HOW TO USE PAROS

PAROS VULNERABILITY SCANNER

MoTech

Makes Things Happen For You

NOEL MOSES MWADENDE

ABOUT THE AUTHOR

Noel Moses Mwadende is the passionate book and article writer based of different books and articles concern computer science in general, especially in cybersecurity and machine learning, currently Noel is employed as youtuber and book author at MoTech which is mini firm dealing with provision of information technology services.

INTRODUCTION.

It happen I had my vulnerability scanner reporting that there was SQL injection in a website, I dived in exploiting it but it was unable to be exploited then I thought it would be false positive result from my scanner, then after I thought how can I know if it is false positive or it was end of my ability in exploiting SQL injection, then it thought it is better to scan vulnerability by using more than one tool, then after I tried to learn how can I use another vulnerability scanner which is called paros, after knowing how to use it today am ready to share my experience to you.

TABLE OF CONTENTS

CHAPTER ONE

CHAPTER TWO

CHAPTER THREE

CHAPTER FOUR

CHAPTER FIVE

CHAPTER ONE.

CONFIGURING PROXY ON BROWSER.

On the top right side of your browser, am using Mozilla Firefox, there is bar as shown in the figure 1, if you place cursor **on it, it is highlighted as Open menu, click it and find preferences.**

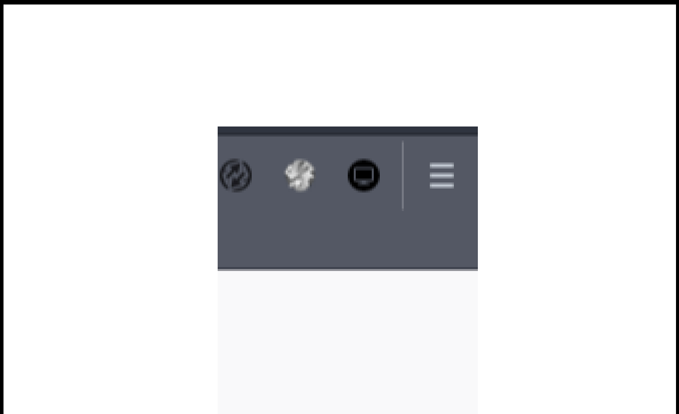


Fig. 1.

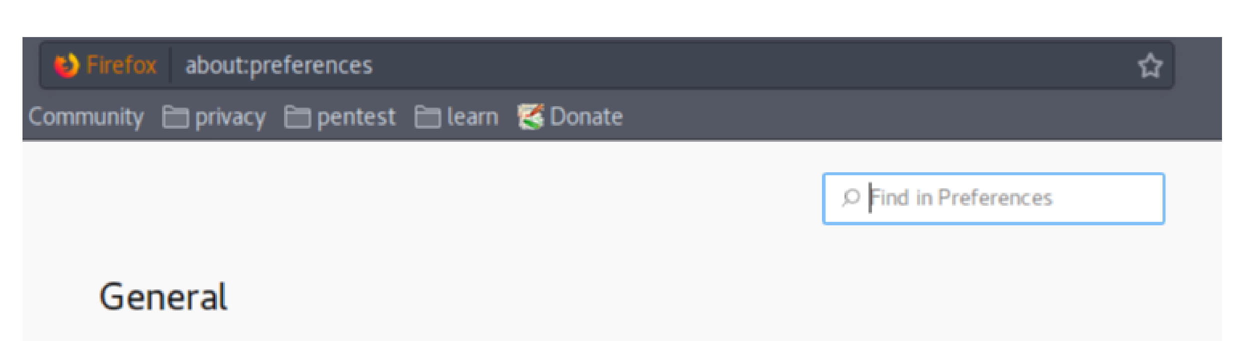
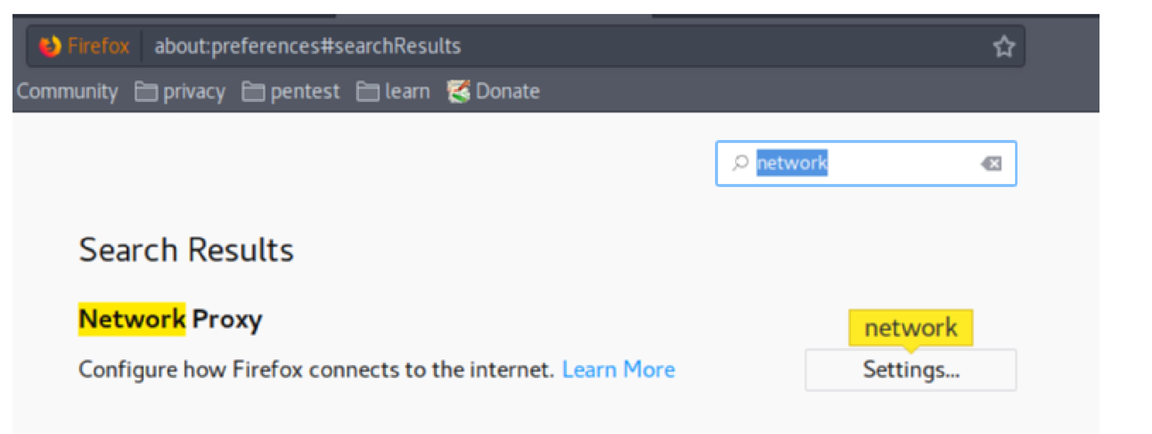


