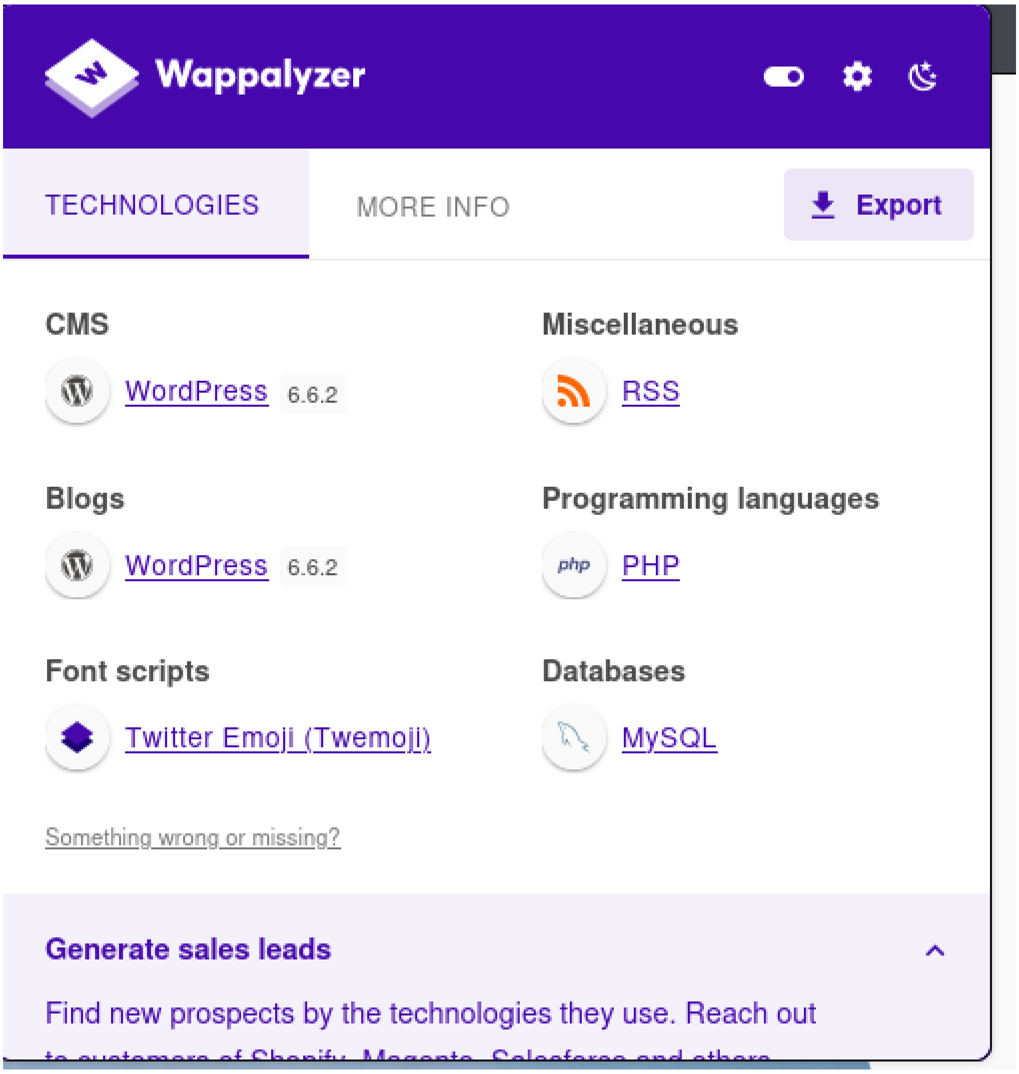
Analyse du site wordpress

https://env-9206928-wp02-nosecure.hidora.com/



CMS

WordPress 6.6.2

Miscellaneous

RSS

Blogs

WordPress 6.6.2

Programming languages

PHP

Font scripts

Twitter Emoji (Twemoji)

Databases

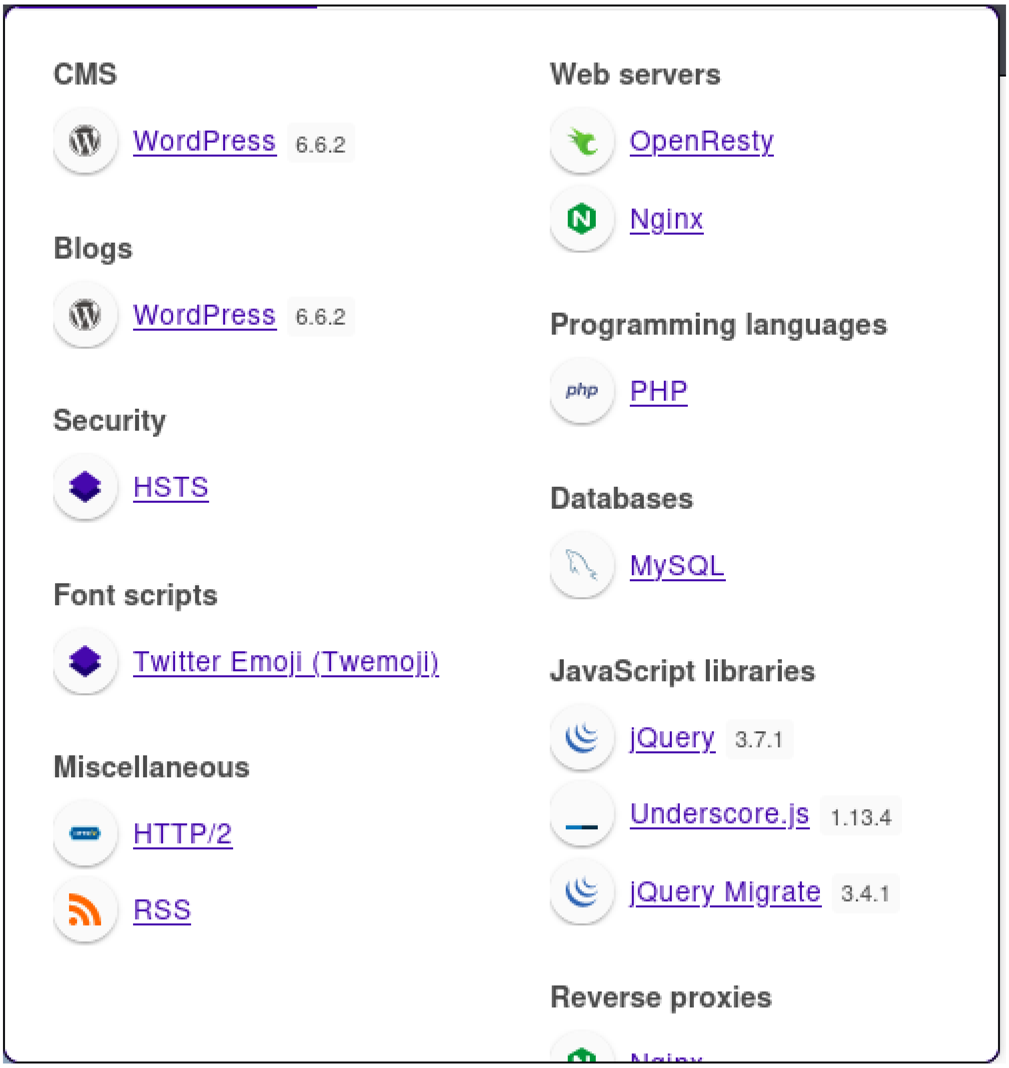
MySQL

Something wrong or missing?

Generate sales leads

Find new prospects by the technologies they use. Reach out to customers of Shopify, Magento, Salesforce and others.

- Utilsation de wapperlyer



CMS

WordPress 6.6.2

Blogs

WordPress 6.6.2

Security

HSTS

Font scripts

Twitter Emoji (Twemoji)

Miscellaneous

HTTP/2

RSS

Web servers

OpenResty

Nginx

Programming languages

PHP

Databases

MySQL

JavaScript libraries

jQuery 3.7.1

Underscore.js 1.13.4

jQuery Migrate 3.4.1

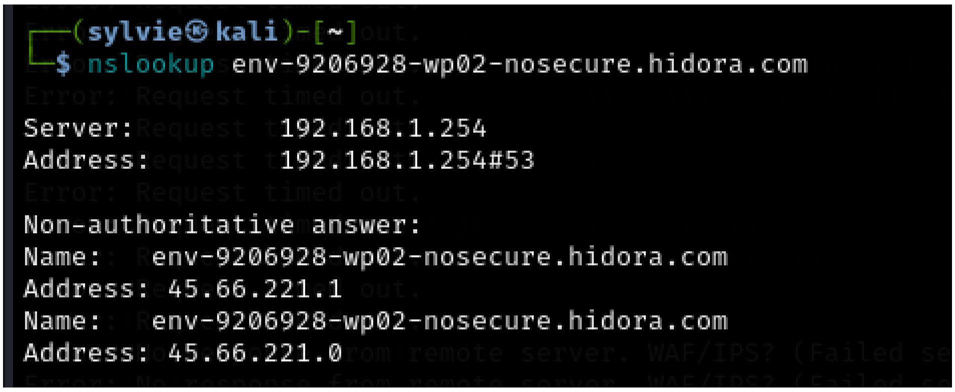
Reverse proxies

Nginx

1. Résumé des Technologies du Site:

- CMS : WordPress 6.6.2 (version actuelle). Serveur Web : Nginx avec un reverse proxy utilisant OpenResty.
- Base de données : MySQL.
- Langage de programmation : PHP.
- Bibliothèques JavaScript : jQuery, Underscore.js, et jQuery Migrate.
- Sécurité : Le site utilise HTTP Strict Transport Security (HSTS), ce qui est un bon point pour la sécurité, car il indique que les connexions doivent être sécurisées via HTTPS.
- Réseau : HTTP/2 est activé, ce qui améliore la performance de la connexion.
- Autres : Le site utilise Twitter Emoji (via Temodji), ce qui peut être lié à l'affichage des émojis.
- Déterminer l'ip associer au domaine

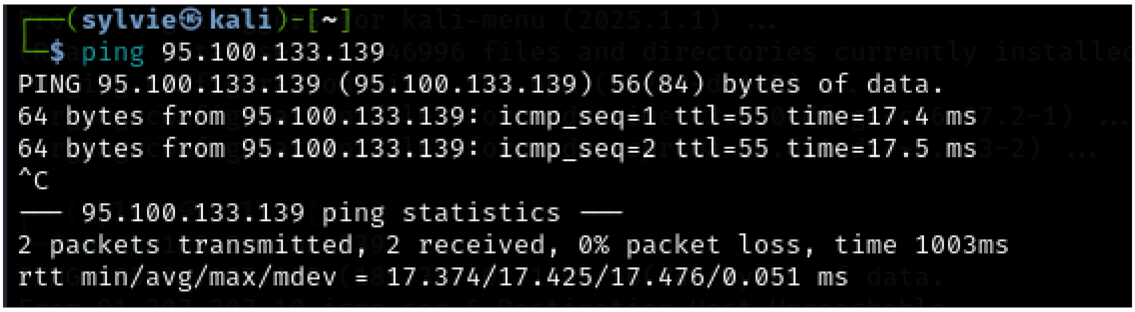
```
nslookup env-9206928-wp02-nosecure.hidora.com
```



```
┌──(sylvie㉿kali)-[~]
└─$ nslookup env-9206928-wp02-nosecure.hidora.com
Server:         192.168.1.254
Address:        192.168.1.254#53

Non-authoritative answer:
Name:   env-9206928-wp02-nosecure.hidora.com
Address: 45.66.221.1
Name:   env-9206928-wp02-nosecure.hidora.com
Address: 45.66.221.0
```

test de conectivité

- Connectivité

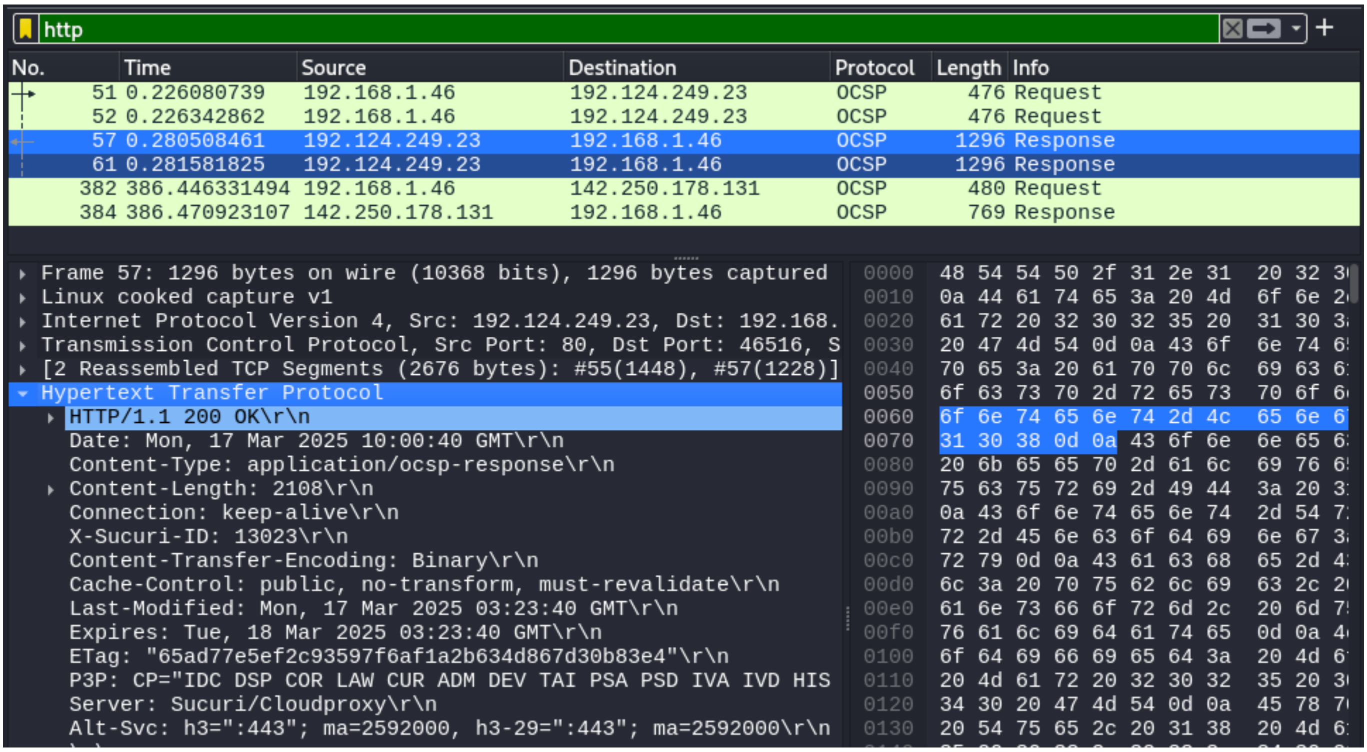


```
┌──(sylvie㉿kali)-[~]
└─$ ping 95.100.133.139
PING 95.100.133.139 (95.100.133.139) 56(84) bytes of data.
64 bytes from 95.100.133.139: icmp_seq=1 ttl=55 time=17.4 ms
64 bytes from 95.100.133.139: icmp_seq=2 ttl=55 time=17.5 ms
^C
--- 95.100.133.139 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1003ms
rtt min/avg/max/mdev = 17.374/17.425/17.476/0.051 ms
```

liste les plugins installés sur le site (des outils comme WPScan peuvent t'aider).

