



웹 취약점 이해

김도연 이용현 이현지

목차 Contents

주제 선정 동기

웹 취약점과 대응 방법

느낀점

지난 프로젝트 소개

실습

1. 주제 선정 동기

주제 선정 동기

<title>

웹과 **HTML**

김도연 안나영 이용현 이현지

</title>



2. 지난 프로젝트 소개

지난 프로젝트

웹과 HTML

1. 인터넷과 웹

- 인터넷과 웹의 역사
- 웹의 구성

2. HTML

- HTML의 역사
- HTML의 기본 문법

지난 프로젝트 인터넷과 웹

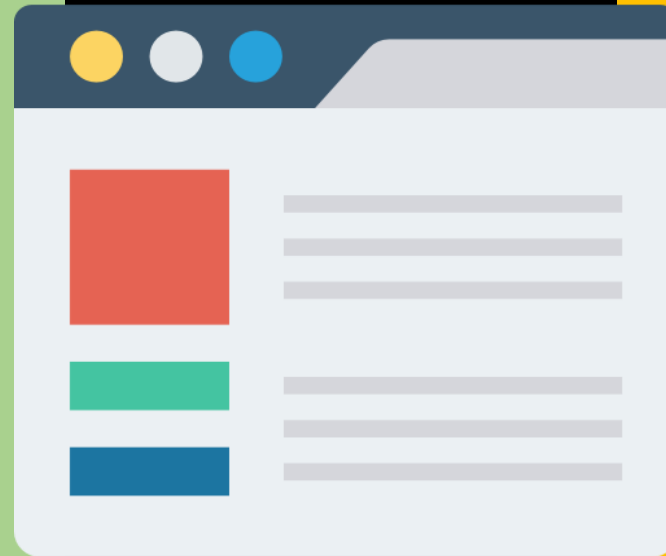


WWW

지난 프로젝트

웹의 구성

**Web
Client**



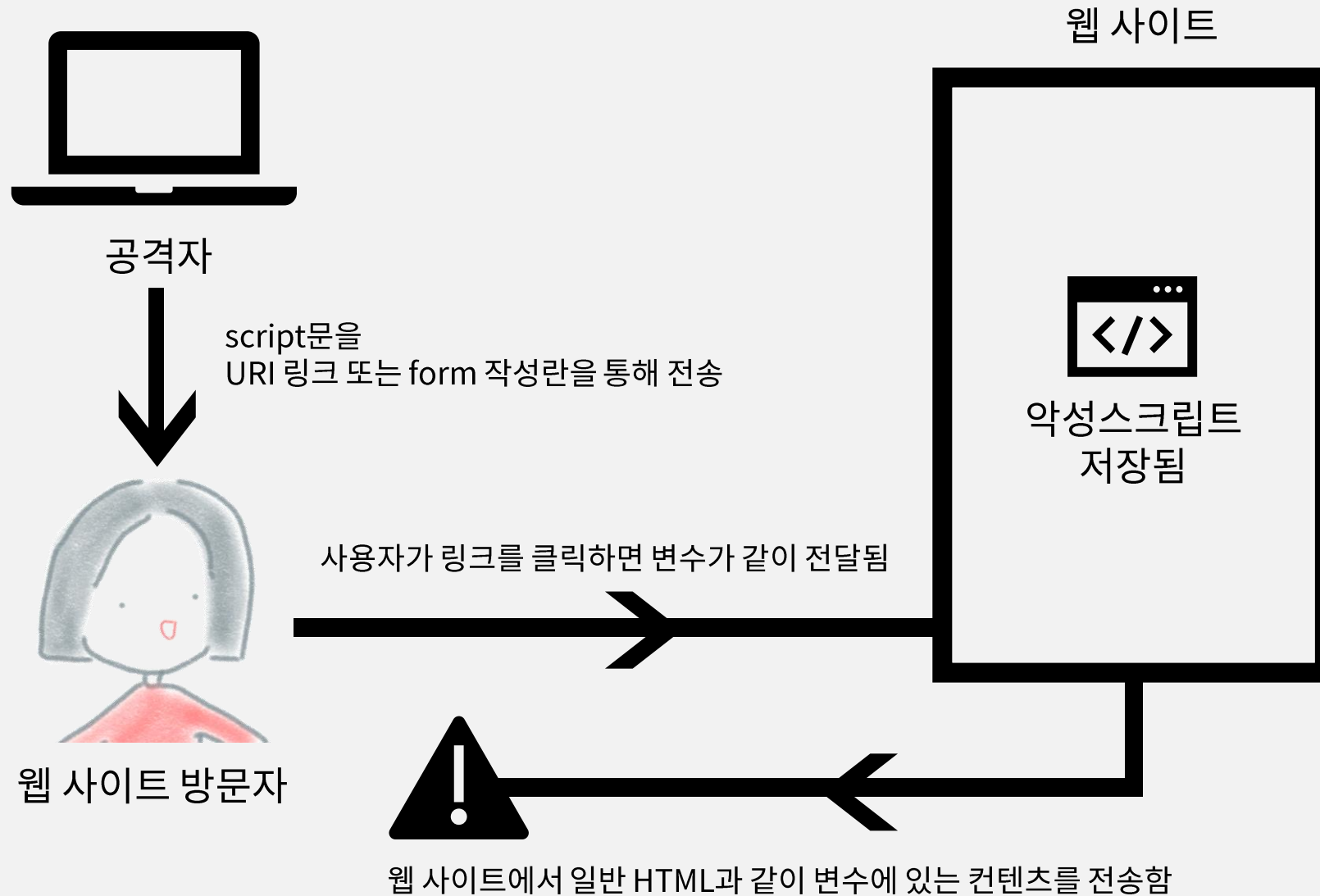
**Web
Server**

3. 웹 취약점

XSS (Reflected)

```
<script>alert(1)</script>
```

XSS (Reflected)



