A. Hack a website by Remote File Inclusion

- A. Building a Web Hacking Lab (w/ XAMPP and DVWA):
- 1. Install XAMPP: XAMPP
- https://www.apachefriends.org/index.html o Create database



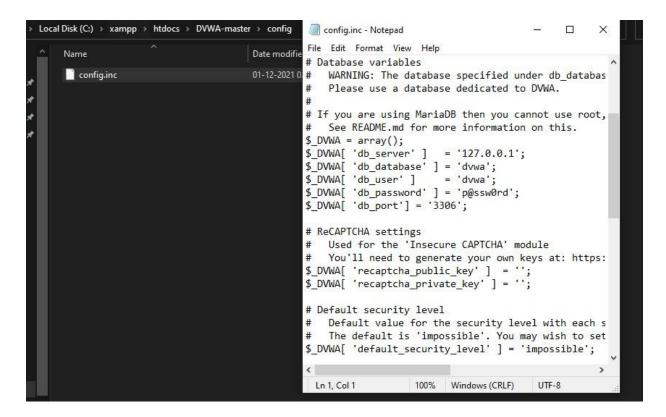
Enter mysql –u root

```
### April ### Ap
```

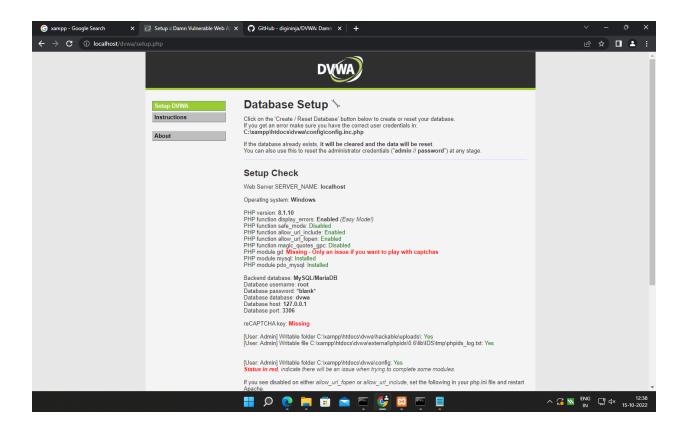
- Download DVWA-master.zip
- Install DVWA in C:\xampp\htdocs

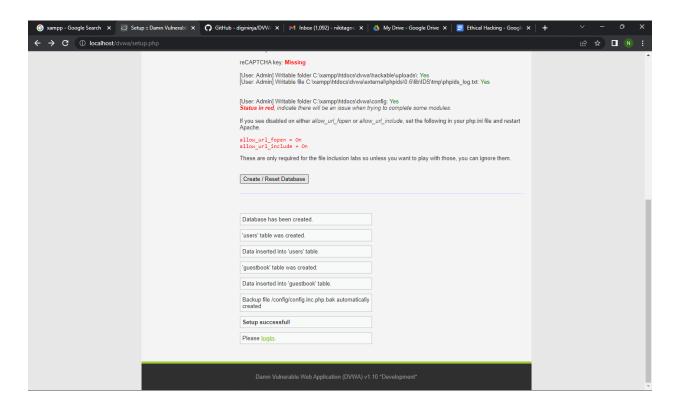
Name	Date modified	Туре	Size
chatify-demo-master	16-07-2021 12:36 PM	File folder	
dashboard	15-05-2021 06:10 PM	File folder	
DVWA-master	01-12-2021 02:29 PM	File folder	
img img	15-05-2021 06:10 PM	File folder	
rjobold	27-05-2021 09:49 AM	File folder	
webalizer	15-05-2021 06:10 PM	M File folder	
xampp	15-05-2021 06:10 PM	File folder	
applications	27-08-2019 07:32 PM	Chrome HTML Do	4 KE
📓 bitnami	27-08-2019 07:32 PM	Cascading Style S	1 KE
DVWA-master	10-12-2021 03:08 PM	WinRAR ZIP archive	1,351 KE
🖾 favicon	16-07-2015 09:02 PM	lcon	31 KE
index 🥏	16-07-2015 09:02 PM	PHP File	1 KE

 $Go to \ C: \ \ Change \ the \ file \ name \ config. in c.php. dist \ to \ config. in c.php$



In the browser, enter http://localhost/dvwa-master/setup.php. Scroll below to find:





