WRITE UP

BABAK PENYISIHAN

CAPTURE THE FLAG

HOLOGY 6.0

NAMA TIM

早上好中国！现在我有冰淇淋。

NAMA PERSONIL

1. Frendy Sanusi
2. Edbert Eddyson Gunawan
3. Frankie Huang

INSTITUSI ASAL

Institut Teknologi Bandung

Daftar Isi

4N6

[20] [His Idol]

[DESCRIPTION]
Why someone hold this poster so dearly, it's 23th year of this century already!

[HINT]
-

[Probsetter]
Hazbiy

Jadi pertama download file poster.jpg. Kemudian didapatkan dari exiftool sebuah string yang mencurigakan.

```
Creator Address                 : eqqmp://p.ry.xz.fa/lofdfkxi-fjxdb
```

Maka dari itu kita bruteforce caesar-cipher lalu didapatkan link dari original image nya (original-logo.jpg). Setelah itu kita cari perbedaan tiap byte antara 2 final tersebut. Berikut solver nya

```python
f1 = open('original_logo.jpg', 'rb').read()
f2 = open('poster.jpg', 'rb').read()

flag = b''
for i in range(len(f1)):
    if (f1[i] != f2[i]):
        print(f'{i}\t{f1[i]}\t{f2[i]}')
        flag += chr(f2[i]).encode()

```

Akan didapatkan

```
$ python3 diffcheck.py
18      0       72
3001    1       111
3004    0       108
3009    0       111
3031    0       103
3035    0       121
3037    0       54
3045    0       123
3053    0       89
3095    0       48
3123    0       117
3126    0       95
3155    0       103
3193    0       111
3216    0       84
3224    0       95
3252    0       77
3256    0       51
3269    0       125
b'Hology6{Y0u_goT_M3}'
```

[FLAG]
Hology6{Y0u_goT_M3}

[20] [Beep Boop]

[DESCRIPTION]
Why someone hold this poster so dearly, it's 23th year of this century already!

[HINT]
-

[Probsetter]
Hazbiy

Pertama kita download filenya lalu kita buka dengan audacity. Trus didapatkan flag.

[FLAG]
Hology6{W3_c4N_rE4D_s0uNd_1T_Se3mS}

CRY

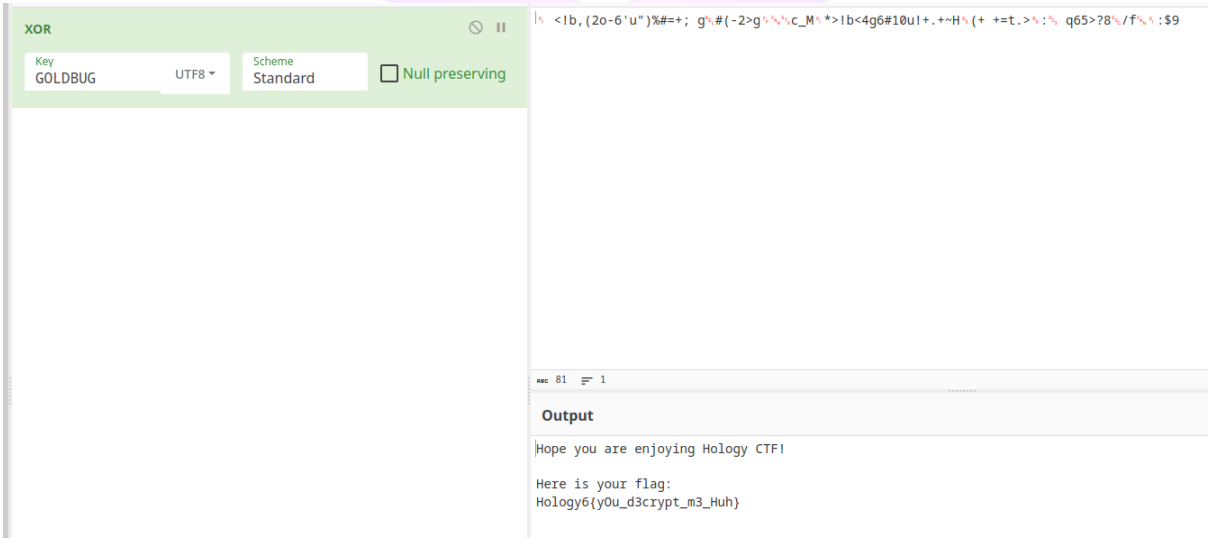
[20] [XOR]

[DESCRIPTION]
Today i visit a museum. It was an animal museum. While it was fun, i see some gold bug with strange name displayed It says "3‡0†2?3", what does that even mean?

