UNIVERSITÄT ZU LÜBECK
INSTITUT FÜR IT-SICHERHEIT

Übungsblatt 7

Web- und Browsersicherheit

Abgabe bis 06. Juni 2023 um 12:00 Uhr im Moodle

Cybersecurity im Sommersemester 2023

Thomas Eisenbarth, Jan Wichelmann, Anja Köhl

Einführung

Die SQL-Injection-Schwachstellen im Kundenportal von ITS sind nun auch beseitigt worden – aber das war immer noch nicht alles: Es lauern noch einige Browser-basierte Angriffsvektoren.

Aufgabe 1 Browser Hardening (5 Punkte)

Bevor Sie Ihre Untersuchung der Website fortsetzen können, bittet das Management Sie um eine kleine Schulung zum Thema *Browser Hardening*: ITS möchte die Mitarbeiter auf Gefahren aus dem Web aufmerksam machen und dafür sorgen, dass die Mitarbeiter sich schützen können. Gehen Sie davon aus, dass in der gesamten Firma Firefox verwendet wird.

1. Informieren Sie sich und machen Sie mindestens drei Vorschläge, mit denen die Mitarbeiter ihre Browser sicherer machen können. Nehmen Sie bei allen Vorschlägen Stellung zu
   - Benötigtem Können der Mitarbeiter,
   - Vor- und Nachteilen, und
   - Usability der Maßnahmen.
2. Bei sogenannten *Phishing*-Angriffen wird versucht, das Opfer dazu zu bringen, sensible Daten wie z.B. Benutzernamen und Passwort einzugeben. Was sind typische Angriffsvektoren für Phishing? Was können Sie den Mitarbeitern von ITS mit auf den Weg geben?

Aufgabe 2 Ressourcentrennung im Browser (5 Punkte)

Nach Ihren Anmerkungen zur (Un-)Sicherheit des Kundenportal-Logins hat Webentwicklerin Wanda mit der Entwicklung eines neuen Login-Formulars begonnen. Leider scheint das restliche Kundenportal den neuen Login zu ignorieren, da sie dort trotz korrekt gesetztem Cookie nur eine „Sie sind nicht angemeldet“-Fehlermeldung bekommt.

Bei einer kurzen Debugging-Sitzung stellen Sie folgendes fest:

- Das Kundenportal läuft unter der Adresse `https://kundenportal.its-hosting.com`.
- Die Testinstanz des neuen Login-Formulars läuft unter der Adresse `https://login.development.its`.

Wanda setzt das Cookie `its-authtoken` in der Testinstanz. Das Kundenportal erwartet ebenfalls ein Cookie namens `its-authtoken`, kann das gleichnamige Cookie aus der Testinstanz allerdings nicht finden.

1. Erklären Sie dieses Verhalten. Warum kann das Kundenportal das Cookie des Login-Formulars nicht finden? Geben Sie ein Beispiel, warum das beobachtete Verhalten grundsätzlich erwünscht ist.
2. Beschreiben Sie eine Möglichkeit, wie sich das Problem beheben bzw. umgehen ließe.

Aufgabe 3 Cross Site Scripting (5 Punkte)

Auf der Website von ITS können Kunden (positive) Bewertungen zu den Hosting-Diensten hinterlassen. Hier gibt es auch ein Freitextfeld, welches Sie als anfällig für *Stored XSS* entdecken.

1. Das Freitextfeld wird auf 50 Zeichen begrenzt. Ist dies eine wirkungsvolle Gegenmaßnahme gegen Cross Site Scripting? Begründen Sie Ihre Antwort.
2. Die Webentwickler haben noch den Hinweis von Ihnen im Kopf: „Vertraue niemals Benutzereingaben“. Was bedeutet das für das aktuelle Szenario? Lassen sich hieraus Gegenmaßnahmen ableiten?
3. Was würden Sie ITS noch raten, um die Seite robuster gegen Cross Site Scripting zu machen?

Aufgabe 4 Cross Site Request Forgery (5 Punkte)

Webentwickler Wilhelm hat in den Medien von *Cross Site Request Forgery*-Angriffen (CSRF) gelesen, und vermutet, dass der Kundenbereich der ITS-Seite davon betroffen sein könnte.

1. Erklären Sie das Prinzip von CSRF-Angriffen mit eigenen Worten.
2. Bewerten Sie folgende Maßnahmen nach ihrer Wirksamkeit gegen CSRF:
   i. ITS implementiert *Login Timeouts*. Wenn der Anwender eine gewisse Zeit lang inaktiv war, wird die Session des Anwenders beendet. Er muss sich dann erneut einloggen.
   ii. ITS erhöht die Mindest-Passwortlänge von 5 Zeichen auf 10.
   iii. ITS führt ein TAN-System ein, sodass für jede Änderung noch eine spezielle TAN eingegeben werden muss.
   iv. ITS empfiehlt, den Kundenbereich nur in einem separaten Browser zu öffnen, der für nichts anderes benutzt wird.
3. Informieren Sie sich über das *Synchronizer Token Pattern*[1] und erklären Sie es in eigenen Worten.

[1] `https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html#synchronizer-token-pattern`