

Cyber security and Digital Forensics

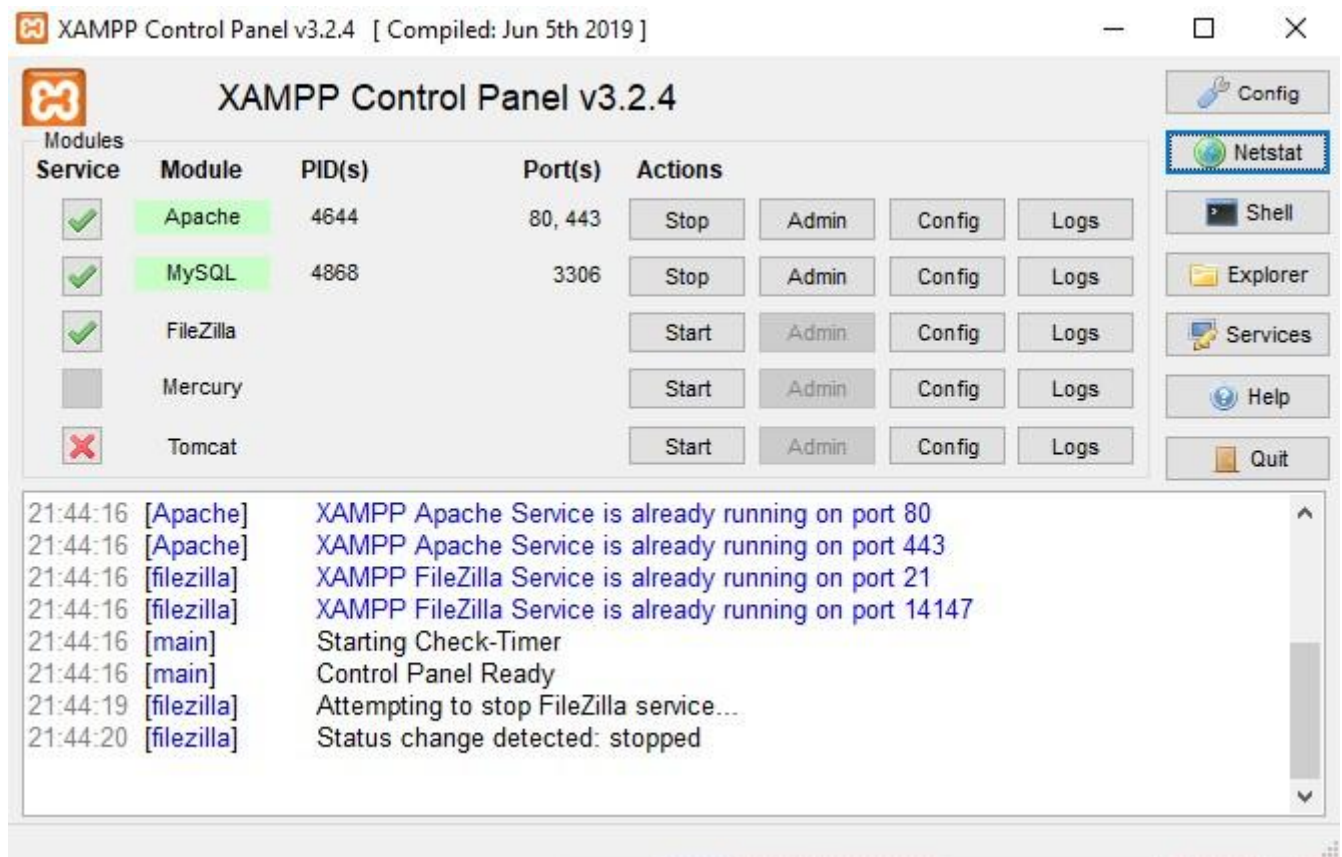
Practical 8: Security Misconfiguration

Tools required for the practical

- Mozilla Firefox Version 38.0.5.
- Burp Suite Community Suite.
- Owasp Mutillidae.

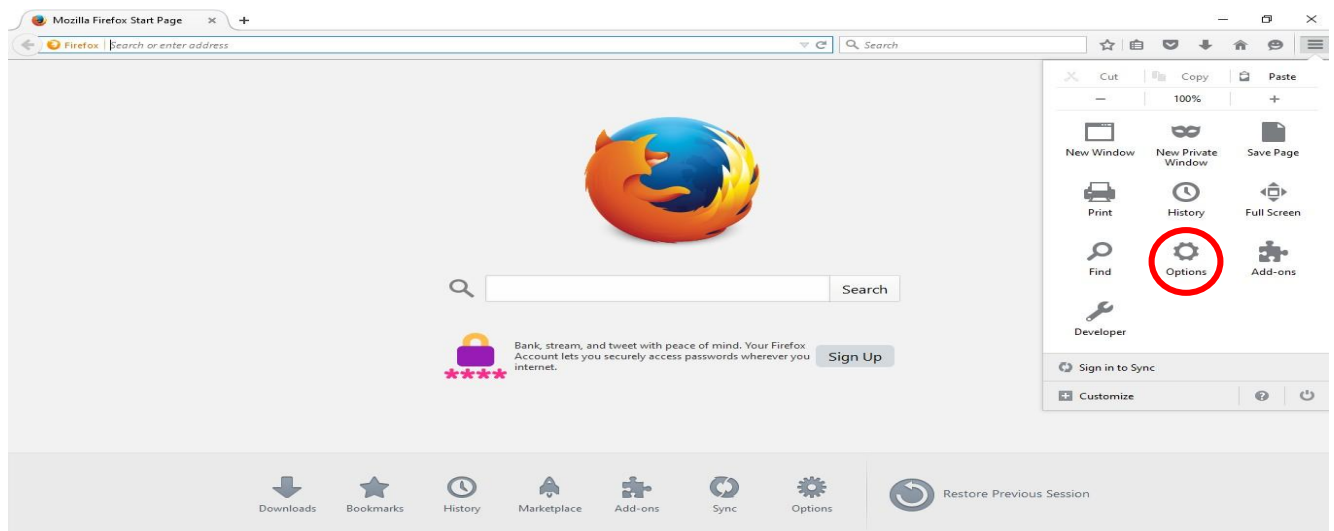
Steps :-

- Run **Xampp** ,make sure **Apache and MySQL** services are running.

