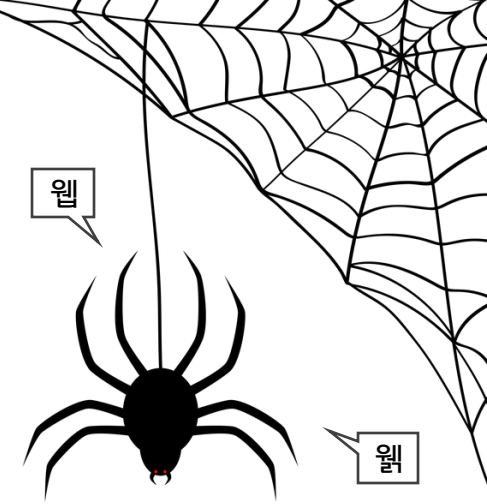
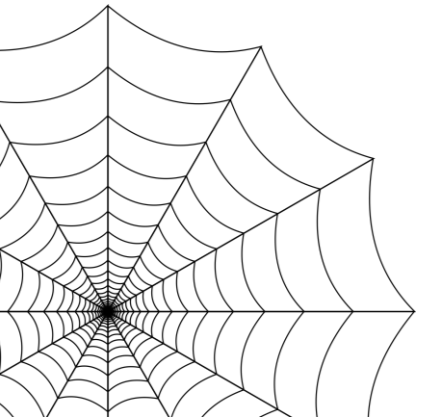
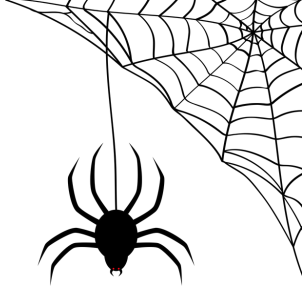


WEB Hacking

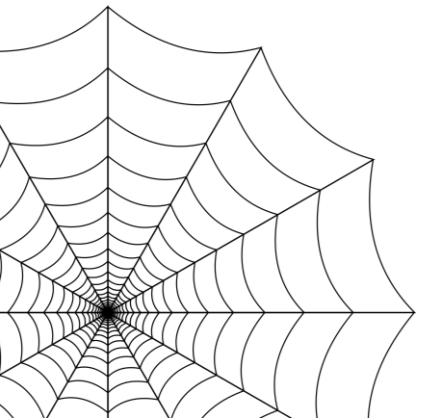
웹해킹 교육 4회차

18학번 서연주





<목차>



</목차>

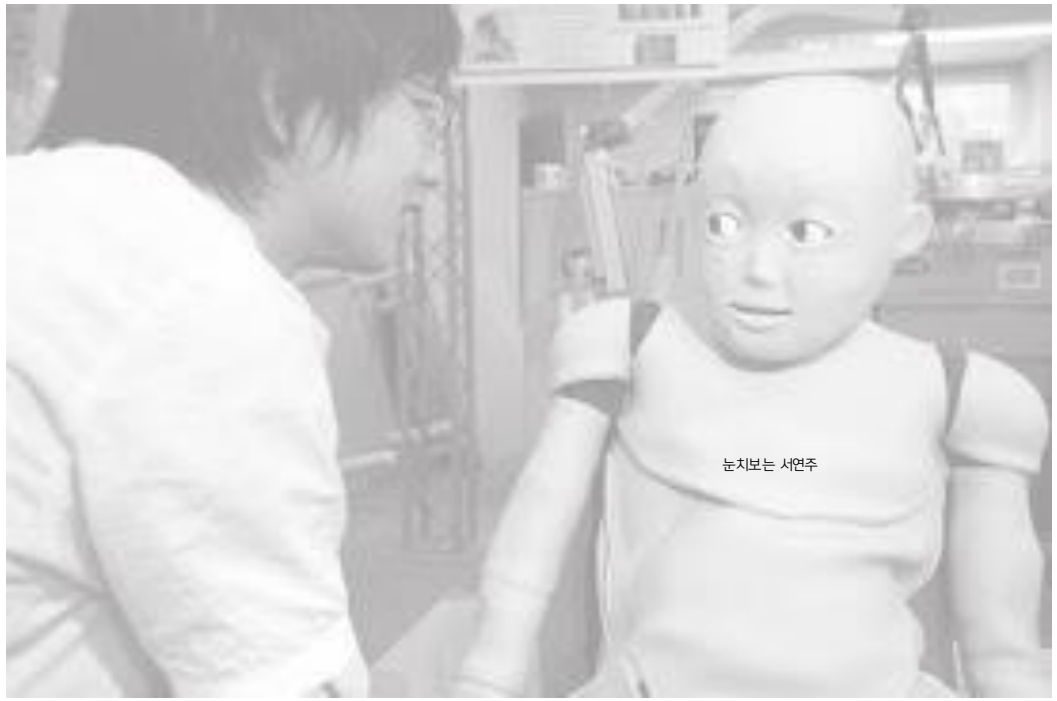
00. 시작하기 전에

00. 시작하기 전에

< 3주차 과제 >

- webhacking.kr 한 문제 풀기
- (2주차 과제)

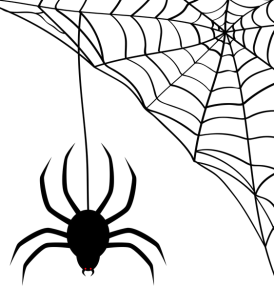
어렵지 않았을 거라 생각합니다!!
프론트 엔드만 알아도 풀 수 있는 문제도 있고,
구글링을 통해 다양한 write-up을 찾을 수 있기때문!!



00. 시작하기 전에

webhacking.kr 난이도 순 / 문제 유형 (old)

문제 번호	요약	문제 번호	요약	문제 번호	요약
가입 문제	webhacking.kr 회원가입을 위한 문제	32	투표 페이지 브루트포스	29	파일업로드 SQLi
15	자바스크립트 접근 제한 우회	34	자바스크립트 난독화 분석	22	SALT 이해
17	변수 값 확인	41	파일업로드 취약점 분석	40	Blind SQLi 필터 우회
14	변수 값 확인 및 기본 함수 학습	28	HTACCESS 관련	55	procedure 응용
16	ascii code 분석	30	HTACCESS 응용	50	mb_convert_encoding 응용
12	자바스크립트 난독화 분석	37	PHP 코드 분석 및 자동화	57	time based blind SQLi
10	HTML 객체 변조	48	COMMAND INJECTION	60	레이스 컨디션
20	스팸방지 필터링 우회	44	COMMAND INJECTION 2	9	Blind SQLi 필터 우회
54	함수 흐름 변조	18	SQLi 기본	13	Blind SQLi 필터 우회
1	쿠키 변조 및 필터링 우회	7	union select SQLi		
4	MD5 Hash의 이해와 base64 디코딩	실습 문제	모의해킹시 사용되는 SQLi 패턴		1일차
6	PHP 코드 분석 및 쿠키 변조	3	논리연산자를 통한 SQLi		2일차
19	쿠키 변조	8	getenv 이해를 통한 SQLi		3일차
24	register_globals 옵션 관련	39	SQLi 필터링 우회		
26	URL 인코딩을 활용한 필터 우회	46	char함수를 통해 필터 우회		
42	파라미터 변조 및 ZIP 크랙	49	hex함수를 통해 필터 우회		
38	Log injection	5	mysql truncation		
47	Mail Header injection	51	md5 raw hash SQLi		
52	HTTP Header injection	61	as 구문 이해		
25	Local file inclusion	27	주석을 통해 필터 우회		
23	null byte를 통해 XSS 필터 우회	56	LIKE문 취약점 이용		
실습 문제	XSS를 사용하여 관리자 계정 탈취	53	Procedure 관련		
36	VI 스왑파일 관련	45	문자열 인코딩 관련 취약점		
11	정규식	21	Blind SQLi		
31	쉘 스크립트와 NC 사용 방법	2	Blind SQLi 응용		
43	Content-Type 변조를 통한 파일 업로드	35	insert문 SQLi		
58	플래시 디컴파일	59	insert문 SQLi 응용		



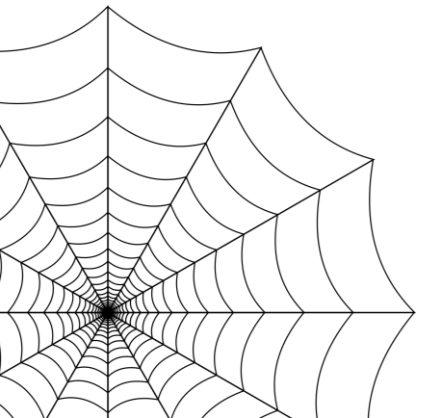
〈01/〉

〈Review〉

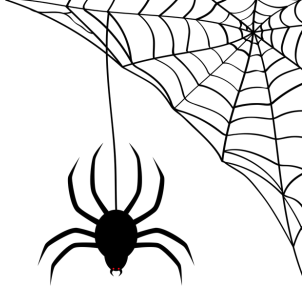
〈 SQL Injection /〉

〈 Practice /〉

〈/Review〉



01. Review - SQL Injection



이용자의 입력값 → SQL구문의 일부로 사용 → 비정상적인 DB 명령을 실행

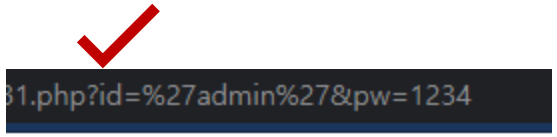
- 인증 우회 (로그인 Form 공격)
- DB 데이터 조작

SQL Injection

- SQL Injection
- Blind SQL Injection : 쿼리 결과의 참/거짓으로부터 DB값을 유출해 내는 기법

01. Review - SQL Injection

①



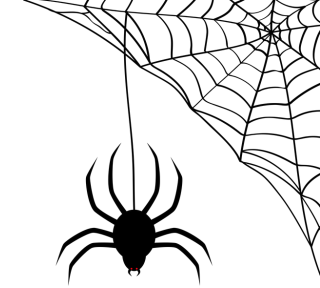
우리가 지금까지 풀었던 문제는 get방식 (url표시)

