XML Attacks

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

SOAP Attacks

- SOAP Action Spoofing
  - https://www.ws-attacks.org/SOAPAction_Spoofing
- Replay Attacks
  - https://www.ws-attacks.org/Replay_Attack
- WSDL Enumeration
  - https://www.ws-attacks.org/WSDL_Disclosure
- SOAP Parameter DOS
- SOAP Array Attack

XML Signature Attacks

- XSLT Code Execution
  - https://www.ws-attacks.org/XML_Signature_%E2%80%93_XSLT_Code_Execution
- XML Signature - Key Retrieval XSA (Cross Site Attack)
  - https://www.ws-attacks.org/XML_Signature_-_Key_Retrieval_XSA_(Cross_Site_Attack)
- XML Signature Exclusion
- XML Signature Wrapping
- Denial of Service
  - Key Retrieval DOS
  - Transformation DOS
    - C14N DOS
    - XSLT DOS
    - XPATH DOS
  - https://www.ws-attacks.org/XML_Signature_%E2%80%93_Transformation_DOS

Misc.

- Attack Obfuscation
  - https://www.ws-attacks.org/Attack_Obfuscation
- Metadata Spoofing
  - WSDL Spoofing
  - WS Security Policy Spoofing
  - https://www.ws-attacks.org/Metadata_Spoofing
- Active WS-MITM
  - Malicious Morphing
  - Routing Detour
- Passive WS-MITM
- Coercive Parsing

References

- https://www.agarri.fr/fr/publications.html
- https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/XML_Security_Cheat_Sheet.md
- https://www.ws-attacks.org/
- https://www.slideshare.net/ssuserf09cba/xxe-how-to-become-a-jedi
- https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/XXE%20Injection
- https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html
- https://github.com/omurugur/XXE_Payload_List
- https://github.com/HLOverflow/XXE-study
- https://github.com/reddelexc/hackerone-reports/blob/master/tops_by_bug_type/TOPXXE.md
- https://gosecure.github.io/xxe-workshop/#0
- https://mohemiv.com/all/exploiting-xxe-with-local-dtd-files/

XSLT Attack

- References
  - https://www.blackhat.com/docs/us-15/materials/us-15-Arnaboldi-Abusing-XSLT-For-Practical-Attacks-wp.pdf
  - https://vulncat.fortify.com/en/detail?id=desc.dataflow.java.xslt_injection
  - https://book.hacktricks.xyz/pentesting-web/xslt-server-side-injection-extensible-stylesheet-languaje-transformations
  - https://www.contextis.com/en/blog/xslt-server-side-injection-attacks
- Cross-Site Scripting
- Arbitrary File Read
- Code Execution
- SSRF
- Data Exfiltration & XXE

Oversized XML Attack

- Oversized SOAP Header
- Oversized SOAP Body
- Oversized SOAP Envelope
- XML Extra Long Names
- XML Namespace Prefix Attack
- XML Oversized Attribute Content
- XML Oversized Attribute Count

Denial of Service

- XML Entity Expansion
  - Billion Laugh Attack
  - Quadratic Blowup Attack
  - Recursive Entity Reference
- XML Flooding
- Reference Redirect Attack
  - Signature Redirect
  - Encryption Redirect

XPATH Injection

- http://projects.webappsec.org/w/page/13247005/XPath%20Injection#:~:text=XPath%20Injection%20is%20an%20attack,query%20or%20navigate%20XML%20documents.
- https://www.soapui.org/docs/security-testing/security-scans/xpath-injection/
- https://rhinosecuritylabs.com/penetration-testing/xpath-injection-attack-defense-techniques/

XML Injection

- http://projects.webappsec.org/w/page/13247004/XML%20Injection
- https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/07-Testing_for_XML_Injection
- https://research.cs.wisc.edu/mist/SoftwareSecurityCourse/Chapters/3_8_4-XML-Injections.pdf

XML External Entities

- Tools
  - XXEServe (https://github.com/joernchen/xxeserve)
  - XXExploiter (https://github.com/luisfontes19/xxexploiter)
  - XXEinjector (https://github.com/enjoiz/XXEinjector)
  - 230-OOB (https://github.com/lc/230-OOB)
  - OXML_XXE (https://github.com/BuffaloWill/oxml_xxe)
  - DOCEM (https://github.com/whitel1st/docem)
- General/Classical XXE
  - Simple Payload Processing
  - Base64 Payload Processing
- XXE with Wrappers
  - data://
  - phar://
  - rar://
  - php://
  - expect://
  - Can result into RCE
- Xincludes based XXE
- Blind XXE
- XXE with Local DTD
- Error Based XXE
- Attack Chaining
  - SSRF
  - Local File Read
  - Denial of Service
    - Large File Retrieval
    - Entity Reference Attack
  - Windows Share Stealing
  - Remote Code Execution
  - Port Scanning
  - Pass The Hash
- XXE via various Files
  - XXE via SVG
    - General Payload Processing
    - OOB via SVG rasterization
  - OOXML (DOCX, XLSX, PPTX), ODF, PDF, RSS
  - XXE inside DTD file
  - XXE via SOAP
  - XXE via XMP
  - Other XML Processing: XMLRPC, WebDAV, SOAP, XMPP, SAML

SAML XML Injection

- https://research.nccgroup.com/2021/03/29/saml-xml-injection/

Note: Some of these techniques may not be actively exploitable. However, always good to look for the possibilities

Review Credits & Thanks:

Avinash K. Thapa - @iw00tr00t
Yatin Sirpaul - @ysirpaul
Aditya Dixit - @zombie007o
Mukesh Kumar - @hack_logic
Jesus A. Espinoza - @ArthusuxD