Fig. 2.

After clicking on the preferences, your browser will look as it is shown in the figure 2, on above search field type network, network proxy will come up as shown in the figure 3 then click on settings.



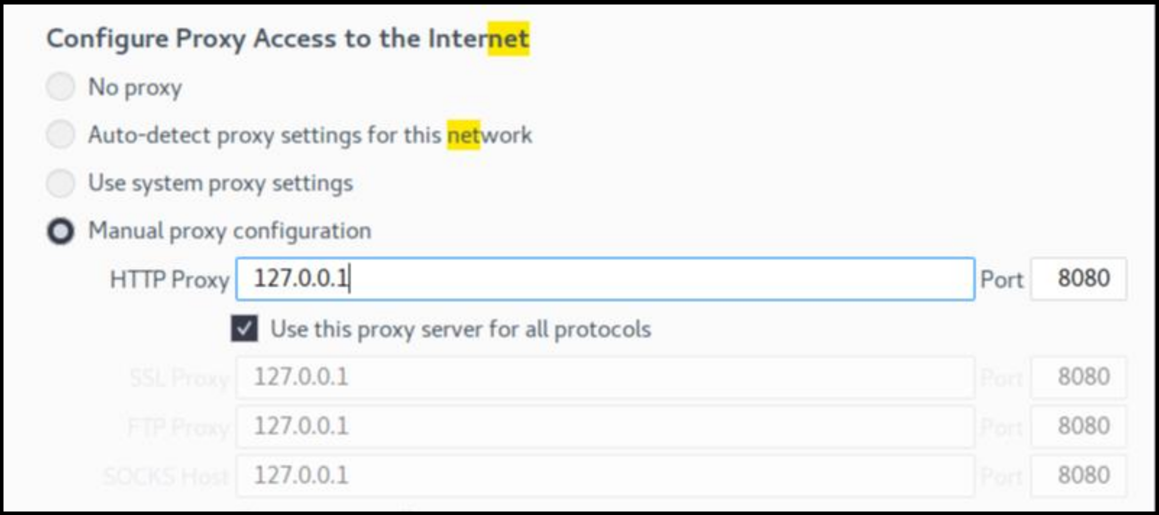
Firefox about:preferences#searchResults

Search Results

Network Proxy

Configure how Firefox connects to the internet. Learn More

Fig. 3.



Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

☑ Use this proxy server for all protocols

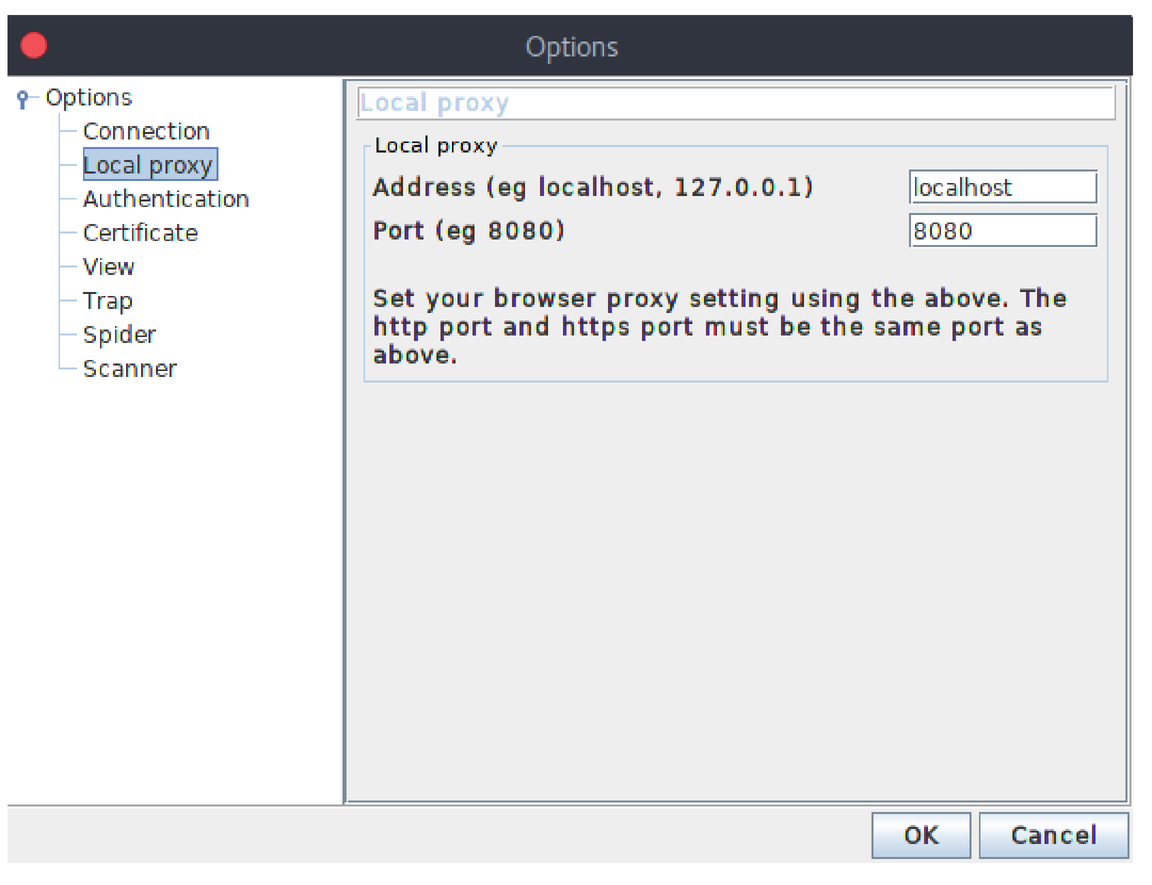
SSL Proxy 127.0.0.1 Port 8080

FTP Proxy 127.0.0.1 Port 8080

SOCKS Host 127.0.0.1 Port 8080

Fig. 4.

Proxy uses 127.0.0.1:8080, that is IP address of the localhost and port it uses that is 8080, make sure everything is configured the same as shown in the figured 4.



Local proxy

Local proxy

Address (eg localhost, 127.0.0.1): localhost

Port (eg 8080): 8080

Set your browser proxy setting using the above. The http port and https port must be the same port as above.

Fig. 5.

If you get any trouble try this, go on the top view of paros find tab called tools → options, and check if above fields are filled as shown in the figure 5, just focus on the second option which is named local proxy.

CHAPTER TWO.

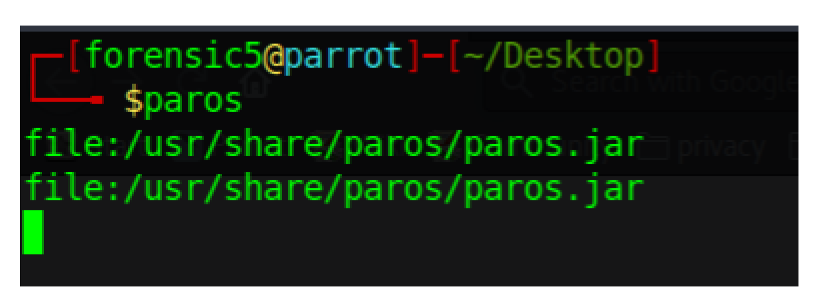
START PAROS.

There are two options to start paros, you can start paros from terminal or search it from menu, but you should make sure that proxy is well configured on your browser.

Option to get and start paros

- ➔ **Terminal.**
- ➔ **Search menu.**

Start paros on terminal. as shown on figure 6 or you can go to menu, search it and double click it to start paros.



```
┌─[forensic5@parrot]─[~/Desktop]
└──╼ $paros
file:/usr/share/paros/paros.jar
file:/usr/share/paros/paros.jar
█
```

Fig. 6.

CHAPTER THREE.

BROWSING TARGET WEB PAGES.

