Cheatography

TryHackMe Cheatsheet - UkletiPHP Cheat Sheet

by UkletiPHP via cheatography.com/217772/cs/47933/

Gobuster

gobuster dir -u (ip) -w /usr/share/wordlists/-dirb/common.txt

gobuster dir -u (ip) -w /usr/share/wordlists/-SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt

NetCat

nc -lvnp [port po zelji] - postavlja listener na tvojoj strani koji ceka za promet ka web serveru, cesto se koristi za pravljenje reverse shell-a

Hydra

hydra -l (username) -P /usr/share/wordlists/-rockyou.txt ftp://(ip)

Podsetnik

Reverse shell: 1. naci exploit na exploit-db za tu verziju web servera 2. pokrenuti python file sa tim exploitom 3. sa netcat napraviti listener na portu po zelji 4. otici na revshells sajt, upisati info i pokrenuti tu komandu unutar exploita

No TTY: shell ne moze da pokrene komandu i mora da se upgradeuje, koristi se ova komanda: python3 -c 'import pty;pt-y.spawn("/bin/bash")'

Google alati

URL kodovi: https://http.cat/

Dekodiranje: https://gchq.github.io/Cybe-rChef/

Exploiti: https://www.exploit-db.com/

Rev shellovi: revshells.com

Eskalacija privilegija

Metoda 1: ako je web server pravljen na FUEL CMS-u pokreni ovu komandu: cat /var/www/html/fuel/application/config/data-base.php - dobices databazu koju posaljes claudu i kazes mu da je pretrazi za passworde, mozda se desi da je iskori-scena za root usera, nakon toga kucas su root da se prebacis na root-a i ukucas password koji si dobio.

Konzola - osnovno

pwd - trenutni direktorijum

ls - listuje fajlove

ls -la - listuje sve fajlove zajedno sa hiddenima

cd - change directory

cat - cita fajl

find/ -name [ime fajla]

find / -name [ime fajla] 2>/dev/null - pronalazi samo taj fajl, sve fajlove koji nisu pristupacni ne prikazuje, bolja alternativa find komandi

grep - cita text u fajlu

whoami - ispisuje tr usera

Pretraga exploita - Konzola

searchsploit [za sta exploit]

Download: searchsploit -m [ime exploita]

Python

python3 (file) - pokrece file u p3

python2 (file) - pokrece file u p2

nano (file) - file editor + pravljenje

By **UkletiPHP**
cheatography.com/ukletiphp/

Published 6th April, 2026.
Last updated 7th April, 2026.