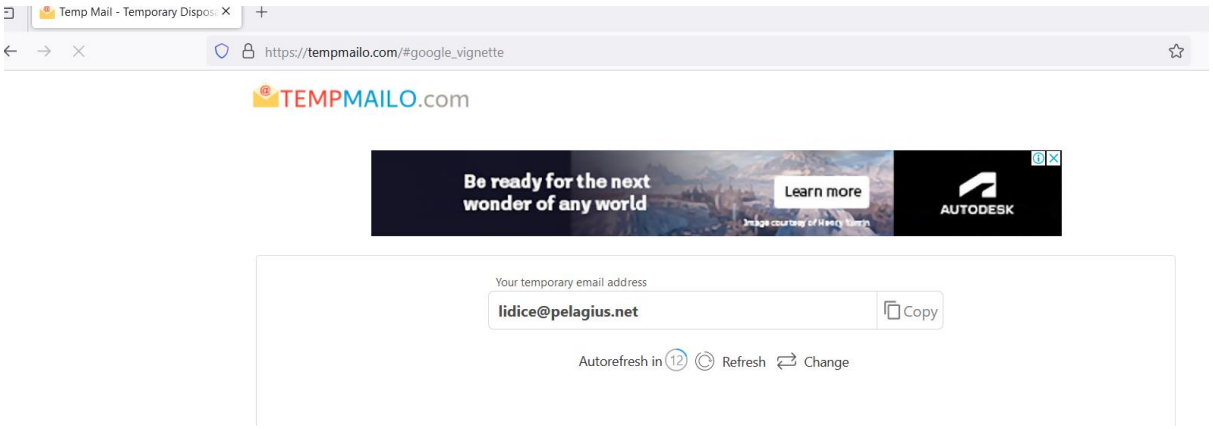
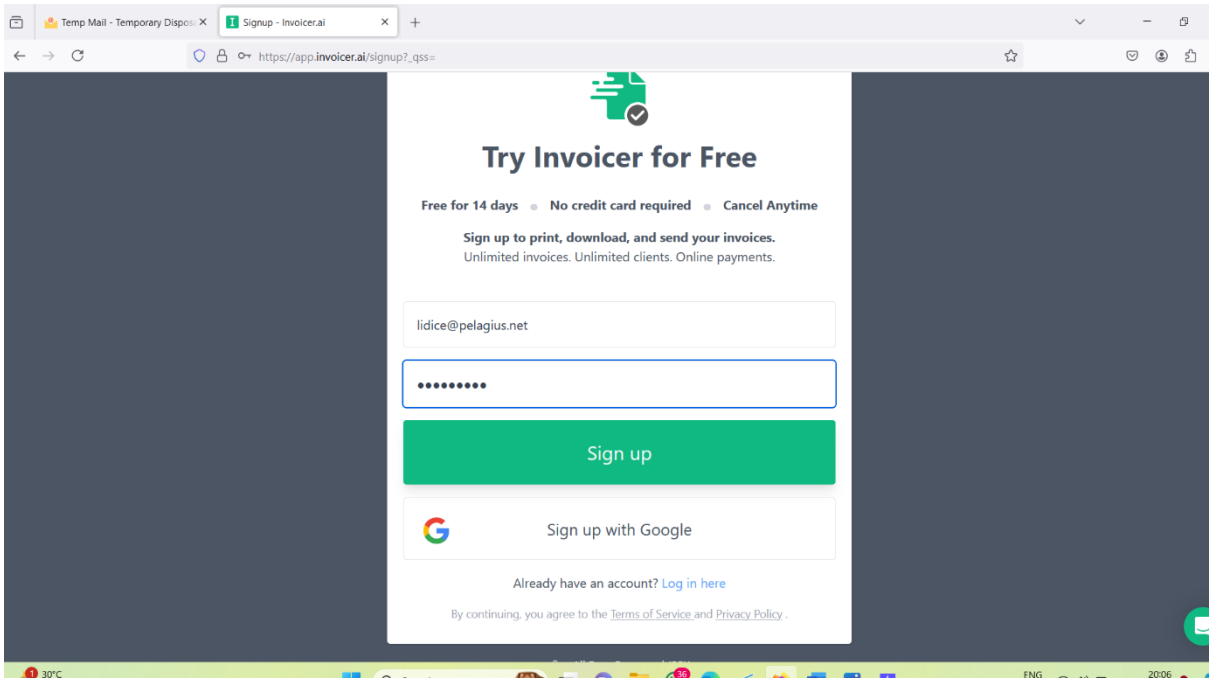
NAME: VAISHNAVI PARULEKAR	ROLL ID: 22203A0048
COURSE:CO (COMPUTER ENGINNERING)	Task Assignment: email rate-limiting feature on the website invoicer.ai
COMPANY: SECURER CYBER FUTURE	COLLEGE: VIDYALANKAR POLYTECHNIC

