Fachbereich Informatik
Prof. Dr. Reiner Hüttl

IT-Security

Übung 9

In dieser Übung behandeln wir das Thema Angriffe auf eine Webapplikation

Für die Übung nehmen wir die **„ OWASP Mutillidae 2 Web Pen Test Training Environment“** her. Diese Applikation ist frei im Web verfügbar und hat zu allen TOP 10 der OWASP Schwachstellen.

Installieren sie sich bitte die Applikation **bevor** sie die Übung besuchen auf ihrem Notebook/Rechner.

Dazu benötigen sie XAMPP auf ihren Rechner. Bitte installieren die Entwicklungsumgebung XAMPP (Apache + MySQL + PHP + Perl) auf ihrem Rechner (https://www.apachefriends.org/index.html)

Anschließend laden sie sich die Applikation Mutillidae 2 von
http://www.irongeek.com/i.php?page=mutillidae/mutillidae-deliberately-vulnerable-php-owasp-top-10
bzw.
https://github.com/webpwnized/mutillidae
herunter.
Dort finden sie auch Anleitungen zur Installation von XAMPP und Mutilidae.

Entpacken sie die Dateien von Mutilidae und kopieren sie die Dateien in den htdocs- Ordner von XAMPP (z.B. „C:\xampp\htdocs).

Starten sie das XAMP Control Panel
Starten sie im Control Panel Apache und MySQL
Starten sie die Anwendung unter http://127.0.0.1/mutillidae/

Hinweis: Wenn sie eine Fehlermeldung der folgenden Art erhalten:
The database server at 127.0.0.1 appears to be offline.
Error: Failed to connect to MySQL database
Dann ändern sie in der Datei mutilidae/includes/database-config.php das Passwort auf leer.
define('DB_PASSWORD', '');

Jetzt können wir gemeinsam in der Anwendung einige Sicherheitslücken suchen.

Zusatzinstallation

Für einige Angriffe muss man die Requests und Responses der Web-Anwendung anschauen oder manupilieren.

Dazu verwenden wir die Applikation **Burp Suite Community Edition**.

Den Download dieser Plattform für Security Tools für Web Applikationen finden sie unter: https://portswigger.net/burp/download.html

Es handelt sich um eine Jar-Datei die nur auf den Rechner kopiert werden muss und dann sofort ausführbar ist. Um Burp als Intercepting Proxy zwischen der Webanwendung und dem Anwender zu konfigurieren sind entweder die Proxy-Einstellungen in ihrem Browser zu modifizeren und aktivieren oder sie verwenden den **integrierten Browser von Burp**.

Jetzt kann jeder in der Anwendung Mutillidae einige Sicherheitslücken suchen und mittels des Proxy in der Burp Suite auch Requests und Responses von Mutillidae anzeigen und manipulieren.