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 dumpfile ‘/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

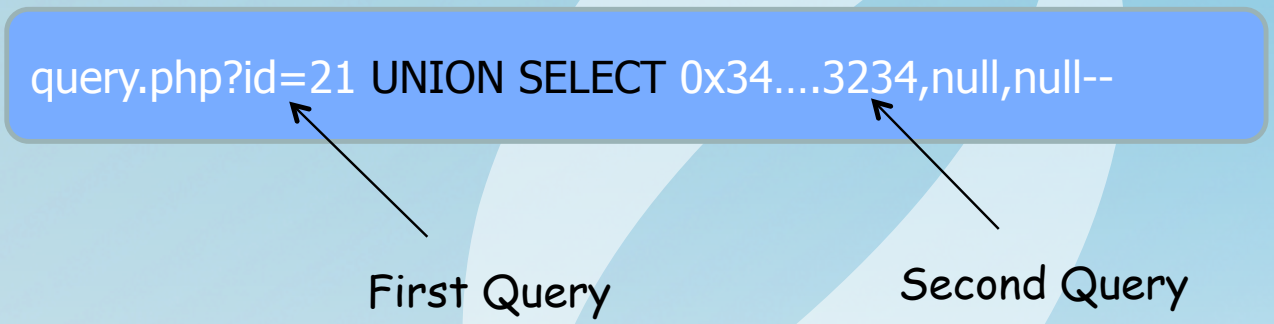
- Remote command execution on MySQL-PHP
  - Traditionally, simple PHP shell is used to execute command
  - Weak and has no strong functionality
- We need a reliable shell!
  - Metasploit contains variety of shellcodes
  - Meterpreter shellcode for post exploitation process
  - VNC shellcode for GUI access on the host

- File read/write access on MySQL-PHP platform
  - SELECT .. LOAD_INFILE is used to read file
  - SELECT .. INTO OUTFILE/DUMPFILE 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 unnecesary data into our arbitrary data. This can potentially corrupt our file

