



Account Registration Bug Hunting Methodology

Become a Successful
Bug Bounty Hunter



ACCOUNT REGISTRATION

- Use Google Dorking to find registration pages around your target
- Examples:

`site:example.com inurl:register inurl:&`
`site:example.com inurl:signup inurl:&`
`site:example.com inurl:join inurl:&`



ACCOUNT REGISTRATION

- Check HTML source and JS files
- Is there a register.js?
- Hunt through all custom .js files
- What parameters are used on this endpoint?
- Any listed in source or JS?
- Mobile version the same?



ACCOUNT REGISTRATION

- What is required to sign up?
Name, location, bio, email etc?
- Where is it reflected?
- Can I upload a photo?
- Follow the Upload section here



ACCOUNT REGISTRATION

- Can I enter < > in display name and profile description?
- What characters are allowed?
`<h2>` `<script>` `<script`
- Try the same on mobile registration
- Maybe XSS prevented in some places but still firing somewhere?



ACCOUNT REGISTRATION

- Can I register with a Social account?
- Is there an Oauth flow? Token Leak?
- Which social media accounts allowed?
- What info is trusted from social media?
- Import `<script>alert(0)</script>` as file name, album name etc.



ACCOUNT REGISTRATION

- Will it read `myemail%00@email.com` as `myemail@email.com`
- Is it the same on mobile app?
- Try `%00` and `%0d`



ACCOUNT REGISTRATION

- Can I sign up using [@target.com](#)
- Or is it blacklisted?
- If blacklisted - why?
- Bypass?



ACCOUNT REGISTRATION

- What happens when revisiting register page after signing up?
- Does it redirect?
- Can I control the redirect parameter?
- Resign up as authenticated user?
- Redirect parameter controllable?



Thank You!

Become a Successful
Bug Bounty Hunter