
SCA

10기 동아리원 모집 발표

부장 송은우 규장 강대성

동아리원 최유민_(이 만들었음), 최유준, 강희찬, 김필립, 박민기

#01

동아리 소개

#01

동아리 소개

Security Cyber Aegis



동아리 소개



Security Cyber Aegis

Security(보안)

Cyber(사이버)

Aegis(방패)

사이버 상의 위협으로부터 방어하기 위해
보안을 공부하는 동아리.

동아리 소개



Security Cyber Aegis

Security(보안)

Cyber(사이버)

Aegis(방패)

사이버 상의 위협으로부터 방어하기 위해
보안을 공부하는 동아리



사실 그냥 대충 만든거예요..? ?

전공 분야

QR code generator
https://dreamhack.io:443/ generate QR code

Burp Suite HTTP history table:

| # | Host | Method | URL | Params | Edited | Status code | Length | MIME type | Extension | Ti |
|---|-------------------------------|--------|---------------|--------|--------|-------------|--------|-----------|-----------|----|
| 1 | http://host3.dreamhack.gam... | GET | /qr_generator | | | 200 | 658 | HTML | | |
| 3 | http://host3.dreamhack.gam... | GET | / | | | 200 | 388 | HTML | ico | |
| 4 | http://host3.dreamhack.gam... | GET | /favicon.ico | | | 200 | 511 | HTML | | |

```

def init_session():
    return
    session['id'] = os.urandom(32).hex()
    print(session)
    os.mkdir('static/users/' + session['id'])

@app.route('/', methods=['GET'])
def index():
    return render_template('index.html')

@app.route('/qr_generator', methods=['GET', 'POST'])
def qr_generator():
    if request.method == 'GET':
        return render_template('qr_generator.html')

    # POST
    url = request.form.get('url')
    if not isinstance(url, str):
        abort(400)
  
```

CPU registers:

| Register | Value |
|----------|------------------|
| EIP | 00401000 <11.0> |
| ECX | 6A 00 |
| EDX | FF15 82204000 |
| ESI | 6A 00 |
| ESP | 68 28104000 |
| EBP | 6A 00 |
| EBX | 6A 25 |
| ESI | 50 |
| EDI | FF15 C6204000 |
| EAX | 6A 00 |
| ECX | FF15 84204000 |
| EDX | 55 |
| ESI | 89E5 |
| ESP | 817D 0C 11010000 |
| EBP | 74 11 |
| EBX | 837D 0C 10 |
| ESI | 0F84 9F000000 |
| EDI | 31C0 |
| EAX | E9 A6000000 |
| ECX | 66:837D 10 04 |
| EDX | 0F84 8D000000 |
| ESI | 66:837D 10 03 |
| ESP | 74 6F |
| EBP | 66:837D 10 02 |
| EBX | 0F85 86000000 |
| ESI | 68 FF000000 |
| EDI | 68 3B224000 |
| EAX | 6A 00 |
| ECX | FF75 08 |
| EDX | FF15 CE204000 |
| ESI | 68 FF000000 |
| ESP | 68 3A234000 |
| EBP | 6A 01 |
| EBX | FF75 08 |
| ESI | FF15 CE204000 |

Registers:

- \$rax: 0x8
- \$rbx: 0x3
- \$rcx: 0x0000000004010b8 → leave
- \$rdx: 0x8
- \$rsi: 0x00007fffffffda8 → 0x000000000a690a ("ni\n")
- \$rbp: 0x00007fffffffda8 → 0x000000000401000 → 0xe58948004010068 ("h")
- \$rsi: 0x00000000040202f → "(snore)\n"
- \$rdi: 0x1
- \$rip: 0x000000000401028 → mov rsp, rbp
- \$r8: 0x0
- \$r9: 0x0
- \$r10: 0x0
- \$r11: 0x246
- \$r12: 0x0
- \$r13: 0x0
- \$r14: 0x0
- \$r15: 0x0

