

## Giftspritze

Hintergrund 06.01.2004 20:00 Uhr – Daniel Bachfeld

**SQL-Injection bezeichnet das Einschleusen von eigenen Befehlen in eine SQL-Datenbank. Überprüft eine Web-Applikation Benutzereingaben nicht ausreichend, ist damit jede Datenbank auf jedem Betriebssystem verwundbar.**

### INHALTSVERZEICHNIS

1. Giftspritze

2. Kung Fu

3. Besser Coden

» [Auf einer Seite lesen](#)

Webshops, News-Boards, Groupware- und Content-Management-Systeme setzen Datenbanken ein, um darin Kundendaten, Artikel und Texte abzulegen. Oft trifft der Besucher solch einer Seite auf Kombinationen von Windows-2000-Server, IIS, MS-SQL-Server und Active Server Pages oder Linux zusammen mit Apache, MySQL und PHP oder Perl.

In Webformularen können Benutzer Informationen eingeben, um Bestellungen einzugeben oder sich als Kunde zu registrieren. Aus diesen Angaben erzeugt die Web-Applikation dynamische Datenbankabfragen. Überprüft die Applikation die Eingabe nicht oder fehlerhaft, ist es möglich, spezielle Zeichenketten einzuschleusen. Mit geschickt gewählten Eingaben kann ein Angreifer dann eigene Parameter und Befehle an die Datenbank übergeben und auf deren Inhalte und sogar das System zugreifen.

### Dienste

[Security Consultant](#)

[Emailcheck](#)

[Netzwerkcheck](#)

[Browsercheck](#)

[Anti-Virus](#)

[Krypto-Kampagne](#)

Anzeige

### Alerts!

[alle Alert-Meldungen »](#)

 **Grub2 BootHole**

 **Magento Commerce 2 / Open Source 2 (alle Plattformen)**

 **Cisco-Produkte**

 **WordPress wpDiscuz**

### Online-Konferenz: IT-Sicherheitstag



## Linguistik

Um Daten in eine SQL-Datenbank zu schreiben oder daraus zu lesen, kommuniziert eine Applikation mit der Datenbank über die Befehlssprache SQL (Structured Query Language). In der Regel übergibt sie einen kompletten String, den sie vorher aus Befehlen und Benutzereingaben zusammengefügt hat. Da es eine Vielzahl von SQL-Datenbank-Lösungen gibt, die teilweise eigene Funktionen unterstützen, ist der SQL-Befehlsumfang mittlerweile recht groß. Eine Schnittmenge von Befehlen, wie etwa Befehle SELECT, UPDATE, DELETE, INSERT, DROP und WHERE, verstehen aber alle. SQL-Datenbanken können mehrere Datenbanken mit jeweils mehreren Tabellen enthalten, die wiederum aus mehreren Spalten bestehen.

## Ungefiltert

Mit dem SQL-Befehl

```
SELECT * FROM kunde WHERE card = 'visa'
```

liefert eine Datenbank alle Datensätze der Tabelle *kunde* zurück, die in der Spalte *card* den Wert *visa* abgelegt haben. Ersetzt man die konstante Zeichenkette *visa* durch eine Variable *\$card*, so sind in Verbindung mit einer Benutzereingabe verschiedene Zeichenketten möglich:

```
SELECT * FROM kunde WHERE card = '$card'
```

Solange in der Variablen Werte wie *visa*, *amex* oder *master* stehen, reagiert die Datenbank wie erwartet. Gibt ein böswilliger Benutzer jedoch die Zeichenkette `';DROP TABLE KUNDE--` ein, schickt die Applikation folgendes an die Datenbank:

```
SELECT * FROM kunde WHERE card = ''';DROP TABLE KUNDE--'
```

Da das Semikolon ein Trennzeichen darstellt, sieht die Datenbank zwei Befehle:



## Neue Cyberangriffe - Wie können Unternehmen sich schützen - Kritische Infrastrukturen & Industrie 4.0 im Fokus

Der IT-Sicherheitstag findet dieses Jahr zum ersten Mal online statt und ist eine Mischung aus Konferenz und Plattform zum Erfahrungsaustausch und Netzwerken. Neben der Notwendigkeit von Cyberabwehrmaßnahmen werden auch verschiedene Konzepte und Vorgehensweisen zur Sicherung der unternehmensinternen IT- und Prozessnetze dargelegt.

