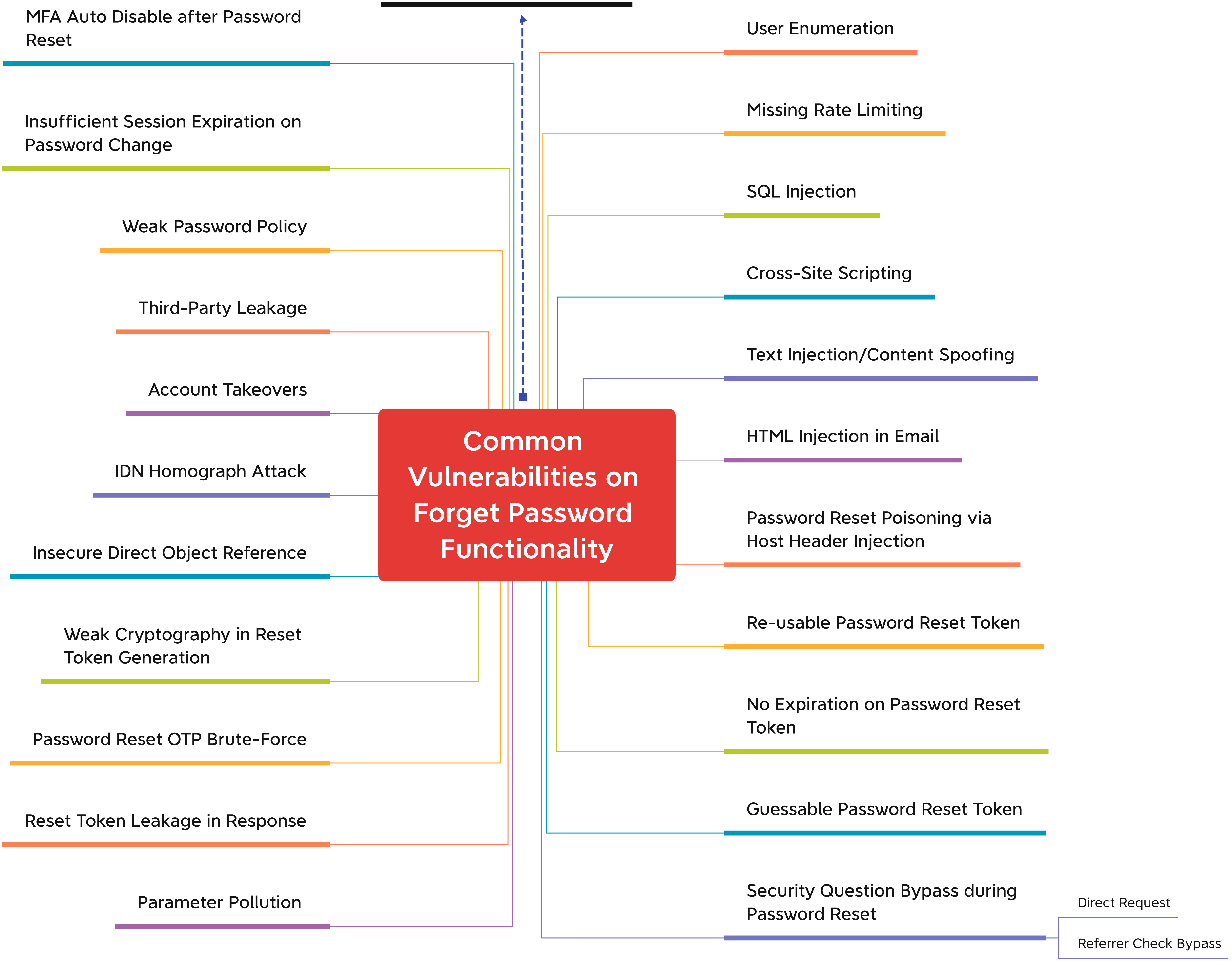
MindMap By: Harsh Bothra
Twitter: @harshbothra_
https://harshbothra.tech



Common Vulnerabilities on Forget Password Functionality

- MFA Auto Disable after Password Reset
- Insufficient Session Expiration on Password Change
- Weak Password Policy
- Third-Party Leakage
- Account Takeovers
- IDN Homograph Attack
- Insecure Direct Object Reference
- Weak Cryptography in Reset Token Generation
- Password Reset OTP Brute-Force
- Reset Token Leakage in Response
- Parameter Pollution
- User Enumeration
- Missing Rate Limiting
- SQL Injection
- Cross-Site Scripting
- Text Injection/Content Spoofing
- HTML Injection in Email
- Password Reset Poisoning via Host Header Injection
- Re-usable Password Reset Token
- No Expiration on Password Reset Token
- Guessable Password Reset Token
- Security Question Bypass during Password Reset
  - Direct Request
  - Referrer Check Bypass