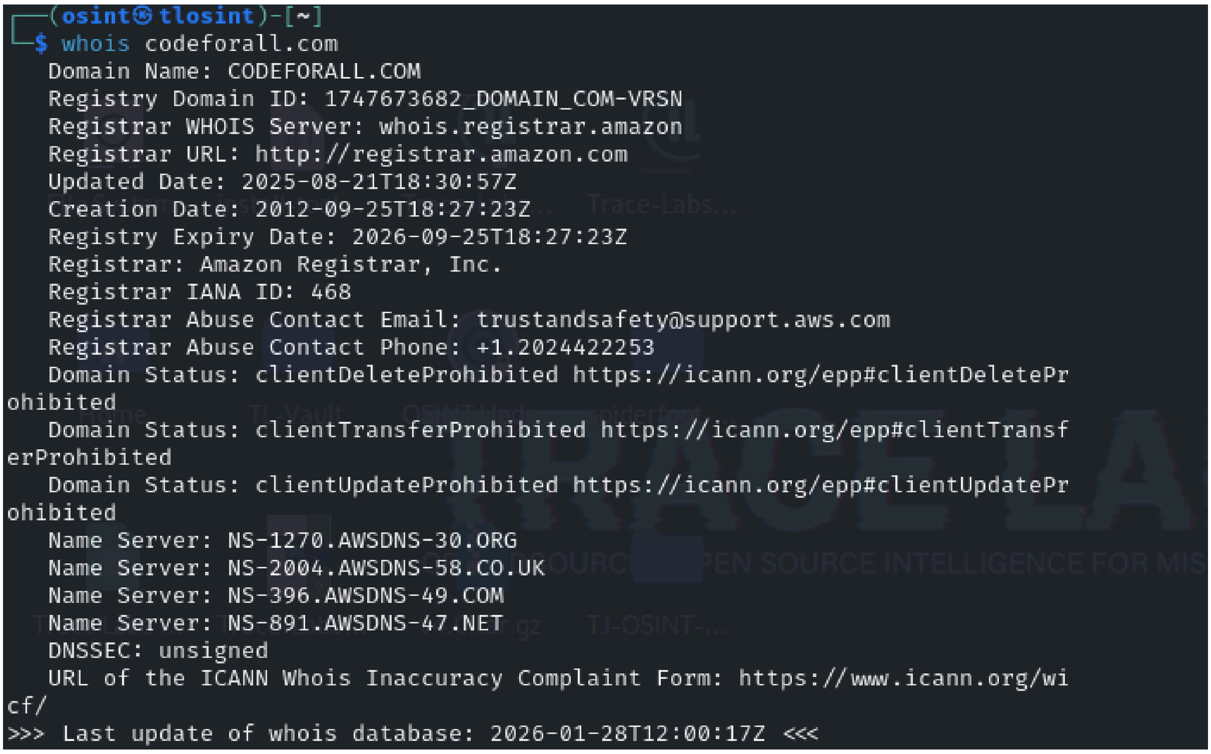
**Brandon Gracy** **28/01/2026**

In this lab, we are going to use techniques to gather information about individuals and organizations using only publicly available tools and data. This simulates the reconnaissance phase of a penetration test or social engineering operation.

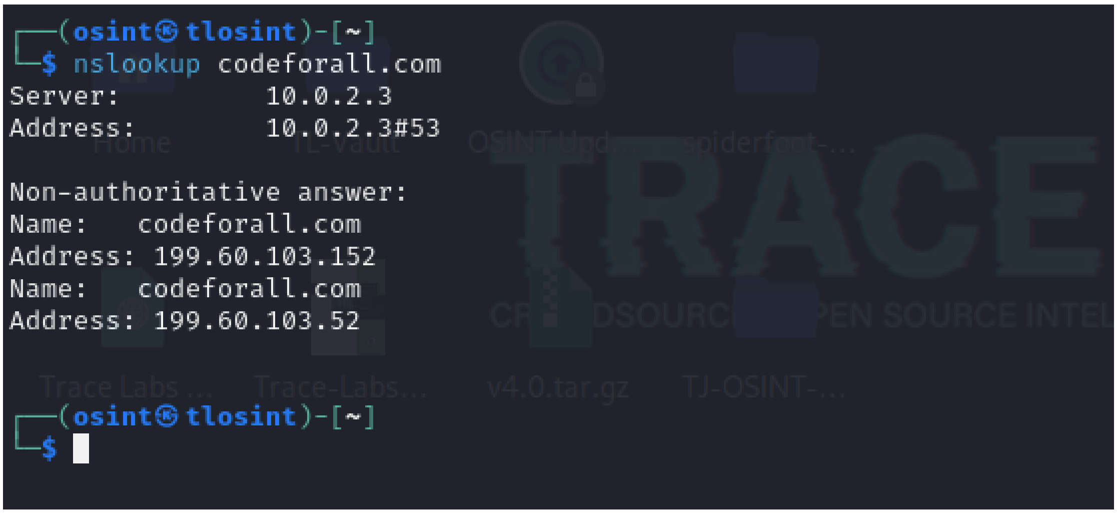
- Domain reconnaissance

Let's start by doing some reconnaissance on the website testphp.vulnweb.com., and see the results.



