1 Einleitung

Willkommen zu »*Tagebuch eines Bughunters*«. Dieses Buch beschreibt den Lebenszyklus ausgewählter Softwareschwachstellen, die ich im Laufe der letzten Jahre gefunden habe. Jedes Kapitel erläutert dabei im Detail, wie ich die jeweilige Schwachstelle gefunden und anschließend ausgenutzt habe, sowie die durchgeführten Schritte zur Behebung der Schwachstelle seitens des Herstellers.

1.1 Ziele des Buches

Das primäre Ziel des Buches besteht darin, dich mit der Welt des Bughuntings vertraut zu machen. Nachdem du das Buch gelesen hast, solltest du ein besseres Verständnis davon haben, wie man vorgeht, um Softwareschwachstellen zu finden, wie man sie ausnutzt und anschließend erfolgreich behebt.

Das zweite Ziel des Buches ist eher etwas idealistisch. So möchte ich den einzelnen beschriebenen Schwachstellen eine Bühne geben und möglichst viele Leser an ihrem zuweilen durchaus interessanten, wenn auch kurzen »Leben« teilhaben lassen. Ich denke, das haben sie verdient :)

1.2 Wer sollte dieses Buch lesen?

Dieses Buch richtet sich an Security Researcher, Security Consultants, C/C++-Programmierer, Penetration Tester und jeden, der einfach mal in die interessante Welt des Bughuntings eintauchen möchte. Um dem Ganzen folgen zu können, empfiehlt es sich, dass du bereits gute Kenntnisse in der Programmiersprache C sowie in x86-Assembler mitbringst.

1.3 Haftungsausschluss

Wir leben heute leider in einer Zeit, in der man gut beraten ist, manche offensichtlichen Dinge nochmals ausdrücklich zu betonen. Auch auf die Gefahr hin, dich gleich zu Beginn des Buches zu langweilen, muss ich darauf hinweisen, dass das eigentliche Ziel dieses Buches darin besteht, darüber aufzuklären, wie man sich vor Schwachstellen in Software schützen kann. Um das dafür notwendige Bewusstsein zu schaffen, ist es erforderlich, dass du die jeweiligen Probleme und Auswirkungen kennst, die Softwareschwachstellen mit sich bringen. Denn nur, wenn man diese Aspekte verstanden hat, ist es möglich, sich zielgerichtet zu schützen oder Schwachstellen erst gar nicht auftreten zu lassen.

Aufgrund der momentanen Gesetzeslage in Deutschland, darf ich dir keine Angriffswerkzeuge (Exploits) zur Verfügung stellen. Um einen Missbrauch der innerhalb dieses Buches beschriebenen Inhalte zu vermeiden, werden daher weder funktionsfähige Angriffswerkzeuge beschrieben noch bereitgestellt. Die Schwachstellen und das sich daraus ergebende Risikopotenzial werden lediglich durch eine Kontrolle des Programmflusses verdeutlicht.

1.4 Weitere Informationen

Alle URLs, die im Laufe des Buches genannt werden, sowie alle Quellcodebeispiele und eventuelle Updates finden sich unter *http://www.trapkit.de/books/bhd/*.