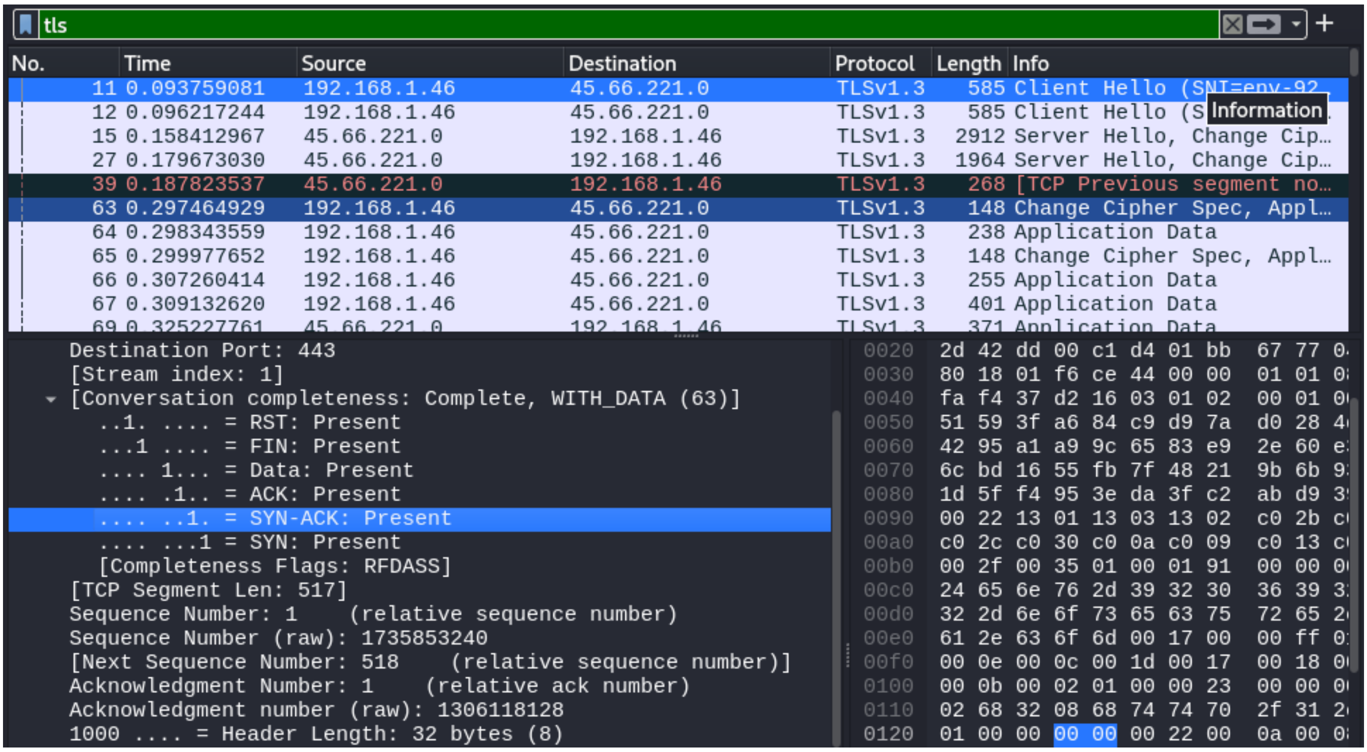
Analyse des flux réseau:

- HTTP



```
http

No.  Time            Source           Destination      Protocol  Length Info
  51 0.226080739     192.168.1.46     192.124.249.23   OCSP         476 Request
  52 0.226342862     192.168.1.46     192.124.249.23   OCSP         476 Request
  57 0.280508461     192.124.249.23   192.168.1.46     OCSP        1296 Response
  61 0.281581825     192.124.249.23   192.168.1.46     OCSP        1296 Response
 382 386.446331494   192.168.1.46     142.250.178.131  OCSP         480 Request
 384 386.470923107   142.250.178.131  192.168.1.46     OCSP         769 Response

▸ Frame 57: 1296 bytes on wire (10368 bits), 1296 bytes captured      0000  48 54 54 50 2f 31 2e 31  20 32
▸ Linux cooked capture v1                                              0010  0a 44 61 74 65 3a 20 4d  6f 6e
▸ Internet Protocol Version 4, Src: 192.124.249.23, Dst: 192.168.     0020  61 72 20 32 30 32 35 20  31 30
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 46516, S     0030  20 47 4d 54 0d 0a 43 6f  6e 74
▸ [2 Reassembled TCP Segments (2676 bytes): #55(1448), #57(1228)]     0040  70 65 3a 20 61 70 70 6c  69 63
▾ Hypertext Transfer Protocol                                          0050  6f 63 73 70 2d 72 65 73  70 6f
  ▸ HTTP/1.1 200 OK\r\n                                                0060  6f 6e 74 65 6e 74 2d 4c  65 6e
    Date: Mon, 17 Mar 2025 10:00:40 GMT\r\n                            0070  31 30 38 0d 0a 43 6f 6e  6e 65
    Content-Type: application/ocsp-response\r\n                        0080  20 6b 65 65 70 2d 61 6c  69 76
  ▸ Content-Length: 2108\r\n                                           0090  75 63 75 72 69 2d 49 44  3a 20
    Connection: keep-alive\r\n                                         00a0  0a 43 6f 6e 74 65 6e 74  2d 54
    X-Sucuri-ID: 13023\r\n                                             00b0  72 2d 45 6e 63 6f 64 69  6e 67
    Content-Transfer-Encoding: Binary\r\n                              00c0  72 79 0d 0a 43 61 63 68  65 2d
    Cache-Control: public, no-transform, must-revalidate\r\n           00d0  6c 3a 20 70 75 62 6c 69  63 2c
    Last-Modified: Mon, 17 Mar 2025 03:23:40 GMT\r\n                   00e0  61 6e 73 66 6f 72 6d 2c  20 6d
    Expires: Tue, 18 Mar 2025 03:23:40 GMT\r\n                         00f0  76 61 6c 69 64 61 74 65  0d 0a
    ETag: "65ad77e5ef2c93597f6af1a2b634d867d30b83e4"\r\n               0100  6f 64 69 66 69 65 64 3a  20 4d
    P3P: CP="IDC DSP COR LAW CUR ADM DEV TAI PSA PSD IVA IVD HIS       0110  20 4d 61 72 20 32 30 32  35 20
    Server: Sucuri/Cloudproxy\r\n                                      0120  34 30 20 47 4d 54 0d 0a  45 78
    Alt-Svc: h3=":443"; ma=2592000, h3-29=":443"; ma=2592000\r\n       0130  20 54 75 65 2c 20 31 38  20 4d
```

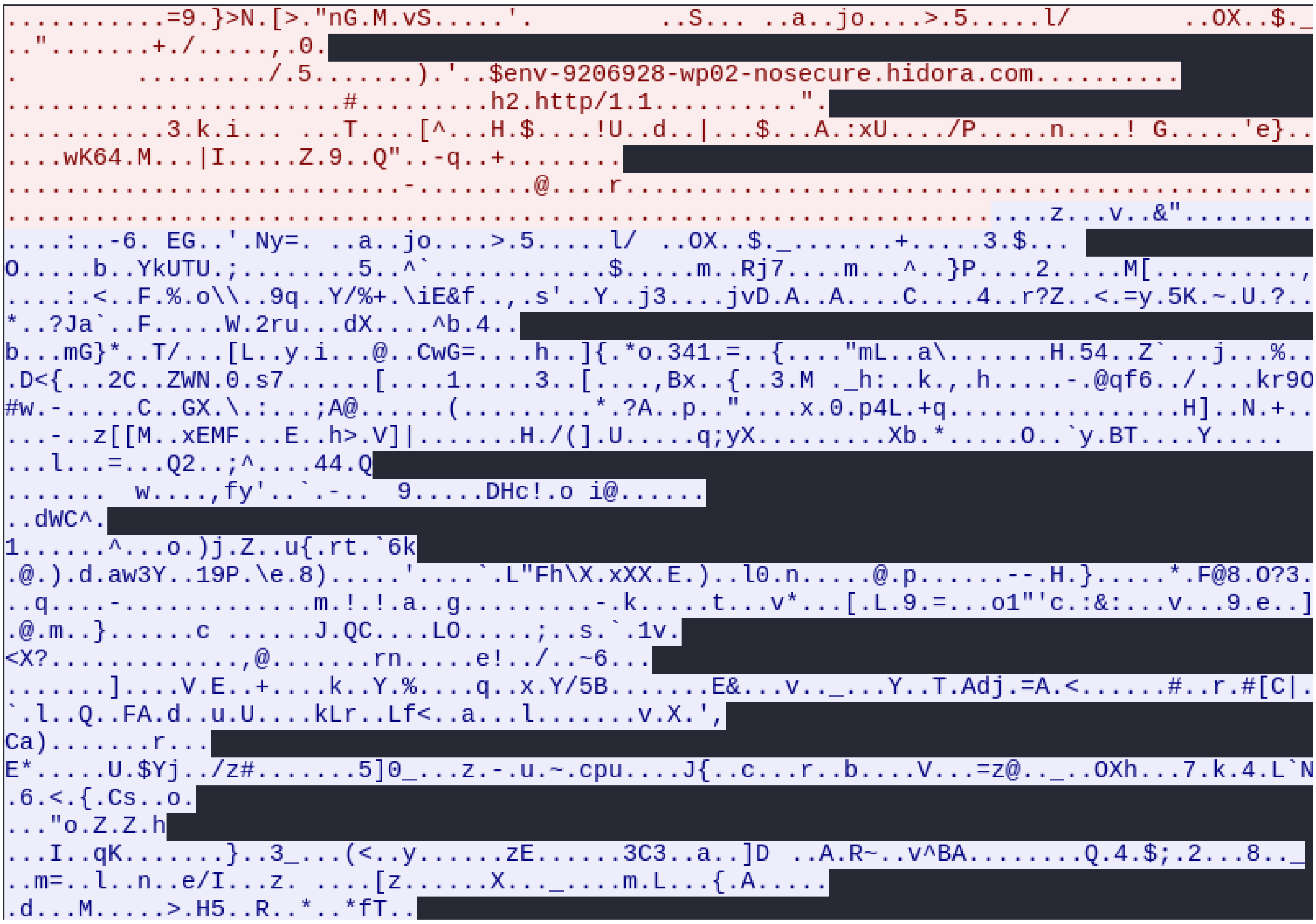
- tls



```
tls
No.   Time         Source         Destination    Protocol  Length Info
   11 0.093759081  192.168.1.46   45.66.221.0    TLSv1.3    585 Client Hello (SNI=env-92
   12 0.096217244  192.168.1.46   45.66.221.0    TLSv1.3    585 Client Hello (S Information
   15 0.158412967  45.66.221.0    192.168.1.46   TLSv1.3   2912 Server Hello, Change Cip…
   27 0.179673030  45.66.221.0    192.168.1.46   TLSv1.3   1964 Server Hello, Change Cip…
   39 0.187823537  45.66.221.0    192.168.1.46   TLSv1.3    268 [TCP Previous segment no…
   63 0.297464929  192.168.1.46   45.66.221.0    TLSv1.3    148 Change Cipher Spec, Appl…
   64 0.298343559  192.168.1.46   45.66.221.0    TLSv1.3    238 Application Data
   65 0.299977652  192.168.1.46   45.66.221.0    TLSv1.3    148 Change Cipher Spec, Appl…
   66 0.307260414  192.168.1.46   45.66.221.0    TLSv1.3    255 Application Data
   67 0.309132620  192.168.1.46   45.66.221.0    TLSv1.3    401 Application Data
   69 0.325227761  45.66.221.0    192.168.1.46   TLSv1.3    371 Application Data
```

