Web Security
Übungsblatt 1

Hackerpraktikum

FAU Erlangen-Nürnberg, Lehrstuhl für Informatik 1

Jeopardy CTF (Aufgabe 1)

Nehmen Sie am HackPra CTF teil und sichern Sie sich die Krone des besten Web-Hackers. Erstellen Sie sich dazu einen Account unter `http://10.0.23.24:1337/` und lösen Sie so viele Challenges wie möglich. Dokumentieren Sie zu jeder Challenge Ihren Lösungsweg.

Hinweis: Nutzen Sie für die XSS-Challenges die Möglichkeit, dem Administrator einen Link zuzusenden (`http://10.0.23.24:8006/`). 8 P.

Social Networks (Aufgabe 2)

Auf `http://10.0.23.22/myspray/` liegt ein auf Django (Python) basierendes, soziales Netzwerk namens MySpray.

1. *SQL Injection* (0.5 P.): Loggen Sie sich als Hanni Ball ein.
   Tipp: Das Datenbank-Layout liegt unter `http://10.0.23.22/dblayout`.

2. *Improper Authentication* (1 P.): Lesen Sie die Inbox, Outbox und „You have been sprayed by“ Liste von N. O'Brian aus.
   Tipp: Die kritischen Code-Auszüge liegen unter `http://10.0.23.22/messages`.

3. *Unrestricted File Upload* (1 P.): Führen Sie auf dem Server beliege Befehle als Benutzer `www-data` aus, indem Sie eine PHP-basierte Eingabeaufforderung platzieren.

4. *Cross-Site Scripting* (2 P.): In der Applikation befinden sich drei Arten von XSS Schwachstellen. Finden Sie diese Schwachstellen und entwickeln sie Exploits, mit deren Hilfe Sie Cookies Ihres Opfers stehlen können. Nutzen Sie anschließend die so erhaltene Session-ID und nehmen Sie die Identität Ihres Opfers an.

5. *Cross-Site Request Forgery* (0.5 P.): Bauen Sie eine eigene Website, die scheinbar gutartig ist aber im Hintergrund per JavaScript das Formular zum Versenden einer Nachricht abschickt. Schicken Sie im Namen des angemeldeten Benutzers eine Nachricht an den Benutzer Hanni Ball.

Hinweis: Der Quellcode liegt unter `http://10.0.23.22/myspray.tar.gz`. 5 P.

Bank (Aufgabe 3)

Auf `http://10.0.23.24:7777` erreichen Sie das Bank-Portal “TheWholeBank”. Finden Sie mindestens sieben Schwachstellen und zeigen Sie durch einen Exploit wie Sie diese jeweils ausnutzen. Schlagen Sie außerdem Patches vor, um die Lücken zu schließen.

Sehen Sie sich bitte *man patch* an, um Ihre patch Dateien zu erstellen. Bitte verwenden Sie die *requests* Bibliothek von *python* für Ihre Exploits. Machen Sie sich mit *docker* vertraut, um Ihre Patches und Exploits zu testen.

Hinweis: Bei dieser Aufgabe handelt es sich um ein typisches Attack/Defense Capture-the-Flag-Setup. Jedes teilnehmende Team (wir und Sie) hostet den selben Service. Sie versuchen uns unter Ausnutzung von Schwachstellen Flaggen (geheime String-Tokens) zu stehlen und gleichzeitig versuchen Sie in Ihrem Service Schwachstellen zu fixen. In unserer Instanz werden innerhalb von wenigen Minuten neue Flaggen hinterlegt. So können Sie Ihre Exploits testen. Nach der Abgabe werden wir Ihre abgegebenen Exploits gegen unser ungepatchtes System anwenden. Weiterhin werden wir Ihre abgegebenen Patches auf unser ungepatchtes System anwenden und durch unsere Exploits auf Wirksamkeit prüfen.

Hinweis: Nutzen Sie die Möglichkeit, die vorliegenden Docker-Container selbst zu starten. Die Container erhalten Sie unter `http://10.0.23.24/thewholebank.tar.gz`. 7 P.

$8 + 5 + 7 =$ **20 Punkte**