

THE BROWSER-BRUTER

By Jafar Pathan

The FIRST-EVER Browser Based Web Fuzzing Tool



Who Am I?

- Information Security Professional 
- I am working as a security analyst & I love doing Research on Cyber Security
- Linkedin - <https://www.linkedin.com/in/jafar-pathan/>
- X - https://twitter.com/zinja_coder
- Github - <https://github.com/zinja-coder>
- Email - jafar.pathan2503@gmail.com



Before We Begin, Ethical code

- All techniques demonstrated in this session are for educational and ethical purposes only.
- It is important to use these skills responsibly and in compliance with applicable laws and regulations.
- Any misuse of these techniques is strictly discouraged

What Is Browser-Bruter?

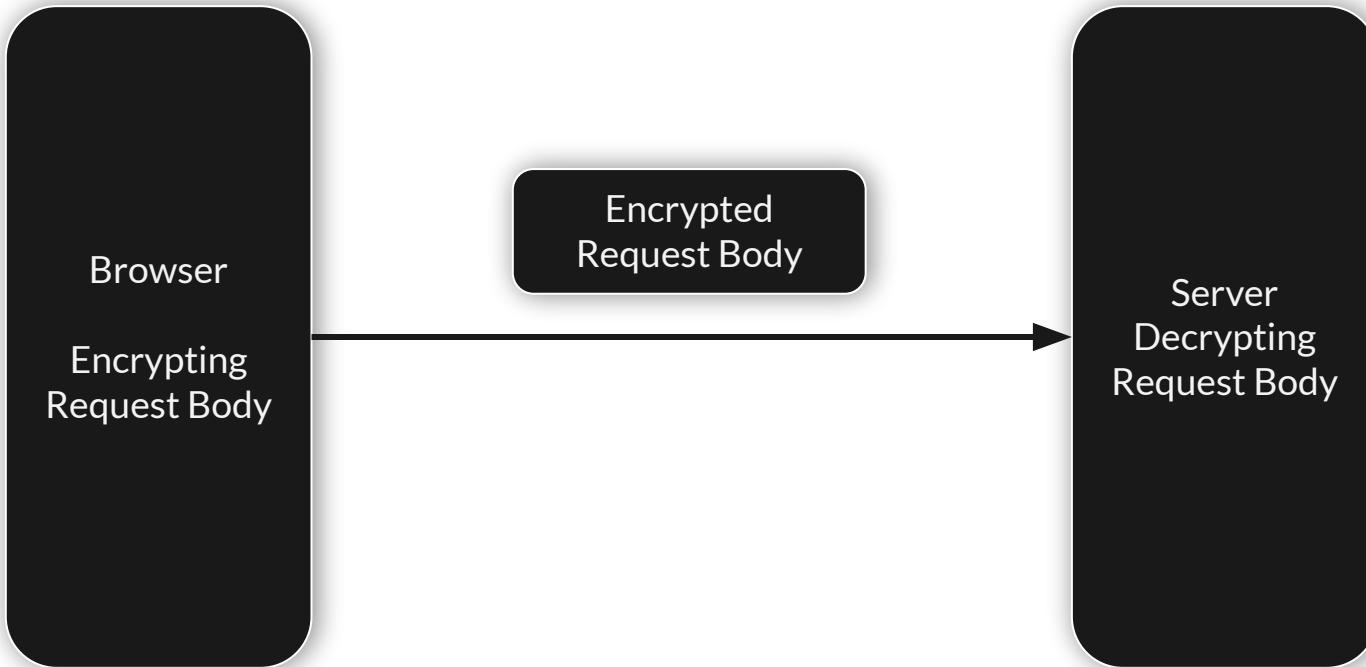
- The BrowserBruter is the **FIRST EVER!** advance browser-based automated web application penetration testing tool.
- Automatically injects payloads into web application using by controlling and automating the browser.
- Fuzzes web applications on browser layer instead HTTP layer
- Completely bypasses the encryptions, encodings and also can tackle captchas.

The Curse Of Encryption

To understand the BrowserBruter, we need to understand why we created it. It is because of "**The Curse Of Encryption**".

- The sole reason behind the birth of the BrowserBruter.
- Worst nightmare during web application assessments.
- Most time consuming barrier in automation of web application penetration testing.

But What Is Curse Of Encryption?



The Curse Of Encryption

Please Sign in

Username	<input type="text" value="Username"/>
Password	<input type="password" value="Password"/>
 Sign in	

The Curse Of Encryption

Please Sign in

Username	<input type="text" value="admin"/>
Password	<input type="password" value="•••••••• "/>
<input type="button" value="➔ Sign in"/> ←	

The Curse Of Encryption

```
Request
Pretty Raw Hex
1 POST /login3.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
   Firefox/115.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
   q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 765
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/login3.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 username=
```

The Curse Of Encryption

Please Sign in

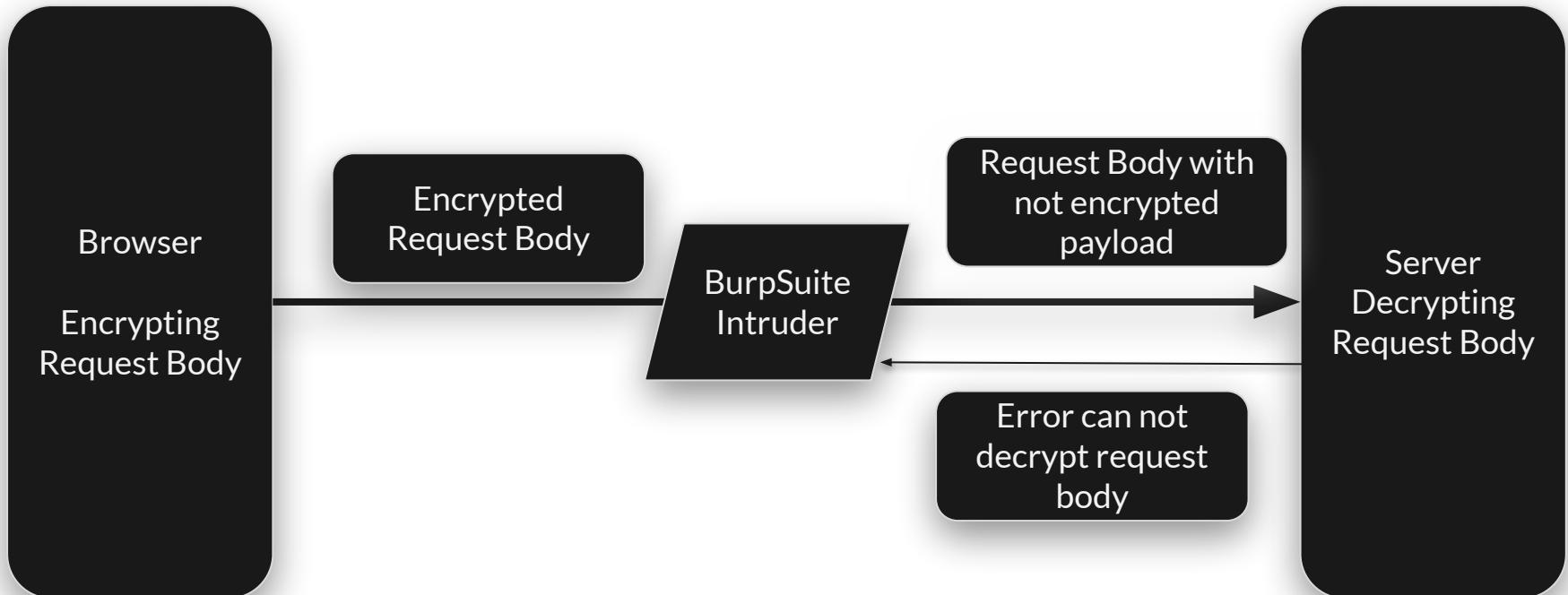
! Username doesnot exists

Username

Password

 Sign in

Attacking At HTTP Layer



Attacking At HTTP Layer

Request

Pretty Raw Hex

```
1 POST /login3.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101
   Firefox/115.0
4 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
   q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 765
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/login3.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 username= FRRTiKF9C2201iJXjWFuZBpeAsNz9eK1zZD%2Fa0YZ0YIDtrc3lX0IzcrGw4M0ShtV0NMwihhEV3Y47y
G57pjmvEUI%2BKu8gt4nlmbzYZ%2Bk6g%2FZtnByud3QGc4PyQsJIIR64PMGheuxda47Cu7pdj9Yutu
l4n3rfdi8XL0MVbRWzs2HtKls8biqsliz2%2FvPZHboU4vmncxgqM0lig8J0WvuOaW7tTGnL54S3v1K%
2Fq%2BVuuu04wnrfxfwk2AS5NX5cMUZ8QjnyWnv%2BA8tD%2FvAeTjei0aiNXyyLZg09gddMq1F4tBV
2os%9%2Buox1YWp0YKZTVXH6btkr%2FafzNkiLoGxp4Njg%3D%3D&password=
lKh3pgEtorIgSGVmzdVwOn099yJRBpPcc9a8xopx7%2BER8%2F0A59mCKC0Dsvh4RPR0KA0oH1ZNpcZH
%2FQPc6%2F5%2BHBx4upof2dAG5N3BnRGVY0v0wgjKkuB9rNwJsVpDkWvY0JjG%2F%2BFWm7Km0FQfo
mHljc%2BuZ6FE%2BRoHue2olasPhNHSX9k1AnPug0mnRPndwdeD2nA3XPcnT6IKZZfxdxAcx0XL%2B1I
LWj4apqIG8AUmUsTtUbmqUWW0MI3huwfL68WaGCqo%2FcNj%2Baazi8iVP2Hp10clu8bZGE6vIGfHS3
39dK00Sg63WRR7xT9SJW%2BzXGBeyKb65Szvmm6ru%2B3S7Tg%3D%3D
```



Attacking At HTTP Layer

Request

Pretty Raw Hex

1 POST /login3.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;
q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 34
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/login3.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 **username=admin'&password=password'**

Attacking At HTTP Layer

Please Sign in

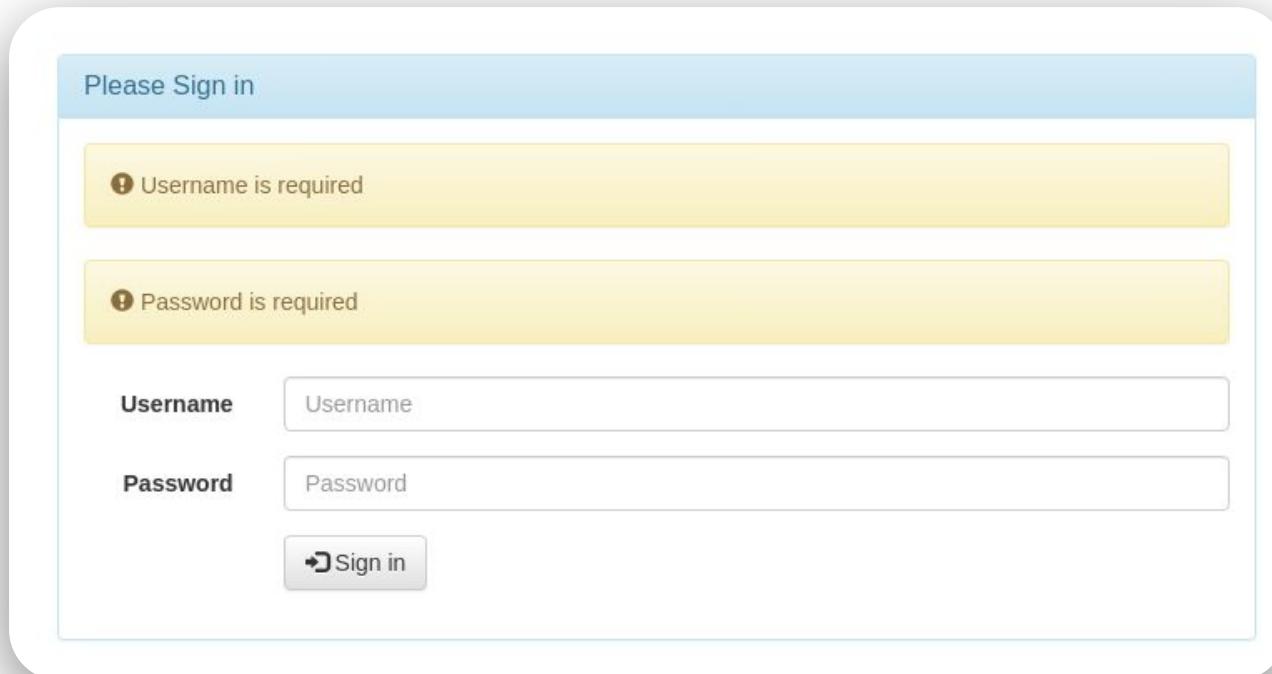
! Username is required

! Password is required

Username

Password

 **Sign in**



Attacking At HTTP Layer

② Choose an attack type

Attack type: Sniper

③ Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

⊕ Target: Update Host header to match target

```
1 POST /login3.php HTTP/1.1
2 Host: localhost
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 34
9 Origin: http://localhost
10 Connection: close
11 Referer: http://localhost/login3.php
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17
18 username=$admin'&password=$password'$
```

Attacking At HTTP Layer

Results	Positions	Payloads	Resource pool	Settings	
Filter: Showing all items					
Request ^	Position	Payload	Status code	Response received	Error
0	0	'	200	4	3765
1	1	'	200	4	3764
2	1	(select*from(select(sleep(20)))a'	200	5	3765
3	1	'+(select*from(select(sleep(20)))a)+'	200	6	3764
4	1	and (select*from(select(sleep(20)))a)--	200	10	3765
5	1	,(select*from(select(sleep(20)))a)	200	17	3764
6	1	'_'	200	17	3765
7	1	admin") or "1"="1"/*	200	11	3764
8	2	'	200	14	3765
9	2	(select*from(select(sleep(20)))a'	200	5	3764
10	2	'+(select*from(select(sleep(20)))a)+'	200	8	3765
11	2	and (select*from(select(sleep(20)))a)--	200	4	3764
12	2	,(select*from(select(sleep(20)))a)	200	18	3765
13	2	'_'	200	22	3764
14	2	admin") or "1"="1"/*	200	5	3765

This Is Not Limited To Burp Suite

```
└─$ sqlmap -r req.txt
```

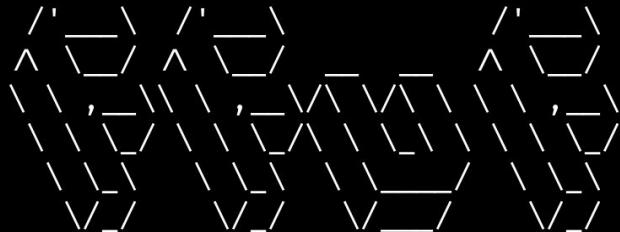


[!] legal disclaimer: Usage of sqlmap for attacking
. Developers assume no liability and are not respons

```
[02:22:11] [INFO] testing Generic UNION query (NULL) - 1 to 10 columns
[02:22:11] [WARNING] POST parameter 'password' does not seem to be injectable
[02:22:11] [CRITICAL] all tested parameters do not appear to be injectable. Tr
e is some kind of protection mechanism involved (e.g. WAF) maybe you could try
```

