

- Filename: eccouncil-ceh31250-v11-14-4-1-csrf.md
- Show Name: CEHV11 (312-50)
- Topic Name: Web Application Hacking - Hacking Web Applications
- Episode Name: CSRF

=====

CSRF

Objectives:

- How does CSRF work?
 - Abuses trust relationship established between the victim and web app
 - Get user to do stuff they don't know about or intend to do
 - Requires an active session
- What do we need to make this work?
 - URL
 - A8: CSRF change password for user
 - Grab URL with Burp
 - Modify parameters to desired password
- How does this change the password for target?
 - Phishing/Social Engineering
 - `csrf.html`
 - If user has active session and clicks phish, then their password will be reset to attacker controlled value
- How can you make this work with XSS?
 - Find XSS (Stored works best)
 - `<script>new Image().src=</script>`
 - Check the account amount