FFUF

☠ Ffuf, Fuzz Faster you Fool 'un kısaltmasıdır.web uygulamalarındaki veya web sunucularındaki öğeleri ve içeriği keşfetmeyi amaçlayan açık kaynaklı bir web fuzzing aracıdır. Bununla ne demek istiyoruz? Genellikle bir web sitesini ziyaret ettiğinizde, web sitesinin sahibinin size sunmak istediği içerik size sunulur; bu, gibi bir sayfada barındırılabilir index.php. Güvenlik kapsamında, genellikle bir web sitesinde düzeltilmesi gereken zorluklar bunun dışında bulunur. Örneğin, web sitesinin sahibi adresinde barındırılan admin.php, hem bilmek hem de test etmek istediğiniz içeriğe sahip olabilir. FFUF, amacınız için bu öğeleri ortaya çıkarmak için bir araçtır.

Kurulum

☠ FFuf'u kendi sayfasından kurmak isterseniz

- go get github.com/ffuf/ffuf

☠ FFuf'u güncellemek içinse şu komutu kullanabiliriz

- go get -u github.com/ffuf/ffuf

☠ **Ffuf şu dağıtımlara yüklü gelmiştir**

- **BlackArch**
- **Pentoo**
- **Kali Linux**
- **Parrot Os**

☠ **Yeniden kurmak için şu komutu kullanabiliriz**

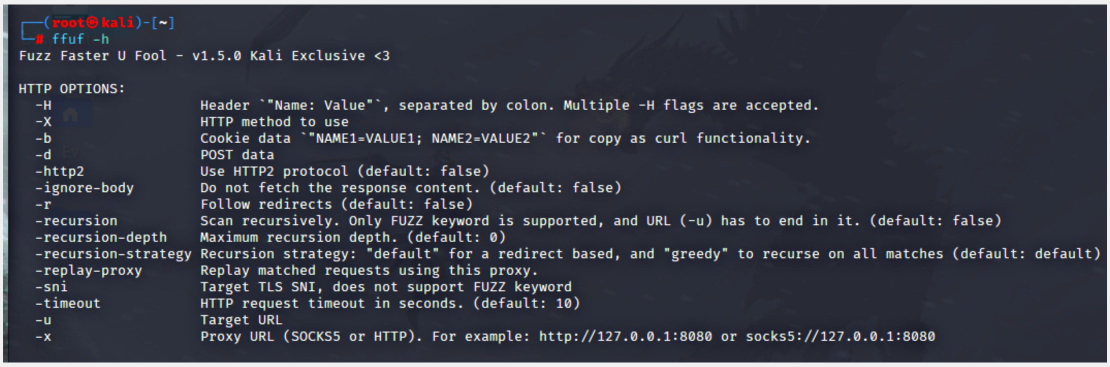
- **sudo apt-get install ffuf**

☠ **Versiyon hakkında bilgi sahibi olabilmek için**

- **ffuf -V**

☠ **Sahip olduğu tüm parametreleri görmek için**

- **ffuf -h**



```
┌──(root㉿kali)-[~]
└─# ffuf -h
Fuzz Faster U Fool - v1.5.0 Kali Exclusive <3

HTTP OPTIONS:
  -H                  Header `"Name: Value"`, separated by colon. Multiple -H flags are accepted.
  -X                  HTTP method to use
  -b                  Cookie data `"NAME1=VALUE1; NAME2=VALUE2"` for copy as curl functionality.
  -d                  POST data
  -http2              Use HTTP2 protocol (default: false)
  -ignore-body        Do not fetch the response content. (default: false)
  -r                  Follow redirects (default: false)
  -recursion          Scan recursively. Only FUZZ keyword is supported, and URL (-u) has to end in it. (default: false)
  -recursion-depth    Maximum recursion depth. (default: 0)
  -recursion-strategy Recursion strategy: "default" for a redirect based, and "greedy" to recurse on all matches (default: default)
  -replay-proxy       Replay matched requests using this proxy.
  -sni                Target TLS SNI, does not support FUZZ keyword
  -timeout            HTTP request timeout in seconds. (default: 10)
  -u                  Target URL
  -x                  Proxy URL (SOCKS5 or HTTP). For example: http://127.0.0.1:8080 or socks5://127.0.0.1:8080
```

Ffuf Parametreleri

HTTP OPTIONS:

☠ **-H Header `"Name: Value"`, separated by colon. Multiple -H flags are accepted.**

☠ **-X HTTP method to use**

-b Cookie data `"NAME1=VALUE1; NAME2=VALUE2"` for copy as curl functionality.