The Encryption Curse Affects All!

```
┌─[root@kali:~]─ ffuf -w usernames.txt:USER -w passwords.txt:PASS -request login.req -request Proto http clusterbomb -mc 302
```



v2.1.0-dev

The Encryption Curse Affects All!

```
[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 6ms]
 * PASS: super_strong_password
 * USER: guest

[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 12ms]
 * PASS: 123
 * USER: guest

[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 16ms]
 * PASS: super_strong_password
 * USER: portaladmin

[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 19ms]
 * PASS: wqwer
 * USER: admin@gmail.com

[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 25ms]
 * PASS: qesdgs6e56
 * USER: guest

[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 29ms]
 * PASS: 123
 * USER: admin@gmail.com

[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 32ms]
 * PASS: 123
 * USER: portaladmin

[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 36ms]
 * PASS: qesdgs6e56
 * USER: portaladmin

[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 39ms]
 * PASS: qesdgs6e56
 * USER: admin@gmail.com

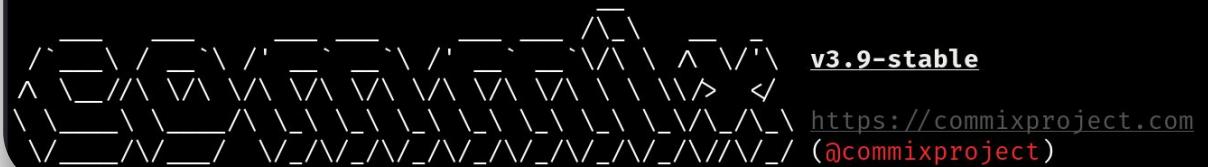
[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 43ms]
 * PASS: wqwer
 * USER: guest

[Status: 200, Size: 3342, Words: 195, Lines: 94, Duration: 46ms]
```

The Encryption Curse Affects All!

```
HTTP POST /login3.php HTTP/1.1
Host: localhost
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4453.89 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Content-Length: 101

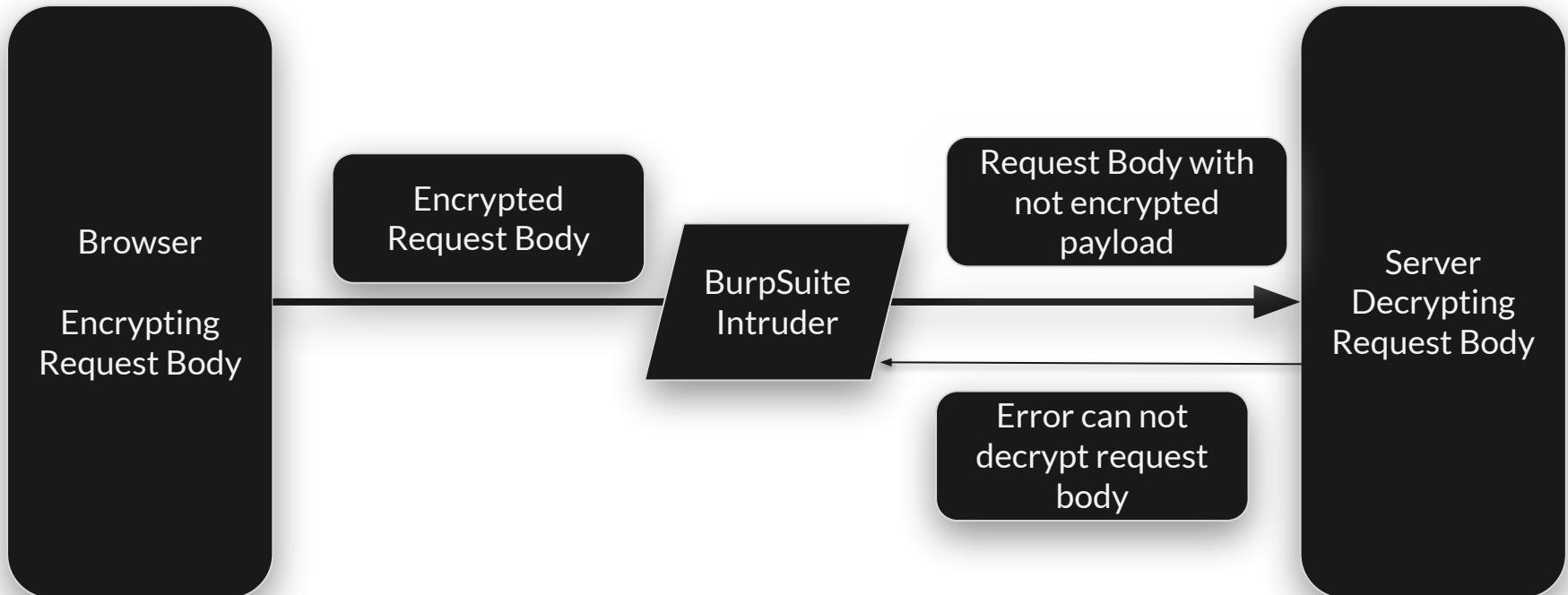
username=TC4aMNjPywcz0xgIm%2F7pUBfWzSwo01h5qz4fgv%2BrvJiKBumMeuUp6IX9xH3CpuO2%2FXJWE40KqPlJGfyzpuXc1ZBGMAR88eM44xKTg54meyCQq3eCNOfhru...&password=IeiNdFqc1SihQd%2FWhSIA4JJF0KXduem%2FARfabv%2B0wXGj0J8dAaJg51lxDdNp74HQ2GYS...&submit=Login
```



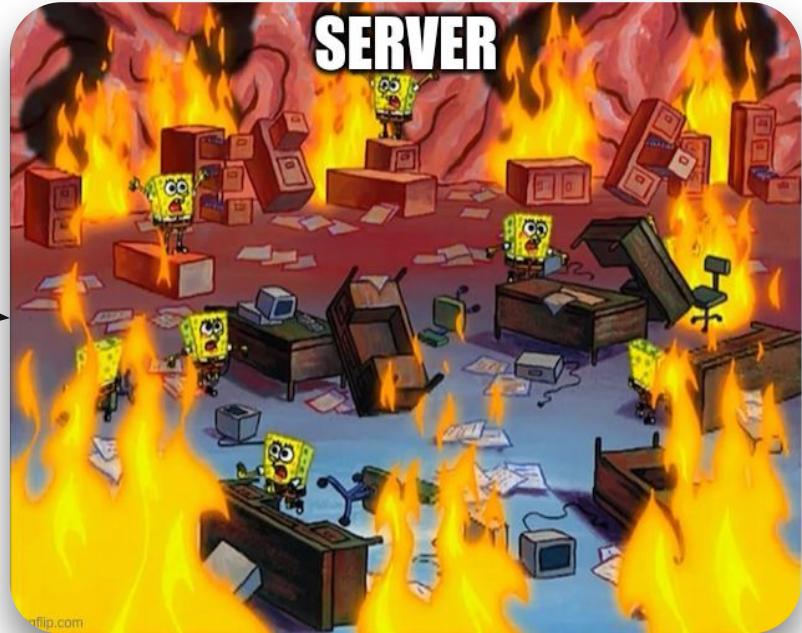
v3.9-stable
<https://commixproject.com>
(@commixproject)

```
[17:57:40] [info] Testing the (semi-blind) tempfile-based injection technique.
[17:57:40] [warning] The tested POST parameter 'password' does not seem to be injectable.
[17:57:40] [error] All tested parameters appear to be not injectable. Try to increase value for '--level' option if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved, maybe you could try to use option '--alter-shell' and/or use option '--tamper' and/or switch '--random-agent'.
```

Attacking At HTTP Layer



Expectation



Reality

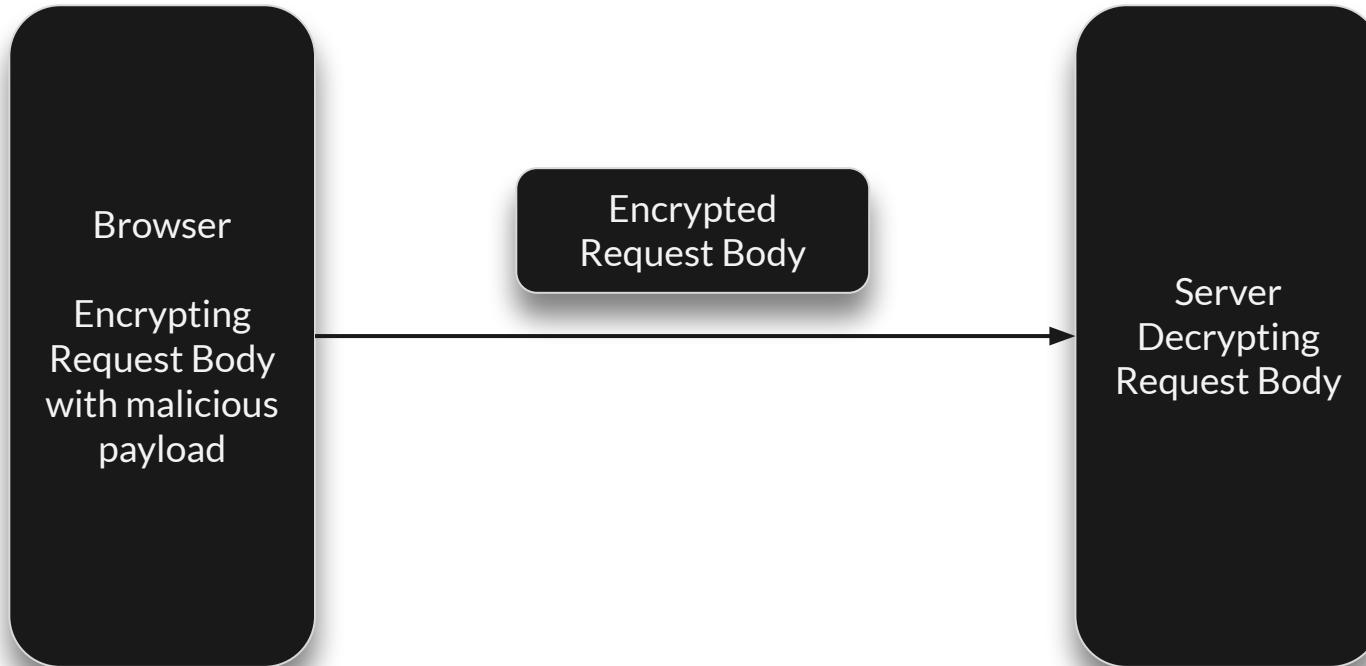


Pentester's Reaction

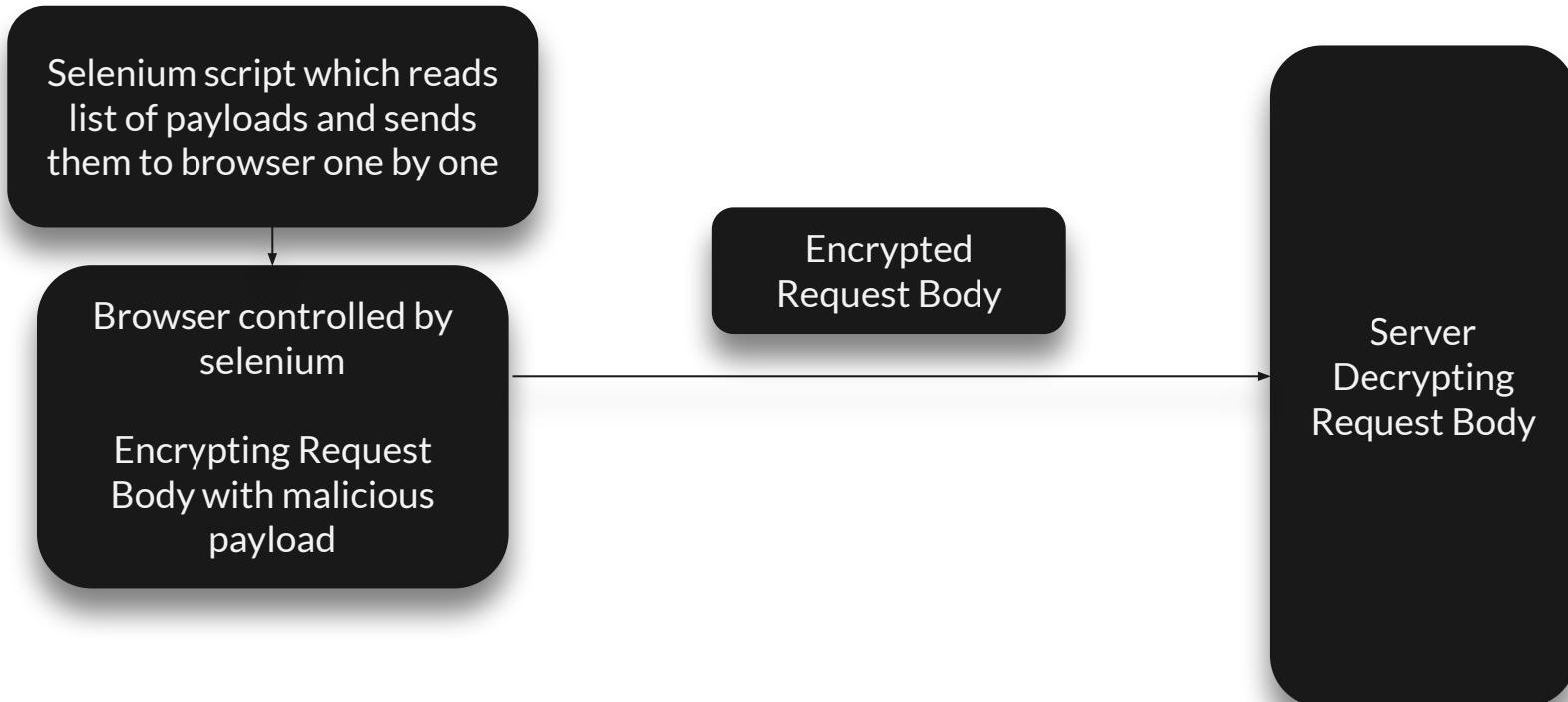


so what is The Solution?

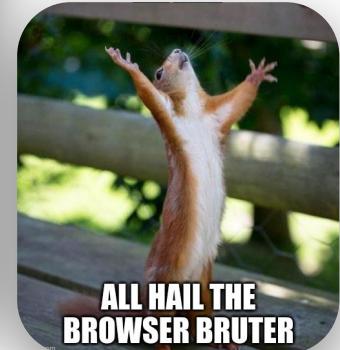
Solution - The Browser-Bruter



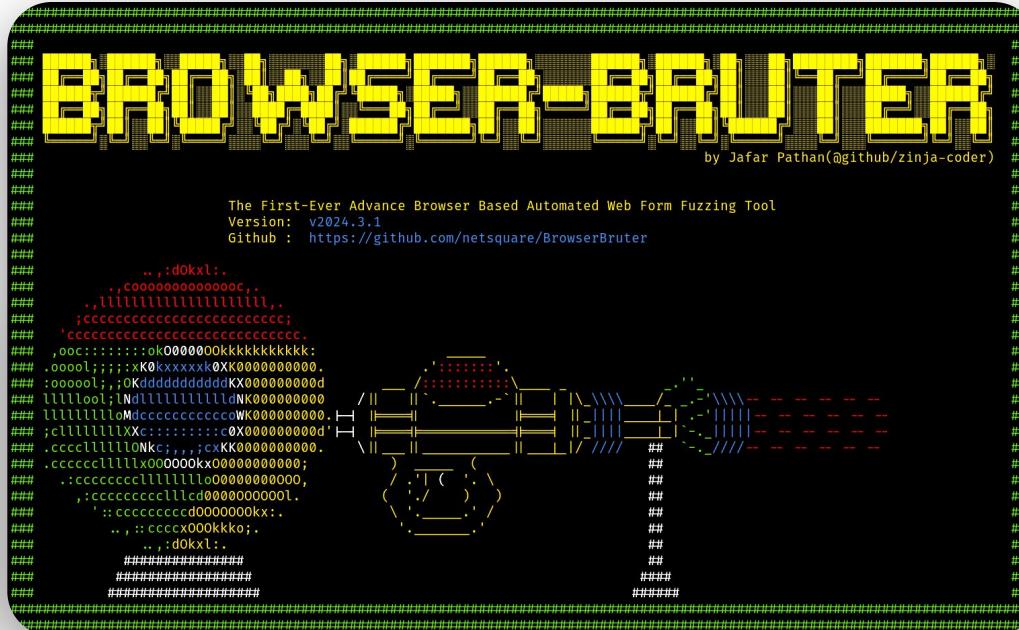
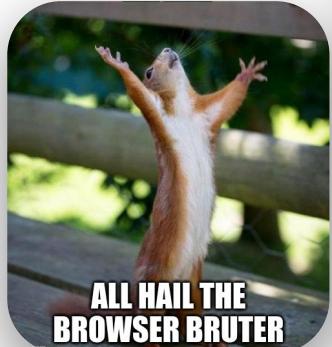
Converting The Solution Into A Tool



And The Browser Bruter Is Born!

