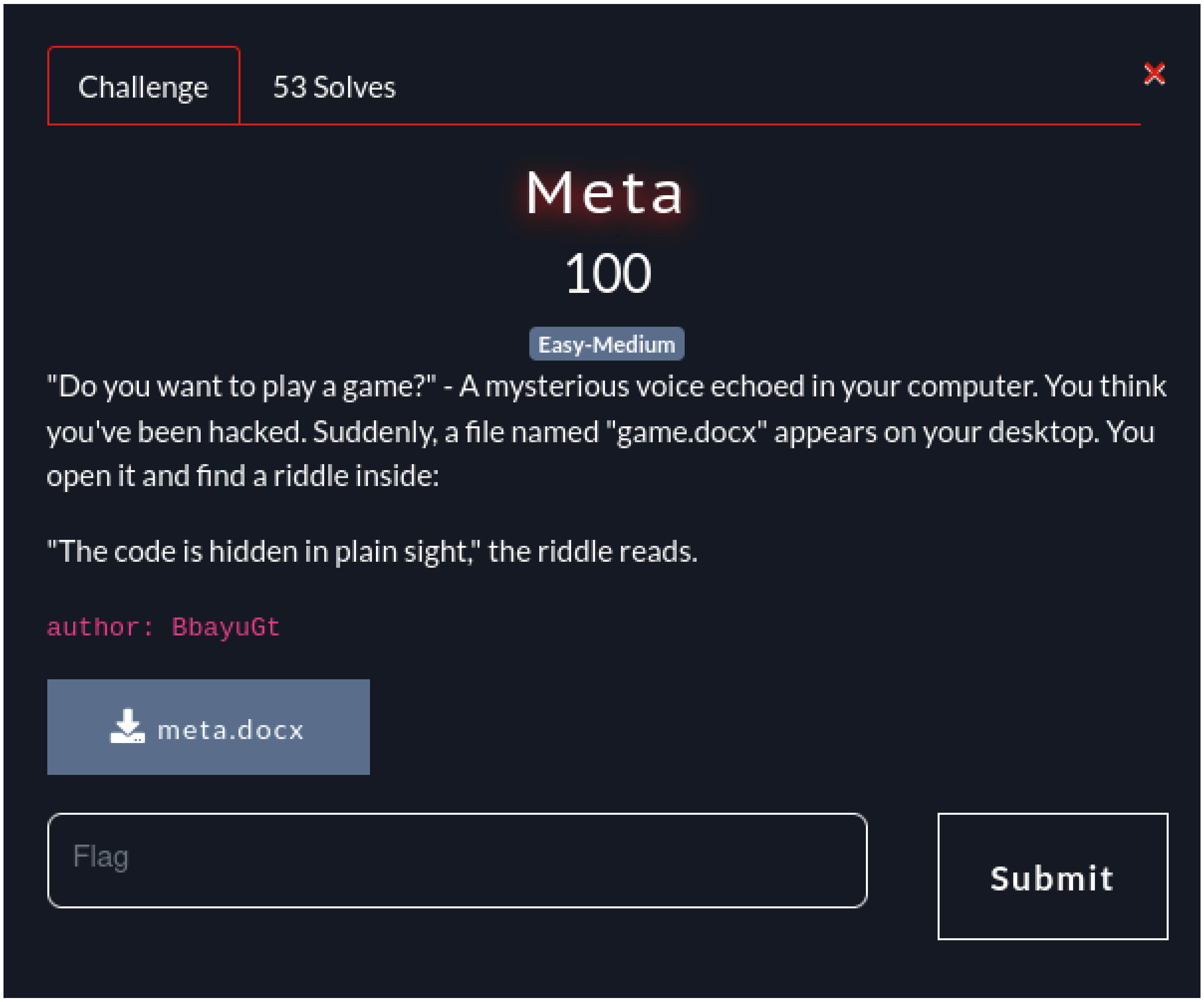
Meta

Player: constantine
Kategori: Forensik



Meta

100

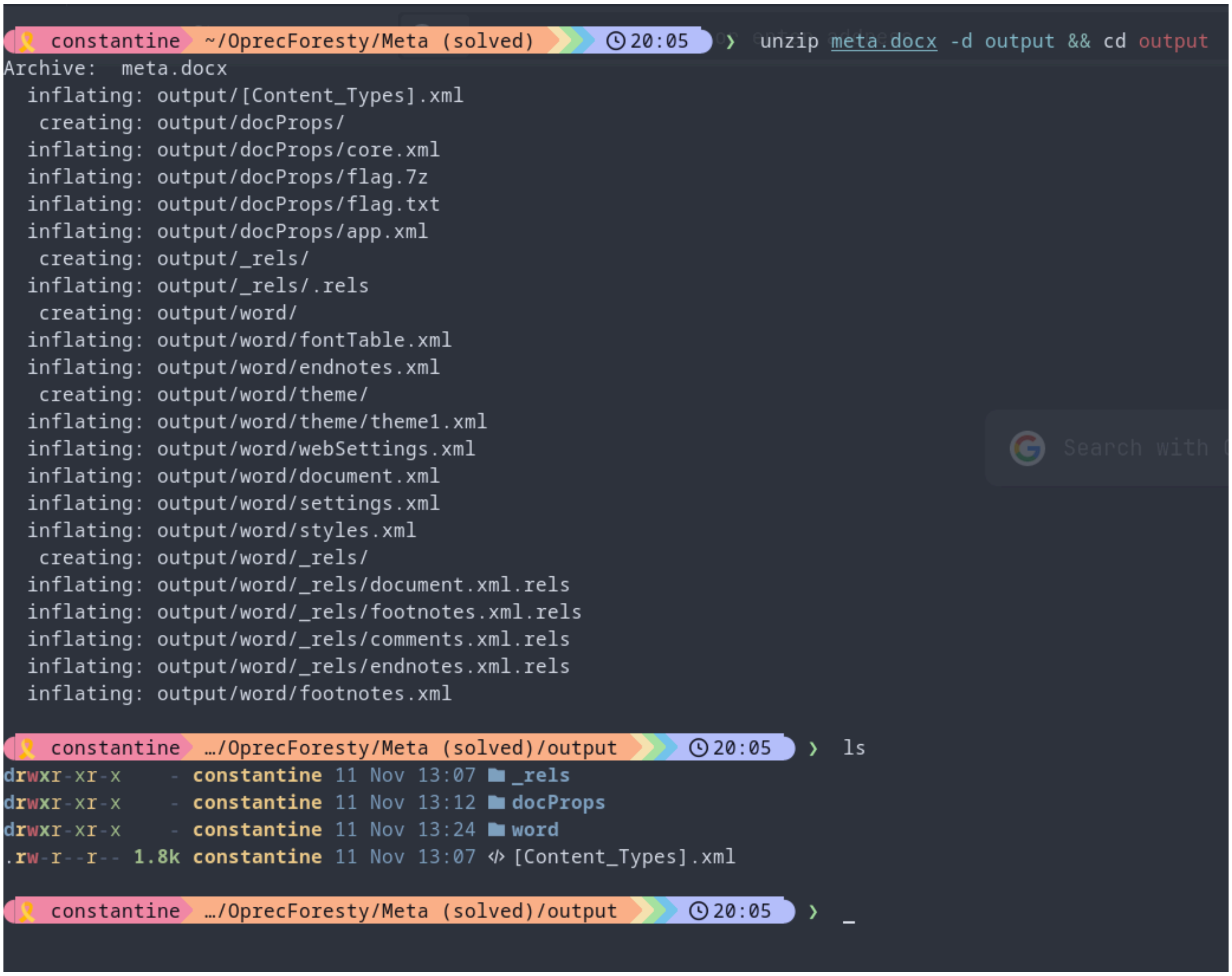
"Do you want to play a game?" - A mysterious voice echoed in your computer. You think you've been hacked. Suddenly, a file named "game.docx" appears on your desktop. You open it and find a riddle inside:

