Sicherheitslücke XSS

Einleitung

Das letzte mal, als ich die Lücke gefunden habe war es in einem Hobby-Browsergame, über die es möglich war, sämtliche Spielaktionen von anderen Spielen durchführen zu lassen, ohne dass sie davon wissen. Das ganze lief über das Einschleusen von Javascript über das Nachrichtensystem. Diese Art des Angriffs nennt man **XSS**.

Beispiel

Nehmen wir als Anfang eine einfache Suchfunktion, die den Suchbegriff angibt:

PHP-Quellcode

```
1. <?php
2. if(isset($_POST['search'])) {
3. echo 'Suche: ' . $_POST['search'];
4. }
5. else {
6. echo '<form method="post" action="index.php"><input type="text" placeholder="Suchbegriff eingeben"
   name="search"><input type="submit" name="submit"></form>';
7. }
```

Alles anzeigen

Geben wir nun in der Suche einen Begriff ein, wird uns dieser genauso wie wir ihn eingegeben haben ausgegeben:
[Blockierte Grafik: http://img853.imageshack.us/img853/588/bm0z.png] gibt uns "Hallo DU!" aus.

Jetzt kommen wir zum Einschleusen von Javascript:
[Blockierte Grafik: http://img600.imageshack.us/img600/5148/oh20.png]

Drücken wir nun auf Senden, erhalten wir nicht etwa "<script type="text/javascript">alert("XSS");</script>Hallo :)" , sondern nur: [Blockierte Grafik: http://img11.imageshack.us/img11/8565/bfad.png] Dafür erscheint eine Alert-Meldung auf, die uns XSS sagt. Damit ist uns möglich über nicht gesicherte Formulare im Nachrichtensystem Scripte zu verschicken, die bestimmte Aktionen ausführen. (Per POST-Request nahezu jede Benutzeraktion ausführen, da so das senden von Formularen simuliert werden kann.)

Schutz

Schützen können wir uns, indem wir die PHP-Funktion htmlspecialchars() nutzen, die HTML-Zeichen (< easy-coding.de/index.php?form=…lexiconID=5&c=0#headline2, >, ...) umwandelt (<, >) und damit das Script vom Browser nicht ausgeführt wird.

PHP-Quellcode

```
1. <?php
2. if(isset($_POST['search'])) {
3. echo 'Suche: ' . htmlspecialchars($_POST['search']);
4. }
5. else {
6. echo '<form method="post" action="index.php"><input type="text" style="width: 400px;" placeholder="Suchbegriff eingeben" name="search"><input type="submit" name="submit"></form>';
7. }
```

Alles anzeigen

Wichtig: Damit werden nicht alle Möglichkeiten abgedeckt.