

Forum:[Hack Forums](#)

Thread: [Wfuzz: The Ultimate Ethical Hackers Guide + Attack Website Example](#)

JoseMar - January 15, 2025, 1:39 pm

Wfuzz: The Ultimate Ethical Hacker's Guide

When it comes to web application vulnerability scanning, Wfuzz is a must have for ethical hackers. This very versatile tool allows you to automate HTTP requests and find hidden files, directories and even security flaws. Whether you are new to security or an experienced tester, Wfuzz has got you covered.

What's so special about Wfuzz?

Customizable testing

Payloads: Use existing wordlists or create your own custom ones for your target.

Filtering: Exclude results based on HTTP codes, content length or specific text to focus on what matters.

Integration: Wfuzz works with Burp Suite and supports proxy for deeper analysis.

Fast: Multithreading and connection reuse for large scale testing without performance hit

How to use Wfuzz

1. Find Hidden Directories and Files Web applications have directories or files not meant to be public. Wfuzz can help you find them:

Code `wfuzz -c -z file,/path/to/wordlist.txt --hc 404 http://example.com/FUZZ`-c: adds color output
-z: specifies the payload source (wordlist)
--hc 404: hides 404 responses (non-existent resources)

2. Test Web Parameters Find parameters in GET or POST requests that expose vulnerabilities:

Code `wfuzz -c -z file,/path/to/parameters.txt http://example.com/page.php?FUZZ=value`

For POST parameter testing:

Code `wfuzz -c -z file,/path/to/parameters.txt -d "FUZZ=value" http://example.com/page.php`

3. Brute-Force Login Credentials Test weak username and password combinations to test authentication:

Code `wfuzz -c -z file,username.txt -z file,passwords.txt --hc 401 -d`

`"username=FUZZ&password=FUZZZ" http://example.com/login`

Here: --hc 401 filters out unauthorized responses, highlighting successful logins

4. SQL Injection Detect SQL injection points with crafted payloads:

Code `wfuzz -c -z file,sql_payloads.txt --hh 1000 http://example.com/index.php?id=FUZZ`

5. HTTP Headers Test custom or modified HTTP headers:

Code `wfuzz -c -z file,headers.txt -H "FUZZ: value" http://example.com/`

6. API Test endpoints in REST APIs:

Code `wfuzz -c -z file,api_endpoints.txt http://example.com/api/FUZZ`

7. Subdomain Find subdomains of a target domain:

Code `wfuzz -c -z file,subdomains.txt -H "Host: FUZZ.example.com" http://example.com`

Real Test Machine:

`-u 192.168.0.42 --> Victim IP website`

Here, the main page is <http://logan.hmv>, but we want to check if there are any subdomains before logan.hmv.

In that case, we add FUZZ before logan.hmv, is mean that we need to add FUZZ.logan.hmv to the command.

But now, something is not good that we have a lot of pages , way too many, so we stop them from scanning:

Here we can hide them so they no longer show,Line Characters, or the third column

In this example we hide by line. We add the following to the previous command:

`--hl=1`

if we want to hide the others column we can use:

`--hw=number`

`--hc=number` (here I will add 404 for hide all 404 error page)

```
Code wfuzz -c --hc=404 --hl=1 -w /usr/share/...dicionar.txt -H "Host: FUZZ.logan.hmv" -u 192.168.0.42
```

Now line 1 is no longer showing because we hid it.

We can see a subdomain called "admin" was found, so the page will be admin.logan.hmv

But the page won't load because it also needs to be added to /etc/hosts

How to add this page to /etc/hosts ?

Open terminal and write:

```
nano /etc/hosts
```

and add IP + domain

Now we can see the website:

Advanced

Wfuzz has advanced features for power users: HTTP Methods: GET, POST, PUT, DELETE

Payload Encoding: Base64, URL encoding, custom schemes

Filtering Options:

Exclude by HTTP status code: --hc

Focus on specific response lengths: --hl or --hh

Search for or exclude keywords in responses: --filter "text='keyword'"

Wfuzz Best Practices

Targeted Wordlists: Use CeWL to create custom wordlists for better precision.

Proxies: Run Wfuzz through Burp Suite to see requests and responses.

Start Small: Run a subset of payloads to see how the app behaves before running big scans.

Monitor Impact: Don't flood the target with too many requests.

Combine Tools: Run Wfuzz with Nmap and OWASP ZAP for full testing.

Legal and Ethical

Remember, ethical hacking requires permission from system owners before testing. Unauthorized activities are illegal and unethical. Always follow responsible disclosure when reporting

vulnerabilities.

Wfuzz is a powerful tool for ethical hackers to do web application testing. By learning its features and best practices you can better identify and fix security issues. If you have any question or need help with your virtual lab setup, ask me!

Bastille - January 16, 2025, 3:57 am

Going to my favs, I've only used this tool a few times on tryhackme for fuzzing, next time I'll use it I'll refer to this thread, thanks for the share !

JoseMar - January 16, 2025, 8:17 am

(Jan 16, 2025 04:57 AM)Bastille Wrote: [\[CITE\]](#) Going to my favs, I've only used this tool a few times on tryhackme for fuzzing, next time I'll use it I'll refer to this thread, thanks for the share !

Can you tell me which programs you use more often for or instead of Wfuzz, which one you prefer, and which one you think is the best all-in-one tool?

I mean for Fuzzing ?

Bastille - January 17, 2025, 12:05 am

(Jan 16, 2025 09:17 AM)JoseMar Wrote: [\[CITE\]](#) Can you tell me which programs you use more often for or instead of Wfuzz, which one you prefer, and which one you think is the best all-in-one tool?

I mean for Fuzzing ?

I use gobuster, I've also heard about dirbuster but it seems that gobuster is faster. Also heard about fuff, I've maybe used it a couple of times back in the days but don't remember.

RoundLettuce - August 24, 2025, 2:47 am

Epic tutorial man! I do love Fuzzing and I'm studying a lot of Web App Security recently. Thanks! :)