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

author: BbayuGt

Phase 1: Recon

File awal berupa **Meta.docx**. Sesuai standar, file .docx hanyalah ZIP berkedok dokumen. Maka langkah pertama:



```
 constantine  ~/OprecForesty/Meta (solved)  20:05  ❯ unzip meta.docx -d output && cd output
Archive:  meta.docx
  inflating: output/[Content_Types].xml
   creating: output/docProps/
  inflating: output/docProps/core.xml
  inflating: output/docProps/flag.7z
  inflating: output/docProps/flag.txt
  inflating: output/docProps/app.xml
   creating: output/_rels/
  inflating: output/_rels/.rels
   creating: output/word/
  inflating: output/word/fontTable.xml
  inflating: output/word/endnotes.xml
   creating: output/word/theme/
  inflating: output/word/theme/theme1.xml
  inflating: output/word/webSettings.xml
  inflating: output/word/document.xml
  inflating: output/word/settings.xml
  inflating: output/word/styles.xml
   creating: output/word/_rels/
  inflating: output/word/_rels/document.xml.rels
  inflating: output/word/_rels/footnotes.xml.rels
  inflating: output/word/_rels/comments.xml.rels
  inflating: output/word/_rels/endnotes.xml.rels
  inflating: output/word/footnotes.xml

 constantine  …/OprecForesty/Meta (solved)/output  20:05  ❯ ls
drwxr-xr-x    - constantine 11 Nov 13:07  _rels
drwxr-xr-x    - constantine 11 Nov 13:12  docProps
drwxr-xr-x    - constantine 11 Nov 13:24  word
.rw-r--r-- 1.8k constantine 11 Nov 13:07  [Content_Types].xml

 constantine  …/OprecForesty/Meta (solved)/output  20:05  ❯ _
```

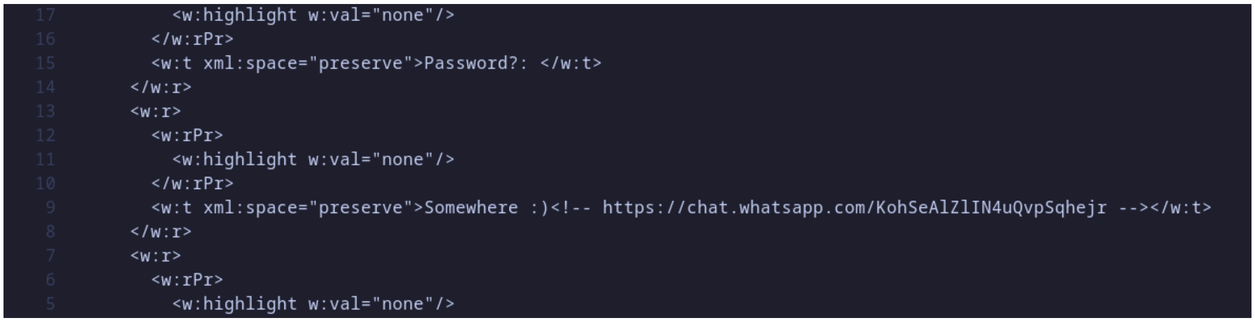
Setelah diekstrak, struktur folder muncul normal seperti file OOXML. Direktori yang paling mencolok adalah:

- docProps/flag.txt
- docProps/flag.7z

flag.txt hanya berisi decoy, jadi satu-satunya target valid adalah flag.7z. Saat diekstrak, file tersebut meminta **password**, sehingga kunci harus tersembunyi dalam struktur XML dokumen.

Phase 2: XML Analysis

Fokus beralih ke direktori /word/ karena semua konten utama .docx berada di sana, khususnya ***/word/document.xml***



```
          <w:highlight w:val="none"/>
        </w:rPr>
        <w:t xml:space="preserve">Password?: </w:t>
      </w:r>
      <w:r>
        <w:rPr>
          <w:highlight w:val="none"/>
        </w:rPr>
        <w:t xml:space="preserve">Somewhere :)<!-- https://chat.whatsapp.com/KohSeAlZlIN4uQvpSqhejr --></w:t>
      </w:r>
      <w:r>
        <w:rPr>
          <w:highlight w:val="none"/>
```

Berkas ini memuat teks yang ditampilkan oleh word processor. Pada bagian scanning manual, ditemukan sebuah paragraf yang secara visual di UI hanya menampilkan:

```
Password?: Somewhere :)
```

Tetapi pada level XML, paragraf tersebut menyembunyikan **HTML comment tag**:

```
<!-- https://chat.whatsapp.com/KohSeAlZlIN4uQvpSqhejr -->
```

Parser Word akan **mengabaikan isi komentar**, sehingga ini menjadi tempat yang “aman” bagi pembuat challenge untuk menyembunyikan password.

