EXPLOITING XXE IN FILE UPLOAD FUNCTIONALITY

BLACKHAT WEBCAST - 11/19/15

Will Vandevanter - @_will_is_

Agenda (30 minutes):

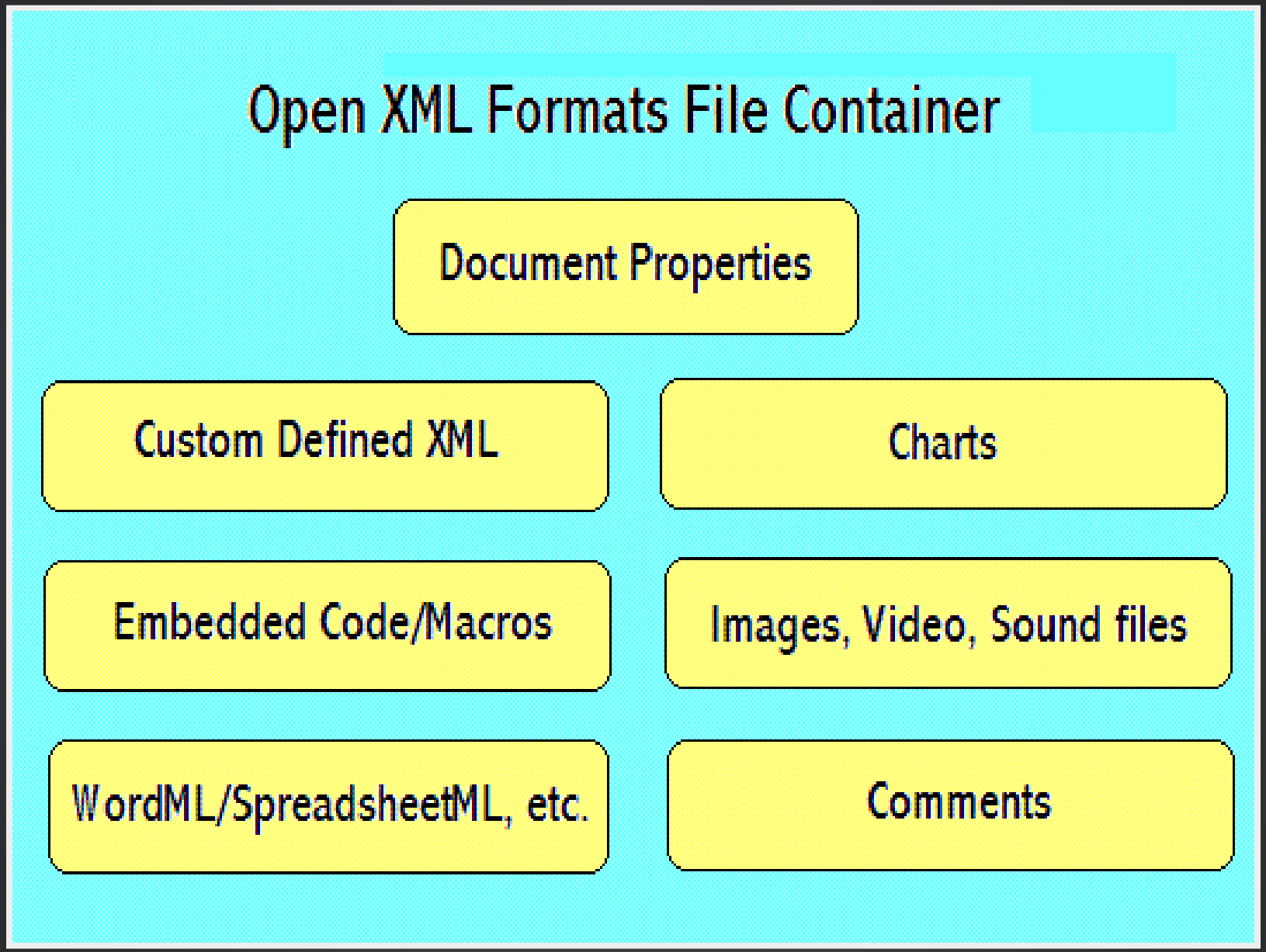
- OOXML Format, Demo
- Other File Formats, Demo
- Further Exploitation