Next, it opens the window below: http://localhost/DVWA-master/login.php

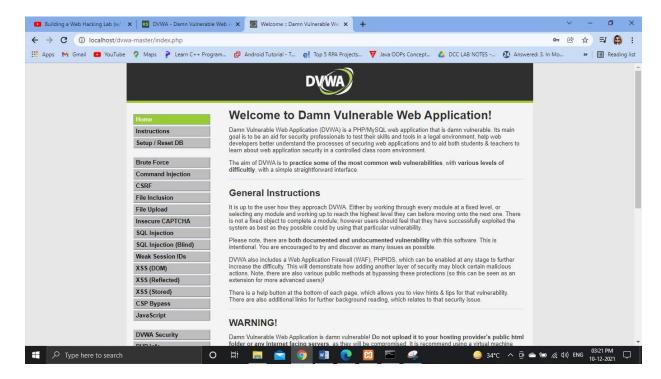


Username		
admin		
Password		

	Login	

 $Enter\ default\ credentials\ username = admin\ and\ password = password$

We are now logged into DVWA



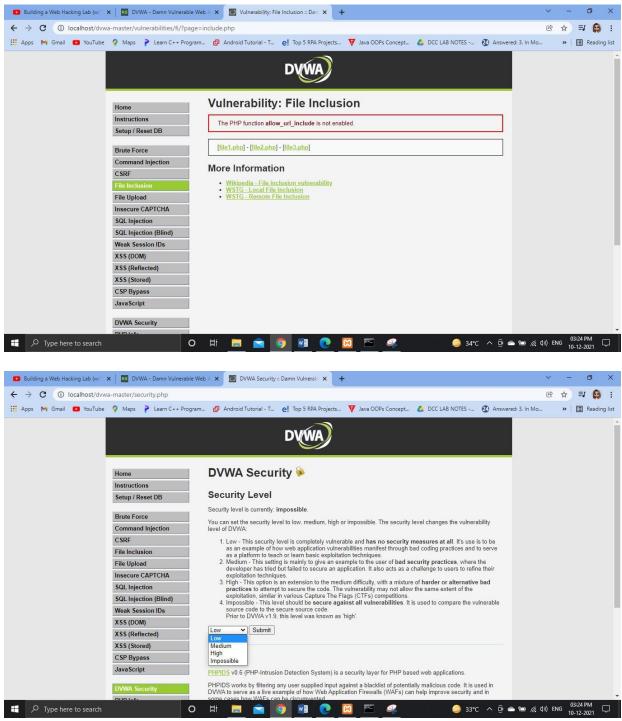
Local file inclusion and Remote file inclusion What is DVWA?

- ☐ PHP/MySQL web application that is vulnerable.
- ☐ Main goals:
- 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.
- Aid teachers/students to teach/learn web application security in a class room environment.
- a. A website attack named Remote file inclusion is basically a one of the most common vulnerability found in web application. This type of vulnerability allows the Hacker or attacker to add a remote file on the web server. If the attacker gets successful in performing the attack he/she will gain access to the web server and hence can execute any command on it.

Questions:

1. Create a login.php/registration.php for your website. Perform local file inclusion using DVWA.

Go to http://localhost/DVWA-master/vulnerabilities/fi/?page=include.php



On the address bar, set page attribute to http://localhost/sqlinjection/login.php

2. Perform remote file inclusion using DVWA. Display the home page of www.google.com On the address bar, set page attribute to http://www.google.com

B. Disguise as Google Bot to view Hidden Content of a Website

Step 1: To determine the user agent of firefox:

- a. Go to Mozilla –http://www.proxyserverprivacy.com/
- b. Select detector proxy
- c. Select advanced proxy detector. Output:

Free Proxy Checker Detection

Your Ip Address: 1.186.122.116 Host: 1.186.122.116.dvois.com

Your Country:

Proxy HTTP_X_FORWARDED Variable: (none)

Proxy HTTP_VIA Variable: (none)

Proxy HTTP_PROXY_CONNECTION: (none)

Cache Pragma: (none)

Your Browser: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0)

Gecko/20100101 Firefox/56.0

Type of your connection, keep-alive

Server Protocol: HTTP/1.1
Your language: en-US,en;q=0.5

Accept: text/html,application/xhtml+xml,application

/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Encoding: gzip, deflate Referer - HTTP Request come

from: http://www.proxyserverprivacy.com/detector-proxy.shtml

Your Port: 23166

Step 2: To find out the string for google bot. To change the above useragent to googlebot a. Goto http://useragentstring.com/

b. Locate the string for google bot Googlebot/2.1 (+http://www.googlebot.com/bot.html)