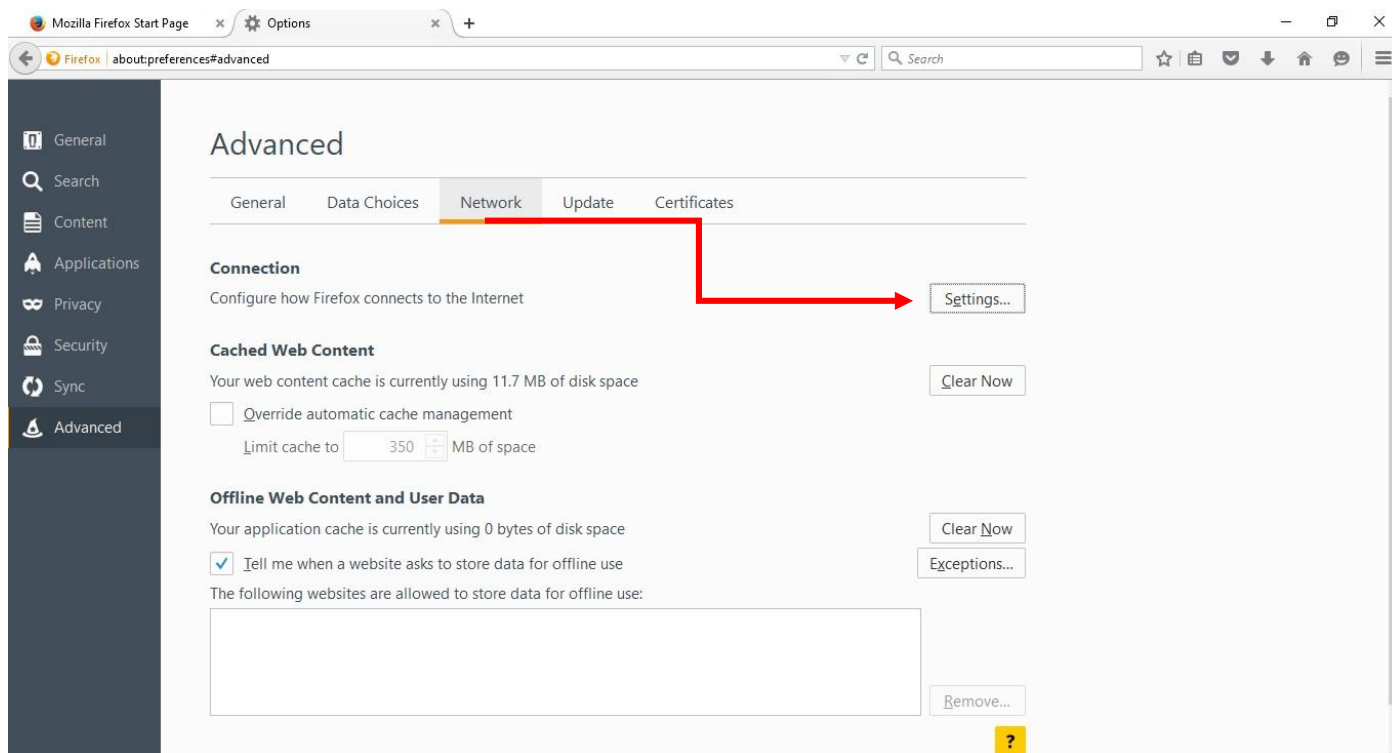


- Configure Firefox Network setting by assigning a manual proxy ,this will help browser to connect with Burp Suite tool.

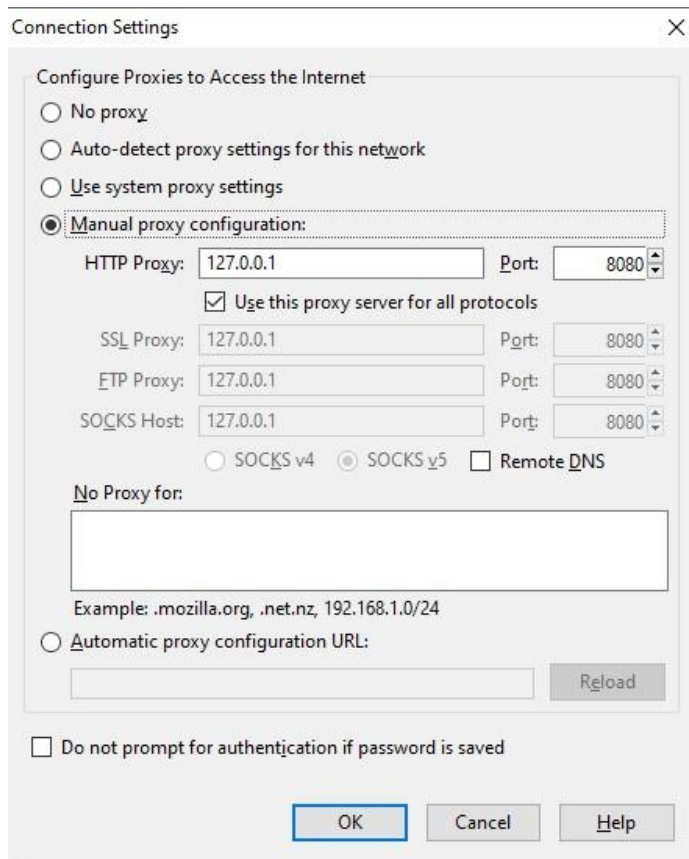
- Open Menu



B. Click on **Options** under **Advanced** tab select **Network** .



C. Open **Settings** besides **Connection**. Connection Setting Dialog will open ,select manual proxy configurations and set **Http proxy as 127.0.0.1** and **Port as 8080** .Check Use this proxy for all protocols.
Click ok to exit.



D. The proxy settings have been configured.

3. Open **Burp Suite tool**

a. The temporary project will be selected by default, click Next

Burp Suite Community Edition v2.1.02

?

Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

Temporary project

New project on disk

Name:

File:

Choose file...

Open existing project

Name	File
------	------

File:

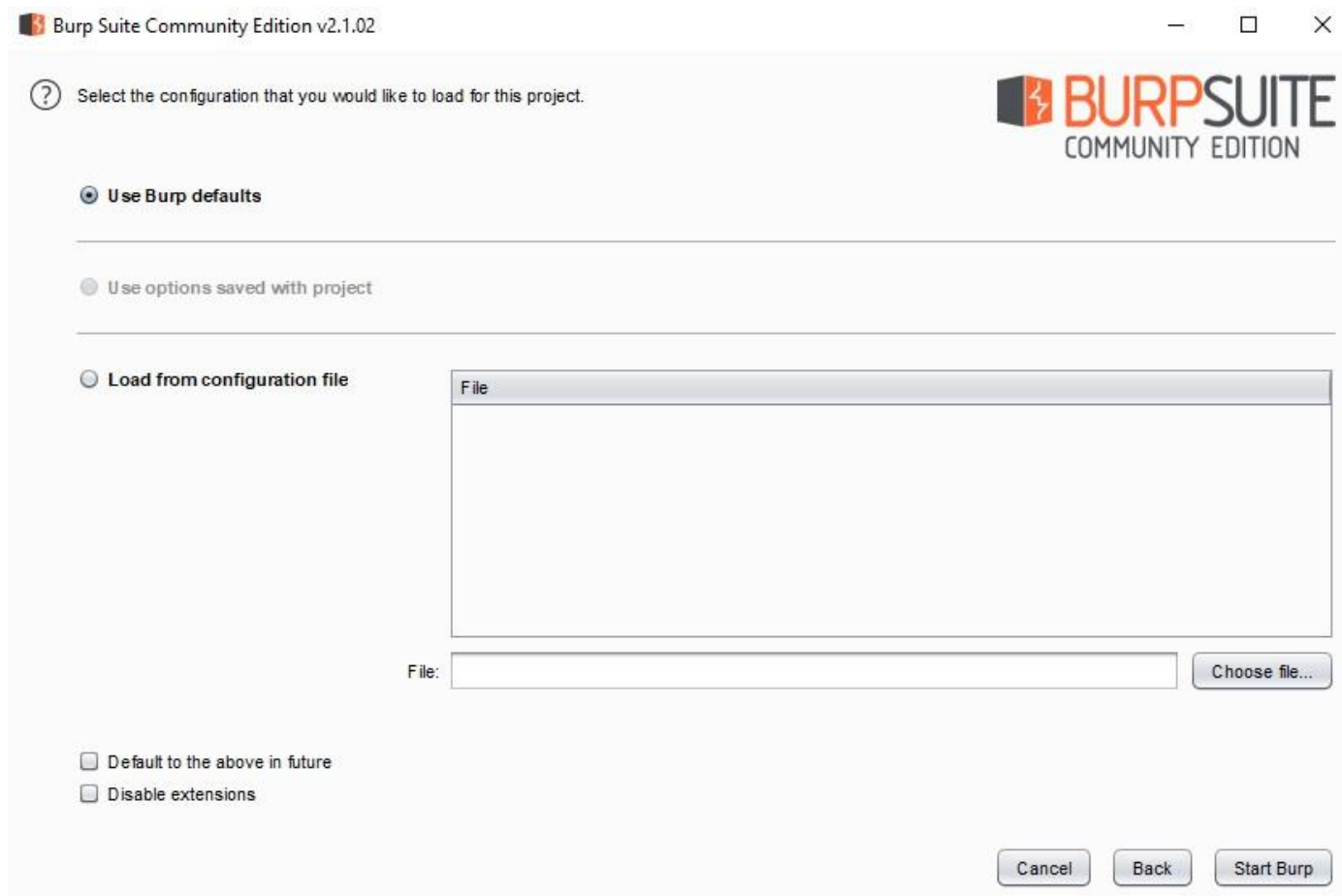
Choose file...

