Web ontwikkeling 3

Lesson 4: XSS

EXAM QUESTIONS…

- ☑ Explain XSS. Use an example and describe in details the solution in order to avoid XSS.
- ☑ What does XSS stand for?
- ☑ …

XSS

- Cross Site Scripting
- Security risk

  eg. stealing session cookie
- Hacker
  - injects **malicious code**
  - into **safe website**
- Often through script in the browser

LOGIN.JSP

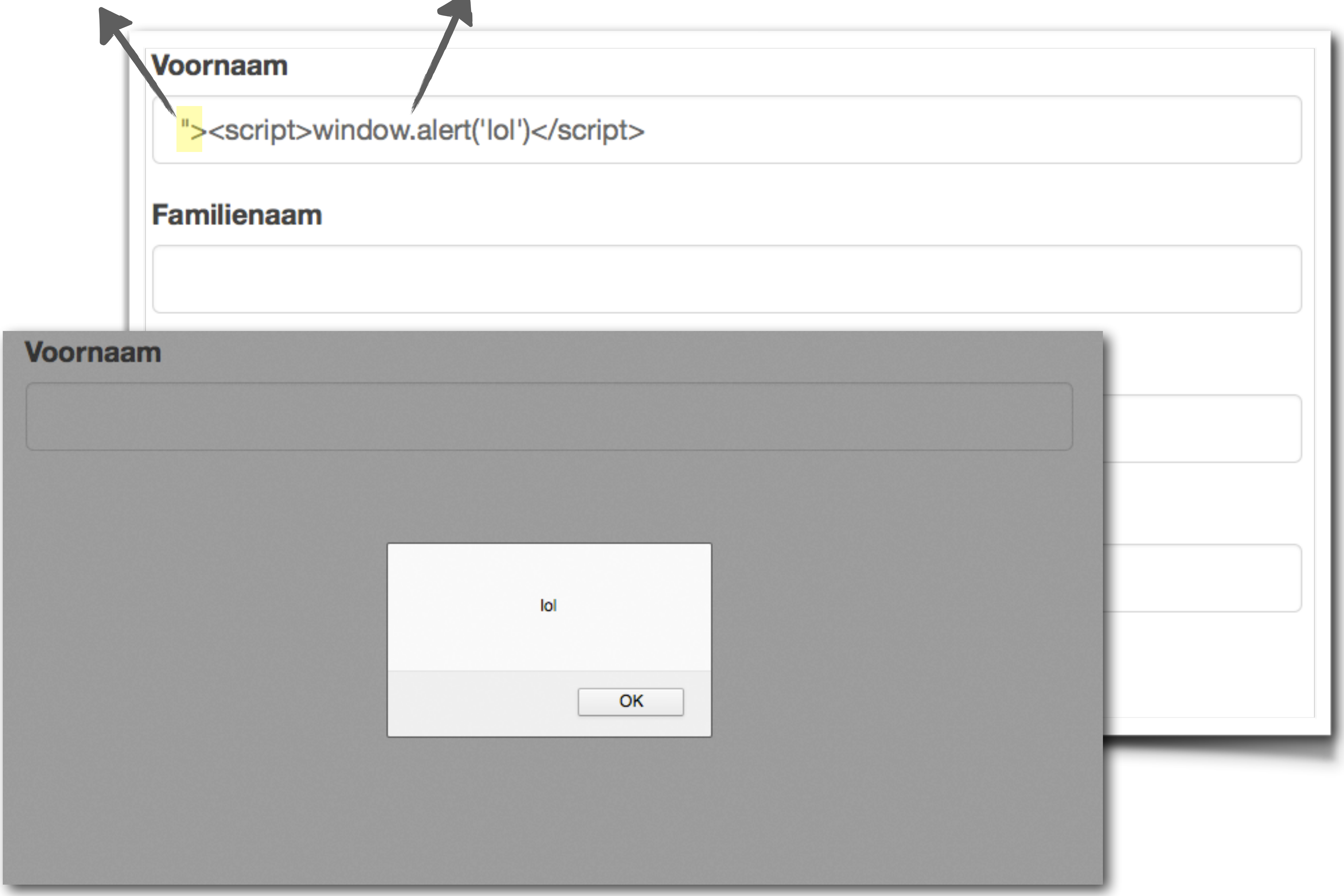
```
<input … value=“${param.username}” />
```

show value again if validation fails

Demo

afsluiten
value attribute

script



Voornaam

"><script>window.alert('lol')</script>

Familienaam

Voornaam

lol

LOGIN.JSP

```
<input … value=“${param.username}” />
```

```
<input … value=“Mieke” />
```

→ no problem

```
<input … value=“”/><script>alert(“lol”);</script>” />
```

↓

problem!

