

Write-up Meta

Player: Constantine

Kategori: Forensik

Challenge

53 Solves

✕

Meta


100

Easy-Medium

"Do you want to play a game?" - A mysterious voice echoed in your computer. You think you've been hacked. Suddenly, a file named "game.docx" appears on your desktop. You open it and find a riddle inside:

"The code is hidden in plain sight," the riddle reads.

author: BbayuGt

 meta.docx

Flag

Submit

Konteks Dikit

Kita semua tau kalau file .docx itu sebenarnya cuma file ZIP yang lagi cosplay jadi dokumen. Isinya full XML. Challenge ini mainin konsep itu, ada hidden data yang diselipin di sela-sela tag XML yang nggak bakal dirender sama word processor seperti libreoffice, msoffice, atau onlyoffice. Misi kita extract file flag.7z yang kekunci.

Phase 1: Recon

Awalnya kita dapet .docx, lalu kita extract isinya. Setelah extract, kita punya output folder structure hasil unzip, hal pertama yang dilakuin adalah mapping aset pake tree.

```
constantine ~/0precForesty/Meta (solved) 22:17 > ls
drwxr-xr-x  constantine 12 Nov 17:03  meta_extracted
-rw-r--r--  53 constantine 13 Nov 10:17  .flag.txt.kate-swp
-rw-r--r--  36 constantine 11 Nov 13:10  flag.txt
-rw-r--r-- 26k constantine 12 Nov 17:00  meta.docx

constantine ~/0precForesty/Meta (solved) 22:17 > cd meta_extracted/

constantine .../0precForesty/Meta (solved)/meta_extracted 22:17 > tree -a
.
├── [Content_Types].xml
├── docProps
│   ├── app.xml
│   ├── core.xml
│   ├── flag.7z
│   └── flag.txt
├── _rels
│   └── .rels
├── word
│   ├── document.xml
│   ├── endnotes.xml
│   ├── fontTable.xml
│   ├── footnotes.xml
│   ├── _rels
│   │   ├── comments.xml.rels
│   │   ├── document.xml.rels
│   │   ├── endnotes.xml.rels
│   │   └── footnotes.xml.rels
│   ├── settings.xml
│   ├── styles.xml
│   ├── theme
│   │   └── theme1.xml
│   └── webSettings.xml
└── 6 directories, 18 files

constantine .../0precForesty/Meta (solved)/meta_extracted 22:17 >
```

Mataku langsung tertuju ke direktori docProps/. Di situ ada 2 kandidat kuat:

1. flag.txt (Terlalu obvious?)
2. flag.7z (Ini pasti targetnya)

Nah, aku coba cat flag.txt buat mastiin. Dan bener aja, isinya decoy: **Boong yahahahaah**

```
constantine .../OprecForesty/Meta (solved)/meta_extracted 22:17 > cat docProps/flag.txt
Boong yahahahaah
```

Jadi, targetnya jelas flag.7z. Tapi pas aku coba extract, dia minta password. Bruteforce is not the way, jadi pasti kuncinya ada di sekitar sini.

Phase 2: XML Analyze

Kita pindah dulu ke /word. File paling penting di struktur DOCX itu word/document.xml karena di situ body teks aslinya berada. Aku buka file itu dan mulai scanning pola aneh. Aku nemu satu paragraph tag yang suspicious parah. Di UI mungkin cuma keliatan "Password?: Somewhere :)", tapi di source codenya ada ini:

```
73      <w:t xml:space="preserve">Password?: </w:t>
74    </w:r>
75  <w:r>
76    <w:rPr>
77      <w:highlight w:val="none" />
78    </w:rPr>
79  <w:t xml:space="preserve">Somewhere :)
80    <!-- https://chat.whatsapp.com/KohSeAlZlIN4uQvpSqhejr
81    -->
      </w:t>
```

Boom! Ada HTML Comment Tag.

