XSS

(Cross-Site-Scripting)

von

Sergej

11.05.2016

Inhalt

- Theoretischer Teil
- Gegenmaßnahmen
- Demo

Was ist XSS?

- Injection
- HTML, JS, CSS, SVG, Bilder, Java-Applet, Flash usw.
- OWASP Top 10
- Gefahren
  - ✦ Identitätsdiebstahl
  - ✦ Rechteausweitung

XSS Typen

- Stored XSS
- Reflected XSS
- DOM Based XSS

XSS Typen

- Stored XSS
- Reflected XSS
- DOM Based XSS

Stored XSS

```
<html>
<body>

   <%
    Statement stmt = conn.createStatement();
    ResultSet rs = stmt.executeQuery("select * from users where id=1");
    rs.next();
    String name = rs.getString("name");
   %>

   User Name: <%= name %>

</body>
</html>
```

XSS wäre möglich, wenn der Name des Benutzers in <script>alert(1)</script> geändert wird

Reflected XSS

```
<html>
<body>

    <% String eid = request.getParameter("eid"); %>
    Employee ID: <%= eid %>

</body>
</html>
```

XSS wäre möglich mit http://IP:PORT/site?eid=<script>alert(1)</script>

DOM Based XSS

```
<html>
<body>

Select your language:
<select>
<script>

document.write("<OPTION
value=1>"+document.location.href.substring(document.location.href.indexOf("
default=")+8)+"</OPTION>");

document.write("<OPTION value=2>English</OPTION>");

</script>
</select>
</body>
</html>

-------------------------------------------------------------------------

XSS wäre möglich mit http://IP:PORT/site?default=<script>alert(1)</script>
```

Gegenmaßnahmen

Escape

& --> &
< --> <
> --> >
" --> "
' --> ' (' not recommended because its not in the HTML spec)

Gegenmaßnahmen

- OWASP XSS Prevention Cheat Sheet

  `<script>...NEVER PUT UNTRUSTED DATA HERE...</script>` directly in a script

  `<div ...NEVER PUT UNTRUSTED DATA HERE...=test />` in an attribute name

  https://www.owasp.org/index.php/XSS_%28Cross_Site_Scripting%29_Prevention_Cheat_Sheet

- Content Security Policy (CSP)
- XSS-Schutz im Web-Framework enthalten
- Keine Blacklist

Demo

Fragen?

Quellen

- https://www.exploit-db.com/exploits/39548/
- https://www.owasp.org/