HANSER

Vorwort

zu

„Web Hacking“

von Manuel Ziegler

ISBN (Buch): 978-3-446-44017-3
ISBN (E-Book): 978-3-446-44112-5

Weitere Informationen und Bestellungen unter
http://www.hanser-fachbuch.de/978-3-446-44017-3
sowie im Buchhandel

Vorwort

Hacker haben im Internet heute besonders leichtes Spiel. Das liegt auf der einen Seite an der Beschaffenheit des Internets und daran, dass der größte Teil der Kommunikation unverschlüsselt und so theoretisch für jedermann sichtbar abläuft. Auf der anderen Seite lassen die Sicherheitsvorkehrungen innerhalb von Webanwendungen häufig zu wünschen übrig. Woran das liegt, das lässt sich nur sehr schwer beurteilen, vermutlich ist das jedoch die Folge mehrerer Faktoren:

So wird häufig zu wenig Budget und zu wenig Zeit für die Entwicklung eines Webauftritts eingeplant, was dazu führt, dass Sicherheitslücken übersehen oder, um Deadlines einzuhalten, bewusst ignoriert werden. Häufig wird die Entwicklung von Webanwendungen auch Personal überlassen, das im Hinblick auf Sicherheit völlig ungeschult ist. Der Hauptgrund für die mangelnde Sicherheit von Webanwendungen dürfte jedoch darin liegen, dass sichere Authentifizierungsprozesse einer angeblich größeren Benutzerfreundlichkeit weichen müssen. So kommt es, dass Benutzern der Schutz ihrer Konten in der Regel selbst obliegt. Alleine die Stärke eines Passwortes entscheidet über die Sicherheit eines Nutzerkontos.

Guter Hacker, böser Hacker oder einfach nur Hacker?

Je nach Kontext ist der Begriff des Hackers positiv, bewundernd oder abwertend, negativ geprägt. Auch die Einteilung von Hackern in die Kategorien White-Hat-, Grey-Hat- und Black-Hat-Hacker löst die Frage danach, ob ein Hacker „gut“ oder „böse“ ist, nicht befriedigend, sondern teilt Hacker lediglich in Kategorien ein, die nicht zuletzt von vielen Hackern ständig gewechselt werden. Bei der Frage nach der Moral eines Hackers stellt sich die Frage, auf welcher Bemessungsgrundlage man diese Moral überhaupt bewerten kann. Inwiefern ist ein Hacker, der für eine Regierung arbeitet und Computerviren für Angriffe auf Atomkraftwerke entwickelt[1], besser als ein Hacker, der Menschen widerrechtlich um ihr Geld erleichtert? Und vor allem: Was ist mit den Hackern, die weder das eine, noch das andere machen? In welche der Kategorien ordnet man diese Hacker ein?

Über alle Hacker gleichermaßen zu urteilen, ist aus ethischer Sicht also ebenso undifferenziert wie die Einteilung dieser in die klassischen drei Kategorien. Ob ein Hacker gegen

[1] Der Computerwurm STUXNET, der im Jahr 2010 entdeckt wurde, diente vermutlich zur Sabotage des iranischen Atomprogramms und wurde wohl unter anderem von der US-amerikanischen und der israelischen Regierung entwickelt. STUXNET war darauf programmiert, gezielt Fehlfunktionen in Atomkraftwerken auszulösen. Dass es dabei zu Zwischenfällen kommen kann, die sich sowohl der Kontrolle des Personals, als auch der Kontrolle der Angreifer entziehen, war den Entwicklern von STUXNET wohl klar.

moralische Grundsätze verstößt, das lässt sich vermutlich nur durch eine Betrachtung des Einzelfalls beurteilen. Anders verhält es sich mit dem Gesetz. In vielen Staaten verstoßen Hacker sehr schnell gegen die Gesetze. Meiner Meinung nach zu schnell. Ein Hacker, der seine Fähigkeiten dazu nutzt, um Sicherheitslücken aufzudecken, und sich dabei weder bereichert, noch sonstigen Schaden verursacht, begeht meines Erachtens nach kein Verbrechen. Dennoch ist bereits das Testen von Webseiten auf Sicherheitslücken in vielen Fällen strafbar und kann im Falle einer Anzeige sogar mit Haftstrafen geahndet werden.