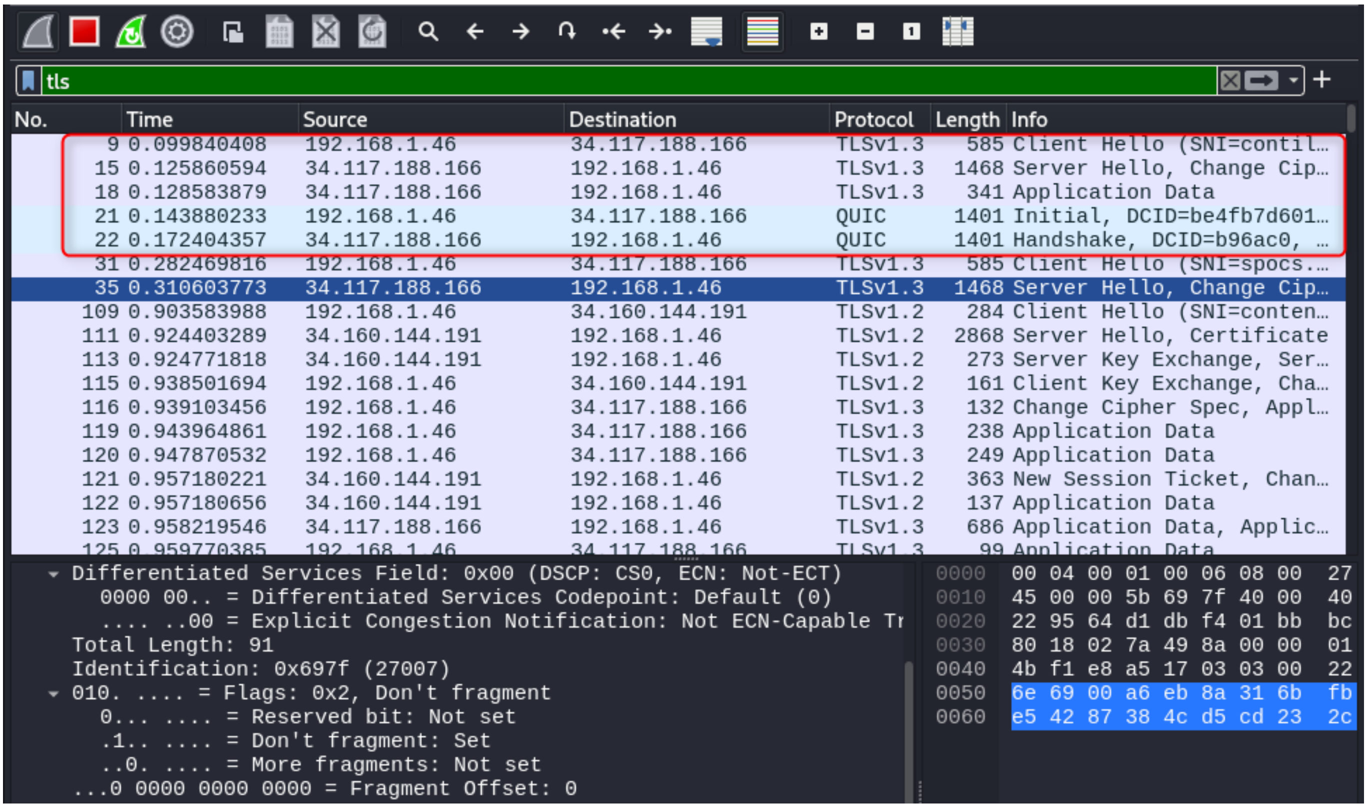
```
    Destination Port: 443                                       0020  2d 42 dd 00 c1 d4 01 bb  67 77 0
    [Stream index: 1]                                           0030  80 18 01 f6 ce 44 00 00  01 01 0
  ▾ [Conversation completeness: Complete, WITH_DATA (63)]       0040  fa f4 37 d2 16 03 01 02  00 01 0
      ..1. .... = RST: Present                                  0050  51 59 3f a6 84 c9 d9 7a  d0 28 4
      ...1 .... = FIN: Present                                  0060  42 95 a1 a9 9c 65 83 e9  2e 60 e
      .... 1... = Data: Present                                 0070  6c bd 16 55 fb 7f 48 21  9b 6b 9
      .... .1.. = ACK: Present                                  0080  1d 5f f4 95 3e da 3f c2  ab d9 3
      .... ..1. = SYN-ACK: Present                              0090  00 22 13 01 13 03 13 02  c0 2b c
      .... ...1 = SYN: Present                                  00a0  c0 2c c0 30 c0 0a c0 09  c0 13 c
      [Completeness Flags: RFDASS]                              00b0  00 2f 00 35 01 00 01 91  00 00 0
    [TCP Segment Len: 517]                                      00c0  24 65 6e 76 2d 39 32 30  36 39 3
    Sequence Number: 1    (relative sequence number)            00d0  32 2d 6e 6f 73 65 63 75  72 65 2
    Sequence Number (raw): 1735853240                           00e0  61 2e 63 6f 6d 00 17 00  00 ff 0
    [Next Sequence Number: 518    (relative sequence number)]   00f0  00 0e 00 0c 00 1d 00 17  00 18 0
    Acknowledgment Number: 1    (relative ack number)           0100  00 0b 00 02 01 00 00 23  00 00 0
    Acknowledgment number (raw): 1306118128                     0110  02 68 32 08 68 74 74 70  2f 31 2
    1000 .... = Header Length: 32 bytes (8)                     0120  01 00 00 00 00 00 22 00  0a 00 0
```

Les données sont cryptées.



```
...........=9.}>N.[>."nG.M.vS.....'.         ..S...  ..a..jo....>.5.....l/       ..OX..$._
.."........+./.....,.0.
.        ........./.5........).'..$env-9206928-wp02-nosecure.hidora.com..........
...........................#.........h2.http/1.1..........".
...........3.k.i...  ...T....[^...H.$....!U..d..|...$...A.:xU..../P.....n....! G.....'e}..
....wK64.M...|I.....Z.9..Q"..-q..+.........
................................-.........@....r.........................................
...................................................................................z...v..&".........
....:..-6. EG..'.Ny=.  ..a..jo....>.5.....l/  ..OX..$._........+.....3.$...
O.....b..YkUTU.;........5..^`.............$.....m..Rj7....m...^..}P....2.....M[..........,
....:.<..F.%.o\\..9q..Y/%+.\iE&f..,.s'..Y..j3....jvD.A..A....C....4..r?Z..<.=y.5K.~.U.?..
*..?Ja`..F.....W.2ru...dX....^b.4..
b...mG}*..T/...[L..y.i...@..CwG=....h..]{.*o.341.=..{...."mL..a\.......H.54..Z`...j...%..
.D<{...2C..ZWN.0.s7......[....1.....3..[....,Bx..{..3.M ._h:..k.,.h.....-.@qf6../....kr9O
#w.-.....C..GX.\.:...;A@......(.........*.?A..p.."....x.0.p4L.+q................H]..N.+..
...-..z[[M..xEMF...E..h>.V]|.......H./(].U.....q;yX.........Xb.*.....O..`y.BT....Y.....
...l...=...Q2..;^....44.Q
.......  w....,fy'..`.-..  9.....DHc!.o i@......
..dWC^.
1......^...o.)j.Z..u{.rt.`6k
.@.).d.aw3Y..19P.\e.8).....'....`.L"Fh\X.xXX.E.)..l0.n.....@.p......--.H.}.....*.F@8.O?3.
..q....-..............m.!.!.a..g.........-.k.....t...v*...[.L.9.=...o1"'c.:&:...v...9.e..]
.@.m..}......c  ......J.QC....LO.....;..s.`.1v.
<X?.............,@.......rn.....e!../..~6...
.......]....V.E..+....k..Y.%....q..x.Y/5B.......E&...v.._...Y..T.Adj.=A.<......#..r.#[C|.
`.l..Q..FA.d..u.U....kLr..Lf<..a...l.......v.X.',
Ca).......r...
E*.....U.$Yj../z#.......5]0_...z.-.u.~.cpu....J{..c...r..b....V...=z@.._..OXh...7.k.4.L`N
.6.<.{.Cs..o.
..."o.Z.Z.h
...I..qK.......}..3_...(<..y......zE......3C3..a..]D  ..A.R~..v^BA........Q.4.$;.2...8.._
..m=..l..n..e/I...z.  ....[z......X..._.....m.L...{.A.....
.d...M.....>.H5..R..*..*fT..
```

- paquets passant par le port 443

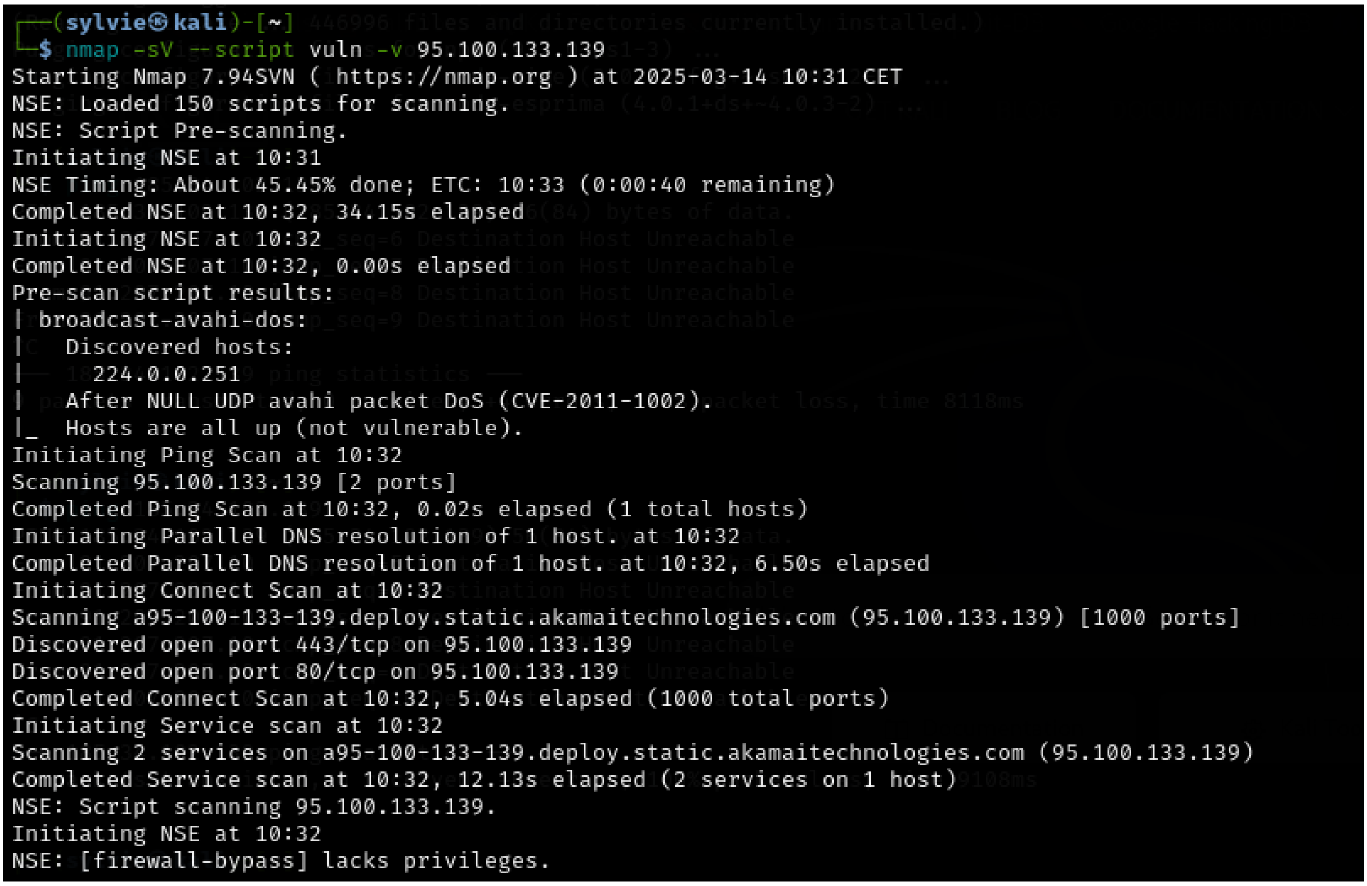


```
No.  Time         Source          Destination     Protocol Length Info
   9 0.099840408  192.168.1.46    34.117.188.166  TLSv1.3   585 Client Hello (SNI=contil…
  15 0.125860594  34.117.188.166  192.168.1.46    TLSv1.3  1468 Server Hello, Change Cip…
  18 0.128583879  34.117.188.166  192.168.1.46    TLSv1.3   341 Application Data
  21 0.143880233  192.168.1.46    34.117.188.166  QUIC     1401 Initial, DCID=be4fb7d601…
  22 0.172404357  34.117.188.166  192.168.1.46    QUIC     1401 Handshake, DCID=b96ac0, …
  31 0.282469816  192.168.1.46    34.117.188.166  TLSv1.3   585 Client Hello (SNI=spocs.…
  35 0.310603773  34.117.188.166  192.168.1.46    TLSv1.3  1468 Server Hello, Change Cip…
 109 0.903583988  192.168.1.46    34.160.144.191  TLSv1.2   284 Client Hello (SNI=conten…
 111 0.924403289  34.160.144.191  192.168.1.46    TLSv1.2  2868 Server Hello, Certificate
 113 0.924771818  34.160.144.191  192.168.1.46    TLSv1.2   273 Server Key Exchange, Ser…
 115 0.938501694  192.168.1.46    34.160.144.191  TLSv1.2   161 Client Key Exchange, Cha…
 116 0.939103456  192.168.1.46    34.117.188.166  TLSv1.3   132 Change Cipher Spec, Appl…
 119 0.943964861  192.168.1.46    34.117.188.166  TLSv1.3   238 Application Data
 120 0.947870532  192.168.1.46    34.117.188.166  TLSv1.3   249 Application Data
 121 0.957180221  34.160.144.191  192.168.1.46    TLSv1.2   363 New Session Ticket, Chan…
 122 0.957180656  34.160.144.191  192.168.1.46    TLSv1.2   137 Application Data
 123 0.958219546  34.117.188.166  192.168.1.46    TLSv1.3   686 Application Data, Applic…
 125 0.959770385  192.168.1.46    34.117.188.166  TLSv1.3    99 Application Data
```

