# 10 - Attacking Web Applications With FFUF

# 模糊测试

### 目录模糊测试

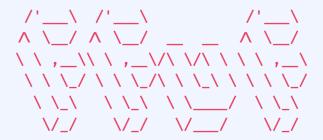
主要的两个选项是 -w 用于单词列表和 -u 用于 URL

```
Chenduoduo@htb[/htb]$ ffuf -w /opt/useful/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ
```

接下来,由于我们想对 Web 目录进行模糊测试,我们可以将 FUZZ 关键字放在目录位于 URL 中的位置,如下所示:

```
Chenduoduo@htb[/htb]$ ffuf -w <SNIP> -u http://SERVER_IP:PORT/FUZZ
```

Chenduoduo@htb[/htb]\$ ffuf -w /opt/useful/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://SERVER\_IP:PORT/FUZZ



v1.1.0-git

:: Method : GET

:: URL : http://SERVER\_IP:PORT/FUZZ

:: Wordlist : FUZZ: /opt/useful/seclists/Discovery/Web-

Content/directory-list-2.3-small.txt

:: Follow redirects : false
:: Calibration : false
:: Timeout : 10

:: Threads : 40

:: Matcher : Response status: 200,204,301,302,307,401,403

\_\_\_\_\_

<SNIP>

blog [Status: 301, Size: 326, Words: 20, Lines: 10]

:: Progress: [87651/87651] :: Job [1/1] :: 9739 req/sec :: Duration:

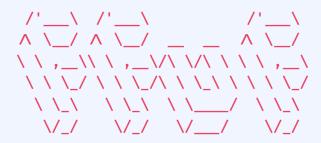
[0:00:09] :: Errors: 0 ::

# 页面模糊测试

Chenduoduo@htb[/htb]\$ ffuf -w /opt/useful/seclists/Discovery/Web-Content/web-extensions.txt:FUZZ <SNIP>

#### 将我们的 FUZZ 关键字放在索引之后的扩展名位置

Chenduoduo@htb[/htb]\$ ffuf -w /opt/useful/seclists/Discovery/Web-Content/web-extensions.txt:FUZZ -u http://SERVER\_IP:PORT/blog/indexFUZZ



v1.1.0-git

:: Method : GET

:: URL : http://SERVER\_IP:PORT/blog/indexFUZZ

:: Wordlist : FUZZ: /opt/useful/seclists/Discovery/Web-

Content/web-extensions.txt

:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 5

:: Matcher : Response status: 200,204,301,302,307,401,403

\_\_\_\_\_

.php [Status: 200, Size: 0, Words: 1, Lines: 1]
.phps [Status: 403, Size: 283, Words: 20, Lines: 10]

```
:: Progress: [39/39] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] :: Errors: 0 ::
```

使用 php 作为扩展名,将 FUZZ 关键字放在文件名应该在的位置,并使用我们用于模糊目录的相同单词列表:

```
Chenduoduo@htb[/htb]$ ffuf -w /opt/useful/seclists/Discovery/Web-
Content/directory-list-2.3-small.txt:FUZZ -u
http://SERVER_IP:PORT/blog/FUZZ.php
      /'__\ /'__\
^\_/ ^\_/ _ _ _ ^'__\
      \\,_\\\,_\\\\\\\\,_\
       \ \ \_/ \ \ \_/\ \ \ \_/
        \ \_\ \ \ \_\ \ \\___/ \ \\_\
        \/_/ \/__/ \/__/
      v1.1.0-git
                  : GET
 :: Method
 :: URL
                  : http://SERVER_IP:PORT/blog/FUZZ.php
 :: Wordlist
             : FUZZ: /opt/useful/seclists/Discovery/Web-
Content/directory-list-2.3-small.txt
 :: Follow redirects : false
 :: Calibration : false
                  : 10
 :: Timeout
 :: Threads
                  : 40
               : Response status: 200,204,301,302,307,401,403
 :: Matcher
                      [Status: 200, Size: 0, Words: 1, Lines: 1]
index
                      [Status: 200, Size: 465, Words: 42, Lines: 15]
REDACTED
:: Progress: [87651/87651] :: Job [1/1] :: 5843 req/sec :: Duration:
[0:00:15] :: Errors: 0 ::
```

# 递归模糊测试

在 ffuf 中,我们可以使用 -recursion 标志启用递归扫描,也可以使用 -recursion-depth 标志指定深度。如果我们指定 -recursion-depth 1 ,它只会模糊测试主目录及其直接子目录。如果标识了任何子子目录(如 /login/user ,它不会对页面进行模糊测试)。在 ffuf 中使用递归时,我们可以使用 -e .php 指定我们的扩展