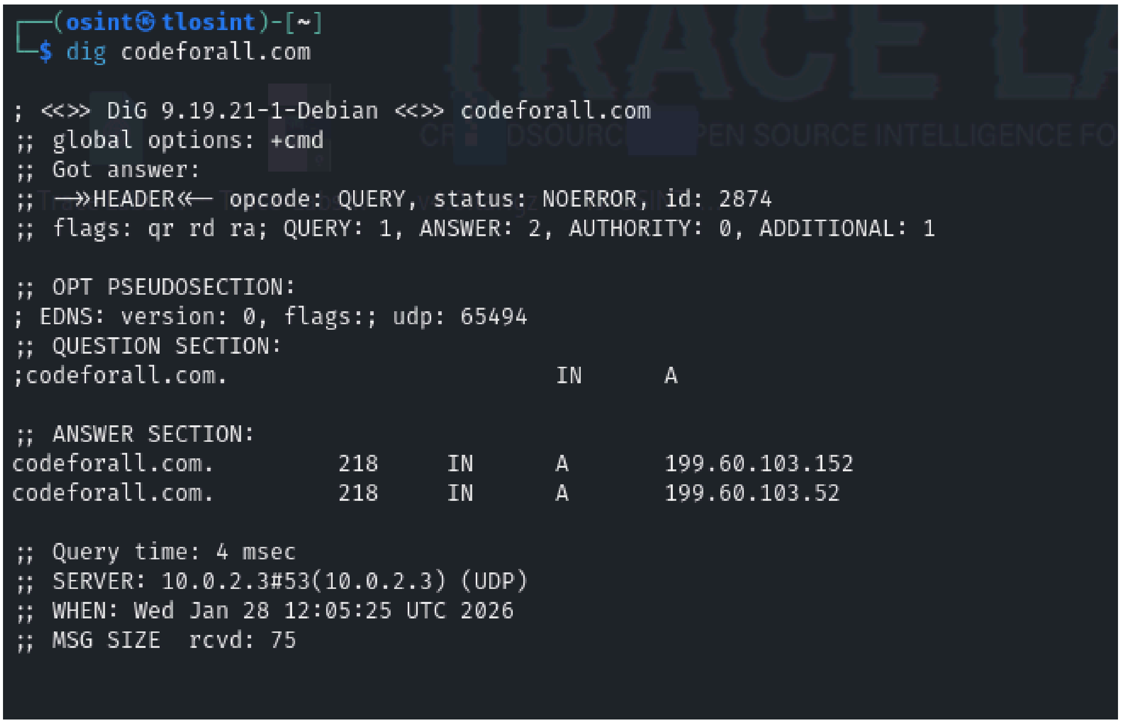
```
┌──(osint㉿tlosint)-[~]
└─$ whois codeforall.com
   Domain Name: CODEFORALL.COM
   Registry Domain ID: 1747673682_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.registrar.amazon
   Registrar URL: http://registrar.amazon.com
   Updated Date: 2025-08-21T18:30:57Z
   Creation Date: 2012-09-25T18:27:23Z
   Registry Expiry Date: 2026-09-25T18:27:23Z
   Registrar: Amazon Registrar, Inc.
   Registrar IANA ID: 468
   Registrar Abuse Contact Email: trustandsafety@support.aws.com
   Registrar Abuse Contact Phone: +1.2024422253
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeletePr
ohibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf
erProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdatePr
ohibited
   Name Server: NS-1270.AWSDNS-30.ORG
   Name Server: NS-2004.AWSDNS-58.CO.UK
   Name Server: NS-396.AWSDNS-49.COM
   Name Server: NS-891.AWSDNS-47.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi
cf/
>>> Last update of whois database: 2026-01-28T12:00:17Z <<<
```

Here we started with the whois tool to find some information about code for all.



```
┌──(osint㉿tlosint)-[~]
└─$ nslookup codeforall.com
Server:         10.0.2.3
Address:        10.0.2.3#53

Non-authoritative answer:
Name:   codeforall.com
Address: 199.60.103.152
Name:   codeforall.com
Address: 199.60.103.52


┌──(osint㉿tlosint)-[~]
└─$ 
```

Here we used a tool called nslookup, and we found two IP addresses.

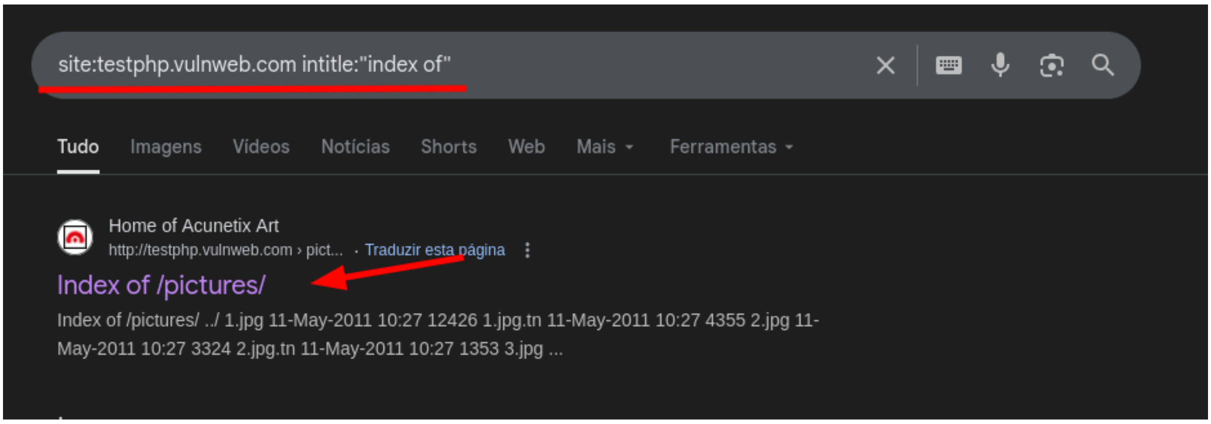


```
┌──(osint㉿tlosint)-[~]
└─$ dig codeforall.com

; <<>> DiG 9.19.21-1-Debian <<>> codeforall.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2874
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;codeforall.com.                        IN      A

;; ANSWER SECTION:
codeforall.com.         218     IN      A       199.60.103.152
codeforall.com.         218     IN      A       199.60.103.52

;; Query time: 4 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Wed Jan 28 12:05:25 UTC 2026
;; MSG SIZE  rcvd: 75
```

Now with the dig tool, we can check some information like nslookup, but with more details.

- Google Dorking

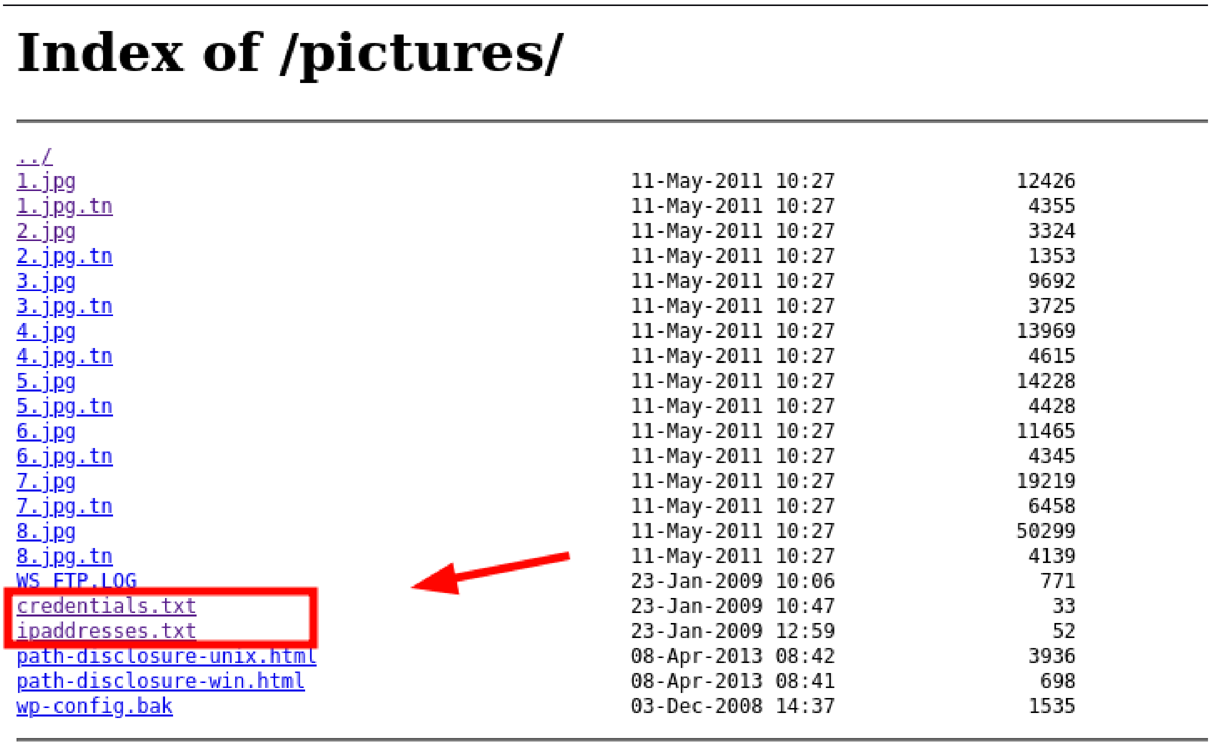
Now, let's see if we can identify any open directories in testphp.vulnweb.com