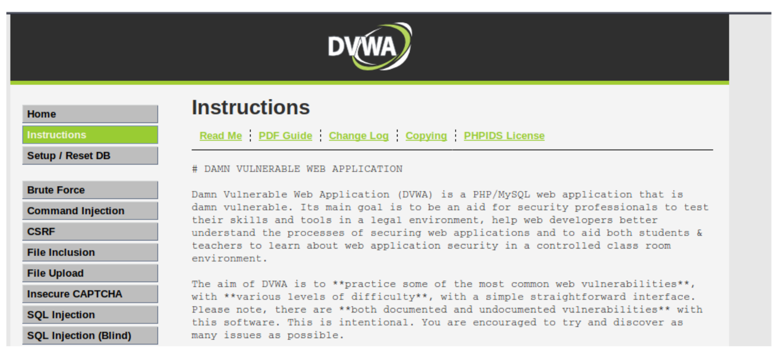
Browse different pages of target so that all request can be intercepted by proxy and being sent to the proxy, make sure you browse a lot of pages so that many requests can be sent to paros.

Important pages to browse.

- ⇨ **Login forms.**
- ⇨ **Register forms.**
- ⇨ **Any other forms in the target site.**
- ⇨ **All application.**
- ⇨ **Subdomain, if any.**
- ⇨ **Uploading options.**

Those are the most sensitive pages to browse, and this is because they sent request direct to the server, they sent queries to the server, as proxy is available, those intercepted request may easily checked and analyzed. For my case, my target is localhost/DVWA/ so I will do the following.

➔ **Browse in different pages.**



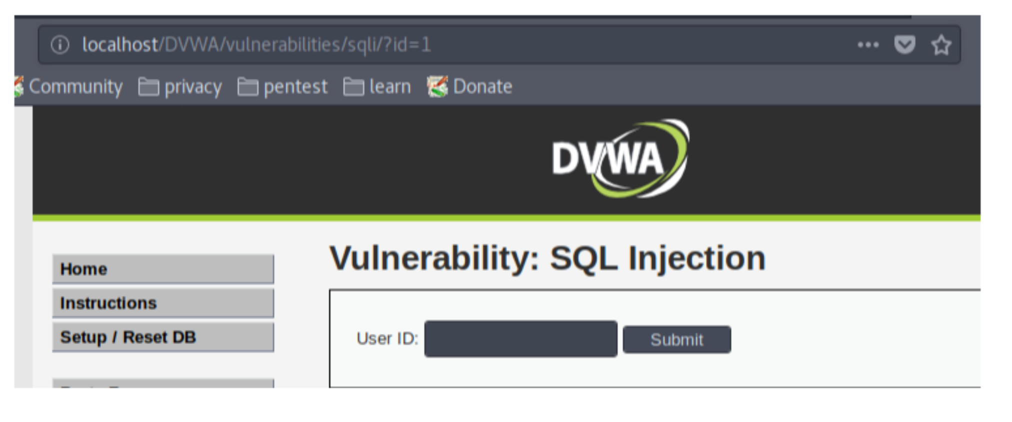
Instructions

```
# 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 difficulty**, with a simple straightforward interface.
Please note, there are **both documented and undocumented vulnerabilities** with
this software. This is intentional. You are encouraged to try and discover as
many issues as possible.
```

Fig. 7.

In the figure 7, I was trying to browse in different pages.

➔ Input data in input fields.



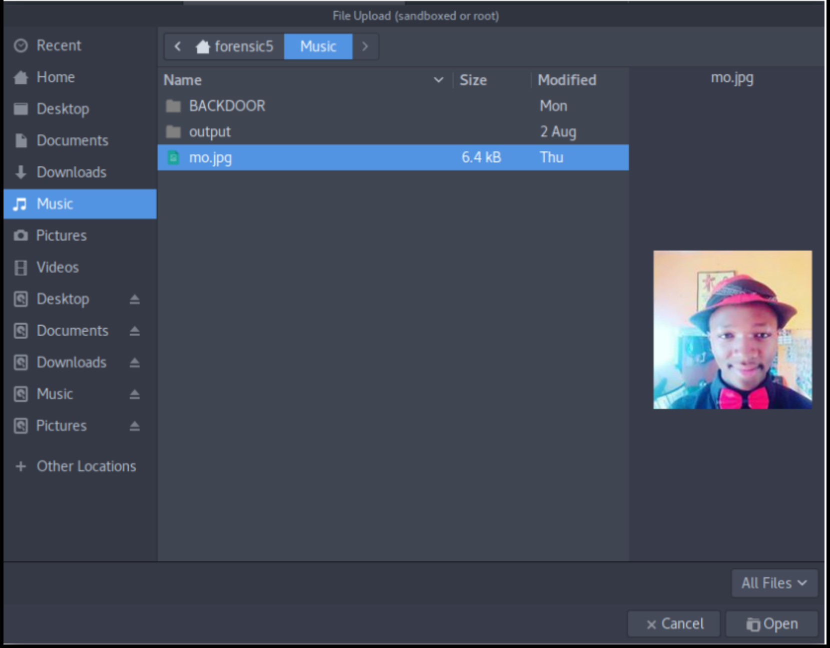
Vulnerability: SQL Injection

User ID:

Fig. 8.