#### ## Recursive Scanning 递归扫描

```
Chenduoduo@htb[/htb]$ ffuf -w /opt/useful/seclists/Discovery/Web-
Content/directory-list-2.3-small.txt:FUZZ -u http://SERVER_IP:PORT/FUZZ
-recursion -recursion-depth 1 -e .php -v
      \\,_\\\,_\\\\\\\\,_\
       \ \ \_/ \ \ \_/\ \ \_\
        \ \_\ \ \ \_\ \ \\___/ \ \\_\
        \/_/ \/__/ \/__/
      v1.1.0-git
                  : GET
 :: Method
 :: URL
                   : http://SERVER IP:PORT/FUZZ
                  : FUZZ: /opt/useful/seclists/Discovery/Web-
 :: Wordlist
Content/directory-list-2.3-small.txt
 :: Extensions
                  : .php
 :: Follow redirects : false
 :: Calibration : false
 :: Timeout
                  : 10
 :: Threads
                  : 40
 :: Matcher
                   : Response status: 200,204,301,302,307,401,403
[Status: 200, Size: 986, Words: 423, Lines: 56] | URL |
http://SERVER_IP:PORT/
   * FUZZ:
[INFO] Adding a new job to the queue: http://SERVER_IP:PORT/forum/FUZZ
[Status: 200, Size: 986, Words: 423, Lines: 56] | URL |
http://SERVER_IP:PORT/index.php
   * FUZZ: index.php
[Status: 301, Size: 326, Words: 20, Lines: 10] | URL |
http://SERVER_IP:PORT/blog | → | http://SERVER_IP:PORT/blog/
   * FUZZ: blog
< ... SNIP ... >
```

```
[Status: 200, Size: 0, Words: 1, Lines: 1] | URL |
http://SERVER_IP:PORT/blog/index.php
  * FUZZ: index.php

[Status: 200, Size: 0, Words: 1, Lines: 1] | URL |
http://SERVER_IP:PORT/blog/
  * FUZZ:

< ... SNIP ... >
```

ffuf -w /usr/share/SecLists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://94.237.54.192:38862/forum/FUZZ.php ? -recursion -recursion-depth 1 -e .php -v

ffuf -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-small.txt -u http://94.237.54.192:38862/forum/FUZZ -e .php -recursion -recursion-depth 2 -v | grep -v Error

# 域模糊测试

# 子域模糊测试

通过检查不同的网站是否具有将我们重定向到正常工作的服务器 IP 的公共 DNS 记录来检查它们是否存在。那么,让我们运行一次扫描,看看我们是否得到任何命中。在开始扫描之前,我们需要两样东西:

- ◆ A wordlist 单词表
- ◆ A target 目标

在 SecLists 存储库中,有一个针对子域词表的特定部分,由通常用于子域的常用词组成。我们可以在 /opt/useful/seclists/Discovery/DNS/ 中找到它。在我们的例子中,我们将使用一个较短的单词列表,即 subdomains-top1million-5000.txt 。如果我们想扩展扫描,我们可以选择一个更大的列表。

```
Chenduoduo@htb[/htb]$ ffuf -w
/opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ
-u https://FUZZ.inlanefreight.com/

/'___\ /'___\ /'___\
^\__/ ^\__/ __ _ _ ^\___\
\\__/ \\__/ \\__/\__\\__\\__\
```



#### v1.1.0-git

:: Method : GET

:: URL : https://FUZZ.inlanefreight.com/

:: Wordlist : FUZZ:

/usr/share/seclists/Discovery/DNS/subdomains-top1million-5000.txt

:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40

:: Matcher : Response status: 200,204,301,302,307,401,403,405,500

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 381ms]

\* FUZZ: support

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 385ms]

\* FUZZ: ns3

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 402ms]

\* FUZZ: blog

[Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 180ms]

\* FUZZ: my

[Status: 200, Size: 22266, Words: 2903, Lines: 316, Duration: 589ms]

\* FUZZ: www

< ... SNIP ... >

Chenduoduo@htb[/htb]\$ ffuf -w
/opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ
-u http://FUZZ.academy.htb/





v1.1.0-git

:: Method : GET

:: URL : https://FUZZ.academy.htb/

:: Wordlist : FUZZ:

/opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt

:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40

:: Matcher : Response status: 200,204,301,302,307,401,403

:: Progress: [4997/4997] :: Job [1/1] :: 131 req/sec :: Duration:

[0:00:38] :: Errors: 4997 ::

### Vhost 模糊测试

:: URL

:: Wordlist : FUZZ:

要扫描 VHosts,而无需手动将整个单词列表添加到我们的 /etc/hosts ,我们将模糊测试 HTTP 标头,特别是 Host: 标头。为此,我们可以使用 -H 标志来指定标头,并在其中使用 FUZZ 关键字,如下所示:

: http://academy.htb:PORT/

```
/opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header
                    : Host: FUZZ
 :: Follow redirects : false
 :: Calibration : false
                   : 10
 :: Timeout
 :: Threads
                    : 40
 :: Matcher
                    : Response status: 200,204,301,302,307,401,403
mail2
                        [Status: 200, Size: 900, Words: 423, Lines: 56]
dns2
                        [Status: 200, Size: 900, Words: 423, Lines: 56]
ns3
                        [Status: 200, Size: 900, Words: 423, Lines: 56]
dns1
                        [Status: 200, Size: 900, Words: 423, Lines: 56]
lists
                        [Status: 200, Size: 900, Words: 423, Lines: 56]
webmail
                        [Status: 200, Size: 900, Words: 423, Lines: 56]
                        [Status: 200, Size: 900, Words: 423, Lines: 56]
static
                        [Status: 200, Size: 900, Words: 423, Lines: 56]
web
                        [Status: 200, Size: 900, Words: 423, Lines: 56]
www 1
< ... SNIP ... >
```

### 筛选结果

#### ## Filtering

在这种情况下,我们不能使用匹配,因为我们不知道来自其他 VHost 的响应大小是多少。我们知道错误结果的响应大小,从上面的测试中可以看出,它是 900 , 我们可以使用 -fs 900 将其过滤掉。现在,让我们重复相同的上一个命令,添加上面的标志,看看我们得到什么:

```
:: Wordlist : FUZZ:
/opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt
 :: Header
                     : Host: FUZZ.academy.htb
 :: Follow redirects : false
 :: Calibration
                   : false
                    : 10
 :: Timeout
 :: Threads
                    : 40
 :: Matcher
                   : Response status: 200,204,301,302,307,401,403
 :: Filter
                    : Response size: 900
< ... SNIP ... >
admin
                        [Status: 200, Size: 0, Words: 1, Lines: 1]
:: Progress: [4997/4997] :: Job [1/1] :: 1249 req/sec :: Duration:
[0:00:04] :: Errors: 0 ::
```

注 1: 别忘了将 "admin.academy.htb" 添加到 "/etc/hosts" 中。 我们看到我们可以访问该页面,但我们得到一个空页面,这与我们使 用 academy.htb 得到的页面不同,因此确认这确实是一个不同的 VHost。我们甚至可 以访问 https://admin.academy.htb:PORT/blog/index.php ,我们会看到我们会得 到一个 404 PAGE NOT FOUND,这证实我们现在确实在不同的 VHost 上。

codewidthme@htb[/htb]\$ ffuf -w /usr/share/SecLists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:55059/ -H 'Host: FUZZ.academy.htb' -fs 986

# 参数模糊测试

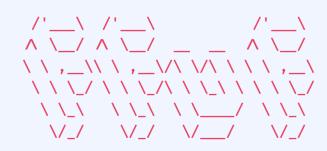
### **GET**

首先从 GET 请求的模糊测试开始,这些请求通常在 URL 之后传递,带有 ? 符号,例如:

http://admin.academy.htb:PORT/admin/admin.php?param1=key

因此,我们所要做的就是将上面示例中的 param1 替换为 FUZZ 并重新运行我们的扫描。然而,在我们开始之前,我们必须选择一个合适的单词列表。 SecLists 再次在 /opt/useful/seclists/Discovery/Web-Content/burp-parameter-names.txt .这样,我们就可以运行扫描了。

```
Chenduoduo@htb[/htb]$ ffuf -w /opt/useful/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://admin.academy.htb:PORT/admin/admin.php?FUZZ=key -fs xxx
```



v1.1.0-git

:: Method : GET

:: URL : http://admin.academy.htb:PORT/admin/admin.php?