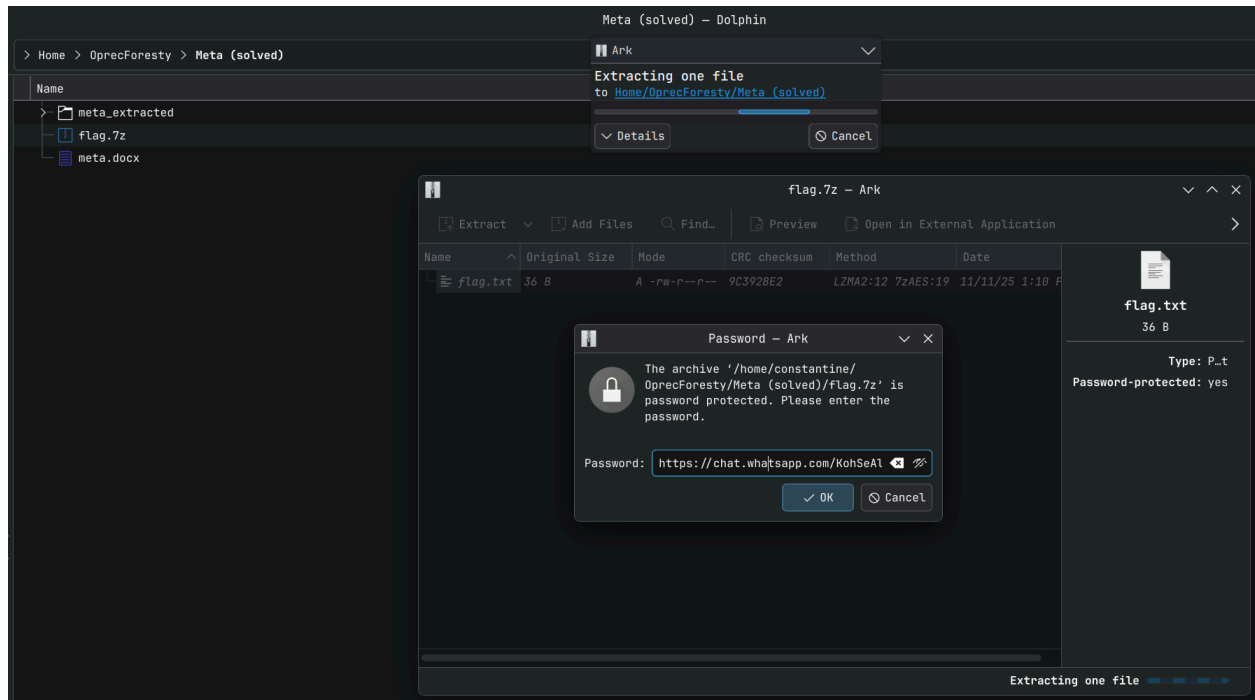
Parser Microsoft Word bakal ignore apapun yang ada di dalam tag komentar ini saat rendering. Jadi, ini tempat sembunyi paling aman buat metadata rahasia. Isinya link grup WhatsApp TelSec.

Phase 3: Execution

Awalnya aku mikir, passwordnya pasti string unik di belakang URL itu (KohSeAlZlIN4uQvpSqhejr). Aku coba extract... Access Denied. Ternyata, passwordnya bukan parsial, tapi full URLnya.

Payload Password: <https://chat.whatsapp.com/KohSeAlZlIN4uQvpSqhejr>

Langsung aku extract aja pakai Ark:



Archive extracted. Bagian Flag.txt kita cat aja:

```
constantine ~/OprecForesty/Meta (solved) 22:44 > ls
drwxr-xr-x  constantine 12 Nov 17:03  meta_extracted
-rw-r--r--  53 constantine 13 Nov 10:17  .flag.txt.kate-swp
-rw-r--r-- 186 constantine 11 Nov 13:12  flag.7z
-rw-r--r--  36 constantine 11 Nov 13:10  flag.txt
-rw-r--r-- 26k constantine 12 Nov 17:00  meta.docx

constantine ~/OprecForesty/Meta (solved) 22:44 > cat flag.txt
FORESTY{3@5y??_r1Ght?_lm0aa00a0a00}

constantine ~/OprecForesty/Meta (solved) 22:44 >
```

Flagnya adalah **FORESTY{3@5y??_r1Ght?_lm0aa00a0a00}**