Stack:

```

0x00007fffffffda8+0x0000: 0x000000000a690a ("ni\n") + $rsp
0x00007fffffffdad0+0x0008: 0x0000000000000000
0x00007fffffffdad8+0x0010: 0x0000000004010000 + 0xe58948004010068 ("h") + $rbp
0x00007fffffffdae0+0x0018: 0x0000000000000001
0x00007fffffffdae8+0x0020: 0x00007fffffffdd42 → "/mnt/a/DreamHack-Wargame/pwn/The night guest/prob"
0x00007fffffffdaf0+0x0028: 0x0000000000000000
0x00007fffffffdaf8+0x0030: 0x00007fffffffdd74 → "PWD=/mnt/a/DreamHack-Wargame/pwn/The night guest"
0x00007fffffffdb00+0x0038: 0x00007fffffffda5 → 0x00313d4c564c4853 ("SHLVL=1")
  
```

Web

Pwn

Memory dump:

```

dword ptr ds:[00402120 <11.InitCommonControls>]=<comctl32.InitCommonControls>
.code:00401000 11.exe:$1000 #200 <OptionalHeader.AddressOfEntryPoint>
  
```

Assembly code:

```

00401000 FF15 20214000 call dword ptr ds:[<InitCommonControls>] optionalHeader
00401006 6A 00 push 0x0
00401008 FF15 88204000 call dword ptr ds:[<GetModuleHandleA>]
0040100E 6A 00 push 0x0
00401010 68 28104000 push 11.401028
00401015 6A 00 push 0x0
00401017 6A 25 push 0x25
00401019 50 push eax
0040101A FF15 C6204000 call dword ptr ds:[<DialogBoxParamA>]
00401020 6A 00 push 0x0
00401022 FF15 84204000 call dword ptr ds:[<ExitProcess>]
00401028 55 push ebp
00401029 mov ebp, esp
0040102B cmp dword ptr ss:[ebp+0xC], 0x111
00401032 je 11.401045
00401034 837D 0C 10 cmp dword ptr ss:[ebp+0xC], 0x10
00401038 je 11.4010DD
0040103E 31C0 xor eax, eax
00401040 jmp 11.4010EB
00401045 66:837D 10 04 cmp word ptr ss:[ebp+0x10], 0x4
0040104A je 11.4010DD
00401050 66:837D 10 03 cmp word ptr ss:[ebp+0x10], 0x3
00401055 je 11.4010C6
00401057 cmp word ptr ss:[ebp+0x10], 0x2
00401059 jne 11.4010E8
0040105C push 0xFF
0040105E push 11.40223B
00401060 push 0x0
00401062 push dword ptr ss:[ebp+0x8]
00401064 call dword ptr ds:[<GetDlgItemTextA>]
00401068 push 0xFF
0040106A push 11.40233A
0040106C push 0x1
0040106E push dword ptr ss:[ebp+0x8]
00401070 call dword ptr ds:[<GetDlgItemTextA>]
  
```

Stack dump:

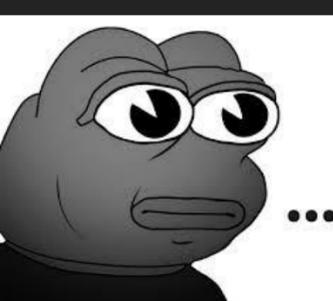
```

ES:0028 0028
ES:0023 0028
ST(0) 0000000000000000 x87r0 비어 있음 0.0000
ST(1) 0000000000000000 x87r1 비어 있음 0.0000
ST(2) 0000000000000000 x87r2 비어 있음 0.0000
ST(3) 0000000000000000 x87r3 비어 있음 0.0000
ST(4) 0000000000000000 x87r4 비어 있음 0.0000
ST(5) 0000000000000000 x87r5 비어 있음 0.0000
ST(6) 0000000000000000 x87r6 비어 있음 0.0000
ST(7) 0000000000000000 x87r7 비어 있음 0.0000
  
```

Kernel memory addresses:

```

1: [esp] 76895D49 kernel32.7689!
2: [esp+4] 003F0000 003F0000
3: [esp+8] 76895D30 <kernel32.Ba
4: [esp+C] 000DFDC 000DFDC
5: [esp+10] 77D2CDEB ntdll.77D2C
  
