

HTB x Uni CTF 2020 - Qualifications

Solver: Will Green (UAHDucky)

Challenge: kapKan

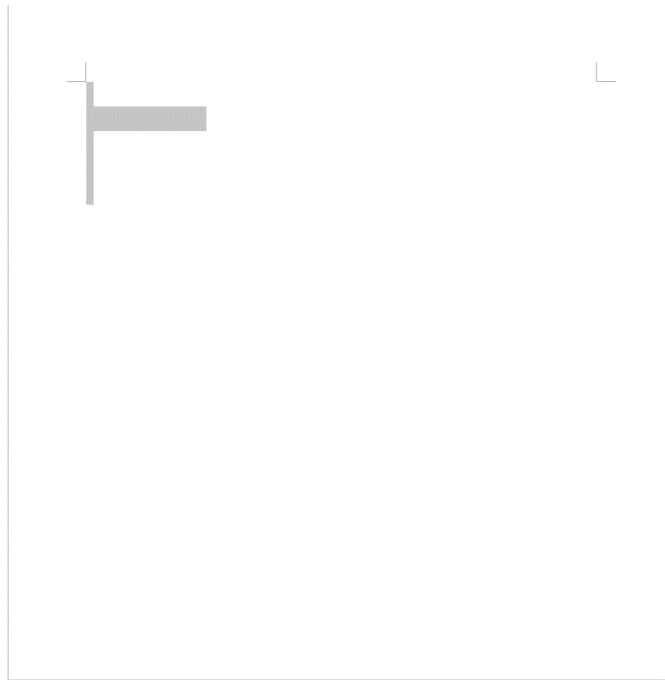
Category: Forensics

Intro:

In this challenge we are given a Word document (.docx) which we are told is very likely to contain malicious code.

Walkthrough:

If we open the document, it appears to be empty except some new line characters:



Trying to view macros shows that there's at least not any visible to us, so my next train of thought was that from previous CTF experience and just general knowledge I know that .docx file formats are actually comprised of multiple XML files in a ZIP archive:

# File Format Specifications

A Docx file comprises of a collection of XML files that are contained inside a ZIP archive. The contents of a new Word document can be viewed by unzipping its contents. The collection contains a list of XML files that are categorized as:

- MetaData Files - contains information about other files available in the archive
- Document - contains the actual contents of the document



So since there's some empty lines, maybe there's some hidden text within the xml files? Changing the file type and unzipping, we're presented with the .xml files. The "document.xml" contains the actual contents of the document as mentioned in the above screenshot, so I opened that document first. We're presented with a pretty ugly .xml document but if we continue scrolling we can see what appears to be some ASCII character encoding:

```
com:office:word"
xmlns:w="http://schemas.openxmlformats.org/wordprocessingml/2006
/main" xmlns:w14
="http://schemas.microsoft.com/office/word/2010/wordml"
xmlns:w15="http://schemas.microsoft.com/office/word/2012/wordml"
xmlns:w16cid="http://schemas.microsoft.com/office/word/2016/word
ml/cid"
xmlns:w16se="http://schemas.microsoft.com/office/word/2015/wordm
l/symex"
xmlns:wpg="http://schemas.microsoft.com/office/word/2010/wordpro
cessingGroup"
xmlns:wpi="http://schemas.microsoft.com/office/word/2010/wordpro
cessingInk"
xmlns:wne="http://schemas.microsoft.com/office/word/2006/wordml"
xmlns:wps="http://schemas.microsoft.com/office/word/2010/wordpro
cessingShape" mc:Ignorable="w14 w15 w16se w16cid wpl4"><w:body>
<w:p w:rsidR="00830AD6" w:rsidRDefault="00830AD6"
w:rsidP="00830AD6"><w:r><w:fldChar w:fldCharType="begin"/></w:r>
<w:r><w:instrText xml:space="preserve"> </w:instrText></w:r>
<w:r><w:instrText>SET c</w:instrText></w:r><w:r><w:instrText
xml:space="preserve"> </w:instrText></w:r><w:r>
<w:instrText>"</w:instrText></w:r><w:fldSimple w:instr=" QUOTE
112 111 119 101 114 115 104 101 108 108 32 45 101 112 32 98 121
112 97 115 115 32 45 101 32 83 65 66 85 65 69 73 65 101 119 66
69 65 68 65 65 98 103 65 51 65 70 56 65 78 65 65 49 65 69 115 65
88 119 66 78 65 68 77 65 88 119 66 111 65 68 65 65 86 119 66 102
65 68 69 65 78 119 66 102 65 72 99 65 77 65 66 83 65 69 115 65
78 81 66 102 65 69 48 65 78 65 65 51 65 68 77 65 102 81 65 61
"><w:r><w:rPr><w:b/><w:noProof/></w:rPr><w:instrText>
</w:instrText></w:r><w:fldSimple><w:r>
<w:instrText>"</w:instrText></w:r><w:r><w:instrText
xml:space="preserve"> </w:instrText></w:r><w:r><w:fldChar
w:fldCharType="end"/></w:r><w:p w:rsidR="00830AD6"
w:rsidRDefault="00830AD6" w:rsidP="00830AD6"><w:r><w:fldChar
w:fldCharType="begin"/></w:r><w:r><w:instrText
xml:space="preserve"> </w:instrText></w:r><w:r><w:instrText>SET
d</w:instrText></w:r><w:r><w:instrText xml:space="preserve">
"</w:instrText></w:r><w:fldSimple w:instr=" QUOTE "><w:r>
<w:rPr><w:b/><w:noProof/></w:rPr><w:instrText> </w:instrText>
</w:r></w:fldSimple><w:r><w:instrText xml:space="preserve">"
</w:instrText></w:r><w:r><w:fldChar w:fldCharType="end"/></w:r>
</w:p><w:p w:rsidR="00830AD6" w:rsidRDefault="00830AD6"
w:rsidP="00830AD6"><w:r><w:fldChar w:fldCharType="begin"/></w:r>
<w:r><w:instrText xml:space="preserve"> </w:instrText></w:r>
<w:r><w:instrText>SET e</w:instrText></w:r><w:r><w:instrText
xml:space="preserve"> "</w:instrText></w:r><w:fldSimple
w:instr=" QUOTE "><w:r><w:rPr><w:b/><w:noProof/></w:rPr>
<w:instrText> </w:instrText></w:r></w:fldSimple><w:r>
<w:instrText xml:space="preserve">" </w:instrText></w:r><w:r>
<w:fldChar w:fldCharType="end"/></w:r></w:bookmarkStart w:id="0"
```