☒ Pause Automated Tasks

Cancel

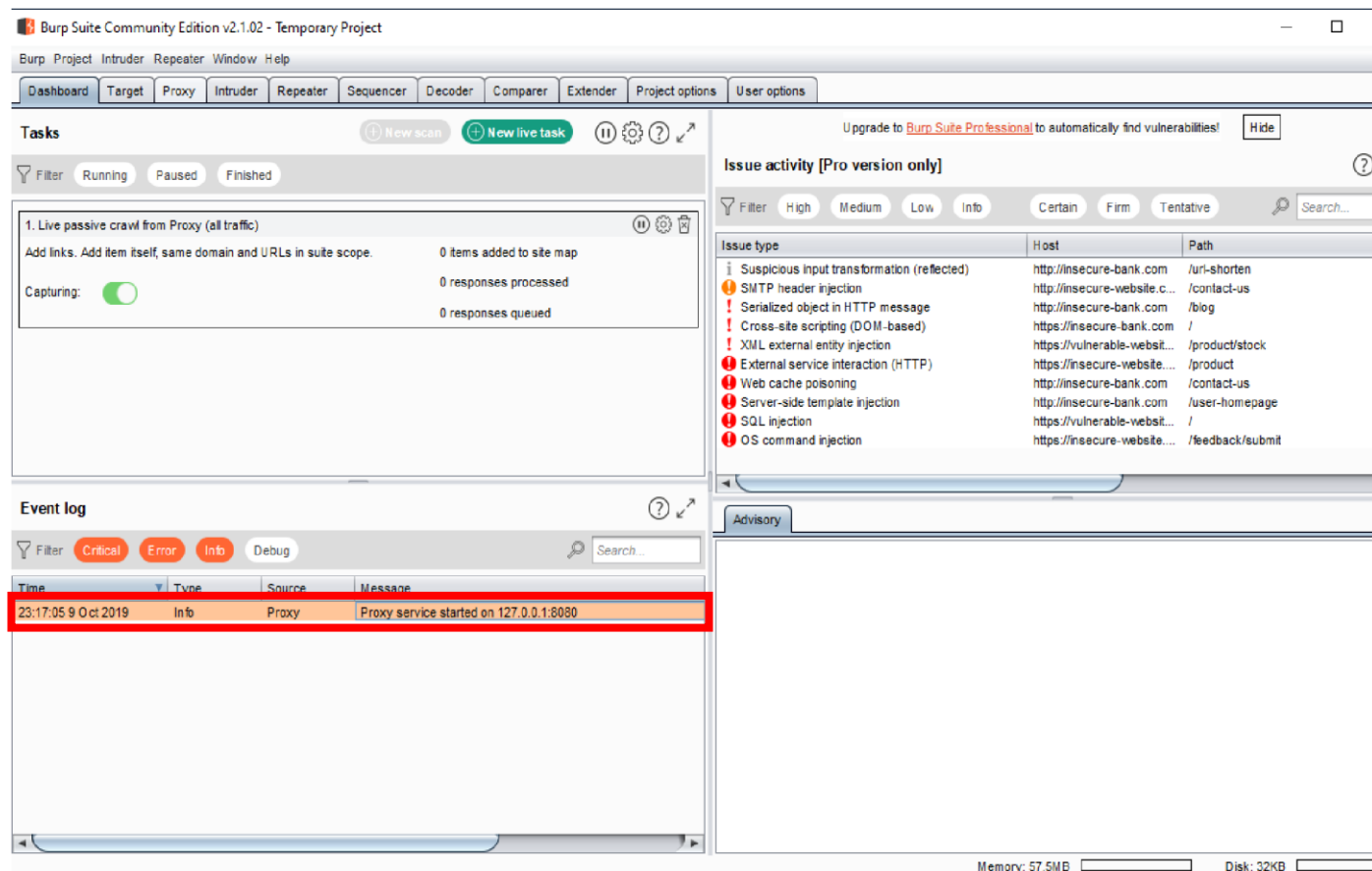
Next

b. In the next Window select Use Burp Default and Start Burp



c. Burp is now running. Check if the **Proxy service** has started correctly on the configured port in under the **Event Log** Tab.