[Probsetter]
Hazbiy

Steps

Dari soal, diberitahukan bahwa terdapat “gold bug”, yaitu sebuah cipher. Jika string "3‡0†2?3" di decrypt, maka akan didapatkan plaintext “GOLDBUG”. Kemudian, dari judul soal diketahui bahwa encrypted telah di-xor dengan suatu value. Maka, kami mencoba untuk mendekripsi ciphertext dengan key GOLDBUG.



[FLAG]
Hology6{yOu_d3crypt_m3_Huh}

WEB

[20] Holo Curl

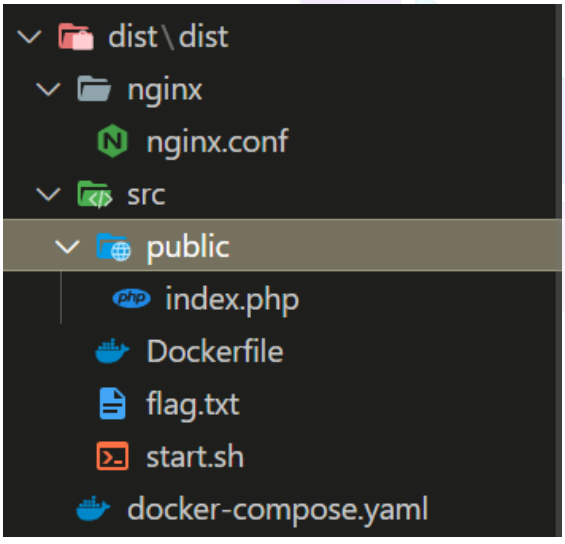
[DESCRIPTION]
The Holo Agency has built a web application that allows you to fetch content from other websites. Would you check it for me?

http://175.45.187.254:31530/

[Probsetter]
dimas

Steps

Diberikan struktur kode seperti berikut



nginx.conf

```
server {
    listen 8080;
    location / {
        rewrite / /index.php;
    }
    location ~\.php$ {
```

```
        root /var/www/html/public/;
        fastcgi_split_path_info ^(.+\.php)(/.+)$;
        fastcgi_pass php-fpm:9000;
        fastcgi_index index.php;
        include fastcgi_params;
                                        fastcgi_param     SCRIPT_FILENAME
$document_root$fastcgi_script_name;
        fastcgi_param PATH_INFO $fastcgi_path_info;
    }
}
```

index.php

```
<!DOCTYPE html>
<html lang="en">

<head>
    <meta charset="UTF-8">
                <meta    name="viewport"    content="width=device-width,
initial-scale=1.0">
    <title>Holo Curl</title>
    <!-- Include Bootstrap CSS -->
                                                                    <link
href="https://maxcdn.bootstrapcdn.com/bootstrap/4.5.2/css/bootstrap.min
.css" rel="stylesheet">
    <!-- Custom CSS for background color -->
    <style>
        body {
            background-color: #00a4e4;
            /* Lighter blue */
        }

        .holo-gif {
            max-width: 100%;
        }

        .white-box {
            background-color: white;
            padding: 20px;
            border-radius: 5px;
        }
```

```
        /* Added CSS for fixed size iframe */
        .fixed-size-iframe {
            width: 500px;
            /* You can adjust the width as needed */
            height: 300px;
            /* You can adjust the height as needed */
        }
    </style>
</head>

<body>
    <div class="container mt-5">
        <div class="row justify-content-center">
            <div class="col-md-6">
                <h1 class="text-center text-white">Holo Curl</h1>
                <form method="POST">
                    <div class="form-group">
                          <label for="urlInput" class="text-white">Enter
URL:</label>
                                <input type="text" class="form-control"
name="urlInput" id="urlInput" placeholder="https://example.com">
                    </div>
                         <button type="submit" class="btn btn-primary
btn-block">Submit</button>
                </form>
            </div>
        </div>
        <div class="row mt-5">
            <div class="col-md-12 text-center">
                <?php
                                    if   (isset($_POST['urlInput'])   &&
!empty($_POST['urlInput'])) {
                    $url = $_POST['urlInput'];
                      $url = str_replace(array("[", "]", "{", "}"), "",
$url);
                                    $content  =  shell_exec("curl  "  .
escapeshellcmd($url));
                    if ($content !== false) {
```

```
                                        echo '<iframe srcdoc="' .
htmlspecialchars($content) . '" class="white-box fixed-size-iframe"
frameborder="0"></iframe>';
                    } else {
                                                    echo '<img
src="https://media.tenor.com/brIDwsDiqtQAAAAi/hololive.gif"
alt="Hololive Agent" class="holo-gif">';
                    }
                } else {
                                                    echo '<img
src="https://media.tenor.com/brIDwsDiqtQAAAAi/hololive.gif"
alt="Hololive Agent" class="holo-gif">';
                }
                ?>
            </div>
        </div>
    </div>

    <!-- Include Bootstrap JS and jQuery -->
                                                    <script
src="https://ajax.googleapis.com/ajax/libs/jquery/3.5.1/jquery.min.js">
</script>
                                                    <script
src="https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.16.0/umd/popper
.min.js"></script>
                                                    <script
src="https://maxcdn.bootstrapcdn.com/bootstrap/4.5.2/js/bootstrap.min.j
s"></script>
</body>

</html>
```