Slides, References, and Code:

oxmlxxe.github.io

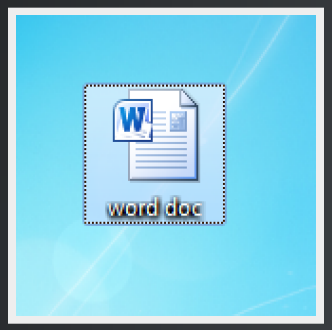
OFFICE OPEN XML (OPENXML; OOXML; OXML)

- *.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

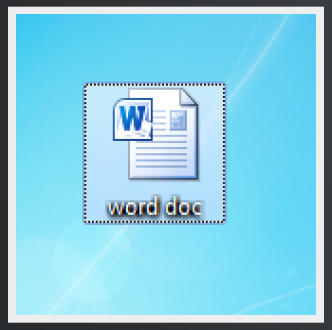



```
 images.docx

   Name
   ----
   [Content_Types].xml
   _rels/.rels
   word/_rels/document.
   word/document.xml
   word/theme/theme1.xm
```

```
<?xml version="1.0" e
<!DOCTYPE [EXPLOIT HE
    <w:webSettings xm
    http://schemas.op
    openxmlformats.or
    com/office/word/2
    <w:optimizeForBro
    <w:allowPNG/>
</w:webSettings>
```

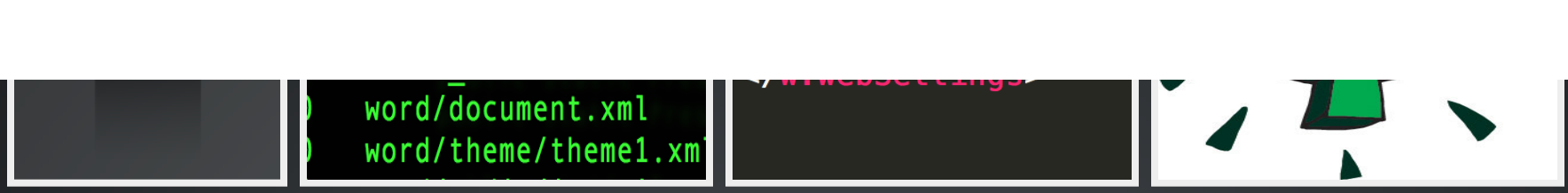
```
adding: [Content_Types].xm
adding: _rels/ (stored 0%)
adding: _rels/.rels (deflat
adding: customXml/ (stored
adding: customXml/_rels/ (s
adding: customXml/_rels/ite
adding: customXml/item1.xm
adding: customXml/itemProps
```



```
 images.docx

   Name
   ----
   [Content_Types].xml
   _rels/.rels
   word/_rels/document.
```

```
<?xml version="1.0" e
<!DOCTYPE [EXPLOIT HE
    <w:webSettings xm
    http://schemas.op
    openxmlformats.or
    com/office/word/2
    <w:optimizeForBro
    <w:allowPNG/>
</w:webSettings>
```



BUG BOUNTY: SLACK.COM

- File Sharing Functionality

BUG BOUNTY: FACEBOOK CAREERS

- Q4 2014 - Mohamed Ramadan
- Resume Upload Functionality

OXML_XXE DEMO

XXE in docx

PDF XXE

- Javascript that included XML with an XXE
  - Exploited in Adobe Reader 7; 2005-06-15
- Extensible Metadata Platform (XMP)
  - ISO Standard, Created by Adobe
  - Provides support for metadata without breaking readability