Problem

- in form
- when reloaded (e.g. after validation errors)
- browser parses previous value
- **if script: executed!**
- example: login.jsp

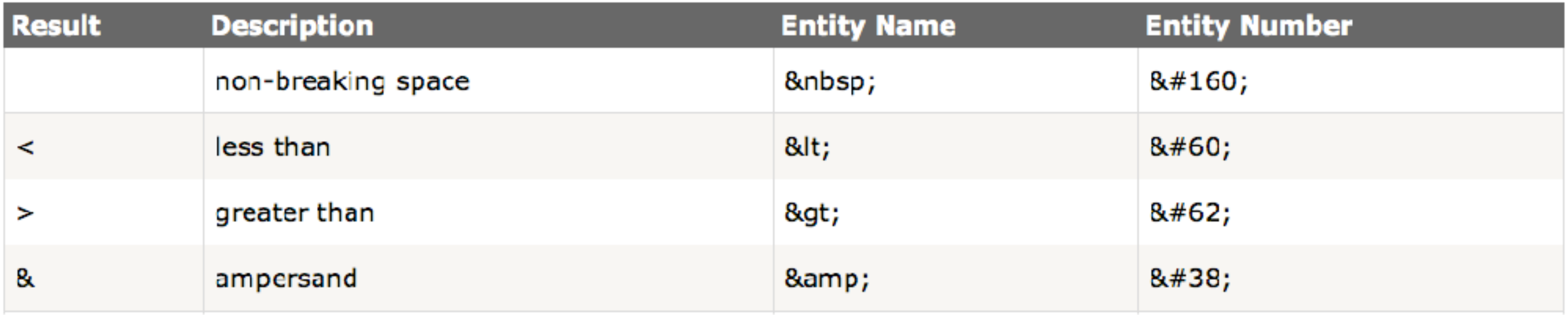
```
<input … value=“${param.username}” />
```

show value again if validation fails

SOLUTION

- cleanup input
  - convert HTML symbols to **HTML entities**
  - browser: shows them but doesn’t interpret it

HTML Special Chars



Result	Description	Entity Name	Entity Number
	non-breaking space	&nbsp;	&#160;
<	less than	&lt;	&#60;
>	greater than	&gt;	&#62;
&	ampersand	&amp;	&#38;

JSP

- Use the JSTL
  - `<c: out>` tag OR
  - `{fn:escapeXml()}` function
- for displaying variables
- **escapes HTML/XML tags!**

NOK

```
<form method="post" action="">
   <fieldset>
      <legend>Login</legend>
      <p>
         <label for="username">Username</label>
         <input type="text" id="username" name="username"
               value="${param.username}">
      </p>
   </fieldset>
   <p>
      <input type="submit" id="save" value="Log in">
   </p>
</form>
```

OK

```
<%@taglib prefix="c" uri="http://java.sun.com/jsp/jstl/core" %>


<form method="post" action="">
   <fieldset>
      <legend>Login</legend>
      <p>
         <label for="username">Username</label>
         <input type="text" id="username" name="username"
               value="<c:out value=‘${param.username}' />">
      </p>
   </fieldset>
   <p>
      <input type="submit" id="save" value="Log in">
   </p>
</form>
```

OK

```
<%@taglib prefix="fn" uri="http://java.sun.com/jsp/jstl/functions" %>
```

```
<form method="post" action="">
   <fieldset>
      <legend>Login</legend>
      <p>
         <label for="username">Username</label>
         <input type="text" id="username" name="username"
               value="${fn:escapeXml(param.username)}">
      </p>
   </fieldset>
   <p>
      <input type="submit" id="save" value="Log in">
   </p>
</form>
```

LOGIN.JSP

```
<input … value=“<c:out value='${param.username}' />” />
```

```
<input … value=“Mieke” />
```

→ no problem

```
<input … value=“&#034;/
&gt;&lt;script&gt;alert(&#034;lol&#034;);&lt;/script&gt;”
```

→ no problem!