☠ **-d POST data**

☠ **-http2 Use HTTP2 protocol (default: false)**

☠ **-ignore-body Do not fetch the response content. (default: false)**

☠ **-r Follow redirects (default: false)**

☠ **-recursion Scan recursively. Only FUZZ keyword is supported, and URL (-u) has to end in it. (default: false)**

☠ **-recursion-depth Maximum recursion depth. (default: 0)**

☠ **-recursion-strategy Recursion strategy: "default" for a redirect based, and "greedy" to recurse on all matches (default: default)**

```
☠-replay-proxy      Replay matched requests using this proxy.
☠ -sni              Target TLS SNI, does not support FUZZ keyword
☠ -timeout          HTTP request timeout in seconds. (default: 10)
☠ -u                Target URL
☠ -x                Proxy URL (SOCKS5 or HTTP). For example: http://127.0.0.1:8080 or
 socks5://127.0.0.1:8080


 GENERAL OPTIONS:
☠ -V                Show version information. (default: false)
☠ -ac               Automatically calibrate filtering options (default: false)
☠ -acc              Custom auto-calibration string. Can be used multiple times. Implies -ac
☠ -ach              Per host autocalibration (default: false)
☠ -ack              Autocalibration keyword (default: FUZZ)
☠ -acs              Autocalibration strategy: "basic" or "advanced" (default: basic)
☠ -c                Colorize output. (default: false)
☠ -config           Load configuration from a file
☠ -json             JSON output, printing newline-delimited JSON records (default: false)
☠ -maxtime          Maximum running time in seconds for entire process. (default: 0)
☠ -maxtime-job      Maximum running time in seconds per job. (default: 0)
☠ -noninteractive   Disable the interactive console functionality (default: false)
☠ -p                Seconds of `delay` between requests, or a range of random delay. For
 example "0.1" or "0.1-2.0"
☠ -rate             Rate of requests per second (default: 0)
☠ -s                Do not print additional information (silent mode) (default: false)
☠ -sa               Stop on all error cases. Implies -sf and -se. (default: false)
☠ -se               Stop on spurious errors (default: false)
☠ -sf               Stop when > 95% of responses return 403 Forbidden (default: false)
☠ -t                Number of concurrent threads. (default: 40)
☠ -v                Verbose output, printing full URL and redirect location (if any) with the results.
 (default: false)
```

MATCHER OPTIONS:

- -mc Match HTTP status codes, or "all" for everything. (default: 200,204,301,302,307,401,403,405,500)
- -ml Match amount of lines in response
- -mmode Matcher set operator. Either of: and, or (default: or)
- -mr Match regexp
- -ms Match HTTP response size
- -mt Match how many milliseconds to the first response byte, either greater or less than. EG: >100 or <100
- -mw Match amount of words in response

FILTER OPTIONS:

- -fc Filter HTTP status codes from response. Comma separated list of codes and ranges
- -fl Filter by amount of lines in response. Comma separated list of line counts and ranges
- -fmode Filter set operator. Either of: and, or (default: or)
- -fr Filter regexp
- -fs Filter HTTP response size. Comma separated list of sizes and ranges
- -ft Filter by number of milliseconds to the first response byte, either greater or less than. EG: >100 or <100
- -fw Filter by amount of words in response. Comma separated list of word counts and ranges

INPUT OPTIONS:

- -D DirSearch wordlist compatibility mode. Used in conjunction with -e flag. (default: false)
- -e Comma separated list of extensions. Extends FUZZ keyword.
- -ic Ignore wordlist comments (default: false)
- -input-cmd Command producing the input. --input-num is required when using this input method. Overrides -w.
- -input-num Number of inputs to test. Used in conjunction with --input-cmd. (default: 100)
- -input-shell Shell to be used for running command
- -mode Multi-wordlist operation mode. Available modes: clusterbomb, pitchfork, sniper (default: clusterbomb)
- -request File containing the raw http request
- -request-proto Protocol to use along with raw request (default: https)
- -w Wordlist file path and (optional) keyword separated by colon. eg. '/path/to/wordlist:KEYWORD'

OUTPUT OPTIONS:

☠-debug-log Write all of the internal logging to the specified file.