### Anzeige

Sind Ihre Filialen Einfallstore für Cyberangriffe?  
Wie Corona die Zukunft der Arbeit gestaltet  
Corona & Phishing: Bieten Sie Hackern die Stirn!  
Zero Trust: Null Vertrauen, aber voll zufrieden  
Container- und Serverless-Umgebungen absichern  
Risk-based Vulnerability Management – jetzt!  
SAP Cloud Platform: Merkmale und Fallbeispiele  
Wie KI den Alltag von Netzwerkadmins erleichtert  
So schützen Sie Ihre Mitarbeiter überall!  
Zeit zu handeln: Jetzt auf S/4HANA umsteigen

```
SELECT * FROM kunde WHERE card = ''
```

zeigt alle Datensätze deren Spalte *card* leer ist. Anschließend führt die Datenbank den zweiten Befehl aus, der die Tabelle *kunde* komplett löscht.

```
DROP TABLE KUNDE--'
```

Die zwei Bindestriche kennzeichnen den Anfang eines Kommentars, weshalb auch das letzte Hochkomma (Quote) ignoriert wird, statt einen Fehler hervorzurufen. In diesem Beispiel kann ein Angreifer ohne vorherige Authentifizierung ganze Tabellen von der Festplatten wischen. Allerdings muss die Web-Applikation die erforderlichen Zugriffsrechte besitzt. Beim Anlegen des entsprechenden Datenbanknutzers muss der Datenbank-Administrator das Löschen mittels DROP erlauben.

Das grundlegende Problem bei SQL-Injection ist die fehlende Filterung der Eingaben auf mögliche Quotes. Viele Applikationen setzen einen SQL-Befehl aus Stringelementen zusammen, die von Hochkommas eingerahmt werden müssen. Unter Java sieht das dann so aus:

```
String sql = new String("SELECT * FROM kunden WHERE  
card= '' + request.getParameter("cardname") ''")
```

Java expandiert die Eingabe *cardname* und fügt sie dem feststehenden String hinzu. Mögliche Quotes in *cardname* bleiben erhalten, erscheinen nun aber in einem anderem Kontext. Der ursprünglichen Befehl kann um weitere Befehle ergänzt werden.

Vorherige

1

2

3

Nächste

TEILE DIESEN BEITRAG



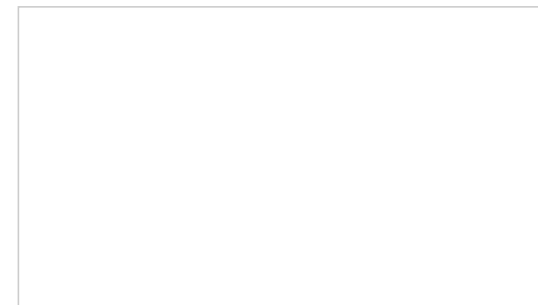
## Artikel



### Microsoft und Emotet: Makroschutz in Office 365 nur für Konzerne

Angeblich kann man das Ausführen der gefährlichen Emotet-Makros mit Gruppenrichtlinien firmenweit abschalten. Doch dieser Schutz hat riesige Löcher, die nur den wenigsten bekannt sind.

Hintergrund 52



### Best of Backdoor-Fails

Hintertüren in Hard- und Software haben fast immer auch Nebenwirkungen - manchmal sogar spektakuläre.

Hintergrund 156



<https://heise.de/-270382>

Drucken

Anzeige

## Rückblick: Die größten Hacks der vergangenen 10 Jahre

Von Stuxnet über Heartbleed bis zum Yahoo-Hack: Das haben Hacker von 2010 bis 2019 "geleistet".


Lesetipp

### Neueste Forenbeiträge

#### Re: Lock Error "Error 5: Zugriff verweigert"

Googeln nach <windows ereignis 225> liefert u.a. in einem Treffer eine anschauliche Anleitung, um den Verursacher zu finden, der das Auswerfen...


Forum: Desinfect

 von Kybfels; vor 48 Minuten

#### Features der 64bit- Desinfect-Software für 32bit - Systeme

Hallo allerseits, es gibt in der Praxis viele 32bit-Systeme, u.a. auch durch die 10Zoll-Mini-Laptop-Klasse. Kann man nicht die 32bit- Version...

Forum: Desinfect

 von desinfektanwender; vor 7 Stunden

**Re: Desinfect installation auf SSD (mit Schreibzugriff)?**

Ja schon klar aber die Frage war ja nicht ob der Stick beschreibbar ist sondern ob man die SSD schreibbar machen könnte. Das das nicht...

Forum: Desinfect



von BR0KK; vor 8 Stunden

NEWS UND ARTIKEL

News  
7-Tage-News  
News-Archiv  
Hintergrund-Artikel  
Alert-Meldungen

SERVICE

Newsletter  
Tools  
Foren  
RSS  
mobil

DIENSTE

Security Consulter  
Netzwerkcheck  
Anti-Virus  
Emailcheck  
Browsercheck  
Krypto-Kampagne