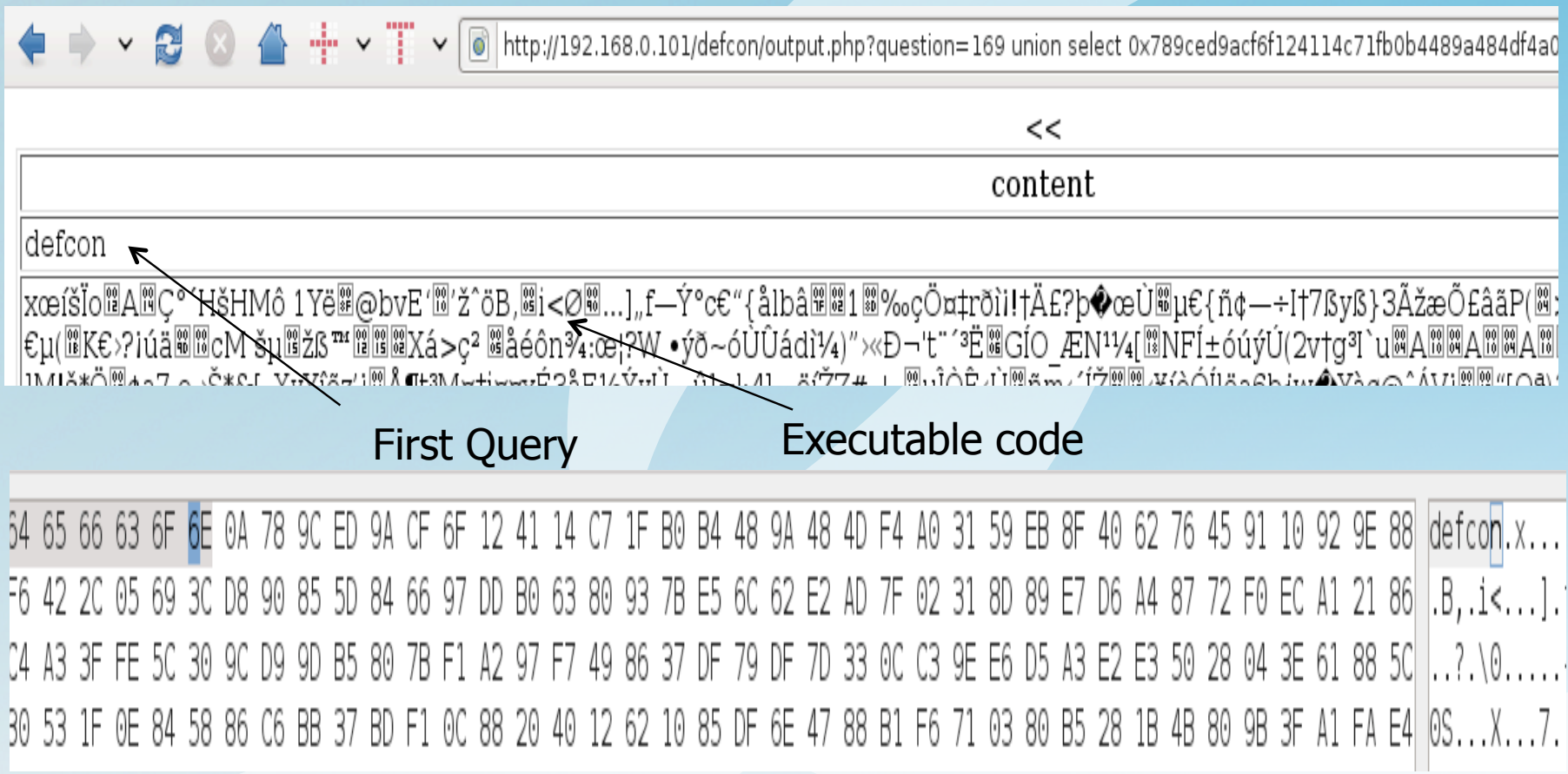
- Fixing the URL length issue
  - PHP Zlib module can be used to compress the arbitrary file
  - 9625 bytes of executable can be compressed to 630 bytes which is able to bypass the max limit request
  - Decompress the file on the destination before the arbitrary file is executed

