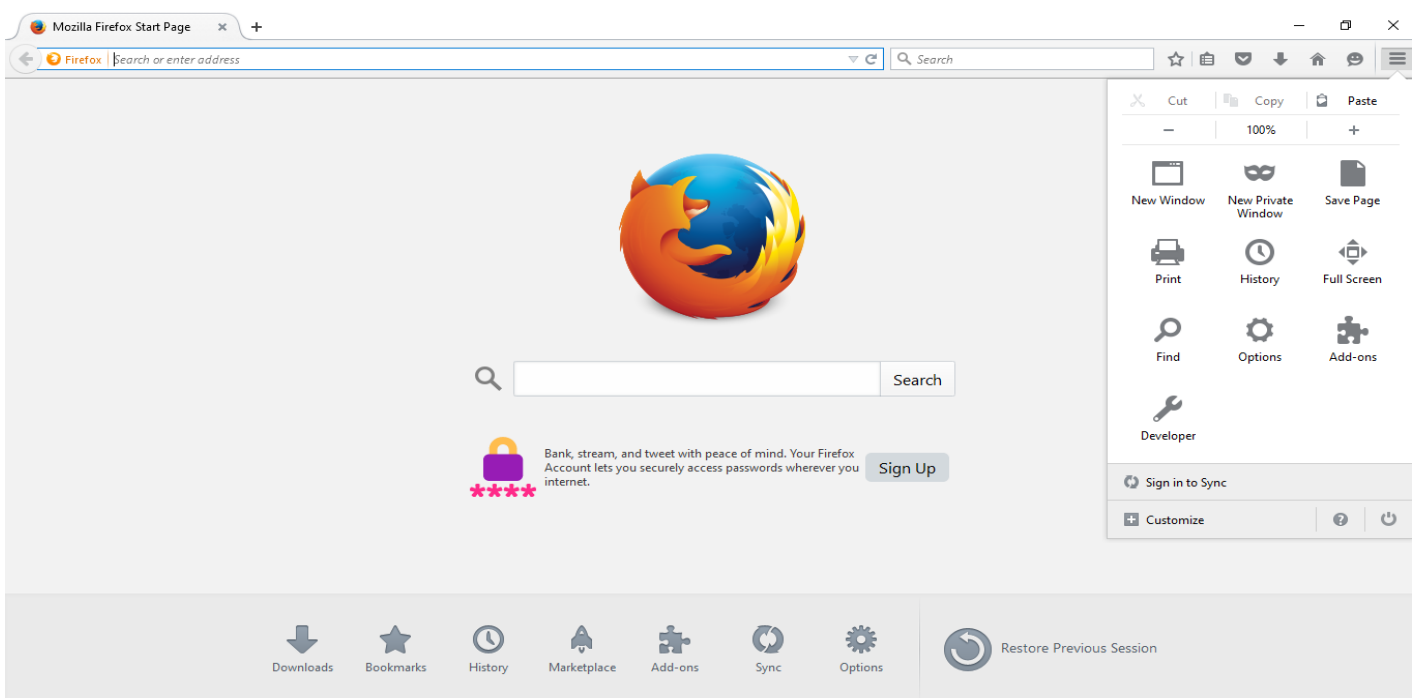
