Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2008/2009
Übungsblatt 3

Abgabetermin: 12.11.2008 bis 14:00 Uhr

Achtung: Die schriftlichen Lösungen aller mit H gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben. Während des Semesters werden drei Übungsblätter korrigiert. Bei drei richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

Aufgabe 6: (H) XSS

a. Erstellen Sie eine Webseite, die einen in der URL der Seite übergebenen Parameter namens *?search=...* in den Seiteninhalt übernimmt und als `<p>`*parameter*`</p>` ausgibt. Wie verhält sich das Programm, wenn der Parameter *search* den Wert `<script>alert("XSS Attack!")</script>` enthält?

b. Löst das folgende Konstrukt das Problem? `<p><![CDATA[` *parameter* `]]></p>`
Warum (nicht)?

Aufgabe 7: (H) SQL-Injection

Gegeben ist das folgende Szenario:
Auf einem Webserver befindet sich ein Webformular, mit dessen Hilfe eine angebundene Datenbank abgefragt werden kann. Die eigentliche Abfrage übernimmt dabei ein CGI-Skript auf dem Webserver. Das Resultat der Abfrage ist abhängig von einem ID Feld, das vom Webformular gesetzt wird und mittels einem Parameter in der URL an das CGI-Skript weitergereicht wird. Ein valider Aufruf des CGI-Skripts lautet z.B. *http://webserver/cgi-bin/query.cgi?ID=86*.

a. Das Skript generiert folgenden SQL Query String: "`SELECT produkt FROM artikel WHERE ID=`" + ID + "`;`"
Modifizieren Sie den Paramter in der URL des CGI-Skriptes so, dass die Abfrage normal ausgeführt wird und anschließend die gesamte Relation Artikel gelöscht wird!

b. Das Skript generiert folgenden SQL Query String: "`SELECT produkt, preis FROM artikel WHERE ID like '%`" + ID + "`%';`"
Modifizieren Sie den Paramter in der URL des CGI-Skriptes so, dass die Abfrage normal ausgeführt wird und anschließend der Preis aller Produkte deren ID auf 2 endet halbiert wird!

c. Das Skript generiert folgenden SQL Query String: ”`SELECT produkt, preis FROM artikel WHERE ID=`” + ID + ”`;`”
Modifizieren Sie den Paramter in der URL des CGI-Skriptes so, dass die Abfrage normal ausgeführt wird und zusammen mit allen Kennungen der Datenbank samt ihren Passwort Hashes ausgegeben wird!

d. Wie können die beschriebenen Attacken verhindert werden?