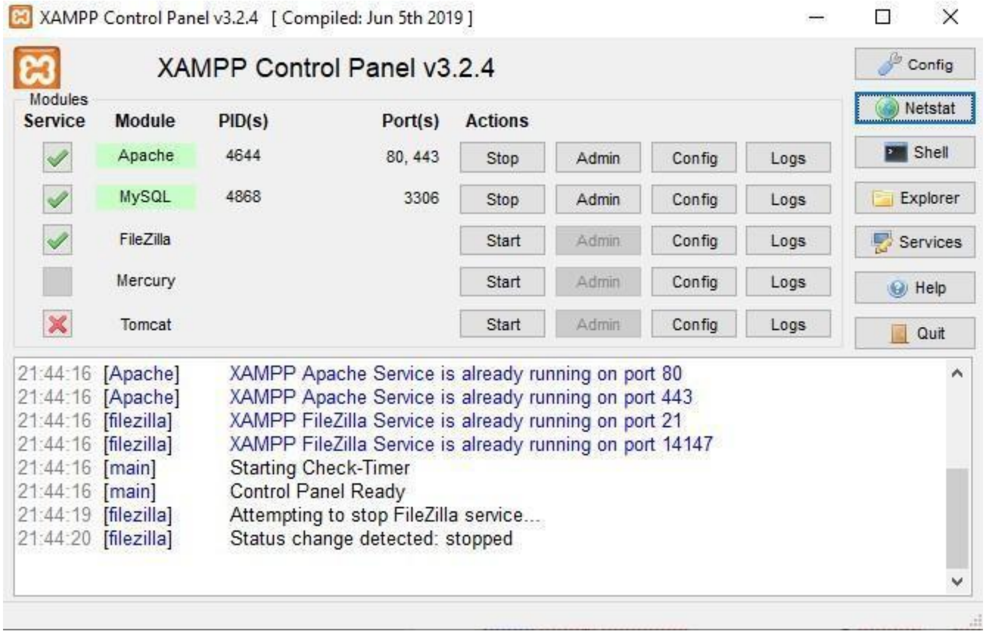
Practical 8: Security Misconfiguration

Tools required for the practical

1. Mozilla Firefox Version 38.0.5.
2. Burp Suite Community Suite.
3. Owasp Mutillidae.

Steps :-

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



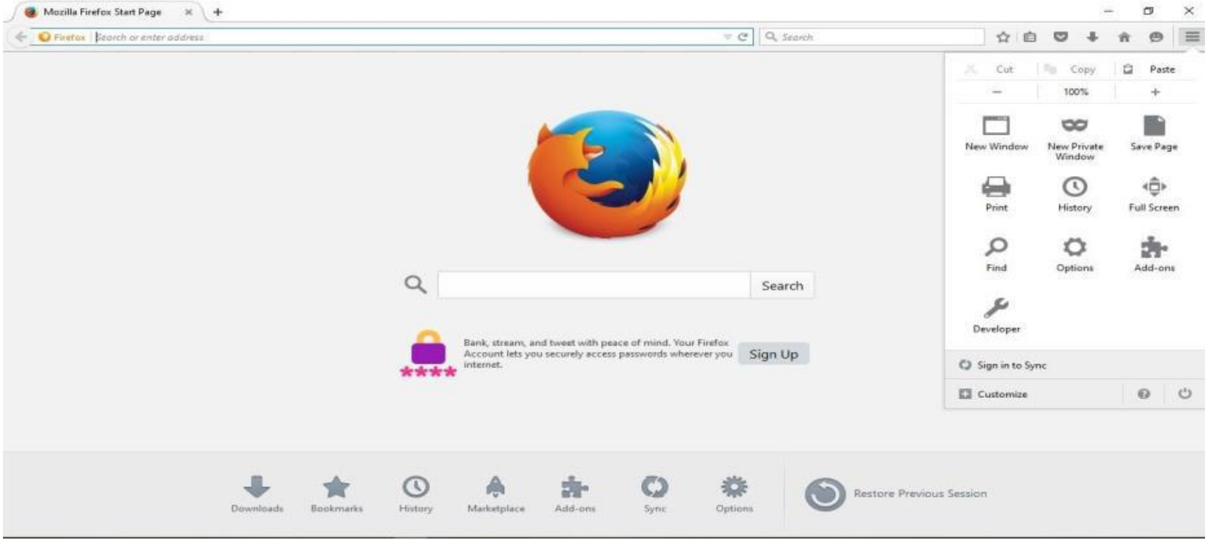
XAMPP Control Panel v3.2.4 [Compiled: Jun 5th 2019]

XAMPP Control Panel v3.2.4

Service	Module	PID(s)	Port(s)	Actions			
✓	Apache	4644	80, 443	Stop	Admin	Config	Logs
✓	MySQL	4868	3306	Stop	Admin	Config	Logs
✓	FileZilla			Start	Admin	Config	Logs
	Mercury			Start	Admin	Config	Logs
✗	Tomcat			Start	Admin	Config	Logs

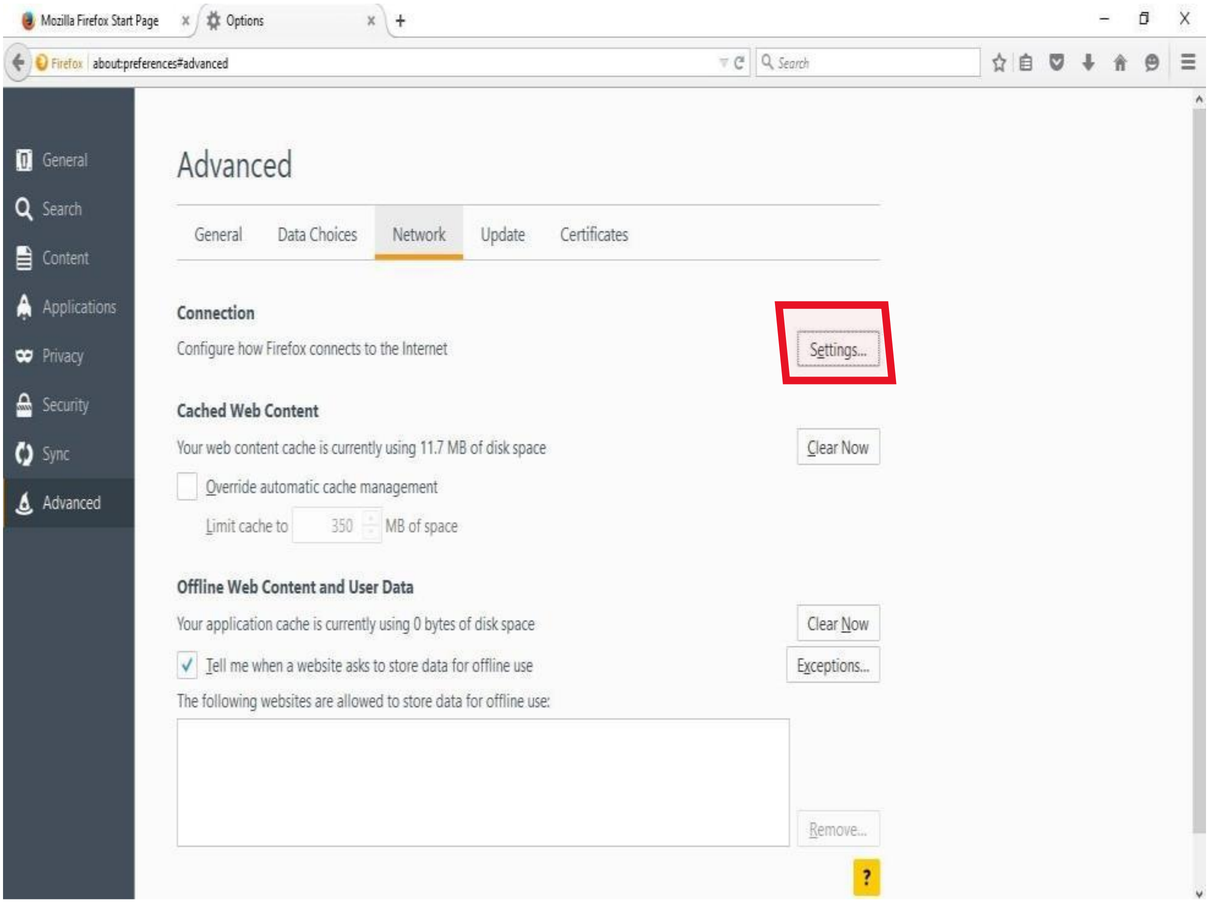
```
21:44:16  [Apache]     XAMPP Apache Service is already running on port 80
21:44:16  [Apache]     XAMPP Apache Service is already running on port 443
21:44:16  [filezilla]  XAMPP FileZilla Service is already running on port 21
21:44:16  [filezilla]  XAMPP FileZilla Service is already running on port 14147
21:44:16  [main]       Starting Check-Timer
21:44:16  [main]       Control Panel Ready
21:44:19  [filezilla]  Attempting to stop FileZilla service...
21:44:20  [filezilla]  Status change detected: stopped
```

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



Bank, stream, and tweet with peace of mind. Your Firefox Account lets you securely access passwords wherever you internet.

Click on **Options** Under **Advanced** Tab Select Network



Mozilla Firefox Start Page | Options

about:preferences#advanced

General
Search
Content
Applications
Privacy
Security
Sync
Advanced

Advanced

General | Data Choices | Network | Update | Certificates

Connection

Configure how Firefox connects to the Internet [Settings...]