Nicht zuletzt wegen derartigen gesetzlichen Regelungen und einem verzerrten Bild des Hackers in der Öffentlichkeit werden Hacker häufig als Kriminelle wahrgenommen. Dabei setzen sich sehr viele Angehörige der Hacker-Szene für Freiheitsrechte (besonders im Internet) ein und distanzieren sich sehr deutlich von jeglicher Form von Verbrechen. Letztendlich muss jeder Hacker für sich selbst entscheiden, an welche Regeln er sich halten will. Es kann durchaus passieren, dass Ihnen jemand zehntausend Euro oder mehr dafür bietet, dass Sie eine bestimmte Person oder eine bestimmte Webseite angreifen oder ihm interne Informationen eines Unternehmens beschaffen. Solche Angebote können durchaus verlockend sein, sollten Sie jedoch ein derartiges Angebot annehmen, sind Sie in keiner Hinsicht besser als ein ordinärer Verbrecher.

Web Hacking - was ist das und wozu brauchen Sie das?

Web Hacking ist das Teilgebiet des Hackings, das sich mit Angriffen auf Webapplikationen und Webseiten beschäftigt. Dabei kommen insbesondere Methoden des High-Level-Hackings zum Einsatz, also desjenigen Hackings, das auf oberster Ebene der Softwareschicht stattfindet. Im Gegensatz zu Low-Level-Hacking Technologien, die sich mit Hardwarenahen Angriffen beschäftigen ist High-Level-Hacking recht leicht zu erlernen und erfordert kein besonders großes Hintergrundwissen. Im Wesentlichen stützt sich das Web Hacking auf logische Programmierfehler und Versäumnisse der Entwickler von Webseiten, also auf Fehler, die eigentlich durchaus vermieden werden könnten.

Dennoch sind viele Sicherheitslücken, die Sie sich beim Web Hacking zunutze machen im Internet sehr weit verbreitet und auch Sicherheitslücken, die keinen besonderen Bekanntheitsgrad besitzen oder die noch gar nicht entdeckt wurden, lassen sich mit einem gewissen Grundwissen schnell aufdecken und nutzen.

In diesem Buch lernen Sie die grundlegenden Konzepte des Web Hackings aus Sicht des Angreifers kennen. Ich glaube, dass man sichere Webseiten nur dann entwickeln kann, wenn man eine genaue Vorstellung davon hat, auf welche Art und Weise Sicherheitslücken entstehen und wie diese von Angreifern in der Praxis ausgenutzt werden können. Weiterhin glaube ich, dass es der Sicherheit einer Webseite oder -anwendung langfristig nicht nützt, wenn, ohne weiter darüber nachzudenken, gewisse Richtlinien eingehalten werden, von denen man sich verspricht, dadurch bekannte Angriffe zu verhindern.

Natürlich ist es der Sicherheit einer Seite zuträglich, Benutzereingaben stets zu validieren, das heißt jedoch noch lange nicht, dass man sich, wenn man alle Benutzereingaben validiert, keine Gedanken mehr um die Sicherheit eines Systems machen muss. Vor allem auf der konzeptionellen Ebene von Authentifikationssystemen schleichen sich oft Lücken in ein System ein, für deren Behebung es kein Patentrezept gibt. Deshalb ist es notwendig, die Sicherheit einer Webseite individuell zu beurteilen und diese dazu auch aus der Perspektive eines Angreifers zu betrachten.

Während Sie im ersten Kapitel dieses Buches die Folgen von Sicherheitslücken im Internet kennenlernen, werden Ihnen im zweiten Kapitel die absoluten Grundlagen des Webhackings näher gebracht. Sie lernen hier vor allem die Denkweise eines Hackers kennen, die in den nachfolgenden Kapiteln immer wieder deutlich wird.

Im dritten Kapitel geht es dann bereits ans Eingemachte: Passwörter mithilfe der Brute-Force-Methode zu knacken ist im Grunde nicht weiter schwierig, wenn einem ausreichend viel Zeit zur Verfügung steht. Deshalb steht in diesem Kapitel der Umgang mit der kombinatorischen Explosion im Vordergrund. Dabei verfolgen wir einerseits Ansätze, bei denen der Suchraum minimiert wird, also beispielsweise Wörterbuchattacken oder Attacken mit Teilalphabeten, andererseits setzen wir auf Parallelisierung, um den Aufwand auf mehrere Rechner oder Rechenkerne zu verteilen.

Auf Basis der Erkenntnisse aus Kapitel drei beschäftigen wir uns in Kapitel vier mit der Frage, wie ein System überhaupt sicher gestaltet werden kann. Wir betrachten unterschiedliche Authentifizierungskonzepte und unterschiedliche Ansätze der Datenspeicherung und untersuchen diese jeweils auf deren Sicherheit.