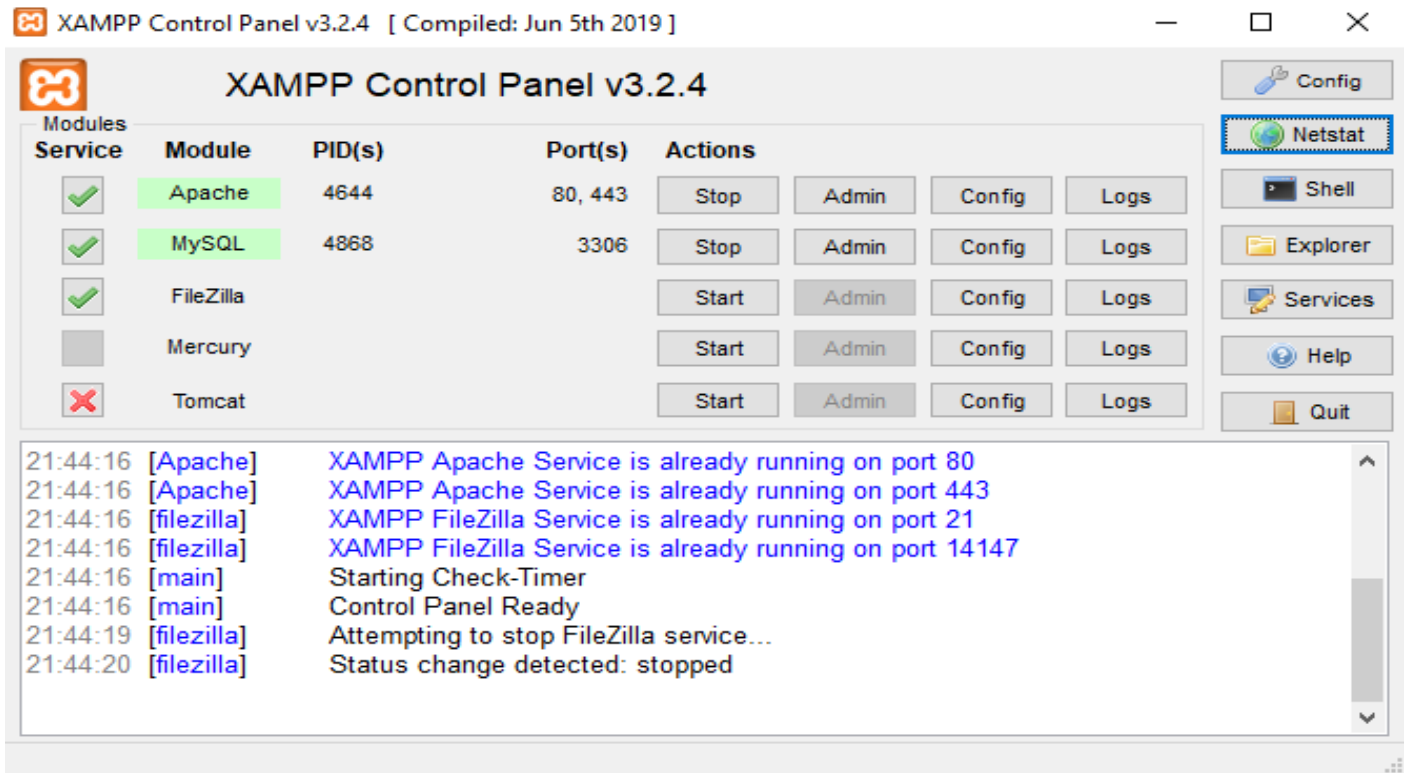
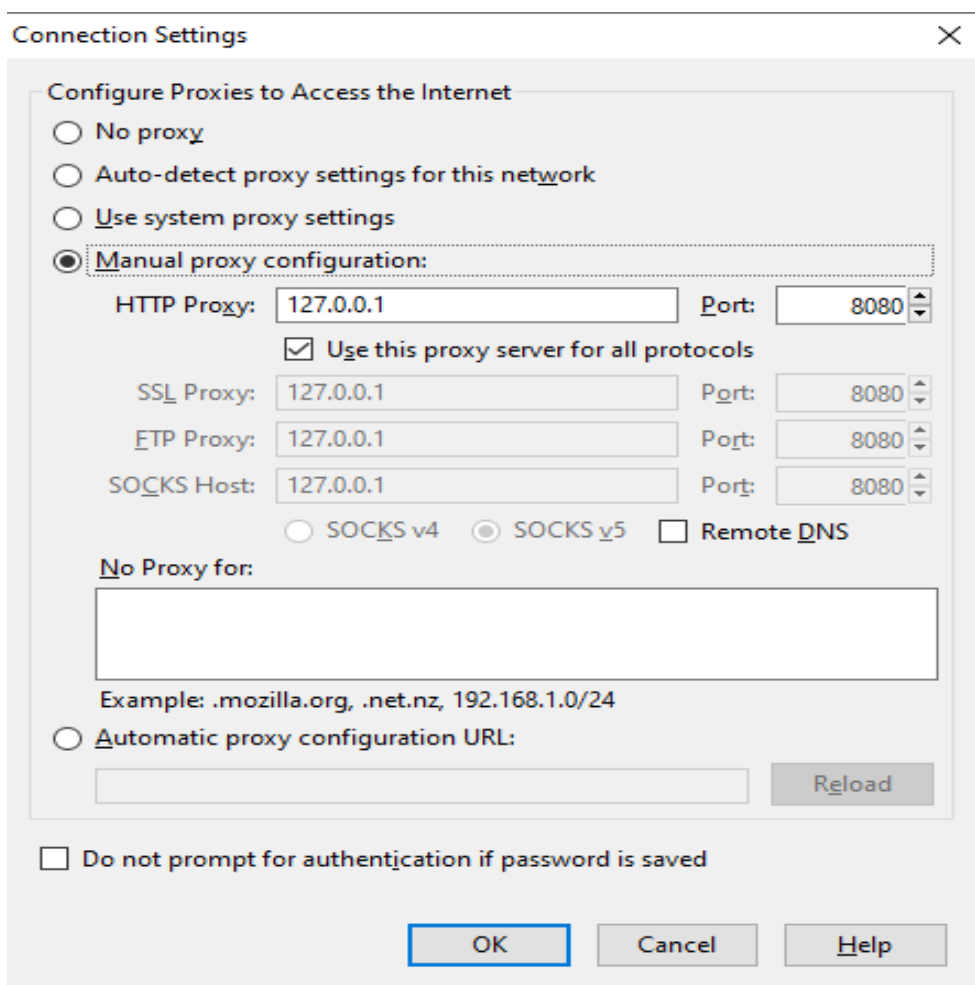