Cached Web Content

Your web content cache is currently using 11.7 MB of disk space [Clear Now]

□ Override automatic cache management

Limit cache to 350 MB of space

Offline Web Content and User Data

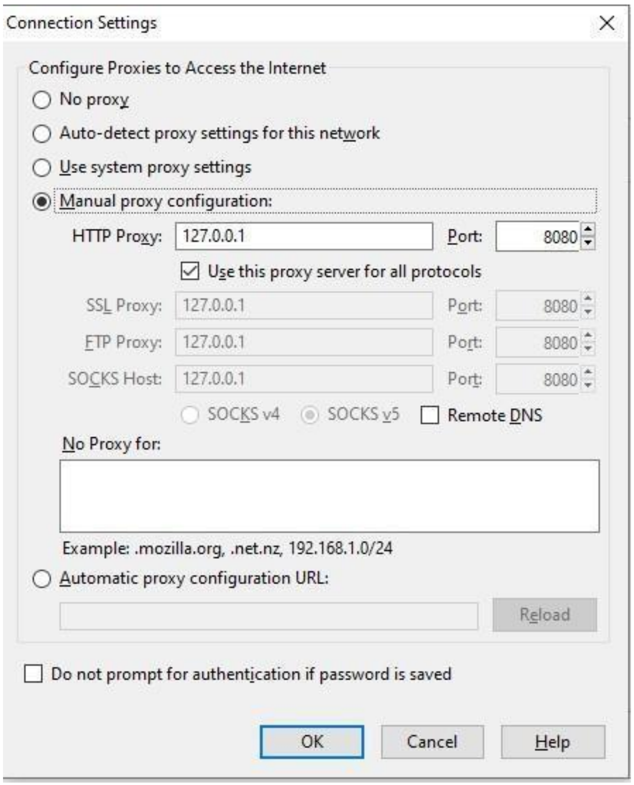
Your application cache is currently using 0 bytes of disk space [Clear Now]

☑ Tell me when a website asks to store data for offline use [Exceptions...]

The following websites are allowed to store data for offline use:

[Remove...]

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.



Connection Settings

Configure Proxies to Access 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

○ SOCKS v4 ● SOCKS v5 □ Remote DNS

No Proxy for:

Example: .mozilla.org, .net.nz, 192.168.1.0/24

○ Automatic proxy configuration URL:

[Reload]

□ Do not prompt for authentication if password is saved

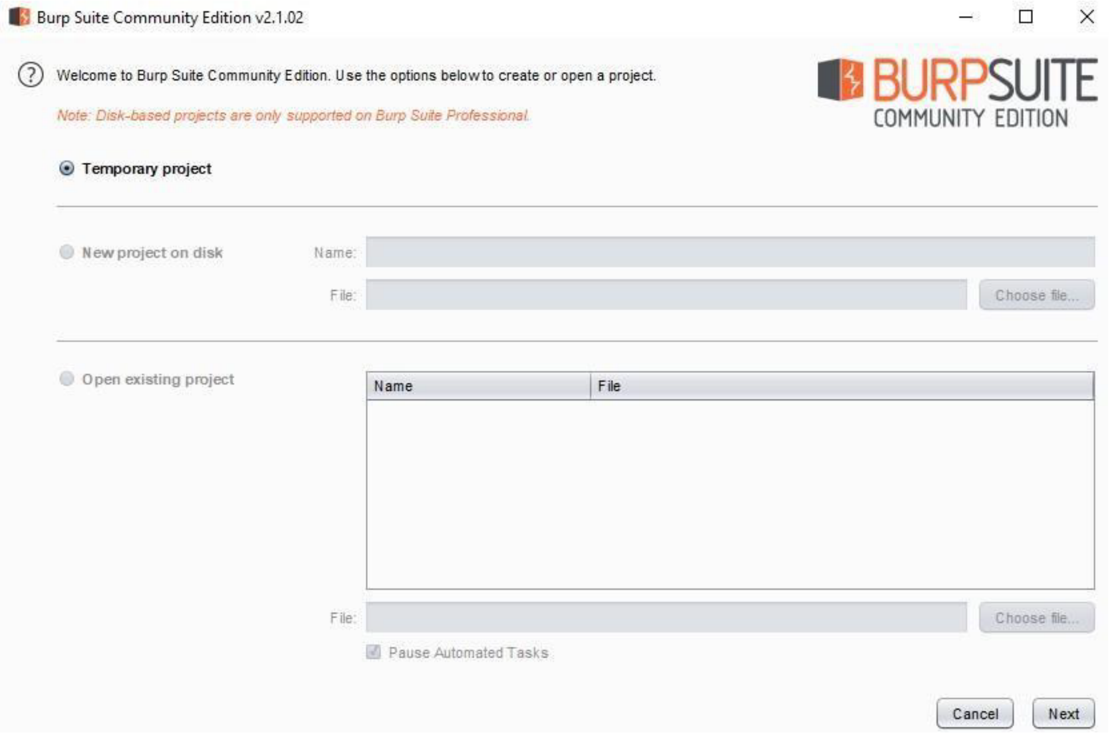
[OK] [Cancel] [Help]

The proxy settings have been configured.

3. Open **Burp Suite tool**

The temporary project will be selected by default, click Next

F-006



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...

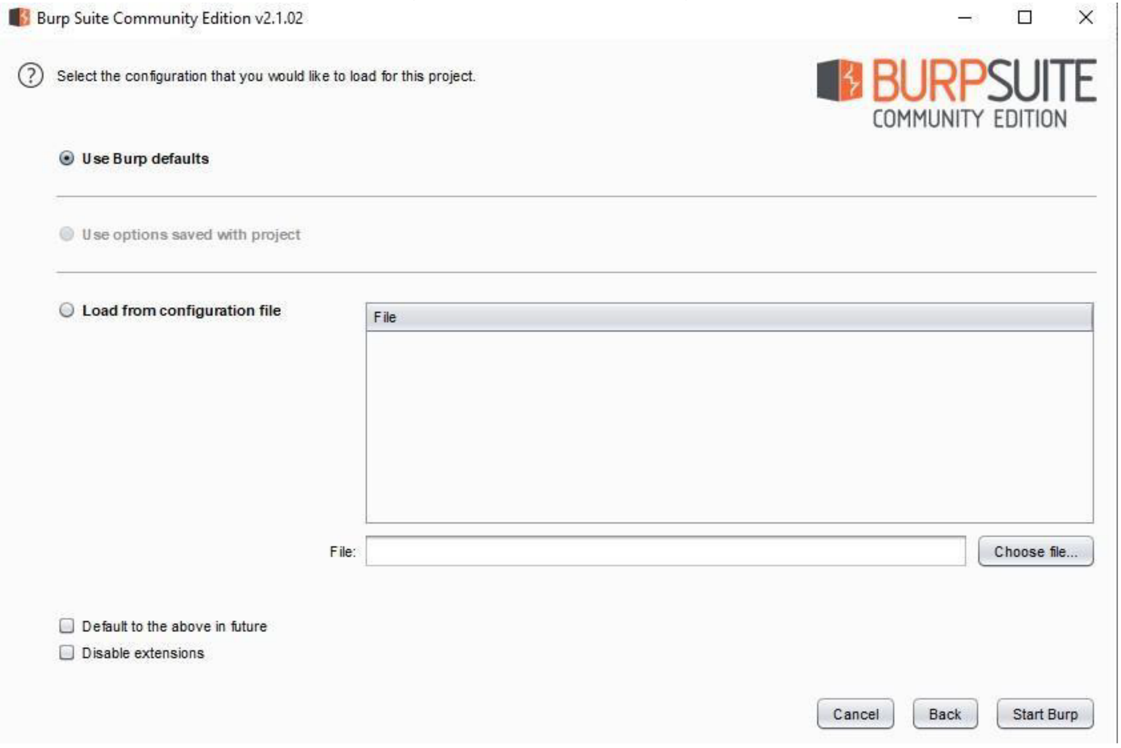
○ Open existing project

Name	File

File: Choose file...

☑ Pause Automated Tasks

In the next Window select Use Burp Default and Start Burp



Burp Suite Community Edition v2.1.02

Select the configuration that you would like to load for this project.

● Use Burp defaults

○ Use options saved with project

○ Load from configuration file

File

File: Choose file...

