



Updating Account Bug Hunting Methodology

Become a Successful
Bug Bounty Hunter



UPDATING ACCOUNT

- Any CSRF protection when updated profile information?
- If yes, how is it validated?
- Send blank CSRF token or a token with the same length.
- Look for `_token`
- Look at CSRF section



UPDATING ACCOUNT

- Any second confirmation for changing email/password?
- If no, chain with XSS to ATO
- XSS to perform CSRF



UPDATING ACCOUNT

- Is updating account info different on mobile app?
- Mobile apps use APIs -> maybe IDORs
- Different filters in place?
- Different code base and endpoints?



UPDATING ACCOUNT

- How they handle video/photo uploads? What sort of filtering is in place?
- Can I upload .txt even though it says .jpg and .png only ?
- Where are the uploads stored? (root domain or elsewhere)
- If hosted elsewhere check if domain is included in CSP



UPDATING ACCOUNT

- What information is available on my public profile that I can control?
- What you can control and where it is reflected?



UPDATING ACCOUNT

- Entering malicious HTML in bio
- How does it handle `< > " '` characters and where are these reflected?
- how does it handle unicode?
`%09 %07 %0d %0a`
- Can I input URL on my profile?
- What filter prevents URL like:
`javascript:alert(0)`



UPDATING ACCOUNT

- Maybe they filter `< >` and reflected as
`<div id="example" onclick="runjs('userinput<"');">`
- But you can use `');alert('example');` which results in
`<div id="example" onclick="runjs('userinput');alert('example');">`



Thank You!

Become a Successful
Bug Bounty Hunter