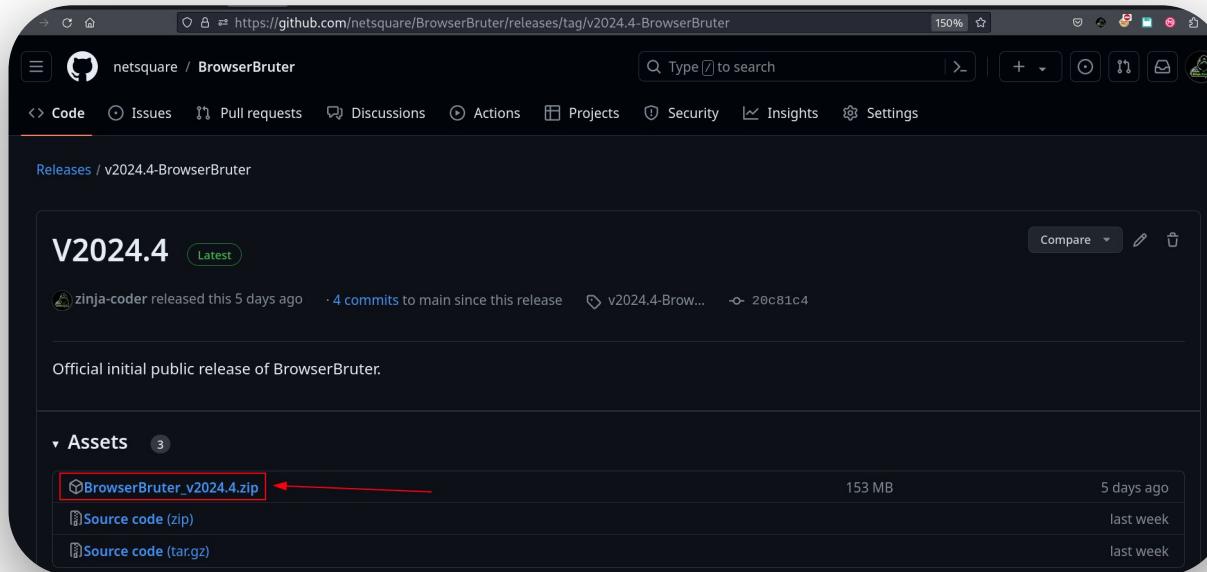


The First Ever Browser Based Fuzzing Tool



Download The Browser Bruter

[https://github.com/netsquare/BrowserBruter/releases/tag/v2024.4-
BrowserBruter](https://github.com/netsquare/BrowserBruter/releases/tag/v2024.4-BrowserBruter)



Installation

```
pip3 install -r requirements.txt
```

```
━ ディレクトリ > pip3 install -r requirements.txt
```

For troubleshooting and comprehensive guide on installation, kindly refer the documentation -
<https://net-square.com/browserbruter/SetupInstallation/>

Let's Have A Rematch

```
━[✗--> python3 BrowserBruter.py --elements username,password --payloads sqli.txt --target http://localhost/login3.php --button btn-default --attack 1 --fill username,password]
```

Attack In Progress

```
[+] ----- [+]
[+] Start Time : 2024-04-04_22-03-59
[+] Target URL : http://localhost/login3.php
[+] Attack Mode: SNIPER
[+] Elements   : username,password
[+] Payloads   : sql.txt
[+] Button     : btn-default
[+] ----- [+]
```

```
[+] ----- [+]
INFO: Press ENTER to pause the attack.
[+] ----- [+]
```

Fuzzing Progress for Browser → 0: 29% 

| 4/14 [00:06<00:15, 1.59s/iteration]

Attack In Progress

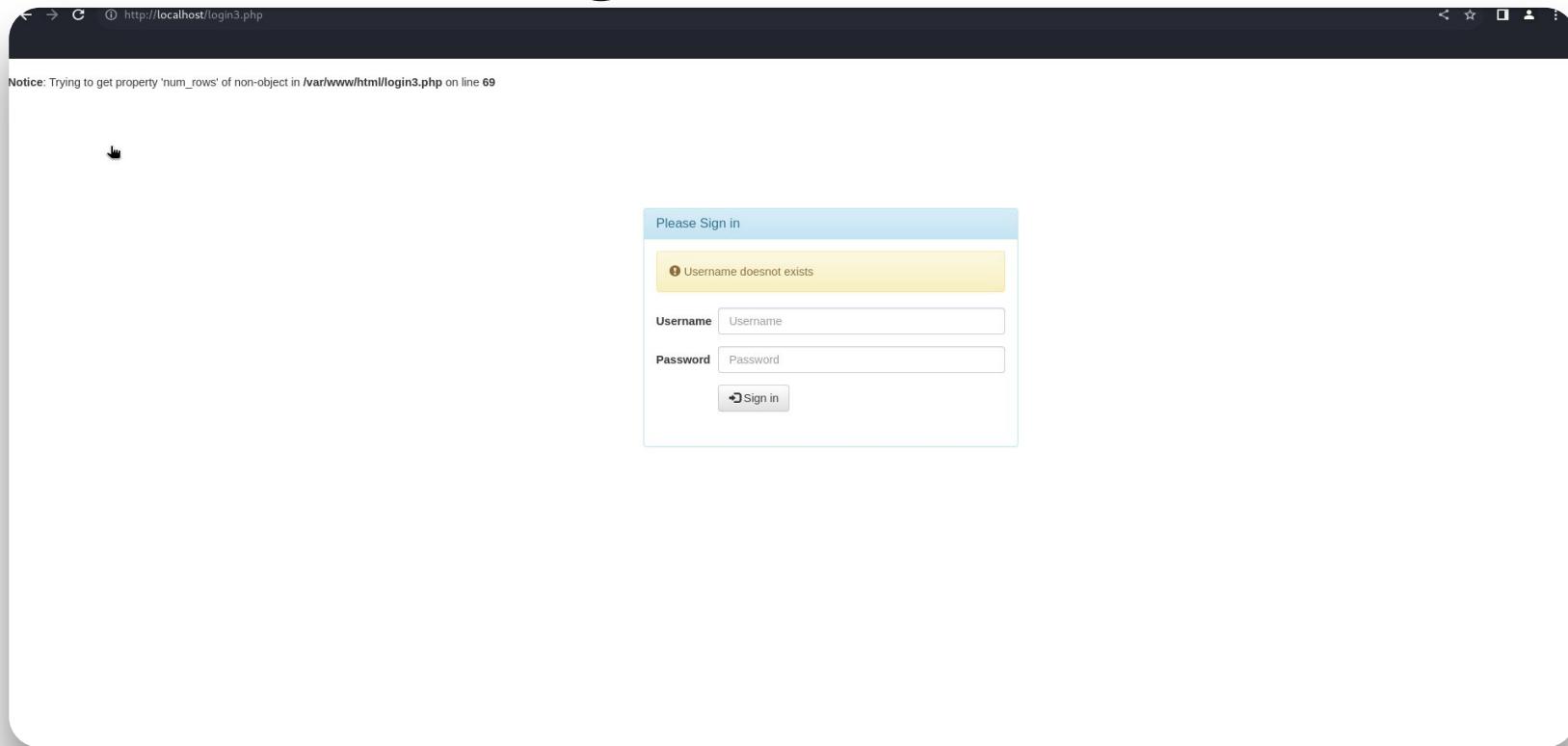
Please Sign in

Username

Password

 **Sign in**

Attack In Progress



Attack Finished

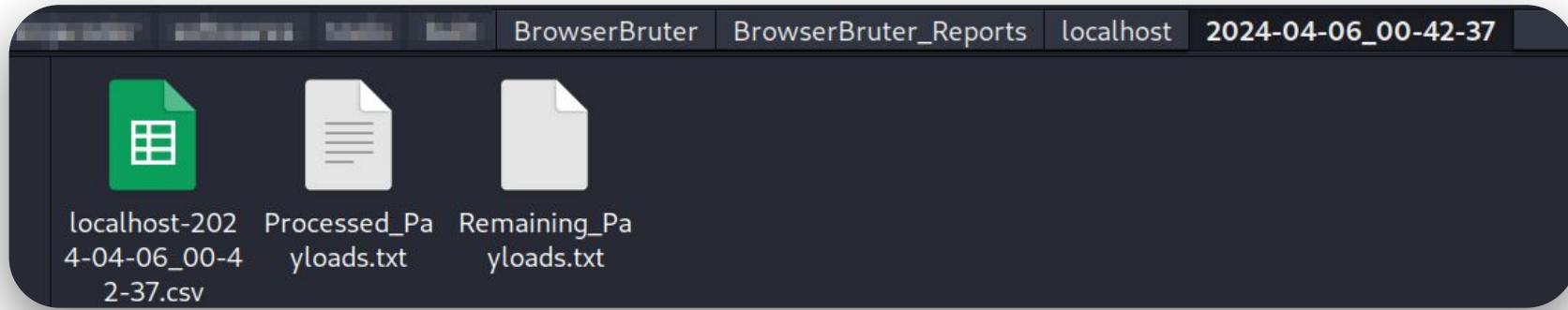
```
[+] ----- [+]
INFO: Remaining Payloads (if any) have been stored → BrowserBruter_Reports/localhost/2024-04-05_22-26-16/Remaining_Payloads.txt
[+] ----- [+]
```

```
[+] ----- [+]
INFO: Processed Payloads (if any) have been stored → BrowserBruter_Reports/localhost/2024-04-05_22-26-16/Processed_Payloads.txt
[+] ----- [+]
```

```
[+] ----- [+]
INFO: Report Generated → BrowserBruter_Reports/localhost/2024-04-05_22-26-16/localhost-2024-04-05_22-26-16.csv
[+] ----- [+]
```

```
[+] ----- [+]
INFO: Fuzzing end time → 2024-04-05_22-33-55 Total Running time → 0:07:39
[+] ----- [+]
```

Attack Finished



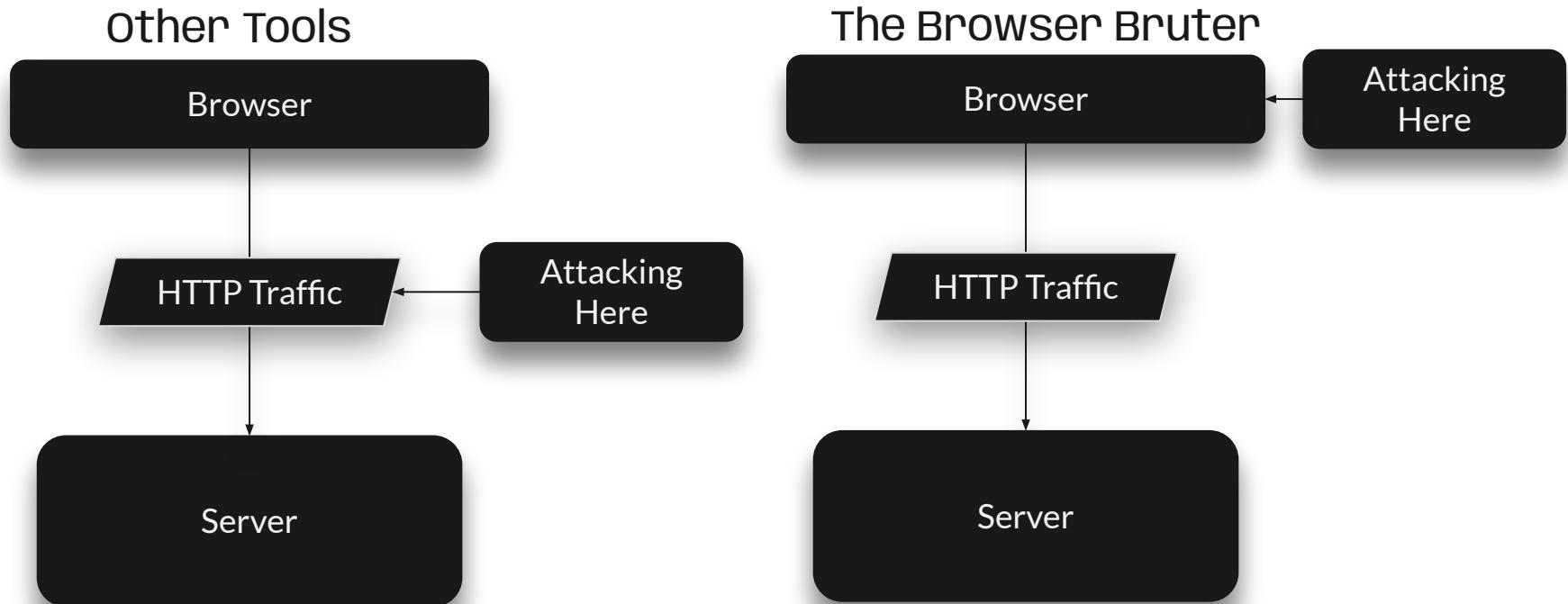
What Next? A Report Viewer Tool For Browser-Bruter

- A GUI based report viewer tool to analyze the results of the attack.
- Bundled with various utilities to search, filter and sort the results.
- A detailed panel to view and analyse the HTTP traffic requests/responses.
- User Friendly UI inspired from Burp Suite UI.
- We will look into it later. Let's continue with our attack.