ID	admin
PW	1234

form을 통해 값을 넣으면,

~~~~~?(input name)= '(넣은값)'
~~~~~

01. Review - SQL Injection



② where 구문 우회

[외부 입력값] - 주석처리
ID : admin '--
PW : 123

[실행 쿼리문]
Select * From Users Where ID = 'admin'-- and Password = '1234';

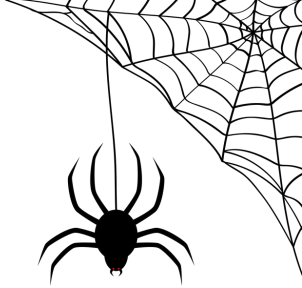
[외부 입력값] - 무조건 참
ID : admin
PW : 123' or '1=1

[실행 쿼리문]
Select * From Users Where ID = 'admin' and PW='123' or '1=1';

[외부 입력값] - 데이터베이스 조작
ID : admin'; delete table users --
PW : 123

[실행 쿼리문]
Select * From Users Where ID = 'admin'; delete table users -- and PW = '123'

01. Review - SQL Injection



②

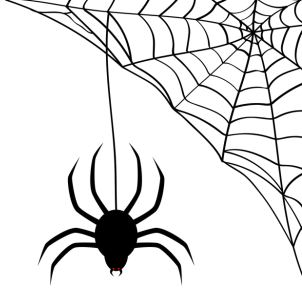
ID	admin
PW	1234

select * from table1 where id='admin' and pw='1234';

ID	admin
PW	' or '1=1

select * from table1 where id='admin' and pw='' or '1=1';

01. Review - SQL Injection



select * from table1 where id='admin' and pw='' or '1=1' ;

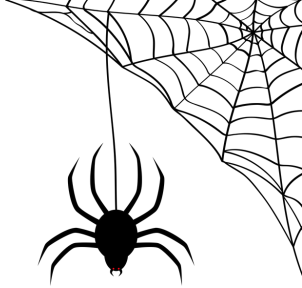
1) false

2) true

3) true

ID	PW
id1	pw1
id2	pw2

01. Review - SQL Injection



```
$query = "select id from prob_gremlin where id='{$_GET[id]}' and pw='{$_GET[pw]}'";
echo "<hr>query : <strong>{$query}</strong><hr><br>";
$result = @mysql_fetch_array(mysql_query($query));
if($result['id']) solve("gremlin");
```

$query = select id from table1 where id='admin' and pw='' or '1=1' ; true

↓

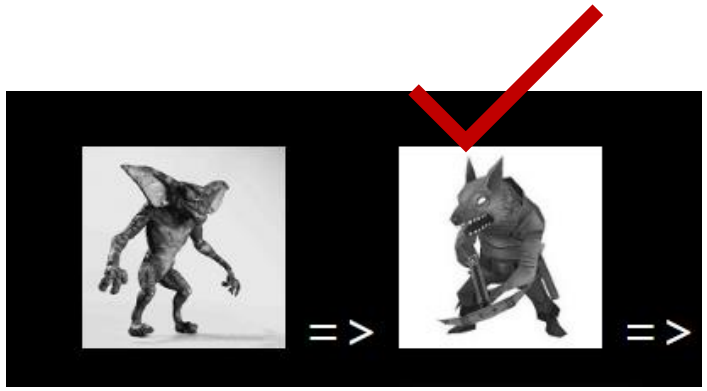
$result가 무조건 존재

↓

가져온 줄에는 id와 pw가 무조건 존재

01. Review - Practice(실습)

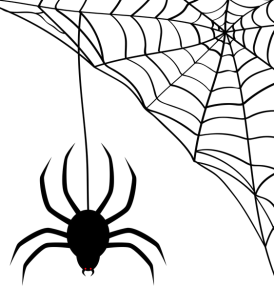
https://los.eagle-jump.org
2번



query : **select id from prob_cobolt where id='' and pw=md5('')**

```php
<?php
  include "./config.php";
  login_chk();
  dbconnect();
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[id])) exit("No Hack ~_~");
  if(preg_match('/prob|_|₩.|₩(₩)/i', $_GET[pw])) exit("No Hack ~_~");
  $query = "select id from prob_cobolt where id='{$_GET[id]}' and pw=md5('{$_GET[pw]}')";
  echo "<hr>query : <strong>{$query}</strong><hr><br>";
  $result = @mysql_fetch_array(mysql_query($query));
  if($result['id'] == 'admin') solve("cobolt");
  elseif($result['id']) echo "<h2>Hello {$result['id']}<br>You are not admin :(</h2>";
  highlight_file(__FILE__);
?>
```

1) 저번과 똑같이 url에 값 전달
2) id=admin
3) 그 뒷 부분을 모두 주석처리하자 (주석처리 후 띄어쓰기 해야 함)



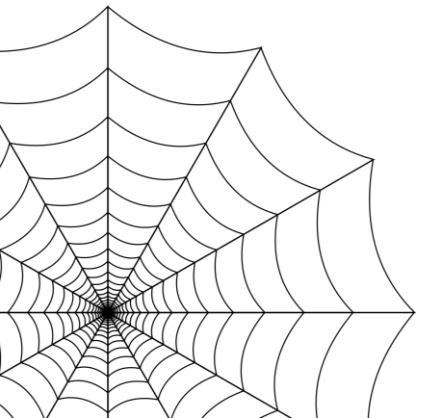
〈01/〉

〈wireshark〉

〈 WireShark? /〉

〈 Practice /〉

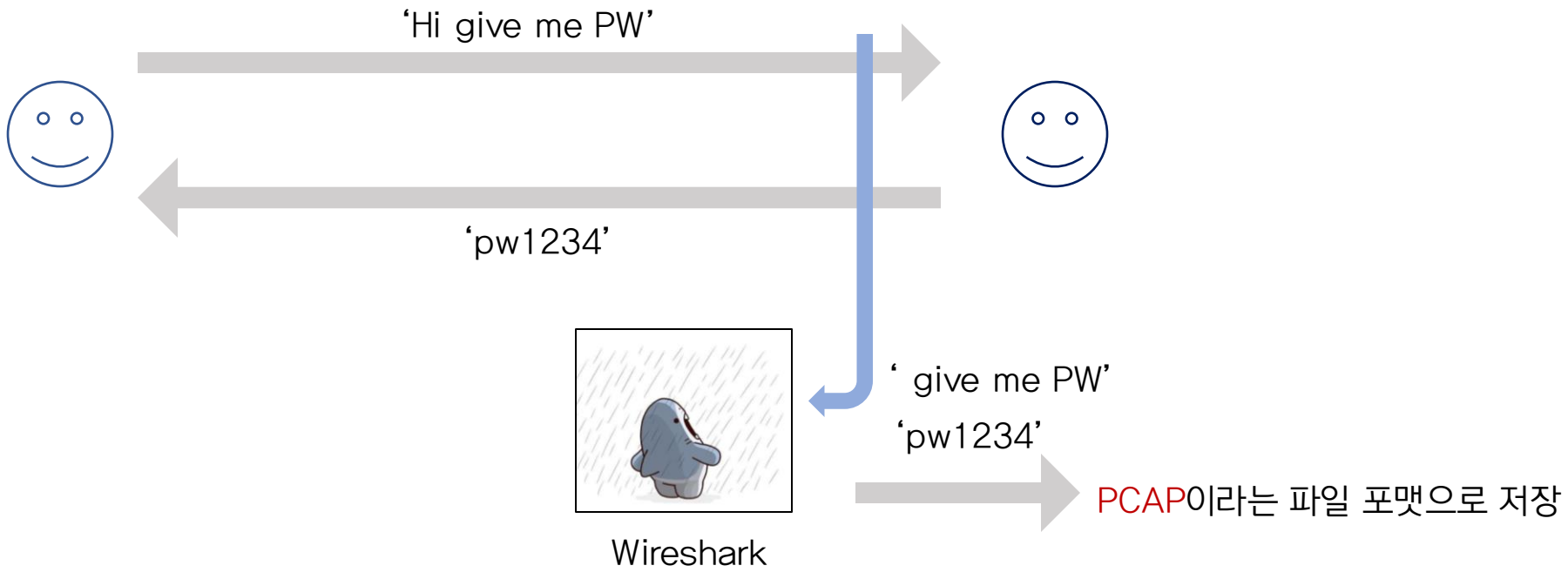
〈/ wireshark 〉



01. WireShark

네트워크 패킷을 캡쳐하고 분석하는 오픈소스 도구

패킷 = 컴퓨터 네트워크가 전달하는 데이터의 형식화된 블록
= 제어 정보와 사용자 데이터(페이로드)



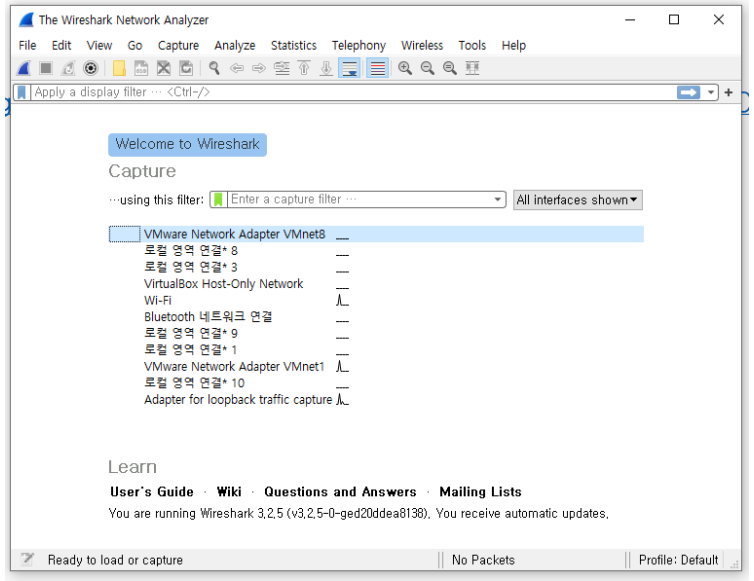
01. WireShark(설치)

https://hongpossible.tistory.com/entry/Wireshark%EB%9E%80-%EC%84%A4%EC%B9%98%EB%B2%95

설치해봅시다!