```



Rev

#01

동아리 소개

동아리 혜택

동아리 소개

동아리 혜택



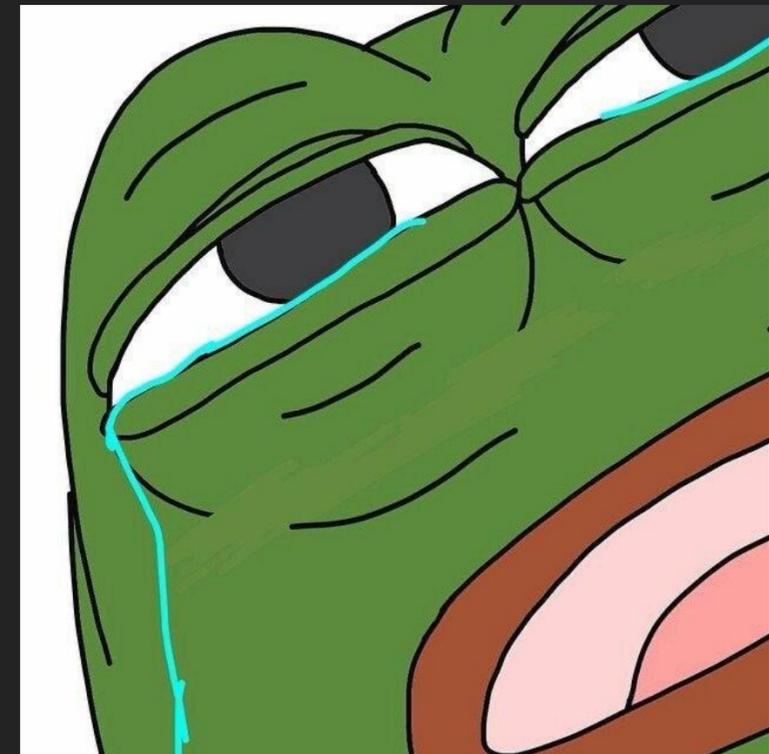
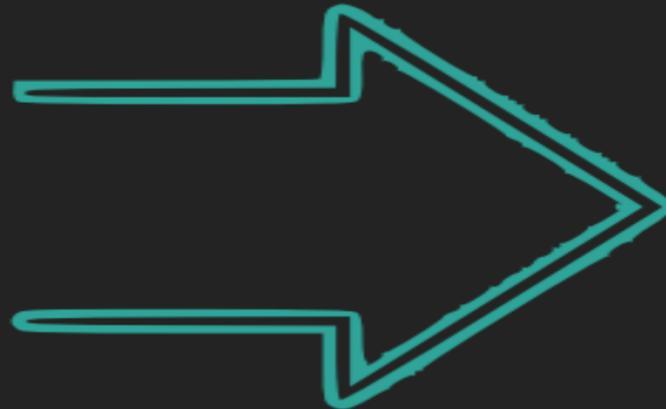
해킹 초짜인 내가
이젠 해킹 마스터..?

동아리 소개

동아리 혜택



해킹 초짜인 내가
이젠 해킹 마스터..?



대부분 어려워서 나가떨어지구..
꾸준한 공부로 키워 나가는겁니다.

동아리 소개

동아리 혜택



와.정말.회식.많이.하고.배고플.일이.없어요.