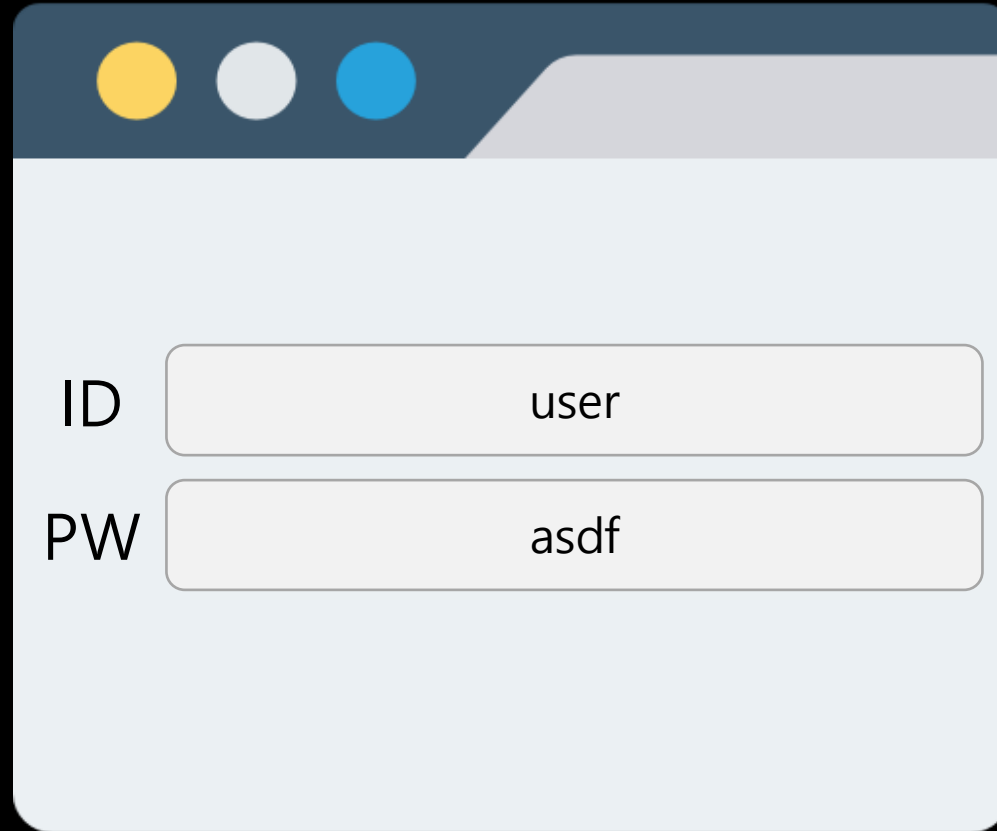


XSS (Reflected)

```
htmlspecialchars($_GET['command'])
```

script문으로 인식하지 않고 문자 그대로 인식한다.

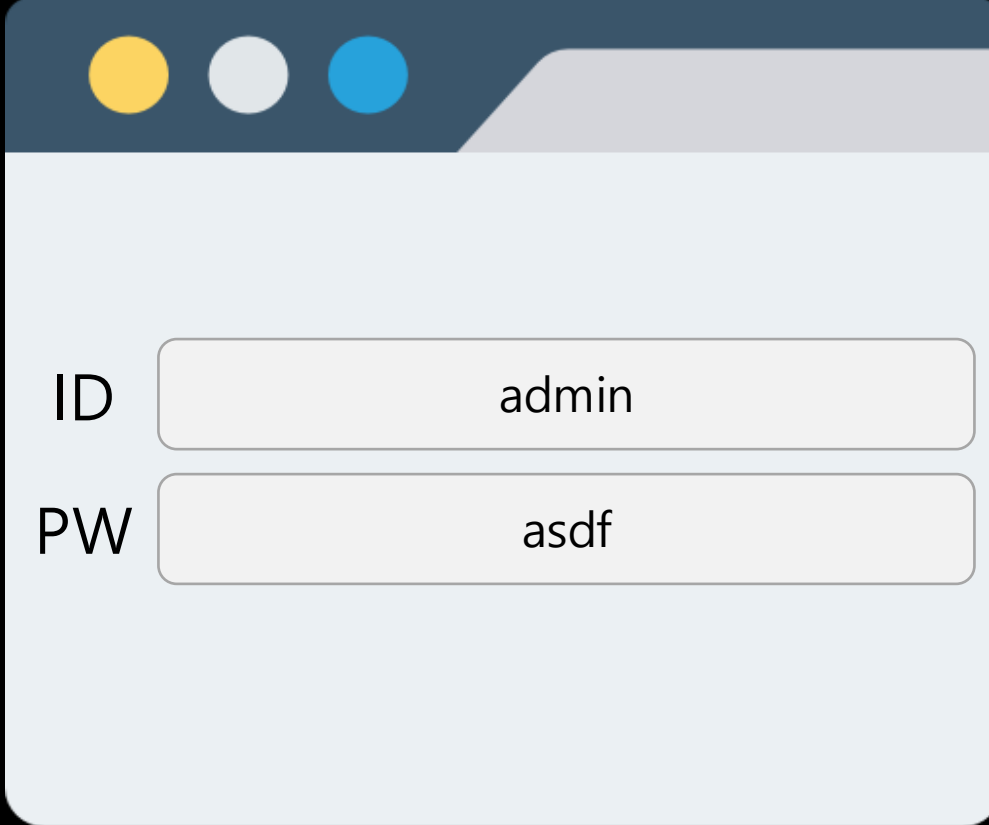
SQL Injection



A web browser window with a light blue header bar containing three colored circles (yellow, white, blue). The main content area is white and contains a login form with two input fields. The first field is labeled 'ID' and contains the text 'user'. The second field is labeled 'PW' and contains the text 'asdf'.

```
select * from user info where id = "admin" and pw = "asdf"
```

