Kurzfassung: Towards Elimination of XSS Attacks with a Trusted and Capability Controlled DOM

Mario Heiderich

März 2012, Ruhr-Universität Bochum

Das Internet hat sich zu einem Austauschmedium für verschiedenste Transaktionen entwickelt. Diese Transaktionen schließen die Übertragung persönlicher und anderer sensibler Daten ein, obgleich das Internet in seinen Grundfesten trotz hoher Anforderungen an Sicherheit und Privatsphäre auf simplen Klartext-Protokollen aufbaut, die den Anforderungen moderner Applikationen und sicherer Übertragungen wenig gewachsen scheinen. Browser und andere Werkzeuge zur Darstellung moderner Webseiten und vergleichbarer HTML-Dokumente müssen immer komplexere Anforderungen bewältigen um den Wünschen der Nutzer und Entwickler moderner Applikationen gerecht werden zu können. Mit wachsender Komplexität gehen neben erweiterten Nutzungsmöglichkeiten jedoch oft Sicherheitsprobleme und Interessen-Konflikte einher; das Internet hat sich in seiner Rolle als Informationsprovider in diversen Nutzungsszenarien zu einem willkommenen Hort für Angreifer und Online-Kriminalität im Allgemeinen gewandelt. Mehr und mehr Angriffe werden auf Nutzer, Seitenbetreiber und ähnliche Instanzen ausgeführt – und können oft im Schatten der Anonymität und im Schutz des enormen Rauschens der konstanten Informationsflut für lange Zeit unentdeckt bleiben. Viele dieser Angriffe werden auf einer sehr spezifischen Leinwand skizziert und durchgeführt: den Browsern und Hypertext-Klienten. Diese Arbeit widmet sich der Thematik komplexer Skript-gesteuerter Angriffe, die im Browser ausgeführt und konkret gegen Anwender gerichtet werden. Dabei wird insbesondere der Wirkungsgrad existierender Schutzmöglichkeiten und Technologien beleuchtet. Dies schließt Skript- und HTML-Filter ein, die von Serverbetreibern genutzt werden, umfasst Browser-basierte Angriffsfilter und beinhaltet nicht zuletzt Sicherheits-Erweiterungen für moderne Browser. Signifikanter Forschungsanteil ist die gründliche Analyse und nachfolgenden Invalidierung der Sicherheitsversprechen, die die existierenden Schutztechniken aussprechen. Aus den empirisch gesammelten Daten über die Sicherheit der analysierten Schutztechniken wird die grundlegende Problematik in Form eines nicht zu reparierenden Sichtbarkeits-Problems abgeleitet. Im Anschluss wird die Architektur eines auf Basis der zuvor extrahierten Erkenntnisse spezifizierten Filtersystems adressiert – einschließlich Design, Diskussion, Implementation und anschließender Evaluation dieser neuartigen Skript-basierten Schutzsoftware. Diese kann mit minimalem Implementationsaufwand von existierenden Webseiten übernommen werden kann. Dabei wird auf Techniken zurückgegriffen, die von den Standrads ECMA Script 5 und dem sich noch in der Entwicklung befindenden Entwurf für ECMA Script 6 befinden. Final diskutiert werden verbleibende Herausforderungen und Limitierungen, zukünftige Entwicklungen im Bereich der Browsertechnologien und Auswirkungen auf die beschriebene neuartige Schutzsoftware.