(설치에 시간이 좀 걸림...ㅎ)

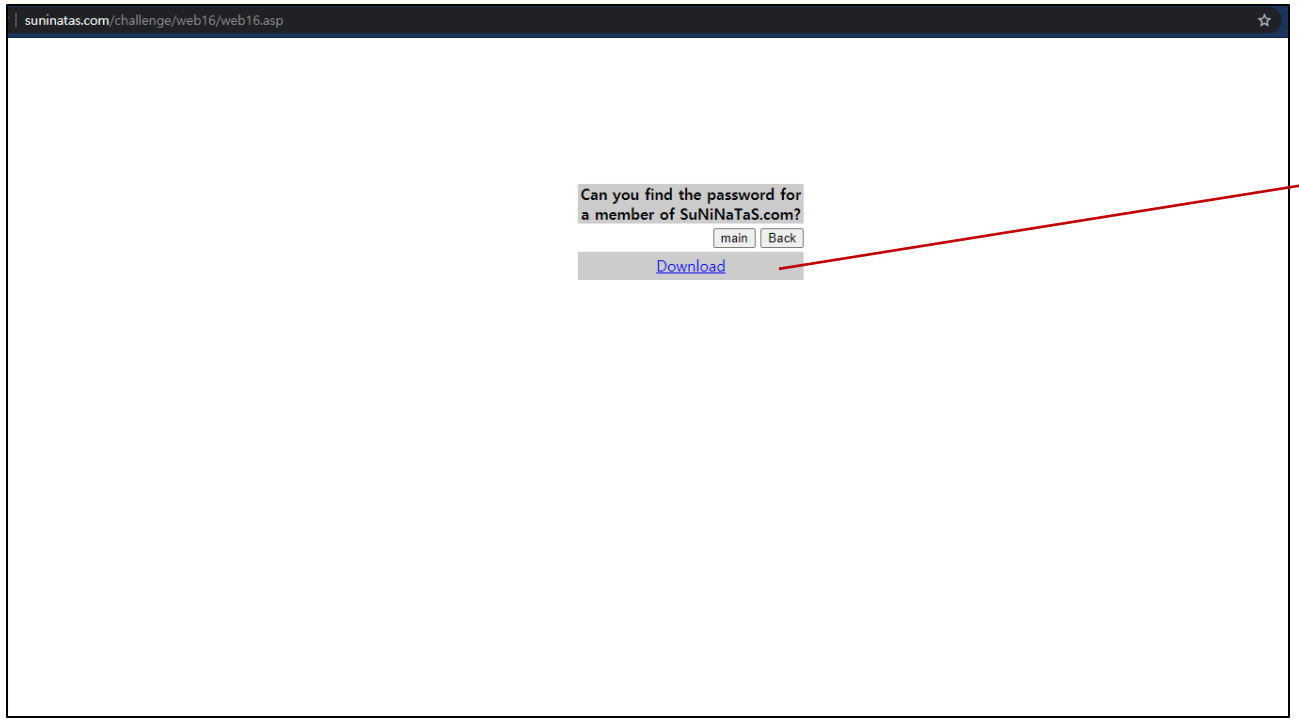
단, Reboot Later을 클릭!!



01. WireShark(실습)

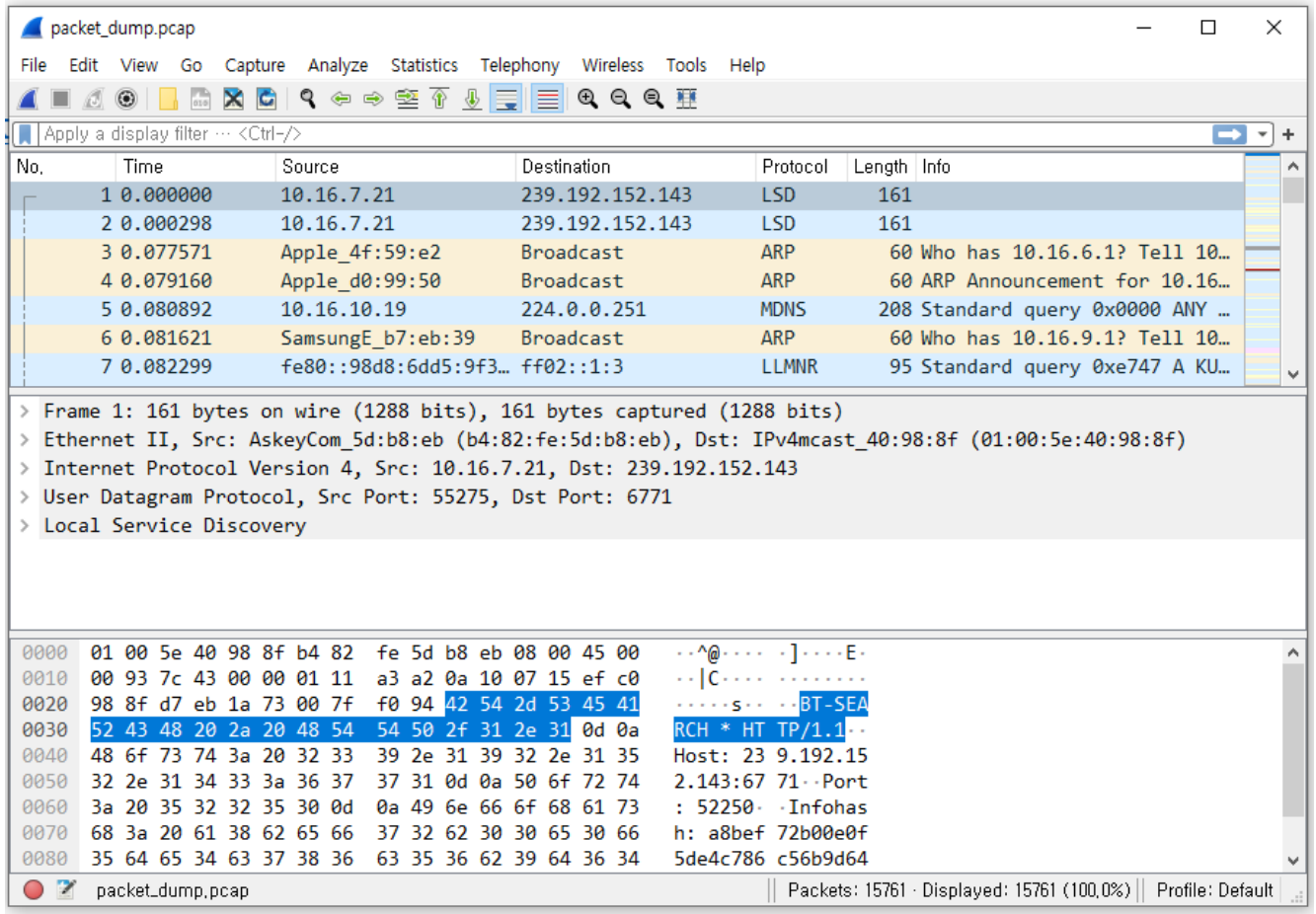
http://suninatas.com/challenge/web16/web16.asp

문제를 풀어보자!



packet_dump.pcap

01. WireShark(실습)



Wireshark - File - Open

Pcap파일 열기

패킷 리스트 / 패킷 디테일 / 가공되지 않은 패킷

[패킷 리스트]