If target Web page have any input forms as shown in the figure 8, input any data then submit.

➔ Upload image.



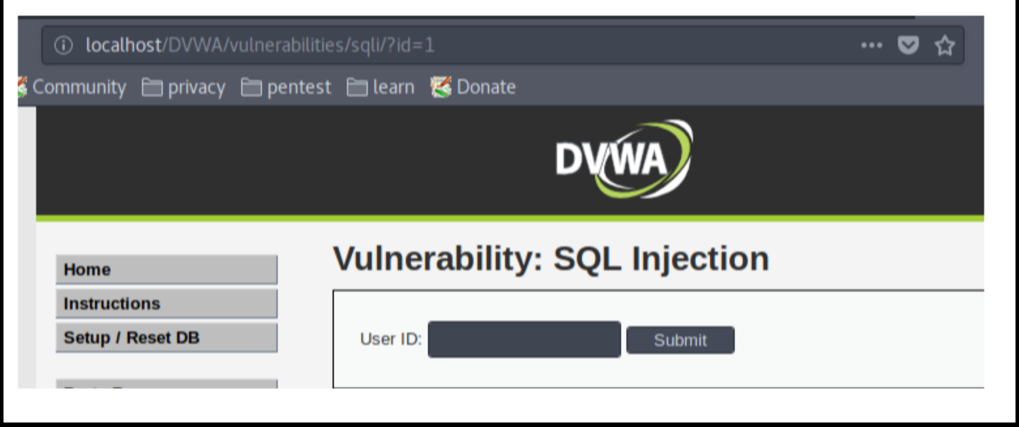
File Upload (sandboxed or root)

Name	Size	Modified
BACKDOOR		Mon
output		2 Aug
mo.jpg	6.4 kB	Thu

Fig. 9.

If web page got option to upload anything, just upload as shown in the figure 9, testing site had option which allow a client to upload images to the server.

➔ Checking all forms.



localhost/DVWA/vulnerabilities/sqli/?id=1

Vulnerability: SQL Injection

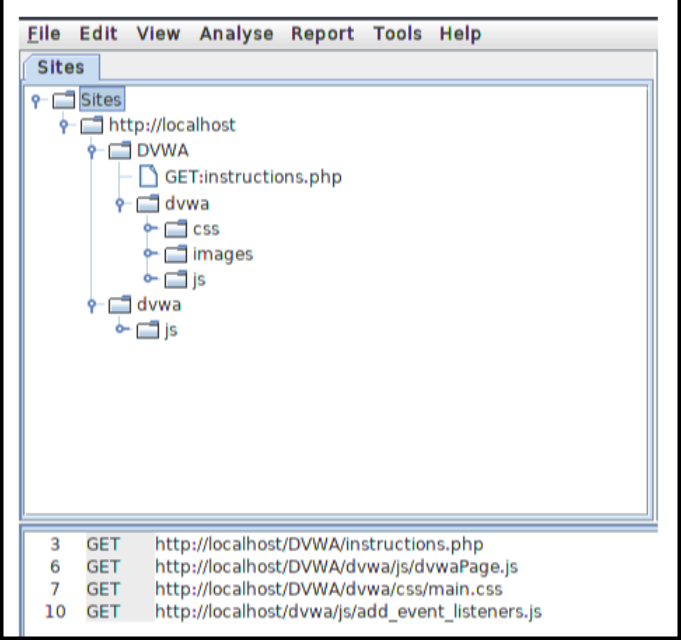
User ID:

Fig. 10.

If there is any form which looks similar with the form shown in the figure 10, fill it and submit the input data.

CHAPTER FOUR.

SCANNING VULNERABILITY.