동아리 실적

대회 수상

- 2023 사이버보안 지방기능경기대회 은메달
- 한국전력공사 사이버 공격 방어 훈련 2022 1st - "한국전력공사 사장 상"
- 순천향대학교 정보보호 페스티벌 2021 2nd - "순천향대학교 총장 상"
- 순천향대학교 정보보호 페스티벌 2022 7th - "(주)이스트시큐리티 대표 상"
- 2021 사이버가디언즈 경진대회 3등 우수상 - "한국정보기술연구원장상"
- 2022 사이버가디언즈 경진대회 3등 우수상 - "한국정보기술연구원장상"
- 2023 사이버가디언즈 경진대회 2등 우수상 - "한국정보기술연구원장상"
- 2024 사이버가디언즈 경진대회 1등 최우수상 - "과학기술정보통신부장관상"
- The Hacking Championship Junior CTF 2020 10th - "(주)이글루시큐리티 대표이사 상"
- The Hacking Championship Junior CTF 2021 4th - "스틸리언 대표 이사 상"
- The Hacking Championship Junior CTF 2022 4th 우수상 - "대구디지털혁신진흥원장상"
- 제 7회 정보보호영재교육원 정보보안 경진대회 단체전 1위 - "부총리 겸 교육부장관상"
- 제 8회 정보보호영재교육원 정보보안 경진대회 개인전 1위 - "서울여자대학교총장상"
- 제 8회 정보보호영재교육원 정보보안 경진대회 단체전 1위 - "부총리 겸 교육부장관상"
- 제 10회 정보보호영재교육원 정보보안 경진대회 단체전 1위 - "부총리 겸 교육부장관상"
- 제 10회 정보보호영재교육원 정보보안 경진대회 단체전 2위 - "한국교육학술정보원장상"
- 제 10회 정보보호영재교육원 정보보안 경진대회 단체전 4위 - "협의회 원장상"
- 2022 KOSPO & 교육부 정보보호 영재교육원 웹 서비스 정보보안 경진대회 최우수상 - "한국남부발전주식회사 사장 상"
- 2024 KOSPO 부산, 울산 정보보안 경진대회 3등
- 2022 KEPCO 한국전력공사 전력분야 실전형 사이버공격 방어훈련 청소년부 1등 및 종합 2등 - "한국전력공사 사장 상"
- 2021 현대오��에버 화이트해커 경진대회 단체전 2위 최우수상 - "현대오��에버 상"
- 2022 현대오��에버 화이트해커 경진대회 단체전 1위 대상 - "교육부장관상"
- 2024 현대오��에버 화이트해커 경진대회 단체전 1위 대상 - "교육부장관상"
- 2024 현대오��에버 화이트해커 경진대회 단체전 3위 우수상 - "현대오��에버 상"
- 중부대학교 JBU CTF 2022 해킹 대회 장려상 - "중부대학교 총장상"
- 중부대학교 JBU CTF 2024 해킹 대회 장려상 - "중부대학교 총장상" x2
- 한국청소년활동진흥원 주최 청소년방과후아카데미 활동수기 공모전 우수상 - "한국청소년활동진흥원장상"
- 2018 육군해킹방어대회 장려상
- 2024 육군 사이버보안 경진대회
- 2024 사이버공격방어대회 7등
- 2025 Lgplus 특별상



교육 프로그램 수료

- 2021 STEALIEN Security Leader 2기 1명 합격
- 서울여자대학교 정보보호영재교육원 6기 합격
- 서울여자대학교 정보보호영재교육원 7기 합격
- 서울여자대학교 정보보호영재교육원 8기 2명 합격
- 서울여자대학교 정보보호영재교육원 9기 4명 합격
- 서울여자대학교 정보보호영재교육원 11기 4명 합격
- 서울여자대학교 정보보호영재교육원 12기 1명 합격
- 한국정보기술연구원 'Best of the Best' 8기 1명 합격
- 한국정보기술연구원 'Best of the Best' 9기 2명 합격
- 한국정보기술연구원 'Best of the Best' 10기 1명 합격
- 한국정보기술연구원 'Best of the Best' 11기 1명 합격
- 한국정보기술연구원 'Best of the Best' 12기 2명 합격
- 한국정보기술연구원 'WhiteHat School' 2기 1명 합격
- 한국정보기술연구원 'WhiteHat School' 3기 2명 합격
- 2020 현대오��에버와 함께하는 특성화 고교생 IT꿈나무 성장지원사업 1명 합격
- 2021 현대오��에버와 함께하는 특성화 고교생 IT꿈나무 성장지원사업 4명 합격
- 2022 현대오��에버와 함께하는 특성화 고교생 IT꿈나무 성장지원사업 2명 합격
- 2024 현대오��에버와 함께하는 특성화 고교생 IT꿈나무 성장지원사업 2명 합격
- 백공팍(P4C) 5기 시스템해킹트랙 1명 합격