NO : 수집된 순

Time : 수집된 시간

Source : 출발지 주소

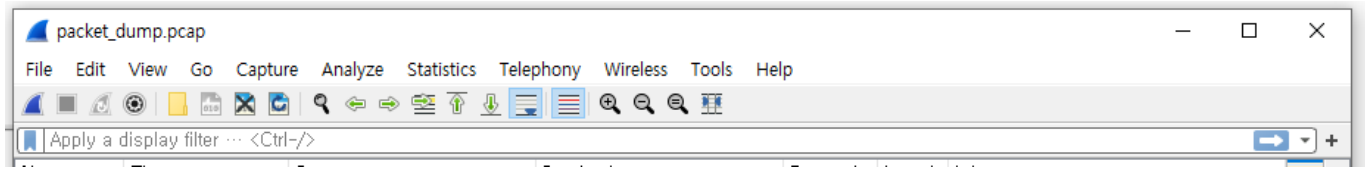
Destination : 도착지 주소

Protocol : 프로토콜 type

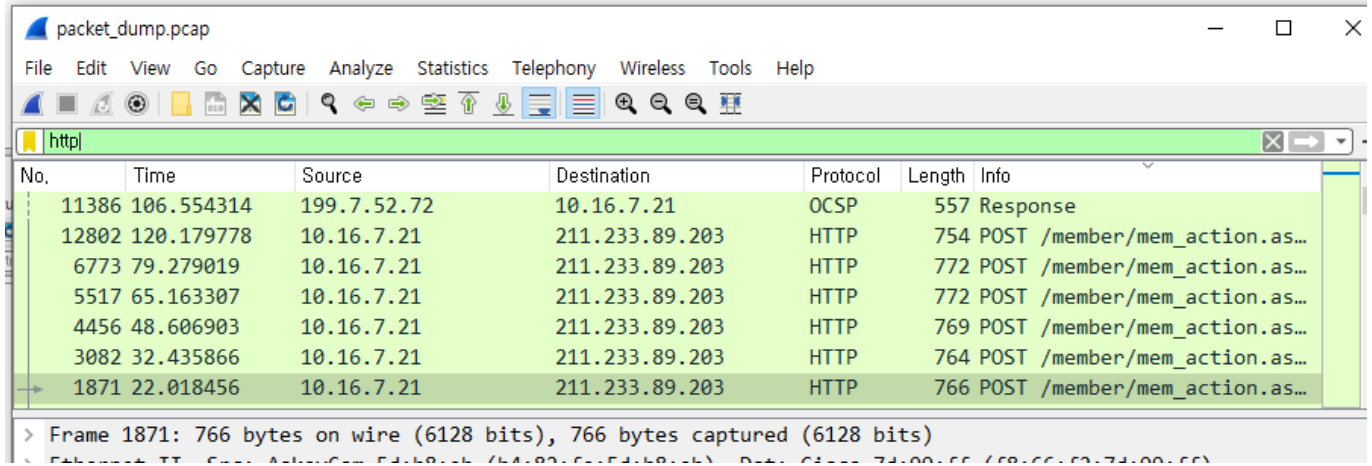
Length : 패킷 길이

Info : 패킷 정보

01. WireShark(실습)

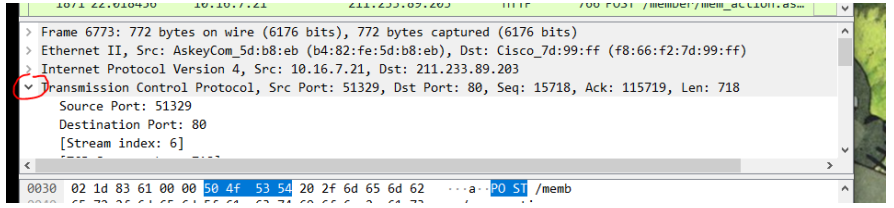


현재 내가 보고싶은 패킷뿐만 아니라
다른 패킷들도 함께 잡힘
→ 필터링

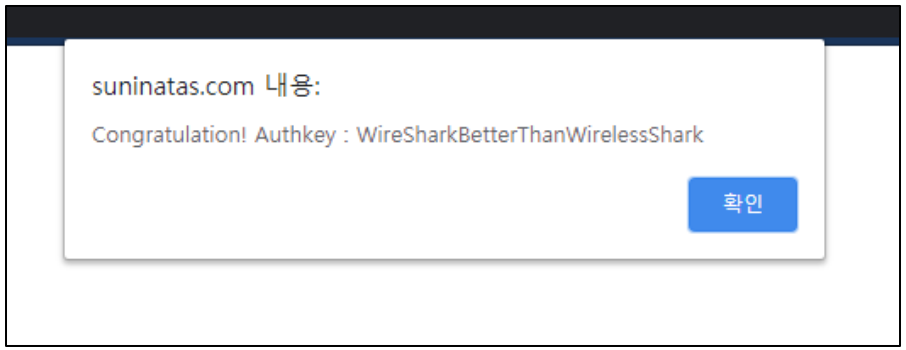


웹 상의 데이터 전달 → http 프로토콜 이용

힌트
- 로그인 form의 전송방식?
- 패킷 디테일



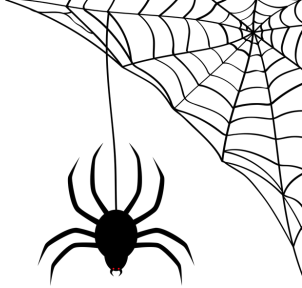
01. WireShark(설치)



그대로 Authkey를 복사하여

Auth탭에 들어가 입력하면 됨

(현재는 로그인 X, 점수를 얻을 수는 없음)



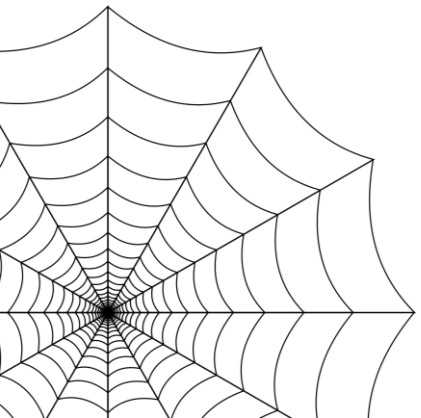
<02/>

<another>

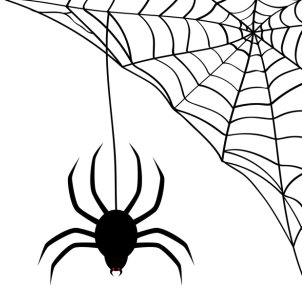
<Bruite Surp />

<Practice />

</ another >



02. Burp Suite(설치)



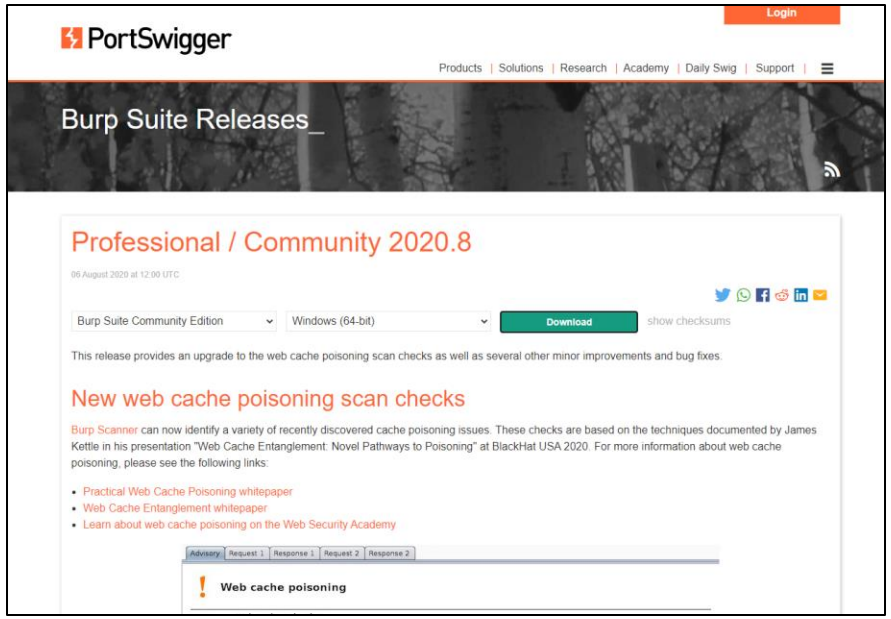
:웹 프록시 서버를 사용하여 클라이언트, 서버의 응답 및 요청 패킷을 확인하고 조작이 가능한 툴

1. local PC 웹 브라우저에서 naver.com HTTP request
2. proxy server(Burp Suite)
3. 네이버 사이트 접속
4. 네이버 사이트 HTTP response
5. Proxy server(Burp Suite)
6. local PC 웹 브라우저

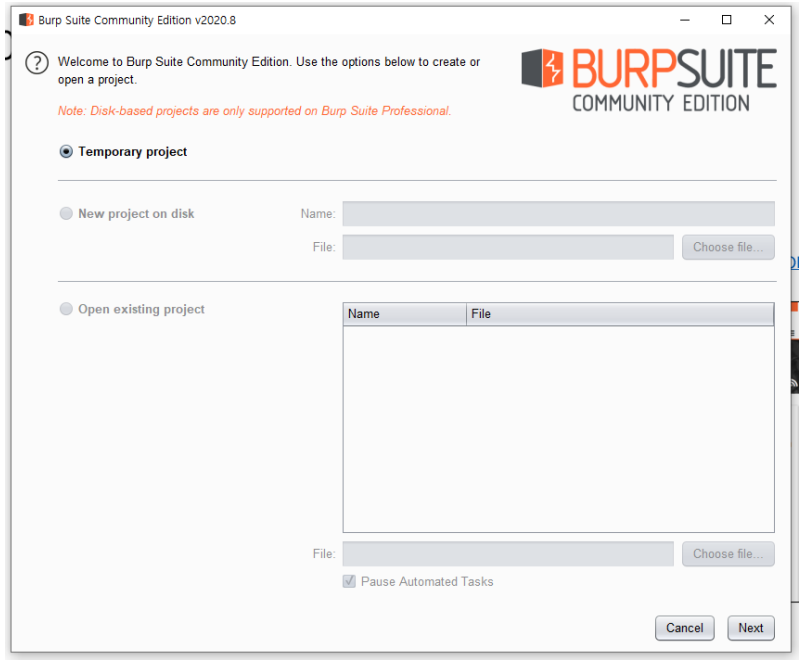
HTTP 요청과 응답 시 항상 proxy server를 거쳐 데이터가 이동하게 되는데
Burp Suite에서 웹 사이트의 우회 공격을 할 수 있게 조작을 할 수 있음

