Angreifbarkeit von Webapplikationen

Vortrag über die Risiken und möglichen Sicherheitslücken bei der Entwicklung datenbankgestützter, dynamischer Webseiten

RDF Die Technikerschule

Angreifbarkeit von Webapplikationen

Gliederung:

- Einführung
- technische Grundlagen
- Strafbarkeit im Sinne des StGB
- populäre Angriffstechniken
- praktische Anwendung
- Fragen / Diskussion

Angreifbarkeit von Webapplikationen

Einführung:

Die Entwicklung von Webapplikationen ist vielfach sehr gut und ausführlich beschrieben.
Viel seltener beschrieben ist die Gefahr aufgrund mangelnder Kenntnis Sicherheits-lücken in seinen Webapplikationen nicht zu schliessen.

Doch was sind eigentlich Webapplikationen?
Und was sind überhaupt Sicherheitslücken?

Angreifbarkeit von Webapplikationen

Einführung:

Webapplikation (lt. Wikipedia):
Eine Webanwendung oder Webapplikation ist ein Computer-Programm, das auf einem Webserver ausgeführt wird, wobei eine Interaktion mit dem Benutzer ausschließlich über einen Webbrowser erfolgt.

Angreifbarkeit von Webapplikationen

Einführung:

Sicherheitslücke (lt. Wikipedia):
Eine Sicherheitslücke birgt Risiken bezüglich der Sicherheit betroffener Computersysteme und entsteht unter anderem [...] durch Programmierfehler im Betriebssystem, Browser oder anderen Software-anwendungen, die auf dem System betrieben werden.

Angreifbarkeit von Webapplikationen

technische Grundlagen:

- Grundlagen Webseiten
- Grundlagen Skriptsprachen
- Grundlagen Datenbanken
- Verarbeitung von Formularen

Angreifbarkeit von Webapplikationen

technische Grundlagen: Webseiten

- HTML (Hypertext Markup Language)
  Grundlage des World Wide Web
- CSS (Cascading Stylesheets)
  Formatierungssprache für HTML-Dateien
- Javascript
  clientseitige Skriptsprache

Angreifbarkeit von Webapplikationen

technische Grundlagen: Webseiten

→ statische Webseiten

Angreifbarkeit von Webapplikationen

technische Grundlagen: Skriptsprachen

- Serverseitige Skriptsprachen
- Programmiersprachen zur Entwicklung dynamischer Webseiten
- viele verschiedene Sprachen (z.B.: PHP, Perl, Python, Ruby, ASP, …)

Angreifbarkeit von Webapplikationen

technische Grundlagen: Skriptsprachen

→ dynamische Webseiten / Webapplikationen

Angreifbarkeit von Webapplikationen

technische Grundlagen: Datenbanken

- System zur elektronischen Datenverwaltung
- Viele verschiedene Datenbanksysteme (MySQL, PostgreSQL, SQLite, Oracle, Sybase, Microsoft SQL Server, …)
- Steuerung über SQL-Befehle
- SQL ist standardisiert nach ISO & ANSI, man kann damit Datenstrukturen definieren, Daten kontrollieren und manipulieren.

Angreifbarkeit von Webapplikationen

technische Grundlagen: Datenbanken

→ datenbankgestützte dynamische Webseiten / Webapplikationen

Angreifbarkeit von Webapplikationen

technische Grundlagen: Formulare

- Verarbeiten von Benutzereingaben
- Steuerung von Webapplikationen
- Schnittstelle zum User
- Höchstes Potential an Sicherheitslücken
- Daten können auf 2 verschiedene Arten übertragen werden: POST & GET

Angreifbarkeit von Webapplikationen

technische Grundlagen: Formulare

- Übertragungsmethode festlegen:

```
<form method="POST">[...]</form>
<form method="GET">[...]</form>
```

Angreifbarkeit von Webapplikationen

technische Grundlagen: Formulare

- GET: Daten werden an die URL angehängt
  z.B.: http://meineseite.de?farbe=rot
- POST: Daten werden nicht sichtbar übertragen

Angreifbarkeit von Webapplikationen

Strafbarkeit im Sinne des StGB

- § 202a Ausspähen von Daten
- [1]: Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Angreifbarkeit von Webapplikationen

Strafbarkeit im Sinne des StGB

- § 202b Abfangen von Daten
- Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten aus einer nichtöffentlichen Datenübermittlung [...] verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

Angreifbarkeit von Webapplikationen

Strafbarkeit im Sinne des StGB

- § 303a Datenveränderung
- [1]: Wer rechtswidrig Daten löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.
- [2]: Der Versuch ist strafbar.