Email rate-limiting feature on the website invoicer.ai

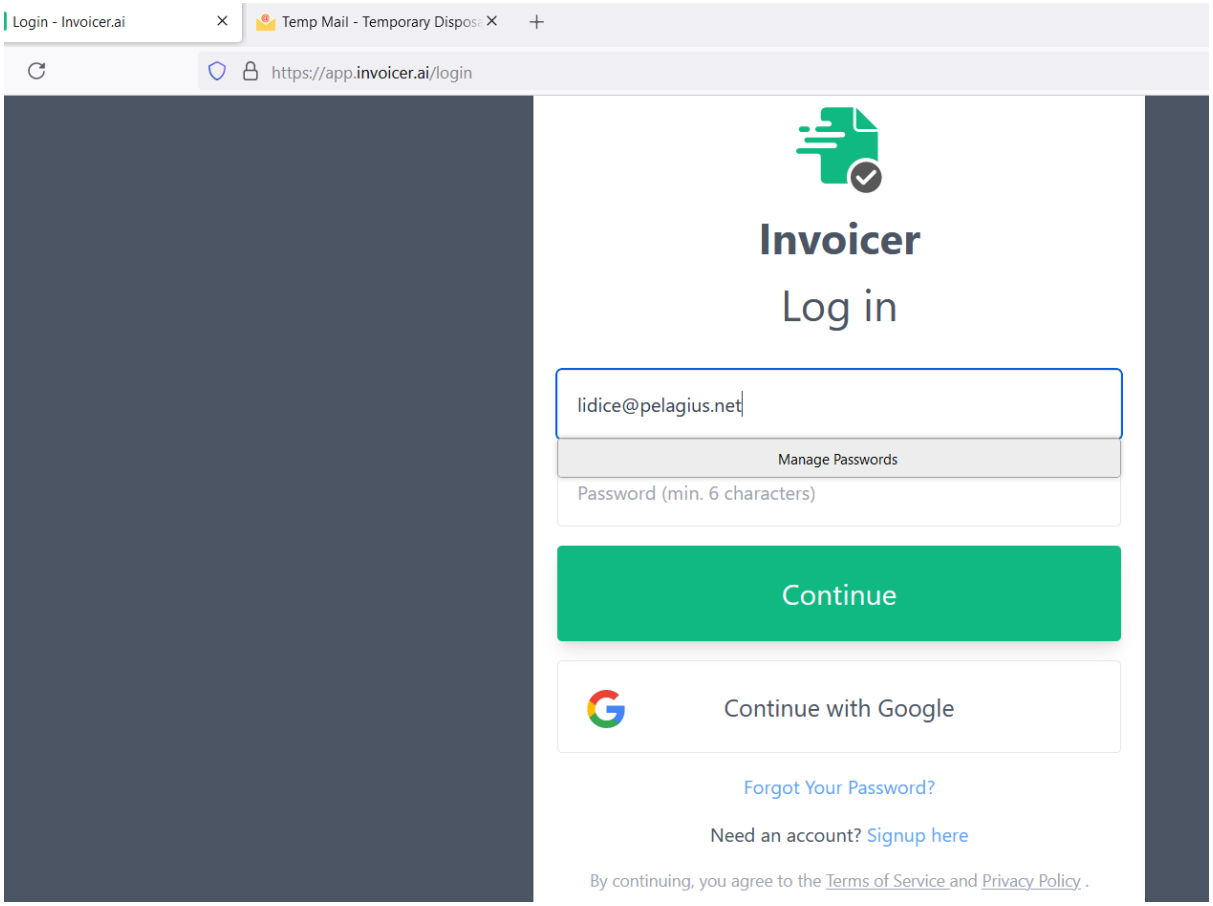
Detailed descriptions of the steps taken to perform the test. The results of testing, including any identified vulnerabilities.



