International Institute of Information Technology Hyderabad

System and Network Security (CS5470)

Lab Assignment 5: Password Cracking using Brute Force attack and SQL Injection Operations

Hard Deadline: April 3, 2019 (23:55 P.M.)

Total Marks: 100 [Implementation (Report + correct results): 75, Vice-voce: 25]

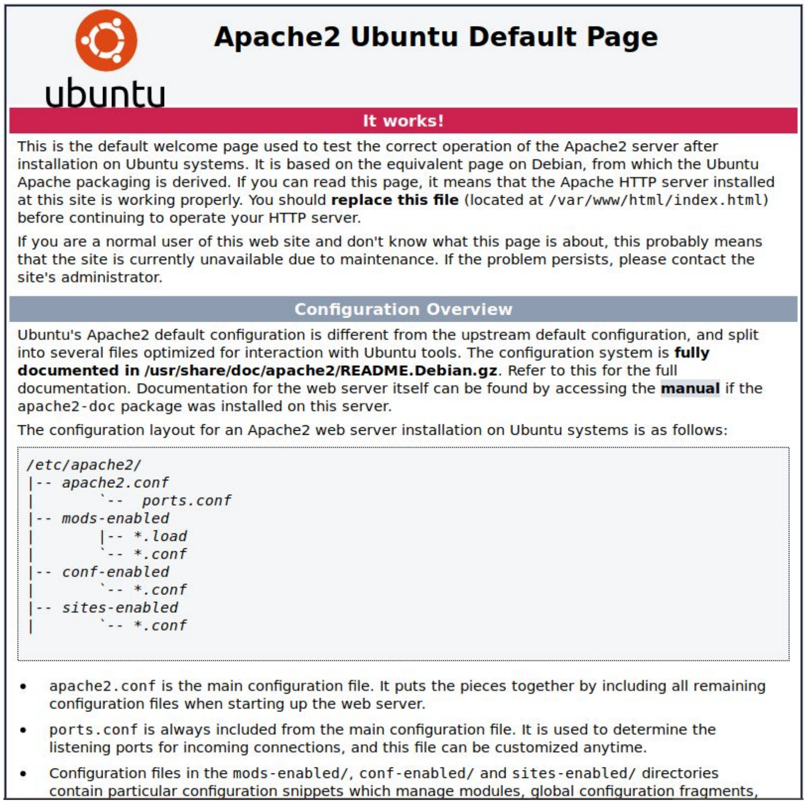
Note:- It is strongly recommended that no student copies any result from others. Hence, if there is any duplicate in the assignment, simply both the parties will be given zero marks without any compromise. Rest of assignments will not be evaluated further and assignment marks will not be considered towards final grading in the course. No assignment will be taken after deadline. Please upload the pdf report file in the course moodle portal through a ZIP file (Lab5-RollNumber.zip).

It is preferable to use a Virtual Box for this assignment.

Setup:-

This will help you create a environment on your local machine wherein you can test before proceeding to solve the Question 1. Question 2 needs to be solved on the environment that you created on your local machine.

1. Download DVWA from http://www.dvwa.co.uk/
2. Use the github link (https://github.com/ethicalhack3r/DVWA) which will help in setting up the tool.
3. In this I have used Ubuntu 18.04 for the setup.
4. After downloading the DVWA-master.zip file, copy the extracted folder to the following location var/www/html (I have renamed to DVWA)
5. Run the following command :- apt-get -y install apache2 mysql-server php php-mysqli php-gd libapache2-mod-php
6. Check if apache2 is running or not by putting 127.0.0.1 (or the ip you have set for apache server) in any of the browsers. You will get the following page