Step 3: Configure a. Go to

firefox

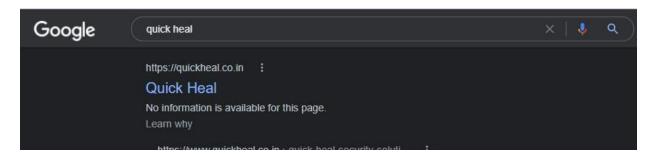
- b. Type about: config
- c. Type general.useragent.override and assign Googlebot/2.1

(+http://www.googlebot.com/bot.html)

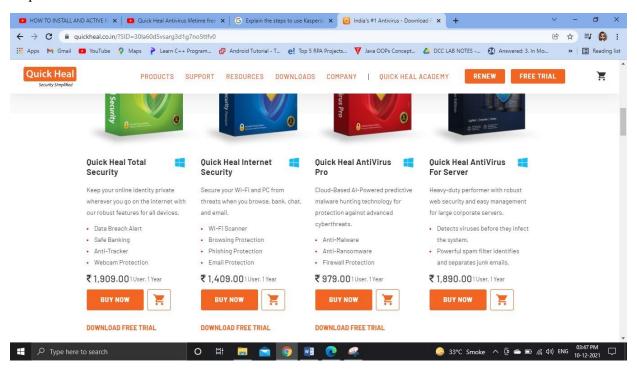
d. Goto http://www.proxyserverprivacy.com/ to check that the useragent is googlebot

C. Use Kaspersky/Quick Heal for Lifetime without Patch

Step 1: search for quick heal website on google



Step2: Download trial version



Step3: After 30 days of trial, uninstall the application

Step4: Again download the trial version of it, likewise you can use quick heal for lifetime by downloading its trial version every month.

C. How to use Kaspersky for Lifetime without Patch

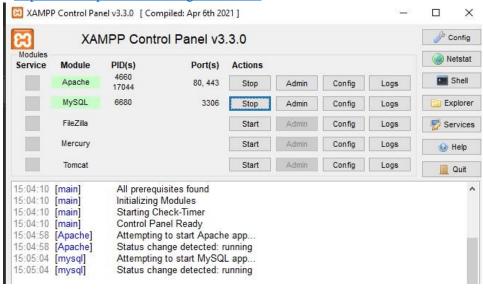
a. Explain the steps to use Kaspersky /Quick for lifetime.

Reference

https://www.youtube.com/watch?v=wn_JbYnKax0

D. Hack a website by Remote File Inclusion

- A. Building a Web Hacking Lab (w/ XAMPP and DVWA):
- 1. Install XAMPP: XAMPP
- https://www.apachefriends.org/index.html o Create database



Enter mysql –u root

```
Setting environment for using XAMPP for Windows.

Admin@BVIMIT-DESKTOP- c:\xampp

# mysql -u root
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 22
Server version: 10.4.25-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

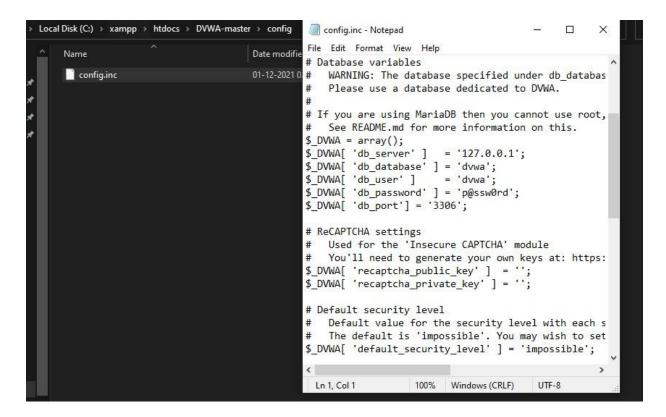
MariaDB [(none)]> __
```

```
### April ### Ap
```

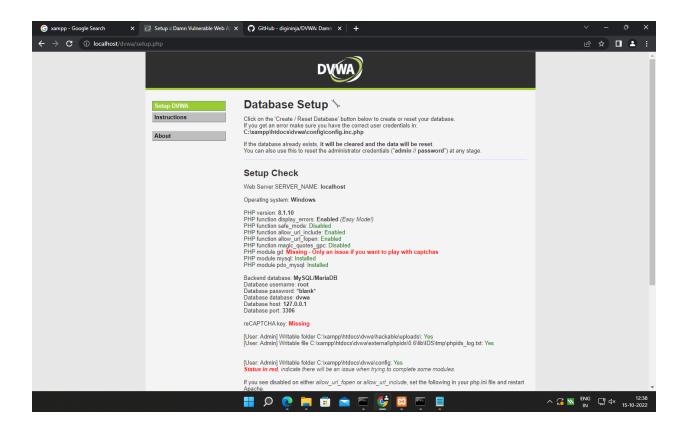
- Download DVWA-master.zip
- Install DVWA in C:\xampp\htdocs

