Prof. Dr. Holger Schmidt
Professur für IT-Sicherheit, Informatik
Fachbereich Informatik – Fachhochschule Dortmund

Fachhochschule Dortmund
University of Applied Sciences and Arts

Übungsblatt 2 **Informationssicherheit SoSe 2023** Datum: 04.04.2023

Aufgabe 2.1 K12

Betrachten Sie die Durchführung einer Überweisung beim Internet-Banking. Die *Bank* bietet dazu eine Formular-basierte *Webseite* an (1), in die ein *Kunde* die *Überweisungsdetails* (z. B. Empfänger, IBAN) eingibt und bestätigt (2). Daraufhin fordert die Webseite nach dem bekannten iTAN-Verfahren anhand einer fortlaufenden natürlichen Zahl (sog. *Index*) eine TAN an (3). Der *Kunde* gibt die entsprechende *TAN* ein und bestätigt die Eingabe (4), woraufhin die Webseite eine *Quittung* über die Durchführung der Überweisung anzeigt (5).

Welche klassischen Sicherheitsziele sind in den einzelnen Schritten (1) bis (5) dieses Szenarios wichtig? Welche Assets werden jeweils von den Sicherheitszielen adressiert und welche Parteien haben ein Interesse an der Wahrung der Sicherheitsziele?

Hinweis: Die Assets und Parteien sind in obigem Text kursiv gedruckt. Bitte verwenden Sie ausschließlich diese Wörter in Ihrem Lösungsvorschlag.

Schritt	Sicherheitsziele (C, I, A)	Asset	Parteien
1			
2			
3			
4			
5			

Aufgabe 2.2 K30

Benutzen Sie die bereits von Ihnen vorbereitete virtuelle Maschine mit *OWASP WebGoat* und bearbeiten Sie die Lektionen zu

- *(A3) Injection → SQL Injection (intro)*,
- *(A3) Injection → SQL Injection (advanced)* und
- *(A3) Injection → SQL Injection (mitigation)*

in WebGoat. Lesen Sie dafür jeden Punkt der Lektionen sorgfältig durch und absolvieren Sie den praktischen Teil mit dem gewonnenen Wissen. Notieren Sie sich jeweils Ihre Lösung zu den einzelnen WebGoat Lektionen. Erläutern Sie zudem warum Ihre Lösung funktioniert. Zusätzlich beantworten Sie folgende Fragen:

a) Was ist eine *SQL Injection*?

b) Welche entwicklerseitigen Möglichkeiten gibt es, um eine SQL Injection zu verhindern? Geben diese Maßnahmen absolute Sicherheit? Falls nein, warum nicht?

c) Erläutern Sie die *Least Privilege* Maßnahmen anhand von *SQL Injections*.

Aufgabe 2.3 K30

Benutzen Sie die bereits von Ihnen vorbereitete virtuelle Maschine mit *OWASP WebGoat* und bearbeiten Sie die Lektion zu

- *(A3) Injection → Cross Site Scripting*

in WebGoat. Lesen Sie dazu jeden Punkt der Lektion sorgfältig durch und absolvieren Sie den praktischen Teil mit dem gewonnenen Wissen. Notieren Sie sich jeweils Ihre Lösung zu den einzelnen WebGoat Lektionen. Erläutern Sie zudem warum Ihre Lösung funktioniert. Zusätzlich beantworten Sie folgende Fragen:

a) Was ist *Cross Site Scripting (XSS)*? Bitte fassen Sie sich kurz.

b) Wo können *XSS* Schwachstellen bevorzugt gefunden werden?

c) Welche Vorteile kann sich ein Angreifer durch *XSS* Angriffe verschaffen?

d) Welche *XSS* Arten gibt es und wie unterscheiden Sie sich? Zeichnen Sie jeweils chematisch den Ablauf eines Angriffs auf.

e) Wie können Sie sich vor *XSS*-Angriffen schützen?