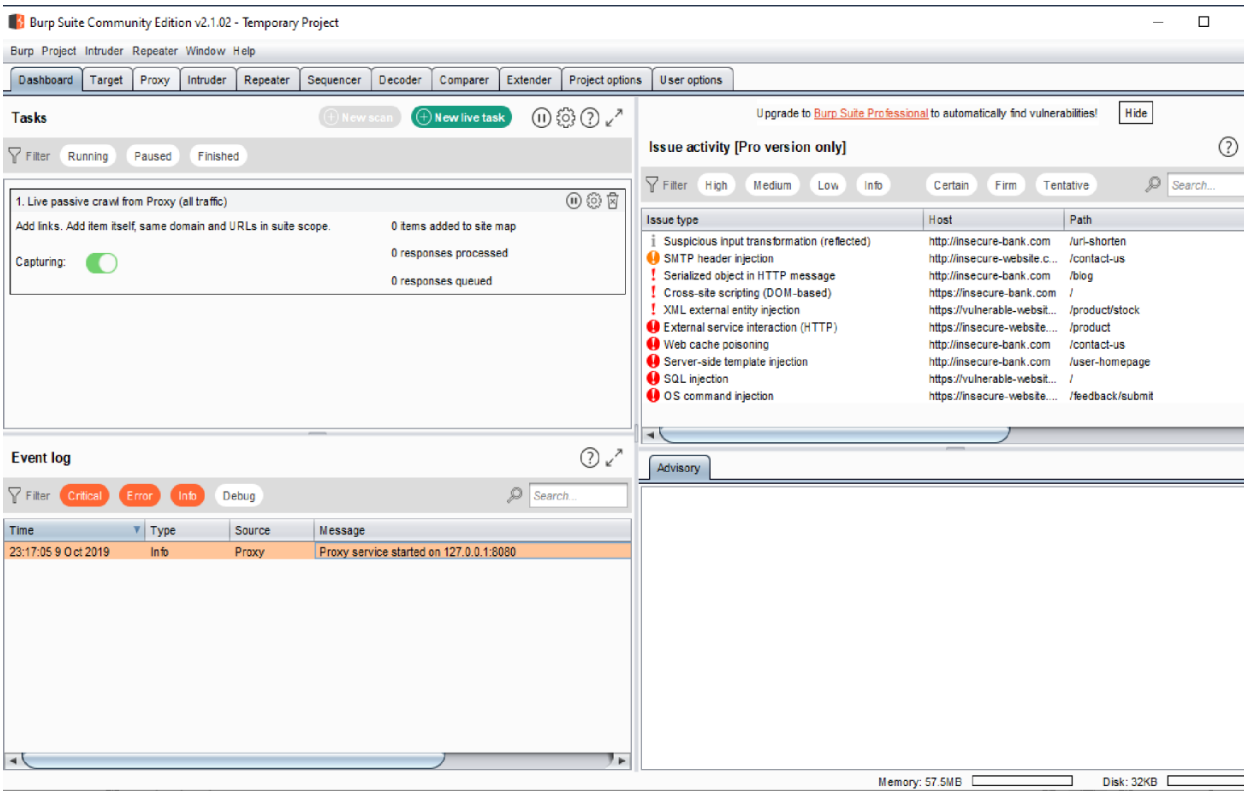
□ Default to the above in future

□ Disable extensions

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

Minimize Burp Suite now open Firefox

F-006



Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
Upgrade to Burp Suite Professional to automatically find vulnerabilities!
Hide
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Tentative
Search...
Event log
Filter Critical Error Info Debug
Search...
Advisory
Memory: 57.5MB
Disk: 32KB

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope.

Capturing:

0 items added to site map

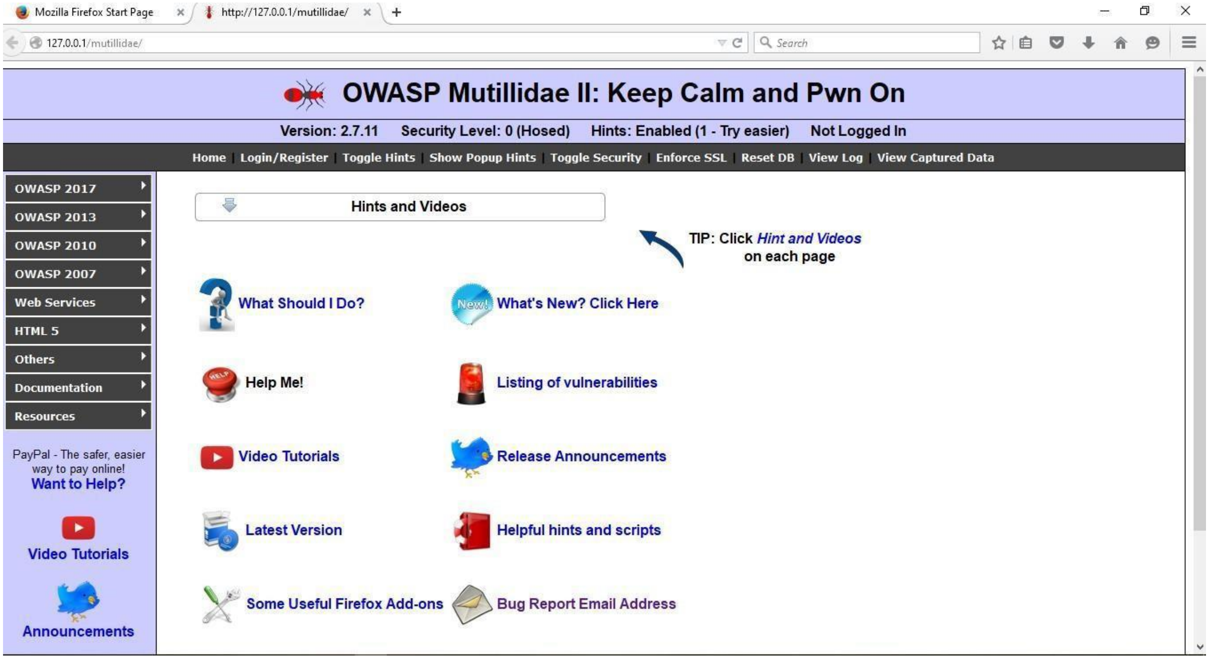
0 responses processed

0 responses queued

Issue type	Host	Path
Suspicious input transformation (reflected)	http://insecure-bank.com	/url-shorten
SMTP header injection	http://insecure-website.c...	/contact-us
Serialized object in HTTP message	http://insecure-bank.com	/blog
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/product/stock
External service interaction (HTTP)	https://insecure-website....	/product
Web cache poisoning	http://insecure-bank.com	/contact-us
Server-side template injection	http://insecure-bank.com	/user-homepage
SQL injection	https://vulnerable-websit...	/
OS command injection	https://insecure-website....	/feedback/submit

Time	Type	Source	Message
23:17:05 9 Oct 2019	Info	Proxy	Proxy service started on 127.0.0.1:8080

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



Mozilla Firefox Start Page
http://127.0.0.1/mutillidae/
127.0.0.1/mutillidae/
Search
OWASP Mutillidae II: Keep Calm and Pwn On
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
Want to Help?
Video Tutorials
Announcements
Hints and Videos
What Should I Do?
What's New? Click Here
Help Me!
Listing of vulnerabilities
Video Tutorials
Release Announcements
Latest Version
Helpful hints and scripts
Some Useful Firefox Add-ons
Bug Report Email Address

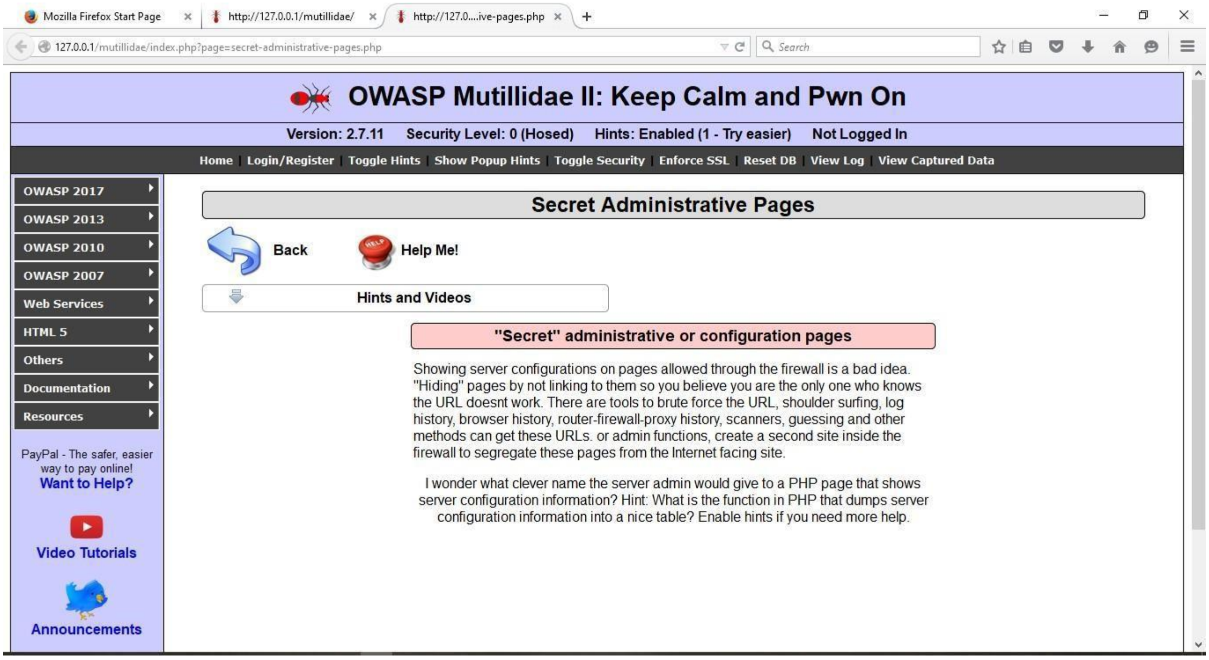
Version: 2.7.11 Security Level: 0 (Hosed) Hints: Enabled (1 - Try easier) Not Logged In

PayPal - The safer, easier way to pay online!