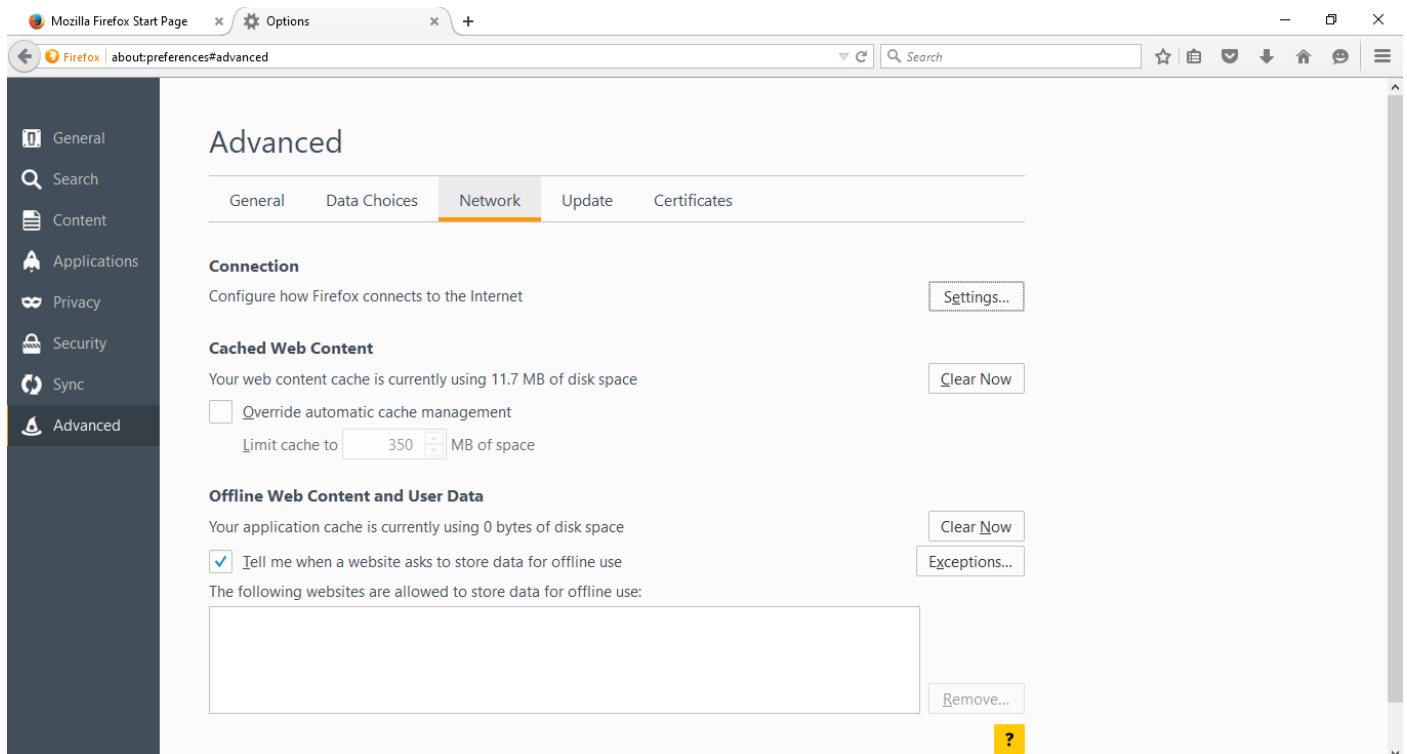