In Kapitel fünf lernen Sie das Konzept der SQL-Injection kennen. Diese Angriffsmethode erlaubt es Ihnen, auf nicht vorgesehenem Weg auf beinahe beliebige Daten in der Datenbank einer Webseite zuzugreifen. Sie lernen dabei auch, wie Sie sich als Webentwickler gegen SQL-Injection erfolgreich verteidigen können.

Cross-Site-Scripting ist eine Angriffsform, bei der Sie Ihren Schadcode direkt auf dem Client zur Ausführung bringen können. Während wir in Kapitel sechs die Verbreitung von Viren bewusst außen vor lassen, betrachten wir, wie Sie als Angreifer Sitzungskennungen von Nutzern einer Webseite entführen können, oder wie Sie gar Sitzungen von völlig fremden Webseiten durch das sogenannte Cross-Site-Tracing stehlen können. Natürlich lernen Sie auch, welche Vorkehrungen Sie als Webentwickler treffen können, um Cross-Site-Scripting auf Ihrer Seite zu unterbinden.

Eine in jüngster Zeit deutlich zunehmende Bedrohung im Internet sind sogenannte DoS beziehungsweise DDoS-Attacken. Diese behandeln wir in Kapitel sieben. Da Ihnen als Webentwickler außer einer Optimierung Ihrer Seite im Hinblick auf Performance kaum Möglichkeiten offen stehen, DoS-Attacken abzuwehren, werden hier vor allem Programmierstile betrachtet, mit denen Sie die Ausführungszeiten Ihrer Scripte deutlich senken können.

Auch wenn Phishing-Angriffe in der Regel nicht Sie als Webseiten-Betreiber, sondern Ihre Nutzer betreffen, können Sie Maßnahmen ergreifen, um Ihre Nutzer vor Identitätsdiebstahl und digitalen Raubüberfällen zu schützen. Wie, das erfahren Sie in Kapitel acht.

Auch wenn das Phishing dem Social Engineering sehr ähnlich ist, genaugenommen ist Phishing sogar ein Teilgebiet des Social Engineerings, werden diese beiden Themen in zwei getrennten Kapiteln behandelt. Der Grund: Social Engineering betrifft Sie als Betreiber wesentlich stärker als Phishing. Leider lassen sich gegen Social Engineering kaum technische Maßnahmen ergreifen; die Abwehr von Social Engineering fällt eher in den Bereich der Unternehmenssicherheit. In Kapitel neun erfahren Sie zumindest welche Gefahren bei einem Angriff durch einen Social Engineer auf Sie zukommen und alles was Sie sonst über Social Engineering wissen sollten.

Das zehnte Kapitel schließlich beschäftigt sich mit weiterführenden Themen, beispielsweise mit kryptografischen Verfahren, sicheren Protokollen, den Methoden von Geheimdiensten sowie ausgewählten Techniken des Low-Level-Hackings.

Fünf Exkurs-Kapitel vertiefen ausgewählte Themen des Buches, darunter Netzwerkprogrammierung, die grundlegende Funktionsweise eines Prozessors, sowie dynamische Datenstruktuen wie Bäume, Listen und Graphen.

Das Online-Angebot zum Buch

Erfolgreiches Hacking erfordert neben den theoretischen Grundlagen auch immer jede Menge Praxiserfahrungen. Diese sind aus verschiedenen Gründen in der Regel nicht besonders einfach zu erlangen. Auf der einen Seite ist es meist illegal, Techniken des Web-Hackings an fremden Webseiten auszuprobieren, auf der anderen Seite sind die meisten größeren Webseiten mittlerweile gegen die simpelsten Angriffe geschützt. Sie müssten also, um Praxiserfahrungen zu gewinnen, bei Angriffstechniken beginnen, die auf komplexeren Konzepten basieren und nicht leicht einzusehen sind. Das ist häufig eine Hürde, die Interessierten so sehr im Weg ist, dass diese es recht früh aufgeben, sich die Techniken des Hackings beizubringen.

Damit Sie bei Ihren ersten Gehversuchen nicht entmutigt werden, sondern nach und nach Erfahrungen zu Angriffen mit zunehmender Komplexität sammeln können, biete ich Ihnen an, viele der im Buch beschriebenen Angriffe innerhalb eines speziell dafür eingerichteten Playgrounds zu erproben. Der Playground besteht aus unterschiedlichen Szenarien, die jeweils eine Webseite repräsentieren, die ganz bestimmte, im jeweiligen Kontext zu trainierende Angriffe ermöglichen. Zusätzlich enthalten einige der Szenarien Hinweise, die Sie dabei unterstützen sollen, die jeweilige Schwachstelle zu finden.

