Vorwort

Noch vor fünfzehn Jahren war das Web so simpel wie unbedeutend: ein schrulliger Mechanismus, der es einer Handvoll Studierender und ein paar kontaktscheuen Kellerkindern ermöglichte, gegenseitig Homepages zu besuchen, die sich mit Wissenschaften, Haustieren oder Dichtkunst beschäftigten. Heute ist es die Plattform der Wahl für komplexe, interaktive Anwendungen (von E-Mail-Clients über Bildbearbeitungsprogramme bis hin zu Spielen) und ein Medium, um Hunderte Millionen interessierter Nutzer auf der ganzen Welt zu erreichen. Es ist auch ein unentbehrliches Werkzeug für die Geschäftswelt geworden, so wichtig, dass es sogar Ursache der Rezession 1999–2001 wurde, auch als Dot-Com-Blase bekannt.

Diese Entwicklung vom Unscheinbaren zum Allgegenwärtigen war erstaunlich schnell, selbst nach den Maßstäben, an die wir uns im heutigen Informationszeitalter gewöhnt haben. Diese Geschwindigkeit brachte ein unerwartetes Problem mit sich: Die Mängel in puncto Design und Implementierung im World Wide Web sind die einer Technologie, die niemals nach ihrer heutigen Bedeutung gestrebt hat und die niemals innehalten und einen Blick auf zurückliegende Fehler werfen konnte. Die sich daraus ergebenden Probleme sind schnell zu den wichtigsten und anhaltenden Bedrohungen der Datensicherheit geworden. Es zeigte sich, dass die Standards im Protokolldesign, die für eine schlichte Website mit tanzenden Hamstern ausreichen, nicht unbedingt dieselben sind wie für einen Online-Shop, der jedes Jahr Millionen von Kreditkartentransaktionen bearbeitet.

Wenn wir einen Blick auf das letzte Jahrzehnt werfen, ist es schwer, nicht ein wenig enttäuscht zu sein: Fast jede nennenswerte Online-Anwendung, die bis heute erfunden wurde, muss ihren Preis für die einfachen Lösungen aus den Anfangstagen des Web zahlen. So umfasste xssed.com – eine Website, die bestimmte Kategorien von Websicherheitslücken verfolgt – nach nur drei Jahren Betrieb bereits mehr als 50.000 Einträge. Trotzdem sind die Entwickler von Webbrowsern weitgehend unbeeindruckt, und die Sicherheits-Community bietet kaum Einblicke oder Ratschläge, wie mit diesem verbreiteten Problem umzugehen ist. Stattdessen erarbeiten viele Sicherheitsexperten weiterhin barock anmutende Klassifikationen von Schwachstellen und beklagen händeringend die möglichen Folgen dieses Durcheinanders.

Ein Teil des Problems besteht darin, dass diese Experten den Websicherheitsstandards lange abweisend gegenüberstanden und nicht erkannten, wozu sie eigentlich dienten. Schnell taten sie Mängel in der Websicherheit etwa als einfache Ausprägungen des »Confused-Deputy-Problems«[1] ab. Und warum sollten sie sich überhaupt um die Websicherheit kümmern? Was sind denn die Folgen eines obszönen Kommentars in einer langweiligen Website über Haustiere verglichen mit einer traditionellen Schwachstelle, die ein ganzes System lahmlegen kann?

Rückblickend denke ich, dass sich die meisten von uns auf die Zunge beißen. Das Web ist nicht nur viel bedeutender geworden als ursprünglich erwartet. Wir haben auch fundamentale Eigenschaften vernachlässigt, die es anders machen, als alles, mit dem wir vertraut und sicher umgehen. Denn selbst die bestentwickelten und bestgeprüften Webanwendungen haben viel häufiger und viel mehr Schwachstellen als ihre Gegenstücke außerhalb des Web.

Wir alle haben Mist gebaut, und es ist Zeit, zu bereuen. Um Buße zu tun, versucht *Tangled Web*, einen kleinen Schritt in Richtung einer dringend notwendigen Normalität zu gehen, und könnte damit die erste Publikation sein, die den aktuellen Stand der Sicherheit von Webanwendungen systematisch und gründlich untersucht. Dabei beleuchtet es die einzigartigen Herausforderungen bei der Sicherheit, denen wir – das heißt: Sicherheitsfachleute, Webentwickler und Anwender – jeden Tag begegnen.

Das Buch konzentriert sich in seinen Ausführungen auf die prominentesten und wichtigsten Bausteine moderner Browser, mit denen Nutzer und Entwickler täglich konfrontiert sind, und analysiert die damit verbundenen Sicherheitsrisiken und Probleme. Ich verwende diesen Ansatz, da er mir informativer und intuitiver erscheint, als einfach eine beliebig ausgewählte Klassifikation vorzustellen (was ich aus anderen Titeln zur Informationssicherheit kenne). Außerdem hoffe ich, dass dieser Ansatz *Tangled Web* zu einer angenehmeren Lektüre macht.

Für Leser, die nach schnellen Antworten suchen, habe ich am Ende der meisten Kapitel Spickzettel erstellt. Sie erläutern vernünftige Ansätze für viele der am häufigsten auftauchenden Probleme bei der Entwicklung von Webanwendungen. Zusätzlich enthält der letzte Teil dieses Buchs ein Glossar jener Schwachstellen, denen man bei der Implementierung am häufigsten begegnet.

---

1. Das »Confused-Deputy-Problem« ist ein grundlegendes Konzept in der Informationssicherheit, das sich auf eine breite Klasse von Design- oder Implementierungsmängeln bezieht. Der Begriff beschreibt jede Schwachstelle, die es dem Angreifer ermöglicht, ein Programm dazu zu bringen, eine gewisse »Autorität« (Zugangsprivilegien) zu missbrauchen, um eine Ressource auf unerwünschte Weise und normalerweise im Sinne des Angreifers zu verändern. Der Begriff »Confused Deputy« wird regelmäßig von Sicherheitsforschern aus dem Hochschulbereich verwendet. Da diese Beschreibung jedoch auf einem bestimmten Abstraktionsniveau auf beinahe alle Sicherheitsprobleme zutrifft, ist der Begriff quasi bedeutungslos.

Danksagungen

Viele Teile dieses Buchs haben ihren Ursprung in den Untersuchungen für das *Browser Security Handbook* von Google, einem technischen Wiki, das ich 2008 erstellt und unter einer Creative-Commons-Lizenz veröffentlicht habe. Sie können das Originaldokument online unter *http://code.google.com/p/browsersec/* einsehen.

Ich bin glücklich, bei einem Unternehmen zu arbeiten, das es mir ermöglicht hat, dieses Projekt zu betreiben, und hocherfreut, mit einer Reihe intelligenter Köpfe zusammenzuarbeiten, die das *Browser Security Handbook* noch nützlicher und genauer gemacht haben. Besonders möchte ich Filipe Almeida, Drew Hintz, Marius Schilder und Parisa Tabriz für ihre Unterstützung danken.

Ich bin stolz, auf den Schultern von Riesen zu stehen. Viel verdankt dieses Buch den Untersuchungen zur Browsersicherheit, die von den Mitgliedern der Informationssicherheits-Community angestellt wurden. Für die Fortschritte beim Verständnis dieses Gebiets möchte ich Adam Barth, Collin Jackson, Chris Evans, Jesse Ruderman, Billy Rios und Eduardo Vela Nava besonders danken.

Vielen Dank euch allen – macht weiter so!

Michal Zalewski