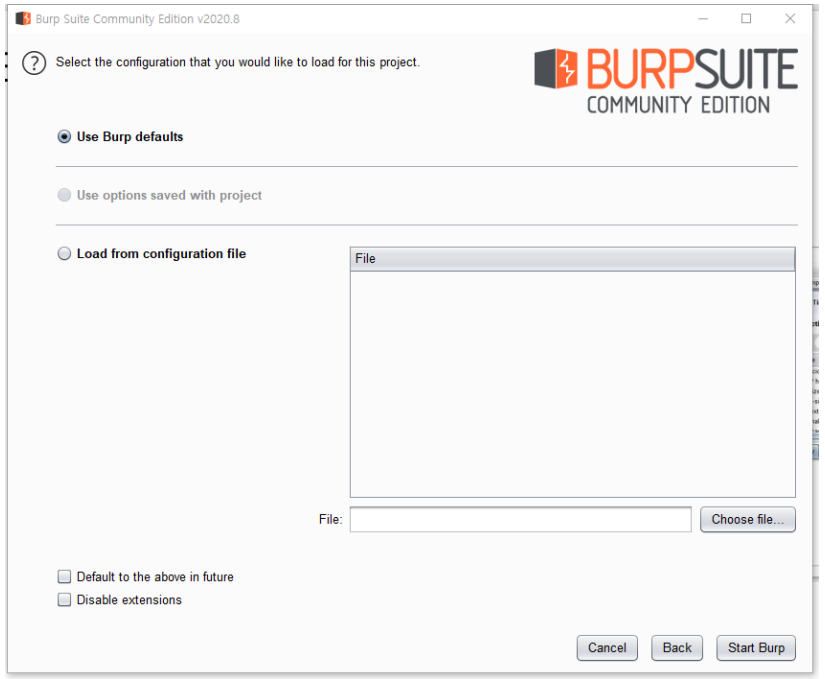
02. Burp Suite(설치)

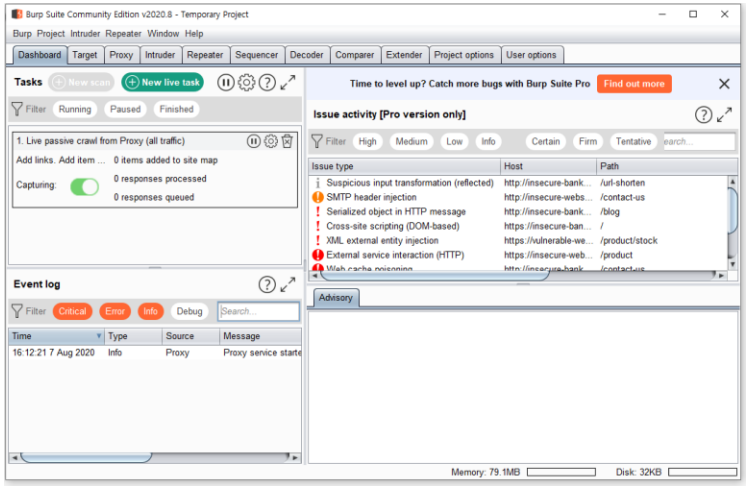
설치→https://portswigger.net/burp/releases/professional-community-2020-8



