

다음과 같이 폼이 있다.

## XSS Challenges

### Stage #2

**What you have to do:**

Inject the following JavaScript command: `alert(document.domain);`

Hint:

Search:

Stage #1과 같이 xss를 시도해보았다.

## XSS Challenges

### Stage #2

**What you have to do:**

Inject the following JavaScript command: `alert(document.domain);`

Hint:

Search:

그러나 xss에 실패했고 아무것도 뜨지 않았다.

그래서 소스를 보았다.

다음이 소스이다.

```
<body><div>
```

```
<h1>XSS Challenges</h1> <!-- Cross Site Scripting (XSS) Quiz -->
```

```
<h2>Stage #2</h2>
```

```
<b>What you have to do:</b><br>
```

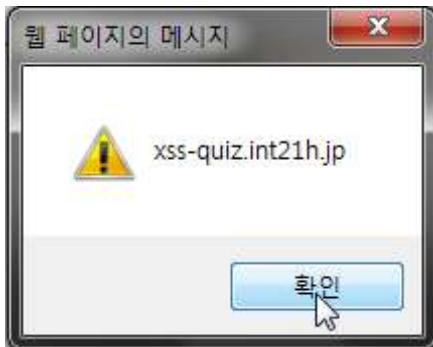
Inject the following JavaScript command: `<code>alert(document.domain);</code>` `<p>`  
`<b>Hint:</b>` `<span id="hide">close the current tag and add SCRIPT tag...</span>`  
`<input type="hidden" name="key" value="tubhf.4/qiq">`  
`<form action="?sid=7d74c13fbf536e73f61fadf3d84549f0b8a9399a" method="post">`  
`<hr class=red>Search: <input type="text" name="p1" size="60" value=""> <input`  
`type="submit" value="Search">`  
`<hr class=red>`  
`</form>`  
`<span id="msg" style="display:none"> </span>`  
`<p>` `<hr>`  
This page was written by yamagata21,  
inspired by `<a href="http://blogged-on.de/xss/"`  
`target=_new>http://blogged-on.de/xss/</a>.`  
`</div>`

`<input type="text" name="p1" size="60" value="">`

우리가 xss를 시도해야하는 곳은 `<input type="text" name="p1" size="60" value="">` 이다.  
value에 들어가므로 ">로 닫고 xss를 시도하면 될 것 같다.

Search:

xss에 성공했다.



stage-3으로 넘어갔다.

**Congratulations!!** Next stage [stage-3.php](#).