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



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

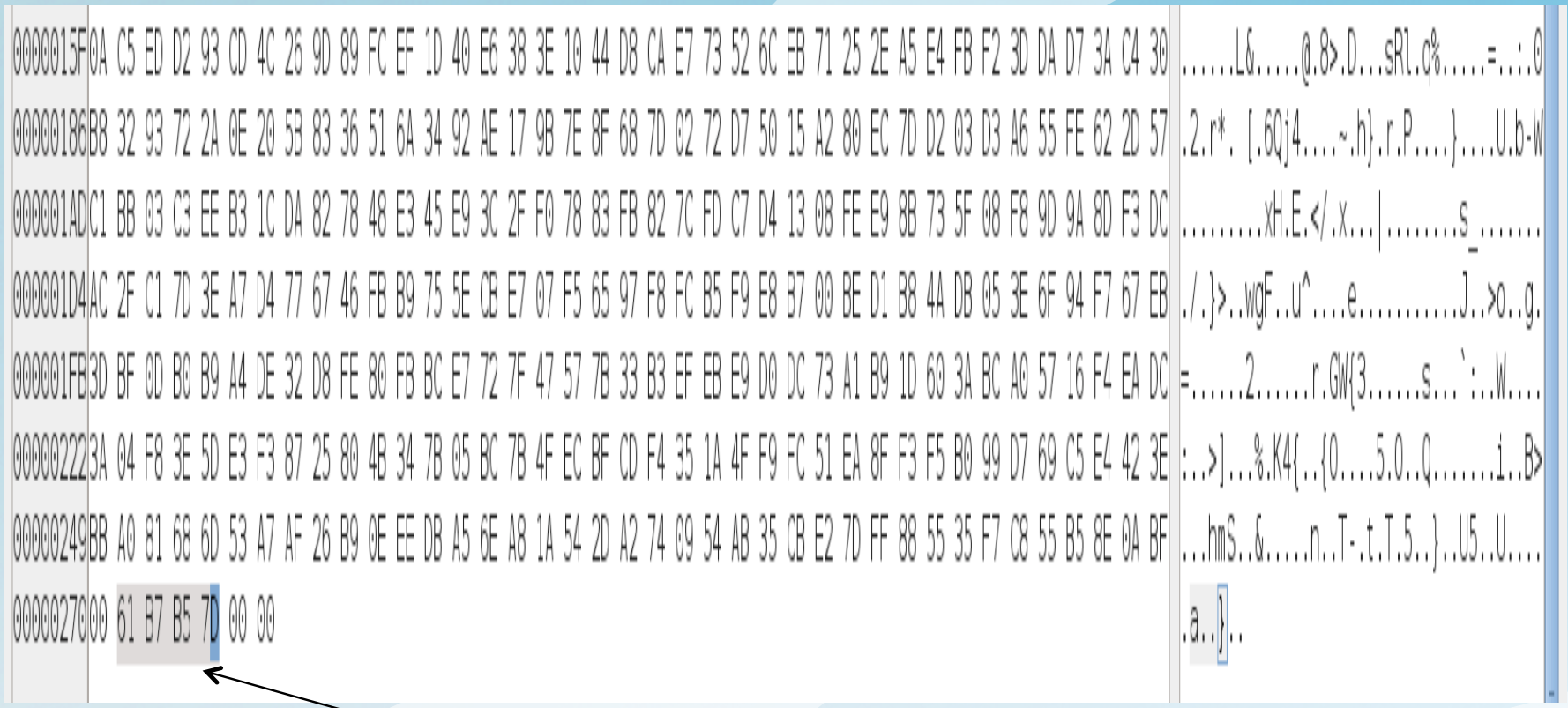
Result from first query data + executable code