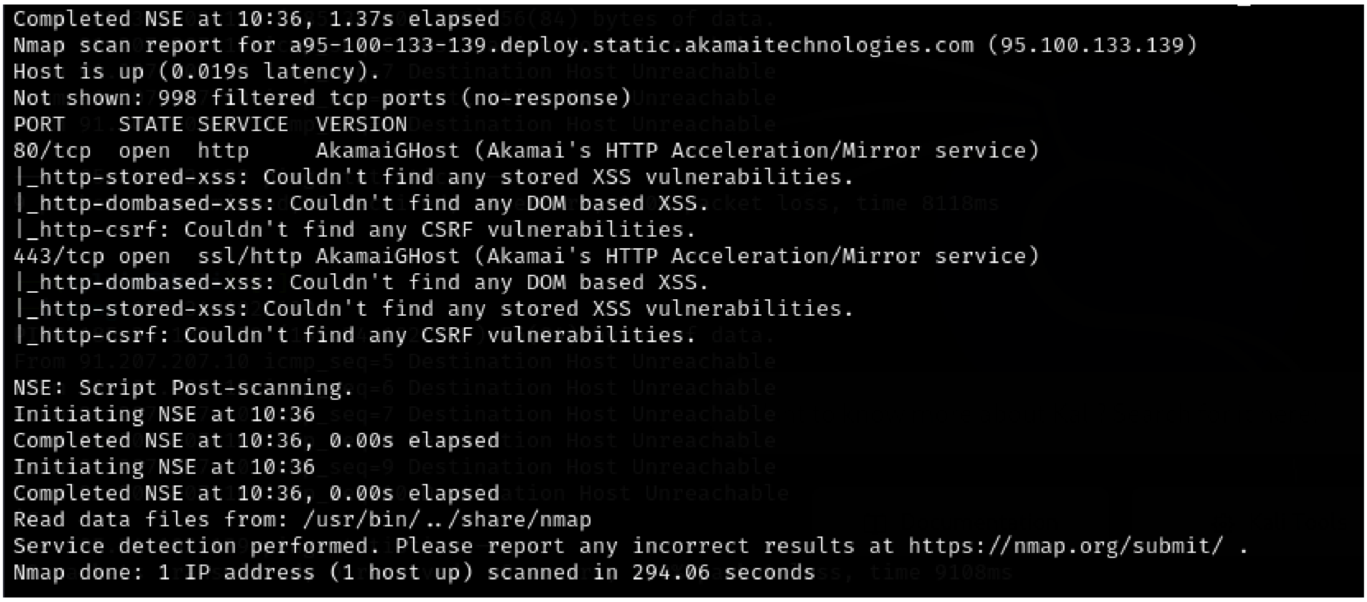
```
  ▾ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Tr
    Total Length: 91
    Identification: 0x697f (27007)
  ▾ 010. .... = Flags: 0x2, Don't fragment
      0... .... = Reserved bit: Not set
      .1.. .... = Don't fragment: Set
      ..0. .... = More fragments: Not set
    ...0 0000 0000 0000 = Fragment Offset: 0
```

```
0000  00 04 00 01 00 06 08 00  27
0010  45 00 00 5b 69 7f 40 00  40
0020  22 95 64 d1 db f4 01 bb  bc
0030  80 18 02 7a 49 8a 00 00  01
0040  4b f1 e8 a5 17 03 03 00  22
0050  6e 69 00 a6 eb 8a 31 6b  fb
0060  e5 42 87 38 4c d5 cd 23  2c
```

Recherche des vunérabilités



```
┌──(sylvie㉿kali)-[~]
└─$ nmap -sV --script vuln -v 95.100.133.139
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-14 10:31 CET
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 10:31
NSE Timing: About 45.45% done; ETC: 10:33 (0:00:40 remaining)
Completed NSE at 10:32, 34.15s elapsed
Initiating NSE at 10:32
Completed NSE at 10:32, 0.00s elapsed
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Initiating Ping Scan at 10:32
Scanning 95.100.133.139 [2 ports]
Completed Ping Scan at 10:32, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 10:32
Completed Parallel DNS resolution of 1 host. at 10:32, 6.50s elapsed
Initiating Connect Scan at 10:32
Scanning a95-100-133-139.deploy.static.akamaitechnologies.com (95.100.133.139) [1000 ports]
Discovered open port 443/tcp on 95.100.133.139
Discovered open port 80/tcp on 95.100.133.139
Completed Connect Scan at 10:32, 5.04s elapsed (1000 total ports)
Initiating Service scan at 10:32
Scanning 2 services on a95-100-133-139.deploy.static.akamaitechnologies.com (95.100.133.139)
Completed Service scan at 10:32, 12.13s elapsed (2 services on 1 host)
NSE: Script scanning 95.100.133.139.
Initiating NSE at 10:32
NSE: [firewall-bypass] lacks privileges.
```



```
Completed NSE at 10:36, 1.37s elapsed
Nmap scan report for a95-100-133-139.deploy.static.akamaitechnologies.com (95.100.133.139)
Host is up (0.019s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE  VERSION
80/tcp  open  http     AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
443/tcp open  ssl/http AkamaiGHost (Akamai's HTTP Acceleration/Mirror service)
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_http-csrf: Couldn't find any CSRF vulnerabilities.

NSE: Script Post-scanning.
Initiating NSE at 10:36
Completed NSE at 10:36, 0.00s elapsed
Initiating NSE at 10:36
Completed NSE at 10:36, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 294.06 seconds
```

```
...........=9.}>N.[>."nG.M.vS.....'.        ..S... ..a..jo....>.5.....l/        ..OX..$._
..".......+./.....,.0.
.        ........./.5.......).'..$env-9206928-wp02-nosecure.hidora.com..........
.......................#.........h2.http/1.1..........".
...........3.k.i... ...T....[^...H.$....!U..d..|...$...A.:xU..../P.....n....! G.....'e}..
....wK64.M...|I.....Z.9..Q"..-q..+........
...........................-........@....r..........................................
...................................................................z...v..&".........
....:..-6. EG..'.Ny=. ..a..jo....>.5.....l/  ..OX..$._.......+.....3.$...
O.....b..YkUTU.;........5..^`............$.....m..Rj7....m...^..}P....2.....M[..........,
....:.<..F.%.o\\..9q..Y/%+.\iE&f..,.s'..Y..j3....jvD.A..A....C....4..r?Z..<.=y.5K.~.U.?..
*..?Ja`..F.....W.2ru...dX....^b.4..
b...mG}*..T/...[L..y.i...@..CwG=....h..]{.*o.341.=..{...."mL..a\.......H.54..Z`...j...%..
.D<{...2C..ZWN.0.s7......[....1.....3..[....,Bx..{..3.M ._h:..k.,.h.....-.@qf6../....kr9O
#w.-.....C..GX.\.:...;A@......(.........*.?A..p.."....x.0.p4L.+q................H]..N.+..
...-..z[[M..xEMF...E..h>.V]|.......H./(].U.....q;yX.........Xb.*.....O..`y.BT....Y.....
...l...=...Q2..;^....44.Q
.......  w....,fy'..`.-..  9.....DHc!.o i@......
..dWC^.
1......^...o.)j.Z..u{.rt.`6k
.@.).d.aw3Y..19P.\e.8).....'....`.L"Fh\X.xXX.E.)..l0.n.....@.p......--.H.}.....*.F@8.O?3.
..q....-..............m.!.!.a..g.........-.k.....t...v*...[.L.9.=...o1"'c.:&:...v...9.e..]
.@.m..}......c ......J.QC....LO.....;..s.`.1v.
<X?.............,@.......rn.....e!../..~6...
.......]....V.E..+....k..Y.%....q..x.Y/5B.......E&...v.._...Y..T.Adj.=A.<......#..r.#[C|.
`.l..Q..FA.d..u.U....kLr..Lf<..a...l.......v.X.',
Ca).......r...
E*.....U.$Yj../z#.......5]0_...z.-.u.~.cpu....J{..c...r..b....V...=z@.._..OXh...7.k.4.L`N
.6.<.{.Cs..o.
..."o.Z.Z.h
...I..qK.......}..3_...(<..y......zE......3C3..a..]D ..A.R~..v^BA........Q.4.$;.2...8.._
..m=..l..n..e/I...z. ....[z......X..._.....m.L...{.A.....
.d...M.....>.H5..R..*..*fT..
```

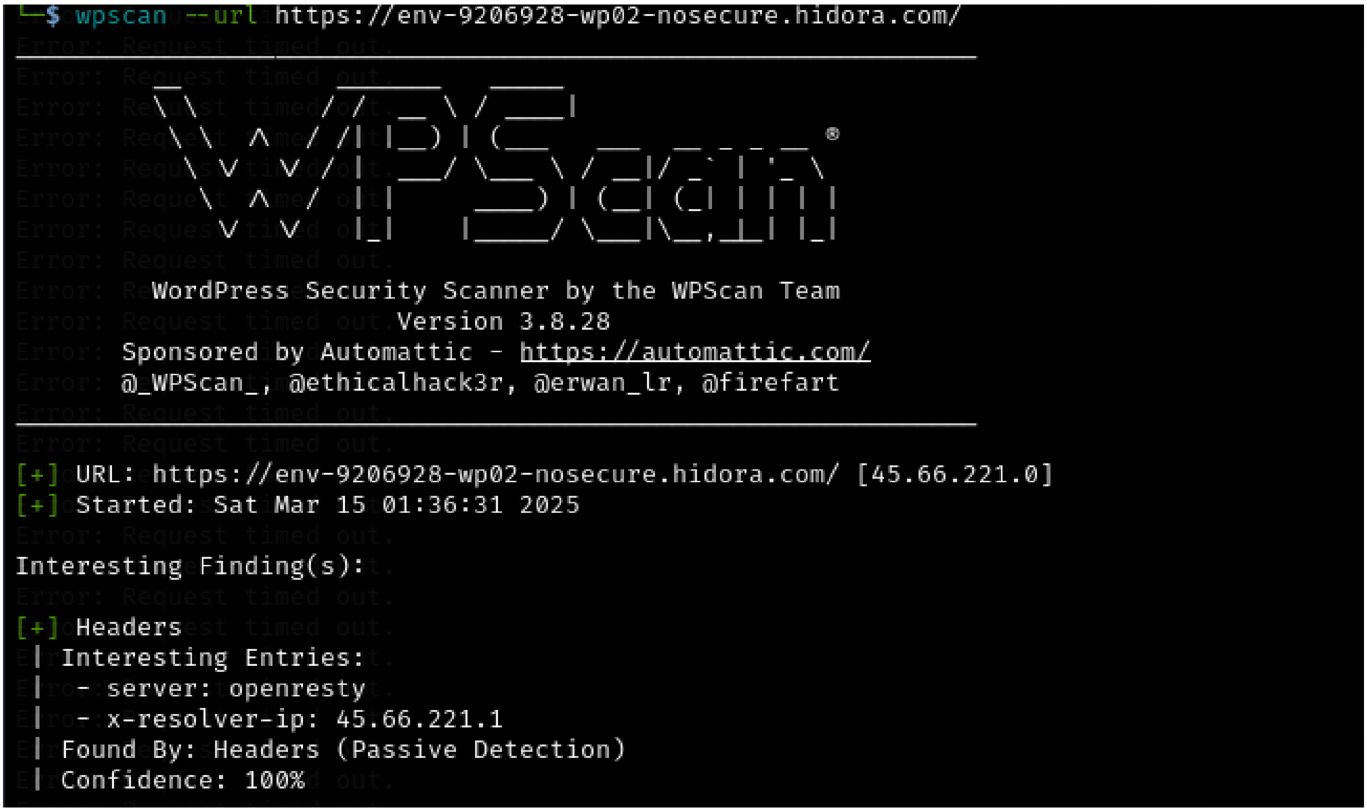
WPScan

- Installer WPScan

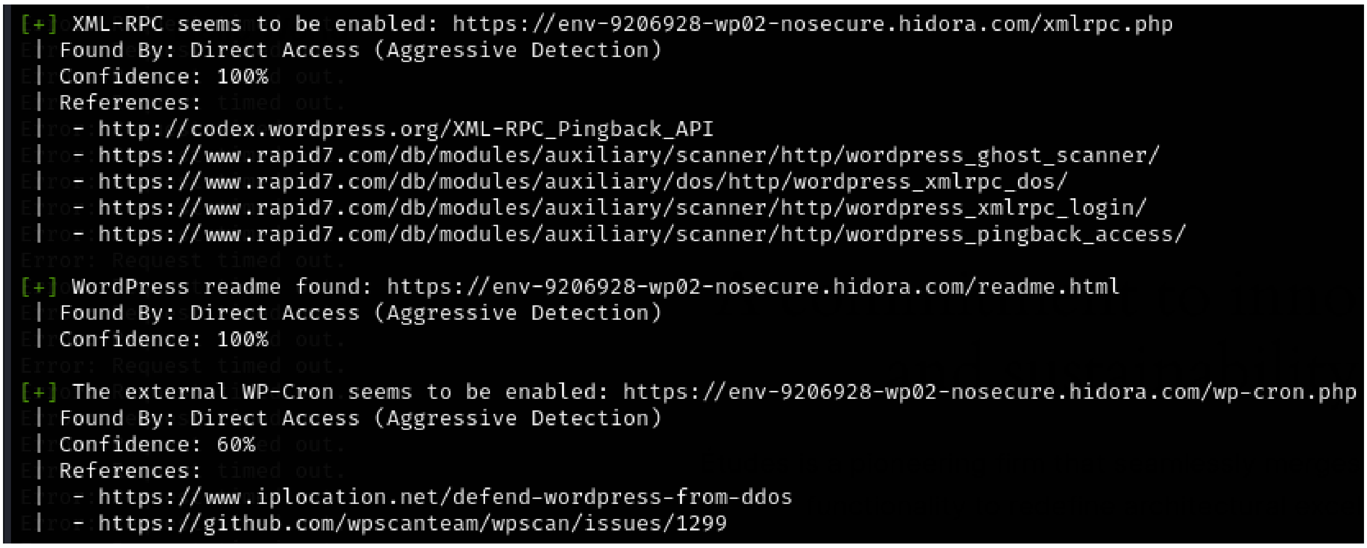
```
sudo apt update
sudo apt install wpscan
```

Lancer un scan basique

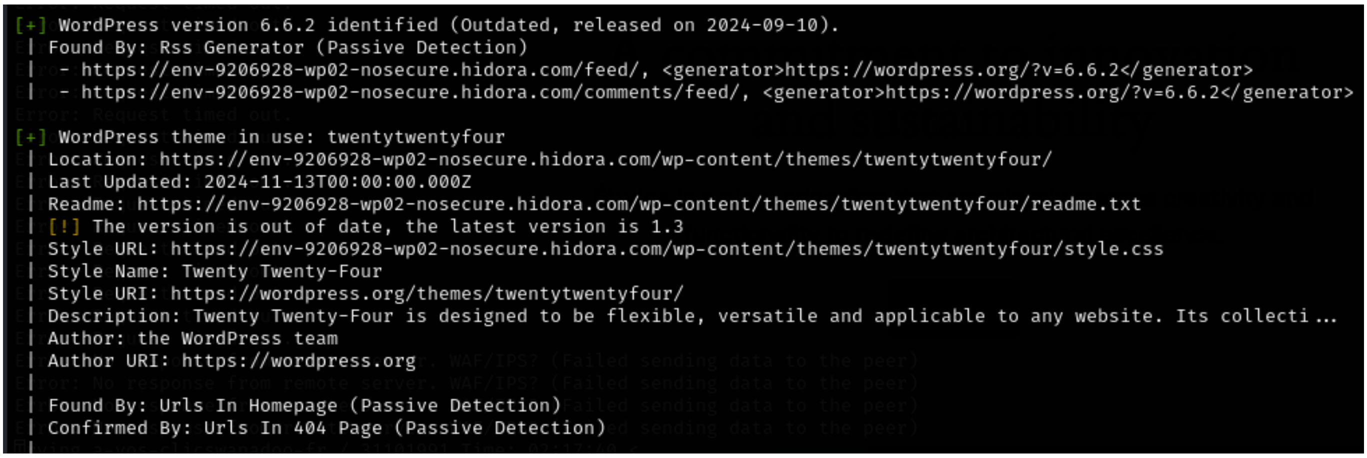
```
wpscan --url https://env-9206928-wp02-nosecure.hidora.com/
```



