XML External Entity-Attacke

Christopher Christensen

XXE

XML External Entity-Attacke

- Analyse von XML-Eingaben durch schwach konfigurierten XML-Parsern ausgenutzt
- Kann zur Offenlegung vertraulicher Daten, DoS und anderen Auswirkungen führen
- seit 2017 bis Platz 4 in OWASP Top 10

Wo liegt die Schwachstelle von XML?

- Links (im XML) zu anderen Dateien / Ressourcen

Wie funktionert XXE?

- Wenn XML geparst wird, folgt XML-Parser den Links und liest verknüpftes Dokument
- Wenn Angreifer Ausgabe des geparsten XMLs sehen kann, hat er Möglichkeit, lokale Dateien auf dem Server zu lesen
- Missbraucht externe Entitäten

Risikofaktoren von XXE

- Anwendung analysiert XML-Dokumente
- Verfälschte Daten sind innerhalb des Systemidentifikators der Entität in der Dokumenttypdeklaration (DTD) erlaubt
- XML-Prozessor ist für Validierung und Verarbeitung der DTD konfiguriert
- XML-Prozessor ist konfiguriert, dass er externe Entitäten innerhalb der DTD auflöst

Passwort von Linux-System mit XXE auslesen

- Beispiel

```
<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE foo [

    <!ELEMENT foo ANY >

    <!ENTITY xxe SYSTEM "file:///etc/passwd" >]>

<foo>&xxe;</foo>
```

Mitigation von XXE

- XML-Prozessor konfigurieren, dass er
  - eine lokale statische DTD verwendet
  - deklariert DTD, die im XML sind, verbietet
- Sicherste Weg
  - DTDs vollständig deaktivieren
  - `factory.setFeature("http://apache.org/xml/features/disallow-doctype-decl", true);`