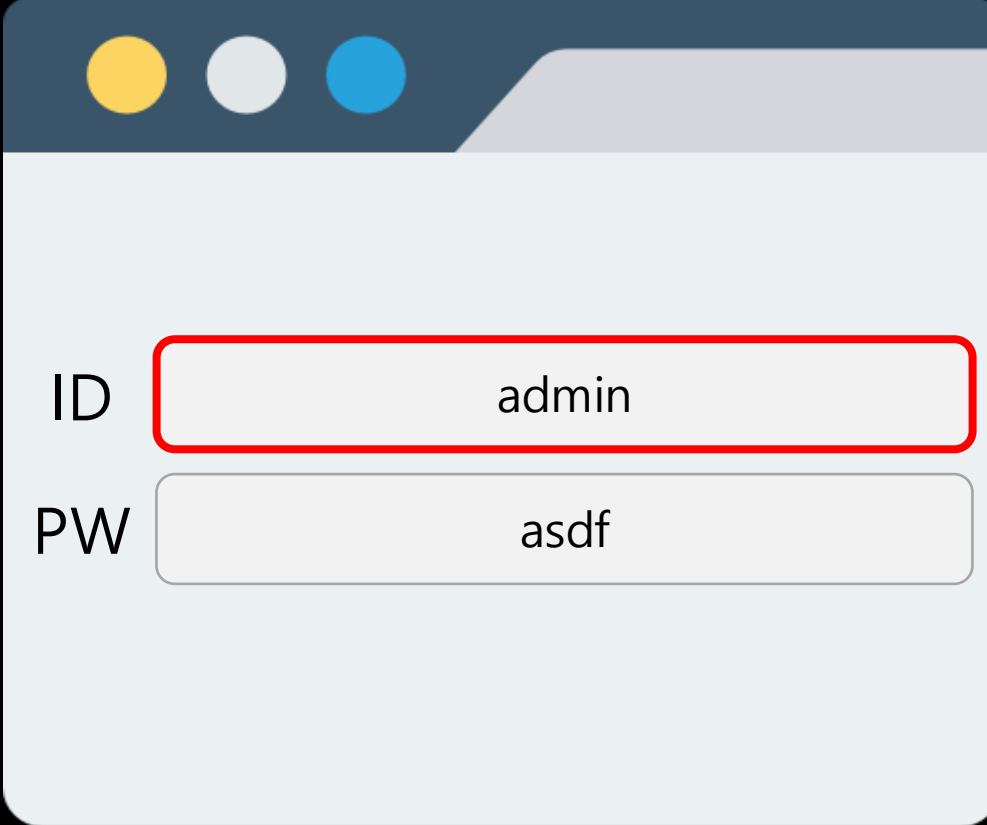
SQL Injection



A login form with two input fields. The first field is labeled 'ID' and contains the text 'admin'. The second field is labeled 'PW' and contains the text 'asdf'. The form has a light blue header with three colored circles (yellow, white, blue) and a light blue body.