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

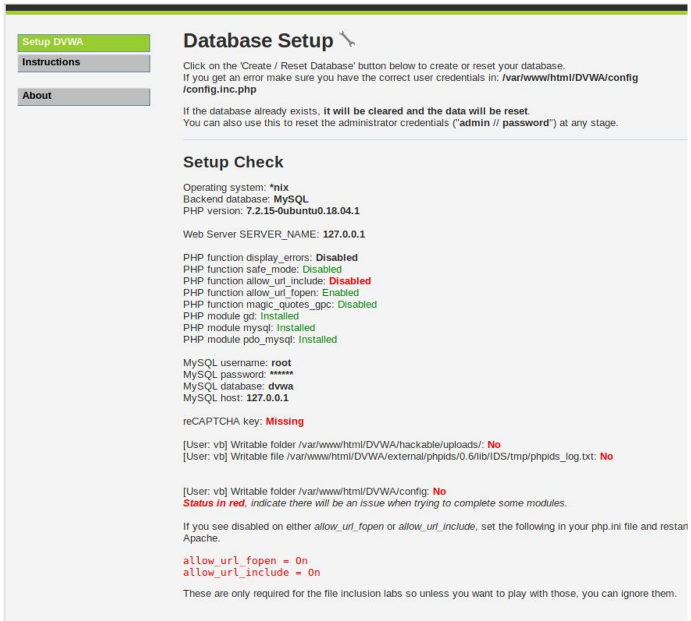
The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments,

7. Try to access the following link:- 127.0.0.1/DVWA/index.php, if you are getting the following error: -
   DVWA System error - config file not found. Copy config/config.inc.php.dist to config/config.inc.php and configure to your environment.

   Rename the /var/www/html/DVWA/config/config.inc.php.dist file to /var/www/html/DVWA/config/config.inc.php after which you should get the following page



Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database.
If you get an error make sure you have the correct user credentials in: **/var/www/html/DVWA/config /config.inc.php**

If the database already exists, **it will be cleared and the data will be reset**.
You can also use this to reset the administrator credentials ("**admin** // **password**") at any stage.

Setup Check

Operating system: ***nix**
Backend database: **MySQL**
PHP version: **7.2.15-0ubuntu0.18.04.1**

Web Server SERVER_NAME: **127.0.0.1**

PHP function display_errors: **Disabled**
PHP function safe_mode: Disabled
PHP function allow_url_include: **Disabled**
PHP function allow_url_fopen: Enabled
PHP function magic_quotes_gpc: Disabled
PHP module gd: Installed
PHP module mysql: Installed
PHP module pdo_mysql: Installed

MySQL username: **root**
MySQL password: **********
MySQL database: **dvwa**
MySQL host: **127.0.0.1**

reCAPTCHA key: **Missing**

[User: vb] Writable folder /var/www/html/DVWA/hackable/uploads/: **No**
[User: vb] Writable file /var/www/html/DVWA/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: **No**

[User: vb] Writable folder /var/www/html/DVWA/config: **No**
Status in red, *indicate there will be an issue when trying to complete some modules.*

If you see disabled on either *allow_url_fopen* or *allow_url_include*, set the following in your php.ini file and restart Apache.

```
allow_url_fopen = On
allow_url_include = On
```

These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.

8. Use the following page to setup your mysql :- https://support.rackspace.com/how-to/installing-mysql-server-on-ubuntu/
   Note that if '/usr/bin/mysql -u root -p' running this command gives error try it with sudo, wherein you give the system password followed by the mysql password which is root
9. To make the changes such that next time login to mysql does not require the system password do the following

