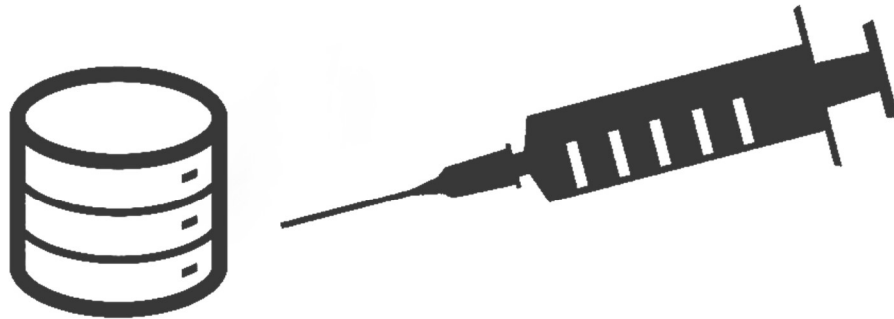


M214 Benutzer/innen im Umgang mit Informatikmitteln instruieren

SQL Injection Burp Suite

Flavio Imhof, Valentino Panico, Yannis Greminger



SQL Injection

Anleitung
18.12.2021

Dokumentgeschichte

Version	Datum	Beschreibung	Geprüft durch
1.0	6.12.2021	Initialversion	YG
1.1	13.12.2021	Ergänzung Einleitung	FI
1.2	18.12.2021	Glossar	VP
1.3	19.12.2021	Abschlussarbeiten	FI, VP, YG

Inhalt

Einleitung.....	2
Was ist eine SQL Injection?	2
Was muss beachtet werden?	2
Was sind mögliche Konsequenzen?	2
Anleitung	3
Vorbereitung	3
Ziel	3
Ausführung	4
Glossar	5



Einleitung

Was ist eine SQL Injection?

Unter einer SQL-Injection versteht man das Ausnutzen einer Sicherheitslücke in relationalen Datenbanksystemen, die bei der Dateneingabe auf die Sprache SQL zurückgreifen. Der Angreifer macht sich dabei solche Benutzereingaben in die Datenbank-Oberflächen zunutze, die nicht ausreichend maskiert sind und Metazeichen wie den doppelten Bindestrich, Anführungszeichen, das Quote-Zeichen oder das Semikolon enthalten. Diese Zeichen besitzen Sonderfunktionen für den SQL-Interpreter und erlauben die externe Beeinflussung der ausgeführten Befehle. Oft tritt eine SQL-Injection in Zusammenhang mit PHP- und ASP-Programmen auf, die auf ältere Interfaces zurückgreifen. Hier erhalten die Eingaben in einigen Fällen nicht die notwendige Maskierung und sind damit das perfekte Ziel für einen Angriff.

Mit dem gezielten Einsatz von Funktionszeichen schleust ein unberechtigter Benutzer auf diese Weise weitere SQL-Befehle ein und manipuliert die Einträge derart, dass er Daten verändern, löschen oder lesen kann. In gravierenden Fällen ist es sogar möglich, dass sich ein Angreifer auf diesem Wege den Zugriff auf die Kommandozeile des befehlsausführenden Systems und damit über den gesamten Datenbankserver verschafft.

Was muss beachtet werden?

Bei allerlei Eingriffen auf nicht eigenes geistliches Eigentum besteht die Gefahr etwas zu beschädigen das so nicht gedacht war/ist. Dabei nimmt man einen Eingriff vor, welcher einem Einbruch gleichkommt. Da entweder vertrauliche Daten gelöscht oder bearbeitet werden besteht auch bei wichtigen Datenbanken die Gefahr notwendige Daten zu löschen welche dann einen großen Schaden anrichten.

Was sind mögliche Konsequenzen?

Je nach Schwere des Verbrechens/Angriffs wird eine Geldstrafe oder Freiheitsstrafe bis zu 3 Jahren. Dies ist teils auch nicht so einfach zu definieren da auch solche Angriffe teils von Unternehmen aktiv gewünscht werden.