Practical 8

OWASP Security Misconfigurations





? 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

? 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

Cancel

Back

Start Burp

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

1. Live passive crawl from Proxy (all traffic)

Add links. Add item itself, same domain and URLs in suite scope. 0 items added to site map

Capturing: ☒ 0 responses processed
0 responses queued

Issue activity [Pro version only]
?
↗

Filter High Medium Low Info Certain Firm Tentative Search...

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-website...	/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-website...	/
OS command injection	https://insecure-website....	/feedback/submit

Event log
?
↗

Filter Critical Error Info Debug Search...

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

Memory: 57.5MB Disk: 32KB

Mozilla Firefox Start Page x http://127.0.0.1/mutillidae/ x +

127.0.0.1/mutillidae/ Search

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

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

TIP: Click [Hint and Videos](#) on each page

Mozilla Firefox Start Page x http://127.0.0.1/mutillidae/ x http://127.0.0.1/...ive-pages.php x +

127.0.0.1/mutillidae/index.php?page=secret-administrative-pages.php


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 Administrative Pages

 Back  Help Me!

 Hints and Videos

"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 doesn't 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.

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

Intercept HTTP history WebSockets history Options

Forward Drop Intercept is on Action

Raw Params Headers Hex

Comment this item

0 matches

Mozilla Firefox Start Page x http://127.0.0.1/mutillidae/ x http://127.0.0.1/ive-pages.php x +

127.0.0.1/mutillidae/index.php?page=secret-administrative-pages.php

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 Administrative Pages

Back Help Me!

Hints and Videos

"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 doesn't 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.

Waiting for 127.0.0.1...

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

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

```
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
```

Type a search term 0 matches

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

Intercept HTTP history WebSockets history Options

Request to http://127.0.0.1:80

Forward Drop Intercept is on Action

Comment this item

Raw Params Headers Hex

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

Scan [Pro version only]
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer
Send to Decoder
Request in browser
Engagement tools [Pro version only]
Change request method
Change body encoding
Copy URL
Copy as curl command
Copy to file
Paste from file
Save item
Don't intercept requests
Do intercept
Convert selection
URL-encode as you type
Cut Ctrl+X
Copy Ctrl+C
Paste Ctrl+V
Message editor documentation
Proxy interception documentation

0 matches 132%

File 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

Start attack

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

Add \$
Clear \$
Auto \$
Refresh

2 x ...