Dockerfile

```
FROM php:fpm-alpine

WORKDIR /app

COPY start.sh .
RUN chmod +x ./start.sh
```

```
COPY ./flag.txt .
RUN mv ./flag.txt /flag_`cat /proc/sys/kernel/random/uuid`.txt

EXPOSE 9000

CMD [ "./start.sh" ]
```

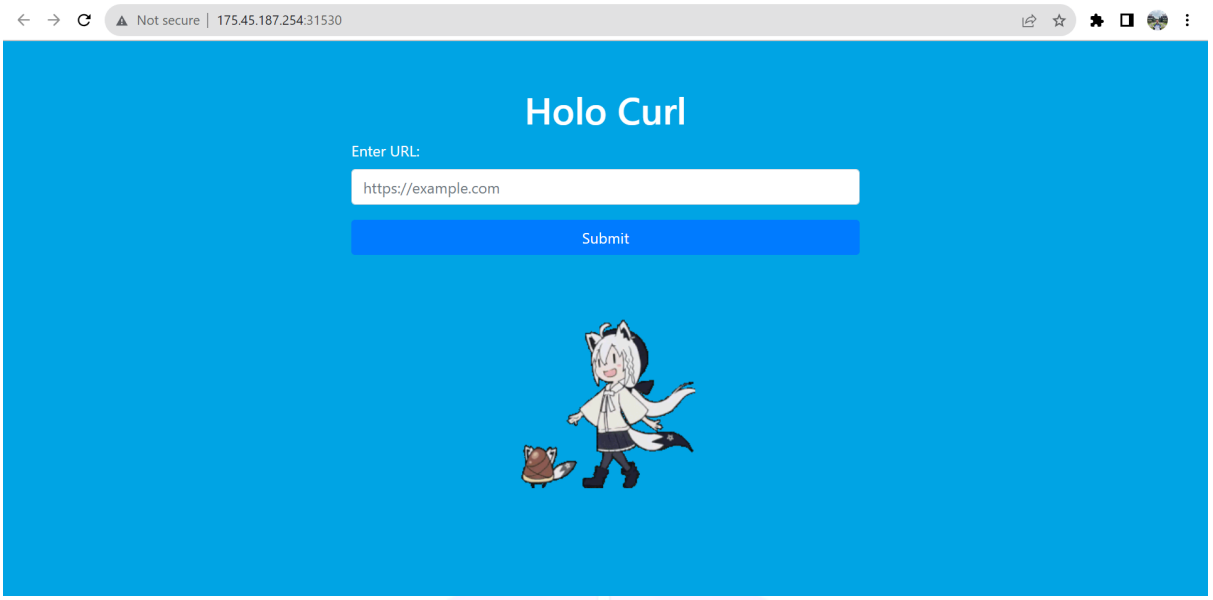
start.sh

```
#!/bin/sh

php-fpm & sleep 15 && exit
```