TIP: Click *Hint and Videos* on each page

6. Minimize Firefox and Open Burp Suite again.

F-006


Mozilla Firefox Start Page
http://127.0.0.1/mutillidae/
http://127.0....ive-pages.php
127.0.0.1/mutillidae/index.php?page=secret-administrative-pages.php
Search
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
Back
Help Me!
Hints and Videos

OWASP Mutillidae II: Keep Calm and Pwn On

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

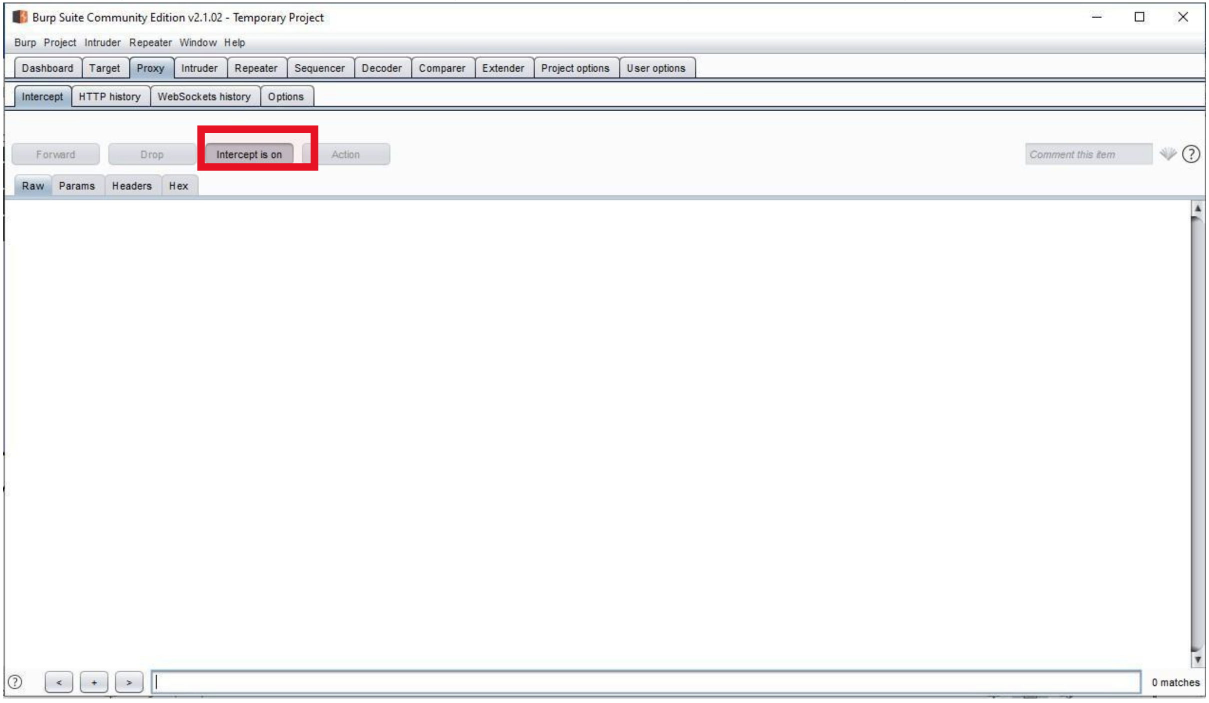
Secret Administrative Pages

"Secret" administrative or configuration pages

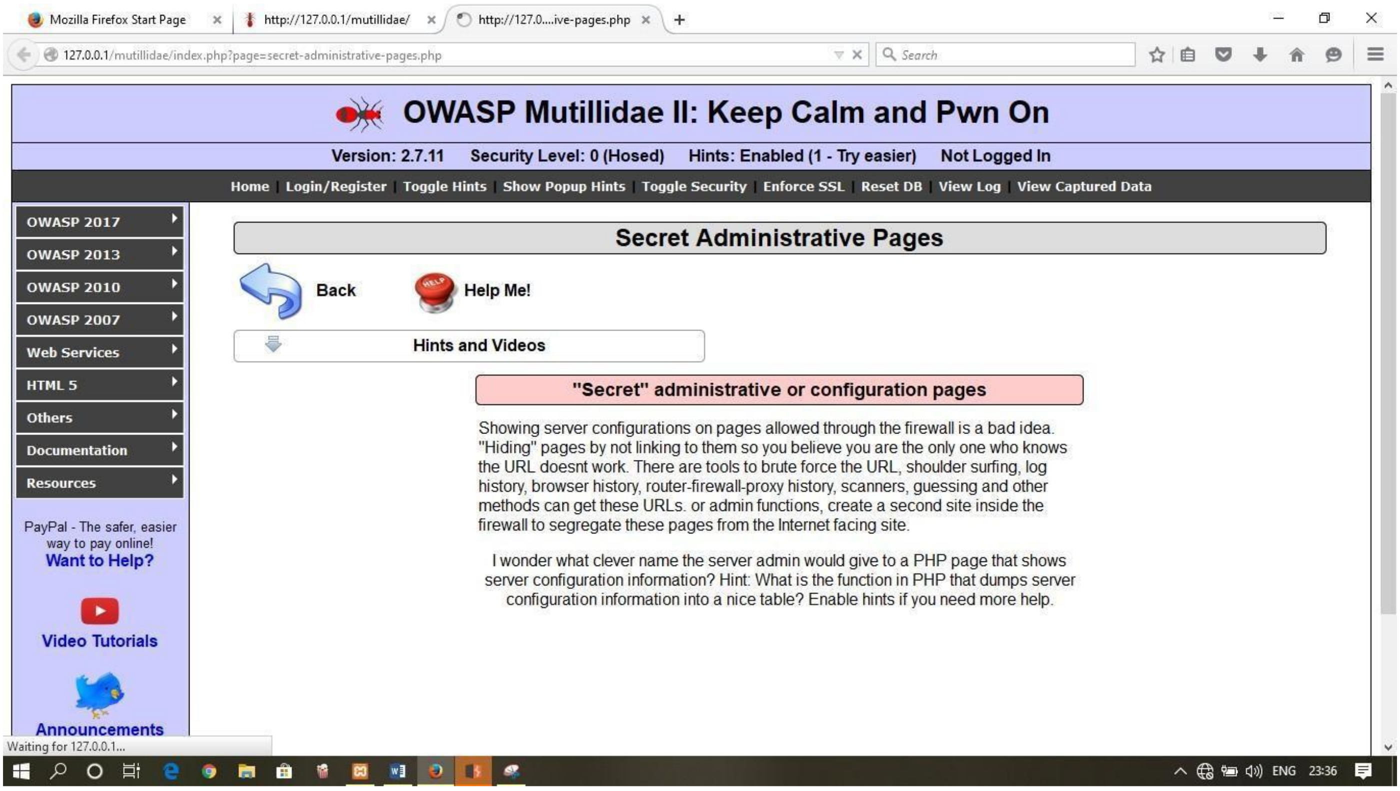
Showing server configurations on pages allowed through the firewall is a bad idea. "Hiding" pages by not linking to them so you believe you are the only one who knows the URL doesnt work. There are tools to brute force the URL, shoulder surfing, log history, browser history, router-firewall-proxy history, scanners, guessing and other methods can get these URLs. or admin functions, create a second site inside the firewall to segregate these pages from the Internet facing site.

I wonder what clever name the server admin would give to a PHP page that shows server configuration information? Hint: What is the function in PHP that dumps server configuration information into a nice table? Enable hints if you need more help.

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


Mozilla Firefox Start Page
http://127.0.0.1/mutillidae/
http://127.0....ive-pages.php
127.0.0.1/mutillidae/index.php?page=secret-administrative-pages.php
Search
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
Back
Help Me!
Hints and Videos
Waiting for 127.0.0.1...
ENG 23:36

