Starting Bug hunting BtoA

Before Starting..

- Discover Subdomains. Tools: “Subfinder”, “Sublist3r”, “Amass”
- Discover URLS. Tools: “Gau”, “Waybackurls”
- Discover Parameter. Tools: “Paramspider”, “GF”
- Scan Host And Ports Using Nmap or Zenmap
- Gather Whois Information
- Gather more informations like “Site technologies”, “cname, dns” etc.

After Information Gathering

- Create 2 accounts on the same website if it has login functionality.
- Try directory brute forcing using tools like "Dirsearch", "Dirb" might be possible some directory may reveal sensitive information.

In the Login Page

- Check Session Expiration
- Check Improper Session Validation
- Check OAuth Bypass
    - OAuth Token Stealing
    - Authentication Bypass
    - SQL Injection (Broken Auth)

In the Registration Page

- Bypassing Mobile or Email Verification
- Brute Forcing OTP Sent
- Try inserting XSS payload wherever possible (Like if you can enter XSS payload in First Name/Last Name/Address etc text box make sure to enter because sometimes it may reflect somewhere else or maybe it's stored XSS).

In the Forgot Pass Page

- Password Reset Poisoning (Kind of similar way we do Host Header Injection)
- Reset Token/Link Expiring (Maybe they pay)
- Reset Token Leaks (This can happen when some website interacts to third party services at that point of time maybe password reset token is sent via referrer header part and maybe it can leak)

Deep Inside

- Test for Default Credentials on admin page/console or any sign in panel.
    - Try submitting default username passwords like "admin":"admin", "admin":"password"
- Check for Subdomain takeover
- SQL Injection: This method may depend on sql injection vuln.
- Check for Directory Traversal Includes File Input
    - You have to check each and every input which your website and its directories take from user

      ### Example

      https://example.com/getuserprofile.jsp?item=manager.html
      https://example.com/index.php?file=content

      https://example.com/getuserprofile.jsp?item=.../../../../etc/passwd
      https://example.com/index.php?file=https://evil.com/

- Check for Insecure Direct Object Reference
    - You can try for getting access to other user data by changing parameter in url.

      ### Example

      https://example.com/user?id=1 https://example.com/user?id=2

- Check for XSS (Stored, Reflected, Blind)
- Check for SQL Injection
- Check for File Upload (Shell Upload)
- Check for Open Redirection

  ### Example

  https://example.com/redirect?url=https://google.com