We Found Time Based SQL Injection

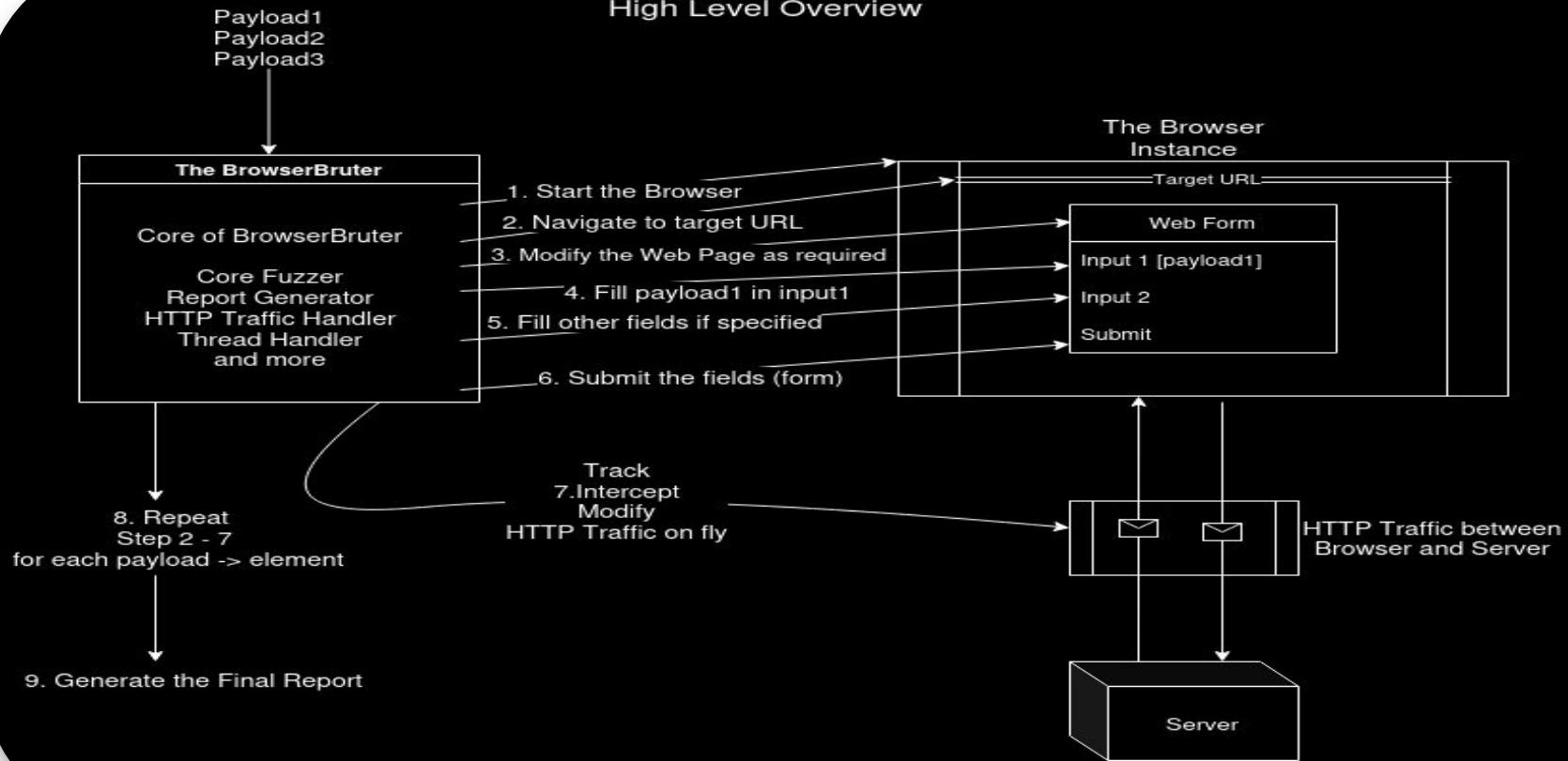
	Payload	Method	URL	Response Time	Cycle Time MilliSeconds	R
	'+(select*from(select(sleep(1) POST	POST	http://localhost/login3.php	2024-04-04 22:04:50	40050	200
	'	POST	http://localhost/login3.php	2024-04-04 22:05:00	57	200
	admin") or "1"="1"/*	POST	http://localhost/login3.php	2024-04-04 22:05:04	54	200
	,(select*from(select(sleep(2) POST	POST	http://localhost/login3.php	2024-04-04 22:04:57	54	200
	'+(select*from(select(sleep(1) POST	POST	http://localhost/login3.php	2024-04-04 22:04:52	53	200
	'	POST	http://localhost/login3.php	2024-04-04 22:05:01	52	200
	and (select*from(select(slee	POST	http://localhost/login3.php	2024-04-04 22:04:55	52	200
	\'	POST	http://localhost/login3.php	2024-04-04 22:04:06	51	200
	and (select*from(select(slee	POST	http://localhost/login3.php	2024-04-04 22:04:53	51	200
	,(select*from(select(sleep(2) POST	POST	http://localhost/login3.php	2024-04-04 22:04:58	50	200
	(select*from(select(sleep(2C) POST	POST	http://localhost/login3.php	2024-04-04 22:04:08	49	200
	\'	POST	http://localhost/login3.php	2024-04-04 22:04:04	49	200
	admin") or "1"="1"/*	POST	http://localhost/login3.php	2024-04-04 22:05:03	49	200
	(select*from(select(sleep(2C) POST	POST	http://localhost/login3.php	2024-04-04 22:04:07	48	200
	\'	GET	http://localhost/login3.php	2024-04-04 22:04:02	7	200
	admin") or "1"="1"/*	GET	http://localhost/login3.php	2024-04-04 22:05:03	6	200
	'+(select*from(select(sleep(1) GET	GET	http://localhost/login3.php	2024-04-04 22:04:51	6	200
	'+(select*from(select(sleep(1) GET	GET	http://localhost/login3.php	2024-04-04 22:04:09	5	200

Attacking At The Browser Layer



The General Working Flow Of BrowserBruter

High Level Overview



4 Problems 1 Solution

- Completely bypasses the **encryptions** affecting HTTP traffic
- Creates a way to bypass **captchas** by allowing the pentester to manually perform the required human interactions and then proceed to payload insertions
- Can fuzz **front-end** when there is **no HTTP traffic**, for example when Input is utilized on the client side, i.e. when you want to brute force OTP input which is validated on the client side, so there is no HTTP Traffic
- Removes the burden of **session management**, auth handling and other micro management like CSRF handling while using HTTP proxy tools.

Features Sneak Peek

Multiple Attacks

Supports four different types of attack modes including -
1. Sniper 3. Pitch Fork
2. Battering Ram 4. Cluster Bomb

stealthy and Fast

Uses advance browser and python libraries to hide itself from bot detection mechanisms. Also has options to increase speed of fuzzing.

Log Tracking

Keeps extensive logs of errors and all http traffics.

Session Handling

Has various advance options to handle the session mechanism including cookie support, custom header support and many more.

Bypasses Defences

Bypasses various HTML defense mechanism completely to allow error free fuzzing.

Javascript support

Has various options to handle javascript including executing javascript code, removing and replacing javascript code.

Tons Of Options

- There are more than **40+ options** available
- This includes -
 - Basic Options
 - Attack Mode Options
 - Fuzzing Options
 - Browser Options
 - Session Handling Options
 - The Python Scripting Engine
 - JavaScript and Navigation Handling Options
 - Debug Options
 - Report Generation Options

Multiple Attack Modes

- SNIPER
- BATTERING RAM
- PITCHFORK
- CLUSTER BOMB

Multiple Attack Modes - Let's Brute Force The Login Page

Please Sign in

Username	<input type="text" value="Username"/>
Password	<input type="password" value="Password"/>
 Sign in	

Multiple Attack Modes - Let's Brute Force The Login Page

```
▶ ⌘=-- ××> python3 BrowserBruter.py --elements-payloads username:us  
ernames.txt,password:passwords.txt --target http://localhost/login3  
.php --button btn-default --attack 4 --remove-session █
```

Multiple Attack Modes - Let's Brute Force The Login Page

```
[+]-----[+]
[+] Start Time : 2024-04-05_00-25-51
[+] Target URL : http://localhost/login3.php
[+] Attack Mode: CLUSTER BOMB
[+] Elements:Payloads: username: usernames.txt
[+] Elements:Payloads: password: passwords.txt
[+] Button      : btn-default
[+]-----[+]
```

```
[+]-----[+]
INFO: Press ENTER to pause the attack.
[+]-----[+]
```

Fuzzing Progress for Browser → 0: 33%  | 4/12 [0]

And We Got The Credentials

Index	Request Time	Fuzzing	Payload	Method	URL	Response Time	Cycle Time MilliSeconds	Response Status Code	Response Length
3	2024-04-05 00:25:57	['username', 'password']	('portaladmin', 'super_strong_password')	POST	http://localhost/login3.p	2024-04-05 00:25:57	52	302	3050
13	2024-04-05 00:26:02	['username', 'password']	('admin@gmail.com', 'qesdg3oe56')	GET	http://localhost/login3.p	2024-04-05 00:26:02	5	200	1084
5	2024-04-05 00:26:02	['username', 'password']	('admin@gmail.com', 'qesdg3oe56')	GET	http://localhost/login3.p	2024-04-05 00:26:02	5	200	1084

ds	Response Status Code	Response Length
	302	3050
	200	1084

Fuzzing	Payload
['username', 'password']	('portaladmin', 'super_strong_password')
['username', 'password']	('admin@gmail.com', 'qesdg3oe56')

Let's Check If They Are Correct

Please Sign in

Username

portaladmin

Password

••••••••••••••••|

➔ Sign in

And We Are In!

The screenshot shows a web-based dashboard interface for NetSquare. At the top, there's a header bar with a back button, a refresh button, and a URL field containing "localhost/dashboard.php". The header also includes a zoom level of "150%", a star icon, and several system icons.

The main content area features a navigation bar with links: Dashboard, Brand, Category, Product, Orders, Report, Import Brand, and a user profile icon. Below this, there are three main data cards:

- Total Product**: A green card with the number "04" in white. It also displays the date "Thursday 04, 2024".
- Low Stock**: A pink card with the number "2" in white.
- Total Orders**: A blue card with the number "6" in white.

On the right side of the dashboard, there's a section titled "User Wise Order" which lists orders by user name and total value in rupees:

Name	Orders in Rupees
portaladmin	320400
Nishith	45176.4

You Are In Control - User Interactions

- Pause the attack on browser startup (manually login, or perform some interaction)
- Can run Browser Bruter in Powerful **Interactive Mode**
- Pause/Resume the attack in the middle
- Get in/out of the **Interactive Mode**
- Stop Current Attack
- Resume Previous Closed/Crashed/Stopped Attack (Attack Mode 1&2)

You Are In Control - Pause Menu

[+]

[+]

WARNING: BROWSERBRUTER IS PAUSED

press ENTER to resume

Press y to Enter Interactive Mode

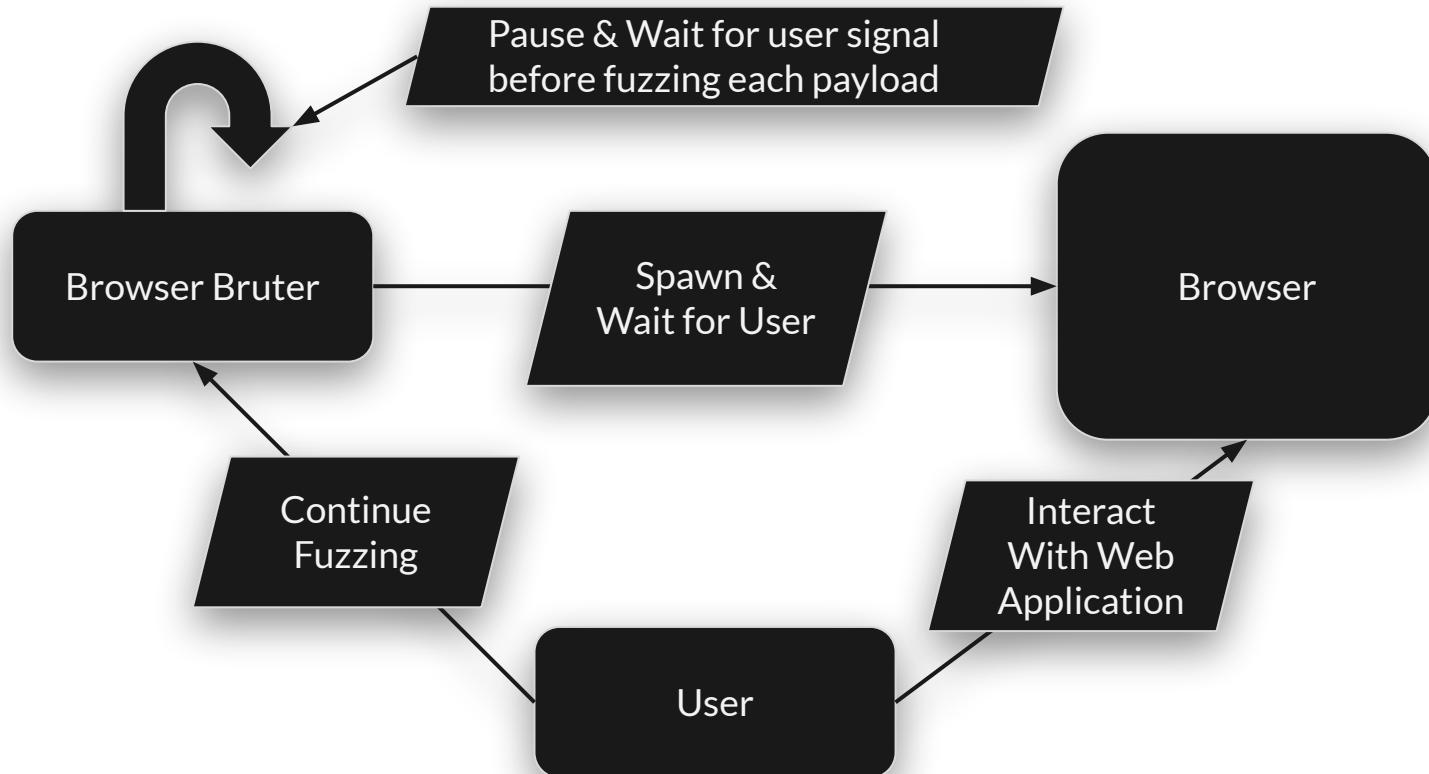
Press n to Exit Interactive Mode

Press CTRL+C to exit

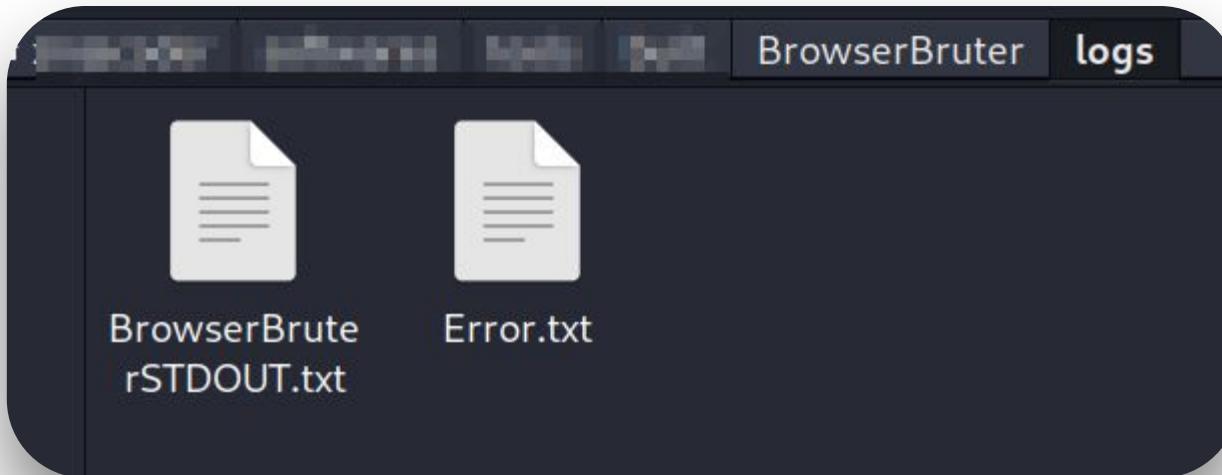
[+]

[+]

The Interactive Mode



The Log Tracking Mechanism



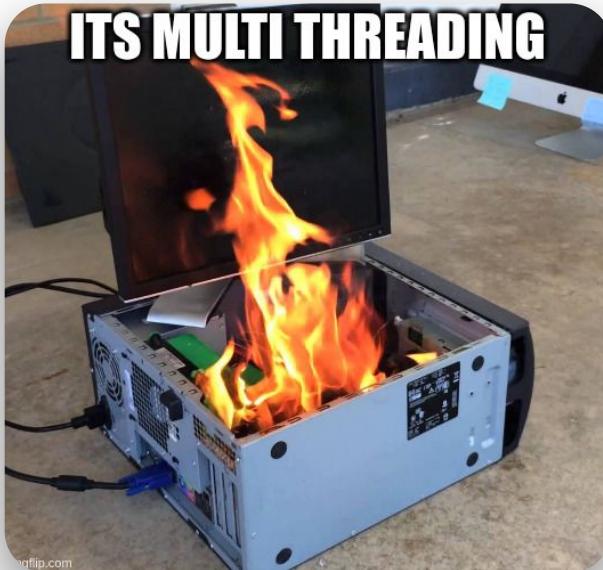
Control The Verbosity

```
[+]-----Single Request/Response Cycle-----[+]
Fuzzing - username
Payload - \
[+]-----REQUEST-----[+]
Time - 2024-04-06 11:10:22
POST http://localhost/login3.php
Host: localhost
Proxy-Connection: keep-alive
Content-Length: 767
Cache-Control: max-age=0
sec-ch-ua: "Not(A:Brand";v="24", "Chromium";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/login3.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=sh9ssr4t074g5ql20n5coo83mf; _ga=GA1.1.1776304807.1712382022; _ga_4V4HC9K0Z6=GS1.1.1712382021.1.0.1712382021.0.0.0

username=gvua2ZTXah2BX5P/TE1lr+3AIblbFqbj1lIViRUm/SEUMbOesRd0wnqL8WCsdt5FRLnKcRrSvSG48anG4VsYUGrlmLi3kRXfgeI++E9VSAbhnA/XGL0z2f38bBmbatyWWAlJ5z5hbDiIFkWWqe08
1SrERMees+4k/1uSyLU/C/D043DrAUq/eUAElv0VQT2Y06/jl39vB0v0rI05mg1+KJrnIo4BhBbPAnTywmTX5SSEi/9LN22rzblN7pylRTociIsY9Y+bGL2IFjYe7Pb2oC+hequHwroBuql04XTkMbt2gH3Ya
6MHj79LSzjakPKjxP3wiwsYcqsh++Loni3qdJxg==&password=fBxcOVdqYH96ir6kxJ4LGAT10xTdk9AbGa2hAS3C6RSmqkDeKvuPt0bxkcDQ94duBmeDU99jD11r7yt0Jb3LaXaS5e08vo5xyxrj6H0ygmv
uzm7bKrNoen7XPBw+80k3FbE9FoVu hvakvcCZM8KSE5jpDYFnxFwEDJPUKbKbfjzX/Ytn6rh502IaSGK8s812JywJJGfZhqEJPnU/10jtmt09LcWTkKx25fJYQWhwCR3zh3qEapSz/CR/cZssGUxthCX/KiJP
8isSZJgibJWNA5U/WG55z1xG9yZi81oIBjWKhUmXqUZskEtK2bT21iv/P6j3d6/K33rlw9oHCnIqNQ==
```

It's Time for The THREADS.....

