Faculty Speaker Notes

Hack the Box: Faculty Machine

Felicitas Pojtinger (fp036, Stuttgart Media University)

2023-01-16

Abstract

Speaker notes for the Voluntary Hacking Report for Winter 2022/2023.

Contents

1 Vorwort **2**

2 Benötigte Fähigkeiten **2**

3 Überblick **2**

4 Informationssammlung **3**

5 Nutzung **3**

6 User-Flag **4**

7 Root-Flag **4**

8 Zusammenfassung **4**

1 Vorwort

- Faculty ist eine Linux-basierte Maschine, erstellt von dem HTB-Benutzer gbyolo.
- Ursprünglich veröffentlicht am 2. Juli 2022 und wird als mittelschwer eingestuft
- CTF-ähnliche Maschine aufgrund von benutzerdefinierter, zweckgebundener Software und Verwendung von selten verwendeten Tools für Hinweise
- Zweckgebundene Software wurde in PHP geschrieben

2 Benötigte Fähigkeiten

- Um die User-Flag zu knacken, sind Kenntnisse in Linux, ein oberflächliches Verständnis von PHP, SQL-Injection und File Inclusion erforderlich.
- Sobald eine Shell erworben wurde, kann Remote Code Execution und der GNU Debugger dazu verwendet werden, um das Root-Flag zu erlangen.

3 Überblick

- Faculty bietet ein benutzerdefiniertes PHP-Fakultätsplanungssystem, das von Nginx auf Ubuntu bereitgestellt wird.
- Schwachstellen wurden durch Fuzzing mit ffuf gefunden, darunter eine SQL-Injection-Schwachstelle im Admin-Bereich.
- Mit sqlmap kann das Anmeldeformular umgangen werden, um Zugriff auf eine Fakultätsliste zu erhalten.
- Liste und andere Daten können als PDF heruntergeladen werden, wobei eine alte Version von mpdf mit einer Datei-Injection-Schwachstelle verwendet wird.
- Durch das Anzeigen eines Stack Traces des Servers kann das Verzeichnis des Quellcodes der App zugänglich gemacht werden, das eine Datei mit hartcodiertem Passwort und Benutzernamen enthält, die auch als SSH-Anmeldeinformationen verwendet werden.
- SSH-Zugang als Benutzer gbyolo ermöglicht es uns, eine Remote-Code-Ausführungsschwachstelle im meta-git-Paket auszunutzen, um auf Benutzer developer zu escalieren, indem wir den entsprechenden SSH-Privatschlüssel herunterladen.
- Das Root-Flag kann erlangt werden, indem eine vorinstallierte gdb verwendet wird, um sich an einen Prozess anzuschließen, der als Root ausgeführt wird und die Debug-Symbole aktiviert sind und die SUID-Bits von bash setzt, was es ermöglicht als root auszuführen.

4 Informationssammlung

- Nmap wurde verwendet, um offene Dienste auf der Maschine zu identifizieren, einschließlich Port 80 (HTTP) und 22 (SSH)
- Der Hostname wurde in /etc/hosts hinzugefügt, um auf die Dienste zugreifen zu können
- Mit ffuf wurde die Maschine gefuzzt und der Endpunkt /admin als interessant identifiziert

5 Nutzung

- Sqlmap wurde auf der Anmeldeseite der API verwendet, um nach SQL-Injection-Schwachstellen zu suchen
- Sqlmap wurde verwendet, um Spalten aufzulisten und Benutzer auszulesen, was einen Administrator-Benutzer und das entsprechende Passwort-Hash enthüllte
- Das Hash war nicht leicht zu knacken, selbst mit großen Passwort-Listen
- Die Datenbank wurde weiter ausgelesen und es konnten Fakultäts-ID-Nummern gefunden werden, die zum Anmelden im nicht-Admin-Bereich verwendet werden können.
- Der Netzwerkeinspektor enthüllte einen RPC-Endpunkt, der vom Frontend aufgerufen wurde, welcher beim Test mit SQLMap eine weitere SQL-Injection-Schwachstelle aufwies
- Die Schwachstelle wurde verwendet, um alle Tabellen abzufragen (mit UNION anstelle der zeitbasierten Methode)
- Die SQL-Injection-Schwachstelle ermöglicht es nicht, auf Dateien zuzugreifen
- Der Fuzzer von früher wurde erneut untersucht, was den Endpunkt /admin enthüllte
- Eine SQL-Injection-Schwachstelle wurde auf http://faculty.htb/admin mit ' OR 1=1# als Benutzername oder Passwort verwendet, was die Ausdrucksbewertung immer auf wahr setzt
- Ein Endpunkt, der PDFs generiert wurde gefunden
- Das Analysieren der Anfrage zeigte, dass der Eingabe HTML in einem base64 und URL-codierten Format war
- Eine POST-Anfrage wurde an den Endpunkt mit cURL gesendet, was die ID des PDFs zurückgab
- MPDF hat einen File-Inclusion-Exploit, der verwendet wurde, um /etc/passwd in das generierte PDF einzufügen
- Gbyolo, Developer und Root wurden als nächste Ziele aufgrund des Inhalts der eingefügten Datei identifiziert
- Der Quellcode der Anwendung wurde durch das Weglassen von Parametern und das Anzeigen eines Stacktraces abgerufen, was dabei half, den Speicherort des Quellcodes zu finden
- Die enthaltene db_connect.php-Datei wurde untersucht, um nach DB-Anmeldeinformationen zu suchen

- Der DB-Verbindungs-Konstruktor wurde gefunden, der den Benutzer als sched und das Passwort als Co.met06aci.dly53ro.per enthüllte
- Es wurde überprüft, ob das Passwort für gbyolo, developer und root übereinstimmt

6 User-Flag

- Das Passwort stimmte mit gbyolo überein
- Es gab eine mbox-Datei im Home-Verzeichnis
- Überprüfte, wie Sudo konfiguriert wurde, um nach Privilegienaufstiegen zu suchen
- In der Lage, meta-git als developer auszuführen
- meta-git hat eine RCE-Schwachstelle, die verwendet wurde, um den SSH-Schlüssel zu lesen
- Der SSH-Schlüssel wurde zur lokalen VM hinzugefügt und es war möglich, sich anzumelden
- War in der Lage, die user flag zu erhalten.

7 Root-Flag

- Eine Kopie von gdb wurde im Benutzerverzeichnis gefunden, war jedoch im Besitz von developer
- /usr/bin/gdb war zugänglich und wurde verwendet, um die Kontrolle über einen der als Root ausgeführten Prozesse zu übernehmen (wählte Postfix)
- Versuchte durch Setzen der SUID-Bits zu escalieren, konnte jedoch aufgrund fehlender Debug-Symbole nicht
- GDB an einen als Root ausgeführten Prozess angehängt (mit python), um die SUID-Bits für bash zu setzen
- Nach dem Verlassen von GDB konnte bash als Root ausgeführt werden
- Das Untersuchen des Home-Verzeichnisses von Root enthüllte verdächtige Dateien, in denen die root flag gefunden wurde.

8 Zusammenfassung

- Die User-Flag wurde innerhalb von ungefähr 4 Tagen geknackt und die Root-Flag war trivial zu erreichen
- Das Medium-Ranking fühlte sich angemessen an, aber mehrere Sackgassen waren demotivierend
- Das erste Machine, die der Autor vollständig allein geknackt hat

- Weitere Informationen und den vollständigen Bericht finden Sie auf meinem GitHub!