동아리 실적

발표

- 2019 Incognito 컨퍼런스 프로젝트 발표 [SMB 취약점 분석]
- 2020 Incognito 컨퍼런스 프로젝트 발표 [IP 카메라 분석]
- 2021 Stony Brook University 화이트 해킹 중앙 동아리 Decompiler 초청 특강
- 제 23회 하계 HackingCamp 발표 - "webhacking.kr 웹해킹의 접근법"
- TeamH4C 학생용 해킹노트 온라인 컨퍼런스 발표자 - "고등학교를 다니면서 BOB 생활을 하는 방법"
- TeamH4C 학생용 해킹노트 온라인 컨퍼런스 발표자 - "메이플에 진심일뿐한 웹쟁이가 알려주는 웹해킹 입문 스토리"
- 2022 TeamH4C 해킹하는 부엉이 발표 - "웹_퍼저_찍먹한_썸.ssl"
- 2022 Codegate 컨퍼런스 - "윈도우 로지컬 버그로 인한 권한 상승 취약점"
- 2022 Stony Brook University 화이트 해킹 중앙 동아리 Decompiler 초청 특강
- 2022 Theori OpenTRS - "Windows Third-Party Privilege Escalation Without Memory Corruption"
- 2023 제 26회 POC 해킹캠프 - "BOB 프로젝트 후기"

취약점 제보

- KVE-2021-1678
- KVE-2022-0743
- LVE-HPC-22001
- LVE-HPC-22002
- LVE-HPC-22003
- CVE-2022-24924(SVE-2021-24089)
- CVE-2022-39846(SVE-2022-1841)
- CVE-2022-39909(SVE-2022-2040)
- CVE-2022-45422(LVE-HOT-220005)
- CVE-2022-44898
- CVE-2022-47449
- CVE-2022-47158
- CVE-2022-47173
- CVE-2022-47140
- CVE-2022-47145
- CVE-2022-4686
- CVE-2022-46858
- CVE-2022-46843
- CVE-2022-47441
- CVE-2022-47435
- CVE-2022-47437
- CVE-2022-47436



#03

파트너십(Hspace)

