XSS-Angriffe auf Webservices

Laboraufgabe Block 4

25HS

Inhaltsverzeichnis

1 Einführung **2**

2 Aufgabe **2**

2.1 Setup 2

2.2 Tipps zum Vorgehen 2

1 Einführung

In diesem Lab werden wir einen Angriff im realen Internet vom Labor aus machen. Wir treffen dabei Vorkehrungen, damit wir nicht als Angreifer im Internet auffallen.

2 Aufgabe

2.1 Setup

Für diese Übung benötigen Sie lediglich einen Zeitgemässen Browser (Firefox oder Chrome tun es völlig), mit dem Sie effizient den Sourcecode einer Seite betrachten können.

Wichtiger Hinweis:

- Tun Sie nichts was in einer Datenbank persistiert wird (also keine Accounts mit speziellen "usernamen" oder Gästebucheinträge und ähnliches).
- Wenn Ihre IP gesperrt wird, dann gehen Sie weiter zu einer anderen Seite.

2.2 Tipps zum Vorgehen

1. Starten Sie den Webbrowser und öffnen Sie eine beliebige Seite, die Sie mittels XSS angreifen möchten. Geeignet sind:
   - Alle Seiten, die "Handgemacht" sind oder nur "Semiprofessionell'
   - Parameter (GET oder POST) akzeptieren.
   - Auf der darauf Folgenden Seite den von Ihnen in den Parametern angegebenen Text wieder ausgeben.
2. Versuchen Sie über den Parameter (z.B. ein Suchfeld; Meistens viel interessanter sind "hidden"-Felder) einen Text wie "<script>alert();</script" zu übergeben. Beobachten Sie wie der Text eingebettet wird (Verwenden Sie nicht die Debug-Konsole von Firefox/Chrome! Sie normalisiert die Ausgabe). Versuchen Sie mittels angefügtem Escaping den Skripttag korrekt auszuführen.
3. Wenn Sie eine Alertbox erhalten, dann haben Sie gewonnen.

Versuchen Sie so viele Seiten wie möglich zu finden.