☠-o Write output to file

☠-od Directory path to store matched results to.

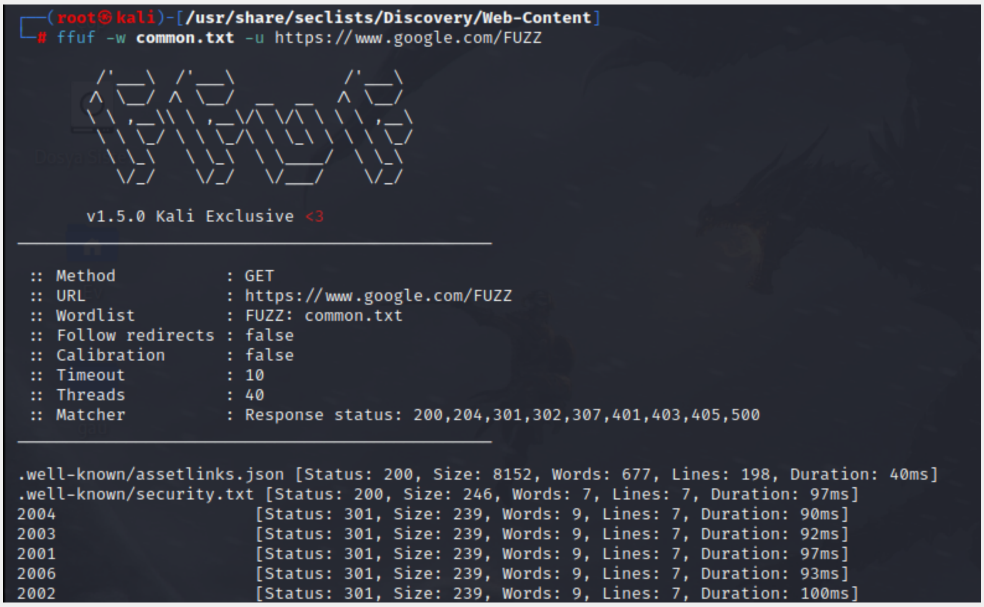
☠-of Output file format. Available formats: json, ejson, html, md, csv, ecsv (or, 'all' for all formats) (default: json)

☠-or Don't create the output file if we don't have results (default: false)

Örnek Komutlar

Web sitesini taramak için brute force kullanır

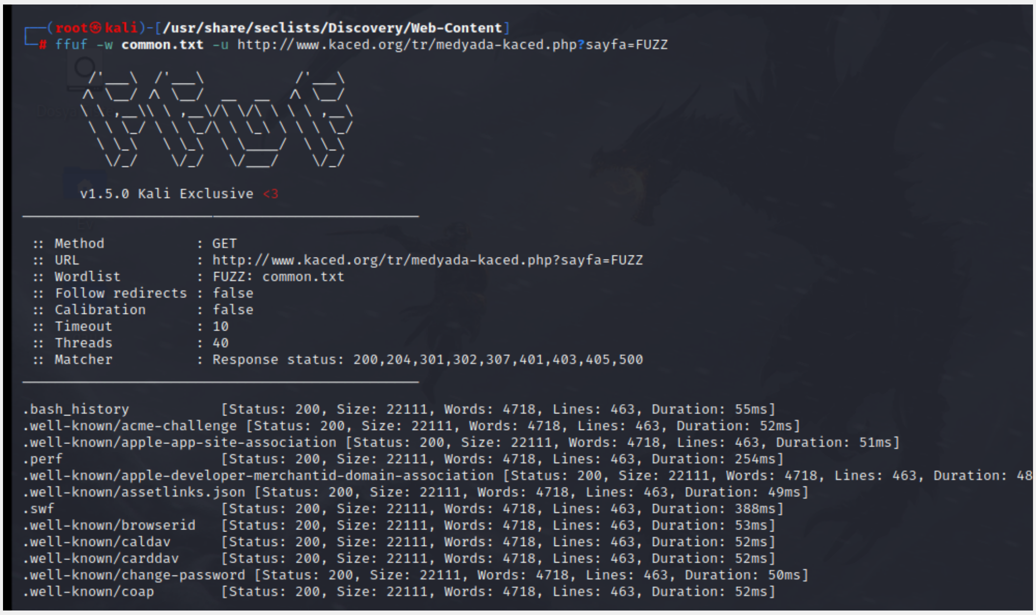
☠ ffuf -w <path-wordlist> -u https://test-url/FUZZ



