

Einfaches XSS Cross-Site-Scripting

Autoren: Sebastian Schreiber, Stefan Arbeiter

Bekannt wurde XSS (Cross-Site-Scripting) bereits im Jahr 2000, als Fehler in Webservern bekannt wurden, die das XSS erst ermöglichen. Im Gegensatz zu anderen Sicherheitslücken ermöglicht XSS nicht, in den betroffenen Webserver einzudringen, sondern den Browser eines Anwenders anzugreifen, ohne dass dies dem auffällt, dass fremder Code ausgeführt. Insbesondere gefährlich war XSS dann, wenn verwundbare Seiten ihre Funktionalität nur bei niedrigen Sicherheitseinstellungen in den Browsern ermöglichten.

Der Angreifer musste nichts weiter tun als an die Adresse eines verwundbaren Systems sein Skript direkt anzuhängen, und diese Adresszeile einem Opfer unterzubeln. Der Angriff beruht auf nichts weiter, als das innerhalb der Fehlermeldung, die der Server, auf dem das entsprechende Skript natürlich nicht vorhanden ist, das Skript ausgeführt und nicht nur der Quelltext angezeigt wird..

Problematisch waren Fehlermeldungen, die nach folgendem Muster erzeugt werden konnten:

Aufruf: `http://www.legitim.legitim/fehler.html`

Fehlermeldung: `http://www.legitim.legitim/fehler.html not found`

In diesem Fall wurde die Anwendereingabe `-fehler.html-` direkt an den Browser weitergegeben. Wird der hier weitergegebene Text als solcher vom Browser interpretiert, weil der Webserver die Eingabe nicht automatisch als Quelltext darstellt, so liegt eine Verwundbarkeit für XSS vor.

Einen gewissen Aufwand bedeutete die Erzeugung des Skriptes schon, damit der User nicht durch eine Mischung von Fehlermeldung und scheinbar legitimer Seiteninhalte misstrauisch wird. Um Anwender zu täuschen, wurden die entsprechenden Skripte auch gerne im Hexadezimal-Format erzeugt.

Heutzutage ist davon auszugehen, dass zumindest praktisch alle aktuellen Webserver kein XSS mehr ermöglichen, anders sieht die Sache bei der für Gästebüchern und Forensoftware verwendeten Skriptsprachen aus. Im Falle solcher Anwendung ist die Verwendung von Skripten durch Anwender u.U. durchaus erwünscht. Dies ist aber nicht unbedingt transparent, da der Einsatz des Codes oft hinter Forenfunktionen verborgen wird - der dann den gewünschten Code automatisch erzeugt. Anwendern ist also nicht bewusst, dass sie jederzeit Skripte selber schreiben und ausführen lassen können.

Insbesondere Foren, die Cookies zur Vereinfachung der Anmeldung verwenden, haben ein Problem, wenn XSS möglich ist - der Angreifer kann so Skripte schreiben, die es ihm ermöglichen, die Cookies anderer User zu stehlen.

Auch in diesem Fall wird er versuchen, die Bösartigkeit des zur Verfügung gestellten Links zu verbergen, am besten so, dass den Opfern nicht auffällt, dass ein Skript ausgeführt wird. Zahlreiche Betreiber von Foren haben daher die Verwendung von Skripten ganz deaktiviert und lassen nur noch einige wenige HTML-Tags zu - Skript-Code wird dann als reiner Text dargestellt, allein der Versuch der Verwendung kann zum Ausschluss aus dem Forum führen.

Foren-Administratoren haben dann darauf zu achten, dass innerhalb der gesamten Funktionalität keinerlei Skripting möglich ist, und z.B. innerhalb von Messaging-Funktionen auch deaktiviert wird.