Index of /pictures/

Index of /pictures/ ../ 1.jpg 11-May-2011 10:27 12426 1.jpg.tn 11-May-2011 10:27 4355 2.jpg 11-May-2011 10:27 3324 2.jpg.tn 11-May-2011 10:27 1353 3.jpg ...

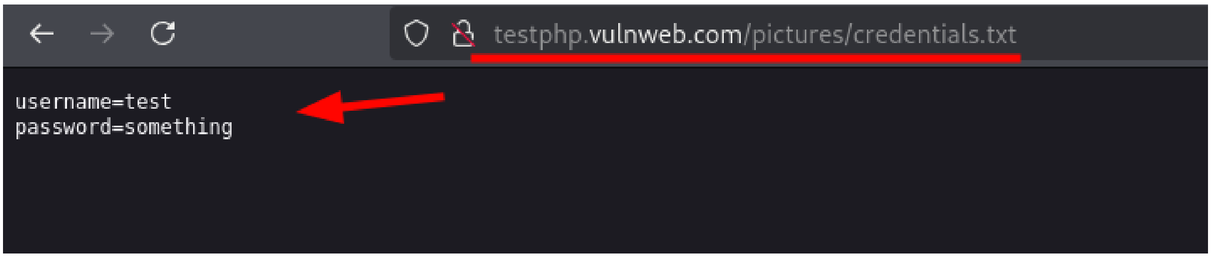
Here we have an example of google dorkink, check that we find a link index of, let’s check what we have inside.



# Index of /pictures/

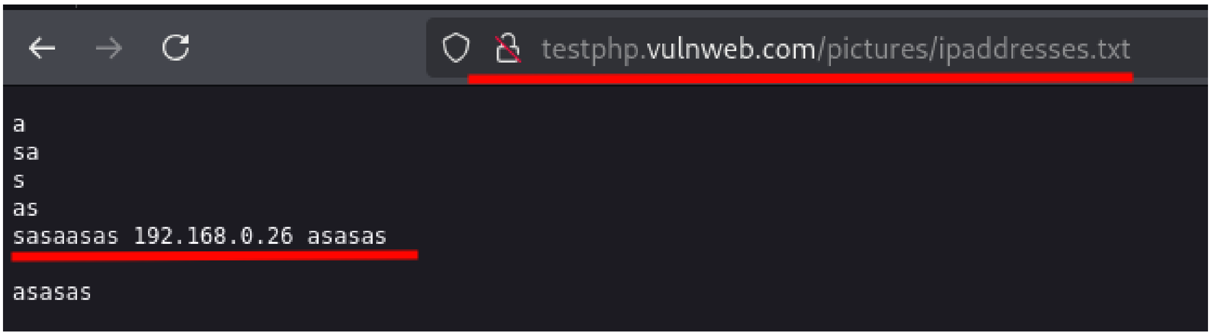
```
../
1.jpg                                              11-May-2011 10:27               12426
1.jpg.tn                                           11-May-2011 10:27                4355
2.jpg                                              11-May-2011 10:27                3324
2.jpg.tn                                           11-May-2011 10:27                1353
3.jpg                                              11-May-2011 10:27                9692
3.jpg.tn                                           11-May-2011 10:27                3725
4.jpg                                              11-May-2011 10:27               13969
4.jpg.tn                                           11-May-2011 10:27                4615
5.jpg                                              11-May-2011 10:27               14228
5.jpg.tn                                           11-May-2011 10:27                4428
6.jpg                                              11-May-2011 10:27               11465
6.jpg.tn                                           11-May-2011 10:27                4345
7.jpg                                              11-May-2011 10:27               19219
7.jpg.tn                                           11-May-2011 10:27                6458
8.jpg                                              11-May-2011 10:27               50299
8.jpg.tn                                           11-May-2011 10:27                4139
WS_FTP.LOG                                         23-Jan-2009 10:06                 771
credentials.txt                                    23-Jan-2009 10:47                  33
ipaddresses.txt                                    23-Jan-2009 12:59                  52
path-disclosure-unix.html                          08-Apr-2013 08:42                3936
path-disclosure-win.html                           08-Apr-2013 08:41                 698
wp-config.bak                                      03-Dec-2008 14:37                1535
```

Here we have some directories to check, but we found two directories that caught my attention, credentials.txt and ipaddresses.txt, let’s check.