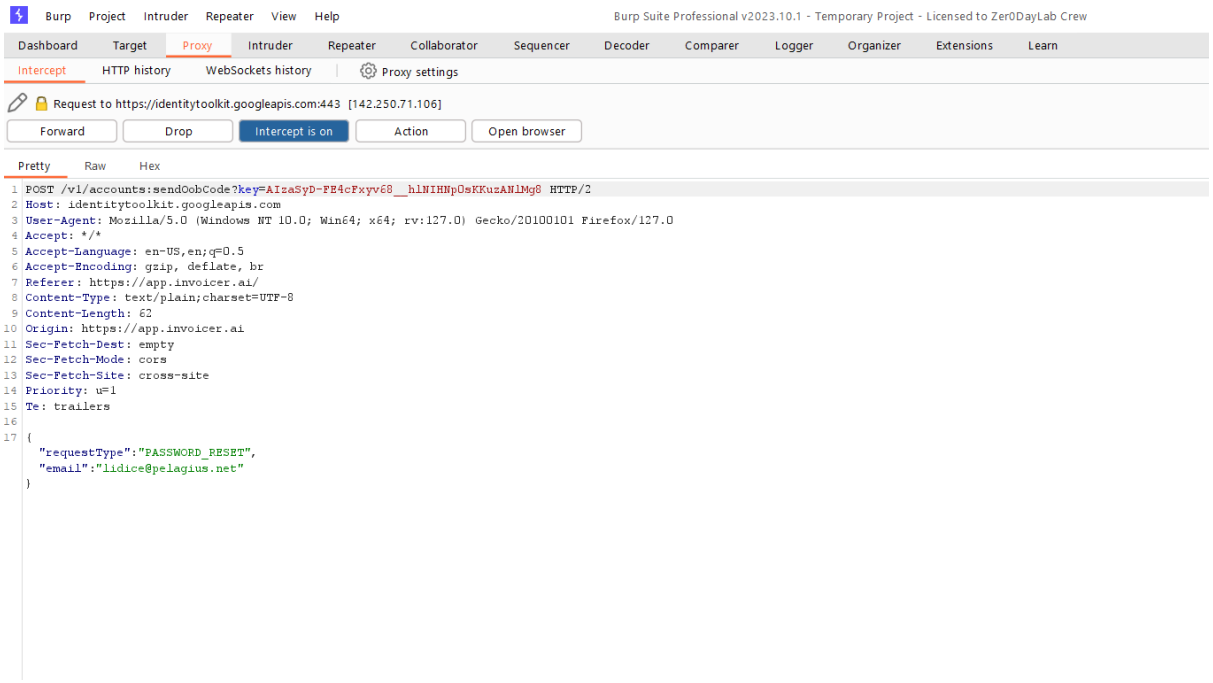
Took the email from the TEMPMAILO.com i.e lidice@pelagius.net



Did the sign up using the email and the password

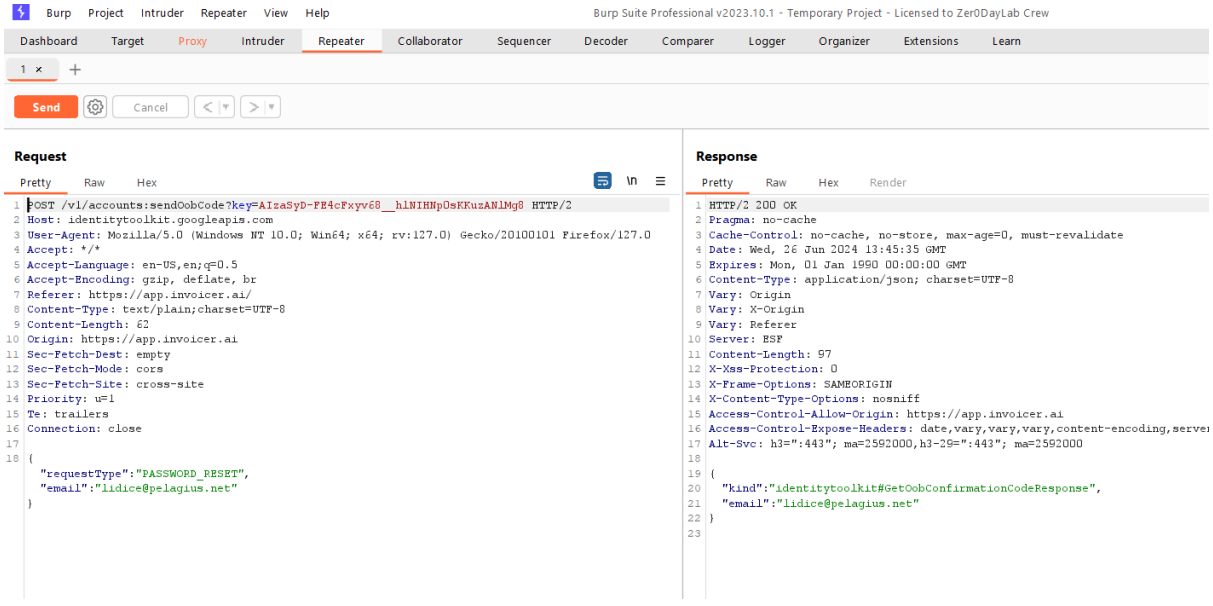


Type the email id and did forget password while the intercept is on.