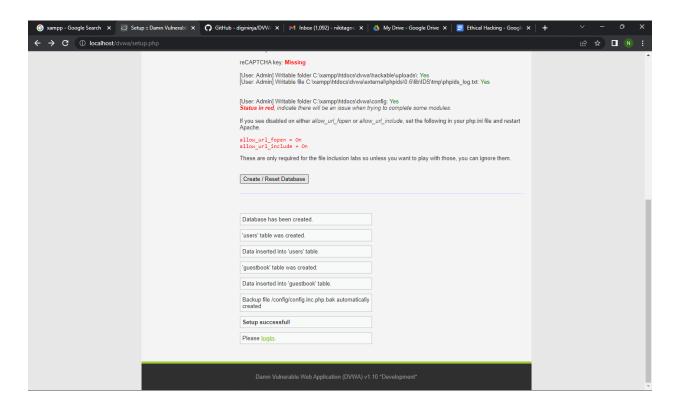
Name	Date modified	Туре	Size
chatify-demo-master	16-07-2021 12:36 PM	File folder	
dashboard	15-05-2021 06:10 PM	File folder	
DVWA-master	01-12-2021 02:29 PM	File folder	
img img	15-05-2021 06:10 PM	File folder	
rjobold	27-05-2021 09:49 AM	File folder	
webalizer	15-05-2021 06:10 PM	M File folder	
xampp	15-05-2021 06:10 PM	File folder	
applications	27-08-2019 07:32 PM	Chrome HTML Do	4 KE
📓 bitnami	27-08-2019 07:32 PM	Cascading Style S	1 KE
DVWA-master	10-12-2021 03:08 PM	WinRAR ZIP archive	1,351 KE
🖾 favicon	16-07-2015 09:02 PM	lcon	31 KE
index 🥏	16-07-2015 09:02 PM	PHP File	1 KE

 $Go to \ C: \ \ Change \ the \ file \ name \ config. in c.php. dist \ to \ config. in c.php$



In the browser, enter http://localhost/dvwa-master/setup.php. Scroll below to find:





Next, it opens the window below: http://localhost/DVWA-master/login.php

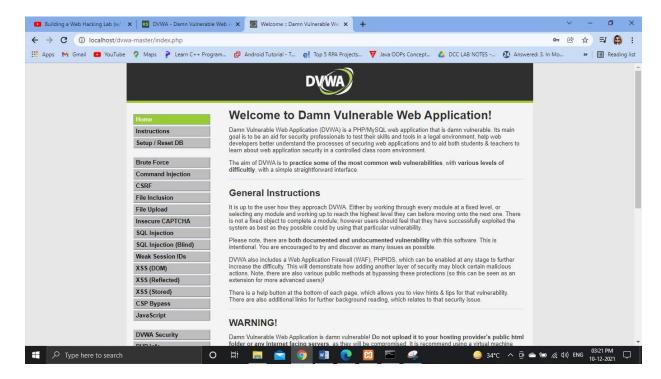


Username		
admin		
Password		

	Login	

 $Enter\ default\ credentials\ username = admin\ and\ password = password$

We are now logged into DVWA



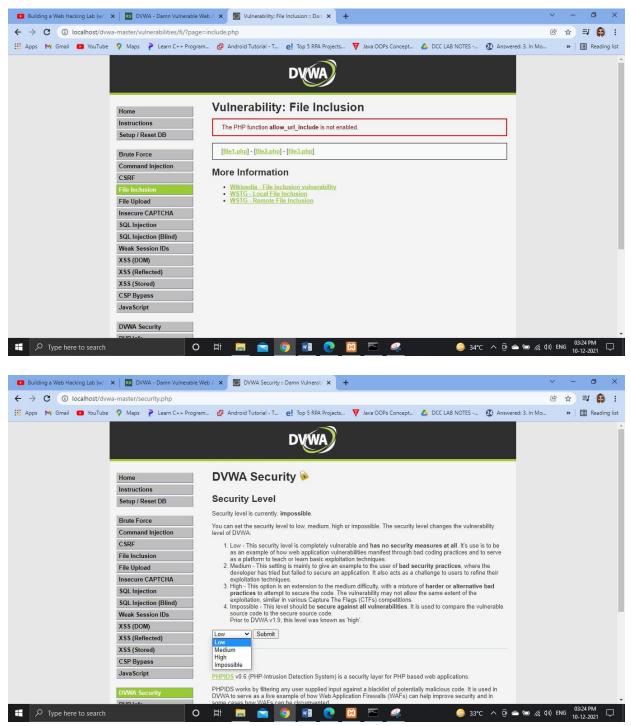
Local file inclusion and Remote file inclusion What is DVWA?