Anleitung

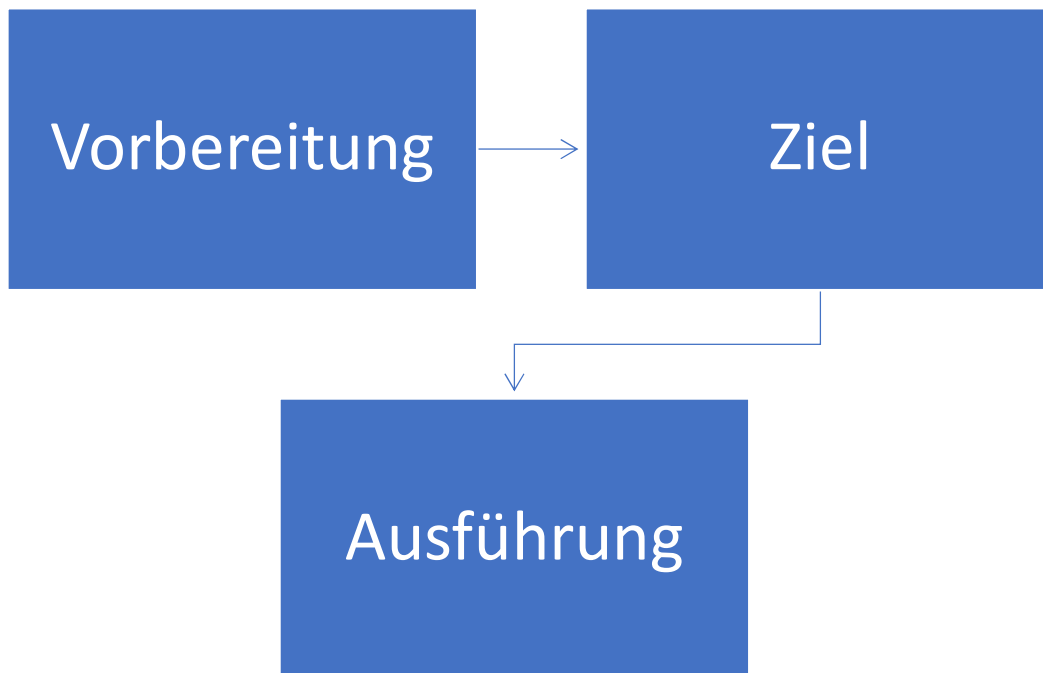


Abbildung 1: Ablauf

Vorbereitung

Um eine SQL Injection zu starten, empfiehlt es sich ein Betriebssystem wie Kali Linux oder Parrot OS zu nutzen. In unserem Fall werden wir es mit einer Kali Linux Maschine machen. Kali ist sehr praktisch da es schon alles installiert hat, dass man braucht. Natürlich braucht man auch ein Target, das man angreifen möchte. Dafür nutzen wir eine „Web application security learning platform“ namens „Bricks“. Diese kann unter diesem Link heruntergeladen werden: <https://sechow.com/bricks/download.html>. Ist alles installiert und die Datenbank bereit, kann die „Attacke“ beginnen.

Ziel

Das Ziel unserer Injection ist, dass wir ein erfolgreiches Login bekommen, ohne dass wir die Login Daten kennen.

Ausführung



Abbildung 2: Kali Linux Terminal Eingabe

Im Terminal zum
starten der Software
„burpsuite“ eingeben
und danach durch die
Fenster durchklicken