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u https://www.google.com/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : https://www.google.com/FUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.well-known/assetlinks.json [Status: 200, Size: 8152, Words: 677, Lines: 198, Duration: 40ms]
.well-known/security.txt [Status: 200, Size: 246, Words: 7, Lines: 7, Duration: 97ms]
2004                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 90ms]
2003                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 92ms]
2001                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 97ms]
2006                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 93ms]
2002                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 100ms]
```

id parametresini taramak için fuzz kullanırız

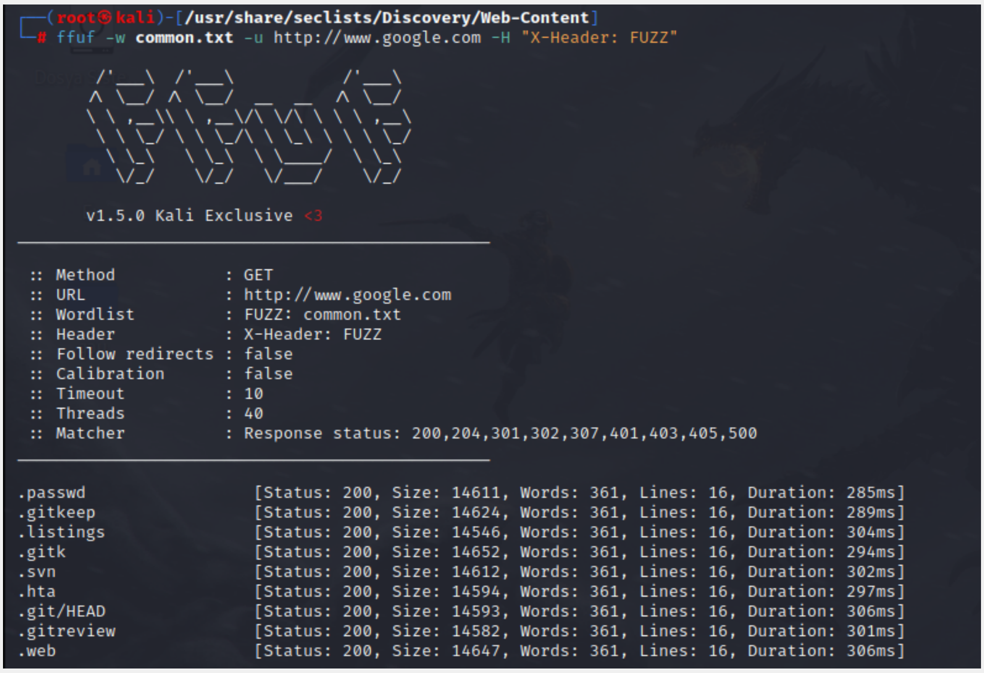
☠ ffuf -w <path-wordlist> -u https://test-url?id=FUZZ



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.kaced.org/tr/medyada-kaced.php?sayfa=FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://www.kaced.org/tr/medyada-kaced.php?sayfa=FUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.bash_history           [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 55ms]
.well-known/acme-challenge [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 52ms]
.well-known/apple-app-site-association [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 51ms]
.perf                   [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 254ms]
.well-known/apple-developer-merchantid-domain-association [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 48
.well-known/assetlinks.json [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 49ms]
.swf                    [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 388ms]
.well-known/browserid   [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 53ms]
.well-known/caldav      [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 52ms]
.well-known/carddav     [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 52ms]
.well-known/change-password [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 50ms]
.well-known/coap        [Status: 200, Size: 22111, Words: 4718, Lines: 463, Duration: 52ms]
```