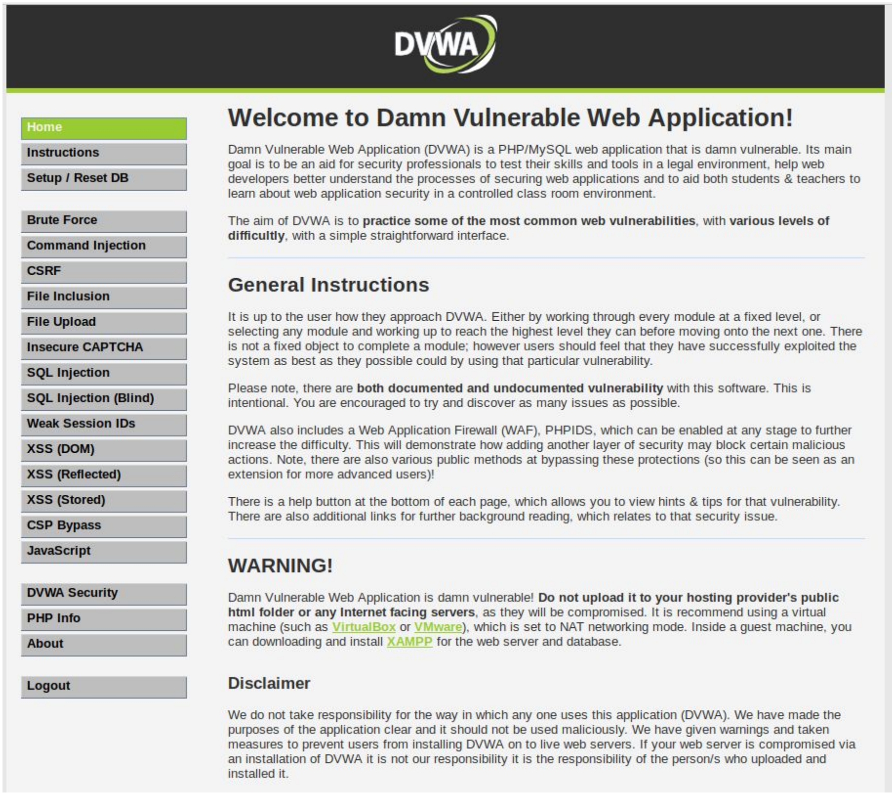
```
$ sudo mysql -u root # I had to use "sudo" since is new installation

mysql> USE mysql;
mysql> UPDATE user SET plugin='mysql_native_password' WHERE User='root';
mysql> FLUSH PRIVILEGES;
mysql> exit;

$ service mysql restart
```

   (https://stackoverflow.com/questions/39281594/error-1698-28000-access-denied-for-user-rootlocalhost)
10. Once done Click on the 'Create/Reset Database' at the end of the Database Setup page and you can login into the DVWA, using admin/password.

11. You get a page like the following:-



Welcome to Damn Vulnerable Web Application!

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goal is to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and to aid both students & teachers to learn about web application security in a controlled class room environment.

The aim of DVWA is to **practice some of the most common web vulnerabilities**, with **various levels of difficultly**, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, or selecting any module and working up to reach the highest level they can before moving onto the next one. There is not a fixed object to complete a module; however users should feel that they have successfully exploited the system as best as they possible could by using that particular vulnerability.

Please note, there are **both documented and undocumented vulnerability** with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to further increase the difficulty. This will demonstrate how adding another layer of security may block certain malicious actions. Note, there are also various public methods at bypassing these protections (so this can be seen as an extension for more advanced users)!

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! **Do not upload it to your hosting provider's public html folder or any Internet facing servers**, as they will be compromised. It is recommend using a virtual machine (such as VirtualBox or VMware), which is set to NAT networking mode. Inside a guest machine, you can downloading and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

From the left menu, click on DVWA Security and change in the security level to Low. or you can change the security from the /var/www/html/DVWA/config/config.inc.php file

Question 1:-

Go to the website http://128.199.255.176/DVWA/login.php, login using admin/password. On the left tab, you will find the BruteForce option. Select it and try to find the password associated with your user_id. Your user_id have been provided in a separate excel sheet. [The password is of length 3 and is made of upper and lowercase English Characters]. You have to find two passwords associated with 2 different accounts. Mention the password in the report and provide the steps that were used to get it.

Bonus: There is also a 4 character password, made of upper and lowercase English characters.

Question 2:-

After setting DVWA in your system, use the SQL Injection to find out the following:-

a. All the users in the database
b. The version of the database being used
c. The hostname
d. The user of the database
e. The schema that is being used

For the above provide the commands used. Mention the findings in a report.

You need to submit only the pdf report as a part of the submission.