- ☐ PHP/MySQL web application that is vulnerable.
- ☐ Main goals:
- 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.
- Aid teachers/students to teach/learn web application security in a class room environment.
- a. A website attack named Remote file inclusion is basically a one of the most common vulnerability found in web application. This type of vulnerability allows the Hacker or attacker to add a remote file on the web server. If the attacker gets successful in performing the attack he/she will gain access to the web server and hence can execute any command on it.

Questions:

3. Create a login.php/registration.php for your website. Perform local file inclusion using DVWA.

Go to http://localhost/DVWA-master/vulnerabilities/fi/?page=include.php



On the address bar, set page attribute to http://localhost/sqlinjection/login.php

4. Perform remote file inclusion using DVWA. Display the home page of www.google.com On the address bar, set page attribute to http://www.google.com

E. Disguise as Google Bot to view Hidden Content of a Website

Step 1: To determine the user agent of firefox:

- d. Go to Mozilla -http://www.proxyserverprivacy.com/
- e. Select detector proxy
- f. Select advanced proxy detector. Output:

Free Proxy Checker Detection

Your Ip Address: 1.186.122.116 Host: 1.186.122.116.dvois.com

Your Country:

Proxy HTTP_X_FORWARDED Variable: (none)

Proxy HTTP_VIA Variable: (none)

Proxy HTTP_PROXY_CONNECTION: (none)

Cache Pragma: (none)

Your Browser: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:56.0)

Gecko/20100101 Firefox/56.0

Type of your connection, keep-alive

Server Protocol: HTTP/1.1
Your language: en-US,en;q=0.5

Accept: text/html,application/xhtml+xml,application

/xml;q=0.9,image/webp,*/*;q=0.8 Accept-Encoding: gzip, deflate Referer - HTTP Request come

from: http://www.proxyserverprivacy.com/detector-proxy.shtml

Your Port: 23166

Step 2: To find out the string for google bot. To change the above useragent to googlebot a. Goto http://useragentstring.com/

b. Locate the string for google bot Googlebot/2.1 (+http://www.googlebot.com/bot.html)

Step 3: Configure

a. Go to

firefox

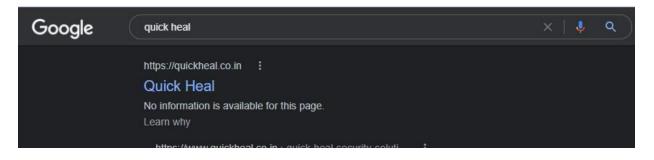
- e. Type about: config
- f. Type general.useragent.override and assign Googlebot/2.1

(+http://www.googlebot.com/bot.html)

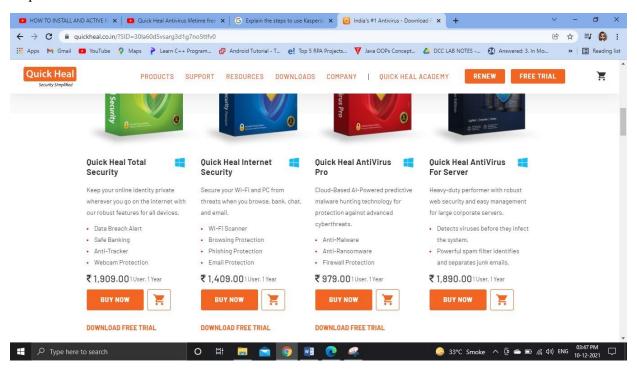
g. Goto http://www.proxyserverprivacy.com/ to check that the useragent is googlebot

C. Use Kaspersky/Quick Heal for Lifetime without Patch

Step 1: search for quick heal website on google



Step2: Download trial version



Step3: After 30 days of trial, uninstall the application

Step4: Again download the trial version of it, likewise you can use quick heal for lifetime by downloading its trial version every month.

F. How to use Kaspersky for Lifetime without Patch

a. Explain the steps to use Kaspersky /Quick for lifetime.

Reference

https://www.youtube.com/watch?v=wn_JbYnKax0
https://www.youtube.com/watch?v=mi_b\//2QRbQw&t=103e