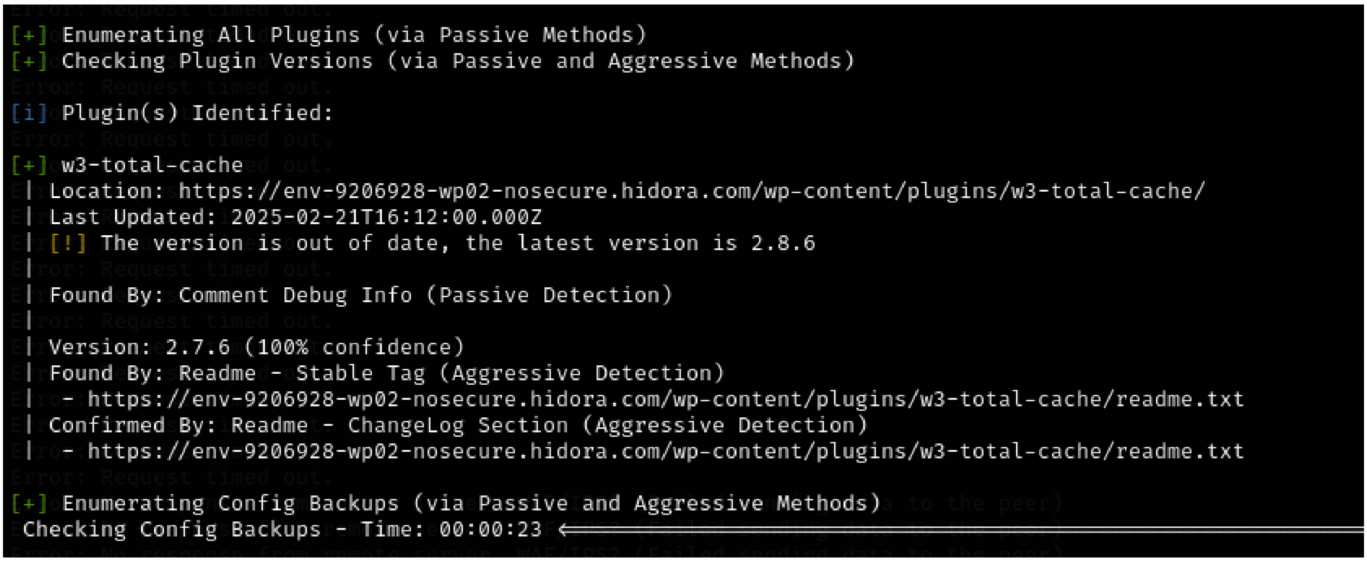
```
└─$ wpscan --url https://env-9206928-wp02-nosecure.hidora.com/
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.28
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: https://env-9206928-wp02-nosecure.hidora.com/ [45.66.221.0]
[+] Started: Sat Mar 15 01:36:31 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - server: openresty
 |  - x-resolver-ip: 45.66.221.1
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```



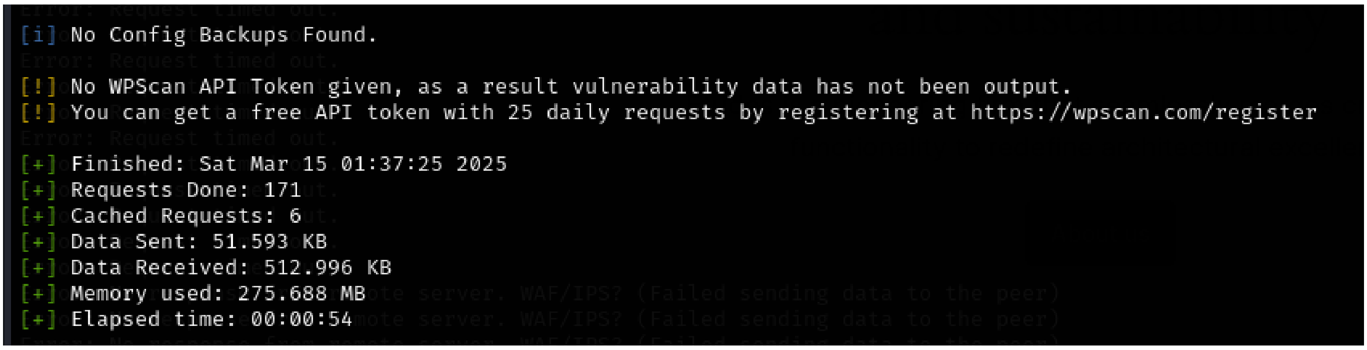
```
[+] XML-RPC seems to be enabled: https://env-9206928-wp02-nosecure.hidora.com/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: https://env-9206928-wp02-nosecure.hidora.com/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: https://env-9206928-wp02-nosecure.hidora.com/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299
```



```
[+] WordPress version 6.6.2 identified (Outdated, released on 2024-09-10).
 | Found By: Rss Generator (Passive Detection)
 |  - https://env-9206928-wp02-nosecure.hidora.com/feed/, <generator>https://wordpress.org/?v=6.6.2</generator>
 |  - https://env-9206928-wp02-nosecure.hidora.com/comments/feed/, <generator>https://wordpress.org/?v=6.6.2</generator>

[+] WordPress theme in use: twentytwentyfour
 | Location: https://env-9206928-wp02-nosecure.hidora.com/wp-content/themes/twentytwentyfour/
 | Last Updated: 2024-11-13T00:00:00.000Z
 | Readme: https://env-9206928-wp02-nosecure.hidora.com/wp-content/themes/twentytwentyfour/readme.txt
 | [!] The version is out of date, the latest version is 1.3
 | Style URL: https://env-9206928-wp02-nosecure.hidora.com/wp-content/themes/twentytwentyfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable to any website. Its collecti...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By: Urls In 404 Page (Passive Detection)
```



```
[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)

[i] Plugin(s) Identified:

[+] w3-total-cache
 | Location: https://env-9206928-wp02-nosecure.hidora.com/wp-content/plugins/w3-total-cache/
 | Last Updated: 2025-02-21T16:12:00.000Z
 | [!] The version is out of date, the latest version is 2.8.6
 |
 | Found By: Comment Debug Info (Passive Detection)
 |
 | Version: 2.7.6 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - https://env-9206928-wp02-nosecure.hidora.com/wp-content/plugins/w3-total-cache/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - https://env-9206928-wp02-nosecure.hidora.com/wp-content/plugins/w3-total-cache/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:23 <==========================================
```



```
[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Sat Mar 15 01:37:25 2025
[+] Requests Done: 171
[+] Cached Requests: 6
[+] Data Sent: 51.593 KB
[+] Data Received: 512.996 KB
[+] Memory used: 275.688 MB
[+] Elapsed time: 00:00:54
```

Points forts:

- Analyse détaillée du site:

WPScan a été utilisé pour effectuer une analyse approfondie du site WordPress, ce qui permet de détecter rapidement les points de sécurité importants.

- Identification des points de vulnérabilité:

L'analyse a permis d'identifier plusieurs aspects critiques, tels que XML-RPC activé, un fichier readme accessible, et le WP-Cron externe activé, qui peuvent représenter des risques de sécurité si non configurés correctement.

Évaluation des versions:

La version de WordPress ainsi que des plugins et thèmes obsolètes ont été identifiés.

Points faibles:

- XML-RPC activé:

L'activation de XML-RPC sur le site représente un risque, car cette fonctionnalité permet des interactions à distance et peut être utilisée dans des attaques par force brute et pingbacks.

- Fichier Readme accessible:

Le fichier readme.html expose la version de WordPress utilisée, ce qui donne des informations précieuses aux attaquants pour exploiter d'éventuelles vulnérabilités connues dans cette version.

- WP-Cron externe activé:

Le WP-Cron externe activé est un point d'attaque potentiel. Mal configuré, il peut être utilisé dans des attaques DDoS en envoyant un grand nombre de requêtes de manière répétée.

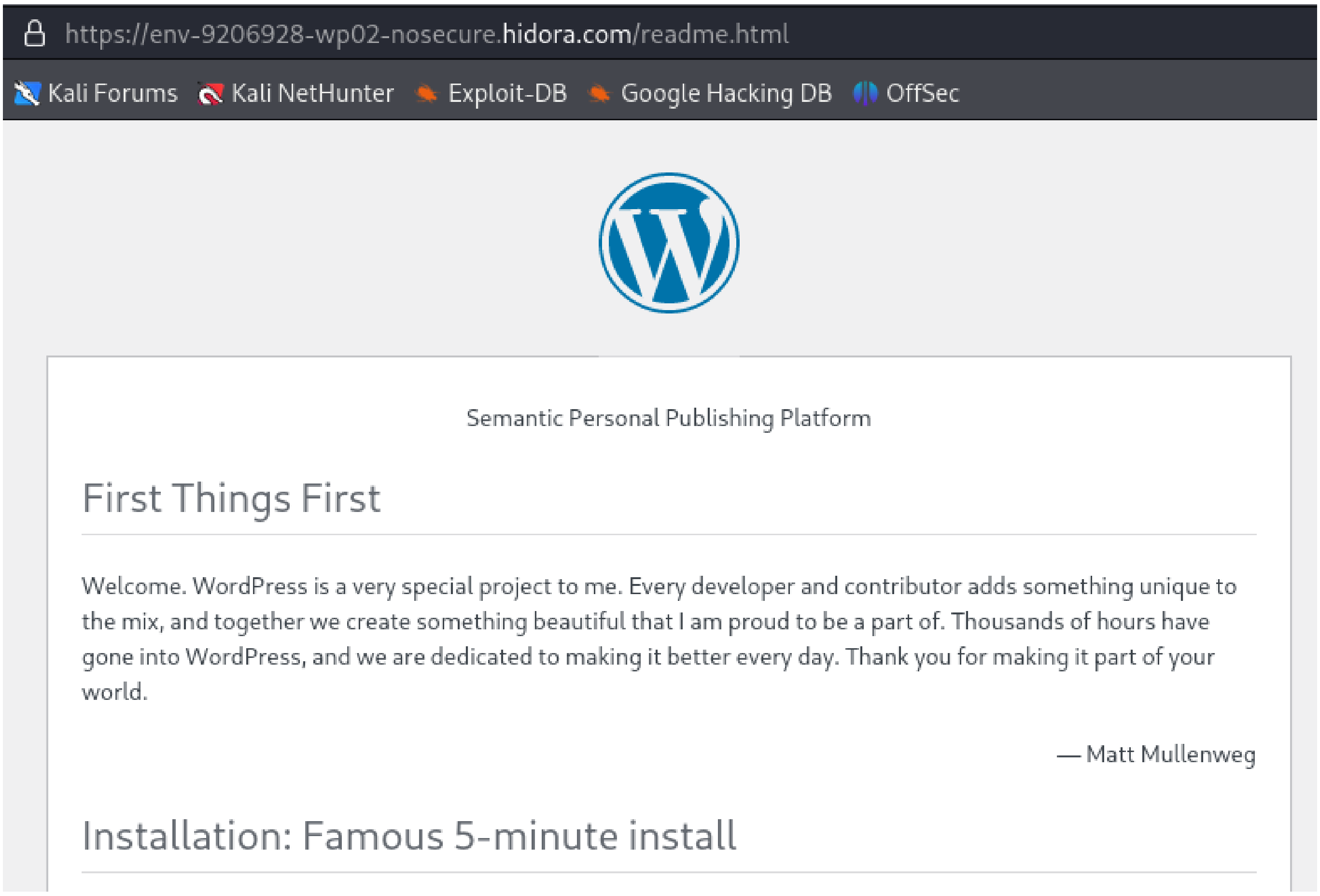
- Version obsolète de WordPress et de plugins:

L'utilisation d'une version obsolète de WordPress (6.6.2) ainsi que des plugins et thèmes non mis à jour (comme w3-total-cache et Twenty Twenty-Four) laisse le site vulnérable aux failles de sécurité non corrigées dans les versions récentes.

- Absence de sauvegardes de configuration:

L'absence de sauvegardes de configuration, bien que cela puisse être un avantage en matière de sécurité, complique la récupération du site en cas de problème.

Fichier readme trouvé : accessible via https://env-9206928-wp02-nosecure.hidora.com/readme.html



Semantic Personal Publishing Platform

First Things First

Welcome. WordPress is a very special project to me. Every developer and contributor adds something unique to the mix, and together we create something beautiful that I am proud to be a part of. Thousands of hours have gone into WordPress, and we are dedicated to making it better every day. Thank you for making it part of your world.

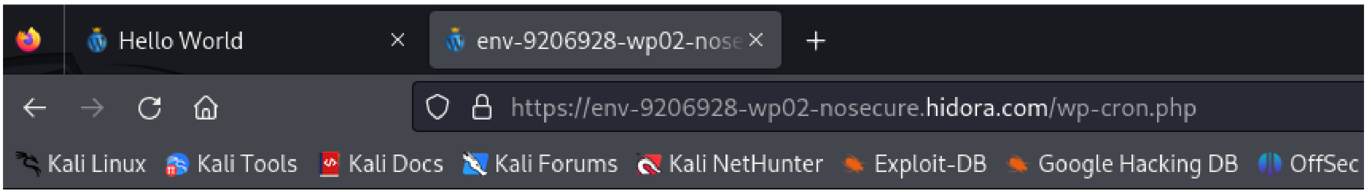
— Matt Mullenweg

Installation: Famous 5-minute install

- Risques: Exposer ce fichier peut fournir des informations sensibles à un attaquant, telles que la version exacte de WordPress en cours d'exécution, ce qui peut faciliter l'exploitation d'anciennes vulnérabilités connues.
- Recommandation: Il est préférable de désactiver l'accès à ce fichier ou de le supprimer pour éviter de fournir des informations utiles aux attaquants.

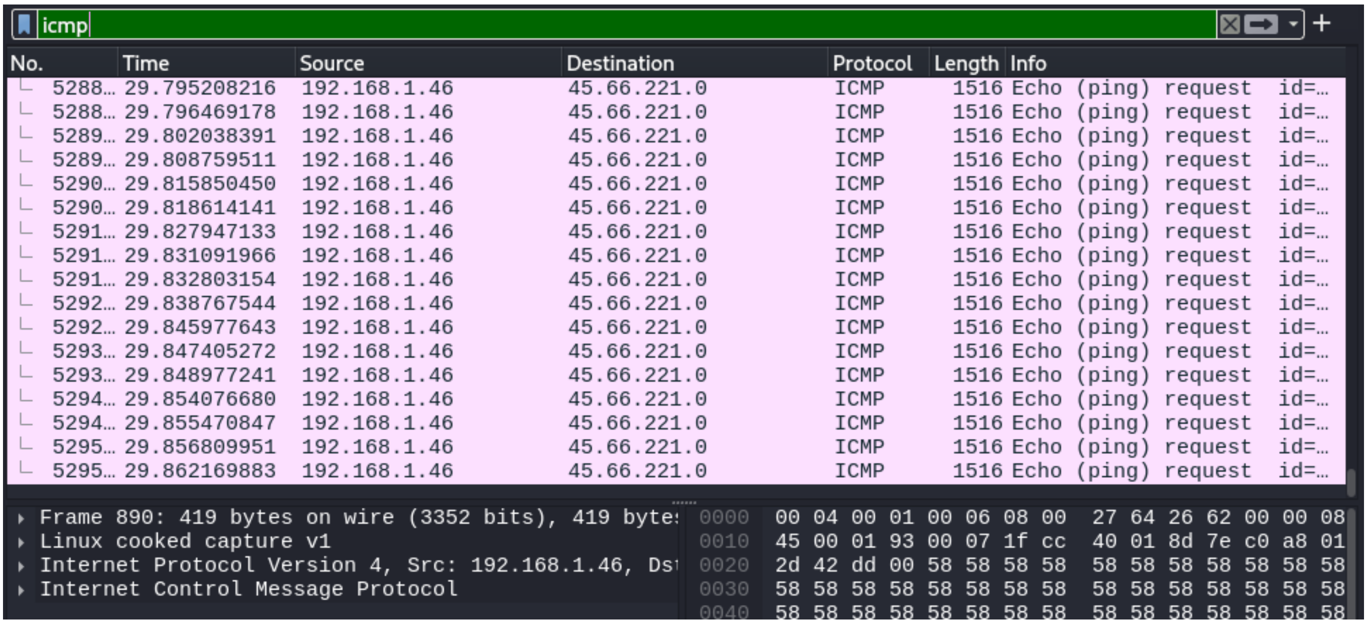
wp-cron activé

URL accessible : https://env-9206928-wp02-nosecure.hidora.com/wp-cron.php



Déni de service