Target Positions Payloads Options

2 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=c125be7f26v1nlctb6gesu7pg0
Connection: close
Cache-Control: max-age=0

0 matches

0 payload positions

Length: 421

2 x ...

Target Positions Payloads Options

2 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.

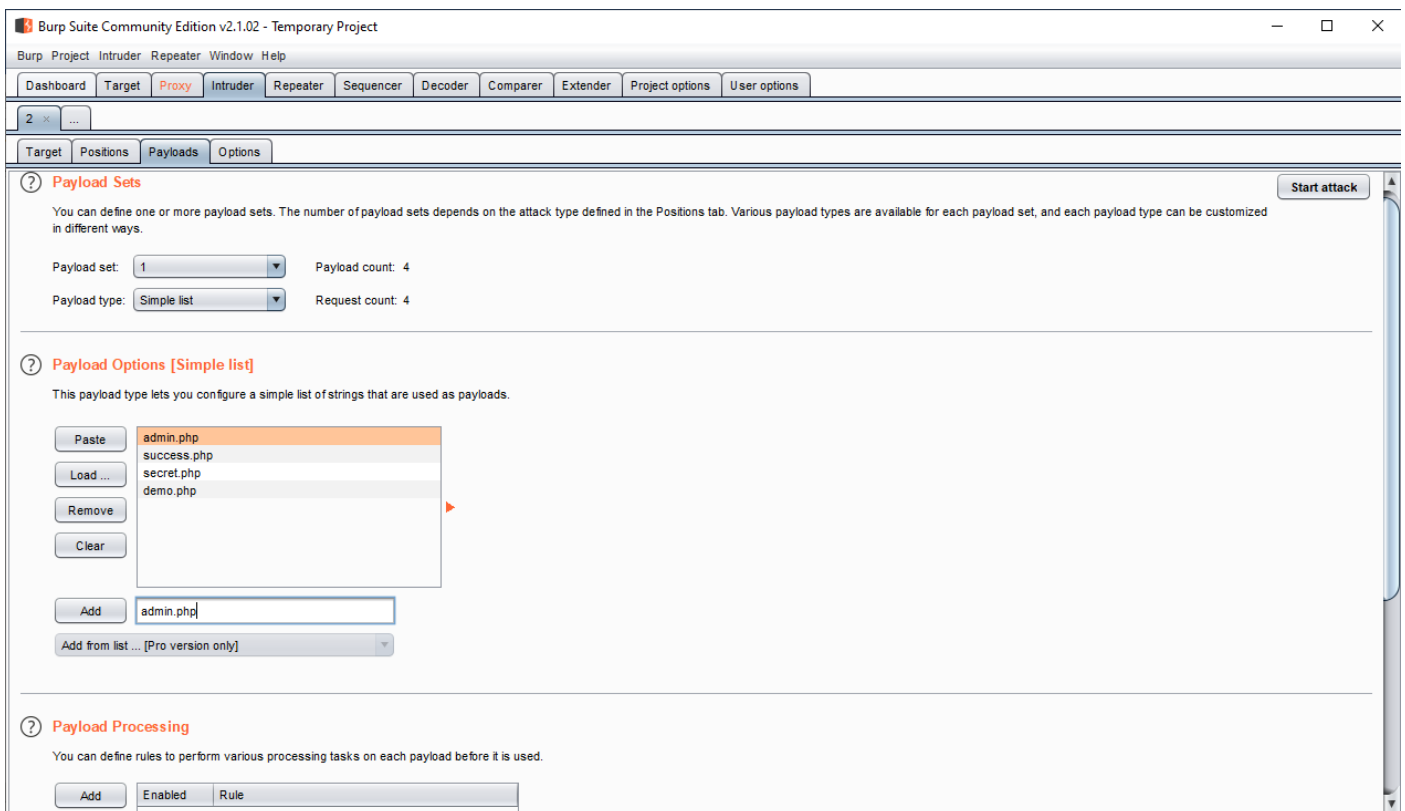
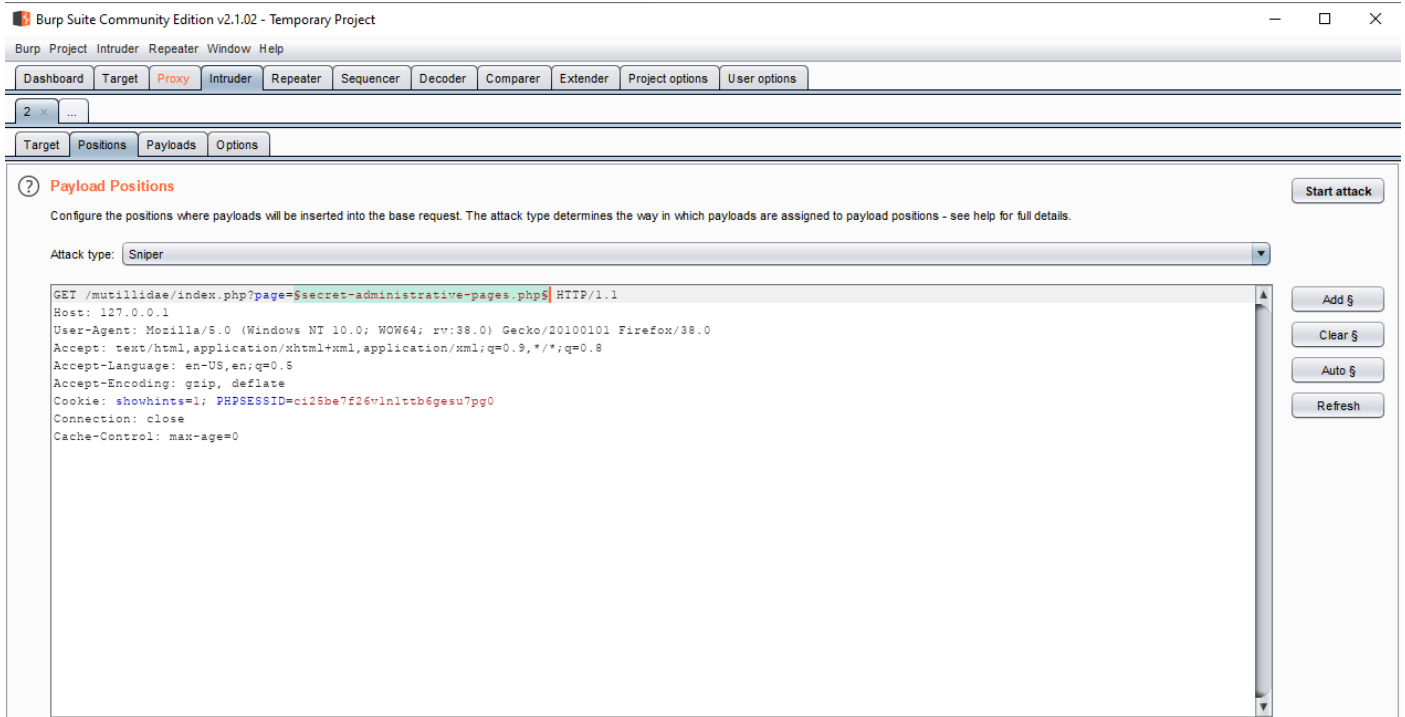
Attack type: **Sniper**