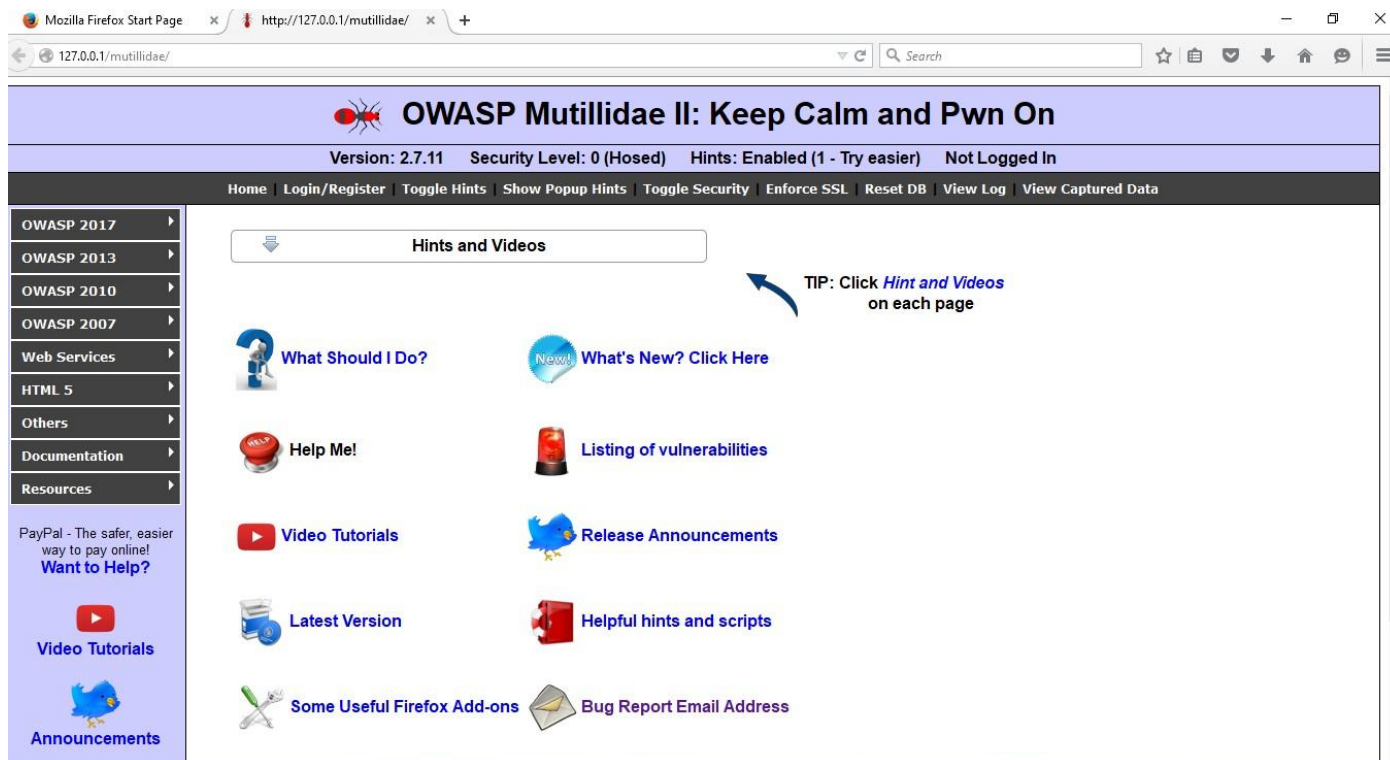
d. Minimize Burp Suite now open Firefox



4. Run **OWASP mutillidae** using Xampp on localhost (localhost address <http://127.0.0.1/mutillidae/>).

Browser version should be **Firefox 38.0.5**

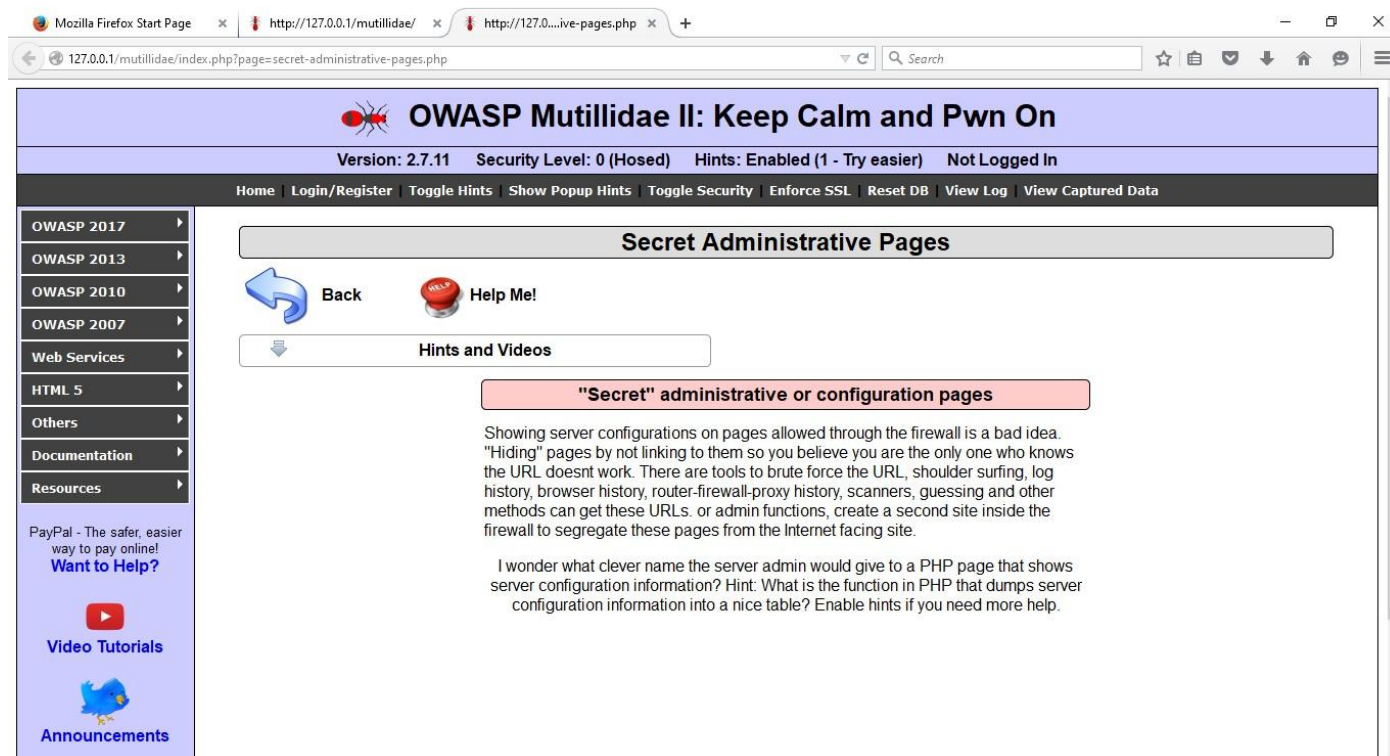
5. In a new tab , Type the following Url



(<http://127.0.0.1/mutillidae/index.php?page=secret-administrative-pages.php>) in address