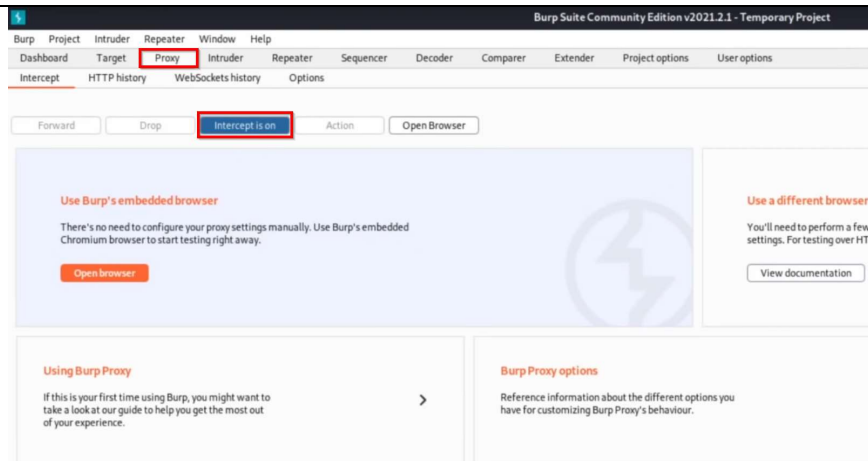


Abbildung 3: BurpSuite Proxy Tab

Nach der Installation von „burpsuite“ muss unter dem Reiter Proxy kontrolliert werden ob „Intercept is on“ aktiviert ist, damit sämtliche Anfragen abgefangen werden können.

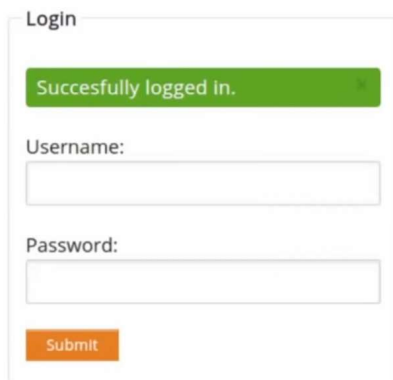


Abbildung 4: Bricks Anmeldefenster

Einfügen von Daten in eine Anmeldemaske



Abbildung 5: abgefangener Beitrag von Burp Suite

Darauf fängt Burp Suite diese abfrage automatisch ab. Dieser Abgefangener Post kann darauf weiterverwendet werden, um mit SQL Map herauszufinden, ob die Webseite verwundbar ist

Glossar

Begriff	Definition Erklärung
SQL	Structured Query Language, wird dazu genutzt, um Datenbankstrukturen zu erstellen, abzufragen, zu verwalten und zu bearbeiten
Sicherheitslücke	Im Code enthaltene Fehler, nicht bedachte Risiken und nicht verschlüsseln von Passwörtern
Relationale Datenbank	Ist ein Typ von Datenbank, welche die Speicherung und den Zugriff auf miteinander Verbundene Datenpunkte ermöglicht
Metazeichen	Sind Zeichen in einer Datei oder Zeichenkette, die innerhalb eines bestimmten Kontextes nicht für sich selbst stehen, sondern ähnlich wie Steuerzeichen eine besondere Bedeutung für die Verarbeitung der Daten haben.
SQL-Interpreter	Versteht den Syntax so dass die Datenbank angezeigt wird
PHP	ist eine Skriptsprache mit einer an C und Perl angelehnten Syntax, die hauptsächlich zur Erstellung dynamischer Webseiten oder Webanwendungen verwendet wird.
ASP	ASP.NET ist ein Web Application Framework von Microsoft, mit dem sich dynamische Webseiten, Webanwendungen und Webservices entwickeln lassen. ASP.NET ist Nachfolger von Active Server Pages und erschien 2002 in der ersten Version. ASP.NET ist Teil des klassischen .NET Frameworks bis zur aktuellen Version 4.8.
Web application security learning platform	In unserem Fall ist das "Bricks". Es ist ein Open-Source Projekt, dass zum Lernen von Sicherheit in Webapplikationen dient.
Burp Suite	Burp Suite ist ein Programm das HTTP Anfragen abfängt. Damit können Sicherheitslücken auf Webseiten gefunden und behoben werden.
Proxy	Schaltet sich zwischen Client und Server, und ist eine Kommunikationsschnittstelle. Nimmt anfragen an und sendet dies emit seiner IP-Adresse weiter.
Intercept	Englisch für Abfangen. Mit dieser Option werden die Anfragen in Burp Suite abgefangen.

Abbildungsverzeichnis

Abbildung 1: Ablauf	3
Abbildung 2: Kali Linux Terminal Eingabe	4
Abbildung 3: BurpSuite Proxy Tab.....	4
Abbildung 4: Bricks Anmeldefenster	4
Abbildung 5: abgefangener Beitrag von Burp Suite	4

