DomainTools PROFILE CONNECT MONITOR SUPPORT Whois Lookup

Domain Profile

Registrar	Go Daddy, LLC IANA ID: 146 URL: https://www.godaddy.com/ Whois Server: whois.godaddy.com abuse@godaddy.com (p) +1.4805058800
Registrar Status	clientDeleteProhibited, clientRenewProhibited, clientTransferProhibited, clientUpdateProhibited
Dates	150 days old Created on 2024-06-19 Expires on 2025-06-19 Updated on 2024-09-06
Name Servers	NS-1389.AWSDNS-45.ORG (has 61,169 domains) NS-1998.AWSDNS-57.CO.UK (has 271 domains) NS-463.AWSDNS-57.COM (has 1,847 domains) NS-699.AWSDNS-23.NET (has 43 domains)
IP Address	76.76.21.98 - 65,963 other sites hosted on this server
IP Location	- California - Walnut - Vercel Inc
ASN	AS16509 AMAZON-02, US (registered May 04, 2000)
IP History	50 changes on 50 unique IP addresses over 0 years
Hosting History	2 changes on 3 unique name servers over 0 year

Whois Record (last updated on 2024-11-16)

```
Domain Name: PAYMEFIN.TECH
Registry Domain ID: D464700684-CNIC
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2024-09-06T05:38:08.0Z
Creation Date: 2024-06-19T07:51:31.0Z
Registry Expiry Date: 2025-06-19T23:59:59.0Z
```

```
Registrar WHOIS Server: whois.godaddy.com
Registrar URL: https://www.godaddy.com/
Updated Date: 2024-09-06T05:38:08.0Z
Creation Date: 2024-06-19T07:51:31.0Z
Registry Expiry Date: 2025-06-19T23:59:59.0Z
Registrar: Go Daddy, LLC
Registrar IANA ID: 146
Domain Status: clientRenewProhibited https://icann.org/epp#clientRenewProhibited
Domain Status: clientTransferProhibited https://icann.org
/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Registrant Organization: Domains By Proxy, LLC
Registrant State/Province: Arizona
Registrant Country: US
Registrant Email: Please query the RDDS service of the Registrar of Record identifie
d in this
output for information on how to contact the Registrant, Admin, or Tech contact of t
he queried
domain name.
Admin Email: Please query the RDDS service of the Registrar of Record identified in
this
output for information on how to contact the Registrant, Admin, or Tech contact of t
he queried
domain name.
Tech Email: Please query the RDDS service of the Registrar of Record identified in t
his output
for information on how to contact the Registrant, Admin, or Tech contact of the quer
ied domain
name.
Name Server: NS-1389.AWSDNS-45.ORG
Name Server: NS-1998.AWSDNS-57.CO.UK
Name Server: NS-463.AWSDNS-57.COM
Name Server: NS-699.AWSDNS-23.NET
DNSSEC: unsigned
Billing Email: Please query the RDDS service of the Registrar of Record identified i
n this
output for information on how to contact the Registrant, Admin, or Tech contact of t
he queried
domain name.
Registrar Abuse Contact Email:  abuse@godaddy.com
Registrar Abuse Contact Phone: +1.4805058800
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
```


File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# nslookup paymefin.tech
Server: 192.168.29.1
Address: 192.168.29.1#53
Non-authoritative answer:
Name: paymefin.tech
Address: 76.76.21.21
┌──(root㉿kali)-[~]
└─# traceroute paymefin.tech
traceroute to paymefin.tech (76.76.21.21), 30 hops max, 60 byte packets
1 reliance.reliance (192.168.29.1) 2.495 ms 3.935 ms 5.758 ms
2 10.12.112.1 (10.12.112.1) 12.086 ms 11.971 ms 11.832 ms
3 172.16.18.5 (172.16.18.5) 14.369 ms 14.230 ms 172.16.18.29 (172.16.18.2
9) 11.752 ms
4 192.168.96.238 (192.168.96.238) 10.942 ms 192.168.96.234 (192.168.96.234
) 13.416 ms 192.168.96.240 (192.168.96.240) 12.856 ms
5 172.26.111.117 (172.26.111.117) 12.164 ms 11.696 ms 11.583 ms
6 172.26.111.131 (172.26.111.131) 11.435 ms 5.875 ms 7.006 ms
7 192.168.44.46 (192.168.44.46) 6.882 ms 192.168.44.42 (192.168.44.42) 6.
713 ms 192.168.44.48 (192.168.44.48) 6.610 ms
8 * * *
9 * * *
10 * * *
11 49.44.18.38 (49.44.18.38) 42.270 ms * *
12 * * *
13 49.44.18.38 (49.44.18.38) 398.297 ms 99.83.67.32 (99.83.67.32) 394.217
ms 49.44.18.38 (49.44.18.38) 147.438 ms
14 * * *
15 99.83.67.32 (99.83.67.32) 29.038 ms * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
┌──(root㉿kali)-[~]

```
┌──(root㉿kali)-[~]
└─# nikto -host paymefin.tech
- Nikto v2.5.0
---------------------------------------------------------------------------
+ Target IP:          76.76.21.21
+ Target Hostname:    paymefin.tech
+ Target Port:        80
+ Start Time:         2024-11-16 09:30:05 (GMT-5)
---------------------------------------------------------------------------
+ Server: Vercel
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'refresh' found, with contents: 0;url=https://paymefin.tech/.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.
anner/vulnerabilities/missing-content-type-header/
+ Root page / redirects to: https://paymefin.tech/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /database.cer: Uncommon header 'x-vercel-id' found, with contents: bom1::m65hj-1731767488284-82f62f746573.
+ /file/../../../../../../../../../etc/: Uncommon header 'x-vercel-mitigated' found, with contents: challenge.
+ /file/../../../../../../../../../etc/: Uncommon header 'x-vercel-challenge-token' found, with contents: 2.1731767732.60.NzBjNDU0MTRkMDg3YWY0ZTcwZWIwNzg1NTQzN2FmMGY7M2ZhMGM4OWE7
iOWY3MjA2ODc5ZWUxNjs0O1w5+aTcjLHuoYRbWW81aeJRYrlG4/LOvttHJrYDACUeX/zh1b+Rpr40fx7o/qcL7mA2WwYd/Y173XQ/eE77ATpHy6TPBHqumQc=.dcbb205a3081bbff1e6a9f01da6ba291.
+ ERROR: Error limit (20) reached for host, giving up. Last error:
+ Scan terminated: 6 error(s) and 6 item(s) reported on remote host
+ End Time:           2024-11-16 09:52:42 (GMT-5) (1357 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