Header taramak için bu parametre kullanılabilir

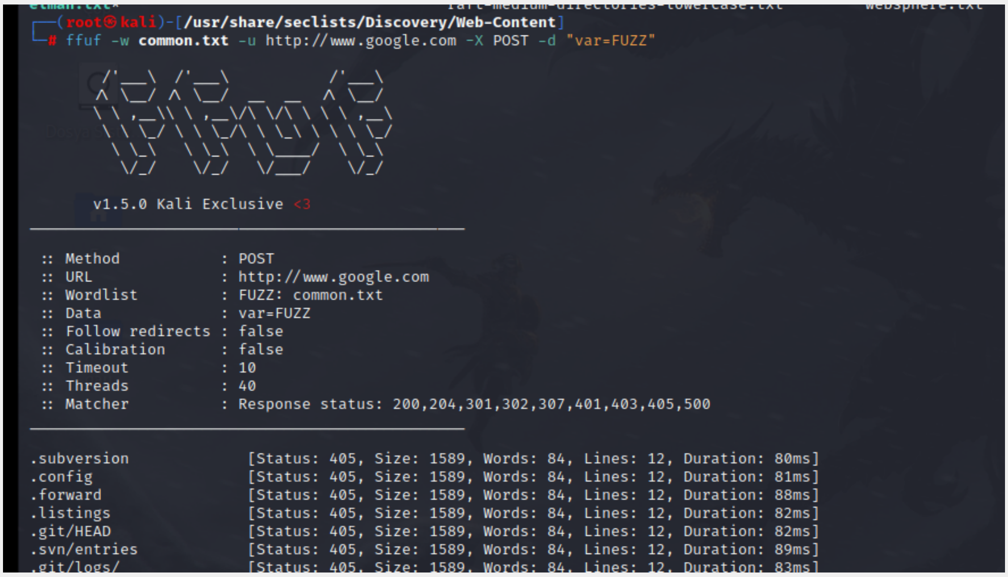
ffuf -w <path-wordlist> -u https://test-url -H "X-Header: FUZZ"



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com -H "X-Header: FUZZ"

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://www.google.com
 :: Wordlist         : FUZZ: common.txt
 :: Header           : X-Header: FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.passwd                 [Status: 200, Size: 14611, Words: 361, Lines: 16, Duration: 285ms]
.gitkeep                [Status: 200, Size: 14624, Words: 361, Lines: 16, Duration: 289ms]
.listings               [Status: 200, Size: 14546, Words: 361, Lines: 16, Duration: 304ms]
.gitk                   [Status: 200, Size: 14652, Words: 361, Lines: 16, Duration: 294ms]
.svn                    [Status: 200, Size: 14612, Words: 361, Lines: 16, Duration: 302ms]
.hta                    [Status: 200, Size: 14594, Words: 361, Lines: 16, Duration: 297ms]
.git/HEAD               [Status: 200, Size: 14593, Words: 361, Lines: 16, Duration: 306ms]
.gitreview              [Status: 200, Size: 14582, Words: 361, Lines: 16, Duration: 301ms]
.web                    [Status: 200, Size: 14647, Words: 361, Lines: 16, Duration: 306ms]
```

URL'yi POST yöntemiyle taramak için

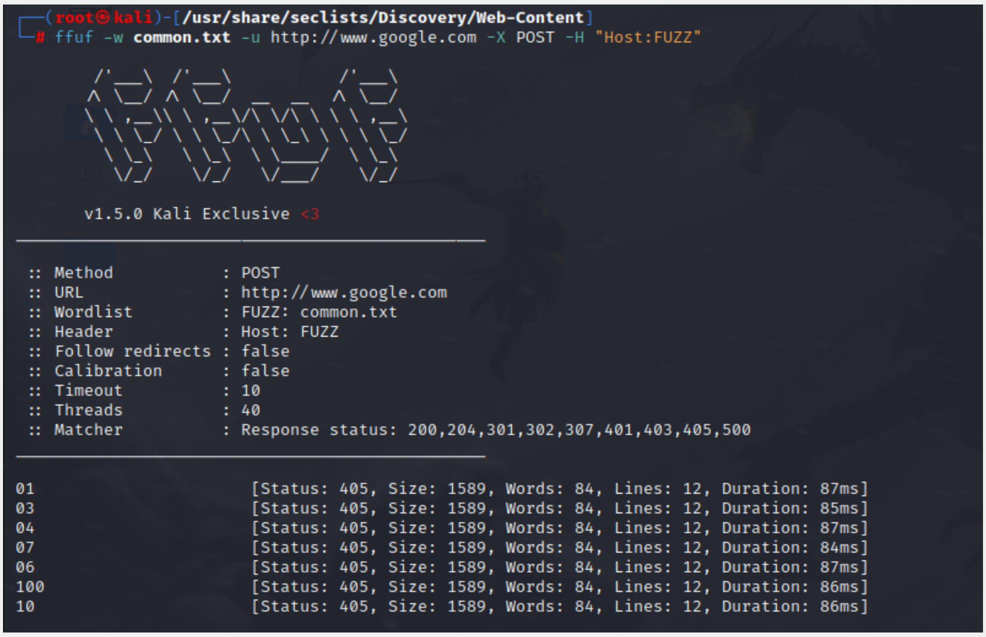
ffuf -w <path-wordlist> -u https://test-url -X POST -d "var=FUZZ"



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com -X POST -d "var=FUZZ"

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : POST
 :: URL              : http://www.google.com
 :: Wordlist         : FUZZ: common.txt
 :: Data             : var=FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.subversion             [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 80ms]
.config                 [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 81ms]
.forward                [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 88ms]
.listings               [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 82ms]
.git/HEAD               [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 82ms]
.svn/entries            [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 89ms]
.git/logs/              [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 83ms]
```