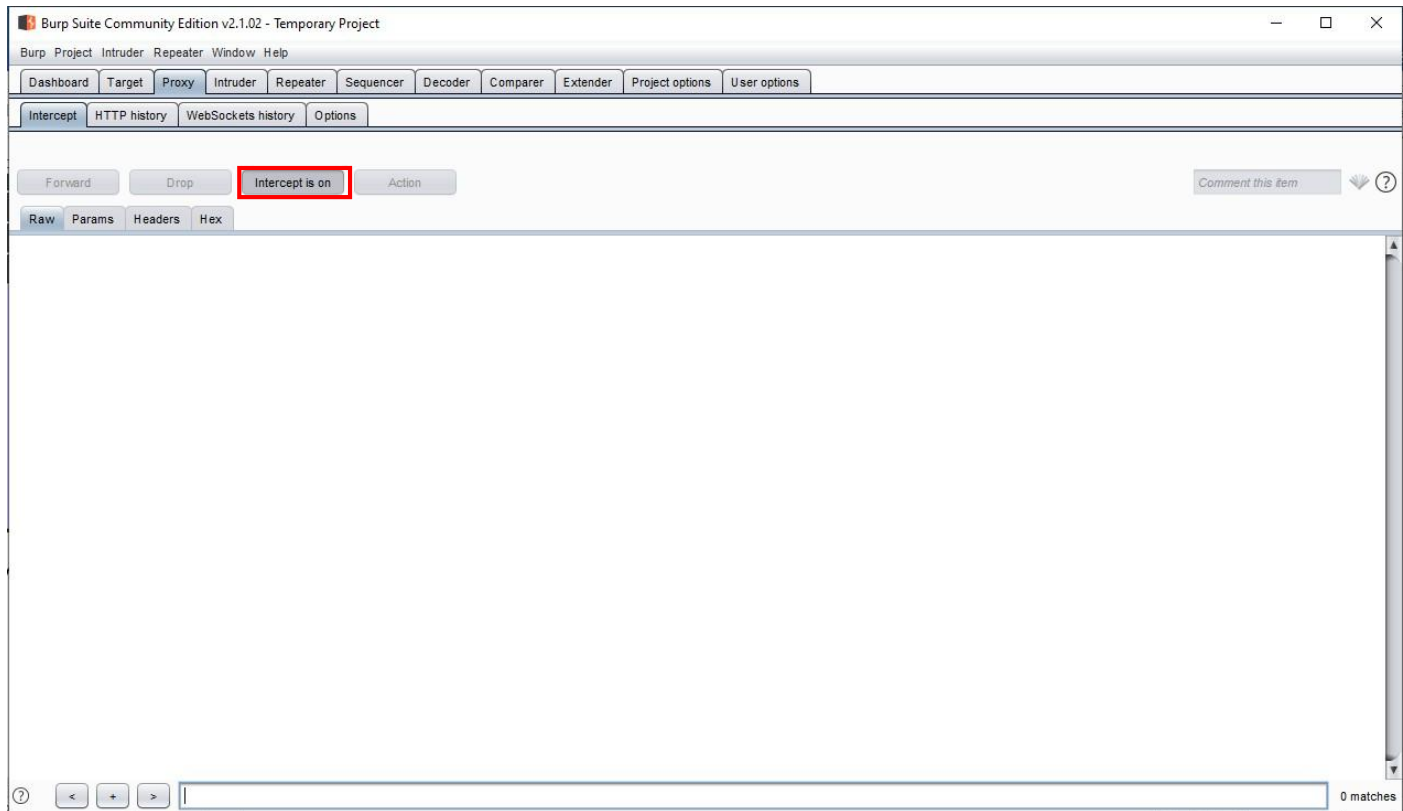
bar.

6. Minimize Firefox and Open Burp Suite again.



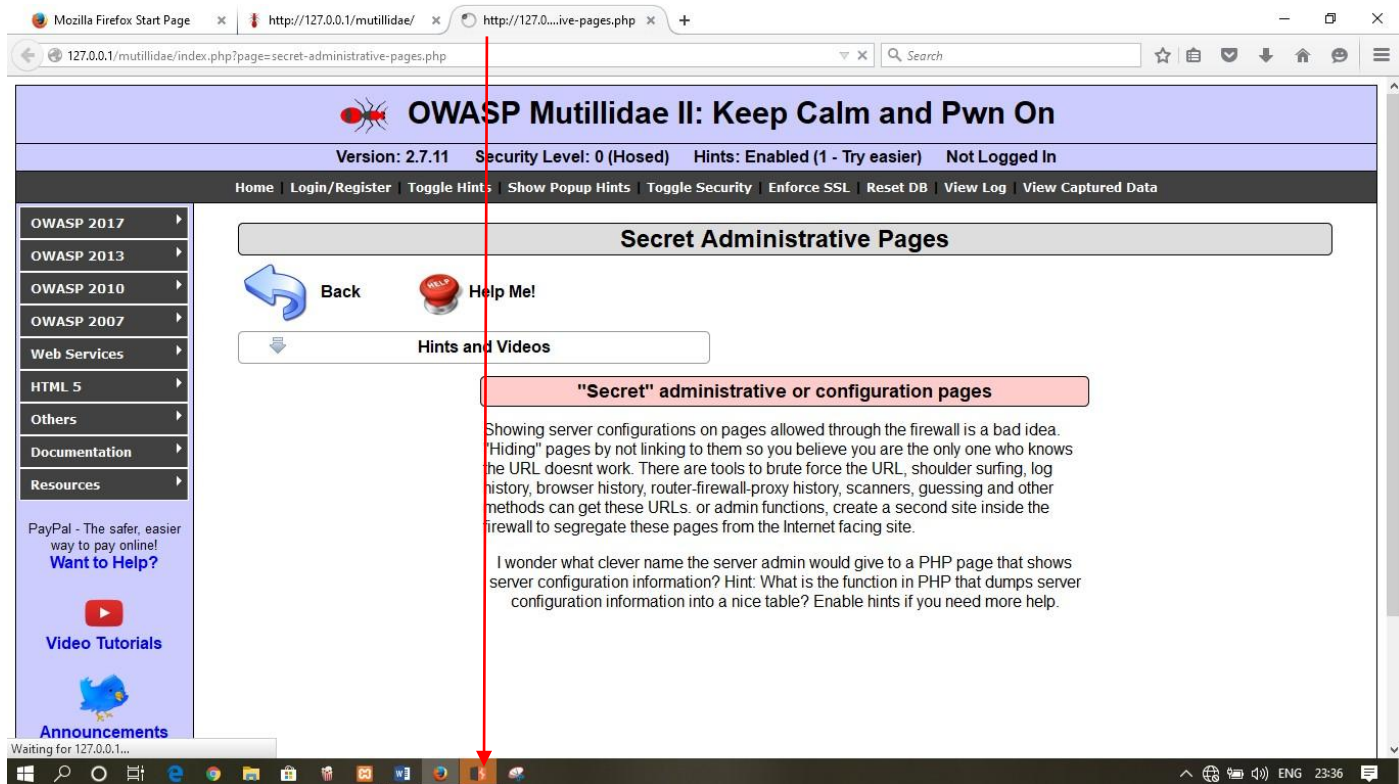
7. Under Proxy tab turn on the intercept if it is off (By turning on the interceptor burp suite will be able to intercept all the requests through the firefox browser)