FUZZ=key

:: Wordlist : FUZZ: /opt/useful/seclists/Discovery/Web-

Content/burp-parameter-names.txt

:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40

:: Matcher : Response status: 200,204,301,302,307,401,403

:: Filter : Response size: xxx

<... SNIP...> [Status: xxx, Size: xxx, Words: xxx,

Lines: xxxl

我们确实得到了回报。让我们尝试访问该页面并添加此 GET 参数,看看我们现在是否可以读取该标志:

ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u "http://admin.academy.htb:40054/admin/admin.php?FUZZ=key" -fs 798

这里有个重点,我们测试的是admin.academy.htb网站,所以需要把这整个域名在/etc/hosts 中与IP进行对应,不然测试不出来任何东西

### **POST**

POST 请求和 GET 请求之间的主要区别在于,POST 请求不随 URL 一起传递,并且不能简单地附加在? 符号之后。 POST 请求在 HTTP 请求的 data 字段中传递

要使用 ffuf 对 数据 字段进行模糊测试,我们可以使用 -d 标志,正如我们之前在 ffuf -h 的输出中看到的那样。我们还必须添加 -X POST 来发送 POST 请求。

提示: 在 PHP 中, "POST" 数据 "content-type" 只能接受 "application/x-www-form-urlencoded"。因此,我们可以在 "ffuf" 中使用 "-H 'Content-Type: application/x-www-form-urlencoded" 进行设置。

```
Chenduoduo@htb[/htb]$ ffuf -w /opt/useful/seclists/Discovery/Web-
Content/burp-parameter-names.txt:FUZZ -u
http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'FUZZ=key' -H
'Content-Type: application/x-www-form-urlencoded' -fs xxx
     \\,_\\\,_\\\\,_\
      \\\_/\\\_/\\\_\\\_/
       \ \_\ \ \ \_\ \ \ \___/ \ \ \_\
       \/_/ \/_/ \/__/
     v1.1.0-git
 :: Method
              : POST
               : http://admin.academy.htb:PORT/admin/admin.php
:: URL
 :: Wordlist : FUZZ: /opt/useful/seclists/Discovery/Web-
Content/burp-parameter-names.txt
 :: Header
            : Content-Type: application/x-www-form-urlencoded
 :: Data
                : FUZZ=kev
 :: Follow redirects : false
 :: Calibration : false
                : 10
 :: Timeout
 :: Threads
               : 40
id
                   [Status: xxx, Size: xxx, Words: xxx, Lines: xxx]
< ... SNIP ... >
```

# Value 模糊测试

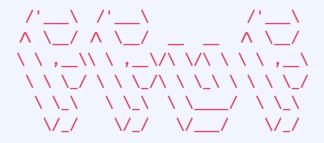
for i in \$(seq 1 1000); do echo \$i >> ids.txt; done 创建此单词列表的方法有很多种,从手动键入文件中的 ID,到使用 Bash 或 Python 编写脚本。最简单的方法是在 Bash 中使用以下命令,将 1-1000 中的所有数字写入文件:

Chenduoduo@htb[/htb]\$ for i in \$(seq 1 1000); do echo \$i >> ids.txt;
done

```
Chenduoduo@htb[/htb]$ cat ids.txt

1
2
3
4
5
6
< ... SNIP ... >
```

```
Chenduoduo@htb[/htb]$ ffuf -w ids.txt:FUZZ -u
http://admin.academy.htb:PORT/admin/admin.php -X POST -d 'id=FUZZ' -H
'Content-Type: application/x-www-form-urlencoded' -fs xxx
```



v1.0.2

:: Method : POST

:: Matcher : Response status: 200,204,301,302,307,401,403

:: Filter : Response size: xxx

<... SNIP...> [Status: xxx, Size: xxx, Words: xxx,

Lines: xxxl

curl -X POST http://admin.academy.htb:40054/admin/admin.php -d "id=73" -x http://127.0.0.1:8080 -

ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-small.txt:FUZZ -u http://faculty.academy.htb:35963/FUZZ ? -recursion -recursion-depth 1 -e .php,.php7,.phps -fs 287 -t 200

ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://faculty.academy.htb:35963/courses/linux-security.php7?FUZZ=key ? -fs 774

ffuf -w /usr/share/wordlists/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://faculty.academy.htb:35963/courses/linux-security.php7 
-X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs 774

ffuf -w /usr/share/wordlists/seclists/Usernames/xato-net-10-million-usernames.txt:FUZZ -u http://faculty.academy.htb:35963/courses/linux-security.php7 -X POST -d 'username=FUZZ' -H 'Content-Type: application/x-www-form-urlencoded' -fs 781

curl http://faculty.academy.htb:35963/courses/linux-security.php7 -X POST -d 'username=harry' -H 'Content-Type: application/x-www-form-urlencoded'