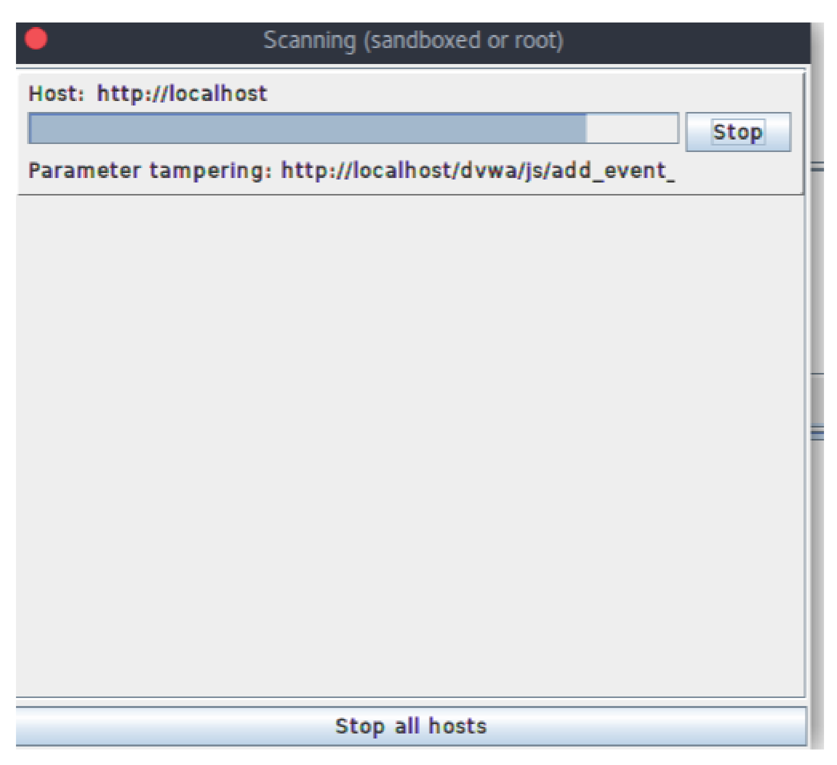
```
 3   GET   http://localhost/DVWA/instructions.php
 6   GET   http://localhost/DVWA/dvwa/js/dvwaPage.js
 7   GET   http://localhost/DVWA/dvwa/css/main.css
10   GET   http://localhost/dvwa/js/add_event_listeners.js
```

Fig. 11.

Target directory structure has been spidered and is displayed under sites button and shown in the figure 11, from 3 to 10, those are requests browsed on the browser. On the top of figure 11 there is option named Analyse, click on it then the following options will appear

- ➔ Spider.
- ➔ Scan All.
- ➔ Scan.
- ➔ Scan Policy.

According to options above you can choose to scan all or scan, after clicking on one of those two options new window come up on paros screen as shown in the figure.

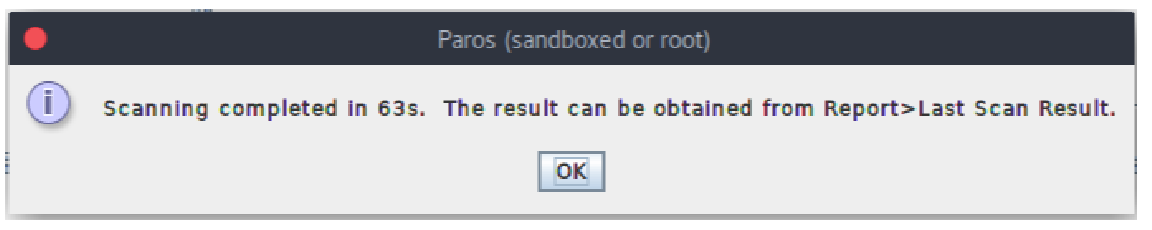


Host: http://localhost

Parameter tampering: http://localhost/dvwa/js/add_event_

Fig. 12.

scanning is finished. Figure 12 shows scanning is in progress.

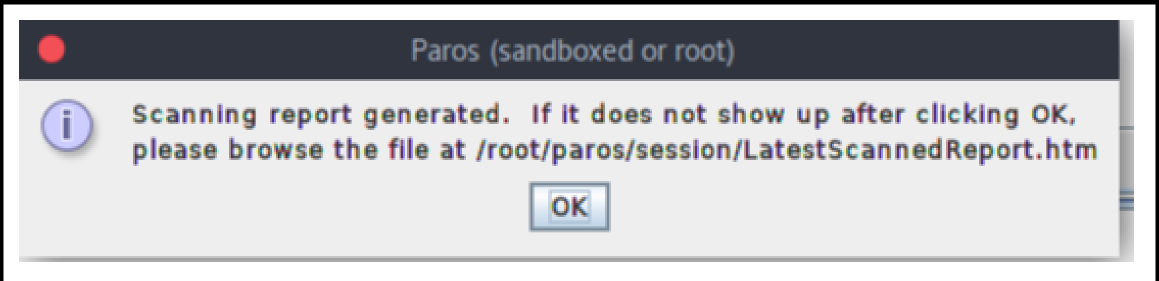


Scanning completed in 63s. The result can be obtained from Report>Last Scan Result.

Fig. 13.

Figure 12 shows the scanning is completed and results for scanning are found from Report>Last Scan

Result. If you go back in the figure 11 you will see option Report, click on that then you will see Last Scan Report, that is where your scan is saved.

