Day 61: My Top 5 Web Hacking Tools

int0x33 Follow
Mar 1 · 3 min read

Burp Suite PRO

I say pro, because honestly if you are serious about pentesting web apps you need this. The free version is too throttled and you miss out on some great plugins, to me it’s well worth the **investment**.

> *Thousands of organizations use Burp Suite to find security exposures before it’s too late. By using cutting-edge scanning technology, you can identify the very latest vulnerabilities. Our researchers frequently uncover brand new vulnerability classes that Burp is the first to report. Burp Suite constantly raises the bar of what security testing is able to achieve.*

Burp Suite documentation: desktop editions

Burp Suite contains a wealth of features and capabilities to support manual and automated security testing. Use the…

portswigger.net

The JSON Web Token Toolkit

ticarpi/jwt_tool

snake: A toolkit for testing, tweaking and cracking JSON Web Tokens - ticarpi/jwt_tool

github.com

The JSON Web Token Toolkit *is great for validating, forging and cracking JWTs (JSON Web Tokens)*.

Its functionality includes:

- Checking the validity of a token
- Testing for the *RS/HS256* public key mismatch vulnerability

- Testing for the *alg=None* signature-bypass vulnerability
- Testing the validity of a secret/key/key file
- Identifying *weak keys* via a High-speed *Dictionary Attack*
- Forging new token header and payload values and creating a new signature with the key or via another attack method

```
python jwt_tool.py
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJsb2dpbiI6InRpY2FycGkifQ.aqNC
vShlNT9jBFTPBpHDbt2gBB1MyHiisSDdp8SQvgw
/usr/share/wordlists/rockyou.txt
```

Sqlmap

Sqlmap is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws and taking over of database servers. It comes with a powerful detection engine, many niche features for the ultimate penetration tester and a broad range of switches lasting from database fingerprinting, over data fetching from the database, to accessing the underlying file system and executing commands on the operating system via out-of-band connections.

SQLMAP has a google dork feature, try it, it’s fun…

```
sqlmap -g "inurl:\'php?id=\'"
```

Wfuzz

Wfuzz is a tool designed for bruteforcing Web Applications, it can be used for finding resources not linked (directories, servlets, scripts, etc), bruteforce GET and POST parameters for checking different kind of injections (SQL, XSS, LDAP,etc), bruteforce Forms parameters (User/Password), Fuzzing,etc.

Some features:

- Multiple Injection points capability with multiple dictionaries
- Recursion (When doing directory bruteforce)
- Post, headers and authentication data brute forcing
- Output to HTML
- Colored output
- Hide results by return code, word numbers, line numbers, regex
- Cookies fuzzing
- Multi threading
- Proxy support

- SOCK support
- Time delays between requests
- Authentication support (NTLM, Basic)
- All parameters bruteforcing (POST and GET)
- Multiple encoders per payload
- Payload combinations with iterators
- Baseline request (to filter results against)
- Brute force HTTP methods
- Multiple proxy support (each request through a different proxy)
- HEAD scan (faster for resource discovery)
- Dictionaries tailored for known applications (Weblogic, Iplanet, Tomcat, Domino, Oracle 9i, Vignette, Coldfusion and many more

```
wfuzz -c -z file,/usr/share/wfuzz/wordlist/general/common.txt --hc 404 http://192.168.1.202/FUZZ
```

Gobuster

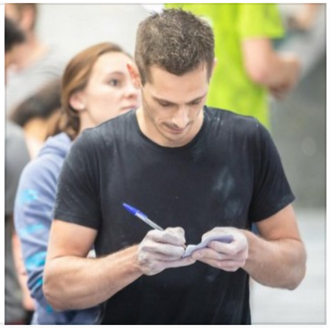
Gobuster is a tool used to brute-force:

- URIs (directories and files) in web sites.
- DNS subdomains (with wildcard support).

OJ/gobuster

Directory/file & DNS busting tool written in Go. Contribute to OJ/gobuster development by creating an account on...

github.com



It's better than dirb and dirbuster so dump those and enoy this.

```
gobuster -u https://mysite.com/path/to/folder -c 'session=123456' -t
50 -w common-files.txt -x .php,.html
```

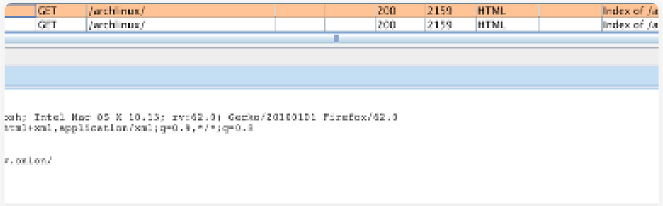
API Hacking Cybersecurity Infosec Web

15 claps

int0x33

Security Researcher / 365 Days of PWN

Follow



	GET	/archlinux/			200	2159	HTML		Index of /a
	GET	/archlinux/			200	2159	HTML		Index of /a

```
osh; Intel Mac OS X 10.13; rv:62.0) Gecko/20100101 Firefox/62.0
html+xml,application/xml;q=0.9,*/*;q=0.8

r.onion/
```

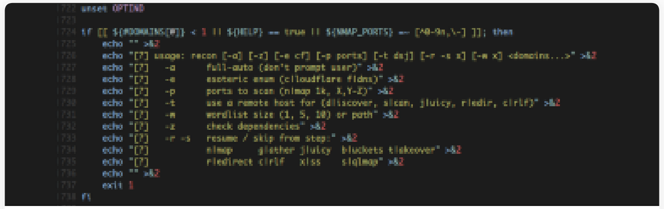
Related reads

How to intercept TOR hidden service requests with Burp

pentest_it

Sep 16, 2018 · 2 min re

101



```
unset OPTIND

if [[ ${#DOMAINS[@]} < 1 || ${HELP} == true || ${NMAP_PORTS} =~ [^0-9n,\-] ]]; then
    echo "" >&2
    echo "[?] usage: recon [-a] [-z] [-e cf] [-p ports] [-t dsj] [-r -s x] [-w x] <domains...>" >&2
    echo "[?]   -a      full-auto (don't prompt user)" >&2
    echo "[?]   -e      esoteric enum (cloudflare fldns)" >&2
    echo "[?]   -p      ports to scan (nmap 1k, X,Y-Z)" >&2
    echo "[?]   -t      use a remote host for (d)iscover, (s)can, (j)uicy, (r)edir, (c)rlf)" >&2
    echo "[?]   -w      wordlist size (1, 5, 10) or path" >&2
    echo "[?]   -z      check dependencies" >&2
    echo "[?]   -r -s   resume / skip from step:" >&2
    echo "[?]           (n)map    (g)ather (j)uicy  (b)uckets (t)akeover" >&2
    echo "[?]           (r)edirect (c)rlf   (x)ss    (s)qlmap" >&2
    echo "" >&2
    exit 1
fi
```

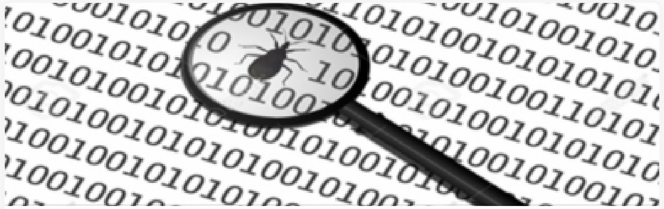
Related reads

Reconnaissance: a eulogy in three acts

europa

Feb 11, 2018 · 8 min re

1.3K



Related reads

★

The BatchOverflow Bug and How to Catch All Bugs

Kiran Garimella

May 11, 2018 · 12 min

208

Responses

Write a response…