SSI Lab 9

# Step 1 - Business Goal und Security Goals

## Business Goal

Eine webbasierte Marktplattform, welche es registrierten Benutzer erlaubt Artikel zu kaufen oder zu verkaufen.

## Security Goals

* Die Vertraulichkeit sämtlicher Benutzerdaten muss absolut gewährleistet werden.
* Das System muss vor jeglichen Manipulationen der Benutzer und Transaktionsdaten geschützt werden.
* Die Webplattform muss stets verfügbar sein.

# Step 3 – Network und Data Flow Diagramme

## Network Diagram



## Data Flow Diagrams



# Step 4 - Identifizieren von Threats

* Angreifer könnten grosses Interesse an den Kreditkartendaten haben. Ihre Angriffsziele werden aus diesem Grunde sicherlich primär die Käufer und Verkäufer sein.

# Step 5 - Identifizieren von Schwachstellen

|  |  |  |  |
| --- | --- | --- | --- |
| Nr. | Element | Cat. | Beschreibung |
| V1 | System Administrators | S | Die Authentifizierung mit dem SQL Server kann mittels Man in the Middle Attacke abgefangen werden, da die Verbindung nicht verschlüsselt ist. |
| V2 | System Administrators | T | Das FTP-Passwort kann abgefangen werden (da Verbindung nicht verschlüsselt). Der Angreifer wäre somit in der Lage, sämtliche Dateien per FTP abzuändern. |
| V3 | FTP / SSH | R | Durch den FTP-Zugriff oder stehlen der SSH Hijacking, wäre es dem Angreifer möglich sämtliche Spuren zu verwischen. Ebenso weil lediglich auf dem Webserver geloggt wird. |
| V4 | Web Application | I | Eine SQL-Injection könnte dem Angreifer die Möglichkeit geben Passwörter aus der Datenbank auszulesen, da diese nicht verschlüsselt sind. |
| V5 | SSH / FTP | D | Sofern dem Angreifern ein SSH Hijacking oder stehlen der FTP Authentifizierungsinformtionen gelingt, könnte er einfach den Server herunterfahren, oder Skripte hochladen, welche die RAM- oder CPU-Auslastung auf ein Maximum treiben. |
| V6 | All Users | E | Der Angreifer könnte durch simple Requests Aktionen durchführen, zu welchen er nicht authorisiert ist. |
| V7 | All Users | S | Session Hijacking erlaubt es dem Angreifer, sämtliche Rechte des Opfers zu übernehmen. |

# Step 6 - Neue Security Requirements

|  |  |  |
| --- | --- | --- |
| Nr. | Beschreibung | Vuln. |
| R1 | Sämtliche Verbindungen von den System Administrators aus müssen zwingend verschlüsselt werden. | V1 / V2 / V5 |
| R2 | Trotz Business Requirement ist es höchst fahrlässig plain-text Passwörter in der DB zu speichern. Es wird empfohlen Salted Passwords zu verwenden oder 2-Way Authentication per SMS oder Codegenerator App anzubieten. | V4 |
| R3 | Der FTP-Zugriff darf lediglich READ-ONLY Rechte aufweisen. | V2 |
| R4 | Die Session ID muss bei jedem Logout und Login Prozess geändert werden. | V7 |
| R5 | Logging von fehlerhaften Logins und Slow queries auf dem DB Server aktivieren. (Slow query Logs könnten evntl. einen Hinweis auf schadhafte Queries geben) | V3 / V4 |
| R6 | Es muss sichergestellt werden, dass sämtliche Aktionen per Standard nicht durchführbar sind, erst nach explizitem Setzen der Berechtigungen. Bsp. Erlauben Servlets auf Klassenebene keine Aktionen. Diese müssen per Methode erlaubt werden. | V6 |