`select * from user info where id = "admin" and pw = "asdf"`

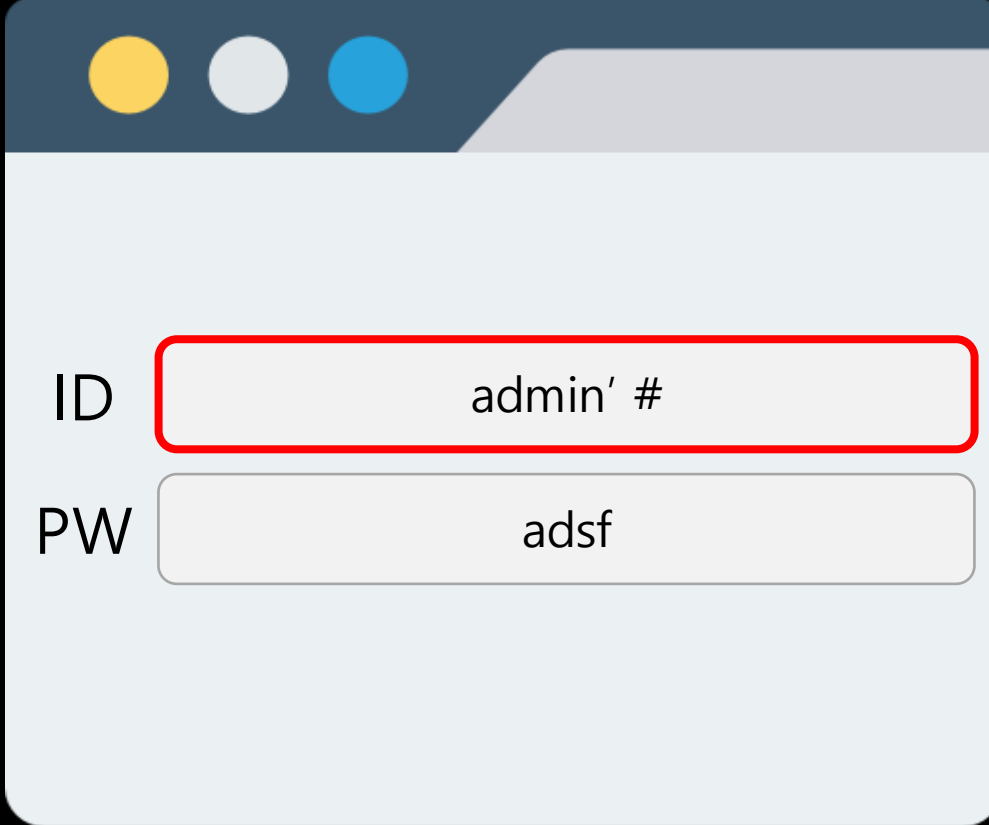
SQL Injection



A web browser window with a login form. The form has two input fields: 'ID' and 'PW'. The 'ID' field contains the text 'admin' and is highlighted with a red border. The 'PW' field contains the text 'asdf'.

```
select * from user where id = "admin" and pw = "asdf"
```

