Methoden und Techniken bei Web-Anwendungen

In diesem Dokument wird beschrieben, welche Techniken und Methoden itforensik.com bei einem Penetrationstest gegen Web-Anwendungen anwendet.

Bei unseren Sicherheitstests orientieren wir uns an den Standards des Open-Source-Security-Testing-Methodology-Manuals (OSSTMM) und des Open-Web-Application-Security-Projects (OWASP). Das OSSTMM ist ein auf vielen Erfahrungen basierendes Modell, wie Sicherheitsüberprüfungen und Bewertungen nachvollziehbar, effizient und umfassend durchzuführen sind. OWASP wurde speziell für Web-Anwendungen entwickelt. Dessen Ziel ist das Aufspüren und das Bekämpfen der Ursachen von unsicheren Anwendungen.

Beide Standards sind unabhängig und speziell für Sicherheitstests geschaffen worden. Sie werden ständig weiter entwickelt, um den aktuellen Anforderungen gerecht zu werden.

Bei Penetrationstests gegen internetbasierte Anwendungen führen wir simulierte Angriffe durch, die sich in folgende Bereiche einteilen lassen:

Authentisierung

auch Authentifizierung.
Die wahre Identität eines Benutzers wird anhand eines bestimmten Merkmals überprüft.
Der Unterschied zur Identifizierung ist, dass bei der Identifizierung nur überprüft wird, ob ein bestimmter Benutzer an einer Transaktion beteiligt ist. Bei der Authentisierung wird auch überprüft, ob der Benutzer tatsächlich der ist, als der er sich ausgibt.
Folgende Möglichkeiten der Authentifizierung werden überprüft: Basic and Digest, NTLM, Authentifizierung auf Forms basierend, MS Passport usw.

Autorisierung

Es wird überprüft, ob der Benutzer zu einer bestimmten Aktion berechtigt ist.
Es gibt drei Möglichkeiten, um zu erweiterten Rechten zu gelangen:

Horizontale Privilegien-Eskalation:
Es kann z.B. möglich sein, mit einer anderen Benutzerkennung einen fremden Account zu übernehmen. Bei dieser Methode werden Daten auf Benutzerebene angegriffen. Der Zugriff auf Systemdaten sollte so nicht möglich sein.

Vertikale Privilegien-Eskalation:
Es wird überprüft, wie sich ein Benutzer erweiterte Rechte verschaffen kann. Denkbar wäre z.B. eine Eskalation der Rechte durch eine Schwachstelle im Session-Management oder das Erraten des Administratorpasswortes.

Willkürlicher Dateizugriff:
Generell liegen Systemdateien außerhalb des Zugriffs von Benutzern einer Online-Anwendung. Verschiedene Angriffe auf Eingabewerte und die Fehlkonfiguration eines Servers können den Zugriff auf diese Dateien ermöglichen. Ein Ausbruch aus dem Web-Root-Verzeichnis fällt in diese Kategorie.

EXPERsT your IT

Session-State-Management

Das HTTP-Protokoll legt keine eindeutige Vorgehensweise fest, wie der Status einer Verbindung gespeichert werden soll. Da HTTP für sich ein zustandsloses Protokoll ist, sind verschiedene Möglichkeiten vorhanden, wie Informationen aufgezeichnet werden können. Das HTTP-Protokoll wurde entwickelt, um bestimmte Webseiten auf den lokalen Computer zu laden.
Es ist z.B. nicht festgelegt, wie der Inhalt eines Warenkorbs behandelt werden soll.
In den Bereich des Session-State-Managements fallen Angriffe auf Header und Cookies, versteckte Felder, URLs usw.