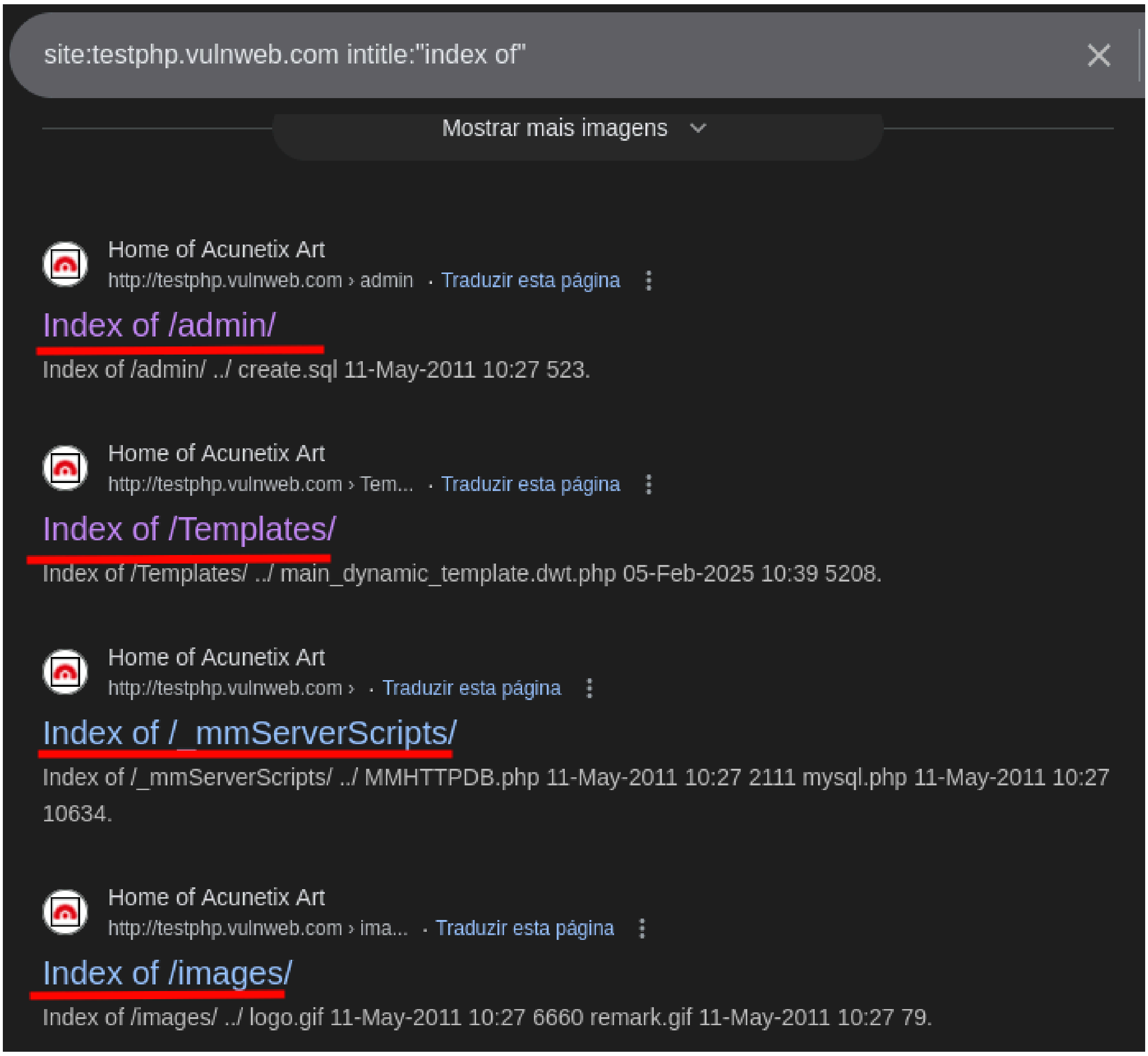
```
username=test
password=something
```

Here we can check that inside of the directory credentials.txt, we have a username and password, it can be important in the future.



```
a
sa
s
as
sasaasas 192.168.0.26 asasas

asasas
```

Here inside of the ipaddresses directory, we found an ip address, let’s keep it.



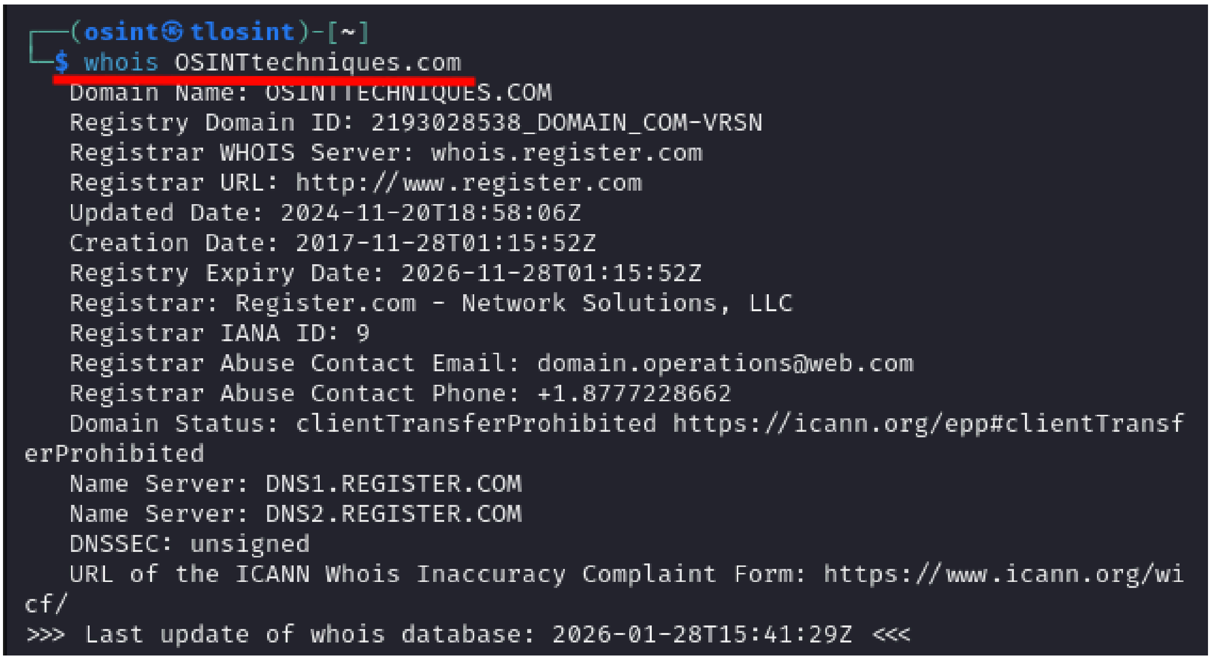
Home of Acunetix Art
http://testphp.vulnweb.com › admin · Traduzir esta página
Index of /admin/
Index of /admin/ ../ create.sql 11-May-2011 10:27 523.

Home of Acunetix Art
http://testphp.vulnweb.com › Tem... · Traduzir esta página
Index of /Templates/
Index of /Templates/ ../ main_dynamic_template.dwt.php 05-Feb-2025 10:39 5208.

Home of Acunetix Art
http://testphp.vulnweb.com › · Traduzir esta página
Index of /_mmServerScripts/
Index of /_mmServerScripts/ ../ MMHTTPDB.php 11-May-2011 10:27 2111 mysql.php 11-May-2011 10:27 10634.