02. Burp Suite(설치)

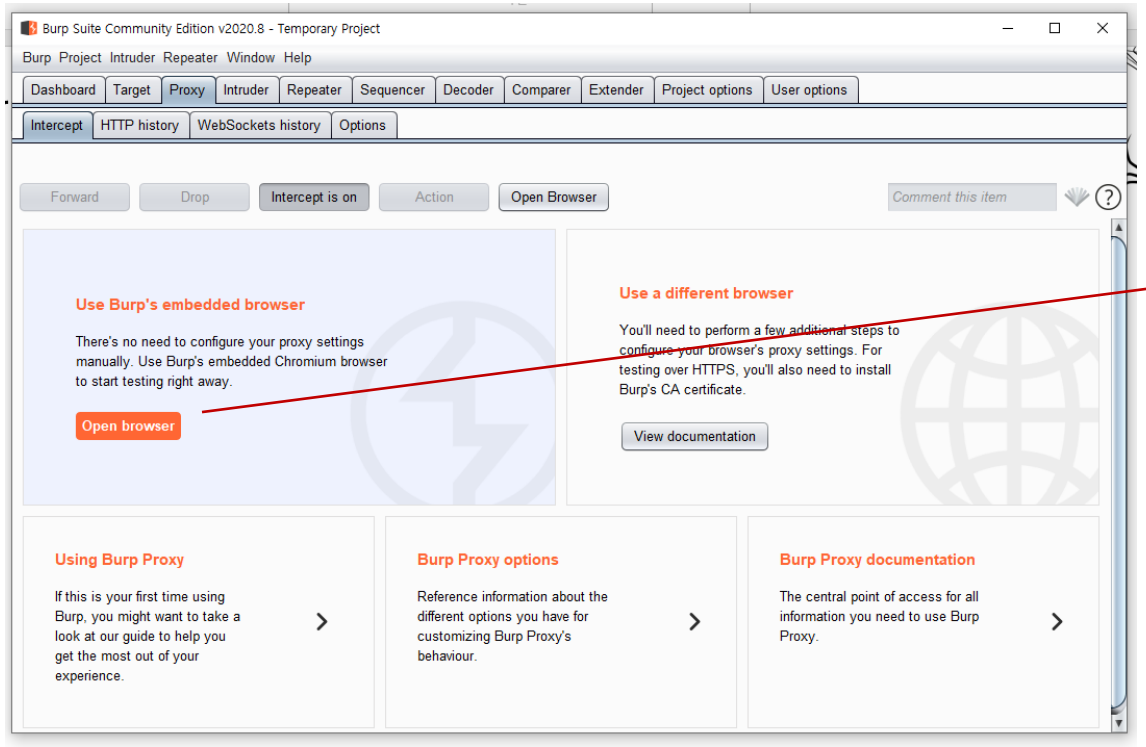


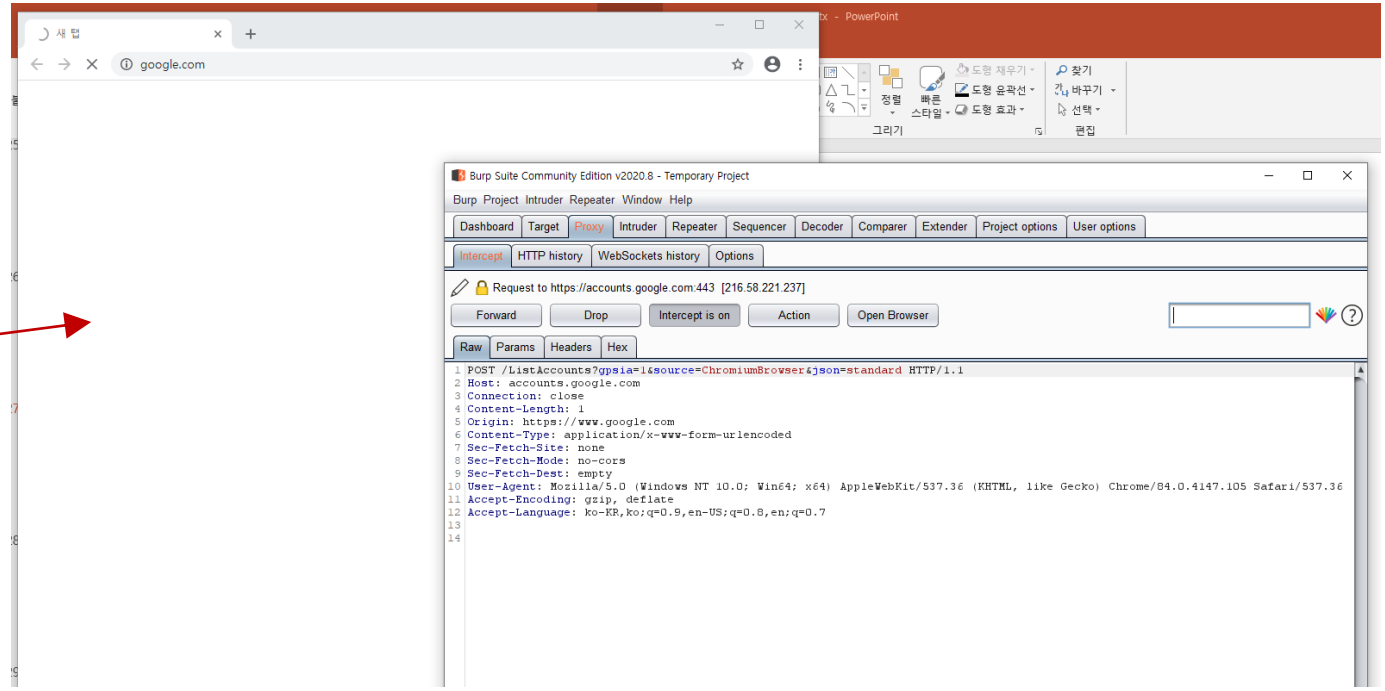




02. Burp Suite(설치)

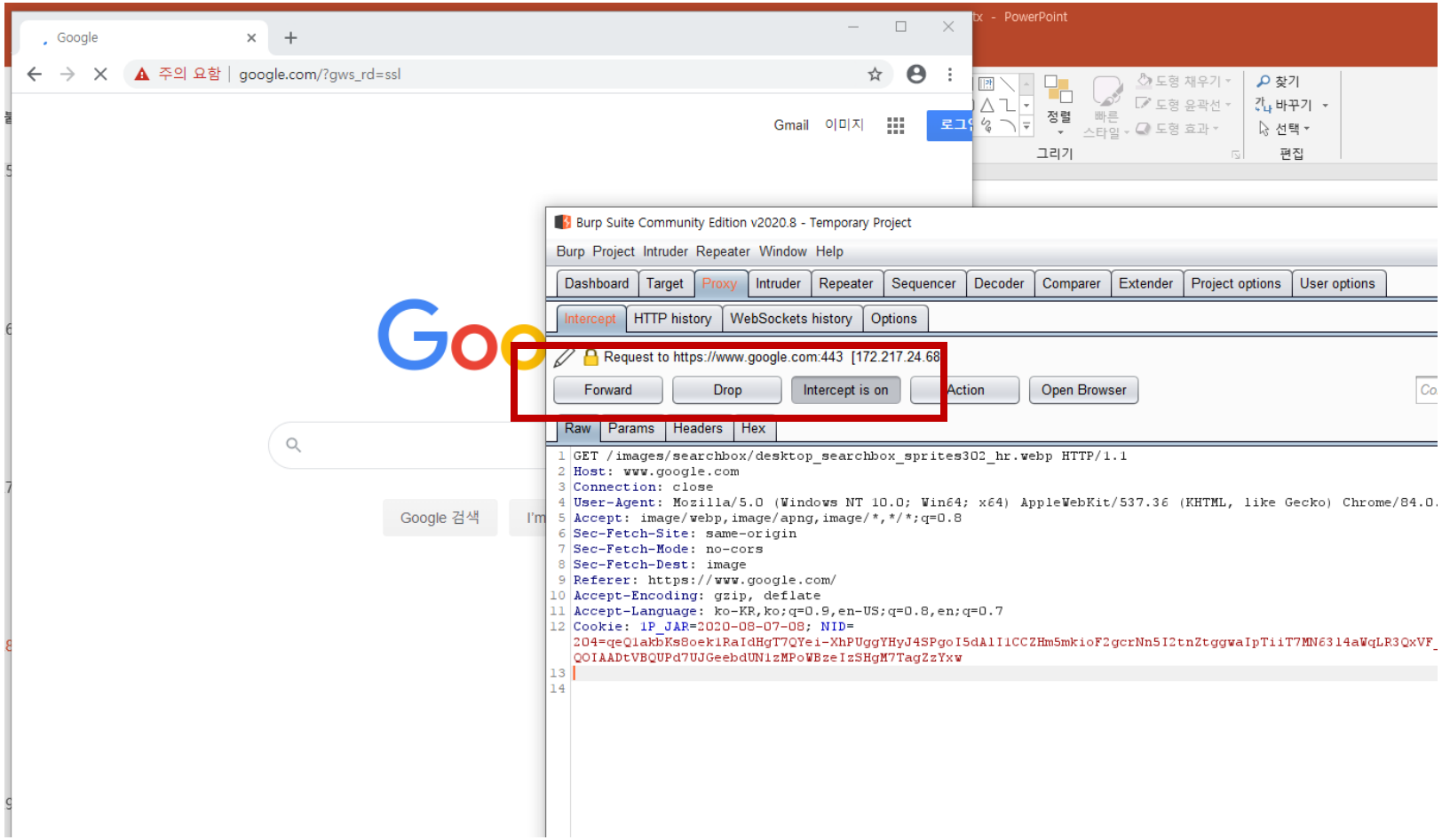
Proxy : web browser와 web server 중간에 위치하여 패킷을 확인하는 메뉴
이 메뉴에서 패킷을 가로채서 요청/응답을 확인하거나 변조/삭제 가능





url에 google.com을 입력
실행이 안되는게 맞음!!