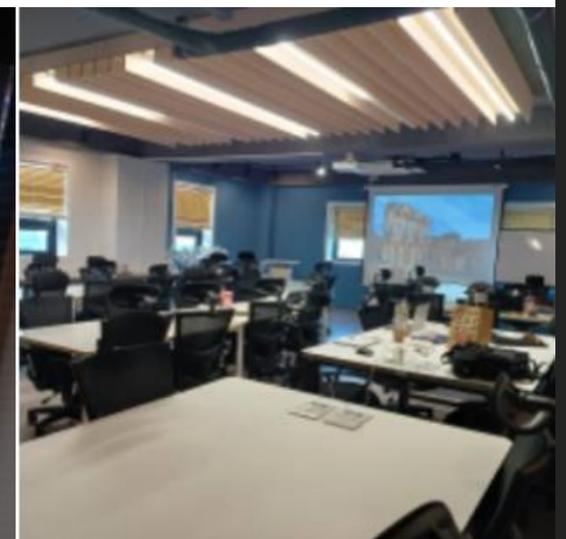
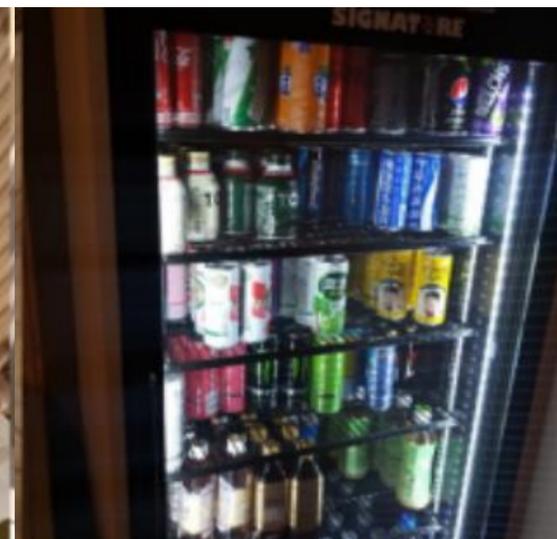
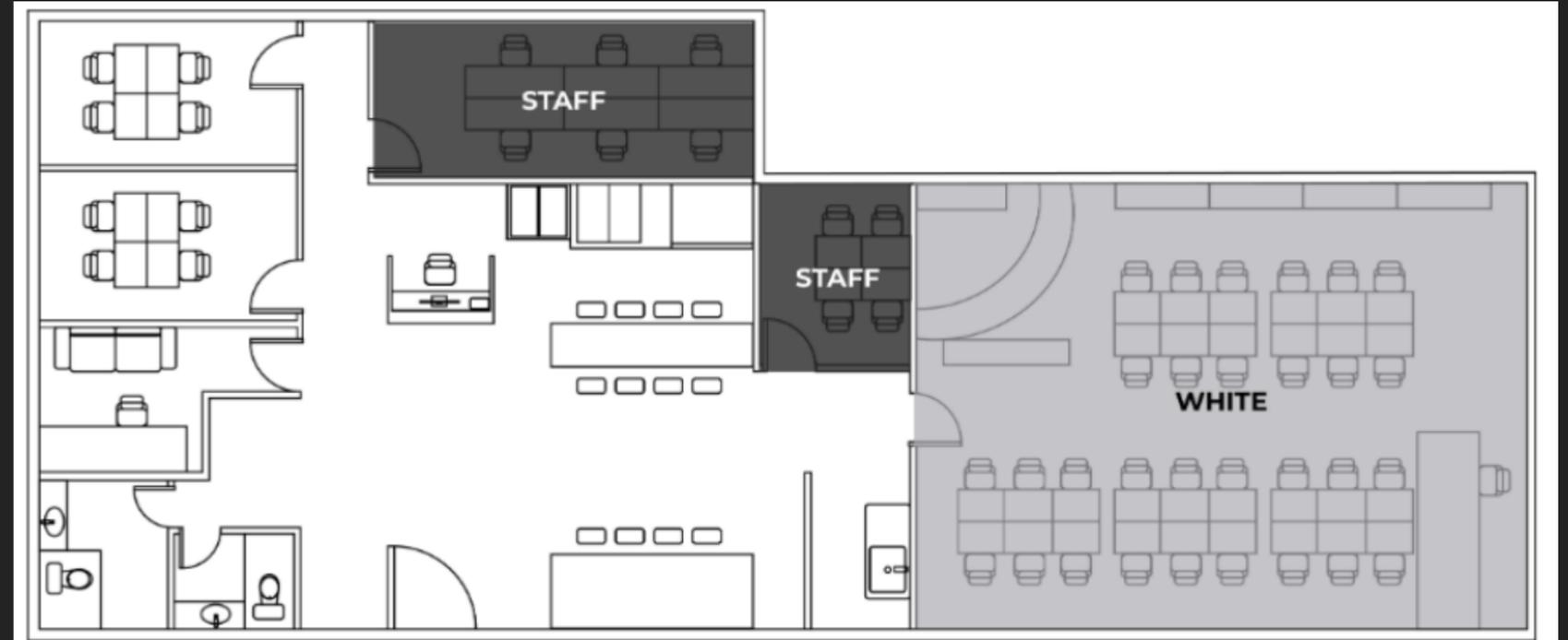
파트너십(Hspace)



사랑해요 hspace



파트너십(Hspace)