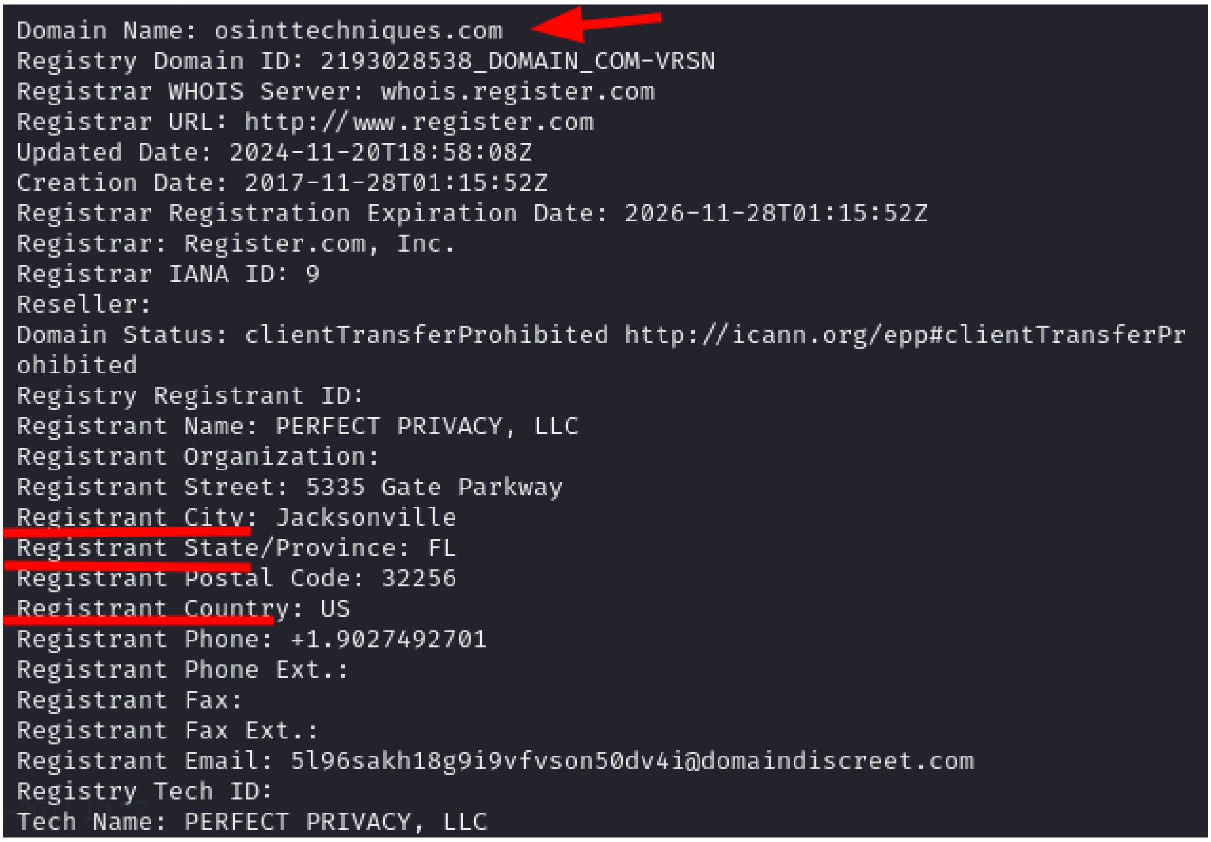
Home of Acunetix Art
http://testphp.vulnweb.com › ima... · Traduzir esta página
Index of /images/
Index of /images/ ../ logo.gif 11-May-2011 10:27 6660 remark.gif 11-May-2011 10:27 79.

And we have more options to check if we want with the filter “index of”.



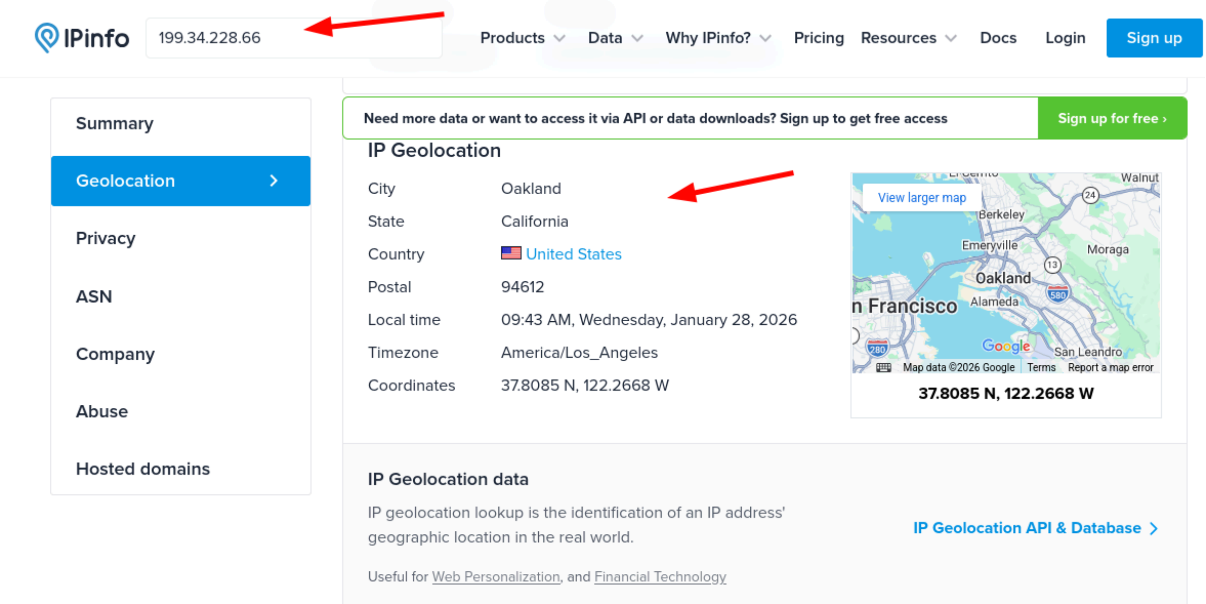
```
┌──(osint㉿tlosint)-[~]
└─$ whois OSINTtechniques.com
   Domain Name: OSINTTECHNIQUES.COM
   Registry Domain ID: 2193028538_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.register.com
   Registrar URL: http://www.register.com
   Updated Date: 2024-11-20T18:58:06Z
   Creation Date: 2017-11-28T01:15:52Z
   Registry Expiry Date: 2026-11-28T01:15:52Z
   Registrar: Register.com - Network Solutions, LLC
   Registrar IANA ID: 9
   Registrar Abuse Contact Email: domain.operations@web.com
   Registrar Abuse Contact Phone: +1.8777228662
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransf
erProhibited
   Name Server: DNS1.REGISTER.COM
   Name Server: DNS2.REGISTER.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wi
cf/
>>> Last update of whois database: 2026-01-28T15:41:29Z <<<
```