02. Burp Suite(실습)



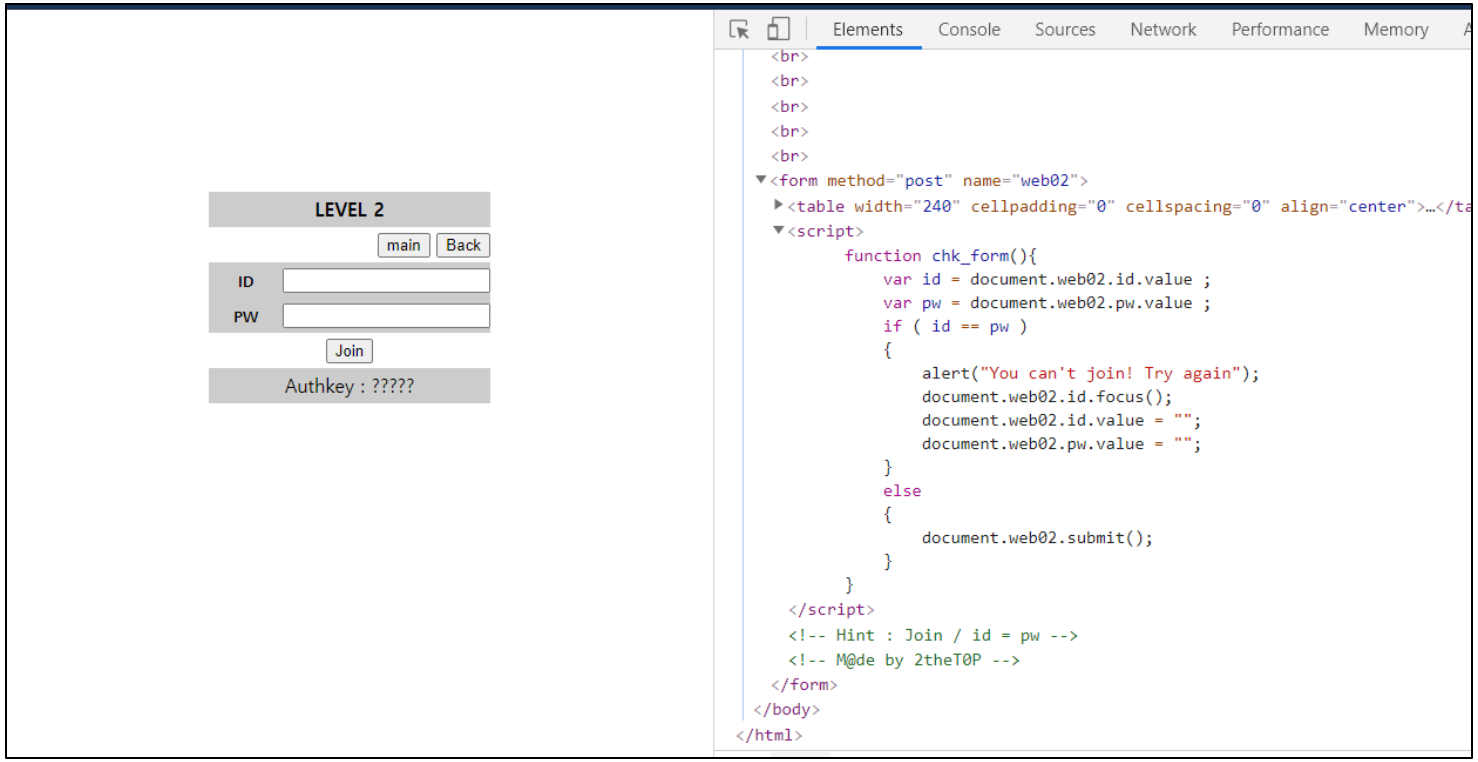
intercept is on을 누르면 '패킷을 가로채겠다'는 의미

forward를 누르면 가로친 패킷을 다시 제출

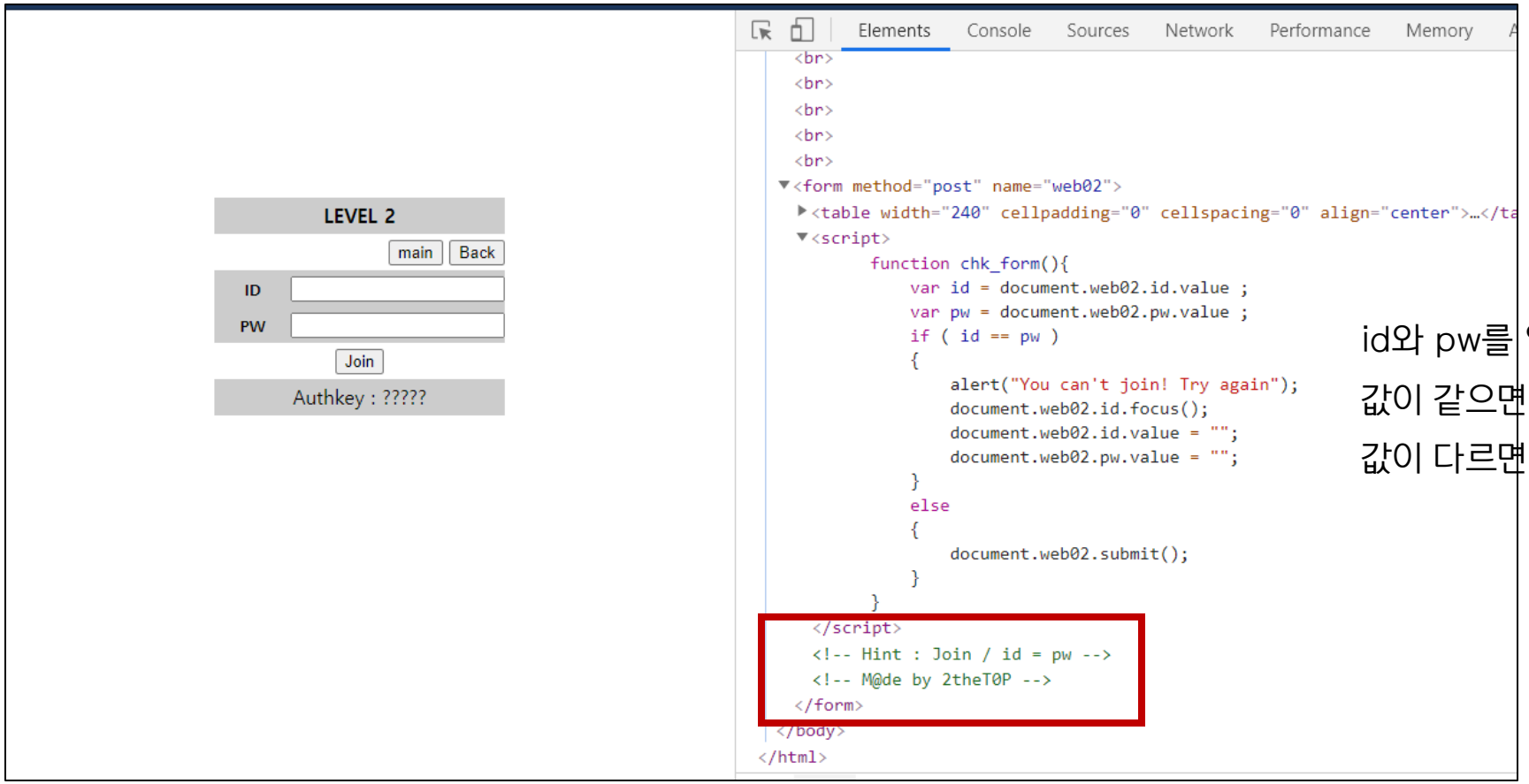
02. Burp Suite(실습)

http://suninatas.com/challenge/web02/web02.asp

Open Browser → suninatas의 2번 문제



02. Burp Suite(실습)

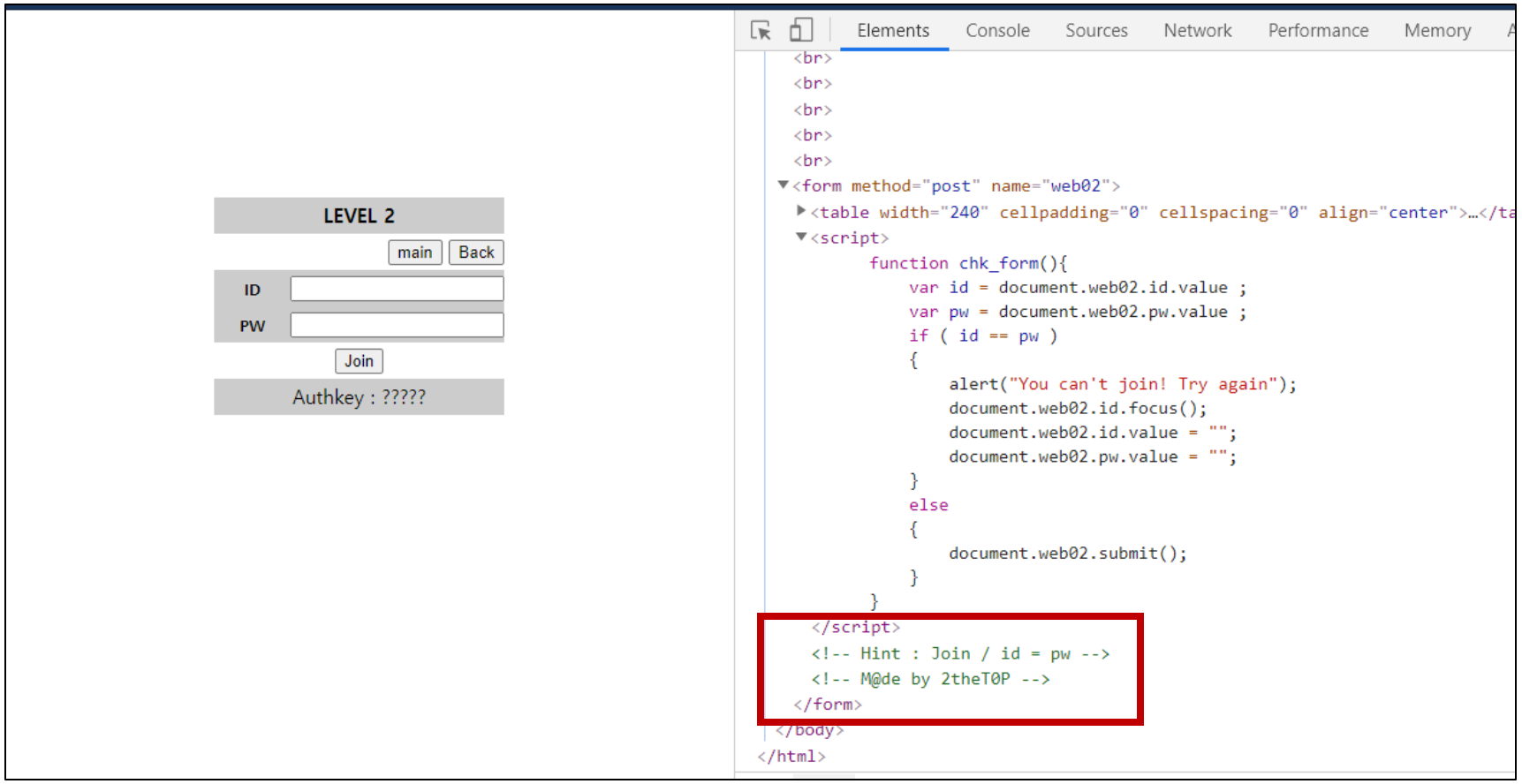


id와 pw를 읽어온 후,

값이 같으면 X

값이 다르면 제출 → 해보면 Authkey를 주지 않음

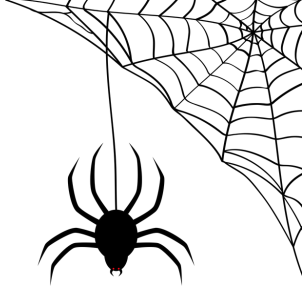
02. Burp Suite(실습)



ID와 PW에 같은 값

→ console창을 통해 submit()도 가능

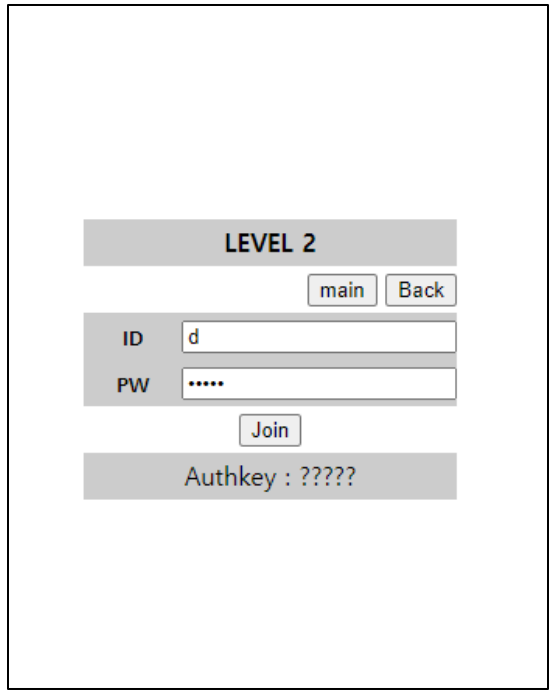
02. Burp Suite(실습)

