

Die Droge XSS - Cross Site Scripting

19:13:37 18.05.2012

Was Cross Site Scripting ist und wie es ungefähr funktioniert, war mir mehr oder weniger bekannt. Richtig realisiert habe ich es durch das Buch "PHP-Sicherheit", das mir von <http://log.446b.org> empfohlen wurde. Mittlerweile bin ich süchtig. Ich kann nicht mehr vernünftig surfen. Bei keiner Homepage kann ich widerstehen. So bald ich irgendwelche Parameter in der URL sehe muss ich es einfach ausprobieren. Die typischen Lücken sind

- Suchformulare
- Login Formulare
- Seite empfehlen

Aber XSS ist nur die Einstiegsdroge. Irgendwann reicht einem das aber nicht mehr aus und man kommt automatisch zu SQL-Injections. Diese Droge ist noch besser, sie hält einfach viel länger an und sie ist so heimtückisch. Nachdem man sie aber ein paar mal genossen hat, merkt man es reicht nicht mehr und man braucht wieder mehr. Als nächstes folgt dann zwangsläufig Stufe 3 - das Hacken von Servern. Man glaubt nicht wie viele Server es gibt die auf alten Apache Versionen laufen. Besonders intensiv ist die Droge, wenn die Internetseiten versucht haben durch 404 Handling zu vermeiden, dass man die Apache Meldung sieht.