Now, with whois, let’s try to find some geolocation related to the OSINTtechniques.



```
Domain Name: osinttechniques.com
Registry Domain ID: 2193028538_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.register.com
Registrar URL: http://www.register.com
Updated Date: 2024-11-20T18:58:08Z
Creation Date: 2017-11-28T01:15:52Z
Registrar Registration Expiration Date: 2026-11-28T01:15:52Z
Registrar: Register.com, Inc.
Registrar IANA ID: 9
Reseller:
Domain Status: clientTransferProhibited http://icann.org/epp#clientTransferPr
ohibited
Registry Registrant ID:
Registrant Name: PERFECT PRIVACY, LLC
Registrant Organization:
Registrant Street: 5335 Gate Parkway
Registrant City: Jacksonville
Registrant State/Province: FL
Registrant Postal Code: 32256
Registrant Country: US
Registrant Phone: +1.9027492701
Registrant Phone Ext.:
Registrant Fax:
Registrant Fax Ext.:
Registrant Email: 5l96sakh18g9i9vfvson50dv4i@domaindiscreet.com
Registry Tech ID:
Tech Name: PERFECT PRIVACY, LLC
```

Here we found some important information, like, Domain name, city, state and country.



Need more data or want to access it via API or data downloads? Sign up to get free access

IP Geolocation

| | |
|---|---|
| City | Oakland |
| State | California |
| Country | United States |
| Postal | 94612 |
| Local time | 09:43 AM, Wednesday, January 28, 2026 |
| Timezone | America/Los_Angeles |
| Coordinates | 37.8085 N, 122.2668 W |

37.8085 N, 122.2668 W

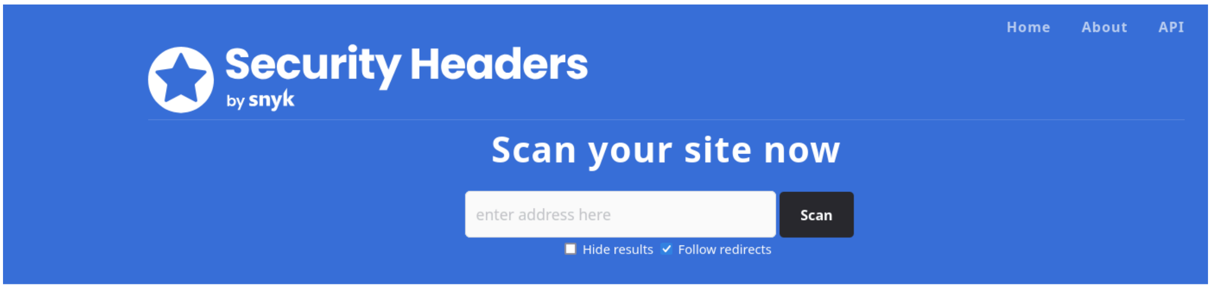
IP Geolocation data

IP geolocation lookup is the identification of an IP address' geographic location in the real world.

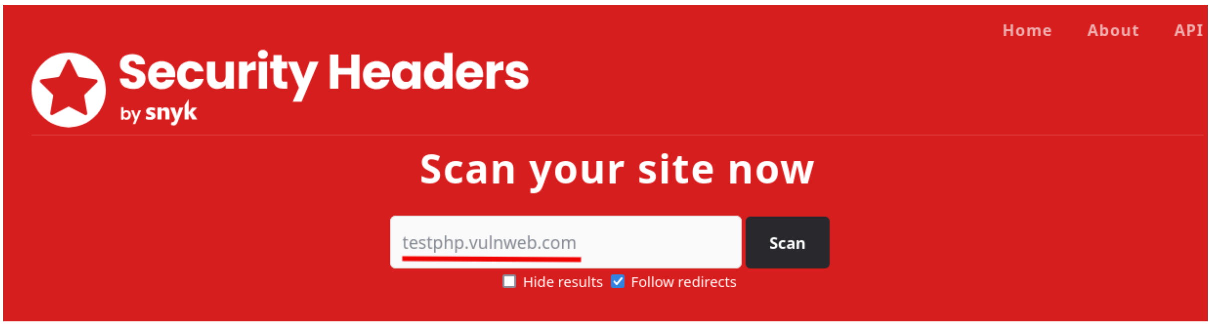
Useful for Web Personalization, and Financial Technology

If we put the IP address that we found in some site of ip location, we can check more details.

- Security Headers Check



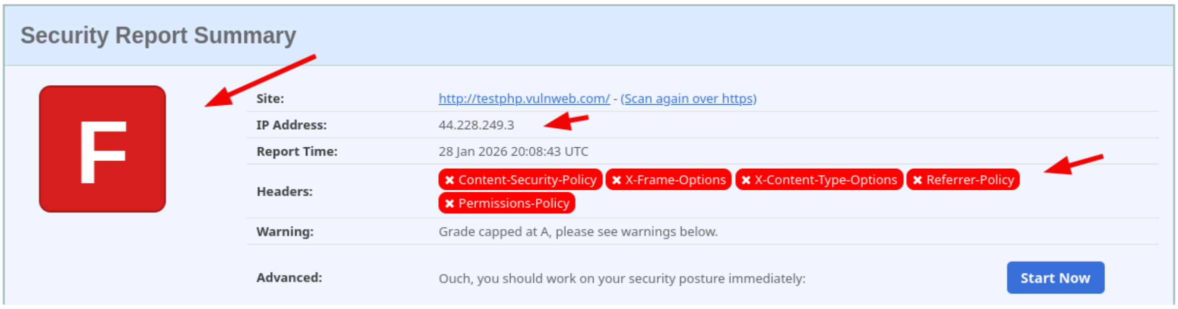
Now, we are going to use a web tool called securityheaders.com , it is an online tool that analyzes a website and shows which security headers it is using and which ones are missing.