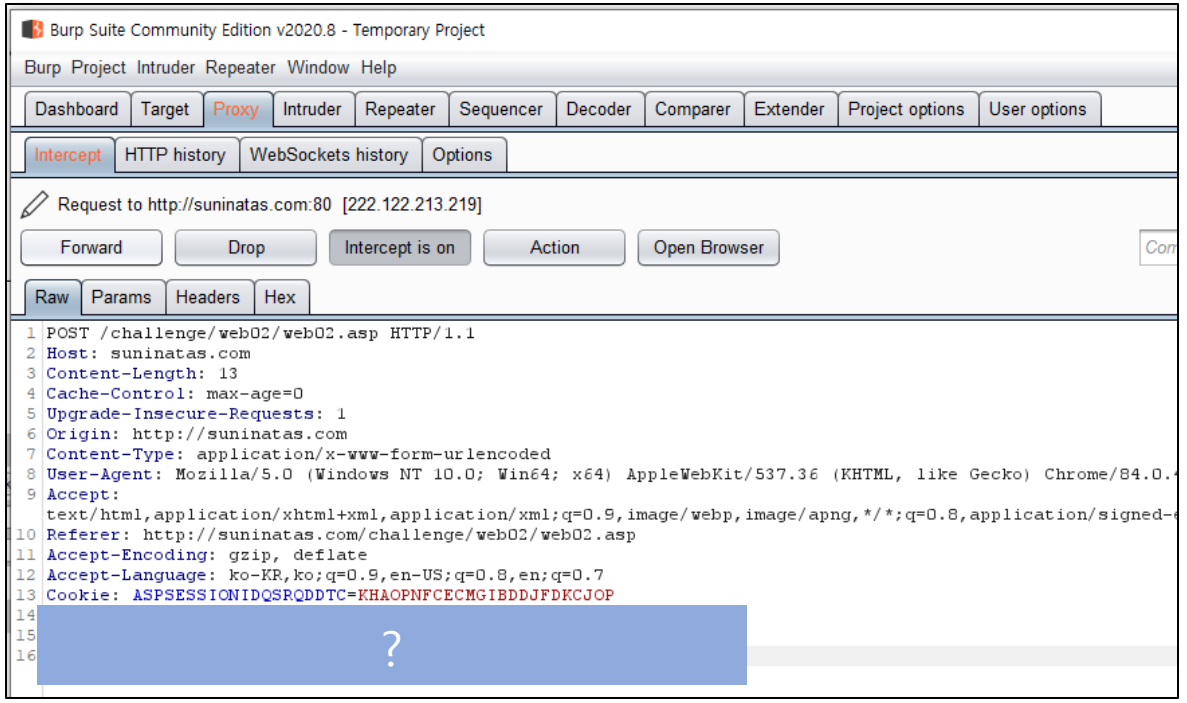


<우리의 계획>

1) id와 pw가 다르게
2) Burp Suite를 통해 서버로 가는 데이터를 잡음
3) 데이터를 수정
4) 다시 서버로 보냄

02. Burp Suite(실습)

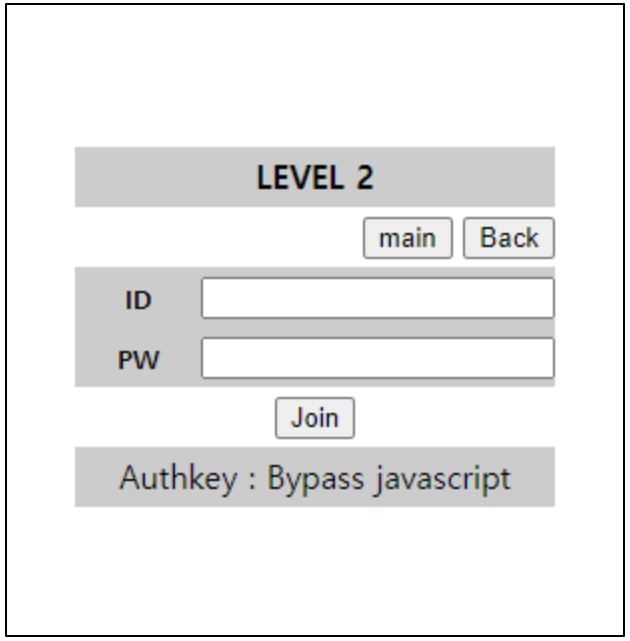




우리가 원하는 데이터(id, pw)가 나올 때까지

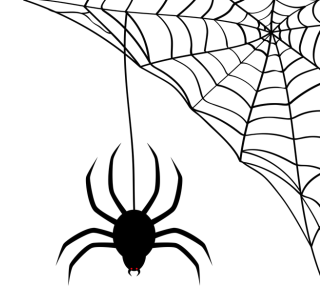
forward 후 → 데이터 수정 → forward

02. Burp Suite(실습)



Authkey를 받아내서 Auth창에 입력하면 score 획득

03. 마무리



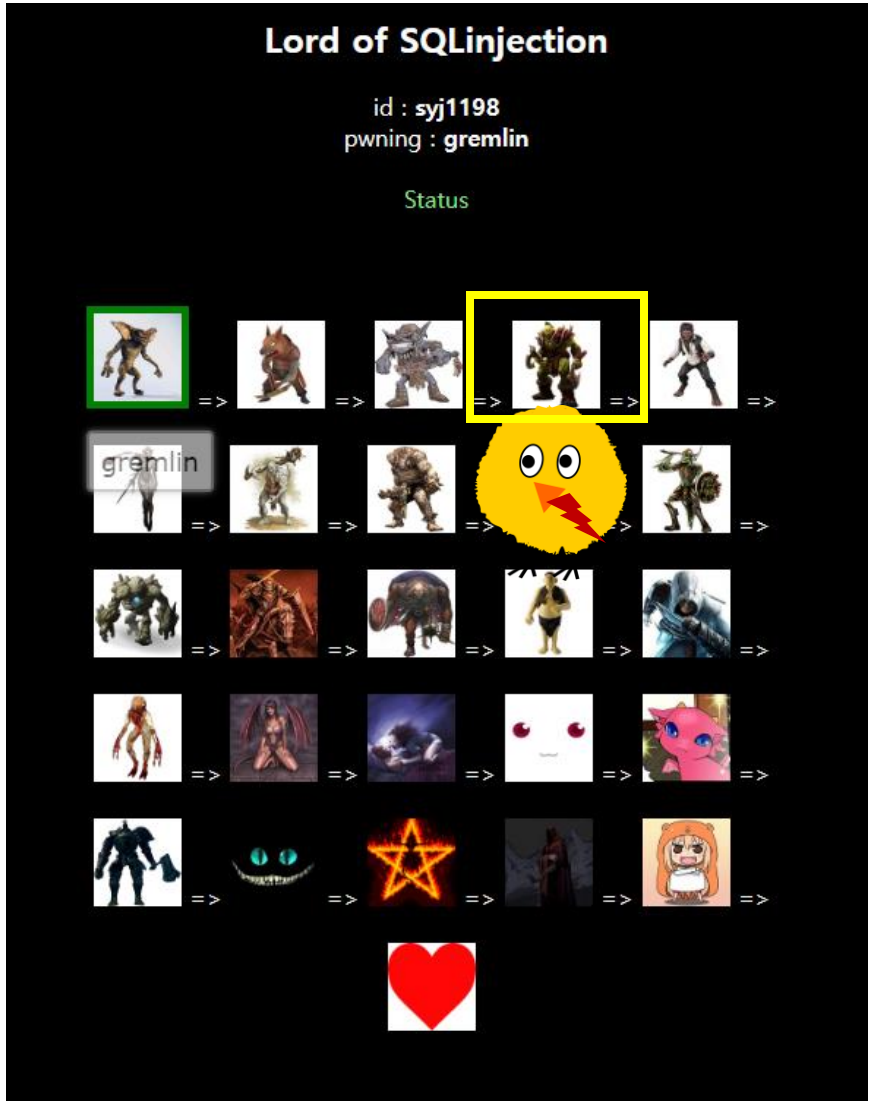
- 다양한 wargame의 문제들을 풀어볼 것

- 사실 문제의 write up (풀이)가 구글링하면 다 나오지만,
  그걸 보고, 아무 의미도 모른 채 그대로 따라하는 건 공부 X

- 구글링하면 나오는 write up처럼
  자신만의 풀이법을 블로그에 적으며, 기록을 남기는 게 좋다!!

- 문제를 어느 순서로 풀지 모르겠으면 저에게 연락

03. 과제



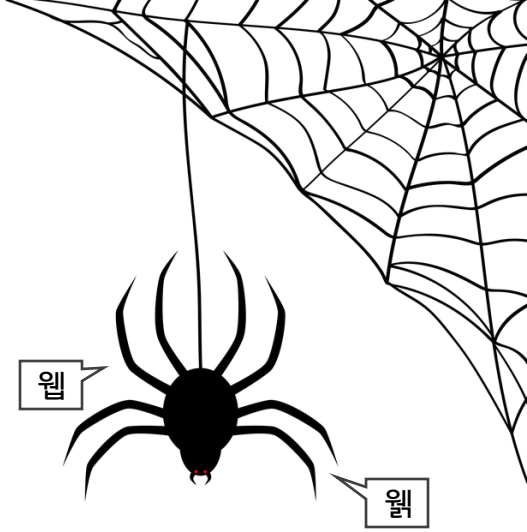
과제!!

https://los.eagle-jump.org/에서

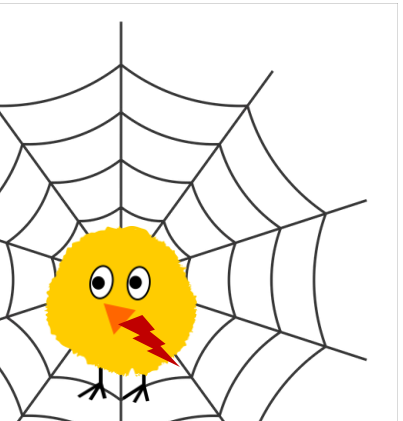
4번 문제

→ Blind SQL Injection 문제

(python코드를 작성하여 푸는 것을 추천)



Q&A



안드로이드 앱 해킹 교육

일시 : **8/10~8/23 (주 선택 2회) | 오후 7시 ~ 오후 9시 | 공5410**

교육자 : 18 박민

주 교육 내용 : 안드로이드 리버싱과 **후킹 테크닉을 이용한 어플리케이션 해킹**

기본 지식 : java, javascript

신청 : https://forms.gle/CJzyVbgsjHfvFn5U6

* 몇몇 실습 및 과제는 실제 서비스 되는 앱을 대상으로 진행하므로 해당 부분 유튜브 영상 제공 불가능

강의구성

0 회차 (교육전) : Nox, frida, adb, jadx, ida 설치

1 회차 : 메서드 후킹과 루팅 탐지 우회 기법

2 회차 : 객체(instance) 후킹과 메서드 강제 호출

3 회차 : JNI 소개 및 네이티브 함수 후킹

4 회차 : JNI 후킹을 이용한 게임 해킹 기법