8. Open Firefox **refresh** the url open in new tab, Burp suite will intercept it and will

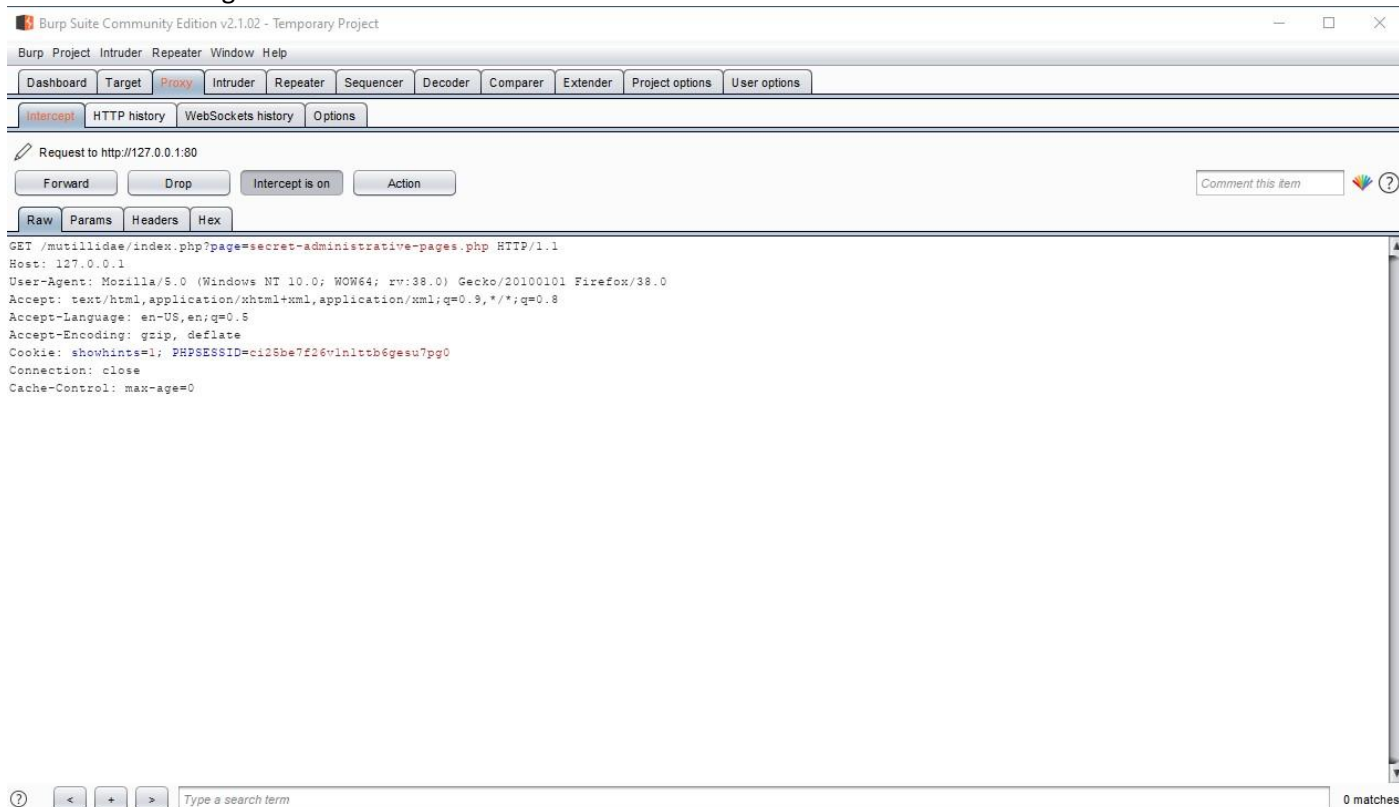


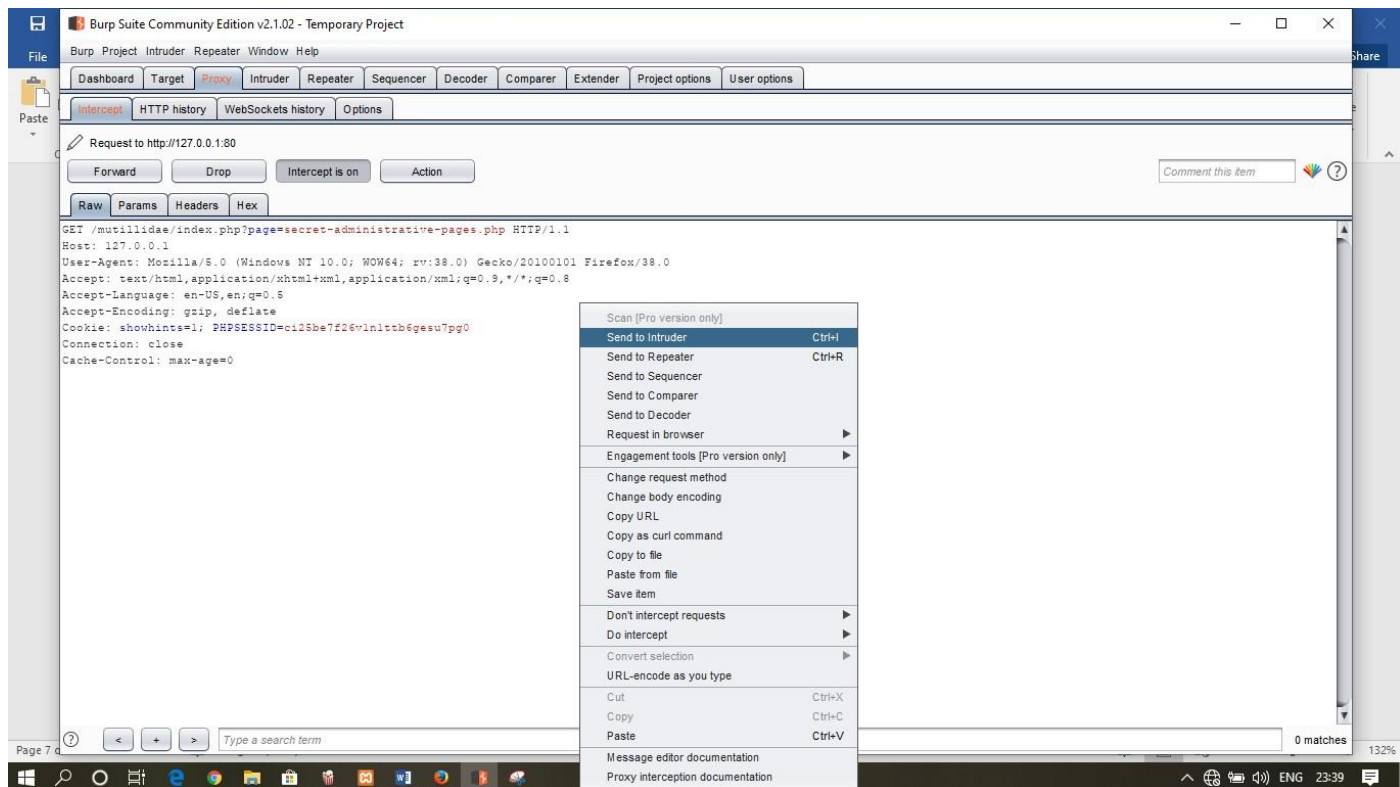
start blinking in the taskbar.