- 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

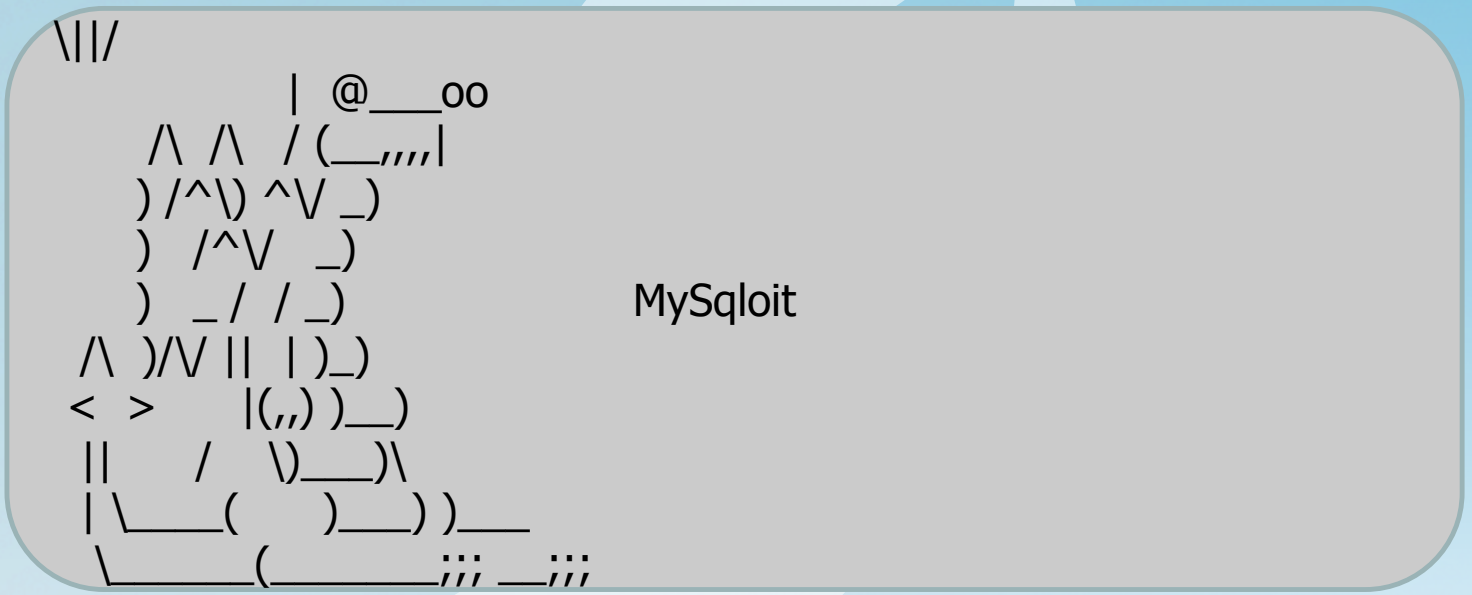


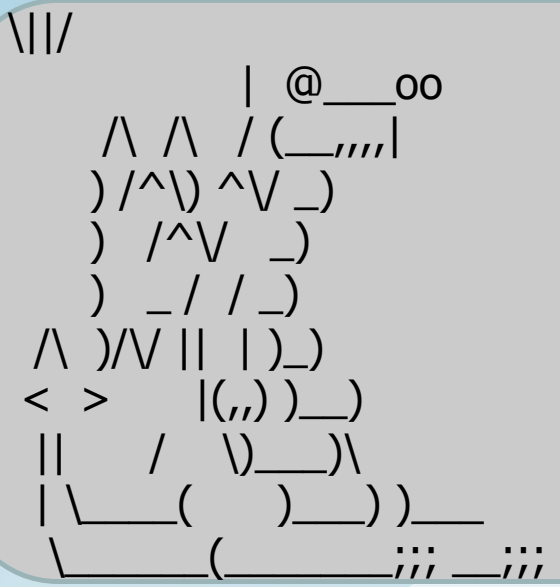
- Remote code execution on LAMP (Linux, Apache, MySQL, PHP)
  - By default, any directory created in Linux is not writable by mysql /web server users
  - When the mysql user has the ability to upload a file onto the web server directory, this directory can be used to upload our arbitrary file
  - By 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

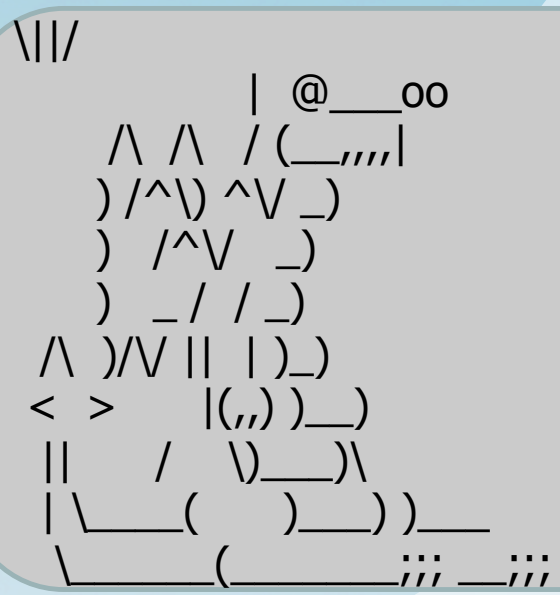
- MySqloit
  - MySqloit is a MySQL injection takeover tool
- Features
  - SQL Injection detection – Detect SQL Injection through deep blind injection method
  - Fingerprint Dir – Fingerprint the web server directory
  - Fingerprint OS – Fingerprint the Operating System
  - Payload – Create a shellcode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

Demo





Questions ?



Thank You

muhaimindz@gmail.com