```
hping3 -d 65495 --icmp --flood 45.66.221.0
```



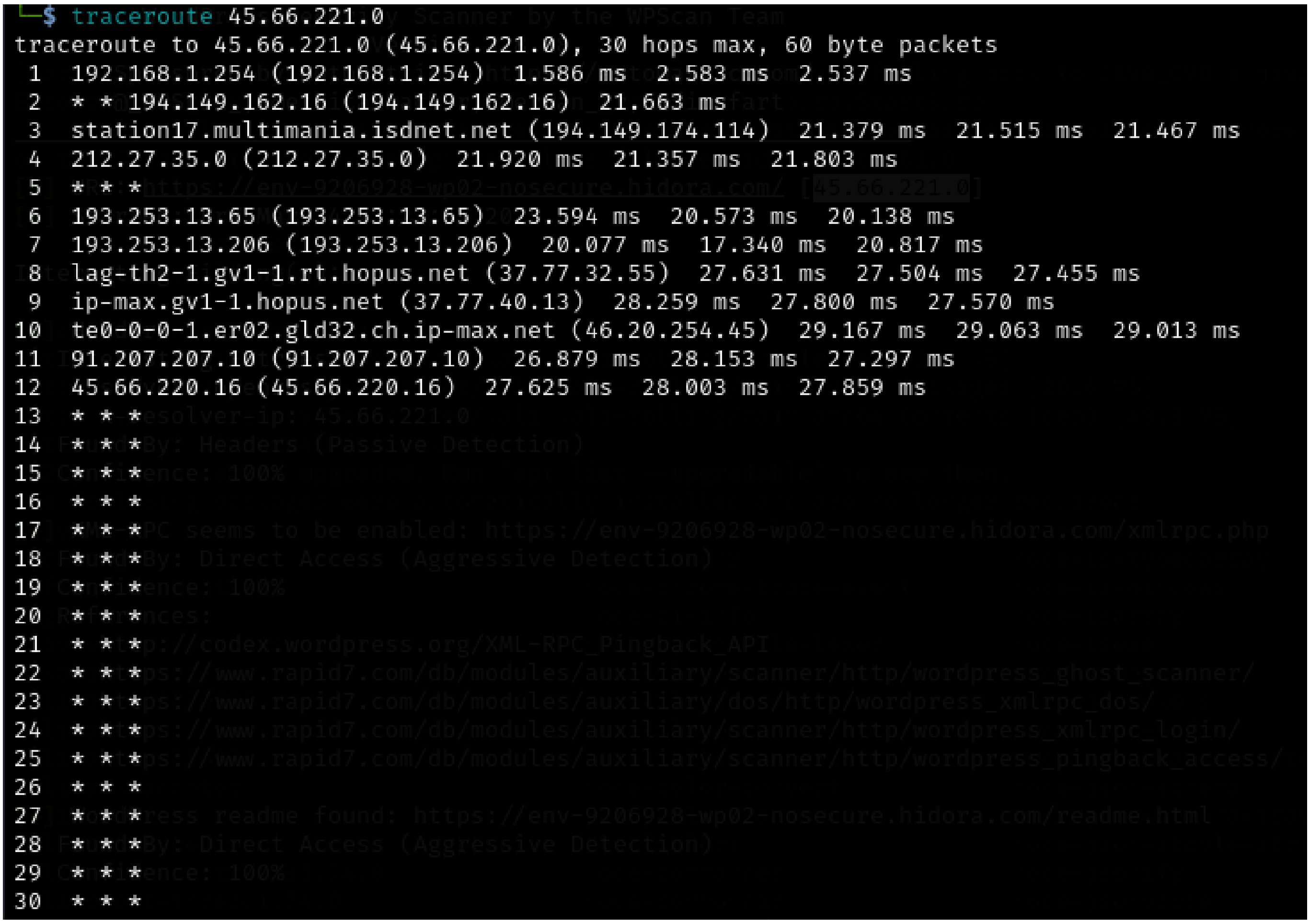
```
icmp
No.      Time          Source          Destination     Protocol  Length Info
5288…  29.795208216  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5288…  29.796469178  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5289…  29.802038391  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5289…  29.808759511  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5290…  29.815850450  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5290…  29.818614141  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5291…  29.827947133  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5291…  29.831091966  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5291…  29.832803154  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5292…  29.838767544  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5292…  29.845977643  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5293…  29.847405272  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5293…  29.848977241  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5294…  29.854076680  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5294…  29.855470847  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5295…  29.856809951  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…
5295…  29.862169883  192.168.1.46   45.66.221.0     ICMP      1516 Echo (ping) request  id=…

› Frame 890: 419 bytes on wire (3352 bits), 419 byte   0000  00 04 00 01 00 06 08 00  27 64 26 62 00 00 08
› Linux cooked capture v1                              0010  45 00 01 93 00 07 1f cc  40 01 8d 7e c0 a8 01
› Internet Protocol Version 4, Src: 192.168.1.46, Ds   0020  2d 42 dd 00 58 58 58 58  58 58 58 58 58 58 58
› Internet Control Message Protocol                    0030  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58
                                                       0040  58 58 58 58 58 58 58 58  58 58 58 58 58 58 58
```

Test d'attaque DDoS :

Le test de déni de service par flood ICMP permet de simuler l'impact d'une attaque DoS sur le serveur cible et de tester la capacité de défense contre ce type de menace.

Tracer le chemin emprunté par les paquets de données

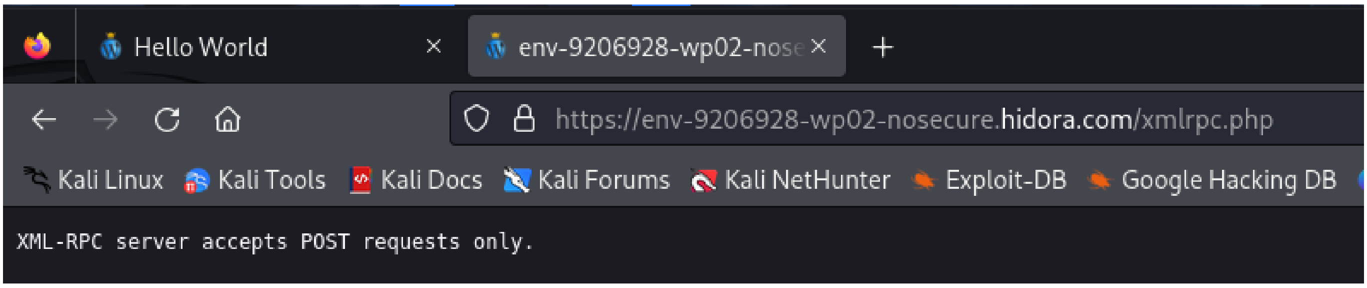
```
traceroute 45.66.221.0
```



```
└─$ traceroute 45.66.221.0
traceroute to 45.66.221.0 (45.66.221.0), 30 hops max, 60 byte packets
 1  192.168.1.254 (192.168.1.254)  1.586 ms  2.583 ms  2.537 ms
 2  * * 194.149.162.16 (194.149.162.16)  21.663 ms
 3  station17.multimania.isdnet.net (194.149.174.114)  21.379 ms  21.515 ms  21.467 ms
 4  212.27.35.0 (212.27.35.0)  21.920 ms  21.357 ms  21.803 ms
 5  * * *
 6  193.253.13.65 (193.253.13.65)  23.594 ms  20.573 ms  20.138 ms
 7  193.253.13.206 (193.253.13.206)  20.077 ms  17.340 ms  20.817 ms
 8  lag-th2-1.gv1-1.rt.hopus.net (37.77.32.55)  27.631 ms  27.504 ms  27.455 ms
 9  ip-max.gv1-1.hopus.net (37.77.40.13)  28.259 ms  27.800 ms  27.570 ms
10  te0-0-0-1.er02.gld32.ch.ip-max.net (46.20.254.45)  29.167 ms  29.063 ms  29.013 ms
11  91.207.207.10 (91.207.207.10)  26.879 ms  28.153 ms  27.297 ms
12  45.66.220.16 (45.66.220.16)  27.625 ms  28.003 ms  27.859 ms
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

XML-RPC activé

URL accessible : https://env-9206928-wp02-nosecure.hidora.com/xmlrpc.php



```
XML-RPC server accepts POST requests only.
```

XML-RPC activé

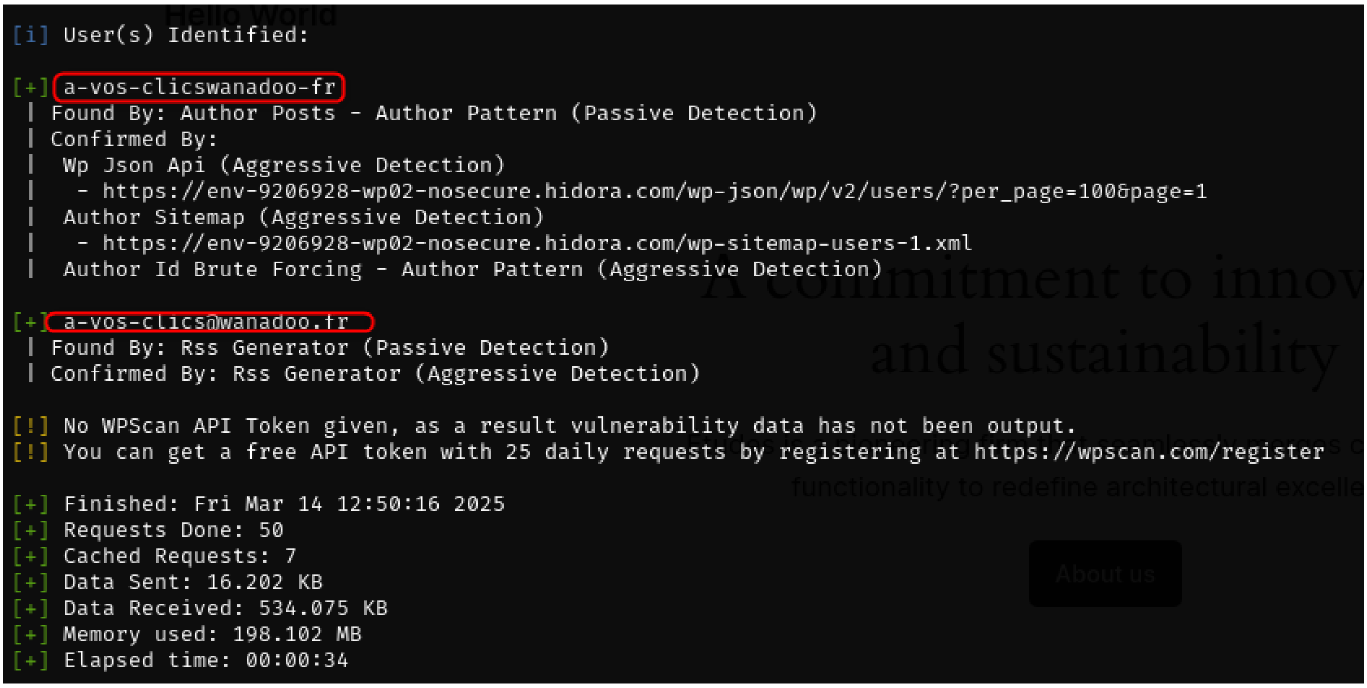
Risques : XML-RPC peut être vulnérable à des attaques par déni de service distribué (DDoS) ou à des attaques par force brute sur les comptes d'administrateurs, en raison de la possibilité de soumettre plusieurs demandes en parallèle.