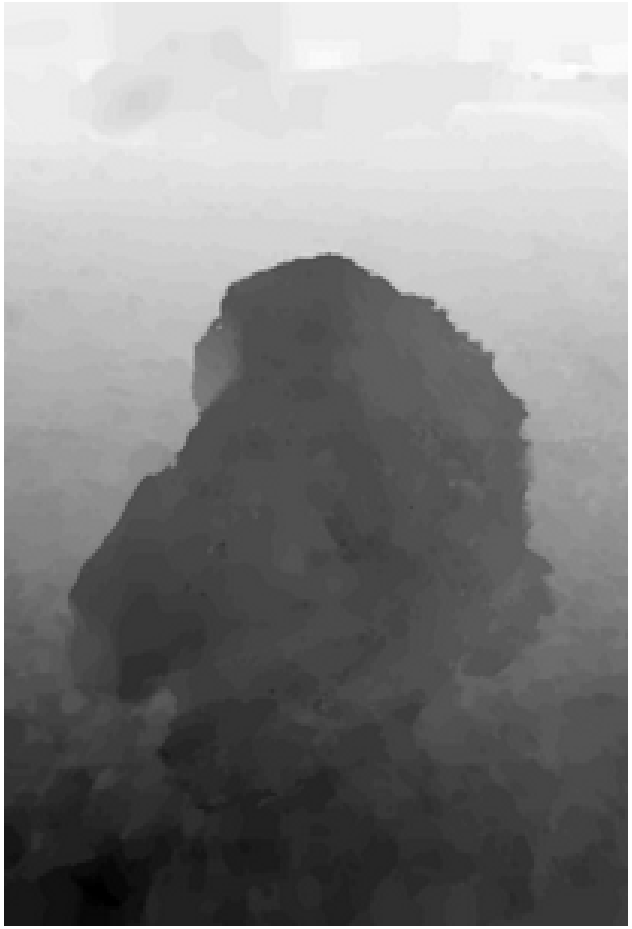
0XML_XXE DEMO

XXE in PDF

XMP IN IMAGE FORMATS

- GIF, PNG
- JPG
  - Lens Blur Camera Photo Feature

One of several input photos



Depth map (black close, white far)

Photo by Colby Brown

Photo with Lens Blur

Google Research - "Lens Blur in the new Google Camera App" (04/16/14)

```
<x:xmpmeta xmlns:x="adobe:ns:meta/" x:xmptk="Adobe XMP Core 5.1.0-jc003">
  <rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#">
    <rdf:Description rdf:about=""
        xmlns:GFocus="http://ns.google.com/photos/1.0/focus/"
        xmlns:GImage="http://ns.google.com/photos/1.0/image/"
        xmlns:GDepth="http://ns.google.com/photos/1.0/depthmap/"
        xmlns:xmpNote="http://ns.adobe.com/xmp/note/"
      GFocus:BlurAtInfinity="0.0083850715"
      GFocus:FocalDistance="18.49026"
      GFocus:FocalPointX="0.5078125"
      GFocus:FocalPointY="0.30208334"
      GImage:Mime="image/jpeg"
      GDepth:Format="RangeInverse"
```

```java
 * Take in a file and parse XMP data from it
import java.io.File;

public class SampleUsage {
    public static void parseXMPJPEG(final File file){
        try {
            ByteSource byteSource = new ByteSourceFile(file);
            String xmp = new JpegImageParser().getXmpXml(byteSource, null);
            DocumentBuilderFactory factory = DocumentBuilderFactory.newInstance();
            DocumentBuilder builder = factory.newDocumentBuilder();
            InputSource is = new InputSource(new StringReader(xmp));

            // parse XMP/XML
            System.out.println(builder.parse(is));

        } catch (Exception e) {
                e.printStackTrace();
            }
    }
```

0XML_XXE DEMO

XXE in JPG

XML ENTITY

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

DOCX

/word/document.xml

PPTX

/ppt/presentation.xml

XLSX

/xl/workbook.xml

+0XML_XXE

XSS Testing

< !ENTITY post "<script>alert(1)...

< !ENTITY post "< ![CDATA[<script>alert(1)...

LFI

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

+OXML FEATURES

- hlinkHover
- XSLTransform
- Embedded "Documents"
- SSRF

+TESTING CHEATSHEET

Classic (X)XE

Canary Testing DTD and XE

XSS XE testing (CDATA/plain/attr)

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

Thanks!

http://oxmlxxe.github.io