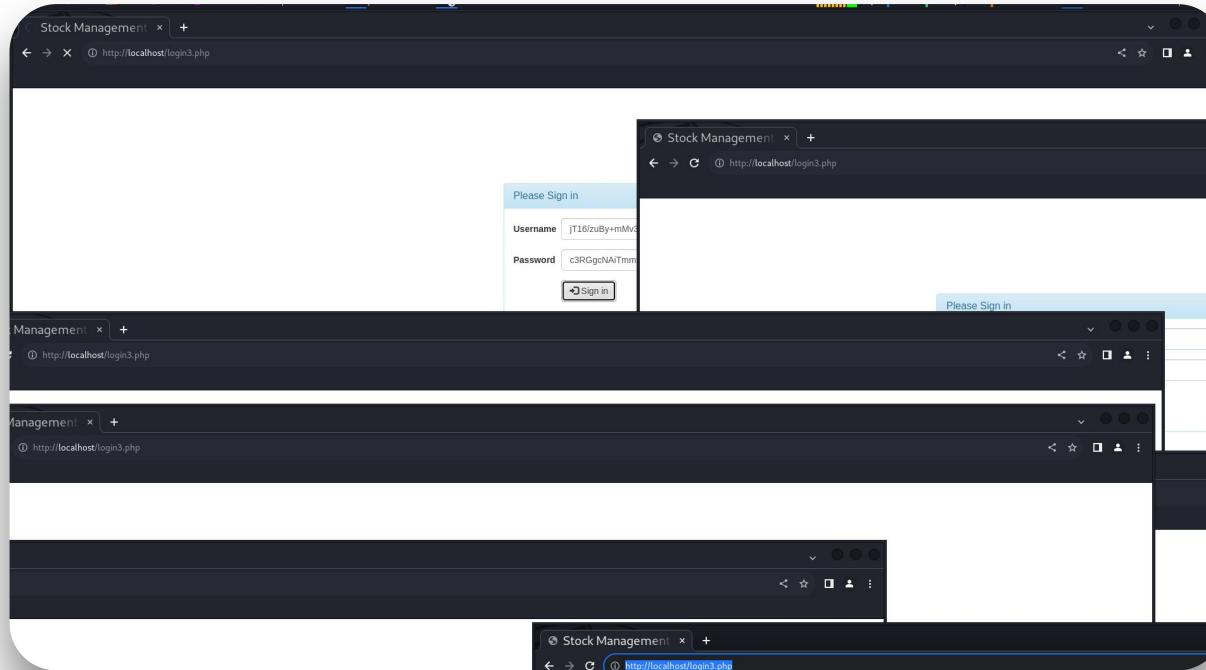
The Browser Bruter can run not 2, not 3, not 5, not 10 ... But upto 20 threads!



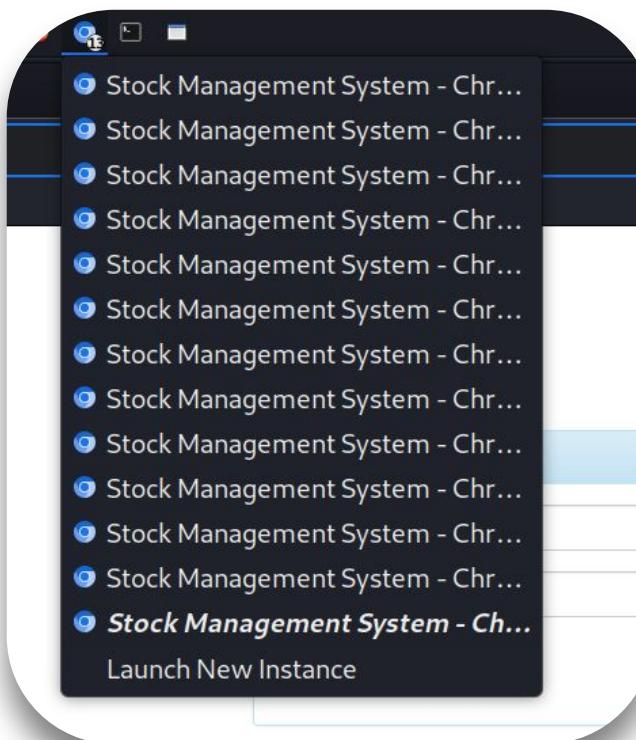
THREADS.....

```
━ ディレクトリ> python3 BrowserBruter.py --elements username,password --payloads fuzz.txt --target http://localhost/login3.php --button btn-default --attack 1 --fill username,password --threads 20 --delay-before 0.3
```

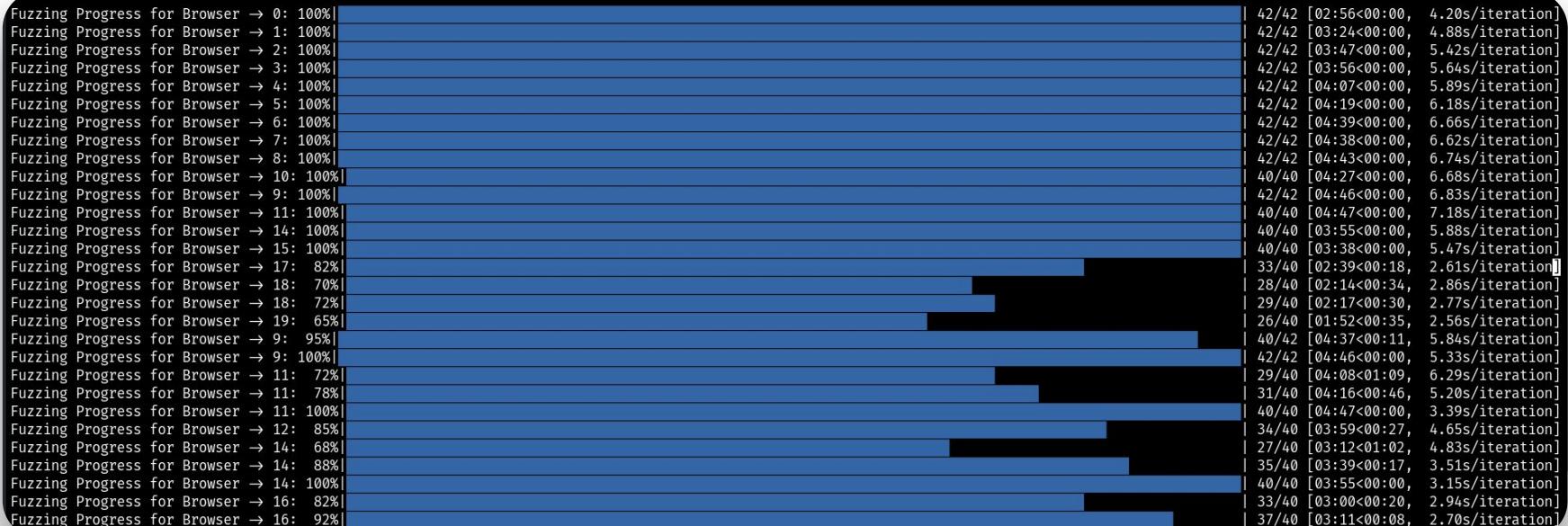
Controlling Multiple Browsers



Controlling Multiple Browsers



Controlling Multiple Browsers



Extensible - The Art of Browser Automation

- The functionality of the browser bruter can be extended using javascript and Python.
- Penetration Tester can write javascript code which will be executed on the browser to further automate the browser as per need.
- Unlocks countless possibilities to tackle various scenarios where only limitation is finding the right javascript code.
- Truly gives the power in the hand of the pentester.

Extending The Browser Bruter

The screenshot shows a web-based application interface for managing brands. At the top, there's a navigation bar with tabs for Dashboard, Brand (which is active), Category, Product, Orders, Report, Import Brand, and User profile. Below the navigation, a breadcrumb trail indicates the current location: Home / Brand. A sub-header 'Manage Brand' is visible above the main content area.

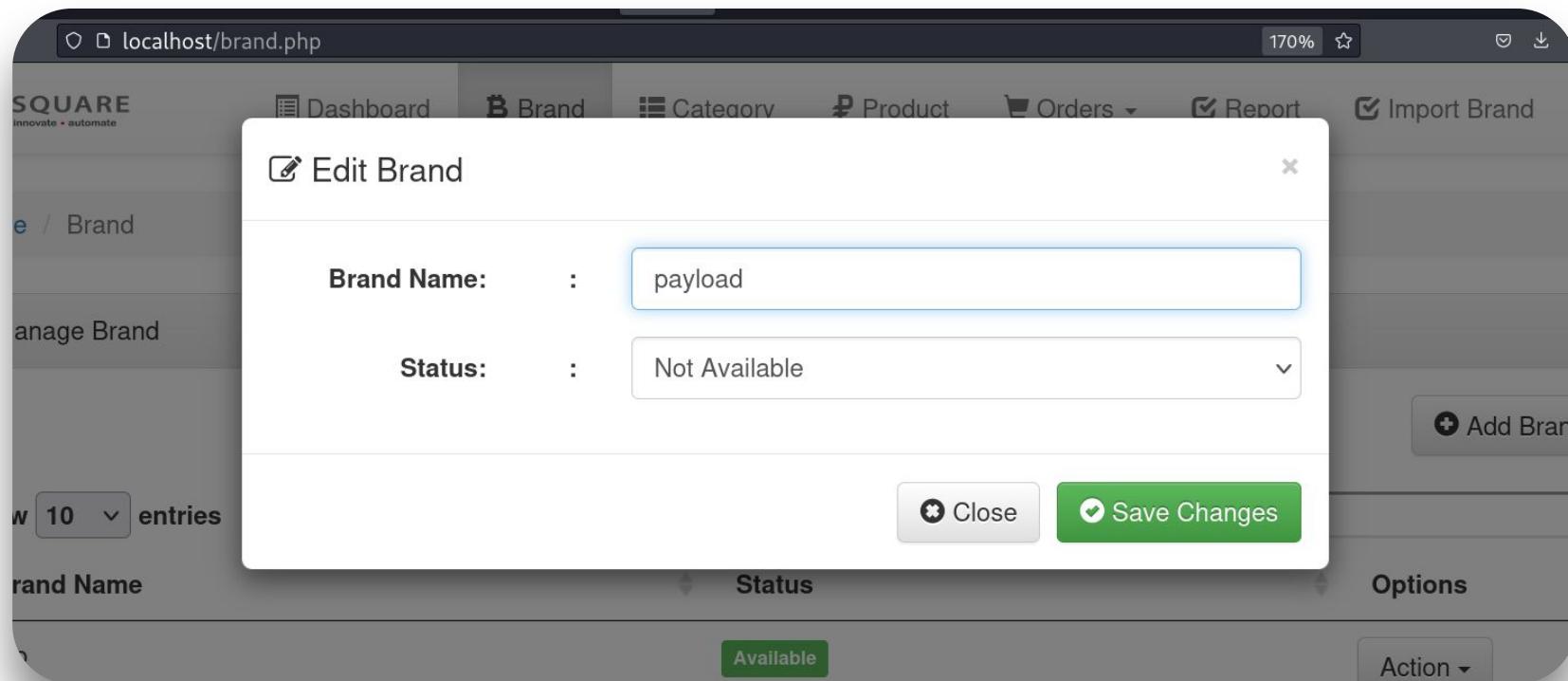
The main content area displays a table of brand entries. The columns are labeled 'Brand Name', 'Status', and 'Options'. The first entry, 'Vivo', has a status of 'Available' and an 'Action' button. The second entry, 'Oppo', also has a status of 'Available' and an 'Action' button. A red arrow points from the text 'Action' in the 'Vivo' row's 'Options' column to the 'Action' button itself, indicating it is the target of the extension. On the right side of the table, there are buttons for 'Add Brand' and 'Search'.

Brand Name	Status	Options
Vivo	Available	Action ▾
Oppo	Available	Action ▾

Extending The Browser Bruter

Brand Name	Status	Options
Vivo	Available	Action ▾
Oppo	Available	 Action ▾
Samsung	Available	Action ▾

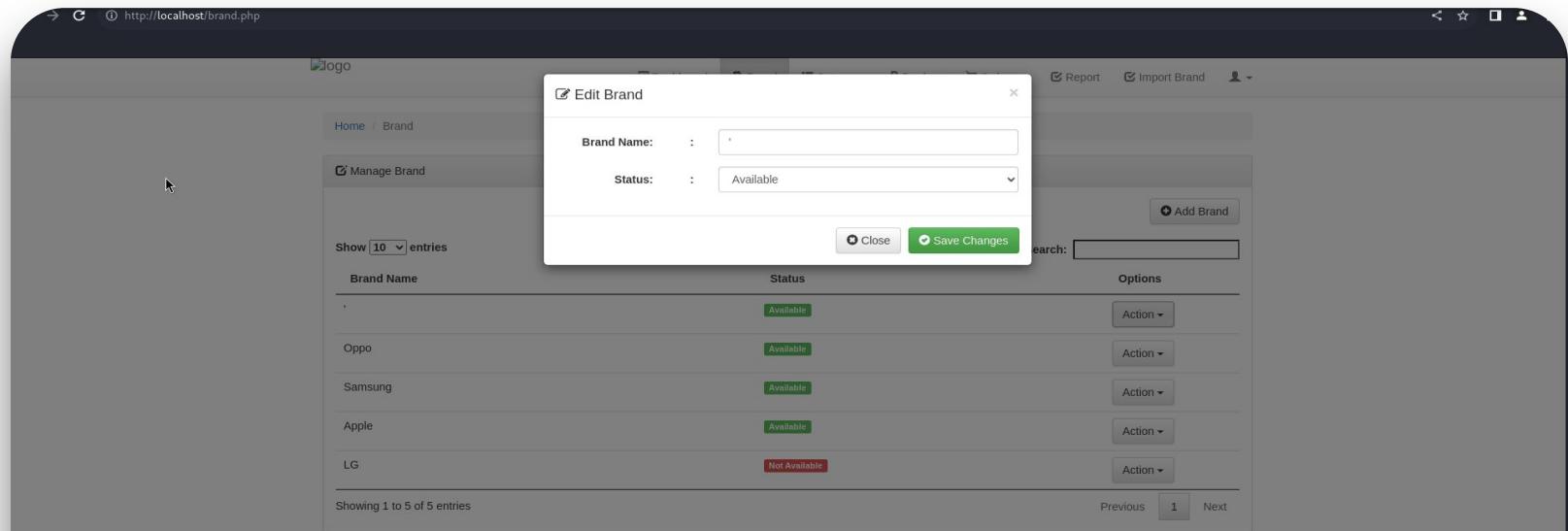
Extending The Browser Bruter



Extending The Browser Bruter

```
→ ディレクトリ> python3 BrowserBruter.py --elements editBrandStatus,editBrandName,brandId --payloads sql.txt --button editBrandBtn --target http://localhost/brand.php --cookie PHPSESSID:ujmrhk6esu84l8r2i2h2ee7f2 --attack 1 --delay-before 0.3 --fill editBrandName --javascript "document.querySelector('button.btn.btn-default.dropdown-toggle').click(); document.querySelector('a[data-target=\\"#editBrandModel\\"]')click();"
```

Extending The Browser Bruter



The Python Scripting Engine



Extensible - The Python Scripting Engine

- Even more powerful than Javascript
- Allows you to control browser directly using 'driver' object
- Use Javascript for single page automation, Use Python for complex automation.
- Allows you to literally do whatever you want to do on browser for example write a python script to bypass captcha and integrate that with Browser Bruter
- Explaining Python Scripting Engine is beyond the capability of this Presentation, Refer Documentation.