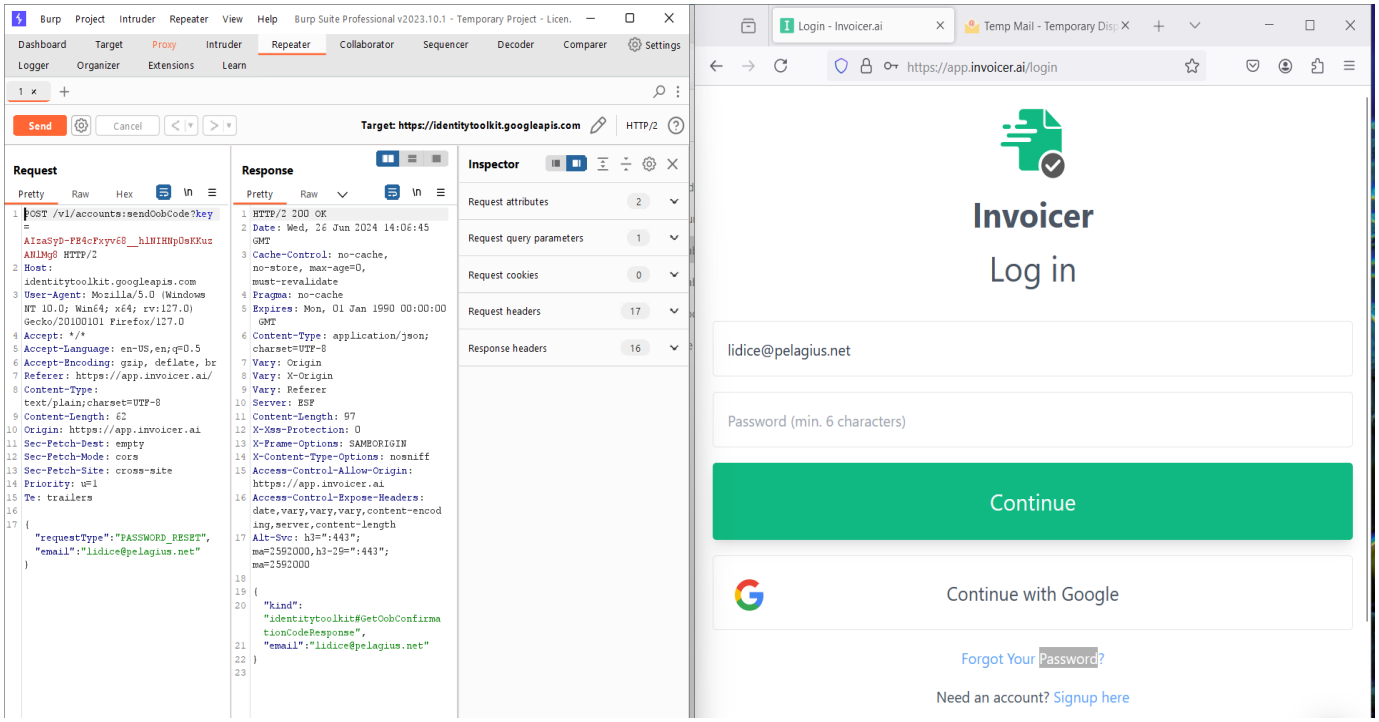


The traffic got catch in the intercept its showing “requestType”: PASSWORD_RESET”, and

