Sicherheit von Webseiten
- was ist aber nicht sein darf -

Andreas Gregor
SG 38.3 – Anlassunabhängige Recherche
LKA Niedersachsen

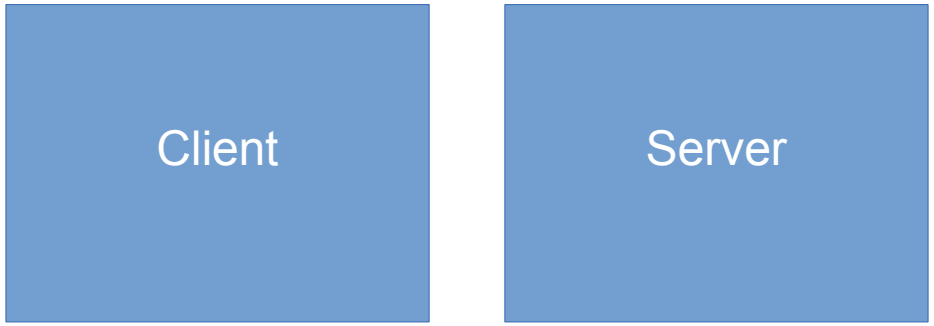
Überblick

- HTML war gestern – Scripte und Gefahren
- Cross-Site-Scripting
- SQL-Injection

HTML war gestern

- Statische Webseiten die Ausnahme
- Dynamische Inhalte werden „on the fly“ erstellt
- Voraussetzung für „Web 2.0“
- Welche (Script-) Sprachen gibt es?
  PHP, Javascript, Java, Python, Perl, Flash und und und.....

Wo werden Scripte ausgeführt?



Javascript	PHP
Java	Perl
Flash	MySQL

Sicherheitsrisiken bei Scripten

- ALLES, was vom Client gesendet wird, kann manipuliert werden
- Beispiele:

  Javascript deaktivieren
  Addon, um Benutzereingaben zu manipulieren (Tamperdata)

Cross Site Scripting

Cross-Site-Scripting (XSS; deutsch Websiteübergreifendes Scripting) 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. Aus diesem vertrauenswürdigen Kontext kann dann ein Angriff gestartet werden.

Ziel ist es meist, an sensible Daten des Benutzers zu gelangen, um beispielsweise seine Benutzerkonten zu übernehmen (Identitätsdiebstahl).

Aus: Wikipedia.de

Cross Site Scripting

Beispiele:

- Fremder Code durch Einfügen von HTML in Kommentaren
- Javascript einfügen
- Benutzervariablen auslesen und verschicken

SQL Injection

SQL-Injection (dt. SQL-Einschleusung) bezeichnet das Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken, die durch mangelnde Maskierung oder Überprüfung von Metazeichen in Benutzereingaben entsteht. Der Angreifer versucht dabei, über die Anwendung, die den Zugriff auf die Datenbank bereitstellt, eigene Datenbankbefehle einzuschleusen. Sein Ziel ist es, Daten auszuspähen, in seinem Sinne zu verändern oder Kontrolle über den Server zu erhalten.

Aus Wikipedia.de

SQL Injection

Beispiele:

- Alle Namen von Nutzern anzeigen
- Ausgabe aller Passwörter

Fragen??

Andreas Gregor

Am Waterlooplatz 11

30169 Hannover

Telefon: 0511/26262-3836

E-Mail:
andreas.gregor@polizei.niedersachsen.de
sg38-aur@lka.polizei.niedersachsen.de