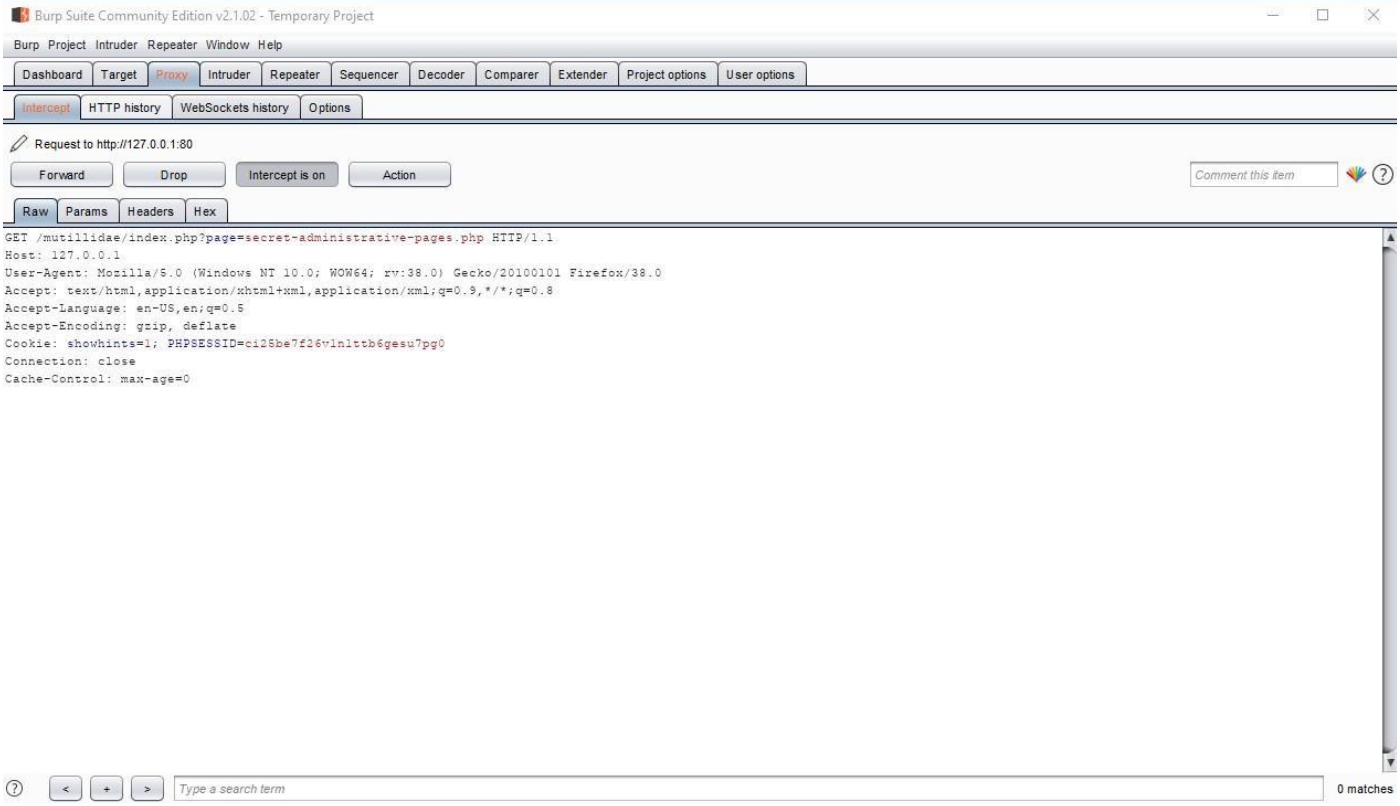
Secret Administrative Pages

"Secret" administrative or configuration pages

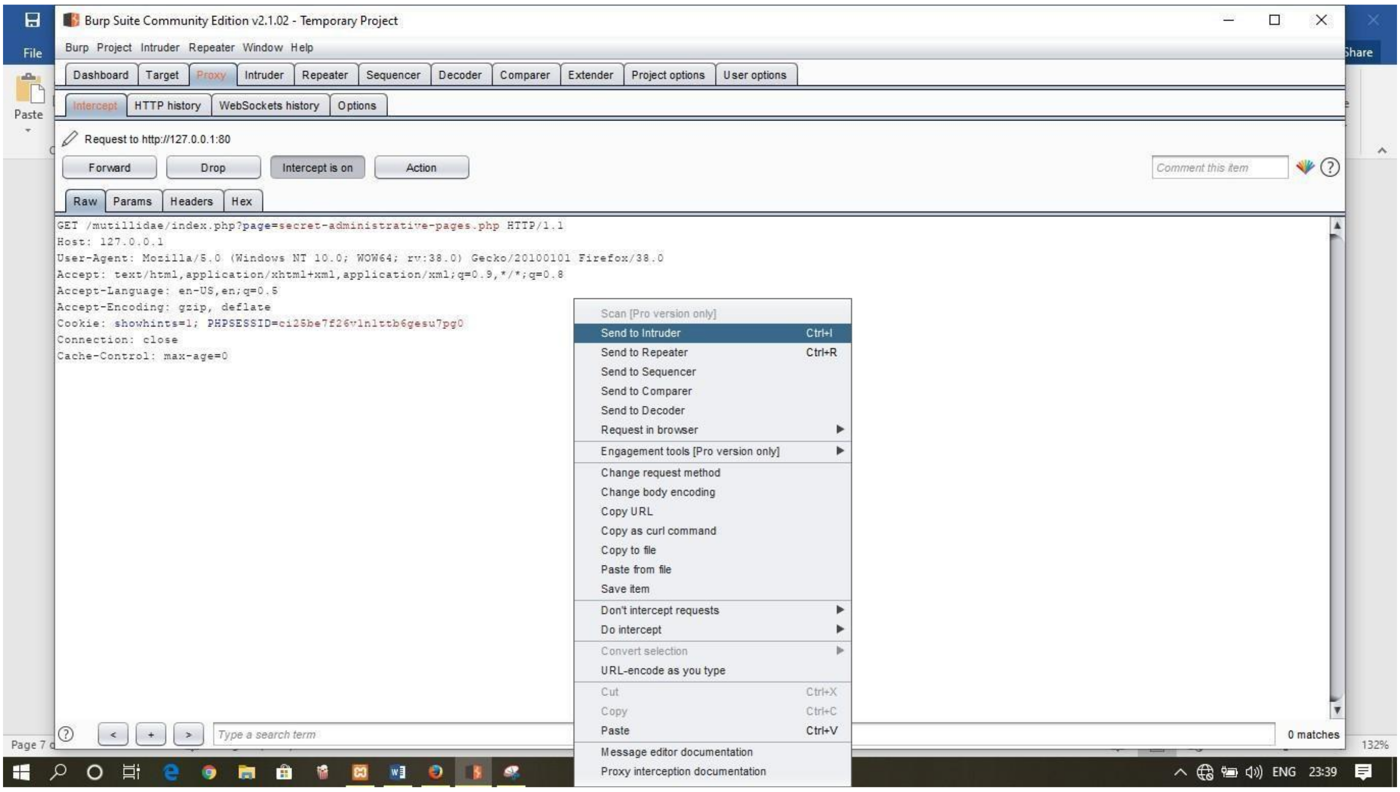
Showing server configurations on pages allowed through the firewall is a bad idea. "Hiding" pages by not linking to them so you believe you are the only one who knows the URL doesnt work. There are tools to brute force the URL, shoulder surfing, log history, browser history, router-firewall-proxy history, scanners, guessing and other methods can get these URLs. or admin functions, create a second site inside the firewall to segregate these pages from the Internet facing site.

I wonder what clever name the server admin would give to a PHP page that shows server configuration information? Hint: What is the function in PHP that dumps server configuration information into a nice table? Enable hints if you need more help.

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



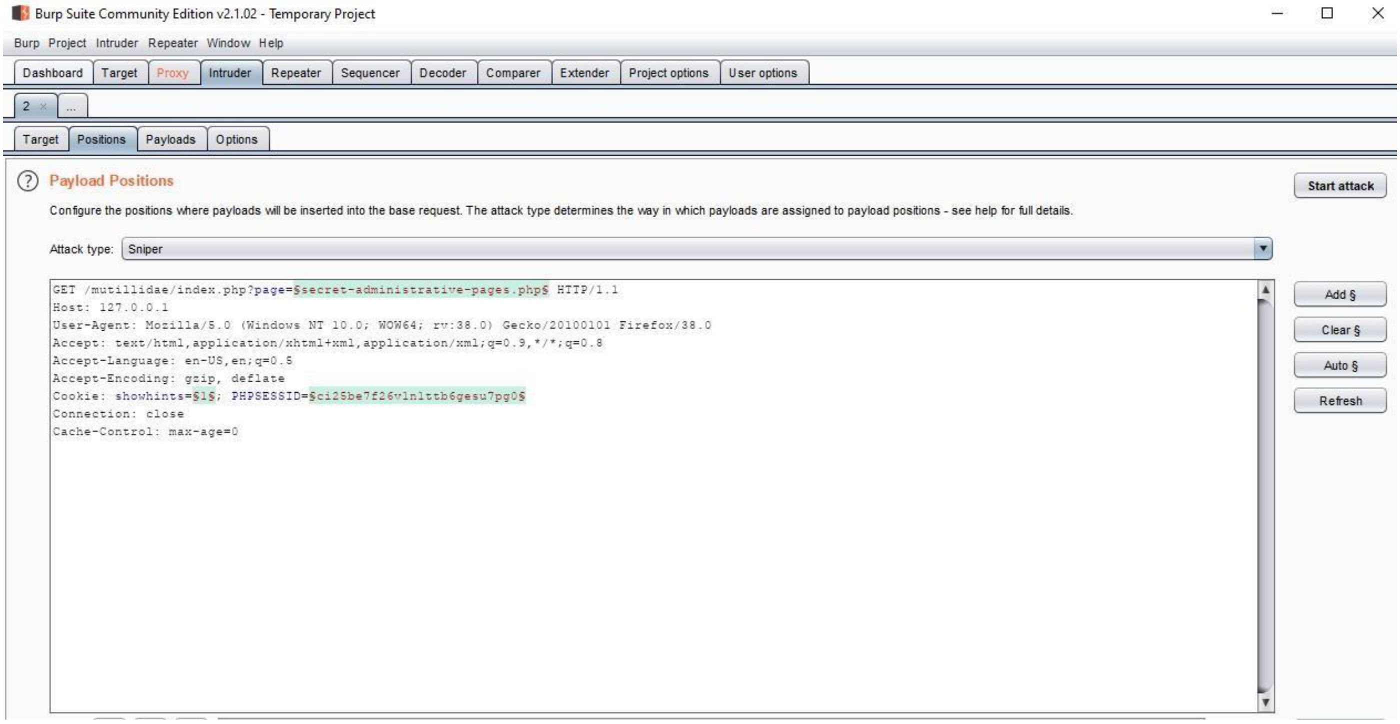
```
GET /mutillidae/index.php?page=secret-administrative-pages.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=1; PHPSESSID=ci25be7f26v1n1ttb6gesu7pg0
Connection: close
Cache-Control: max-age=0
```



Request to http://127.0.0.1:80

```
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=ci25be7f26v1n1ttb6gesu7pg0
Connection: close
Cache-Control: max-age=0
```