Recommandation: Si XML-RPC n'est pas nécessaire pour ton site, il est conseillé de le désactiver pour éviter ces risques.

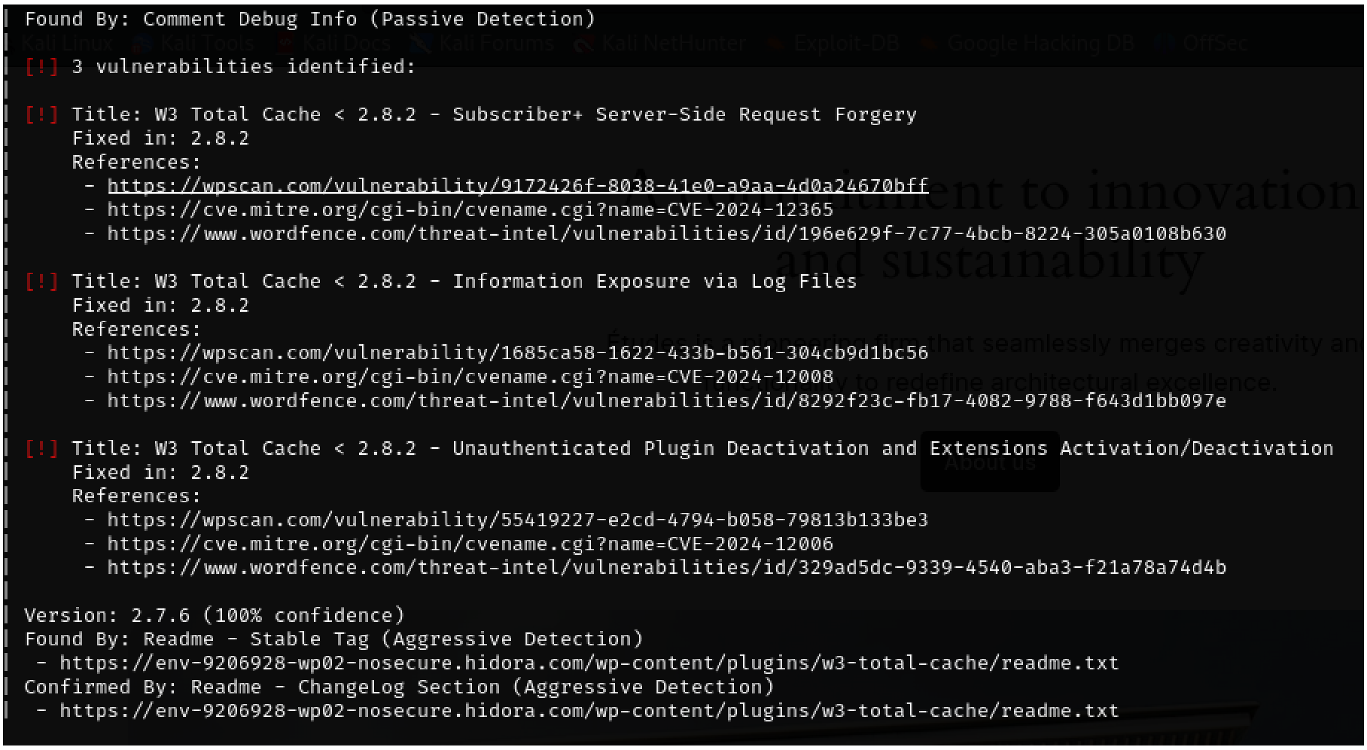
```
wpscan --url https://env-9206928-wp02-nosecure.hidora.com/ -e vp --plugins-detection mixed --api-token VOTRE_API_TOKEN
```

Enumérer les utilisateurs du site web

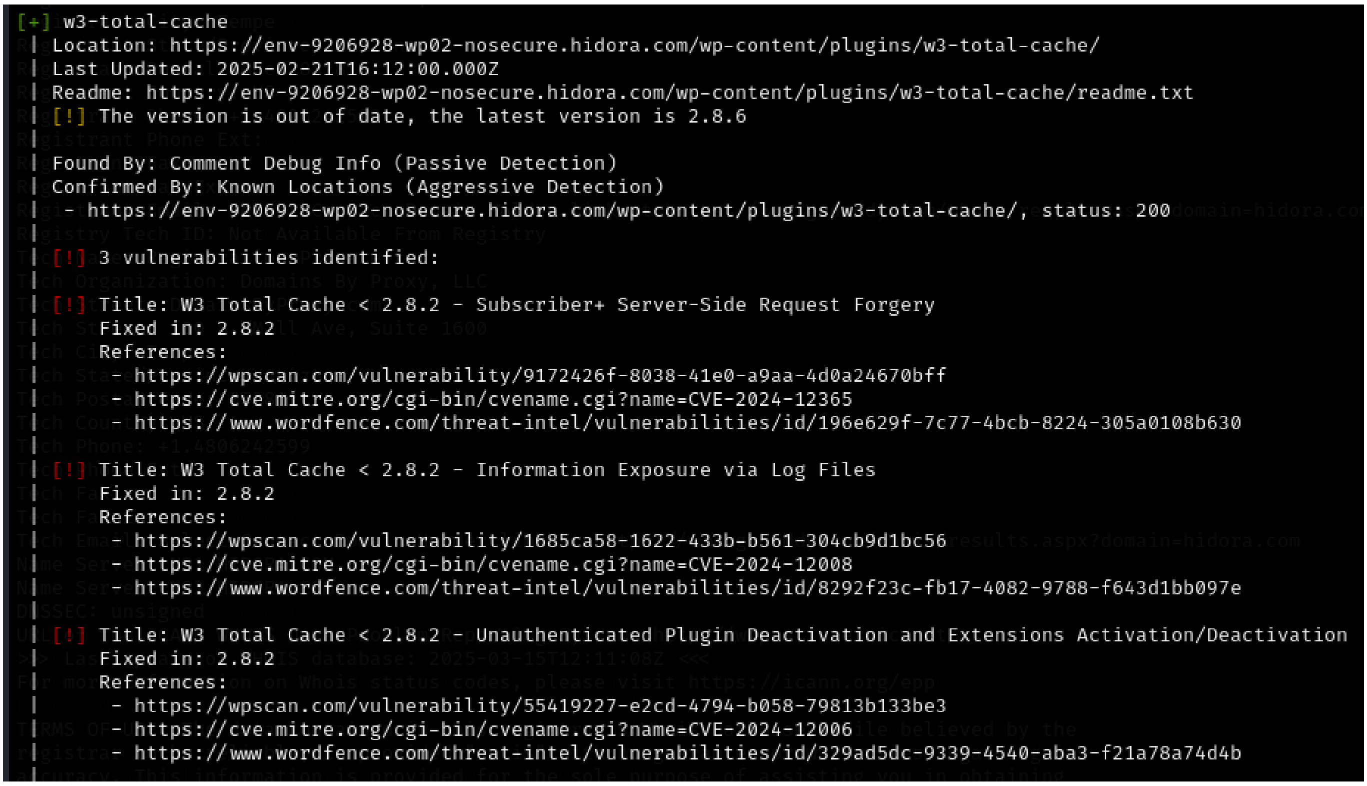
```
wpscan --url https://env-9206928-wp02-nosecure.hidora.com/ --enumerate u
```



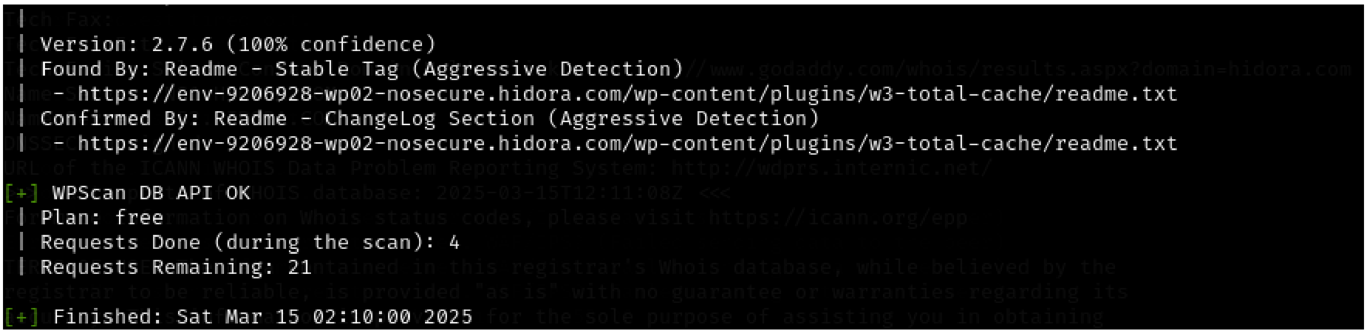
```
[i] User(s) Identified:

[+] a-vos-clicswanadoo-fr
 | Found By: Author Posts - Author Pattern (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - https://env-9206928-wp02-nosecure.hidora.com/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Sitemap (Aggressive Detection)
 |   - https://env-9206928-wp02-nosecure.hidora.com/wp-sitemap-users-1.xml
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] a-vos-clics@wanadoo.fr
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By: Rss Generator (Aggressive Detection)

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Fri Mar 14 12:50:16 2025
[+] Requests Done: 50
[+] Cached Requests: 7
[+] Data Sent: 16.202 KB
[+] Data Received: 534.075 KB
[+] Memory used: 198.102 MB
[+] Elapsed time: 00:00:34
```



```
| Found By: Comment Debug Info (Passive Detection)
|
| [!] 3 vulnerabilities identified:
|
| [!] Title: W3 Total Cache < 2.8.2 - Subscriber+ Server-Side Request Forgery
|     Fixed in: 2.8.2
|     References:
|      - https://wpscan.com/vulnerability/9172426f-8038-41e0-a9aa-4d0a24670bff
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-12365
|      - https://www.wordfence.com/threat-intel/vulnerabilities/id/196e629f-7c77-4bcb-8224-305a0108b630
|
| [!] Title: W3 Total Cache < 2.8.2 - Information Exposure via Log Files
|     Fixed in: 2.8.2
|     References:
|      - https://wpscan.com/vulnerability/1685ca58-1622-433b-b561-304cb9d1bc56
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-12008
|      - https://www.wordfence.com/threat-intel/vulnerabilities/id/8292f23c-fb17-4082-9788-f643d1bb097e
|
| [!] Title: W3 Total Cache < 2.8.2 - Unauthenticated Plugin Deactivation and Extensions Activation/Deactivation
|     Fixed in: 2.8.2
|     References:
|      - https://wpscan.com/vulnerability/55419227-e2cd-4794-b058-79813b133be3
|      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-12006
|      - https://www.wordfence.com/threat-intel/vulnerabilities/id/329ad5dc-9339-4540-aba3-f21a78a74d4b
|
| Version: 2.7.6 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
|  - https://env-9206928-wp02-nosecure.hidora.com/wp-content/plugins/w3-total-cache/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
|  - https://env-9206928-wp02-nosecure.hidora.com/wp-content/plugins/w3-total-cache/readme.txt
```



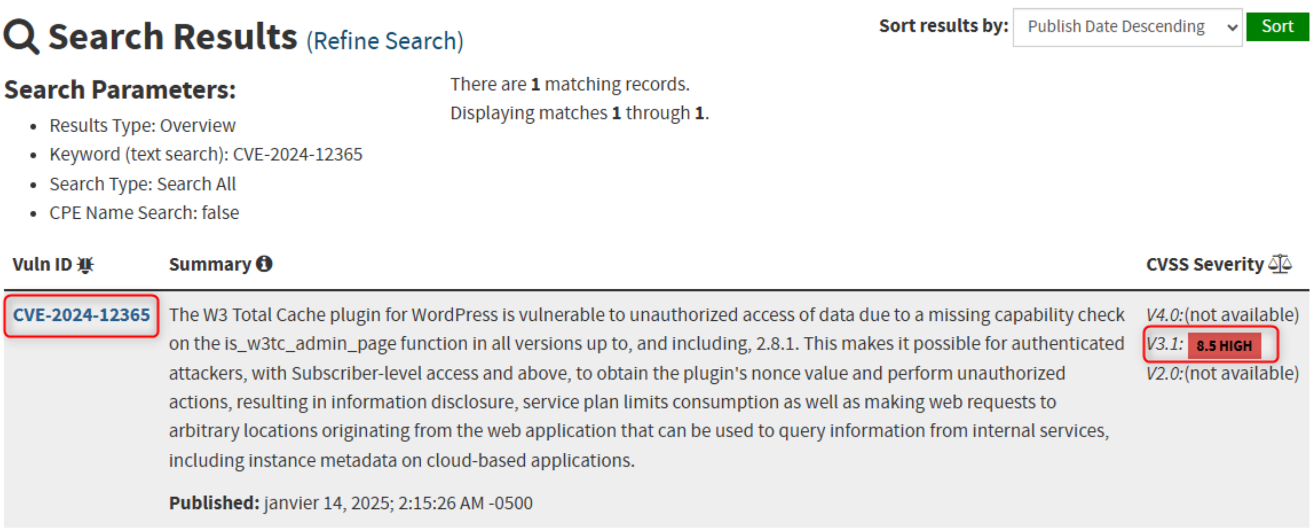
```
[+] w3-total-cache
 | Location: https://env-9206928-wp02-nosecure.hidora.com/wp-content/plugins/w3-total-cache/
 | Last Updated: 2025-02-21T16:12:00.000Z
 | Readme: https://env-9206928-wp02-nosecure.hidora.com/wp-content/plugins/w3-total-cache/readme.txt
 | [!] The version is out of date, the latest version is 2.8.6
 |
 | Found By: Comment Debug Info (Passive Detection)
 | Confirmed By: Known Locations (Aggressive Detection)
 |  - https://env-9206928-wp02-nosecure.hidora.com/wp-content/plugins/w3-total-cache/, status: 200
 |
 | [!] 3 vulnerabilities identified:
 |
 | [!] Title: W3 Total Cache < 2.8.2 - Subscriber+ Server-Side Request Forgery
 |     Fixed in: 2.8.2
 |     References:
 |      - https://wpscan.com/vulnerability/9172426f-8038-41e0-a9aa-4d0a24670bff
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-12365
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/196e629f-7c77-4bcb-8224-305a0108b630
 |
 | [!] Title: W3 Total Cache < 2.8.2 - Information Exposure via Log Files
 |     Fixed in: 2.8.2
 |     References:
 |      - https://wpscan.com/vulnerability/1685ca58-1622-433b-b561-304cb9d1bc56
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-12008
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/8292f23c-fb17-4082-9788-f643d1bb097e
 |
 | [!] Title: W3 Total Cache < 2.8.2 - Unauthenticated Plugin Deactivation and Extensions Activation/Deactivation
 |     Fixed in: 2.8.2
 |     References:
 |      - https://wpscan.com/vulnerability/55419227-e2cd-4794-b058-79813b133be3
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-12006
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/329ad5dc-9339-4540-aba3-f21a78a74d4b
```



```
 |
 | Version: 2.7.6 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - https://env-9206928-wp02-nosecure.hidora.com/wp-content/plugins/w3-total-cache/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - https://env-9206928-wp02-nosecure.hidora.com/wp-content/plugins/w3-total-cache/readme.txt

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 4
 | Requests Remaining: 21

[+] Finished: Sat Mar 15 02:10:00 2025
```