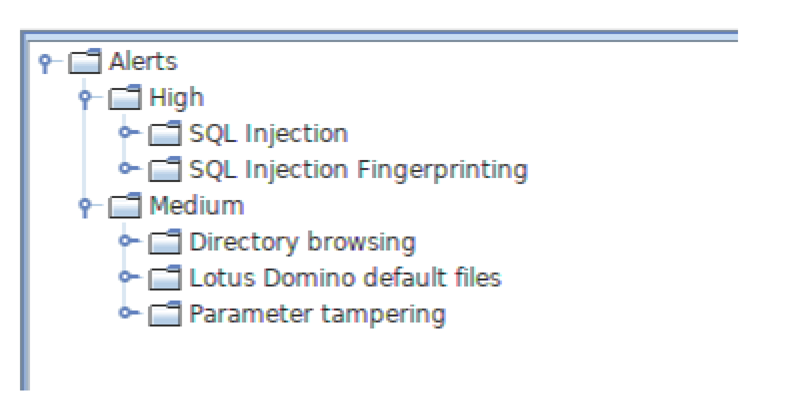


Scanning report generated. If it does not show up after clicking OK, please browse the file at /root/paros/session/LatestScannedReport.htm

Fig. 14.

For more analysis of scan results change directory to /root/paros/session/LatestScannedReport.htm as shown in the figure 14, that is the directory where all scanned results by paros are stored.

After scanning is completed you should be able to see scan result summary as shown in the figure.

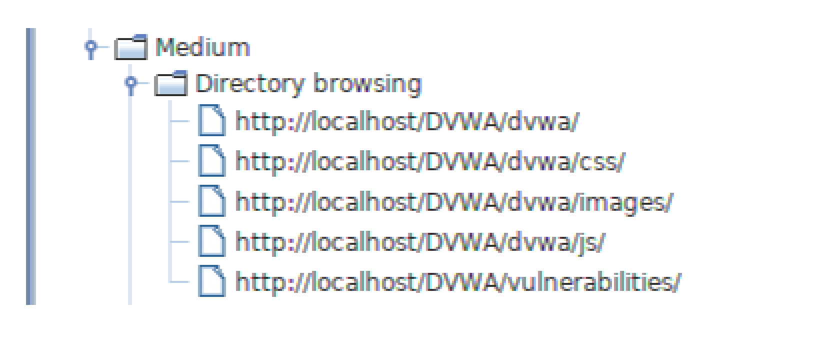


```
Alerts
  High
    SQL Injection
    SQL Injection Fingerprinting
  Medium
    Directory browsing
    Lotus Domino default files
    Parameter tampering
```

Fig. 15.

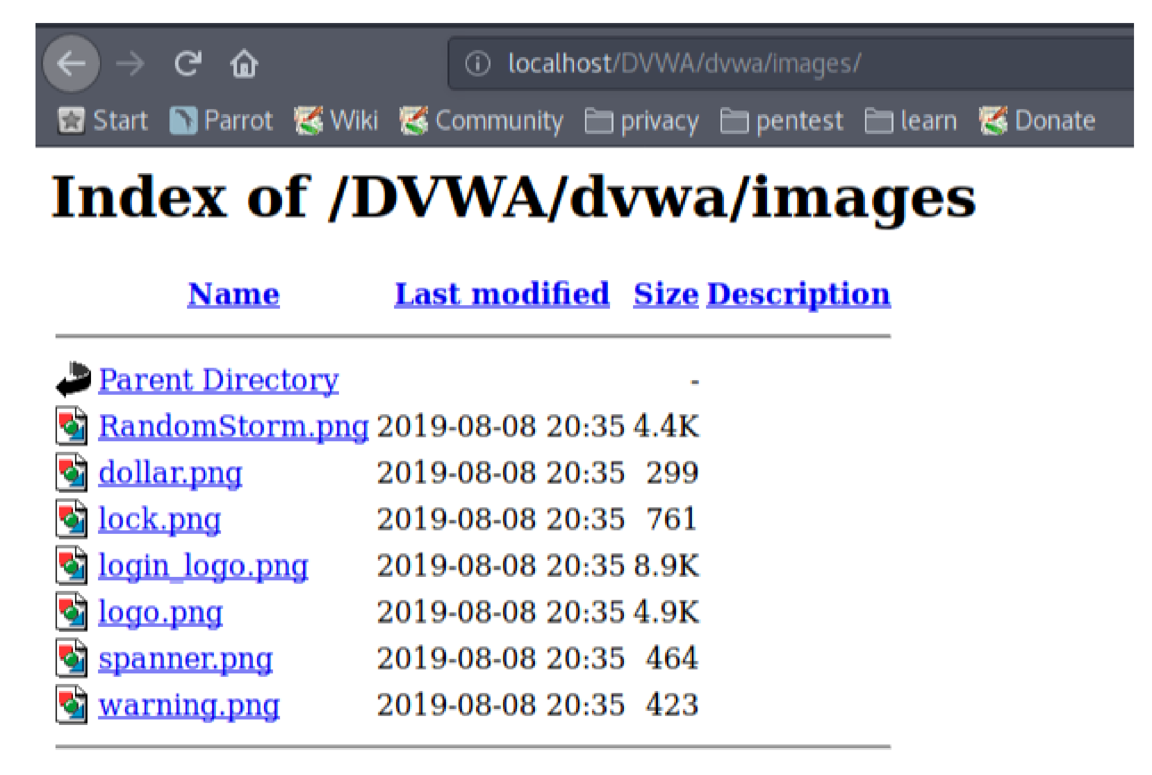
CHAPTER FIVE.