Scan your site now

testphp.vulnweb.com

☐ Hide results ☑ Follow redirects

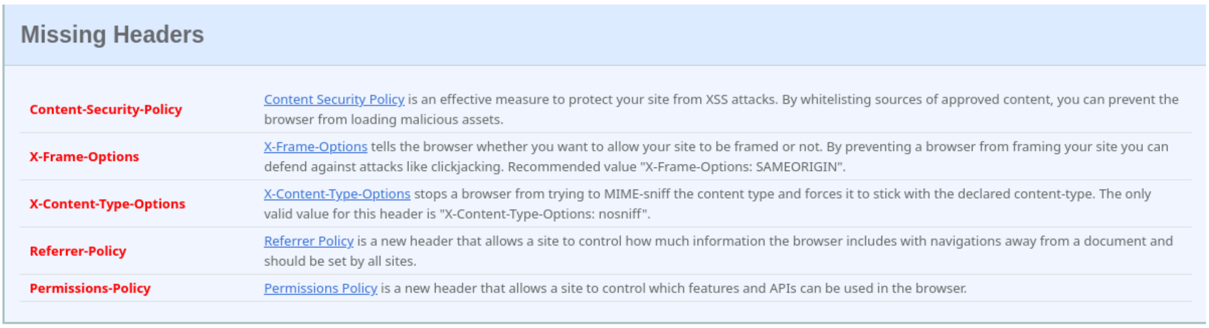


Security Report Summary

F

| | |
|---|---|
| Site: | http://testphp.vulnweb.com/ - (Scan again over https) |
| IP Address: | 44.228.249.3 |
| Report Time: | 28 Jan 2026 20:08:43 UTC |
| Headers: | ✗ Content-Security-Policy ✗ X-Frame-Options ✗ X-Content-Type-Options ✗ Referrer-Policy ✗ Permissions-Policy |
| Warning: | Grade capped at A, please see warnings below. |
| Advanced: | Ouch, you should work on your security posture immediately: |

Here we can check some important information, like, we scanned the testphp.vulnweb.com, in the headers part, we can check that there are five security headers that are missing on this site, and we can check the rating on this site, which is terrible.



Missing Headers

| | |
|---|---|
| Content-Security-Policy | Content Security Policy is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets. |
| X-Frame-Options | X-Frame-Options tells the browser whether you want to allow your site to be framed or not. By preventing a browser from framing your site you can defend against attacks like clickjacking. Recommended value "X-Frame-Options: SAMEORIGIN". |
| X-Content-Type-Options | X-Content-Type-Options stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff". |
| Referrer-Policy | Referrer Policy is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites. |
| Permissions-Policy | Permissions Policy is a new header that allows a site to control which features and APIs can be used in the browser. |

Now, let’s talk a little about this five security headers,

1) Content-Security-Policy (CSP), Controls where the website can load content (scripts, images, iframes, etc.) without the CSP the site may be vulnerable to XSS(cross-site scripting), very high importance.

2) X-Frame-Options, It indicates whether the website can be loaded within an iframe. Without this, the site may suffer

Clickjacking (The user thinks they are clicking on one thing, but it's something else) high importance.

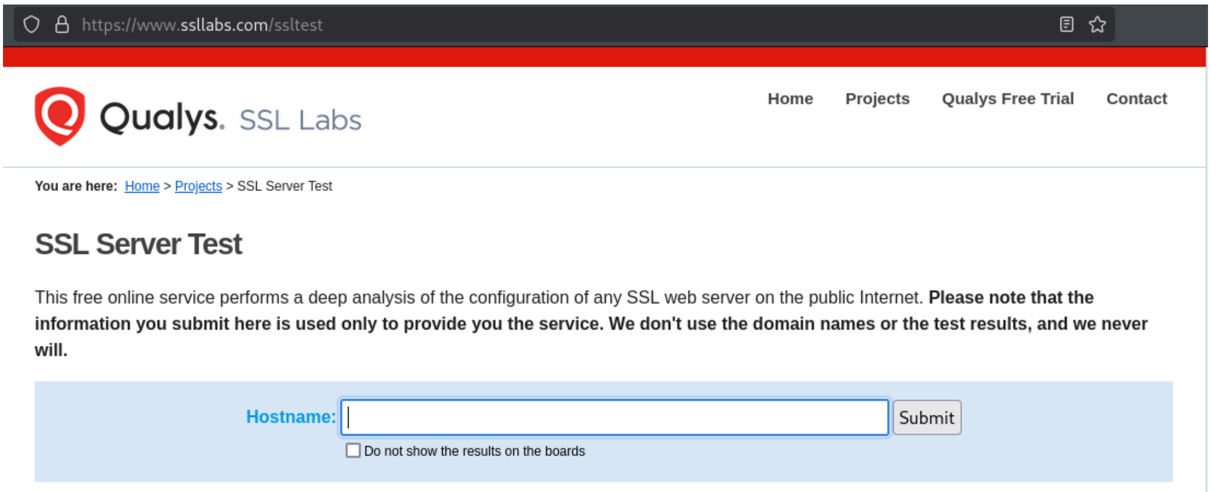
3) X-Content-Type-Options, It prevents the browser from "guessing" the file type, Without this, the following may occur executing files as scripts when they shouldn't, medium importance.

4) Referrer-Policy, Controls what source information is sent when the user clicks on links; without this Internal URLs can leak, Sensitive parameters may be exposed, medium importance.

5) Permissions-Policy, Controls access to browser resources, camera, microphone, location, Without it Scripts may request unnecessary permissions, medium importance.

The main recommendation is to correctly implement HTTP security headers, as they significantly reduce the risk of common web attacks.

