Keller Ruben

DVWA Dokumentation

Contents

[1. Grundlagen 2](#_Toc188004119)

[2. Brute Force 2](#_Toc188004120)

[3. Command Injection 3](#_Toc188004121)

[4. CSRF 3](#_Toc188004122)

[5. File Inclusion 3](#_Toc188004123)

[6. File Upload 3](#_Toc188004124)

[7. Insecure CAPTCHA 3](#_Toc188004125)

[8. SQL Injection 3](#_Toc188004126)

[9. SQL Injection (Blind) 3](#_Toc188004127)

[10. Weak Session Ids 4](#_Toc188004128)

[11. XSS (DOM) 4](#_Toc188004129)

[12. XSS (Reflected) 4](#_Toc188004130)

[13. XSS (Stored) 4](#_Toc188004131)

[14. CSP Bypass 4](#_Toc188004132)

[15. JavaScript 4](#_Toc188004133)

[16. Authorisation Bypass 4](#_Toc188004134)

[17. Open HTTP Redirect 4](#_Toc188004135)

# Grundlagen

Benutzername: admin

Passwort: password

Die Damn Vulnerable Web Application (DVWA) ist eine absichtlich unsichere Webanwendung, die für Schulungszwecke und das Testen von Sicherheitstools entwickelt wurde. Sie bietet verschiedene Sicherheitsstufen, um Benutzer in den Grundlagen von Webanwendungssicherheit und Angriffstechniken zu schulen. DVWA dient als Übungsumgebung für Ethische Hacker, Entwickler und Sicherheitsexperten, um in einer kontrollierten Umgebung Schwachstellen zu verstehen und zu beheben.

Ein Bild, das Grafiken, Schrift, Text, Logo enthält.

Automatisch generierte Beschreibung

# Brute Force

Information  
Ein Brute-Force-Angriff ist eine Methode, bei der ein Angreifer systematisch alle möglichen Kombinationen von Werten, wie Passwörter oder Verzeichnisnamen, ausprobiert, um unbefugten Zugang zu einem System zu erlangen oder versteckte Inhalte zu entdecken. Dies kann mit Tools wie DirBuster oder WebRoot durchgeführt werden, die Anfragen automatisieren und Serverantworten analysieren, um gültige Einträge zu finden. Der Angriff ist besonders effektiv, wenn Sicherheitsmaßnahmen wie Konto-Sperrrichtlinien oder Anforderungen an die Passwortkomplexität schwach oder nicht vorhanden sind. Gegenmaßnahmen umfassen Werkzeuge, die Scanning-Aktivitäten erkennen, oder strengere Sicherheitskontrollen, um Schwachstellen zu reduzieren.  
Quelle: <https://owasp.org/www-community/attacks/Brute_force_attack>

Ein Brute-Force-Angriff auf ein Webformular ist eine Methode, bei der ein Angreifer systematisch verschiedene Kombinationen von Benutzernamen und Passwörtern ausprobiert, um unautorisierten Zugriff zu erlangen. Tools wie THC-Hydra und Burp Suite können verwendet werden, um solche Angriffe zu automatisieren, indem sie Anfragen an den Server senden und die Antworten analysieren. Voraussetzung dafür sind eine Wortliste und die richtigen Parameter des Ziel-Webformulars, wie die Felder für Benutzername und Passwort sowie die Fehlermeldung bei falscher Eingabe. Solche Angriffe sollten nur in kontrollierten Umgebungen und mit Genehmigung durchgeführt werden, da sie andernfalls illegal sind.

Quelle: <https://www.golinuxcloud.com/brute-force-attack-web-forms>

Visuelles Beispiel



Code-Beispiel (pro und contra) courier new code

<?php

if( isset( $\_GET[ 'Login' ] ) ) {

// Get username

$user = $\_GET[ 'username' ];

// Get password

$pass = $\_GET[ 'password' ];

$pass = md5( $pass );

// Check the database

$query = "SELECT \* FROM `users` WHERE user = '$user' AND password = '$pass';";

$result = mysqli\_query($GLOBALS["\_\_\_mysqli\_ston"], $query ) or die( '<pre>' . ((is\_object($GLOBALS["\_\_\_mysqli\_ston"])) ? mysqli\_error($GLOBALS["\_\_\_mysqli\_ston"]) : (($\_\_\_mysqli\_res = mysqli\_connect\_error()) ? $\_\_\_mysqli\_res : false)) . '</pre>' );

if( $result && mysqli\_num\_rows( $result ) == 1 ) {

// Get users details

$row = mysqli\_fetch\_assoc( $result );

$avatar = $row["avatar"];

// Login successful

echo "<p>Welcome to the password protected area {$user}</p>";

echo "<img src=\"{$avatar}\" />";

}

else {

// Login failed

echo "<pre><br />Username and/or password incorrect.</pre>";

}

((is\_null($\_\_\_mysqli\_res = mysqli\_close($GLOBALS["\_\_\_mysqli\_ston"]))) ? false : $\_\_\_mysqli\_res);

}

?>

Warum ist dieser Code unsicher: Es kann unbegrenzt versucht werden, sich anzumelden und der Angreifer kriegt direkte fehlermeldung und kann sogleich die nächste Anfrage stellen

Wie kann dieser Code sicherer gemacht werden: Begrenzte versuche pro Minute, Für bestimmte Zeit sperren, Zeige statt spezifischer Fehlermeldungen wie "Benutzername und/oder Passwort falsch" eine allgemeine Meldung wie "Ungültige Anmeldedaten" an, um Angreifern keine Hinweise zu geben was sie ändern müssen um rein zu kommen.

Tools zum Hacken

# 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

# Authorisation Bypass

# Open HTTP Redirect