9. This will be the following output in burp Suite

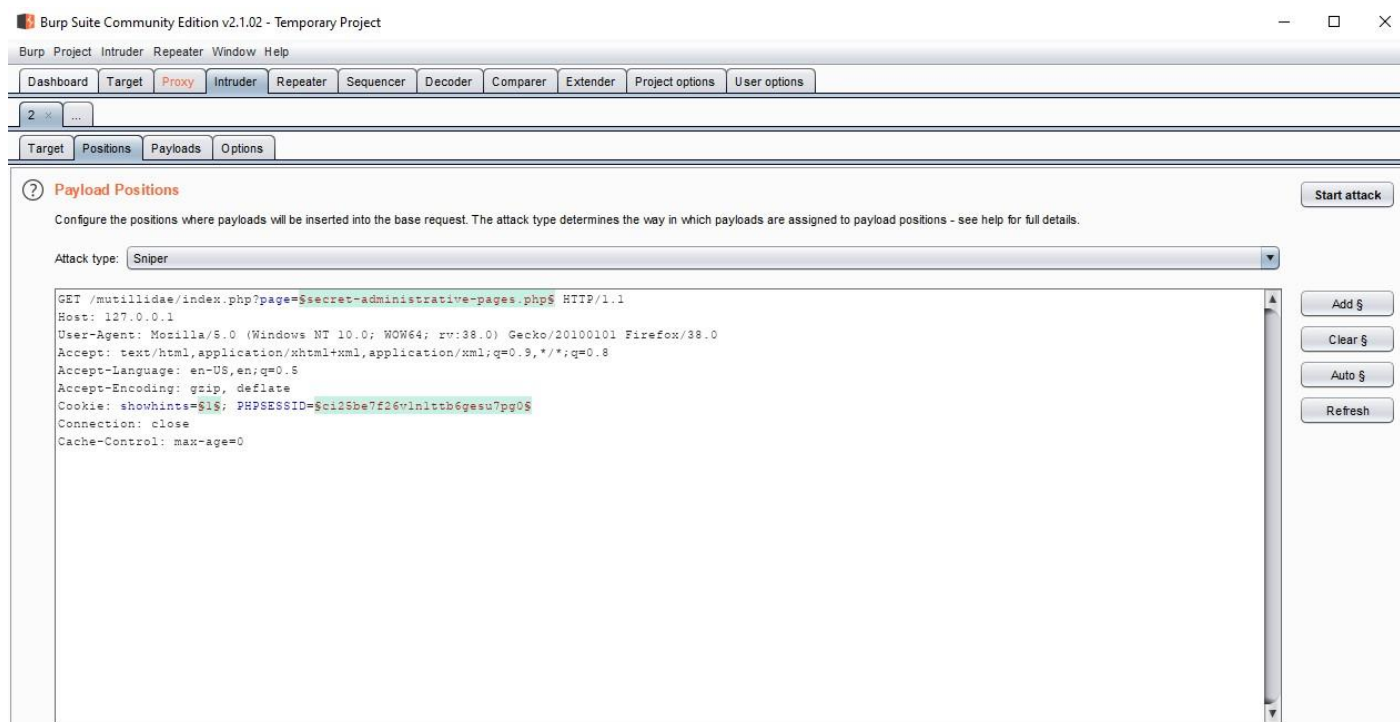


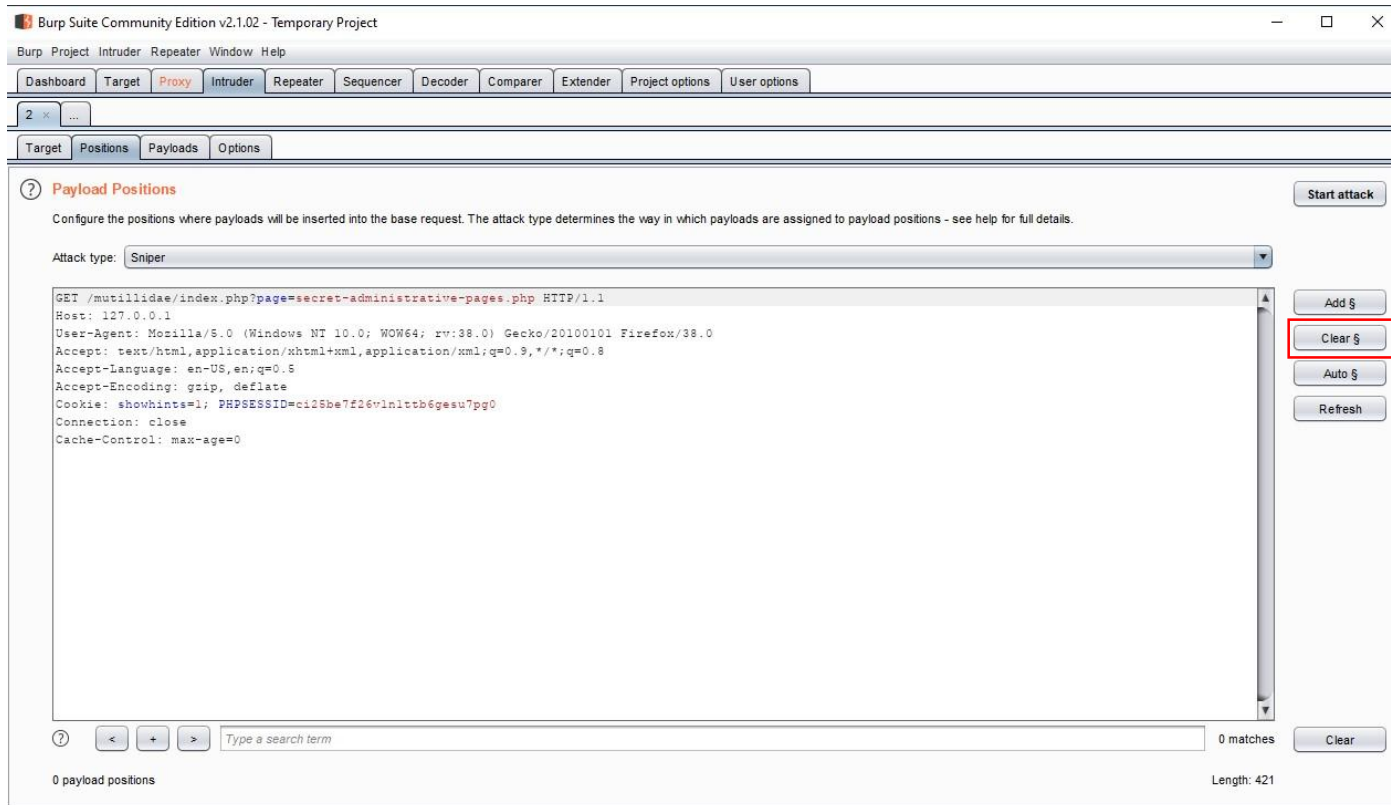
10. Right Click in the window and select Send to intruder.





11. Under Intruder tab Select Positions Click on Clear .





12. Select the highlighted path then click Add.

Burp Suite Community Edition v2.1.02 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

2 x ...