Angriffe auf die Benutzereingaben

Bei dieser Art von Angriffen werden Daten eingeschleust, die die Anwendung nicht erwartet. Normalerweise überprüft ein Programm auf Richtigkeit und Plausibilität der Benutzereingaben. Dies ist notwendig, um die Anwendung vor unerlaubten Datenmanipluationen und den Server vor einem Absturz zu schützen.
Typischerweise gibt es drei Kategorien, wie man über Eingaben Sicherheitslücken ausnutzen kann:

Unerwartete Eingabe:
Dies beinhaltet Befehle, die in der Datenbanksprache SQL abgesetzt werden, Cross-Site-Scripting-Befehle (auch XSS), die Passwörter ausspionieren, und die Eingabe eines jeden Zeichens, das Fehlermeldungen hervorruft.

Besondere Zeichen, durch die ein Befehl ausgeführt wird:
Dies könnten betriebssystemspezifische Zeichen sein, um einen Befehl z.B. auf der Shell auszuführen. Oder man könnte eine Web-Anwendung durch das Einschleusen von SQL-Befehlen, JavaScript oder ASP-Code zu unerlaubten Reaktionen veranlassen.

Buffer-Overflow:
Die Ausführung von Pufferüberläufen ist eines der einfachsten Angriffe, vorausgesetzt, der Überlauf ist bereits an die Plattform und das Betriebssystem angepasst. Durch eine ausgeklügelte Wahl der Eingabe kann so z.B. die Rücksprungadresse überschrieben und fremder Code eingeschleust werden.

Web-Datenspeicher

Die Spannweite von Informationen, die Web-Seiten anbieten, reicht von Produktkatalogen über Online-Shops bis zu Finanztransaktionen in Echtzeit. Die Daten, die hinter einer Anwendung liegen, können unter Umständen ausgelesen, verändert oder gelöscht werden. So könnte ein Kreditkartendiebstahl durchgeführt oder der Preis eines Produkts herabgesetzt werden, um anschließend große Mengen zu ordern. Ein sehr bekannter Vertreter dieser Angriffsart ist SQL-Injection.

Web-Services

Microsoft definierte eine Unterscheidung zwischen Web-Services und den schon lange gebräuchlichen Web-Seiten folgendermaßen: „Im Gegensatz zu Web-Seiten, Browser basierten Transaktionen und plattformabhängigen Technologien sind Web-Services Dienste, die direkt zwischen Computer und Computer agieren. Dazu werden bestimmte Datenformate und Protokolle in einer betriebssystemunabhängigen Sprache verwendet.“
SOAP (Simple Object Access Protocol) ist so ein Protokoll, mit dessen Hilfe Daten zwischen Systemen ausgetauscht und RPC-Calls ausgeführt werden könnnen. Diese Dienste können natürlich auch direkt angegriffen werden.

Web-Application-Management

Viele Web-Anwendungen bieten für den Administrator eine große Zahl von Möglichkeiten, diese zu kontrollieren, sie zu konfigurieren und deren Inhalte zu pflegen.
Oft sind diese Zugänge auch über das Internet möglich, da die Fernwartung eine immer größere Bedeutung erlangt.
Folgende Angriffe sind möglich:

- Angriffe über die Administration des Web-Servers
- Angriffe über das Content-Management
- Internetbasiertes Netzwerk und System-Management

Das Ausnutzen von Buffer-Overflows in Management-Tools fällt ebenfalls in diesen Bereich.

Client der Web-Anwendung

Viele Web-Anwendungen verlassen sich oft auf die Sicherheit und Fehlerfreiheit des Clients.
Ob nun ein Angriff über einen Webbrowser des Kunden erfolgt oder über die E-Commerce-Site direkt, ist für den Kunden gleich dramatisch.
Umsatzverluste durch Angriffe auf Client-Seite sind ebenso existent wie Angriffe direkt auf den Server.
Der Client ist eng mit der Anwendung verwoben und deren Sicherheit ist integraler Bestandteil der ganzen Anwendungssicherheit.
Drei Kategorien sind hier maßgebend:

- Anriffe über aktive Inhalte
- Cross-Site-Scripting
- Manipulationen der Cookies

Rupert-Gugg-Str. 53 • A-5280 Braunau • Tel.: +43 / 77 22 / 98 200 • mobil: +43 / 699 / 18 19 94 63 • Christian.Perst@itEXPERsT.at