Username List

First name	Surname	ID number		User_Id(4 character)	User_Id(3 character)	User_Id(3 character)
Bhargava	Somu	201501017		bhargava	bhargava1	bhargava2
Megh	Parikh	201501184		megh	megh1	megh2
Nikhil	Parasaram	201501202		nikhil	nikhil1	nikhil2
shadaab	siddiqie	201502030		shadaab	shadaab1	shadaab2
Sai Teja Reddy	Moolamalla	201564086		sai	sai1	sai2
Aman	Bansal	20161008		amanb	amanb1	amanb2
Sudheer	Achary	20161076		sudheer	sudheer1	sudheer2
RAJESH	DANSENA	20163005		rajesh	rajesh1	rajesh2
NIHARIKA	KHARE	2018201002		niharika	niharika1	niharika2
Sarvat	Ali	2018201009		sarvat	sarvat1	sarvat2
Padma	Dhar	2018201011		padma	padma1	padma2
Ishan	Tyagi	2018201017		ishan	ishan1	ishan2
ANJUL	GUPTA	2018201021		anjul	anjul1	anjul2
NAWAB	ALAM	2018201030		nawab	nawab1	nawab2
Manojit	Chakraborty	2018201032		manojit	manojit1	manojit2
DARSHAN	KANSAGARA	2018201033		darshan	darshan1	darshan2
Divyanshi	Kushwaha	2018201046		divyanshi	divyanshi1	divyanshi2
Pranav	Verma	2018201047		pranav	pranav1	pranav2
Lokesh	Singh Mahar	2018201049		lokesh	lokesh1	lokesh2
Prabha	Pandey	2018201053		prabha	prabha1	prabha2
Meghashree	K A	2018201055		meghashree	meghashree1	meghashree2
ADITI	SHRIVASTAVA	2018201056		aditi	aditi1	aditi2
SHAFIYA	NAAZ	2018201062		shafiya	shafiya1	shafiya2
SOPNESH	GANDHI	2018201064		sopnesh	sopnesh1	sopnesh2
Amrit	Kataria	2018201067		amrit	amrit1	amrit2
Aman	Sharma	2018201084		amans	amans1	amans2
Aman	Raj	2018201085		amanr	amanr1	amanr2
Varun	Bhatt	2018201086		varun	varun1	varun2
Sonakshi	Sharma	2018201090		sonakshi	sonakshi1	sonakshi2
Shreya	Upadhyay	2018201091		shreya	shreya1	shreya2

Manik	Langer	2018201092		manik	manik1	manik2
Pranjal	Patidar	2018201094		pranjal	pranjal1	pranjal2
AJAY	JADHAV	2018201095		ajay	ajay1	ajay2
Shashi	Jangra	2018202001		shashi	shashi1	shashi2
Sayan	Ghosh	2018202002		sayan	sayan1	sayan2
SURAJ	GARG	2018202003		suraj	suraj1	suraj2
Shubham	Das	2018202004		shubham	shubham1	shubham2
AISHWARYA	SHIVACHANDRA	2018202005		aishwarya	aishwarya1	aishwarya2
Jatin	Paliwal	2018202006		jatin	jatin1	jatin2
TARUN	MUNJAL	2018202007		tarun	tarun1	tarun2
Sanket	Tilotkar	2018202008		sanket	sanket1	sanket2
Supriya	Priyadarshani	2018202009		supriya	supriya1	supriya2
Shruti	Chandra	2018202010		shruti	shruti1	shruti2
Yaswanth	Koravi	2018202011		yaswanth	yaswanth1	yaswanth2
PRIYA	UPADHYAY	2018202012		priya	priya1	priya2
SARAT	SRISTI	2018202013		sarat	sarat1	sarat2
Himani	Gupta	2018202014		himani	himani1	himani2
Kopal	Agarwal	2018202015		kopal	kopal1	kopal2
AISHWARY	DEWANGAN	2018202016		aishwary	aishwary1	aishwary2
ritik	agarwal	2018202017		ritik	ritik1	ritik2
RAJNEESH	SINGHATIYA	2018202018		rajneesh	rajneesh1	rajneesh2
Indraneel	Das	2018202019		indraneel	indraneel1	indraneel2
YASHDEEP	SAINI	2018202020		yashdeep	yashdeep1	yashdeep2
VISHAL	CHUGH	2018202021		vishal	vishal1	vishal2
PALAK	BAGGA	2018801015		palak	palak1	palak2
Arshad	Mohammed	2018900056		arshad	arshad1	arshad2