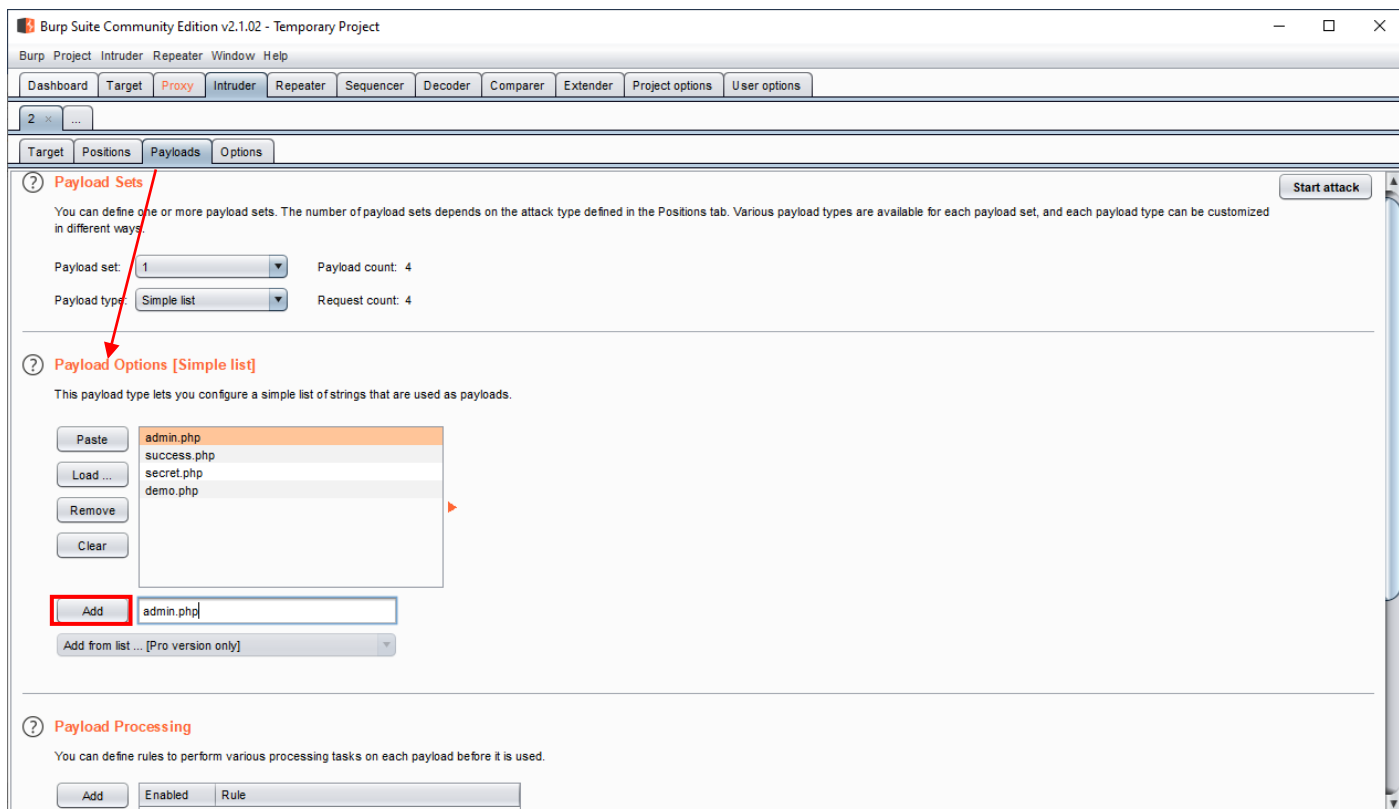
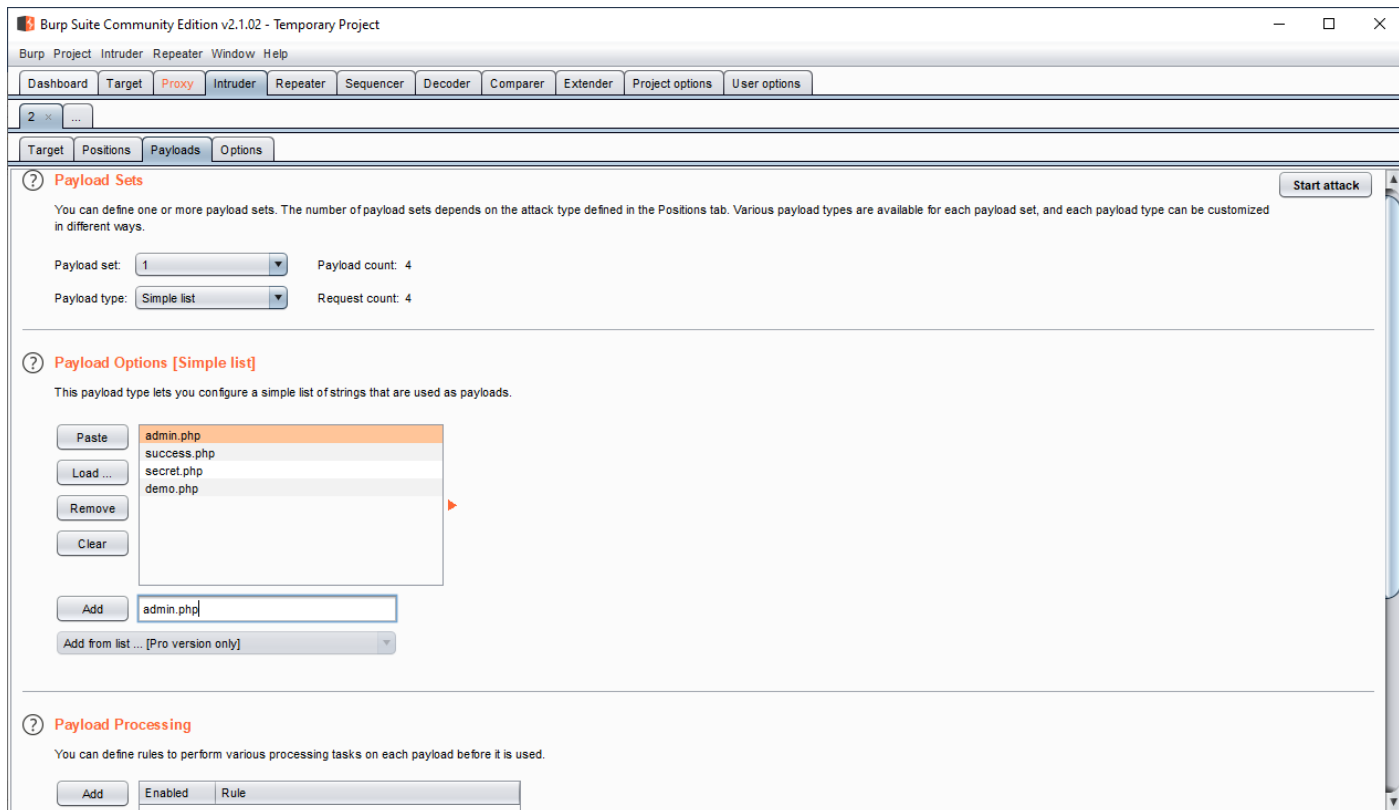
GET /mutillidae/index.php?page=secret-administrative-pages.php HTTP/1.1
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:38.0) Gecko/20100101 Firefox/38.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: showhints=1; PHPSESSID=c125be7f26v1nlctb6gesu7pg0
Connection: close
Cache-Control: max-age=0

0 matches

0 payload positions

Length: 421





2 x ...

Target Positions Payloads Options

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 payloads.

Paste admin.php
Load ... success.php
Remove secret.php
Clear demo.php

Add admin.php

Add from list ... [Pro version only]

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.

OK

Payload Processing

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

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

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

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	

Request Response

Raw Headers Hex HTML Render

Click to render page

Finished

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-builddeps_aux\oracle\v64\instantclient_12_1\sdk,shared" "--with-oci8-12c=c:\php-snap-builddeps_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