- Vulnérabilités détectées (plugin w3-total-cache):

- CVE-2024-12365: SSRF (Server-Side Request Forgery) dans les versions inférieures à 2.8.2.
- CVE-2024-12008: Exposition d'informations via des fichiers journaux dans les versions inférieures à 2.8.2.
- CVE-2024-12006: Désactivation non authentifiée du plugin et activation/désactivation des extensions dans les versions inférieures à 2.8.2.
- Fonctionnalités spécifiques:
- XML-RPC activé: accessible via https://env-9206928-wp02-nosecure.hidora.com/xmlrpc.php. XML-RPC est souvent utilisé pour des attaques comme les attaques par déni de service (DoS).
- wp-cron activé: accessible via https://env-9206928-wp02-nosecure.hidora.com/wp-cron.php. Cette fonctionnalité peut être vulnérable à des attaques DDoS si elle est mal configurée. Fichier readme trouvé : accessible via https://env-9206928-wp02-nosecure.hidora.com/readme.html.
- CVE associé aux vulnérabilités:



Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

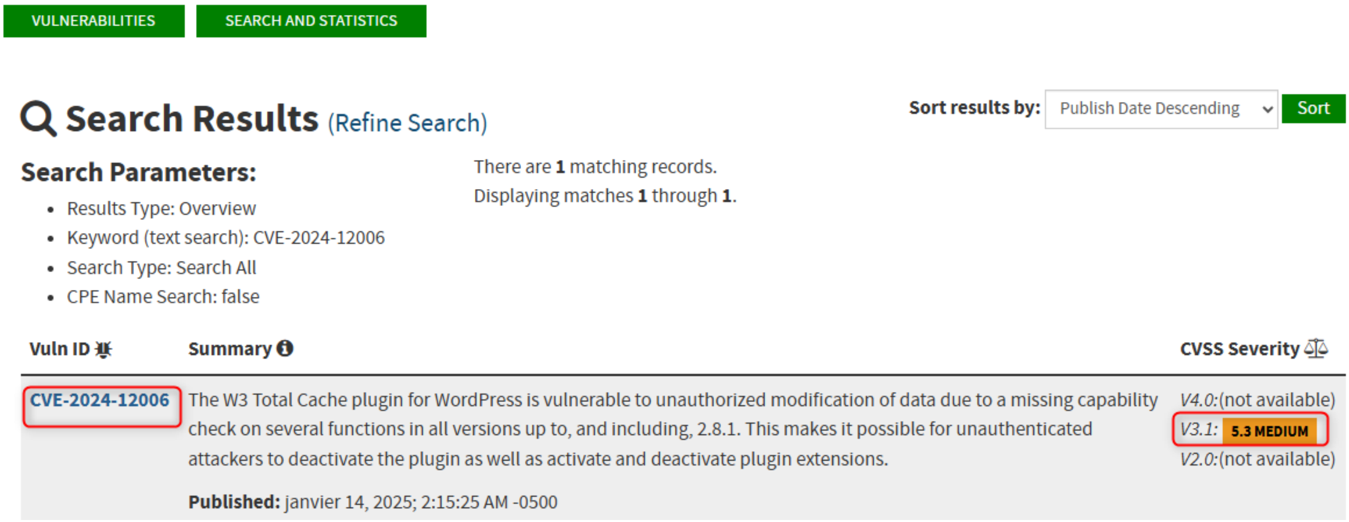
- Results Type: Overview
- Keyword (text search): CVE-2024-12365
- Search Type: Search All
- CPE Name Search: false

There are **1** matching records.
Displaying matches **1** through **1**.

Vuln ID	Summary	CVSS Severity
CVE-2024-12365	The W3 Total Cache plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the is_w3tc_admin_page function in all versions up to, and including, 2.8.1. This makes it possible for authenticated attackers, with Subscriber-level access and above, to obtain the plugin's nonce value and perform unauthorized actions, resulting in information disclosure, service plan limits consumption as well as making web requests to arbitrary locations originating from the web application that can be used to query information from internal services, including instance metadata on cloud-based applications. **Published:** janvier 14, 2025; 2:15:26 AM -0500	*V4.0:*(not available) *V3.1:* 8.5 HIGH *V2.0:*(not available)

1. Tester la vulnérabilité CVE-2024-12365 : SSRF (Server-Side Request Forgery)

- Détails de la vulnérabilité : CVE-2024-12365 permet à un attaquant de déclencher des requêtes HTTP malveillantes vers des services internes ou externes via une attaque de type SSRF, exploitant des failles dans la gestion des requêtes par le plugin.



Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

- Results Type: Overview
- Keyword (text search): CVE-2024-12006
- Search Type: Search All
- CPE Name Search: false

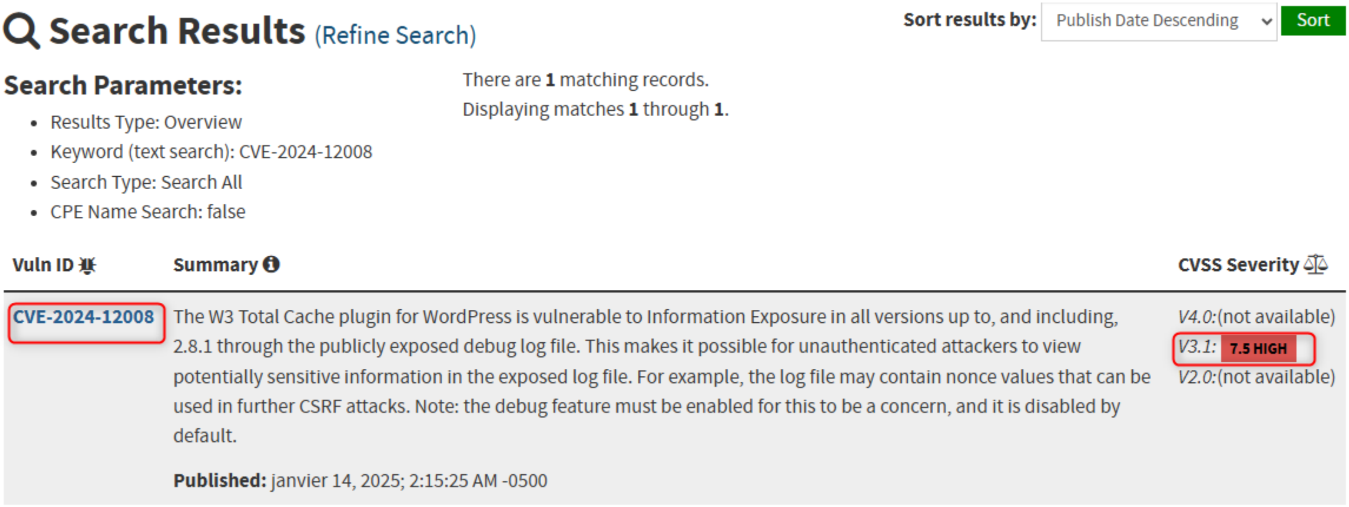
There are **1** matching records.
Displaying matches **1** through **1**.

Vuln ID	Summary	CVSS Severity
CVE-2024-12006	The W3 Total Cache plugin for WordPress is vulnerable to unauthorized modification of data due to a missing capability check on several functions in all versions up to, and including, 2.8.1. This makes it possible for unauthenticated attackers to deactivate the plugin as well as activate and deactivate plugin extensions. **Published:** janvier 14, 2025; 2:15:25 AM -0500	*V4.0:*(not available) *V3.1:* 5.3 MEDIUM *V2.0:*(not available)

2. Tester la vulnérabilité CVE-2024-12008 : Exposition d’informations via les fichiers de log

Détails de la vulnérabilité:

CVE-2024-12008 expose potentiellement des informations sensibles à travers les fichiers de logs. Cela peut inclure des données privées, des informations sur la configuration du serveur, des erreurs ou des détails sur les utilisateurs ou les requêtes.



Search Results (Refine Search)

Sort results by: Publish Date Descending Sort

Search Parameters:

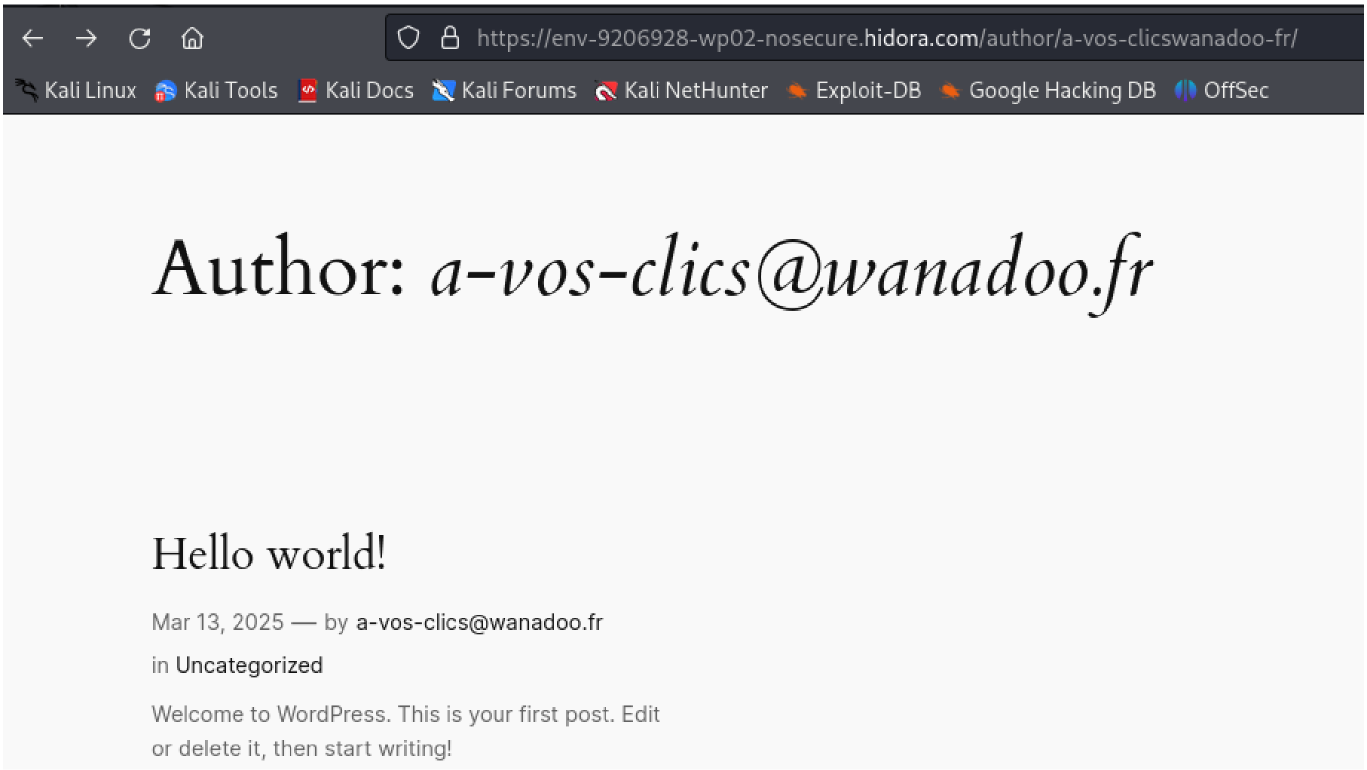
- Results Type: Overview
- Keyword (text search): CVE-2024-12008
- Search Type: Search All
- CPE Name Search: false

There are **1** matching records.
Displaying matches **1** through **1**.

Vuln ID	Summary	CVSS Severity
CVE-2024-12008	The W3 Total Cache plugin for WordPress is vulnerable to Information Exposure in all versions up to, and including, 2.8.1 through the publicly exposed debug log file. This makes it possible for unauthenticated attackers to view potentially sensitive information in the exposed log file. For example, the log file may contain nonce values that can be used in further CSRF attacks. Note: the debug feature must be enabled for this to be a concern, and it is disabled by default. **Published:** janvier 14, 2025; 2:15:25 AM -0500	*V4.0:*(not available) *V3.1:* 7.5 HIGH *V2.0:*(not available)

3. Tester la vulnérabilité CVE-2024-12006 : Désactivation non authentifiée du plugin et activation/désactivation des extensions

Détails de la vulnérabilité: CVE-2024-12006 permet à un attaquant de désactiver le plugin W3 Total Cache ou d'activer/désactiver des extensions sans authentification adéquate.



https://env-9206928-wp02-nosecure.hidora.com/author/a-vos-clicswanadoo-fr/

Author: *a-vos-clics@wanadoo.fr*

Hello world!

Mar 13, 2025 — by a-vos-clics@wanadoo.fr

in Uncategorized

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!