11. Under **Intruder** tab Select **Positions** Click on **Clear**.



Payload Positions

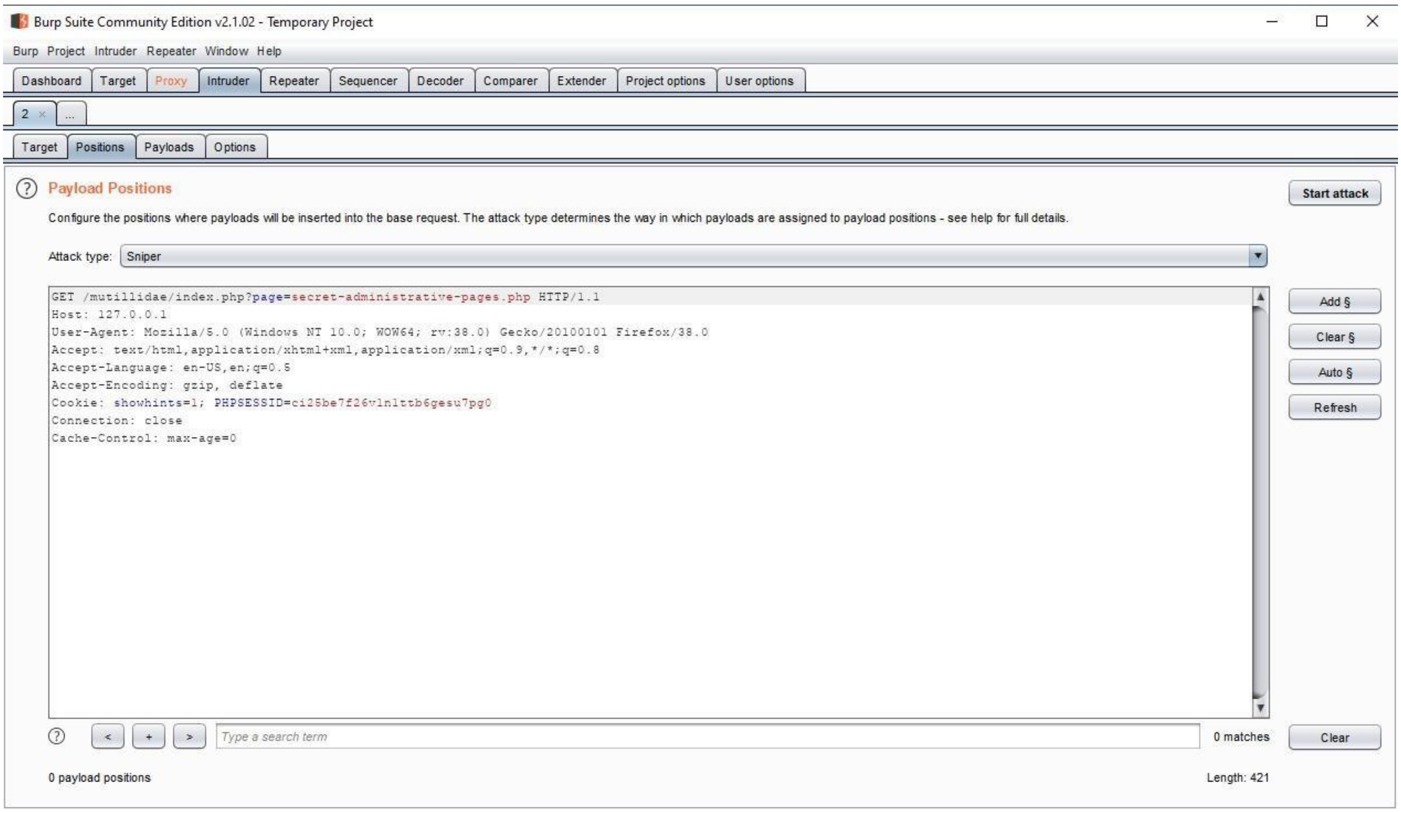
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

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=§ci25be7f26v1n1ttb6gesu7pg0§
Connection: close
Cache-Control: max-age=0
```

Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
2 ×
...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh

F-006


Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
2 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
< + >
Type a search term
Clear

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

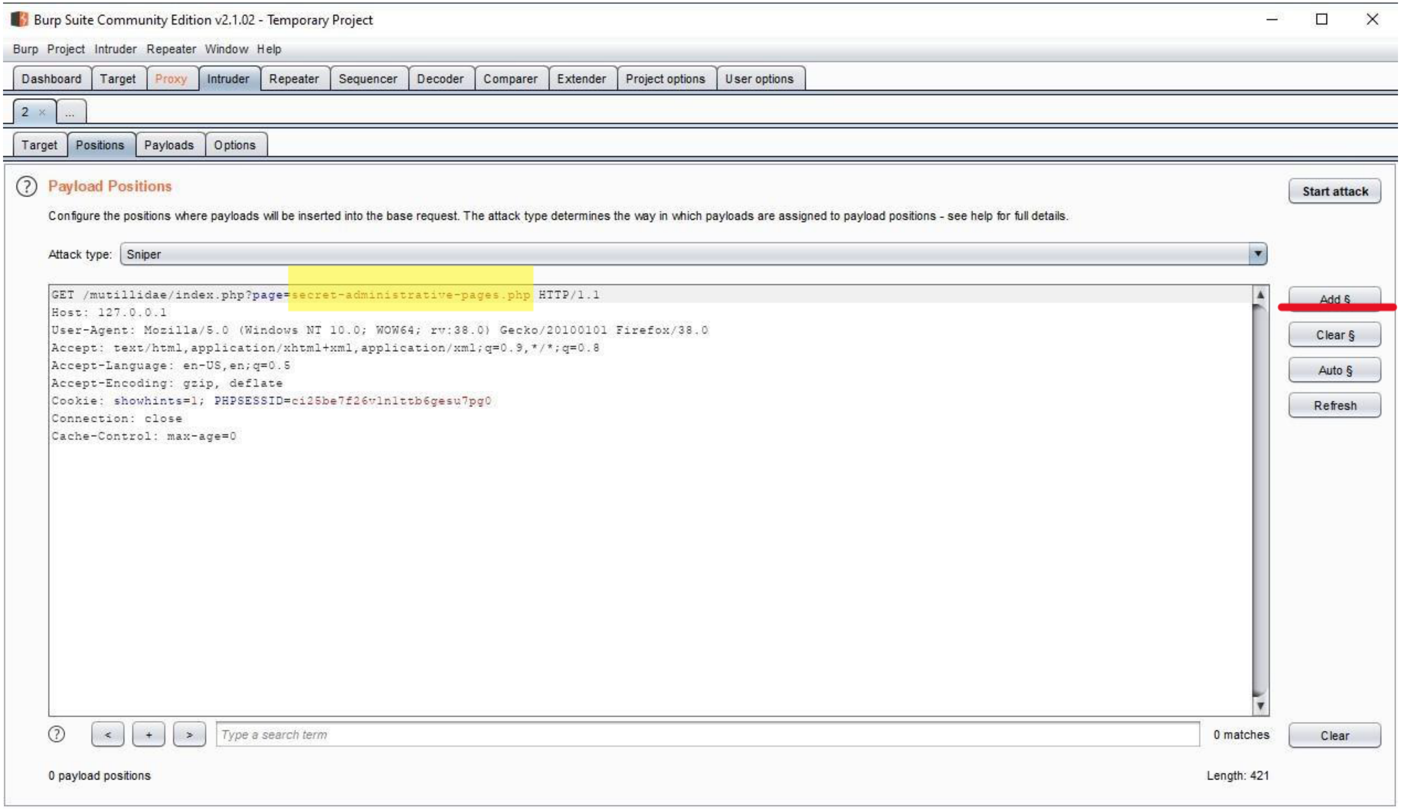
```
GET /mutillidae/index.php?page=secret-administrative-pages.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=1; PHPSESSID=ci25be7f26vlnlttb6gesu7pg0
Connection: close
Cache-Control: max-age=0
```

0 matches

0 payload positions

Length: 421

12. Select the highlighted path then click Add.


Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
2 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
< + >
Type a search term
Clear

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

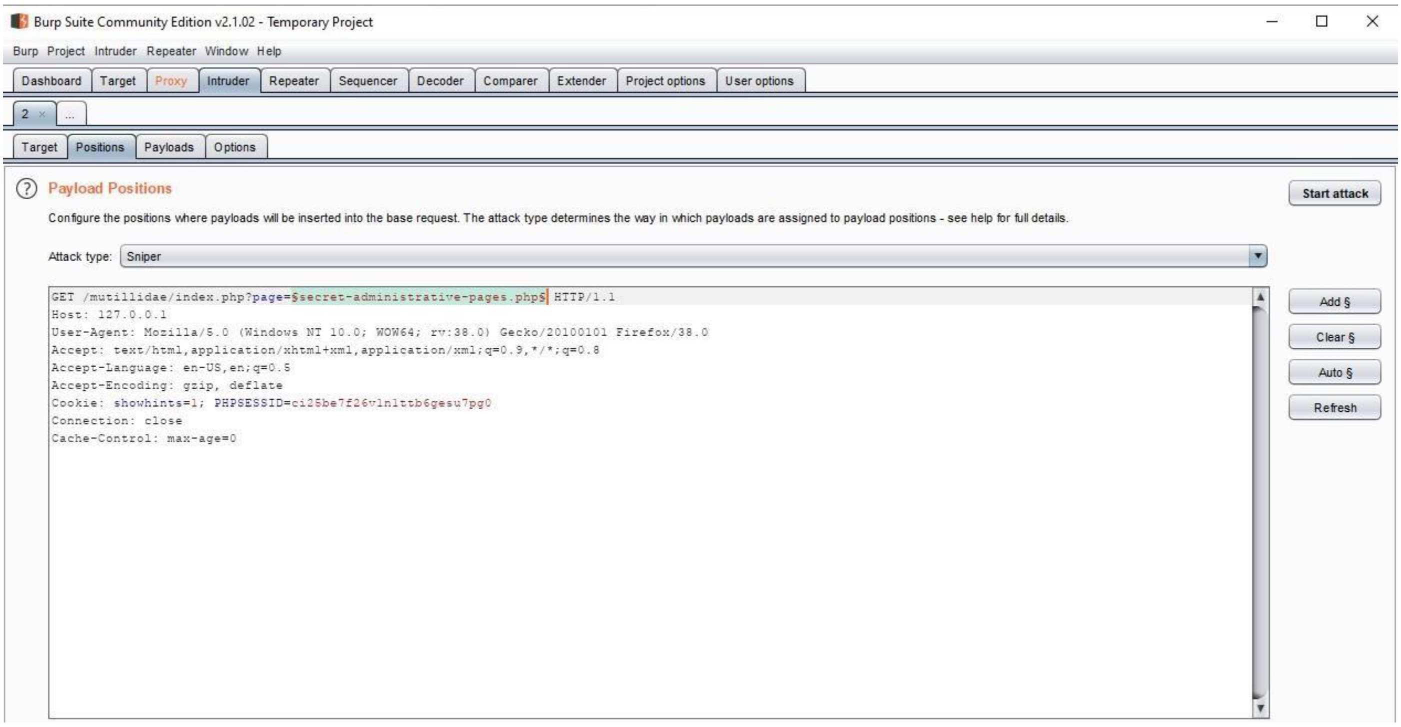
```
GET /mutillidae/index.php?page=secret-administrative-pages.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=1; PHPSESSID=ci25be7f26vlnlttb6gesu7pg0
Connection: close
Cache-Control: max-age=0
```

0 matches

0 payload positions

Length: 421

F-006

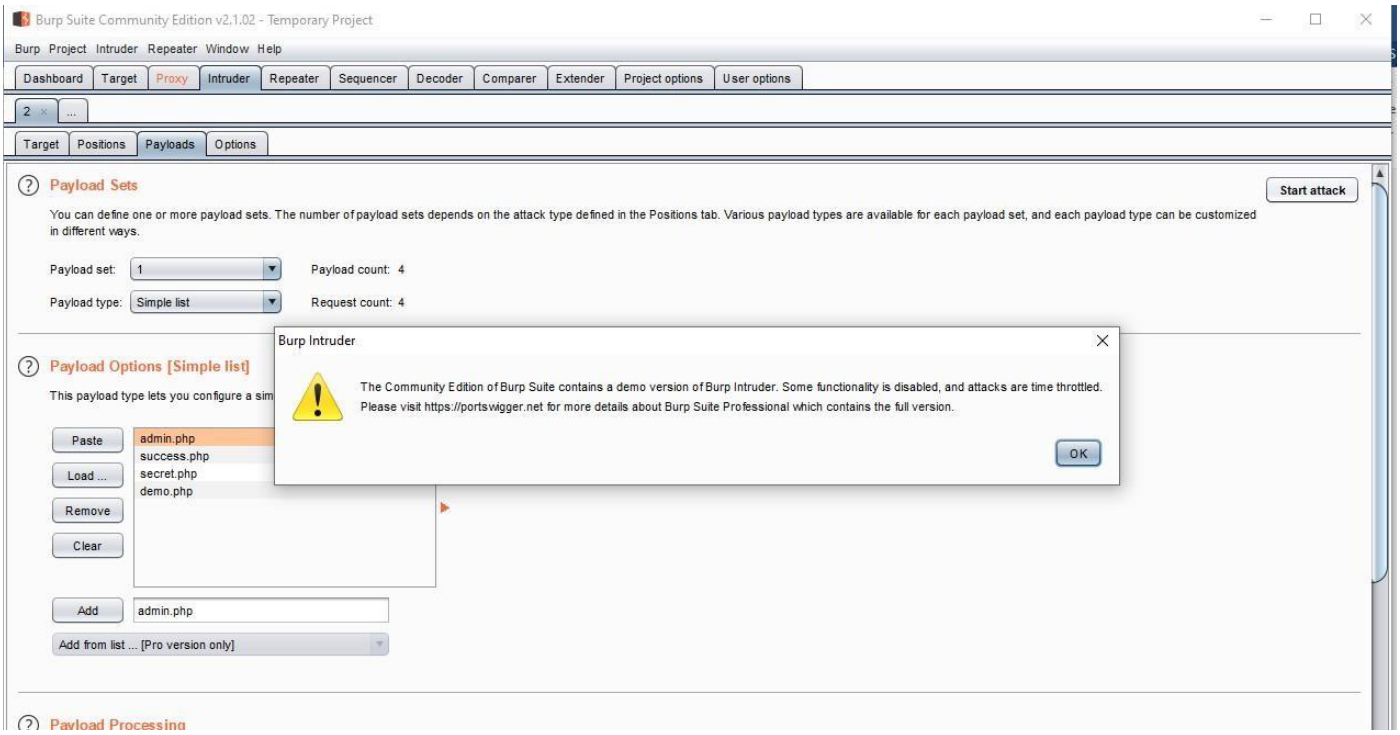

Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
2 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh

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=ci25be7f26vlnlttb6gesu7pg0
Connection: close
Cache-Control: max-age=0
```


Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
2 × ...
Target Positions Payloads Options
Start attack
Paste
Load ...
Remove
Clear
Add
Add from list ... [Pro version only]
OK

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 4

Payload type: Simple list Request count: 4

Payload Options [Simple list]

This payload type lets you configure a sim

admin.php
success.php
secret.php
demo.php

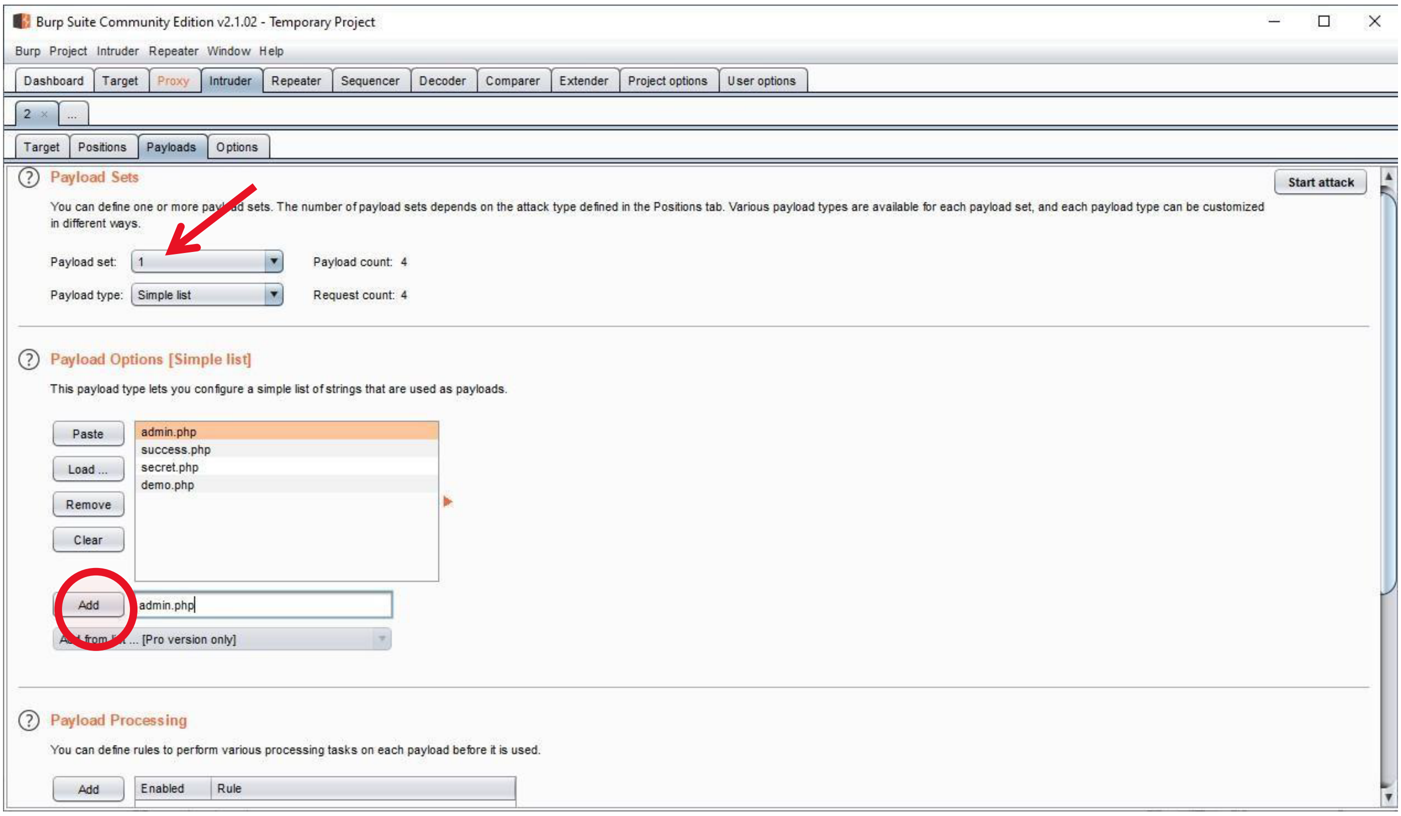
admin.php

Payload Processing

Burp Intruder

The Community Edition of Burp Suite contains a demo version of Burp Intruder. Some functionality is disabled, and attacks are time throttled. Please visit https://portswigger.net for more details about Burp Suite Professional which contains the full version.

F-006


Burp Suite Community Edition v2.1.02 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
2 ×
...
Target Positions Payloads Options
Start attack
Paste
Load ...
Remove
Clear
Add
Add from list ... [Pro version only]
Add
Enabled Rule