Die Szenarien sind zusätzlich in 10 verschiedene Schwierigkeitsstufen gruppiert, wobei die erste Stufe in der Regel ohne größere Kenntnisse zu bewältigen ist und Sie die zehnte Schwierigkeitsstufe vor lösbare, aber sehr komplexe Probleme stellt. Für das Lösen eines Szenarios erhalten Sie eine bestimmte Anzahl von Punkten, die jeweils von der Schwierigkeitsstufe des Angriffs abhängt. Damit ist es Ihnen möglich, sich mit anderen Nutzern des Playgrounds zu vergleichen. In der Regel werden Ihre Punkte und Ihr Nutzername nicht veröffentlicht, falls Sie das wünschen, können Sie sich jedoch in einer Bestenliste auflisten lassen.

Im Buch wird in der Regel mithilfe einer Infobox darauf hingewiesen, wenn es zu einem Kapitel entsprechende Übungsszenarien im Playground gibt. Bitte beachten Sie, dass ich aus naheliegenden Gründen keine Infrastruktur für das Testen von DoS-Attacken bereitstellen kann. Sie finden im Playground ein entsprechendes Simulationsprogramm, mit dem Sie eine DoS-Attacke simulieren können.

Playground

Sie finden den Playground zum Buch unter der Web-Adresse *hackers-playground.de*. Bitte beachten Sie unbedingt die dort angezeigten Nutzungshinweise. Insbesondere übernehme ich keinerlei Haftung für eventuell entstehende Schäden auf Ihrem Rechner. Wenn Sie eine Seite des Playgrounds besuchen, die von

Angreifern zur Verbreitung von Schadcode missbraucht werden könnte, werden Sie noch einmal gesondert auf die erhöhte Gefahr beim Besuch dieser Seite hingewiesen. In jedem Fall sollten Sie jedoch einen aktuellen Browser verwenden und unter Umständen die Ausführung von Javascript-Code deaktivieren, wenn Sie eine solche Seite besuchen.

Neben dem Playground zum Buch, auf dem Sie Ihre neu gewonnen Fertigkeiten erproben können, gibt es auch eine Buch-Webseite, auf der Sie weiterführende Informationen zu bestimmten Angriffen sowie zahlreiche hilfreiche Programme für den Alltag als Hacker finden. Außerdem werden Sie auf dieser Seite durch regelmäßig erscheinende Artikel über neue Entwicklungen und aktuelle Themen aus dem Bereich des Web-Hackings informiert.

Auf die zusätzlichen Informationen zu einem bestimmten Thema, die Sie auf der Buch-Webseite finden, werden Sie im Buch ebenfalls mittels einer Infobox hingewiesen. Bitte beachten Sie, dass Sie die Informationen und Programme, die Sie auf dieser Seite finden, zwar kostenlos verwenden dürfen, die Weiterverbreitung oder die Nutzung zu bestimmten Zwecken in einigen Fällen aber durch das Urherberrecht sowie die Lizenzbestimmungen eingeschränkt sein kann. Insbesondere die Nutzung der dort bereitgestellten Software zum Zwecke der Kompromittierung fremder Internetseiten ist nicht gestattet!

Weblink

Auf der Webseite zum Buch unter der Adresse *webhacking.de* finden Sie:

- alle PHP- und C/C++-Listings aus dem Buch
- aktuelle Informationen
- viele Zusatzmaterialien

Danksagungen

Ich danke dem Carl Hanser Verlag mit all seinen Mitarbeitern für die stets freundliche und vor allem erfreuliche Zusammenarbeit. Im Zusammenhang mit diesem Buch möchte ich mich ganz besonders bei meiner Lektorin Sieglinde Schärl bedanken, die schon vor zwei Jahren einen ersten Denkanstoß zu diesem Buch bei mir auslöste. Weiterhin bedanke ich mich bei Frau Gottmann, die meine Fehler im Umgang mit der deutschen Sprache beseitigte und meine Ausdrucksweise an einigen Stellen etwas mäßigte, sowie bei Frau Weilhart, die für die Produktion des Buches zuständig ist.

Auch bei Frau Rothe möchte ich mich für die äußerst angenehme Zusammenarbeit im Vorfeld der Veröffentlichung bedanken. Natürlich danke ich auch allen anderen Mitarbeitern des Carl Hanser Verlags, die still zum Gelingen dieses Buches beigetragen haben. Besonders hervorheben möchte ich hier noch das Engagement von Herrn Gerhardy, der mich vor allem bei technischen Problemen bereitwillig unterstützt hat.

Besonderen Dank möchte ich auch Anna aussprechen, die mich in meinem Vorhaben, dieses Buch zu schreiben, immer wieder bekräftigt und ermuntert hat.