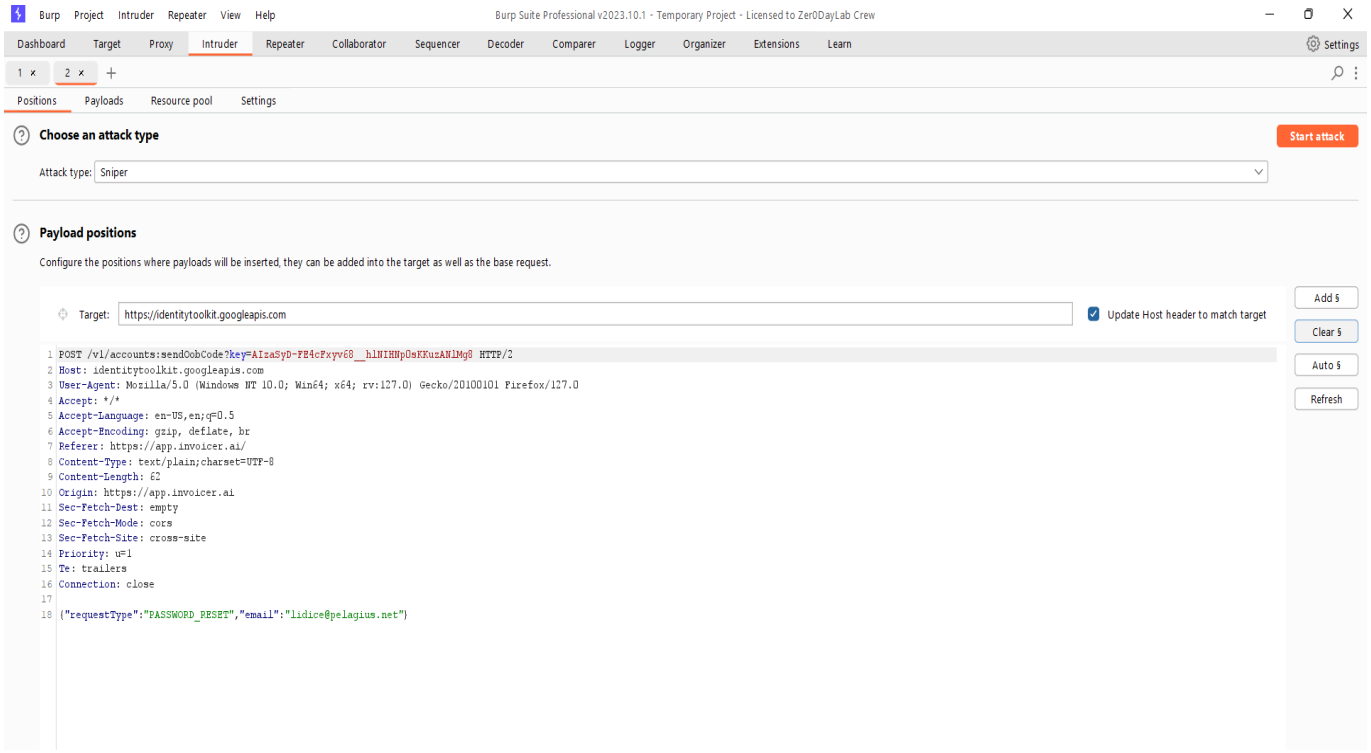
“email”: lidice@pelagius.net



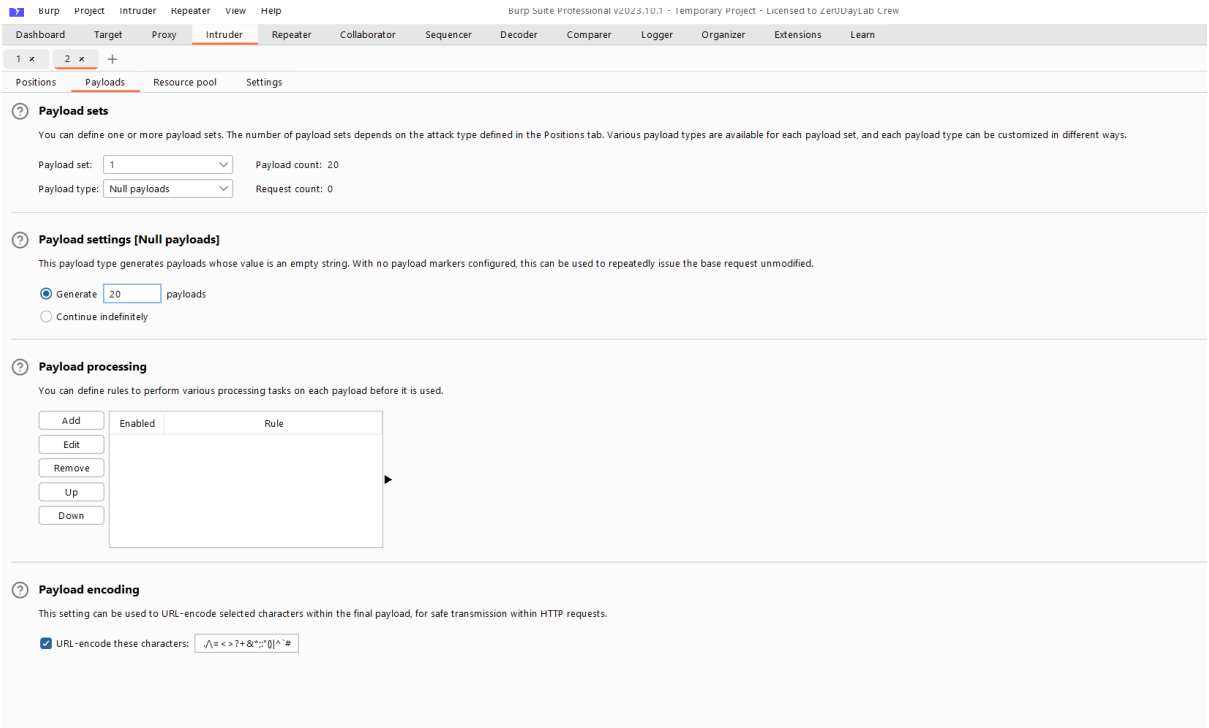
