Pentesting0x

FFuf

START

By: sudobyter

What's FFuf ?

FFUF (Fuzz Faster U Fool) is a fast web fuzzer written in Go, designed for web security testing. It automates the process of sending requests to a web server and analyzing the responses, aiming to discover hidden files, directories, and vulnerabilities

FFUF (Fuzz Faster U Fool) هي أداة فحص ويب سريعة مكتوبة بلغة Go، مصممة لاختبار أمان الويب. تعمل على أتمتة عملية إرسال الطلبات إلى خادم الويب وتحليل الاستجابات بهدف اكتشاف الملفات والدلائل المخفية والثغرات الأمنية.

How to install Fuff?

- Debian

```
$_ > sudo apt-get install ffuf
```

```
$_ > go get -u github.com/ffuf/ffuf
```

Examples of using Fuff?

- Directory Discovery

```
$_> ffuf -u https://target.com/FUZZ -w wordlist.txt
```

- File Enumeration

```
$_> fffuf -u https://target.com/FUZZ -w wordlist.txt -e .php,.html
```

Examples of using Fuff?

- Subdomain Enumeration

```
$_ > ffuf -u http://FUZZ.target.com -w subdomains.txt
```

- Filtering results

```
$_ > ffuf -u http://target/FUZZ -w /path/to/wordlist.txt -fc 404 -mc 200
```

Examples of using Fuff?

- VHOST

```
$_> ffuf -w /path/to/vhost_wordlist.txt -u https://target -H
"Host: FUZZ"
```

- Parameter Discovery

```
$_> ffuf -u http://target/?FUZZ=test -w /path/to/parameters.txt
```

Examples of using Fuff?

- POST Data Fuzzing

```
$_> ffuf -X POST -d "username=FUZZ&password=test" -u
http://target/login -w /path/to/usernames.txt
```

- Recursive Fuzzing

```
$_> ffuf -u http://target/FUZZ -w /path/to/wordlist.txt -recursion
```

Examples of using Fuff?

- HTTP Method Fuzzing

```
$_> ffuf -X FUZZ -u http://target -w /path/to/http_methods.txt
```

- Header Fuzzing

```
$_> ffuf -H "User-Agent: FUZZ" -u http://target -w
/path/to/user_agents.txt
```

Examples of using Fuff?

- Cookie Fuzzing

```
$_> ffuf -b "SESSIONID=FUZZ" -u http://target -w
/path/to/session_ids.txt
```

- Rate Limiting & Timeout Adjustments

```
$_> ffuf -u http://target/FUZZ -w /path/to/wordlist.txt -p 1-5 -timeout
10
```

Examples of using Fuff?

- Using Proxy

```
$_> ffuf -u http://target/FUZZ -w /path/to/wordlist.txt -x
http://127.0.0.1:8080
```

- Fuzzing Multiple Points

```
$_> ffuf -u http://target/FUZZ1/FUZZ2 -w
/path/to/wordlist1.txt:FUZZ1,/path/to/wordlist2.txt:FUZZ2
```

aliwaleedhum

Y0U C4N
F1ND M3 @T

https://aliwaleed.xyz

sudobyter@gmail.com