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

Vulnerability Checklist for SAML

- Golden SAML Attack
- XML External Entities
- Certificate Injection Attack
- Certificate Faking Attack
- Tools & Burp Extensions
  - SAML Raider
- Labs & Resources
  - https://github.com/yogisec/VulnerableSAMLApp
  - https://github.com/dogangcr/vulnerable-sso
- References
  - https://workos.com/blog/fun-with-saml-sso-vulnerabilities-and-footguns
  - https://github.com/harsh-bothra/learn365/blob/main/days/day3.md
  - https://research.aurainfosec.io/bypassing-saml20-SSO/
  - http://sso-attacks.org/Category:Attack_Categorisation_By_Attack_on_SAML
  - https://epi052.gitlab.io/notes-to-self/blog/2019-03-07-how-to-test-saml-a-methodology/
  - https://epi052.gitlab.io/notes-to-self/blog/2019-03-13-how-to-test-saml-a-methodology-part-two/
  - https://epi052.gitlab.io/notes-to-self/blog/2019-03-16-how-to-test-saml-a-methodology-part-three/
  - https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/SAML_Security_Cheat_Sheet.md
  - https://research.nccgroup.com/2021/03/29/saml-xml-injection/
  - https://www.sygnia.co/golden-saml-advisory
- XML Signature Wrapping Attacks [XSW]
- SAML XML Injection
- SAML Message Integrity Abuse
- Missing/Invalid Signature
- SAML Message Replay
- Cross-Site Request Forgery
- XML Comment Handling
- XSLT
- Token Recipient Confusion