Repeater screenshot



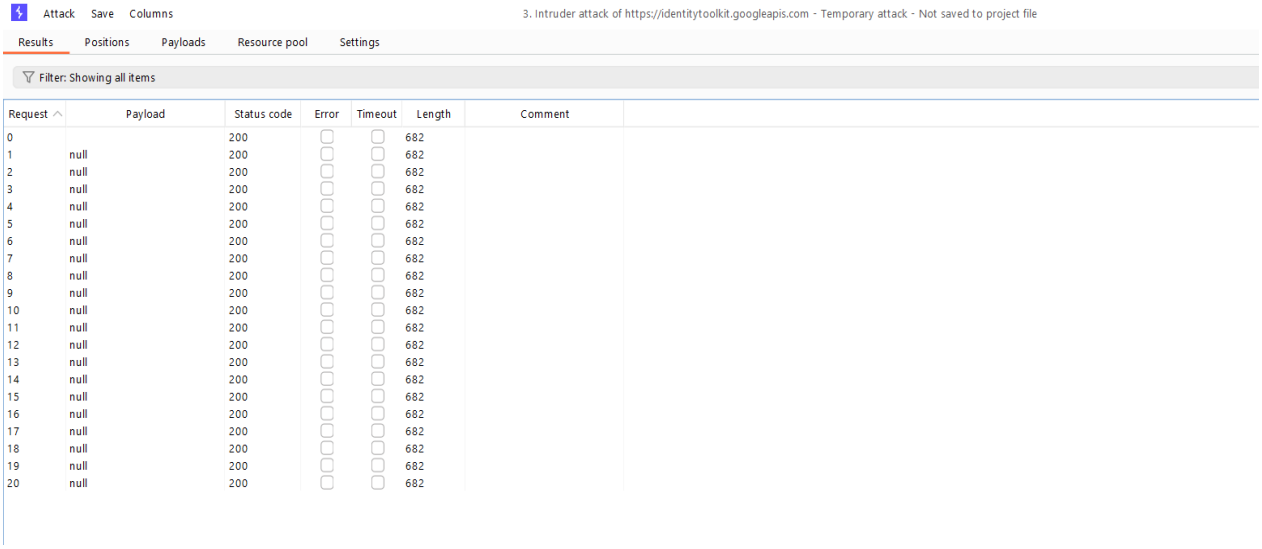
The repeater is showing the same mail id as in the Log in page



