Aufgabe SoSe 2022

In der Aufgabe zum Injection-Teil steht Ihnen eine virtuelle Maschine zur Verfügung, auf der Sie eine Webseite finden. Diese weist einige Schwachstellen auf, die Ihnen bekannt vorkommen könnten. Nutzen Sie diese Schwachstellen, um die auf dem Server vorhandenen Kreditkarten-Informationen zu extrahieren.

Sie werden dafür in mehreren Schritten unterschiedliche Techniken anwenden müssen, die wir uns in den zwei Übungen angeschaut haben. Für jeden erfolgreichen Schritt gibt es Punkte, verzagen Sie also nicht, falls Sie nicht alle Schwachstellen finden und nicht bis zu den Kreditkartendaten vordringen können!

Als Lösung laden Sie bitte eine Textdatei oder PDF hoch, in der Sie die o.g. Informationen auflisten sowie kurz Ihr Vorgehen beschreiben - also die einzelnen Schritte, die Sie getan haben, um die Daten zu extrahieren. Sie müssen nicht die technischen Hintergründe im Detail beschreiben, aber Ihr Vorgehen sollte nachvollziehbar und reproduzierbar sein. Vom Umfang her sind 1-2 Seiten A4 (je nachdem ob/wie viel Code/Screenshots Sie verwenden) ausreichend, mehr als 5 Seiten wären zu viel. Der Inhalt ist hier wichtiger, als der Umfang.

Da die virtuelle Maschine zu groß ist, um Sie per Moodle zur Verfügung zu stellen, finden Sie den download hier:

https://cloud.htw-berlin.de/s/DrBmjCFjBD4Rc5A

Das Passwort für den Dateizugriff lautet: SgcdwBPYGX

Sie können die ova-Datei direkt in VirtualBox importieren. Die Regeln für das port forwarding sind so eingestellt, dass Sie, nachdem Sie die Maschine gestartet haben, direkt im Browser den folgenden Link aufrufen können:

http://127.0.0.1:8800/

um die Zielseite zu sehen.

Sollten Sie Probleme haben, zögern Sie bitte nicht, sich im Forum zu melden.

Als freiwillige Zusatzaufgabe (ohne Extra-Punkte, einfach nur zum Spaß) können Sie auch versuchen, eine shell auf der Maschine zu bekommen und dann Ihre Rechte auf root zu eskalieren. Allerdings müssen Sie dafür die Netzwerkkonfiguration ändern: Im Standardzustand ist die Maschine in "NAT"-Modus mit port forwarding konfiguriert, damit Sie nicht erst die IP herausfinden müssen. In diesem Modus wird aber die reverse shell nicht funktionieren - stattdessen müssten Sie, um die Zusatzaufgabe zu lösen, die Konfiguration wie bei Metasploitable auf "Host-only network" umstellen und entweder die unterschiedlichen IPs in dem Netzwerk (vermutlich wird es .101, .102 oder .103 sein) ausprobieren, oder sich kurz in nmap einlesen und Ihr host-only-Netzwerk scannen, um die IP herauszubekommen.

Viel Erfolg!