SQL Injection

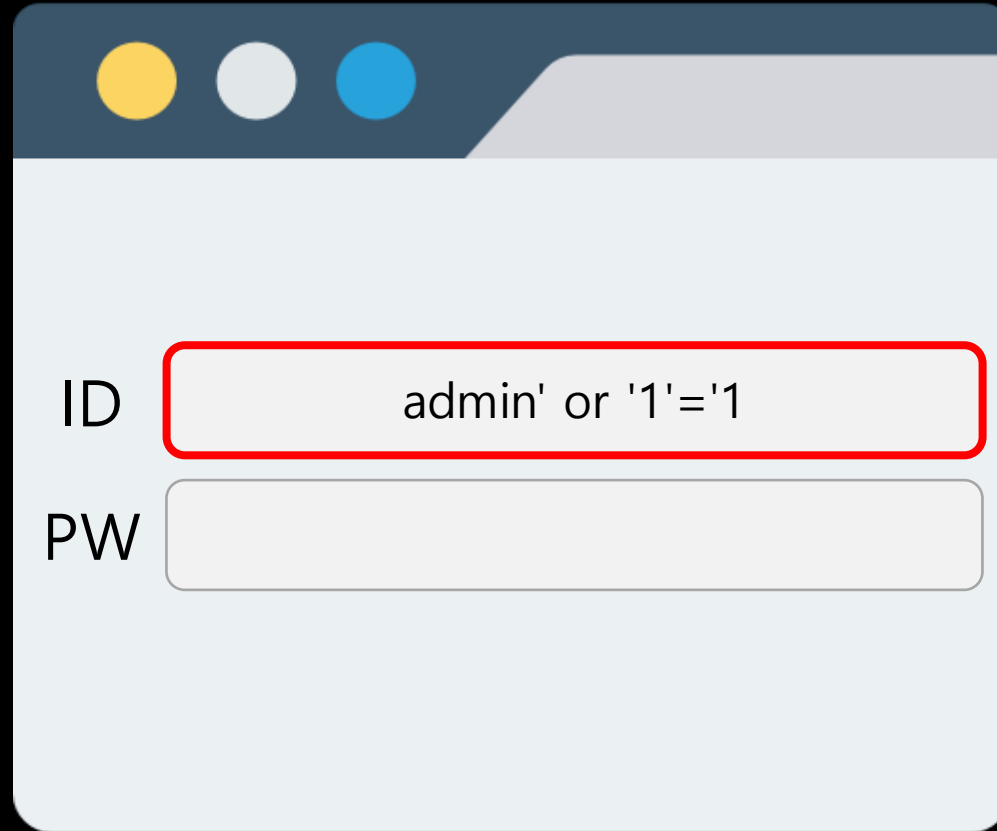


ID

PW

`select * from user where id = 'admin' # password = 'asdf'`

SQL Injection



The image shows a web browser window with a login form. The ID field contains the text "admin' or '1'='1" and is highlighted with a red border. The PW field is empty.

ID	admin' or '1'='1
PW	

`select * from user where id = 'admin' or '1'='1' password = ''`

SQL Injection

```
$conn = mysqli_connect($IP,$ID,$PASSWORD,$DATABASE,$PORT);
$query = "select * from user where id='$id' and password='$pw'";
$result = mysqli_query($conn, $query);
$row = mysqli_fetch_array($result);
mysqli_close($conn);
if(isset($row['id']) && isset($row['password'])) { // id와 pw가 맞다면 login
    $_SESSION['id'] = $row['id'];
    $_SESSION['name'] = "어드민";
    echo "<script>location.href='SQL_injection.php';</script>";
} else { // id 또는 pw가 다르다면 login 폼으로
    // $debug_pw = $row['id'];
    echo "<script>console.log(\"$query\");</script>"; // 잘못된 아이디 또는
    echo "<script>window.alert('invalid username or password');</script>";
```

```
$conn = mysqli_connect($IP,$ID,$PASSWORD,$DATABASE,$PORT);
$query = "select * from user where id='$id' and password='$pw'";
$result = mysqli_query($conn, $query);
$row = mysqli_fetch_array($result);
mysqli_close($conn);
if($id==$row['id'] && $pw==$row['pw']) { // id와 pw가 맞다면 login
    $_SESSION['id'] = $row['id'];
    $_SESSION['name'] = "어드민";
    echo "<script>location.href='SQL_es_injection.php';</script>";
```

SQL Injection

4. 실습!

5. 느낀점



느낀점



이용현

이번에 웹 취약점을 하면서 php에 대해 더욱 알아 볼 수 있었으며, 1차 프로젝트에 비해 대면으로 진행된 타인지 소통은 시작부터 매우 잘 났었습니다. 처음부터 버그와 버그, 버그들로 머리가 빠질 뻔 했지만 사이트가 제대로 돌아가게 되어서 기쁩니다.

느낀점



이현지

웹 서버를 구축하는 것은 처음이었기에 자료를 찾는 것 외에는 별로 도움된 것이 없었지만, 너무 잘 만들어 주어서 고맙습니다. 그리고 완성된 웹 서버를 보니 괜스레 저도 뿌듯하였습니다.



느낀점



김도연

1차 프로젝트 때는 온라인으로 진행돼서 소통의 문제가 조금 있었는데, 이번 프로젝트는 오프라인으로 진행되어서 훨씬 더 수월했습니다. 1차 때 했던 주제의 심화단계 프로젝트를 진행해서 배운게 더 많았습니다. 실습 사이트를 만드는데 여러 오류가 생겨서 많이 당황하고 시간내에 못 만들까봐 걱정됐지만 튜터쌤과 오류 찾아가면서 끝까지 완성한 게 너무 뿌듯합니다.



감사합니다.

김도연 이용현 이현지