```
File  Actions  Edit  View  Help
skipfish version 2.10b by lcamtuf@google.com

  - paymefin.tech -

Scan statistics:

      Scan time : 0:01:11.064
  HTTP requests : 1096 (15.4/s), 33635 kB in, 200 kB out (476.1 kB/s)
    Compression : 0 kB in, 0 kB out (0.0% gain)
    HTTP faults : 0 net errors, 0 proto errors, 0 retried, 0 drops
 TCP handshakes : 14 total (78.4 req/conn)
     TCP faults : 0 failures, 0 timeouts, 4 purged
 External links : 0 skipped
   Reqs pending : 1

Database statistics:

         Pivots : 2 total, 2 done (100.00%)
     In progress : 0 pending, 0 init, 0 attacks, 0 dict
  Missing nodes : 0 spotted
     Node types : 1 serv, 1 dir, 0 file, 0 pinfo, 0 unkn, 0 par, 0 val
   Issues found : 6 info, 0 warn, 1 low, 0 medium, 0 high impact
      Dict size : 2 words (2 new), 1 extensions, 256 candidates
     Signatures : 77 total

[+] Copying static resources ...
[+] Sorting and annotating crawl nodes: 2
[+] Looking for duplicate entries: 2
[+] Counting unique nodes: 2
[+] Saving pivot data for third-party tools ...
[+] Writing scan description ...
[+] Writing crawl tree: 2
[+] Generating summary views ...
[+] Report saved to 'skip/index.html' [0×adaa76d4].
[+] This was a great day for science!

┌──(kali㉿kali)-[~]
└─$
```

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hackin

Crawl results - click to expand:

https://paymefin.tech/ 1 6
Code: 403, length: 30901, declared: text/html, detected: application/xhtml+xml, charset: utf-8 [show trace +]

Document type overview - click to expand:

application/xhtml+xml (1)

text/plain (1)

Issue type overview - click to expand:

SSL certificate host name mismatch (1)

1. https://paymefin.tech/ [show trace +]
   Memo: HV

Generic MIME used (low risk) (1)

1. https://paymefin.tech/ [show trace +]
   Memo: text/plain

New 404 signature seen (1)

1. https://paymefin.tech/sfi9876 [show trace +]

New 'X-*' header value seen (2)

1. https://paymefin.tech/ [show trace +]
   Memo: X-Vercel-Challenge-Token
2. https://paymefin.tech/ [show trace +]
   Memo: X-Vercel-Mitigated

New 'Server' header value seen (1)

1. https://paymefin.tech/ [show trace +]
   Memo: Vercel

SSL certificate issuer information (1)

1. https://paymefin.tech/ [show trace +]
   Memo: /C=US/O=Let's Encrypt/CN=R10

NOTE: 100 samples maximum per issue or document type.

Wapiti vulnerability report

Target: https://paymefin.tech/

Date of the scan: Sat, 16 Nov 2024 14:42:37 +0000. Scope of the scan: folder

Summary

Category	Number of vulnerabilities found
Backup file	0
Blind SQL Injection	0
Weak credentials	0
CRLF Injection	0
Content Security Policy Configuration	1
Cross Site Request Forgery	0
Potentially dangerous file	0
Command execution	0
Path Traversal	0
Htaccess Bypass	0
HTTP Secure Headers	3
HttpOnly Flag cookie	0
Open Redirect	0
Secure Flag cookie	0
SQL Injection	0
Server Side Request Forgery	0
Cross Site Scripting	0

Cross Site Scripting	0
XML External Entity	0
Internal Server Error	0
Resource consumption	0
Fingerprint web technology	0

Content Security Policy Configuration

Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
CSP is not set
```

Solutions

Configuring Content Security Policy involves adding the Content-Security-Policy HTTP header to a web page and giving it values to control what resources the user agent is allowed to load for that page.

References

- Mozilla: Content Security Policy (CSP)
- OWASP: Content Security Policy Cheat Sheet
- OWASP: How to do Content Security Policy (PDF)

HTTP Secure Headers

Description

HTTP security headers tell the browser how to behave when handling the website's content.

Vulnerability found in /

HTTP Secure Headers

Description

HTTP security headers tell the browser how to behave when handling the website's content.

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-Frame-Options is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-XSS-Protection is not set
```

Vulnerability found in /

Description | HTTP Request | cURL command line

```
X-Content-Type-Options is not set
```

Solutions

Use the recommendations for hardening your HTTP Security Headers.

References

- Netsparker: HTTP Security Headers: An Easy Way to Harden Your Web Applications
- KeyCDN: Hardening Your HTTP Security Headers
- OWASP: HTTP SECURITY HEADERS (Protection For Browsers) (PDF)