BENUTZERDOKUMENTATION (ALEPHINO 5.0)

Vorbeugung gegen Cross-Site-Scripting (XSS) Attacken

Autor: Frank Bieber

Vorbemerkungen 2
1) Methode 3
2) Implementierung 3

Vorbemerkungen

Laut Wikipedia bezeichnet *Cross-Site-Scripting eine Art der HTML-Injection. Cross-Site-Scripting tritt dann auf, wenn eine Webanwendung Daten annimmt, die von einem Nutzer stammen, und diese Daten dann an einen Browser weitersendet, ohne den Inhalt zu überprüfen. Damit ist es einem Angreifer möglich, auch Skripte indirekt an den Browser des Opfers zu senden und damit Schadcode auf der Seite des Clients auszuführen.*
Mit anderen Worten: Stets dann, wenn Nutzereingaben durch eine Anwendung wie den Alephino OPAC auf den zurückgelieferten Seiten reflektiert werden, kann es zum Mißbrauch derart kommen, daß per eingeschleusten Skript-Elementen, zumeist JavaScript, Umleitungen auf fremde Webseiten initiiert werden. Die Fehlertoleranz der Browser gegenüber ungültigem HTML-Code erleichtert derartige Angriffe.

Erfolgreiche Attacken auf die zugrundeliegenden Programme, die Datenbank oder die unterliegenden Server sind bei Alephino bislang erfolglos geblieben, gleichwohl es, wie Logdateien gehosteter Alephino-Instanzen vielfach aufzeigen, an Versuchen von Hackern und Script-Kiddies aus aller Welt, Alephino zu „knacken“, nicht mangelt.

Die Widerstandsfähigkeit von Alephino hat etwas mit der zugrundeliegenden Technologie zu tun. So laufen Angriffsversuche per SQL-Injektion oder Ausnutzung bekannter Schwachstellen in PHP, Java, Perl, Python, MySQL etc. regelmäßig in’s Leere.

1) Methode

Vereinfacht ausgedrückt, basiert das in Alephino implementierte Verfahren zur Abwehr von XSS-Attacken darin, alle Argumente einer URL nach verdächtigen Zeichenfolgen zu durchsuchen, und diese vor der Verarbeitung zu entfernen, um sie „unschädlich“ zu machen. Beispiele für solche Zeichenfolgen sind:

<script
<meta
javascript:
onerror
onload

Möchte man verhindern, daß beliebige HTML-Elemente eingeschleust werden können, ist der generelle Ausschluß von Spitzklammern, die zu deren Notierung notwendig sind empfehlenswert. Allerdings beraubt man sich, da diese in der Abfragesyntax von Alephino zugleich als Operatoren dienen, der Möglichkeit, Bereichsabfragen auf numerische Suchbegriffe anzuwenden, etwa zur Abfrage eines Bereiches von Erscheinungsjahren oder Identnummern.

Groß- bzw. Kleinschreibung sind für die Mustererkennung irrelevant, ebenso die Kodierung von (Sonder-)Zeichen, sog. URL Encoding.

Das Verfahren kann, da gesteuert durch Parameter in der Konfiguration des OPAC, jederzeit um weitere Zeichenfolgen erweitert werden.
Einstweilen bin ich zuversichtlich, damit die prominentesten Vertreter des Cross-Site-Scripting abwehren zu können. Einen Ersatz für die Möglichkeiten professioneller Firewalls bietet Alephino jedoch gewiß nicht. Dem Anspruch, alle bereits bekannten und erst recht künftige Varianten von Attacken abzuwehren, wird Alephino nicht gerecht werden können.

Überhaupt sind Zweifel angebracht, ob ein vollständiger Schutz von Web-Anwendungen gegen alle denkbaren Angriffsmöglichkeiten jemals darstellbar sein wird.

2) Implementierung

Die Programme ***alipac***(***.exe***) und ***aliadm***(***.exe***) wurden mit der zuvor erläuterten Filterfunktion ausgestattet und sind zunächst zu ersetzen. Dies geschieht durch Entpacken des Service-Packs:


XSS Service Pack für Microsoft® Windows)
bzw.

XSS Service Pack für Linux (Architektur IA32)

im Verzeichnis des Servers.
Linux-Nutzer beachten bitte die Empfehlung, sollte das Entpacken mit ***root*** ausgeführt worden sein, ausführbare Programme der Alephino gewidmeten **uid** und **gid**, etwa ***alephino*** und ***exlibris*** zuzuordnen und ggfs. Zugriffsrechte zu setzen:

chown alephino:exlibris alipac aliadm
chmod ug+xs alipac aliadm

Es sei an dieser Stelle erwähnt, daß Bibliotheken, die unsere Hosting-Dienstleistung nutzen, nichts unternehmen müssen. Programme und zugehörige Kontrolltabellen wurden von uns bereits auf den aktuellen Stand gebracht, so auch in diesem Fall.

2.1) Konfiguration

In der Konfigurationsdatei des Web OPAC ***etc/alipac.cfg*** sind folgende Einträge vorzunehmen, die Sie nach Entpacken des Service-Pack in der Datei ***etc/xss.txt*** vorfinden.

```
(XSSPrevent)
Denied = <script
Denied = <meta
Denied = javascript:
Denied = onerror
Denied = onload
```

Zusätzlich (oder ersatzweise) mögen Sie, wie bereits erwähnt, alle Spitzklammern verbieten, mit:

Denied = <
Denied = >

Sofern das Service-Modul, das grundsätzlich ebenso betroffen sein kann, öffentlich zugänglich ist, sollten dieselben Einträge auch in der Konfigurationsdatei ***etc/alephino.cfg*** eingefügt werden.
Wie erläutert, kann die Liste der zu unterdrückenden Zeichenfolgen bei Bedarf bzw. Auftauchen neuer Varianten beliebig erweitert werden.