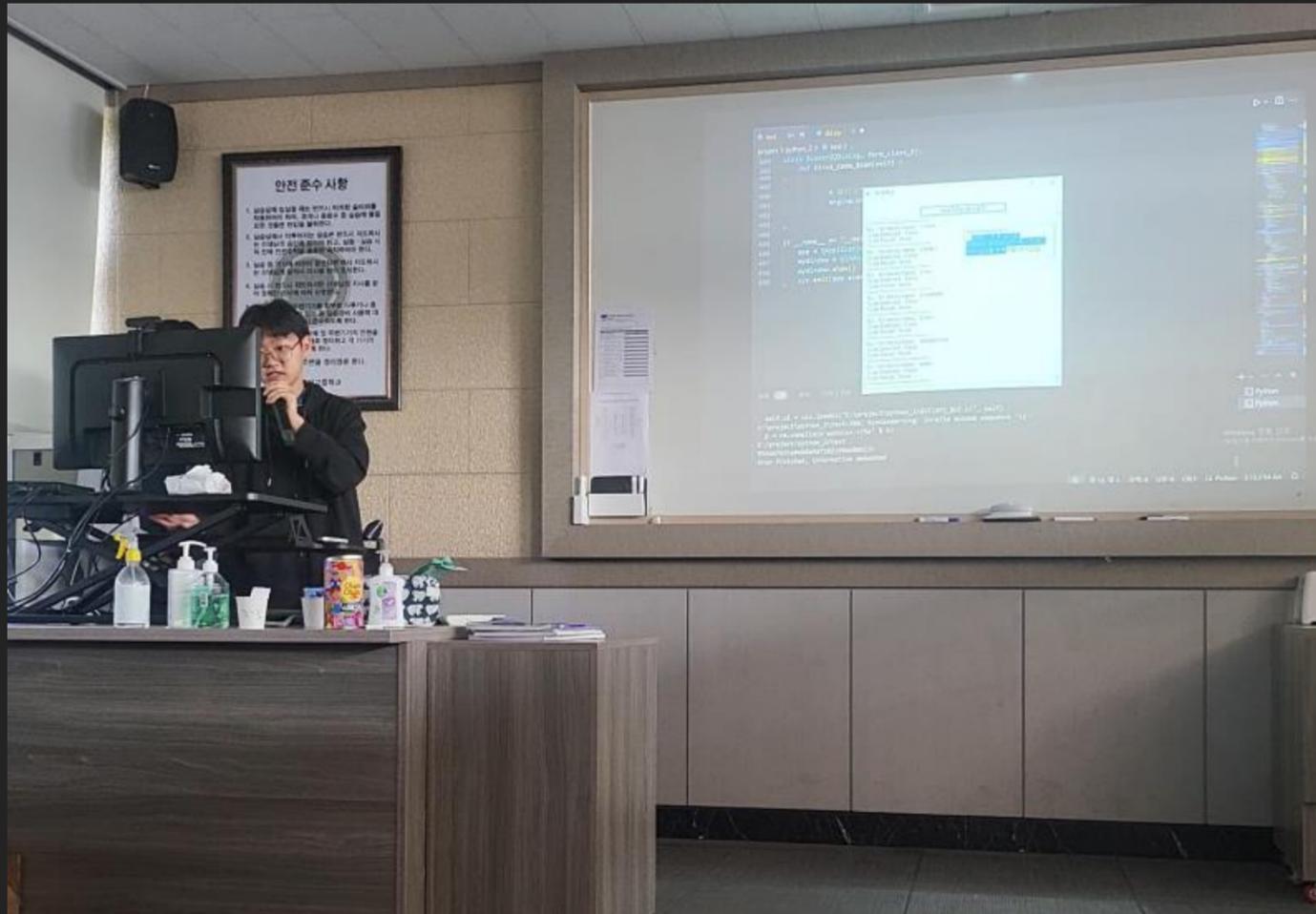


사랑해요 hspace

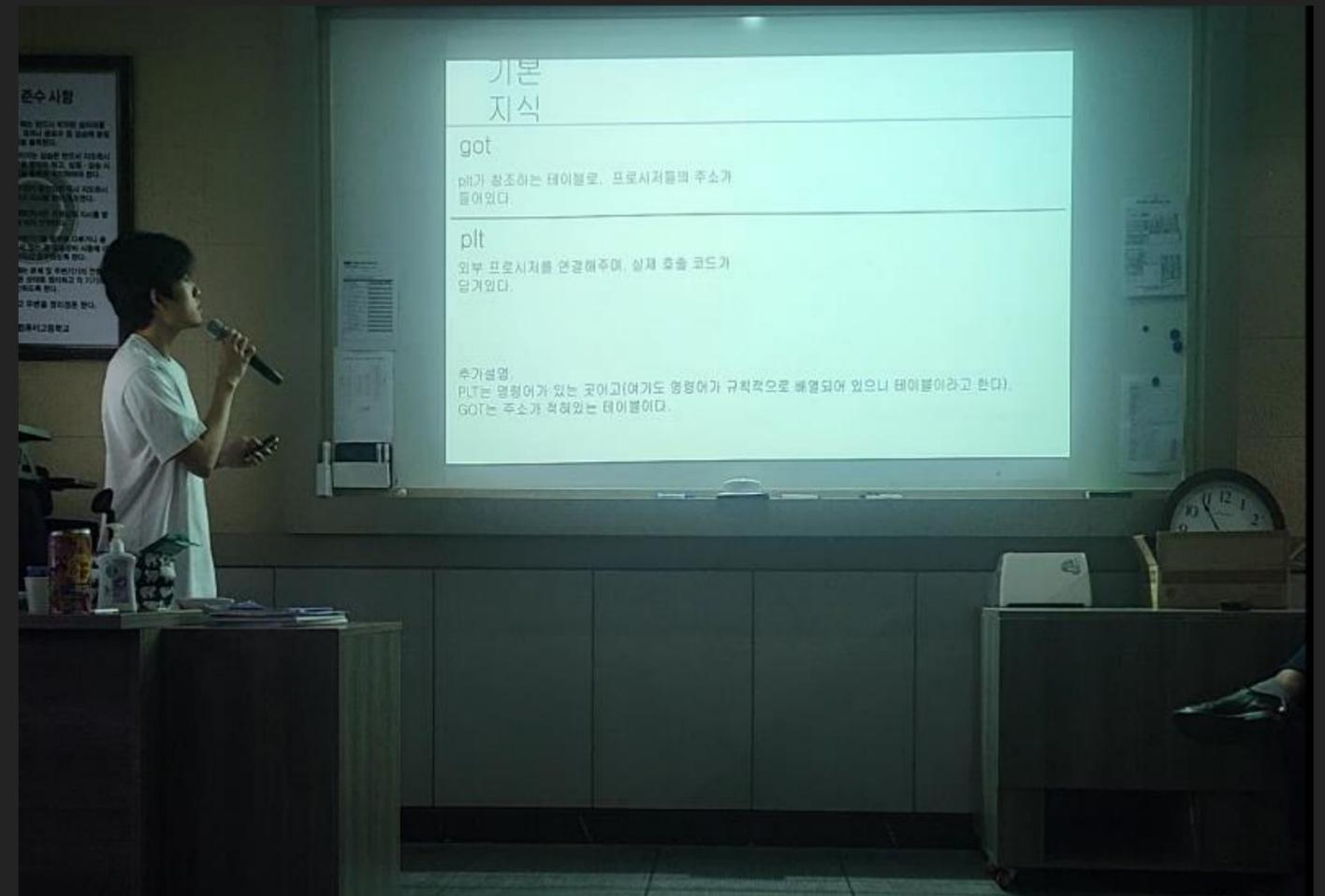


세미나

내부 세미나



귀욤



부장님 나이스샷



세미나

외부 세미나



?



그저 god..



SCA 체험 일정

체험 일정

동아리 체험 신청 - 3월 10일~12일
동아리 체험 - 3월 12일, 17일, 19일
동아리 면접 - 3월 24일

체험 세부내용

3월 12일 - Web Hacking 체험
3월 17일 - Reversing 체험
3월 19일 - Pwnable 체험

동아리 시간

매 주 월요일, 수요일
방과후 9시 30분까지

문의

Instagram : @sca_cr4ck
부장 : 010-8621-1575
선생님 : 양지환 선생님



신청 QR

동아리 가입 신청



동아리 체험 신청