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 4

Payload type: Simple list Request count: 4

Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

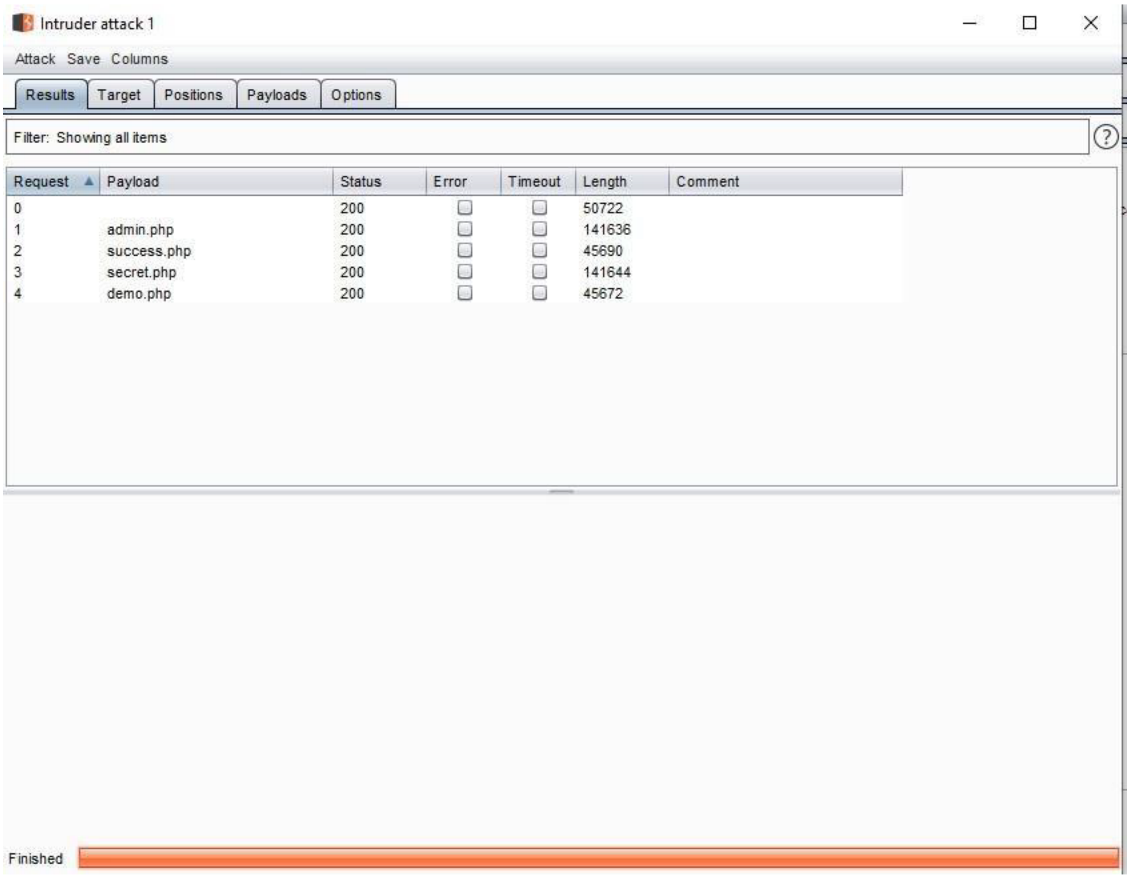
admin.php
success.php
secret.php
demo.php

admin.php

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

13. Under Payloads (7) 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

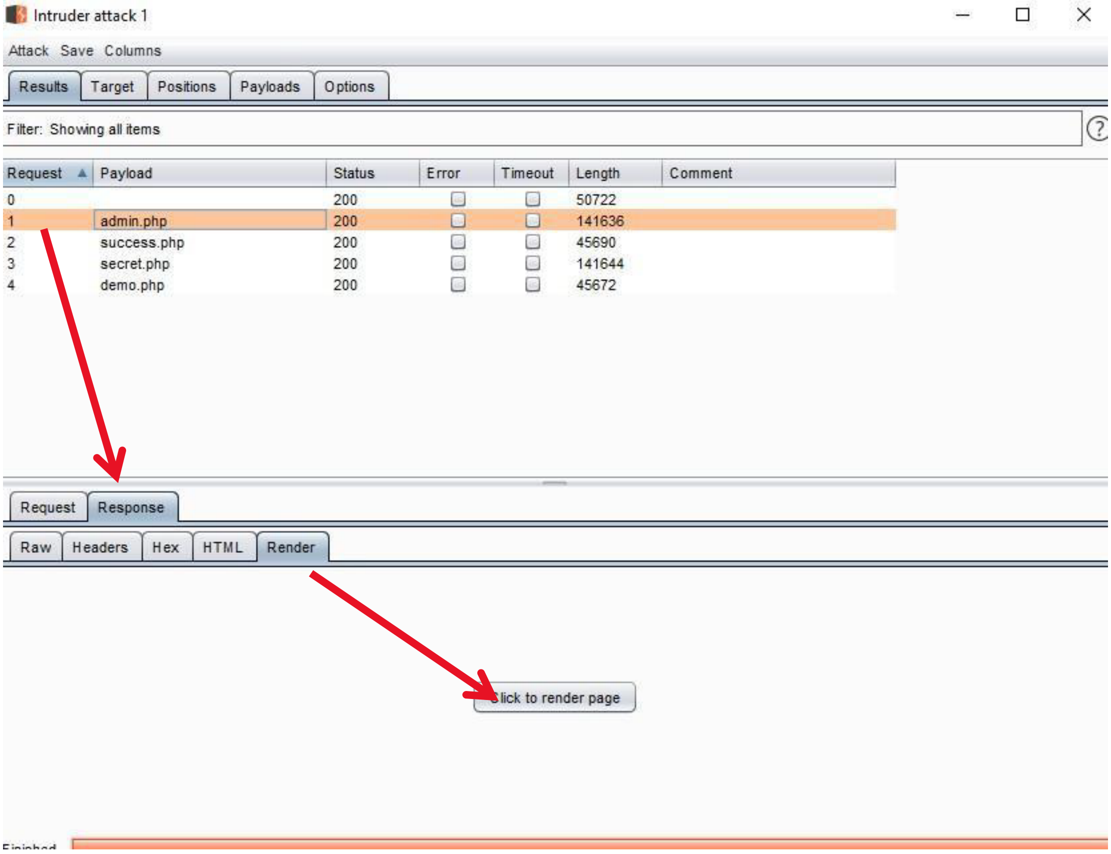


Filter: Showing all items

Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	50722	
1	admin.php	200	□	□	141636	
2	success.php	200	□	□	45690	
3	secret.php	200	□	□	141644	
4	demo.php	200	□	□	45672	

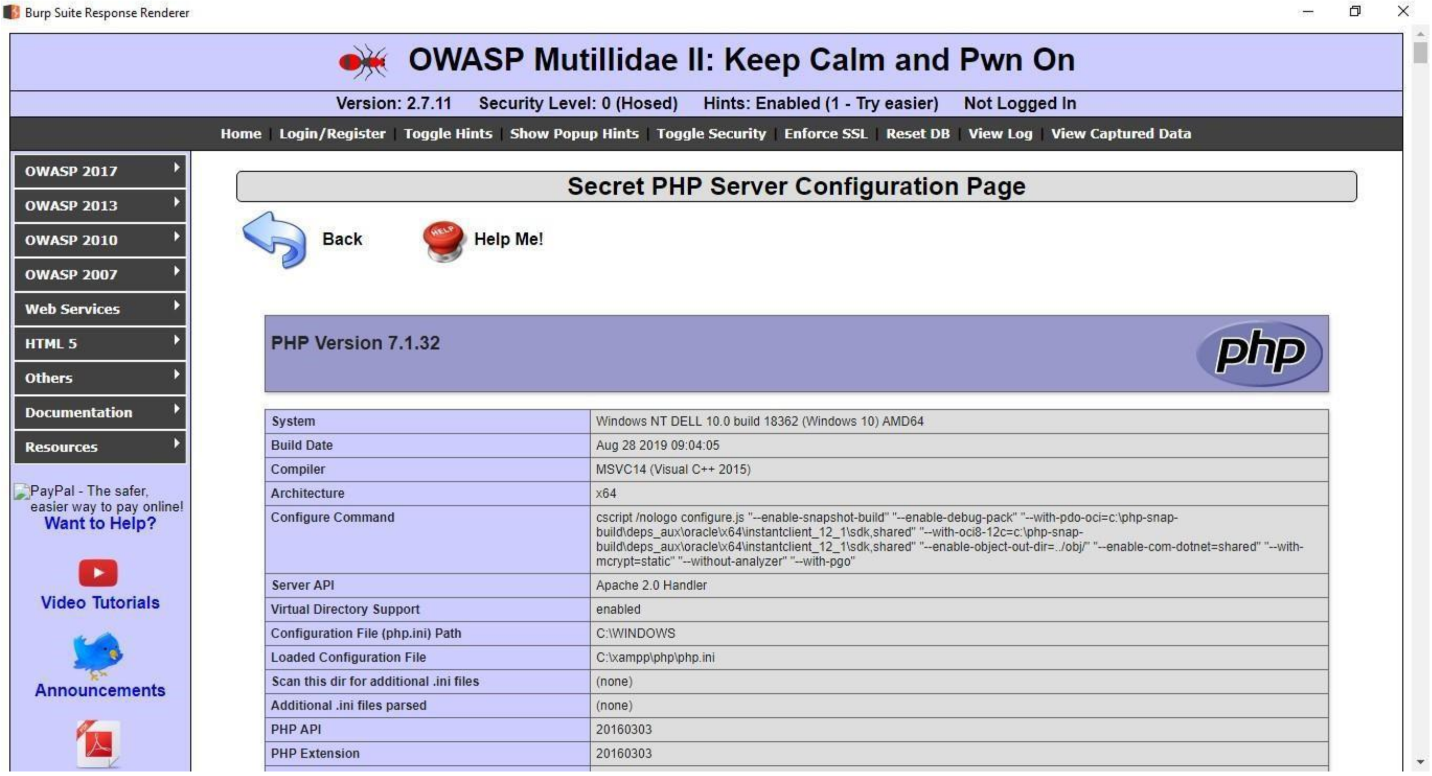
Finished

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.


Intruder attack 1
Attack Save Columns
Results Target Positions Payloads Options
Filter: Showing all items
Request Response
Raw Headers Hex HTML Render
Click to render page
Finished

Request ▲	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	50722	
1	admin.php	200	□	□	141636	
2	success.php	200	□	□	45690	
3	secret.php	200	□	□	141644	
4	demo.php	200	□	□	45672	

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
Back
Help Me!
php

Secret PHP Server Configuration Page

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	cscript /nologo configure.js "--enable-snapshot-build" "--enable-debug-pack" "--with-pdo-oci=c:\php-snap-build\deps_aux\oracle\x64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-build\deps_aux\oracle\x64\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