Extensible - The Python Scripting Engine

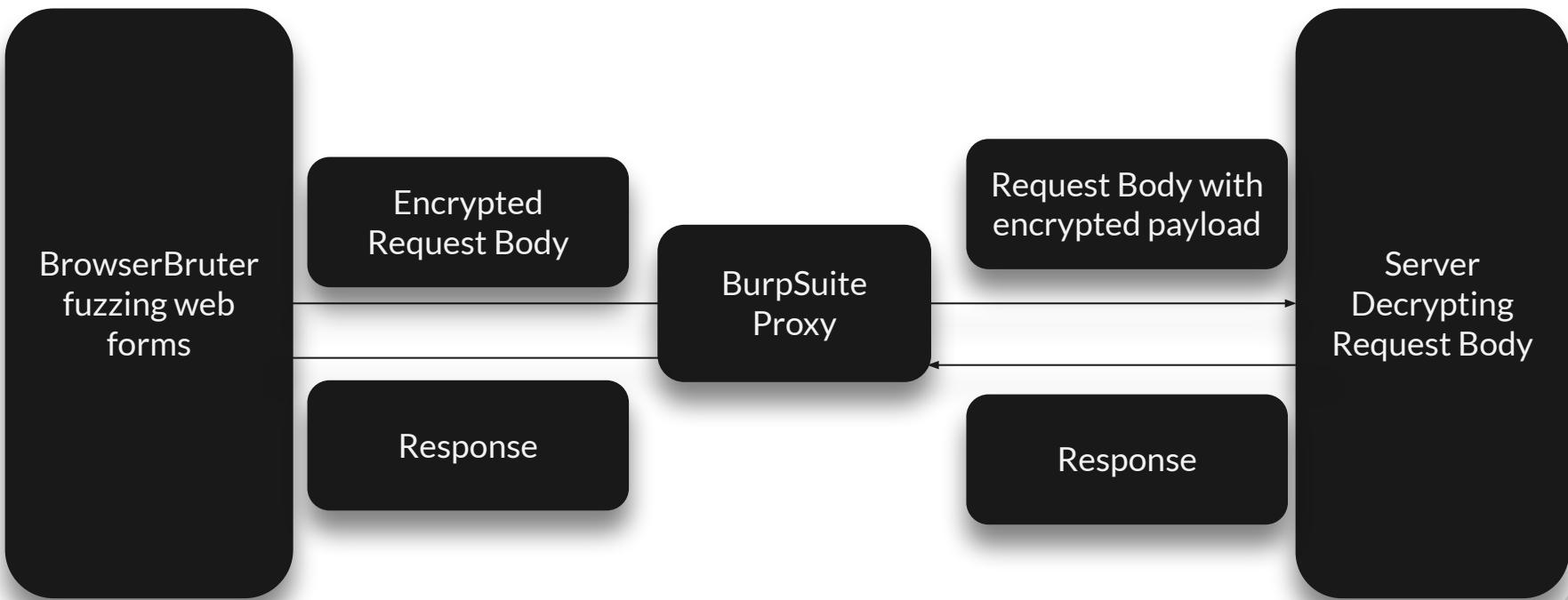
- python3 BrowserBruter.py --elements mfa-code --button submit --target https://<LAB-ID>.web-security-academy.net/login --cookie session:<COOKIE> --attack 1 --payloads mfa.txt --**python 'driver.find_element(By.NAME, 'username').send_keys('carlos');**
driver.find_element(By.NAME,'password').send_keys('montoya');
driver.find_element(By.XPATH,
'/html/body/div[2]/section/div/section/form/button').click();'

Note: Above code demonstrates automation only, does not solves the lab

Extensible - The Art of Browser Automation

- Unlocks countless possibilities to tackle various scenarios where only limitation is finding the right javascript code and python code
- Truly gives the power in the hand of the pentester
- Do whatever you want to do, only barrier is coding and imagination

BurpSuite Support The `--proxy` option



BurpSuite Support The `--proxy` Option

```
▶ ディレクトリ> python3 BrowserBruter.py --elements username  
,password --payloads sqli.txt --target http://localhost  
/login3.php --button btn-default --attack 1 --fill user  
name,password --proxy http://127.0.0.1:8080
```

BurpSuite Support The `--proxy` option

Intercept HTTP history WebSockets history Proxy settings

Logging of out-of-scope Proxy traffic is disabled Re-enable

#	Host	Method	URL	Params	Edited	Status code	Length	MIME type	Extension	Title	Notes	TLS	IP
57	http://localhost	GET	/login3.php		✓	200	3578	HTML	php	Stock Management Sy...		127.0.0.1	
56	http://localhost	POST	/login3.php			200	3543	HTML	php	Stock Management Sy...		127.0.0.1	
55	http://localhost	GET	/login3.php			200	3578	HTML	php	Stock Management Sy...		127.0.0.1	
54	http://localhost	POST	/login3.php		✓	200	3527	HTML	php	Stock Management Sy...		127.0.0.1	
53	http://localhost	GET	/login3.php			200	3578	HTML	php	Stock Management Sy...		127.0.0.1	
52	http://localhost	POST	/login3.php		✓	200	3527	HTML	php	Stock Management Sy...		127.0.0.1	
51	http://localhost	GET	/login3.php			200	3578	HTML	php	Stock Management Sy...		127.0.0.1	
50	http://localhost	POST	/login3.php		✓	200	3527	HTML	php	Stock Management Sy...		127.0.0.1	
49	http://localhost	GET	/login3.php			200	3578	HTML	php	Stock Management Sy...		127.0.0.1	
48	http://localhost	POST	/login3.php		✓	200	3527	HTML	php	Stock Management Sy...		127.0.0.1	
47	http://localhost	GET	/login3.php			200	3578	HTML	php	Stock Management Sy...		127.0.0.1	
46	http://localhost	POST	/login3.php		✓	200	3527	HTML	php	Stock Management Sy...		127.0.0.1	
45	http://localhost	GET	/login3.php			200	2270	HTML	html	Stock Management Sy...		127.0.0.1	

Filter settings: Hiding CSS, image and general binary content

Request

Pretty Raw Hex

```
1 POST /login3.php HTTP/1.1
2 Host: localhost
3 Content-Length: 763
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not(A:Brand";v="24", "Chromium";v="122"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,
image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;
q=0.7
13 Sec-Fetch-Site: same-origin
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Fri, 05 Apr 2024 19:12:50 GMT
3 Server: Apache/2.4.38 (Debian)
4 X-Powered-By: PHP/7.4.16
5 Expires: Thu, 19 Nov 1981 08:52:00 GMT
6 Cache-Control: no-store, no-cache, must-revalidate
7 Pragma: no-cache
8 Vary: Accept-Encoding
9 Content-Length: 3215
10 Connection: close
11 Content-Type: text/html; charset=UTF-8
12
13
14 <!DOCTYPE html>
15 <html>
16   <head>
17     <title>
```

BurpSuite Support The `--proxy` Option

#	Host	Method	URL	Params	Edited	Status code
62	http://localhost	POST	/login3.php	✓		200
61	http://localhost	GET	/login3.php			200
60	http://localhost	POST	/login3.php	✓		200
59	http://localhost	GET	/login3.php			200
58	http://localhost	POST	/login3.php	✓		200
57	http://localhost	GET	/login3.php			200
56	http://localhost	POST	/login3.php	✓		200
55	http://localhost	GET	/login3.php			200
54	http://localhost	POST	/login3.php	✓		200
53	http://localhost	GET	/login3.php			200
52	http://localhost	POST	/login3.php	✓		200
51	http://localhost	GET	/login3.php			200
50	http://localhost	POST	"login3.php	✓		200

The Report Explorer

- A GUI based report viewer tool to analyze the results of the attack.
- Bundled with various utilities to search, filter and sort the results.
- A detailed panel to view and analyse the HTTP traffic requests/responses.
- User Friendly UI inspired from Burp Suite UI.
- Includes options like - '--report', '--grep', '--split'

The Report Explorer

BrowserBruter Report Explorer

Index	Request Time	Selected	Payload	Method	URI	Request Headers	Request Body	Response Time	Cycle Time
0	11-25-27	textarea	ORDER BY 15	GET	http://localhost:3000/favico	Host: localhost:3000		11-25-27	52
1	11-25-27	textarea	ORDER BY 15	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=M8VjSLOx-vRPHyNQ	11-25-27	52
2	11-25-30	select	ORDER BY 15	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=3kR14U60kysZOCbs7	11-25-30	67
3	11-25-33	yesno	ORDER BY 15	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=AAWXAnjd-YJdEuB1s	11-25-33	102
4	11-25-36	hobbies	ORDER BY 15	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=H6hxwPj98q51ZQK	11-25-37	78
5	11-25-40	phone	ORDER BY 15	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=Xbn342hR-Yg9FCBNs1	11-25-40	91
6	11-25-43	data	ORDER BY 15	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=LoGky7c-vz1vnKAkBk	11-25-43	81
7	11-25-47	time	ORDER BY 15	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=gP6t85nEp-ewynw80tg	11-25-47	62
8	11-25-50	calendar	ORDER BY 15	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=U837Xb1-mOBw9yQz	11-25-50	66
9	11-25-53	color	ORDER BY 15	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=fUfHQ11x-27kgo_ppr	11-25-53	64
10	11-25-56	textarea	ORDER BY 16	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=qEUo2yu-Qrhmeoxs	11-25-56	82
11	11-26-00	select	ORDER BY 16	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=846fdm1t-9yD-H9-NF	11-26-03	83
12	11-26-03	yesno	ORDER BY 16	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=WWo7Zls-zB-O97Dc	11-26-06	66
13	11-26-06	hobbies	ORDER BY 16	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=tODL8Rn-HngfCefu	11-26-10	67
14	11-26-10	phone	ORDER BY 16	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=tYfHsol-jpI42_65Wd	11-26-13	65
15	11-26-13	data	ORDER BY 16	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=6Pt85nEp-ewynw80tg	11-25-22	50
16	11-25-22	textarea	ORDER BY 15#	GET	http://localhost:3000/favico	Host: localhost:3000		11-25-22	50
17	11-25-22	textarea	ORDER BY 15#	POST	http://localhost:3000/submi	Host: localhost:3000	_csrf=BuTtvOkb-p2qBldhzkl	11-25-22	50

Request/Response Web Page Before/After

```
POST http://localhost:3000/submit
Host: localhost:3000
Proxy-Connection: keep-alive
Content-length: 224
Cache-Control: max-age=0
sec-ch-ua: "Not A Brand";v="8", "Chromium";v="120"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost:3000
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.0.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cookie: _csrf=d20p83pd1dq-Xt9yC0vT
._csrf=6Pt85nEp-ewynw80tgulBfk5FR3hm1My5soU&data=text&yesno=no&hobbies=reading&hobbies=writing&hobbies=painting&phone=9123456789&calendar=2023-06-17&time=0RDER+BY+15&color=%23ff0000&select=option1&textarea=randomTextAreaValue
```

HTTP/1.1 200 OK
X-Powered-By: Express
Content-Type: text/html; charset=utf-8
Content-Length: 312
ETag: W/"138-NOVjbkb0lhDjsE1SCWjN/ztfLY"
Date: Sat, 16 Dec 2023 05:55:46 GMT
Connection: keep-alive
Keep-Alive: timeout=5

<h1>
Received Data
</h1>
<p>
Data: text
</p>
<p>
Yes/No: no
</p>
<p>
Hobbies: reading, writing, painting
</p>
<p>
Phone Number: 9123456780
</p>
<p>
Calendar: 2023-06-17
</p>
<p>
Time: ORDER BY 15
</p>

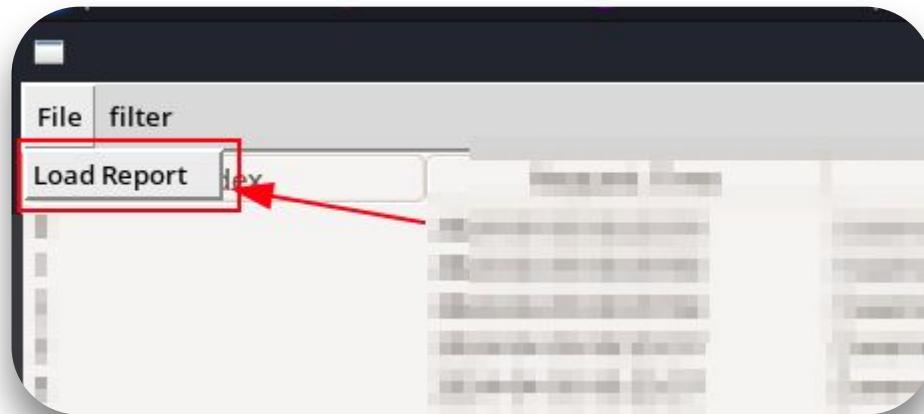
Loading The Report

1. Using `--report` option -

```
▶ ➔ python3 ReportExplorer.py --report BrowserBrowser_Reports/localhost/2024-04-05_00-25-51/localhost-2024-04-05_00-25-51.csv
```

