**Firing 8 Account Takeover Methods**

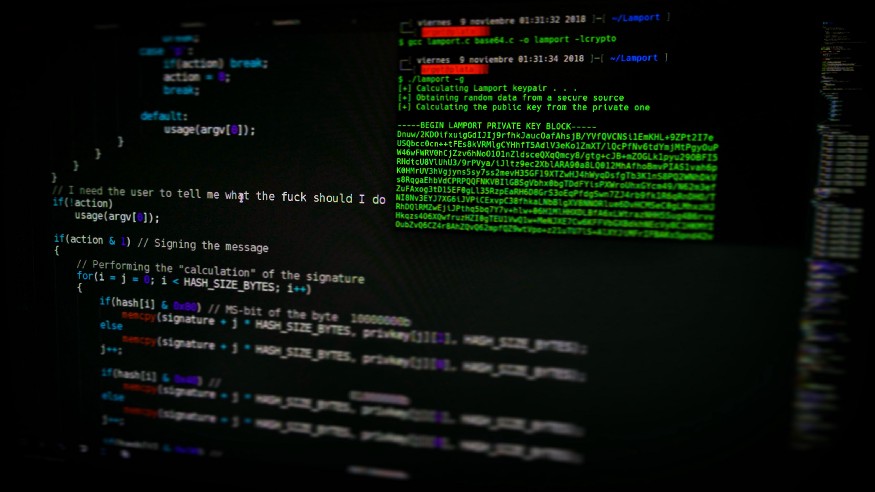


Photo by [Arget](https://unsplash.com/@arget?utm_source=medium&utm_medium=referral" \t "_blank) on [Unsplash](https://unsplash.com/?utm_source=medium&utm_medium=referral" \t "_blank)

Hello! this is Md Maruf Hosan a bug bounty hunter from Bangladesh.  
I am gonna be firing some account takeover methods

1. **Unicode Normalization Issue**1. victim account victim@gmail.com  
   2. create an account using Unicode  
   example: vićtim@gmail.com  
   list of Unicode character: <https://en.wikipedia.org/wiki/List_of_Unicode_characters>  
   Note: check where verification doesn’t require
2. **Authorization Issue**  
   1. change email of Account Aand put email B  
   2. check confirmation mail in account B  
   3. open the confirmation mail from account C  
   Taken over Account C
3. **Reusing Reset Token**if target allows you to reuse the reset link then hunt for more reset link via gau ,wayback or scan.io
4. **Pre Account Taekover**  
   1. signup using normal signup form as a hacker but attacker has no verification link.  
   2. then if victim signs up using oauth .  
   3. now attacker can login the victim account without verification link with the password he entered while registering.
5. **CORS Misconfiguration to Account Takeover**  
   1. check api , any endpoint has access access token/session/secret/fingerprint  
   2. if yes check for CORS misconfiguration does it allow us to fetch data from target?  
   3. make a payload to fetch data and replace headers and boom
6. **Csrf to Account Takeover**if profile modification in cookie based authentication doesn’t generate any token  
   1. open Account A change&Put email that you own click save intercept the request and generate a csrf poc.  
   2. if fully cookie based auth then you dont have to modify anything send the csrf file to victim.  
   3. if it requires UUID/UserID or unique token it becomes hard to do that but that doesn't mean it is secure , just start playing with target  
   hint: password reset page helps many times for UUID/GUID and UserID
7. **Host Header Injection**  
   well in this case there are 4 ways do that.  
   1. click reset password change host header.  
   2. or change proxy header ex: X-Forwarded-For: attacker.com  
   3. or change host, referrer, origin headers at once as attacker.com  
   4. click reset then click resend mail and do all 3 methods above
8. **Response Manipulation**1. code manipulation \* to 200 OK  
   2. code and body manipulation  
   code \* to 200 OK  
   body \* to {"success":true} or {}  
   it works when json is being used to transfer and receive data.

kick me on twitter: <https://twitter.com/0xmaruf>