ANALYSIS OF SCAN RESULTS.



```
Medium
  Directory browsing
    http://localhost/DVWA/dvwa/
    http://localhost/DVWA/dvwa/css/
    http://localhost/DVWA/dvwa/images/
    http://localhost/DVWA/dvwa/js/
    http://localhost/DVWA/vulnerabilities/
```

Fig. 16.

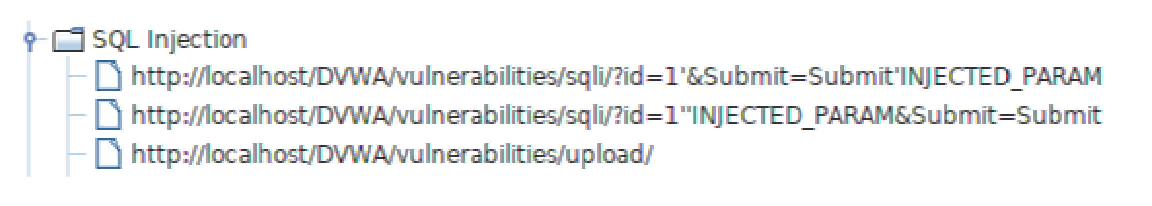


Index of /DVWA/dvwa/images

Name	Last modified	Size	Description
Parent Directory		-	
RandomStorm.png	2019-08-08 20:35	4.4K	
dollar.png	2019-08-08 20:35	299	
lock.png	2019-08-08 20:35	761	
login_logo.png	2019-08-08 20:35	8.9K	
logo.png	2019-08-08 20:35	4.9K	
spanner.png	2019-08-08 20:35	464	
warning.png	2019-08-08 20:35	423	

Fig. 17.

Site have directory browsing enabled as shown in the scan result in the figure 16 and how it looks like when pasted on the browser, this means black hacker can browse different folders and files in the server, and this can lead to leakage of sensitive information which is undesirable in security point of view. System administrators should be carefully in their configuration which should not allow black hackers to view these files.



```
SQL Injection
    http://localhost/DVWA/vulnerabilities/sqli/?id=1'&Submit=Submit'INJECTED_PARAM
    http://localhost/DVWA/vulnerabilities/sqli/?id=1"INJECTED_PARAM&Submit=Submit
    http://localhost/DVWA/vulnerabilities/upload/
```

CONCLUSION.

That is the end of this article about how to use paros scanner, thank you all for following this session untill the end, if you get any trouble contact us, but also if you have any issue let us know it, MoTech says you’re warm welcome for our services.

WAYS TO GET IN TOUCH WITH MoTech.

Linkedin.com

https://www.linkedin.com/in/motech-inc-720261191/

YouTube.com

https://www.youtube.com/channel/UCtuaigKZF3okQnKON5RM1qQ

Amazon.com

https://www.amazon.com/s?k=noel+moses+mwadende&ref=nb_sb_n oss

Github.com

https://github.com/MoTechStore/

Scribd.com

https://www.scribd.com/user/470459684/MoTech

SlideShare.com

https://www.slideshare.net/MoTechInc?utm_campaign=profiletracking&utm_medium=sssite&utm_source=ssslideview

REFERENCES.

1. https://tools.kali.org/web-applications/paros
2. https://null-byte.wonderhowto.com/forum/hiob-using-paros-for-web-application-auditing-and-debugging-0158950/
3. http://beginnerhack.blogspot.com/2013/08/paros-in-kali-linux.html
4. https://www.ehacking.net/2011/05/paros-proxy-web-application-security.html
5. https://sectools.org/tool/paros/