Target Positions **Payloads** Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /mutillidae/index.php?page=secret-administrative-pages.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=1; PHPSESSID=c125be7f26vlnlttb6gesu7pg0
Connection: close
Cache-Control: max-age=0
```

0 payload positions

Length: 421

Start attack

Add \$

Clear \$

Auto \$

Refresh

0 matches

Clear

Burp Suite Community Edition v2.1.02 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Sequencer Decoder Comparer Extender Project options User options

2 x ...

Target Positions **Payloads** Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /mutillidae/index.php?page=$secret-administrative-pages.php$ HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=1; PHPSESSID=c125be7f26vlnlttb6gesu7pg0
Connection: close
Cache-Control: max-age=0
```

0 payload positions

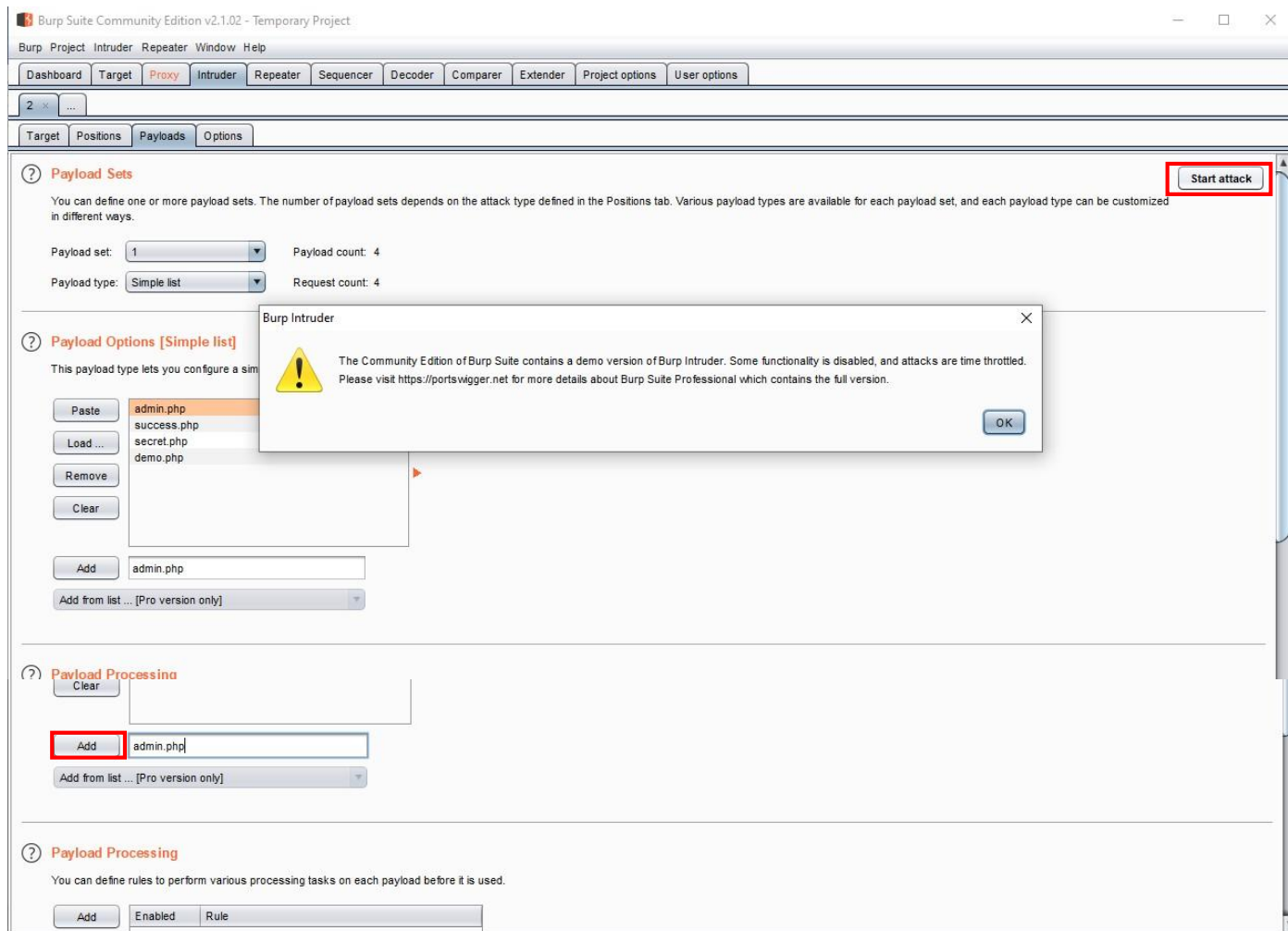
Start attack

Add \$

Clear \$

Auto \$

Refresh



13. Under Payloads → Payload options add 4 Php files(admin.php,success.php,secret.php,demo.php) not necessarily inserted in the same order.

14. Now click on start attack .Warning occurs everytime we carry attack Click OK to continue.

15. After the attack has Finished **Intruder attack** windows will open

Intruder attack 1

Attack Save Columns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	50722	
1	admin.php	200	<input type="checkbox"/>	<input type="checkbox"/>	141636	
2	success.php	200	<input type="checkbox"/>	<input type="checkbox"/>	45690	
3	secret.php	200	<input type="checkbox"/>	<input type="checkbox"/>	141644	
4	demo.php	200	<input type="checkbox"/>	<input type="checkbox"/>	45672	

Finished

16. Render the php to get secret info from the webpage. Select any one of the php files to render. Under response tab select Render and then click on render.

The screenshot shows the 'Intruder attack 1' window in Burp Suite. The 'Results' tab is active, displaying a table of requests. A red arrow points from the 'admin.php' entry in the table to the 'Response' tab. In the 'Response' tab, the 'Render' button is highlighted, and another red arrow points from it to a 'Click to render page' button.

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	50722	
1	admin.php	200	<input type="checkbox"/>	<input type="checkbox"/>	141636	
2	success.php	200	<input type="checkbox"/>	<input type="checkbox"/>	45690	
3	secret.php	200	<input type="checkbox"/>	<input type="checkbox"/>	141644	
4	demo.php	200	<input type="checkbox"/>	<input type="checkbox"/>	45672	

Request Response

Raw Headers Hex HTML Render

Click to render page

Finished

17. A new window will open displaying the hidden info only known to privileged users on the webpage.

Burp Suite Response Renderer

**OWASP Mutillidae II: Keep Calm and Pwn On**

Version: 2.7.11 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In

Home | Login/Register | Toggle Hints | Show Popup Hints | Toggle Security | Enforce SSL | Reset DB | View Log | View Captured Data

OWASP 2017

OWASP 2013

OWASP 2010

OWASP 2007

Web Services

HTML 5

Others

Documentation

Resources

PayPal - The safer, easier way to pay online!

Want to Help?


Video Tutorials

Announcements

Secret PHP Server Configuration Page

 Back  Help Me!

PHP Version 7.1.32



System	Windows NT DELL 10.0 build 18362 (Windows 10) AMD64
Build Date	Aug 28 2019 09:04:05
Compiler	MSVC14 (Visual C++ 2015)
Architecture	x64
Configure Command	cscrip /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\v64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\v64\instantclient_12_1\sdk,shared" "--enable-object-out-dir=../obj/" "--enable-com-dotnet=shared" "--with-mcrypt=static" "--without-analyzer" "--with-pgo"
Server API	Apache 2.0 Handler
Virtual Directory Support	enabled
Configuration File (php.ini) Path	C:\WINDOWS
Loaded Configuration File	C:\xampp\php\php.ini
Scan this dir for additional .ini files	(none)
Additional .ini files parsed	(none)
PHP API	20160303
PHP Extension	20160303