Webbasierte Anwendungen (SoSe2024)

Praktikum 10

1. Erklären Sie in eigenen Worten, was *SQL-Injection* ist. *(4 Punkte)*

2. Geben Sie ein eigenes Beispiel für eine SQL-Anfrage an. Geben Sie an, an welcher Stelle in dieser Anfrage Benutzereingaben getätigt werden können. Welche Eingaben kann ein Angreifer eingeben, um einen Angriff durchzuführen. Geben Sie auch die resultierende modifizierte SQL-Anfrage an.

   Für SQL-Injection Angriffe können Sie Ihr Vier–gewinnt–Spiel aus dem vorigen Praktikum nutzen. Dazu sollten Sie Ihr Projekt so modifizieren, dass mittels Konkatenation ein SQL-Befehl zusammengebaut wird und so eine Sicherheitslücke existiert. *Geben Sie Ihre Erläuterungen in plain Text. (6 Punkte)*

3. In den folgenden Aufgaben wird *Parameter-Injection* in Abgrenzung zu *SQL-Injection* und *Cross Site Scripting* behandelt.

   (a) Erläutern Sie in eigenen Worten, was *Parameter-Injection* ist. *Geben Sie Ihre Erläuterungen in plain Text. (4 Punkte)*

   (b) Geben Sie ein Beispiel für *Parameter-Injection* an. Geben Sie die Angriffsstelle (ggf. Quelltext) und auch den Angriff (auch Quelltext) an. *Geben Sie Ihre Erläuterungen in plain Text. (2 Punkte)*

   (c) Nennen Sie zwei Beispiele, mit denen *Parameter-Injection* unterbunden werden kann. *Geben Sie Ihre Erläuterungen in plain Text. (4 Punkte)*

4. Erläutern Sie, was *Enumeration* ist. Woran kann Enumeration erkannt werden? Nennen Sie eine Variante, mit der Enumeration erschwert werden kann. *Geben Sie Ihre Erläuterungen in plain Text. (8 Punkte)*

Die Aufgaben dieses Praktikums sind als Gruppenarbeit abzugeben. Die Lösungen sind in **elektronischer Form** unter `https://wba.cs.hs-rm.de/PraGA/` abzugeben. Bitte beachten Sie das dort angegebene Abgabedatum.