Web Security
Übungsblatt 2

Hackerpraktikum

FAU Erlangen-Nürnberg, Lehrstuhl für Informatik 1

Hackme (Aufgabe 1)

Unter `http://10.0.23.21/` finden Sie ein Hackme mit verschiedenen Sicherheitslücken. Nutzen Sie alle Lücken aus und dokumentieren Sie ihr Vorgehen.

Hinweis: Nutzen Sie die Möglichkeit, den Source-Code einzusehen. 2 P.

HackPra Jeopardy CTF (Aufgabe 2)

Nehmen Sie am HackPra Jeopardy CTF teil und sichern Sie sich die Krone des besten Web-Hackers. Erstellen Sie sich dazu einen Account unter `http://10.0.23.24/` und lösen Sie alle Challenges. Für jede gelöste und dokumentierte Challenge erhalten Sie 0.5 Punkte. Die Dokumentation Ihres Lösungsweges reichen Sie bitte über das StudOn-Portal ein.

Nutzen Sie als Nutzernamen ihre OpenVPN-Kennung und als Mailadresse Ihre @fau-Adresse.
Der Registrierungscode und die Credentials fuer .htaccess sind `workshop:workshop`.
Flags haben immer das Format `fau-ctf-<md5hash>`.

Dokumentieren Sie zu jeder Aufgabe ihr Vorgehen. Geben Sie Ihre selbstgeschriebenen (Hilfs-)programme ebenfalls ab.

Hinweis: Nutzen Sie für die XSS-Challenges die Möglichkeit, dem Administrator einen Link zuzusenden (`http://10.0.23.24:8080/xss-helper`). 11 P.

Social Networks (Aufgabe 3)

Auf `http://10.0.23.22/myspray/` liegt ein auf Django (Python2) 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.

$2 + 11 + 5 =$ **18 Punkte**