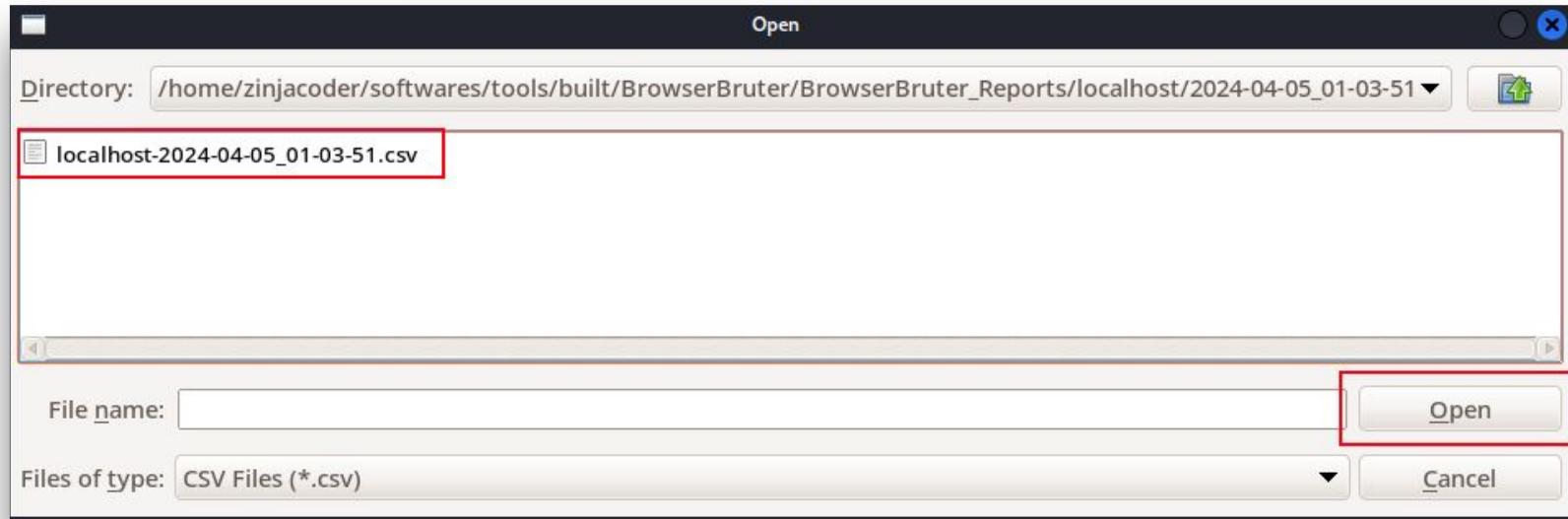
Loading The Report

2. Loading from 'Load Report' option-

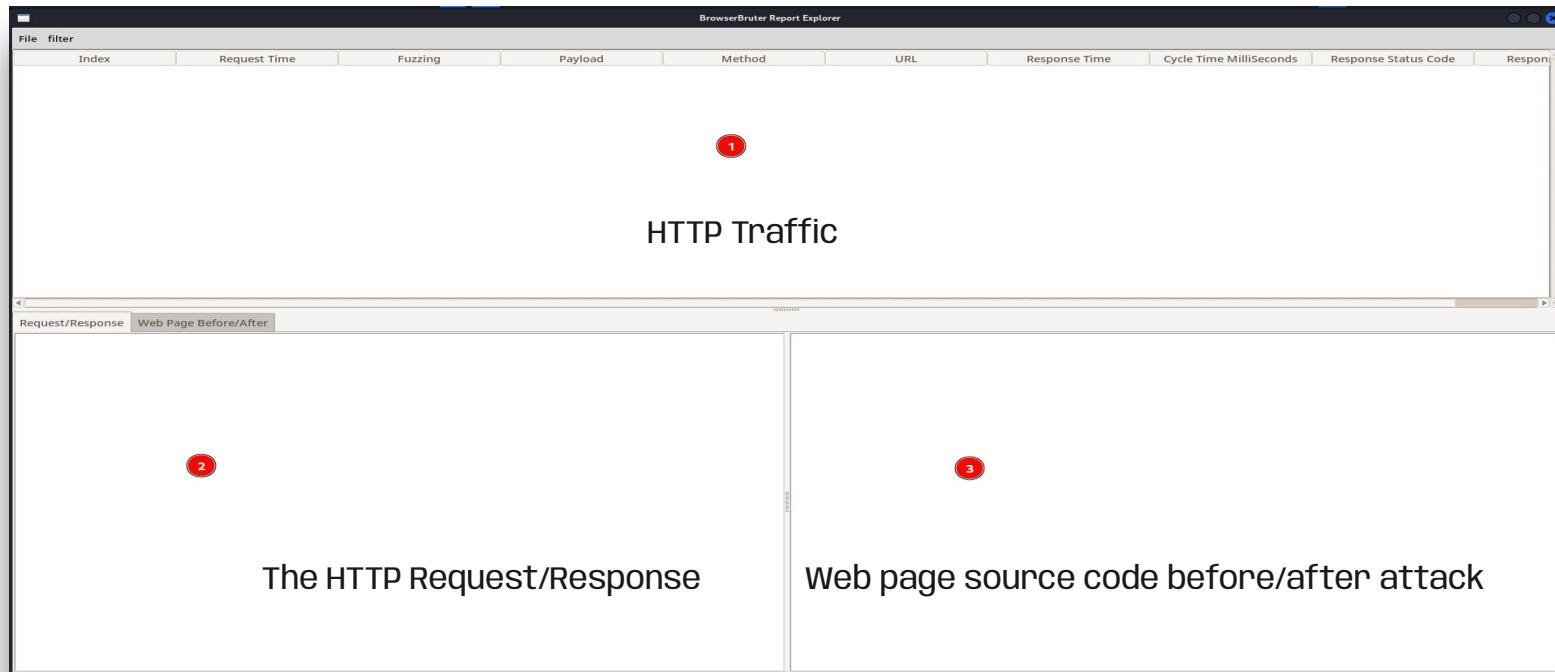


Loading The Report

2. Loading from 'Load Report' option-



The Report Explorer - GUI



The Report Explorer - GUI - Traffic

Index	Request Time	Fuzzing	Payload	Method	URL	Response Time	Cycle Time MilliSeconds	Response Status Code	Response
0	2024-04-05 00:25:54	['username', 'password']	('portaladmin', '123')	GET	http://localhost/login3.php	2024-04-05 00:25:54	7	200	1084
1	2024-04-05 00:25:56	['username', 'password']	('portaladmin', '123')	POST	http://localhost/login3.php	2024-04-05 00:25:56	53	200	1141
2	2024-04-05 00:25:56	['username', 'password']	('portaladmin', 'super_stron')	GET	http://localhost/login3.php	2024-04-05 00:25:56	5	200	1084
3	2024-04-05 00:25:57	['username', 'password']	('portaladmin', 'super_stron')	POST	http://localhost/login3.php	2024-04-05 00:25:57	52	302	3050
4	2024-04-05 00:25:57	['username', 'password']	('portaladmin', 'super_stron')	GET	http://localhost/dashboard.	2024-04-05 00:25:57	12	200	2124
5	2024-04-05 00:25:58	['username', 'password']	('portaladmin', 'qesdg5e56')	GET	http://localhost/login3.php	2024-04-05 00:25:58	5	200	1084
6	2024-04-05 00:25:58	['username', 'password']	('portaladmin', 'qesdg5e56')	POST	http://localhost/login3.php	2024-04-05 00:25:58	49	200	1141
7	2024-04-05 00:25:59	['username', 'password']	('portaladmin', 'wqwer')	GET	http://localhost/login3.php	2024-04-05 00:25:59	5	200	1084
8	2024-04-05 00:25:59	['username', 'password']	('portaladmin', 'wqwer')	POST	http://localhost/login3.php	2024-04-05 00:25:59	52	200	1141
9	2024-04-05 00:26:00	['username', 'password']	('admin@gmail.com', '123')	GET	http://localhost/login3.php	2024-04-05 00:26:00	5	200	1084
10	2024-04-05 00:26:00	['username', 'password']	('admin@gmail.com', '123')	POST	http://localhost/login3.php	2024-04-05 00:26:00	48	200	1134
11	2024-04-05 00:26:01	['username', 'password']	('admin@gmail.com', 'super')	GET	http://localhost/login3.php	2024-04-05 00:26:01	5	200	1084
12	2024-04-05 00:26:01	['username', 'password']	('admin@gmail.com', 'super')	POST	http://localhost/login3.php	2024-04-05 00:26:01	50	200	1134
13	2024-04-05 00:26:02	['username', 'password']	('admin@gmail.com', 'qesdg')	GET	http://localhost/login3.php	2024-04-05 00:26:02	5	200	1084
14	2024-04-05 00:26:02	['username', 'password']	('admin@gmail.com', 'qesdg')	POST	http://localhost/login3.php	2024-04-05 00:26:02	54	200	1134
15	2024-04-05 00:26:03	['username', 'password']	('admin@gmail.com', 'wqwwe')	GET	http://localhost/login3.php	2024-04-05 00:26:03	5	200	1084
16	2024-04-05 00:26:03	['username', 'password']	('admin@gmail.com', 'wqwwe')	POST	http://localhost/login3.php	2024-04-05 00:26:04	47	200	1134
17	2024-04-05 00:26:04	['username', 'password']	('guest', '123')	GET	http://localhost/login3.php	2024-04-05 00:26:04	5	200	1084
18	2024-04-05 00:26:04	['username', 'password']	('guest', '123')	POST	http://localhost/login3.php	2024-04-05 00:26:05	49	200	1134
19	2024-04-05 00:26:05	['username', 'password']	('guest', 'super_strong_pass')	GET	http://localhost/login3.php	2024-04-05 00:26:05	4	200	1084
	2024-04-05 00:26:06	['username', 'password']	('guest', 'super_strong_pass')	POST	http://localhost/login3.php	2024-04-05 00:26:06	53	200	1134

The Report Explorer - GUI - Columns

- Index
- Request Time
- Fuzzing (Specifies the element being fuzzed)
- Payload
- Method
- URL
- Response Time
- Cycle Time MilliSeconds
- Response Status Code
- Response Length

The Report Explorer - GUI - Request/Response

Request/Response Web Page Before/After

```
GET http://localhost/login3.php
Host: localhost
Proxy-Connection: keep-alive
sec-ch-ua: "Not(A:Brand";v="24", "Chromium";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
```

HTTP/1.1 200 OK
Date: Thu, 04 Apr 2024 18:55:56 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.4.16
Set-Cookie: PHPSESSID=llvf5a4jn5ojebj7u4bq6dka41a; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Vary: Accept-Encoding
Content-Encoding: gzip
Content-Length: 1084
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html>
<html>
<head>
<title>
 Stock Management System
</title>
<!-- bootstrap -->
<link href="assests/bootstrap/css/bootstrap.min.css" rel="stylesheet"/>
<!-- bootstrap theme-->
<link href="assests/bootstrap/css/bootstrap-theme.min.css" rel="stylesheet"/>
<!-- font awesome -->
<link href="assests/font-awesome/css/font-awesome.min.css" rel="stylesheet"/>
<!-- custom css -->
<link href="custom/css/custom.css" rel="stylesheet"/>
<!-- jquery -->

① REQUEST

② RESPONSE

The Report Explorer - GUI - Web Page

Request/Response | Web Page Before/After

WEB PAGE SOURCE CODE BEFORE ATTACK

```
<html>
<head>
    <title>
        Stock Management System
    </title>
    <!-- bootstrap -->
    <link href="assests/bootstrap/css/bootstrap.min.css" rel="stylesheet"/>
    <!-- bootstrap theme-->
    <link href="assests/bootstrap/css/bootstrap-theme.min.css" rel="stylesheet"/>
    <!-- font awesome -->
    <link href="assests/font-awesome/css/font-awesome.min.css" rel="stylesheet"/>
    <!-- custom css -->
    <link href="custom/css/custom.css" rel="stylesheet"/>
    <!-- jquery -->
    <script src="assests/jquery/jquery.min.js">
    </script>
    <!-- Cryptajs -->
    <script src="libraries/cryptojs/example/aes.js">
    </script>
    <script src="libraries/cryptojs/aes-json-format.js">
    </script>
    <script src="custom/js/senccrypt.min.js">
    </script>
    <script src="custom/js/encrypt_login3.js">
    </script>
    <!-- jquery ui -->
    <link href="assests/jquery-ui/jquery-ui.min.css" rel="stylesheet"/>
    <script src="assests/jquery-ui/jquery-ui.min.js">
    </script>
    <!-- bootstrap js -->
    <script src="assests/bootstrap/js/bootstrap.min.js">
    </script>
    <meta content="AymqpwRC7u88Y4JPvFI2F37QKy1C04248hLcdJAshtXg0fe/dVJPV3S3wLFca1ZMVotnBfVjaCMTVudWM//5g4AAAB7eyJvcmlnaW410JodHlwczovL3d5dy5nbGv8YwdtYw5hZ2zVlMvbToNDMILCjmZWfd0XJ1joiUHJpdmeVNhbmRb3hBZHNUElzIwiZXhwXJ5ijoxNjk1MTY30Tk5LCpc1RoaxJkUGFydkHkionRydW9" http-equiv="origin-trial"/>
</head>
<body>
    Global site tag (gtag.js) - Google Analytics -->
    <script async="" src="https://www.googletagmanager.com/gtag/js?id=G-4V4HC9K0Z6">
    </script>
    <script>
        window.dataLayer = window.dataLayer || [];
    
```

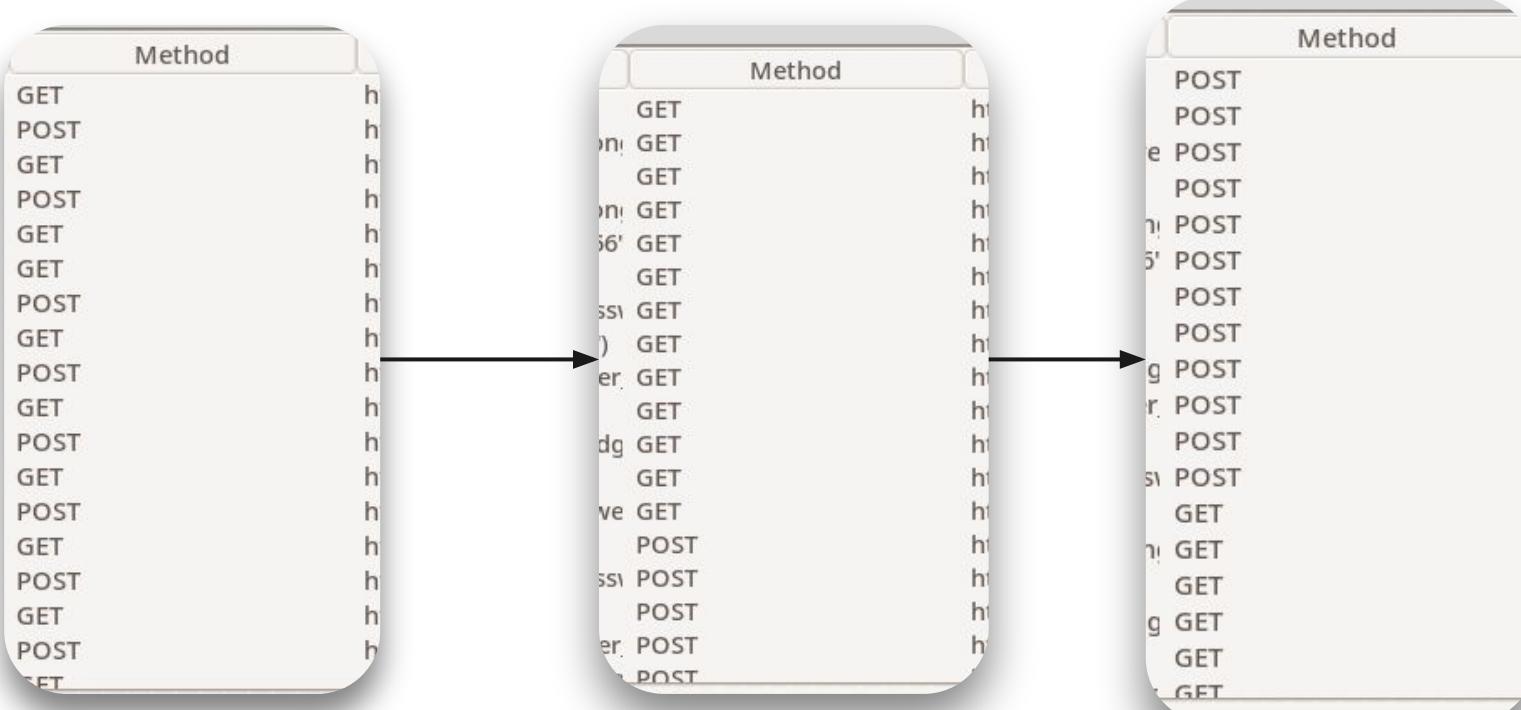
WEB PAGE SOURCE CODE AFTER ATTACK

```
<html>
<head>
    <title>
        Stock Management System
    </title>
    <!-- bootstrap -->
    <link href="assests/bootstrap/css/bootstrap.min.css" rel="stylesheet"/>
    <!-- bootstrap theme-->
    <link href="assests/bootstrap/css/bootstrap-theme.min.css" rel="stylesheet"/>
    <!-- font awesome -->
    <link href="assests/font-awesome/css/font-awesome.min.css" rel="stylesheet"/>
    <!-- custom css -->
    <link href="custom/css/custom.css" rel="stylesheet"/>
    <!-- DataTables -->
    <link href="assests/plugins/datatables/jquery.dataTables.min.css" rel="stylesheet"/>
    <!-- file input -->
    <link href="assests/plugins/fileinput/css/fileinput.min.css" rel="stylesheet"/>
    <!-- jquery -->
    <script src="assests/jquery/jquery.min.js">
    </script>
    <!-- jquery ui -->
    <link href="assests/jquery-ui/jquery-ui.min.css" rel="stylesheet"/>
    <script src="assests/jquery-ui/jquery-ui.min.js">
    </script>
    <!-- bootstrap js -->
    <script src="assests/bootstrap/js/bootstrap.min.js">
    </script>
    </head>
    <body>
        <nav class="navbar navbar-default navbar-static-top">
            <div class="container">
                <!-- Brand and toggle get grouped for better mobile display -->
                <div class="navbar-header">
                    <button aria-expanded="false" class="navbar-toggle collapsed" data-target="#bs-example-navbar-collapse-1" data-toggle="collapse" type="button">
                        <span class="sr-only">
                            Toggle navigation
                        </span>
                        <span class="icon-bar">
                        </span>
                        <span class="icon-bar">
                        </span>
                        <span class="icon-bar">
                        </span>
                    
```