- SSL/TLS Analysis



You are here: Home > Projects > SSL Server Test

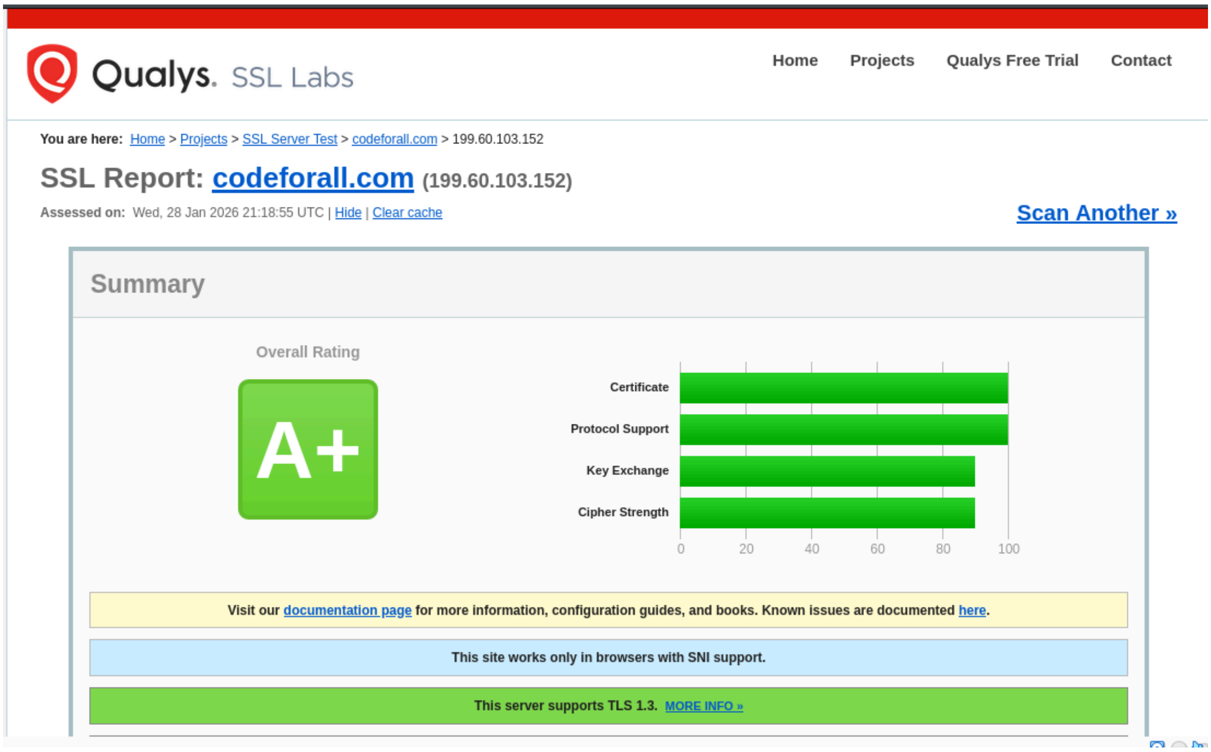
SSL Server Test

This free online service performs a deep analysis of the configuration of any SSL web server on the public Internet. **Please note that the information you submit here is used only to provide you the service. We don't use the domain names or the test results, and we never will.**

Hostname:

□ Do not show the results on the boards

Now, we are going to use a new tool, https://ssllabs.com/ssltest, The SSL Labs SSL Test tool is used to analyze a website's HTTPS security configuration. It evaluates the digital certificate, the encryption protocols used, the strength of the ciphers, and the presence of known vulnerabilities. Based on these criteria, the tool assigns a score indicating the level of security of the communication between the user and the server.



You are here: Home > Projects > SSL Server Test > codeforall.com > 199.60.103.152

SSL Report: codeforall.com (199.60.103.152)

Assessed on: Wed, 28 Jan 2026 21:18:55 UTC | Hide | Clear cache

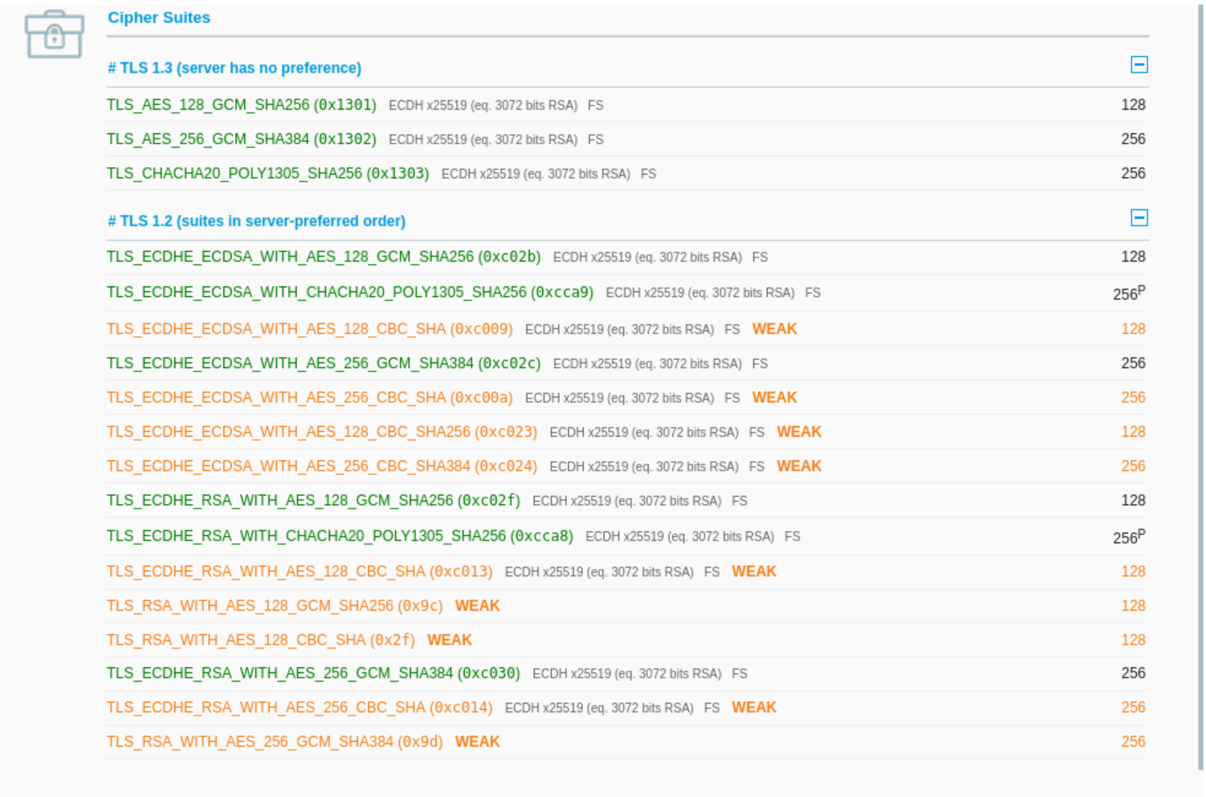
Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This site works only in browsers with SNI support.

This server supports TLS 1.3. MORE INFO »

Here we put a domain in the url field, which was supposed to be another site, the testphp.vulnweb.com, but it is out of system, let’s check the code for all domains however.

In this image we can check that code for all has the greatest rating score. It 's very safe. We can check the supported TLS version is 1.3.



Cipher Suites

| # TLS 1.3 (server has no preference) | | |
|---|---|---|
| TLS_AES_128_GCM_SHA256 (0x1301) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_AES_256_GCM_SHA384 (0x1302) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_CHACHA20_POLY1305_SHA256 (0x1303) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |

| # TLS 1.2 (suites in server-preferred order) | | |
|---|---|---|
| TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9) | ECDH x25519 (eq. 3072 bits RSA) FS | 256P |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xc009) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xc00a) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xc023) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xc024) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) | ECDH x25519 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8) | ECDH x25519 (eq. 3072 bits RSA) FS | 256P |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK** | | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK** | | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) | ECDH x25519 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) | ECDH x25519 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK** | | 256 |

Here we can check some weak and misconfigurations.

In my opinion, the tool that i liked it the most was Sherlock, i think it is very useful, we got a lot of information that can be used to a reconnaissance, OSINT only uses information that the company itself allows to be released; OSINT never hacks, so we must train our employees to prevent this from happening, remove sensitive information from the web, reduce infrastructure exposure, among other things.