So let's go convert that to text:

### Convert ASCII to Text

112 111 119 101 114 115 104 101 108 108  
32 45 101 112 32 98 121 112 97 115 115 32  
45 101 32 83 65 66 85 65 69 73 65 101 119  
66 69 65 68 65 65 98 103 65 51 65 70 56 65  
78 65 65 49 65 69 115 65 88 119 66 78 65  
68 77 65 88 119 66 111 65 68 65 65 86 119  
66 102 65 68 69 65 78 119 66 102 65 72 99  
65 77 65 66 83 65 69 115 65 78 81 66 102  
65 69 48 65 78 65 65 51 65 68 77 65 102 81  
65 61

↔

```
powershell -ep bypass -e  
SABUAEIAewBEADAAbgA3AF8ANAA1AEsAX  
wBNADMAXwBoADAAVwBfADEANwBfAHcA  
MABSAEsANQBfAE0ANAA3ADMfQA=
```

Lines: 1

It appears to be Powershell command to bypass the execution policy, definitely malicious! There's a Base64 string there, so let's also decode that:

### Decode from Base64 format

Simply enter your data then push the decode button.

SABUAEIAewBEADAAbgA3AF8ANAA1AEsAXwBNADMAXwBoADAAVwBfADEANwBfAHcAMABSAEsANQBfAE0ANAA3ADMfQA=

For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

AUTO-DETECT

▼

Source character set.

☐ Decode each line separately (useful for multiple entries).

Live mode OFF

Decodes in real-time when you type or paste (supports only UTF-8 character set).

< DECODE >

Decodes your data into the textarea below.


H T B ( D 0 n 7 \_ 4 5 K \_ M 3 \_ h 0 W \_ 1 7 \_ w 0 R K 5 \_ M 4 7 3 ) 

That looks like the flag! Let's remove those replacement characters:

### Decode from Base64 format


Simply enter your data then push the decode button.

```
SABUAEIAewBEADAAbgA3AF8ANAA1AEsAXwBNADMAXwBoADAAVwBfADEANwBfAHcAMABSAEsANQBfAE0ANAA3ADM  
AfQA=
```

 For encoded binaries (like images, documents, etc.) use the file upload form a bit further down on this page.

AUTO-DETECT  Source character set

☐ Decode each line separately (useful for multiple entries).

 Live mode OFF Decodes in real-time when you type or paste (supports only UTF-8 character set).

**< DECODE >** Decodes your data into the textarea below.

```
HTB{D0n7_45K_M3_h0W_17_w0RK5_M473}
```

Flag: HTB{D0n7\_45K\_M3\_h0W\_17\_w0RK5\_M473}