

Forum:[Hack Forums](#)

Thread: [\[Spoofing Values\] Friends don't let friends use SQLMap](#)

SIM-1073426 - December 23, 2015, 11:53 am

I'm pretty sure everyone here knows what the SQL Injection tool SQLMap is. The requests being sent from the program are enormous and the program is very easy to fool.

I'm gonna show you how I managed to spoof DB values on SQLMap by making it think the injection is actually error-based when it's not. The script I made for this is 30 lines of PHP code.

Let's see how the session looks like when trying to inject my site:

Spoiler [\(Click to View\)](#)

But how does it work?

Well the first request I'm gonna get from the injector (after some gay heuristic tests) are

Quote:1) AND (SELECT 9374 FROM(SELECT COUNT(*),CONCAT(0x7176766271,(SELECT (CASE WHEN (4708=4708) THEN 1 ELSE 0 END)),0x71706b7171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND (9697=9697

This is just gonna display 2 random codes in Hex

It looks like this in MySQL terminal:

```
mysql> SELECT 4237 FROM(SELECT COUNT(*),CONCAT(0x7176766271,(SELECT (ELT(4237=4237,1))),0x71706b7171,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a;
```

ERROR 1062 (23000): Duplicate entry 'qvwbq1qpkqq1' for key 'group_key'

The second request looks like this:

Quote:1) AND (SELECT 9242 FROM(SELECT COUNT(*),CONCAT(0x7171627171,(SELECT (CASE WHEN (5136=5136) THEN 1 ELSE 0 END)),0x716b6a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND (6799=6799
and it tries to output the same as above but in a different way.

The third is

Quote:1) AND (SELECT 2712 FROM(SELECT COUNT(*),CONCAT(0x7171627171,(SELECT IFNULL(CAST(COUNT(schema_name) AS CHAR),0x20) FROM INFORMATION_SCHEMA.SCHEMATA),0x716b6a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND (8093=8093

and it displays how many databases there is.

Then the forth it starts grabbing databases one by one with

Quote:1) AND (SELECT 3573 FROM(SELECT COUNT(*),CONCAT(0x7171627171,(SELECT MID((IFNULL(CAST(schema_name AS CHAR),0x20)),1,50) FROM INFORMATION_SCHEMA.SCHEMATA LIMIT 0,1),0x716b6a7671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a) AND (1675=1675

Simple enough.

All the requests being sent here are these: <http://pastebin.com/raw/4ed5qU6v>

So Spoofing this is incredibly simple. All we need to do is getting both of the hex values then display our spoofed value between them (un-hexed) then we put it in:

Duplicate entry 'HERE' for key 'group_key'

And SQLMap now thinks it's vulnerable.

You can easily write on this and make a honeypot to see what people are targeting in your site or you can simply display such big of a value that the program just can't operate and goes on a never-ending loop. Lol

Here's the code:

PHP Code

```
<?php
```

```
$number_of_dbs = "1";
```

```
$db_msg = "stop_using_sqlmap_on_my_site";
```

```
# Getting the first Hex value
```

```
preg_match('/\CONCAT\((.*?),/', urldecode($_GET["id"]), $matches);
```

```
if(!empty($matches[1]))
```

```
{
```

```
    $first_hex = str_replace("0x", "", trim($matches[1]));
```

```
    $string = hex2bin($first_hex) . "1";
```

```
# Getting the second Hex value
```

```
preg_match('/,0x(.*?),FLOOR/', urldecode($_GET["id"]), $sec_matches);
```

```
if(!empty($matches[1])) $string .= hex2bin(trim($sec_matches[1])) . "1";
```

```
# Get the DB count
```

```
if(strpos(urldecode($_GET["id"]), 'COUNT(schema_name)')!==false) die("Duplicate entry " . hex2bin($first_hex) . $number_of_dbs . hex2bin($second_hex) . " for key 'group_key'");
```

```
# Getting the DB name
```

```
if(strpos(urldecode($_GET["id"]), "FROM INFORMATION_SCHEMA.SCHEMATA LIMIT")!==false ) die("Duplicate entry " . hex2bin($first_hex) . $db_msg . hex2bin($second_hex) .
```

```
" for key 'group_key'");
```

```
    echo "Duplicate entry '$string' for key 'group_key'";  
}
```

?>

The command I was:

Quote:sqlmap.py -u "http://www.site.com/manipulate.php?id=1" --threads=10 --dbs

Sorry If the thread was hard to understand, I wrote it in a hurry.

Mr.0_0 - December 23, 2015, 12:30 pm

I like, neat stuff there.

h?ck?r - December 23, 2015, 12:32 pm

That's awesome!! Hope people stop using sqlmap. Manuals more fun/challenging

HaxOr? - December 23, 2015, 7:47 pm

(Dec 23, 2015 01:32 PM)[DarkSide] Wrote: [\[CITE\]](#) That's awesome!! Hope people stop using sqlmap. Manuals more fun/challenging

Ok tell me how will you dump 500k lines in under 20 minutes by doing it manually?

SIM-1073426 - December 23, 2015, 8:34 pm

(Dec 23, 2015 08:47 PM)HaxOr? Wrote: [\[CITE\]](#) Ok tell me how will you dump 500k lines in under 20 minutes by doing it manually?

Multiple keyboards

Viktory - December 23, 2015, 9:49 pm

(Dec 23, 2015 09:34 PM)Aces. Wrote: [\[CITE\]](#) Multiple keyboards
<https://giant.gfycat.com/TemptingCourageousAfricanmolesnake.mp4>

krankenstein - December 25, 2015, 1:23 am

Trying..... :-()