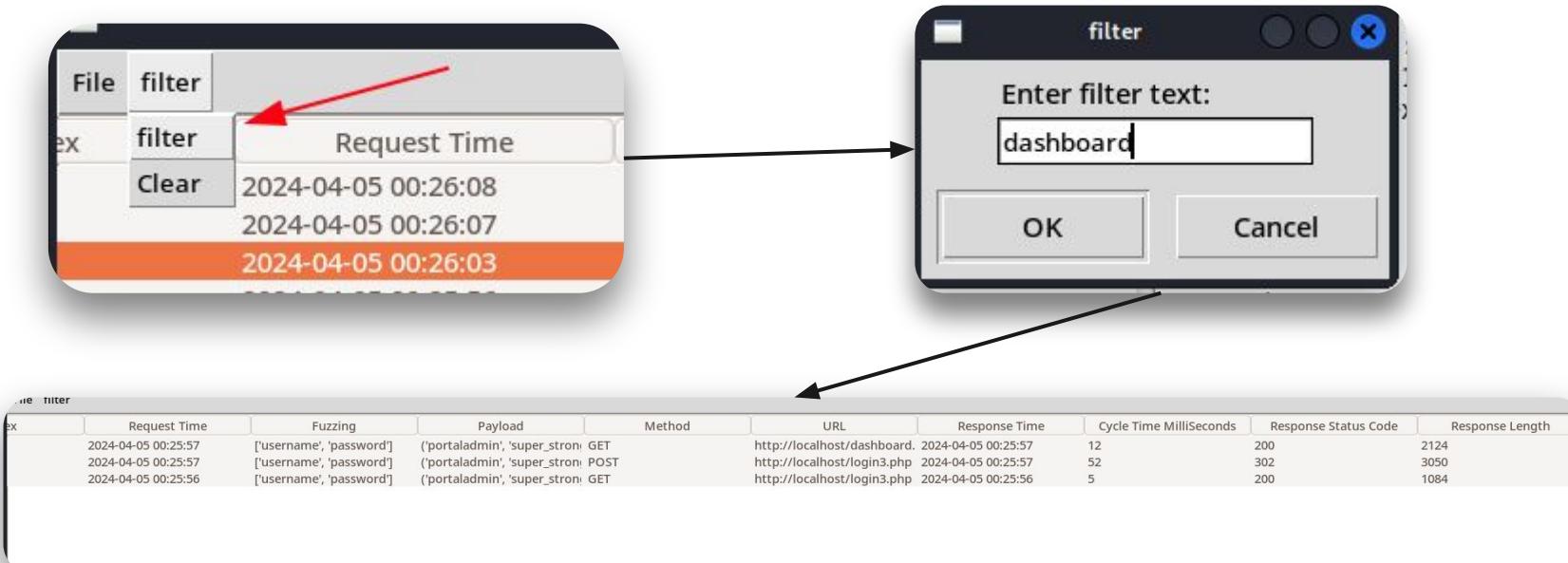
The Report Explorer - Sorting

Index	Request Time	Fuzzing	Index
0	2024-04-05 00:25:54	['username', 'password']	24
1	2024-04-05 00:25:56	['username', 'password']	23
2	2024-04-05 00:25:56	['username', 'password']	22
3	2024-04-05 00:25:57	['username', 'password']	21
4	2024-04-05 00:25:57	['username', 'password']	20
5	2024-04-05 00:25:58	['username', 'password']	19
6	2024-04-05 00:25:58	['username', 'password']	18
7	2024-04-05 00:25:59	['username', 'password']	17
8	2024-04-05 00:25:59	['username', 'password']	16
9	2024-04-05 00:26:00	['username', 'password']	15
10	2024-04-05 00:26:00	['username', 'password']	14
11	2024-04-05 00:26:01	['username', 'password']	13
12	2024-04-05 00:26:01	['username', 'password']	12
13	2024-04-05 00:26:02	['username', 'password']	11
14	2024-04-05 00:26:02	['username', 'password']	10
15	2024-04-05 00:26:03	['username', 'password']	9
16	2024-04-05 00:26:03	['username', 'password']	8
17	2024-04-05 00:26:04	['username', 'password']	7

The Report Explorer - Sorting



The Report Explorer - Filtering



The Report Explorer - Right click & Copy

Request Time	Fuzzing	Payload	Method
2024-04-05 00:26:08	['username', 'password']	('guest', 'wqwer')	POST
2024-04-05 00:26:07	['username', 'password']	('guest', 'qesdgs6e56')	POST
2024-04-05 00:26:03	['username', 'pas	Copy Payload ('admin@gmail.com', 'wqwe	POST
2024-04-05 00:25:56	['username', 'pas	Copy Row ('portaladmin', '123')	POST
2024-04-05 00:25:57	['username', 'pas	('portaladmin', 'super_stron	POST
2024-04-05 00:25:58	['username', 'password']	('portaladmin', 'qesdgs6e56')	POST
2024-04-05 00:25:59	['username', 'password']	('portaladmin', 'wqwer')	POST
2024-04-05 00:26:00	['username', 'password']	('admin@gmail.com', '123')	POST

The Report Explorer - Select & Copy

Request/Response Web Page Before/After

```
POST http://localhost/login3.php
Host: localhost
Proxy-Connection: keep-alive
Content-Length: 771
Cache-Control: max-age=0
sec-ch-ua: "Not(A:Brand";v="24", "Chromium";v="122"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://localhost
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://localhost/login3.php
Accept-Encoding: gzip, deflate, br
Accept-Language: en-GB,en-US;q=0.9,en;q=0.8
Cookie: PHPSESSID=s6cru8qhjog127lqosgjhtc5ht; _ga=GA1.1.1861091042.1712256963;
ga_4V4HC9K0Z6=GS1.1.1712256963.1.0.1712256963.0.0.0
username=U2sVNcwlkL2+X6ygfaQPs1RCMCSiIq0dKRVWzWIMpmvHM0Yw/c+u4xlK4lRKDG2MChh07EbZHqPcB9y/RhIQ4UPiYsMV5p0NDDZHgHtGLGK+t4vaxyTAyhCZ5VSP08pXmJ69EiWJoGFpT23jPXL/QzYe+rCC+wv+eo1OxW+7dVTyW8W710dP0mM7tA00qgKbNrR9NXAkPF5F+9wh7xCuic6YHu9sdGRgFx/UsQV/JmQBTx6wTq91k0y6fsyVGMrJepCn7Fv+PB91X2dajgbesRsF8j+JRyLzudPG3iyhOry44Pukv0fFP5D+d7608a21JyryrExQ1jY9RZas6bCg==&password=dHwm8dQ+PTZhiHqF53QCCs5JMzZHBOYa6ZEIINZHshBBum2UNzIR0s5ULy0zwZ17DbhtSvQaQHWrj9+1KKvrUuUq+e0JE1SMLI6fnQtMk/9E
GahbVD4F5S1bXpYCxsh/kCTTb0J2FN9068Cy+waF5t+bOMUA1bP8r8gkSpvRtscvXuEh9pdPbGgaXVu/aYuUbqX6tPWNGAz0HzH/A7965xaKeyrg2Rkx
07snfUavk0mxNNQBJDFUkl0LsBEd9nffWsLHRtatPT+7LJ08cB+MKQe1xmD41IWQAQfeR3Ud0vtqlntTwnJ58MKUUsf9tD1/Cb7AGBYZ0yWUYXZyi1ww==
```

CTRL+C

The Report Explorer - Grepping

- It allows you to specify various words or strings that you want to check whether they appear in HTTP traffic, Web page or not.
- You can use --grep to search for multiple words or strings, providing flexibility in your analysis.
- This feature enables targeted analysis of the report, focusing on specific aspects of the HTTP traffic or web pages.
- --grep helps in quickly identifying relevant information

The Report Explorer - Grepping - Example

```
▶ デ==> python3 ReportExplorer.py --report BrowserBr  
uter_Reports/localhost/2024-04-05_00-25-51/localhost-20  
24-04-05_00-25-51.csv --grep welcome,error,dashboard
```

The Report Explorer - Grepping -Additional Columns

Response Length	welcome	error	dashboard
1084	0	0	0
1141	0	0	0
1084	0	0	4
3050	0	0	5
2124	0	0	9
1084	0	0	0

The Report Explorer - Grepping - We Found The Dashboard

The image shows a screenshot of a report explorer interface. At the top, there's a table with columns: Method, URL, Response Time, Cycle Time MilliSeconds, Response Status Code, Response Length, welcome, error, and dashboard. The table contains five rows of log entries. An arrow points from the 'dashboard' column of the table to a summary dashboard at the bottom.

Method	URL	Response Time	Cycle Time MilliSeconds	Response Status Code	Response Length	welcome	error	dashboard
GET	http://localhost/dashboard	2024-04-05 00:25:57	12	300	2124	0	0	9
POST	http://localhost/login3.php	2024-04-05 00:25:57	52	302	3050	0	0	5
GET	http://localhost/login3.php	2024-04-05 00:25:56	5	200	1684	0	0	4
POST	http://localhost/login3.php	2024-04-05 00:26:00	48	200	1134	0	0	0

At the bottom, there's a summary dashboard with the title 'dashboard'. It displays the following values:

- 9
- 5
- 4
- 0
- 0
- 0

The Report Explorer - Grepping - Here's The HTTP Request/Response

The screenshot shows a browser-based application interface for monitoring network traffic. At the top, there's a table with columns for 'Request/Response', 'Web Page Before/After', and several status indicators. Below this is a detailed view of a single request-response pair.

Request/Response: POST http://localhost/login3.php

Headers:

```
Host: localhost
Proxy-Connection: keep-alive
Content-Length: 749
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua: "Not(A:Brand);v="24", "Chromium";v="122"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36
Accept: */*
Accept-Language: en-US;q=0.9, en;q=0.8
Cookie: PHPSESSID=1tv5a4jh5ojebj48edgk414; ga=GAI.1.774328382.1712256957;
ga_4V4HCK0ZG-S5...; 1712230956; .0.0.0.0
Accept-Encoding: gzip, deflate, br
```

Body:

```
username=qFbfYkZ2dM...&password=jPjwUu...&rememberme=1&submit=Log+In
```

Response Headers:

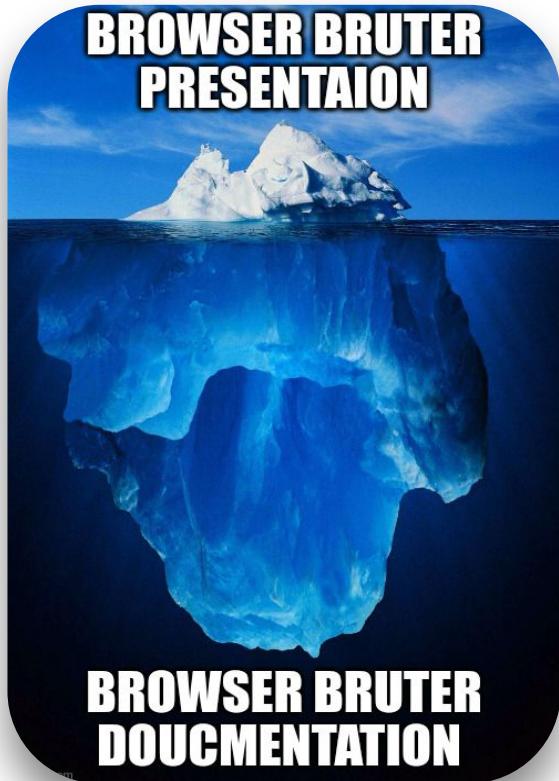
```
HTTP/1.1 302 Found
Date: Thu, 04 Apr 2024 18:55:57 GMT
Server: Apache/2.4.38 (Debian)
X-Powered-By: PHP/7.4.16
Expires: Sat, 09 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: analytics_uid=%3A1%3A%221%22%3B; expires=Sat, 04-May-2024 18:55:57 GMT; Max-Age=2592000; path=/; domain=.dashboard.php
Content-Length: 300
Content-Type: text/html; charset=UTF-8
```

Response Body (HTML):

```
<!DOCTYPE html>
<html>
<head>
<title>
Stock Management System
</title>
<!-- bootstrap theme-->
<link href="assets/bootstrap/css/bootstrap.min.css" rel="stylesheet"/>
<!-- bootstrap theme-->
<link href="assets/bootstrap/css/bootstrap-theme.min.css" rel="stylesheet"/>
<!-- font -->
<link href="assets/fonts/font-awesome/css/font-awesome.min.css" rel="stylesheet"/>
<!-- custom css -->
<link href="custom/css/custom.css" rel="stylesheet"/>
<!-- library -->
<script src="assets/jquery/jquery.min.js">
```

The response body continues with more script tags and CSS imports, ending with a closing

This Is Just A Tip of An Iceberg



It is impossible to cover all of the functionalities of the Browser Bruter. I highly recommend to go check out the documentation.

As we said there are over 40+ options and switches available to tackle various scenarios and test cases. So what we have shown is just a tip of an iceberg of what browser bruter can do.

Read the official documentation for the Browser Bruter -

- <https://net-square.com/browserbruter/>

Download the Browser Bruter now -

- <https://github.com/netsquare/BrowserBruter/releases>

Contribute & Help

- **Improve:** You can contribute by forking the repository, making your changes, and submitting a pull request.
- **Reporting Issues:** If you encounter a bug or issue while using BrowserBruter, please report it on the GitHub issue tracker.
- **Feature Requests:** If you have a feature request or idea for improving BrowserBruter, you can submit it on the GitHub issue tracker.
- **Spread the Word:** You can also contribute by spreading the word about BrowserBruter. Share it with your friends, colleagues, or on social media to help grow the user community.

Contribute & Help - Spread The Word

- **Write a medium post, write a blog about it. Share it in groups, chats, clients, repost, mention, story anything will be appreciated.**
- **Twitter** - https://x.com/zinja_coder/status/1776482335732727884
- **LinkedIn** -
https://www.linkedin.com/posts/jafar-pathan_the-browserbruter-activity-7182247758693625856-Zs0G?utm_source=share&utm_medium=member_desktop
- **Threads** -
https://www.threads.net/@jafar.khan.pathan_/post/C5alJ-aNCnU

Thanks & Happy Hacking

The BrowserBruter By Jafar Pathan



Browser-Bruter

Web-Forms

Me