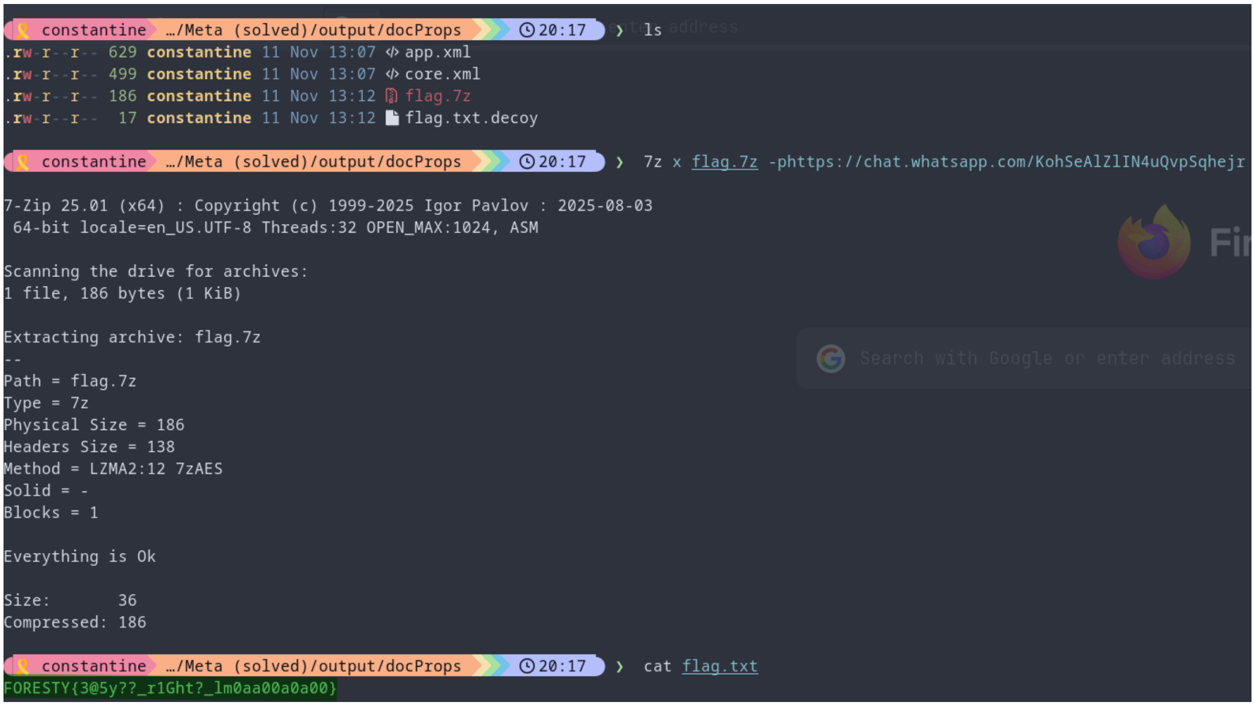
Phase 3: Execution

Awalnya terlihat passwordnya hanyalah bagian unik dari URL (KohSeAlZlIN4uQvpSqhejr), namun percobaan ekstraksi flag.7z menunjukkan:

- Partial string → **Access Denied**
- Full URL → **Password valid**

Correct Password: **https://chat.whatsapp.com/KohSeAlZlIN4uQvpSqhejr**

Kita extract aja flag.7z:



```
 constantine  …/Meta (solved)/output/docProps  20:17  ❯ ls
.rw-r--r-- 629 constantine 11 Nov 13:07 app.xml
.rw-r--r-- 499 constantine 11 Nov 13:07 core.xml
.rw-r--r-- 186 constantine 11 Nov 13:12 flag.7z
.rw-r--r--  17 constantine 11 Nov 13:12 flag.txt.decoy

 constantine  …/Meta (solved)/output/docProps  20:17  ❯  7z x flag.7z -phttps://chat.whatsapp.com/KohSeAlZlIN4uQvpSqhejr

7-Zip 25.01 (x64) : Copyright (c) 1999-2025 Igor Pavlov : 2025-08-03
 64-bit locale=en_US.UTF-8 Threads:32 OPEN_MAX:1024, ASM

Scanning the drive for archives:
1 file, 186 bytes (1 KiB)

Extracting archive: flag.7z
--
Path = flag.7z
Type = 7z
Physical Size = 186
Headers Size = 138
Method = LZMA2:12 7zAES
Solid = -
Blocks = 1

Everything is Ok

Size:       36
Compressed: 186

 constantine  …/Meta (solved)/output/docProps  20:17  ❯  cat flag.txt
FORESTY{3@5y??_r1Ght?_lm0aa00a0a00}
```

Isi flag.txt:

FORESTY{3@5y??_r1Ght?_lm0aa00a0a00}

Final Flag

FORESTY{3@5y??_r1Ght?_lm0aa00a0a00}