**1. Cài mã nguồn DVWA để thực hành khai thác lỗi web cũng như demo tấn công**

**1.1 Download mã nguồn của DVWA**

# cd /var/www/html/ [14]

#wget<ahref="https://github.com/RandomStorm/DVWA/archive/v1.0.8.zip">https://github.com/RandomStorm/DVWA/archive/v1.0.8.zip</a>

# unzip v1.0.8.zip

# cd v1.0.8

# mv ./\* ../

# ls /var/www/html/

about.php COPYING.txt external ids\_log.php login.php php.ini security.php

CHANGELOG.md docs favicon.ico index.php logout.php README.md setup.php

config dvwa hackable instructions.php phpinfo.php robots.txt vulnerabilities

**1.2 Khởi tạo database và user cho DVWA**

# mysql -u root -p

Enter password :

> CREATE DATABASE dvwa\_db;

Query OK, 1 row affected (0.00 sec)

> GRANT ALL PRIVILEGES ON dvwa\_db.\* TO 'dvwa\_admin'@'localhost' IDENTIFIED BY '123456';

Query OK, 0 rows affected (0.00 sec)

> FLUSH PRIVILEGES;

Query OK, 0 rows affected (0.00 sec)

> exit

**1.3 Cấu hình config của DVWA**

# vi /var/www/html/config/config.inc.php

# 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' ] = 'localhost';

$\_DVWA[ 'db\_database' ] = 'dvwa\_db';

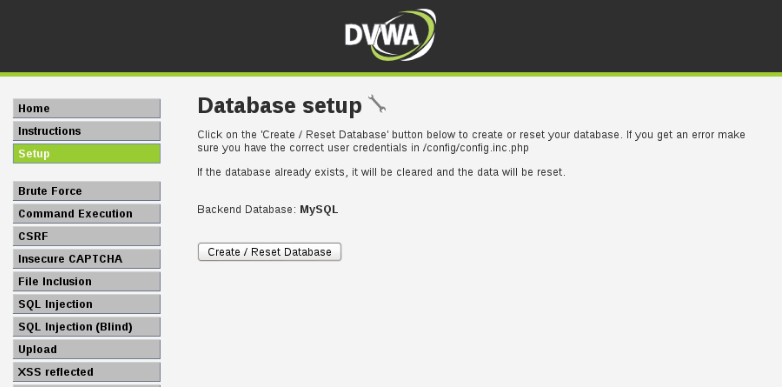
$\_DVWA[ 'db\_user' ] = 'dvwa\_admin';

$\_DVWA[ 'db\_password' ] = '123456';

**1.4 Thiết lập database cơ bản của DVWA**

Truy cập đường dẫn <http://10.0.0.2/setup.php> (10.0.0.2 là ip máy server)

Nhấn “Create/Reset Database” như vậy là trong CSDL của DVWA có 2 table duy nhất là “guestbook” dành cho lỗi XSS và “users” dành cho các lỗi khác



Hình 19: Nhấn Create/Reset Database để tạo database

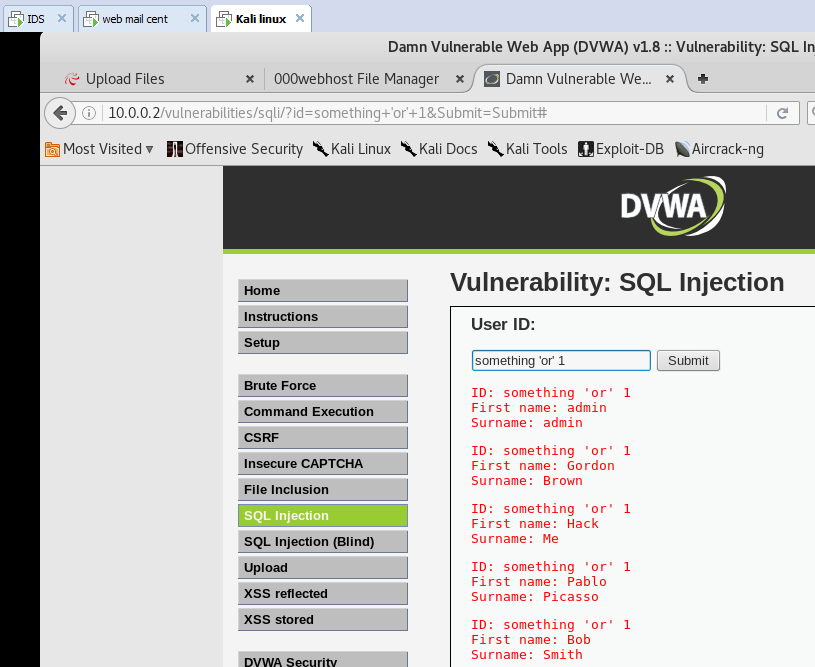
**1.5 Truy cập web DVWA bắt đầu thực hành**

Truy cập <http://10.0.0.2/login.php> để đăng nhập và thực hành khai thác lỗi

Tài khoản mặc định sẽ là: admin/password

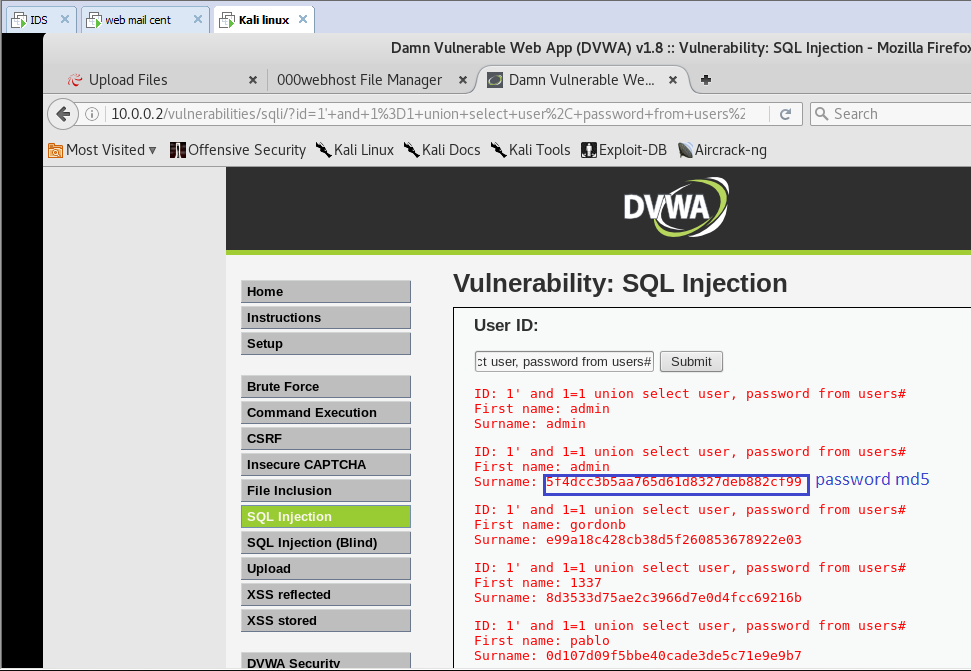
**1.6 Tấn công SQL Injection, ex**

* Thử truy vấn tất cả các user có trong CSDL



Hình 57: Tất cả user name hiện ra

* Và truy vấn ra cả user name và password



Hình 58: Password với dạng mã hóa md5