Angreifbarkeit von Webapplikationen

Strafbarkeit im Sinne des StGB

- § 303b Computersabotage
- [1] Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er [...] eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

Angreifbarkeit von Webapplikationen

populäre Angriffstechniken:

- Cross-Site-Scripting (XSS)
  - persistentes XSS
  - nicht persistentes XSS
- SQL-Injection
  - Veränderung von Daten
  - Ausspähen von Daten
  - Einschleusen von beliebigen Code
  - zeitbasierte Angriffe

Angreifbarkeit von Webapplikationen

populäre Angriffstechniken: XSS

- Cross-Site Scripting (lt. Wikipedia)
  [...] bezeichnet das Ausnutzen einer Computersicherheitslücke in Webanwendungen, indem Informationen aus einem Kontext, in dem sie nicht vertrauenswürdig sind, in einen anderen Kontext eingefügt werden, in dem sie als vertrauenswürdig eingestuft werden.

Angreifbarkeit von Webapplikationen

populäre Angriffstechniken: XSS

- Persistentes XSS:
  - Schadcode wird auf dem Webserver gespeichert und bei jedem Aufruf der manipulierten Seite mit ausgeliefert.
  - Möglich bei Webanwendungen die Benutzereingaben speichern und später wieder ausgeben (z.B. Gästebücher), wenn die Eingaben nicht ausreichend geprüft werden.

Angreifbarkeit von Webapplikationen

populäre Angriffstechniken: XSS

- Nicht Persistentes XSS:
  - Schadcode wird beim Aufruf der Seite (meist über die URL) eingeschleust.
  - Möglich bei Webanwendungen die Benutzereingaben sofort am Monitor wieder ausgeben (z.B. Suchfunk-tionen), wenn die Eingaben nicht ausreichend geprüft werden.

Angreifbarkeit von Webapplikationen

populäre Angriffstechniken:SQL-Injection

- SQL-Injection (lt. Wikipedia)
  [...] bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken [...]. Der Angreifer versucht dabei, über die Anwendung, die den Zugriff auf die Datenbank bereitstellt, eigene Datenbankbefehle einzuschleusen.

Angreifbarkeit von Webapplikationen

populäre Angriffstechniken:SQL-Injection

- Veränderung von Daten:
  - An den auszuführenden SQL-String wird mit Semikolon ein weiterer angehängt, um Daten in der Datenbank zu verändern.
  - Beide SQL-Befehle werden nacheinander abgearbeitet.
  - Der Angreifer braucht Kenntnisse über den Aufbau der Datenbank (oder Kreativität).

Angreifbarkeit von Webapplikationen

populäre Angriffstechniken:SQL-Injection

- Ausspähen von Daten:
  - Der auszuführenden SQL-String wird so manipuliert, dass er andere Daten ausgibt als ursprünglich vorgesehen.
  - Der Zugriff auf andere Tabellen ist möglich.
  - Der Angreifer braucht Kenntnisse über den Aufbau der Datenbank (oder Kreativität).

Angreifbarkeit von Webapplikationen

populäre Angriffstechniken:SQL-Injection

- Einschleusen von beliebigem Code:
  - statt in die Datenbank wird aufs Dateisystem geschrieben.
  - Server können so z.B. mit Viren/Würmern infiziert werden.
  - Der Angreifer braucht Kenntnisse über den Aufbau der Datenbank, das Betriebssystem und die Dateisystemstrukur (oder Kreativität).

Angreifbarkeit von Webapplikationen

populäre Angriffstechniken:SQL-Injection

- zeitbasierte Angriffe:
  - Über zeitintensive Befehle (z.B. Datenbank-Benchmarks) wird der Server ausgebremst.
  - Server können so stark belastet werden, dass sie nicht mehr erreichbar sind.
  - Der Angreifer braucht Kenntnisse über den Aufbau der Datenbank (oder Kreativität).

Angreifbarkeit von Webapplikationen

praktische Anwendung:

- per SQL-Injection als beliebiger Benutzer anmelden
- per XSS beliebigen Content einschleusen

Angreifbarkeit von Webapplikationen

Quellen:

- http://de.wikipedia.org
  die freie Enzyklopädie
- http://bundesrecht.juris.de
  Bundesministerium der Justiz
- http://www.rdfnuernberg.de
  Rudolf-Diesel-Fachschule Nürnberg

Danke für Eure Aufmerksamkeit!

Angreifbarkeit von Webapplikationen

Fragen / Diskussion