Sent to intruder to add null payloads

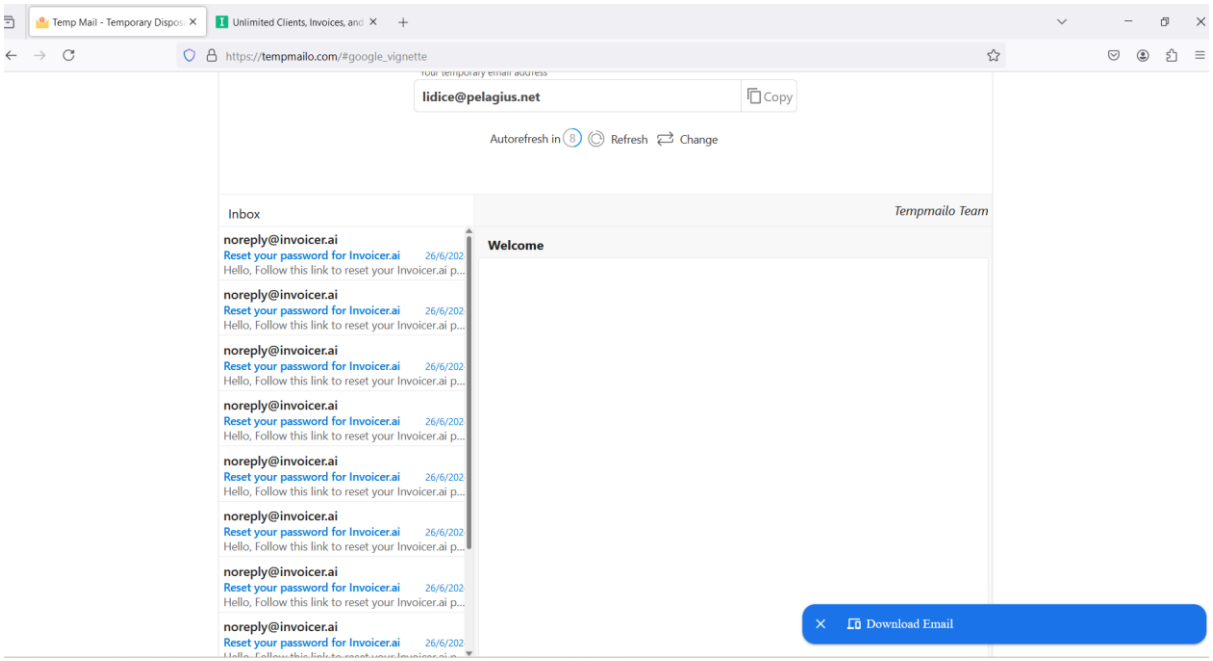


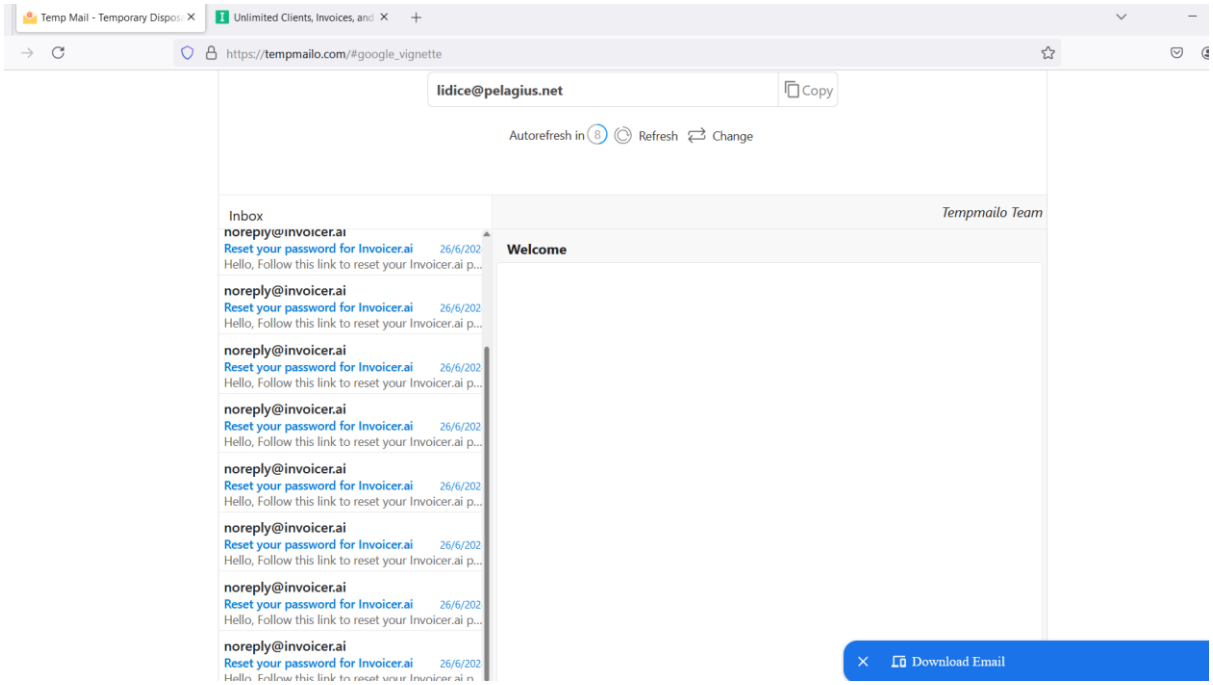
Addes Null payload to generate 20 payloads and start the attack