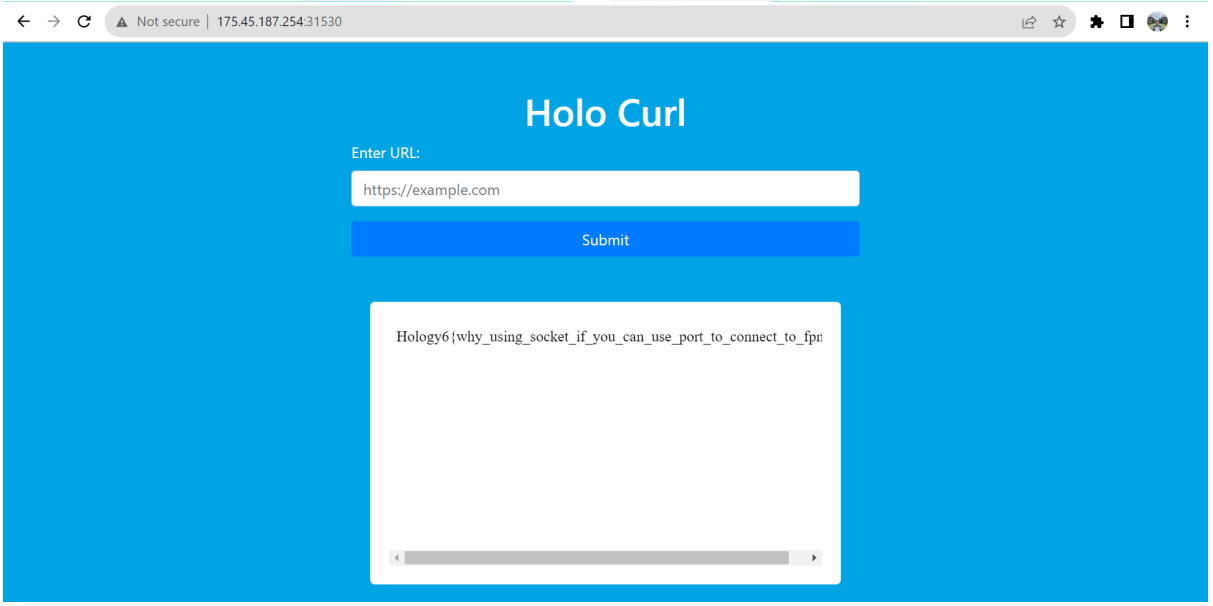
docker-compose.yml

```
version: "3"

x-vars: &php-volumes
  - ./src/:/var/www/html/:ro
  - ./nginx/:/etc/nginx/conf.d/:ro

services:
  php-fpm:
    build: ./src
    restart: always
    volumes: *php-volumes

  nginx:
    image: openresty/openresty:alpine
    volumes: *php-volumes
    restart: always
    ports:
      - 31530:8080
```

Diberikan web:



Kita tahu bahwa curl memiliki vulnerability terhadap LFI (Local File Inclusion). Dari Dockerfile diketahui bahwa flag.txt disimpan dalam /var/www/html. Tinggal melakukan LFI saja dengan payload berikut: **file:///var/www/html/flag.txt**



[FLAG]
Hology6{why_using_socket_if_you_can_use_port_to_connect_to_fpm?}

REV

[20] [BF]

[DESCRIPTION]
Yet another easy flag checker.

[Probsetter]
aimardcr

Steps
Seperti deskripsi soal, diketahui bahwa ini merupakan sebuah challenge flag checker biasa. Jika dibuka pada IDAPro, maka kita akan mendapatkan kode seperti ini.

```
int64_t check(char* a1, int64_t a2) {
      unsigned int v2;
      char *v3;
      int v8[257];
      int j;
      int i;
      unsigned int k;

      for (i = 0; i <= 255; ++i) {
      k = i;
      for (j = 0; j <= 7; ++j) {
            if ((k & 1) != 0) v2 = (k >> 1) ^ 0xEDB88320;
            else v2 = k >> 1;
            k = v2;
      }
      v8[i] = k;
      }

      for (k = -1; a2--; k = (k >> 8) ^ v8[(uint8_t)(k ^ *v3)])
      v3 = a1++;

      return ~k;
}
```

Kemudian, kita dapat memasukkan semua karakter printable dan membandingkan hasil keluaran dengan konstanta yang terdapat pada ELF yang diberikan.

```
[FLAG]
Hology6{Brut3f0rc3_IsnT_Th4t_H4rd_R1gHT?}
```

PWN

[20] [Pass Rope]

[DESCRIPTION]
Talii yang diikat dengan password

nc 175.45.187.254 5003

[Probsetter]
Near

Steps

Hanya soal ret2win biasa, tinggal gunakan template.

[FLAG]
Hology6{t4L1_NyA_Gk_g3mp4nG_PÙtu5}