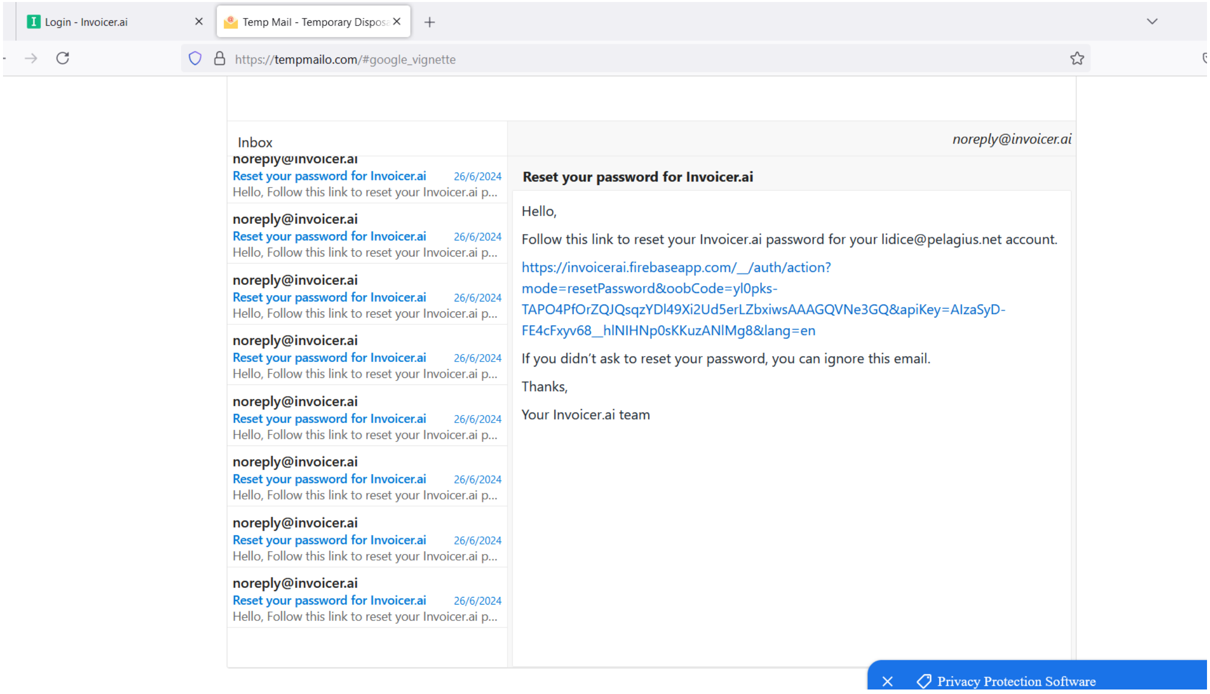


Request	Payload	Status code	Error	Timeout	Length	Comment
0		200			682	
1	null	200			682	
2	null	200			682	
3	null	200			682	
4	null	200			682	
5	null	200			682	
6	null	200			682	
7	null	200			682	
8	null	200			682	
9	null	200			682	
10	null	200			682	
11	null	200			682	
12	null	200			682	
13	null	200			682	
14	null	200			682	
15	null	200			682	
16	null	200			682	
17	null	200			682	
18	null	200			682	
19	null	200			682	
20	null	200			682	

The 20 null payloads


Temp Mail - Temporary Dispos
Unlimited Clients, Invoices, and
https://tempmailo.com/#google_vignette
lidice@pelagius.net
Copy
Autorefresh in 8
Refresh
Change
Inbox
Tempmailo Team
noreply@invoicer.ai
Reset your password for Invoicer.ai 26/6/202
Hello, Follow this link to reset your Invoicer.ai p...
Welcome
Download Email


Temp Mail - Temporary Dispos
Unlimited Clients, Invoices, and
https://tempmailo.com/#google_vignette
lidice@pelagius.net
Copy
Autorefresh in 8
Refresh
Change
Inbox
Tempmailo Team
noreply@invoicer.ai
Reset your password for Invoicer.ai 26/6/202
Hello, Follow this link to reset your Invoicer.ai p...
Welcome
Download Email



The email from the inbox

The vulnerability is of receiving a huge number of reset password verification code in my email using the same Intruder attack with null payloads.

Potential impacts of the identified issues.

The inbox is showing huge number of emails of reset password verification code it requires Implementation of proper rate limiting on password reset requests is essential to mitigate these risks, ensuring the security, reliability, and user satisfaction of the service.

If not controlled it may lead to various issues: -

Security Risks

User Experience

Operational Issues as the way the user operates

Reputation Damage for both trust and damage of brand

Recommendations for mitigation if any vulnerabilities are found.

Limit the number of passwords reset requests a user can make within a specific timeframe.

Increase the time interval between subsequent reset requests after each attempt.

Implement CAPTCHA to verify that the requests are coming from humans and not automated bots, especially after a certain number of failed attempts.

Implement the I am not the robot for any automated tools are accessing or not

Educate users about phishing attacks and how to recognize legitimate communications from your service.

Encourage the use of strong, unique passwords and provide guidelines for creating them by using special symbols in it like @, #, $, & etc.

Validate all inputs and outputs to prevent injection attacks and other common vulnerabilities.