☠️ Vhost listesi taramak için

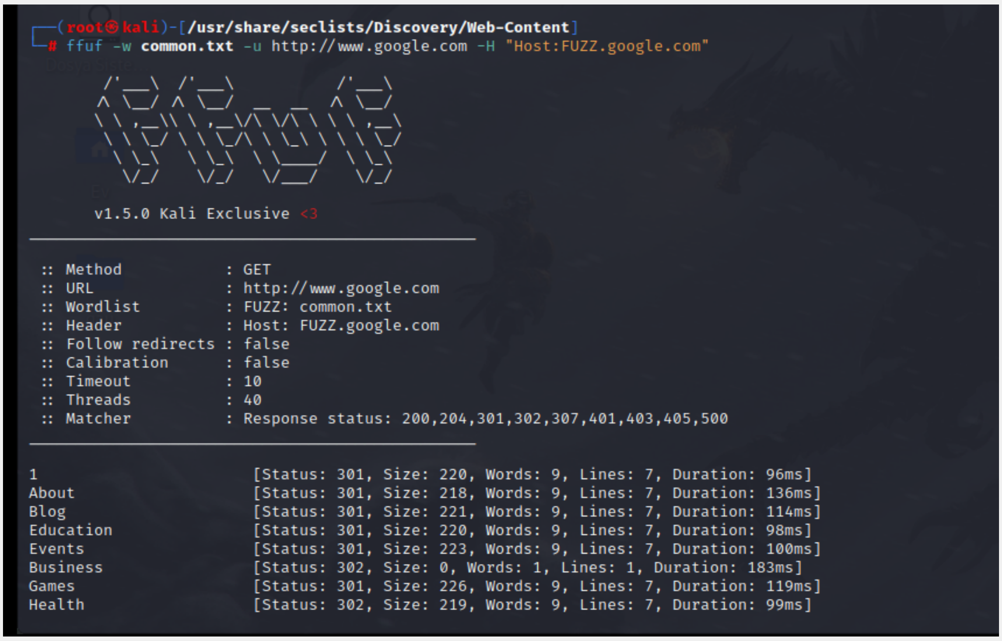
ffuf -w <path-vhosts> -u https://test-url -H "Host: FUZZ"



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com -X POST -H "Host:FUZZ"

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : POST
 :: URL              : http://www.google.com
 :: Wordlist         : FUZZ: common.txt
 :: Header           : Host: FUZZ
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

01                      [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 87ms]
03                      [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 85ms]
04                      [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 87ms]
07                      [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 84ms]
06                      [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 87ms]
100                     [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 86ms]
10                      [Status: 405, Size: 1589, Words: 84, Lines: 12, Duration: 86ms]
```

☠️ DNS kayıtları olmayan alt etki alanlarını bulmak için

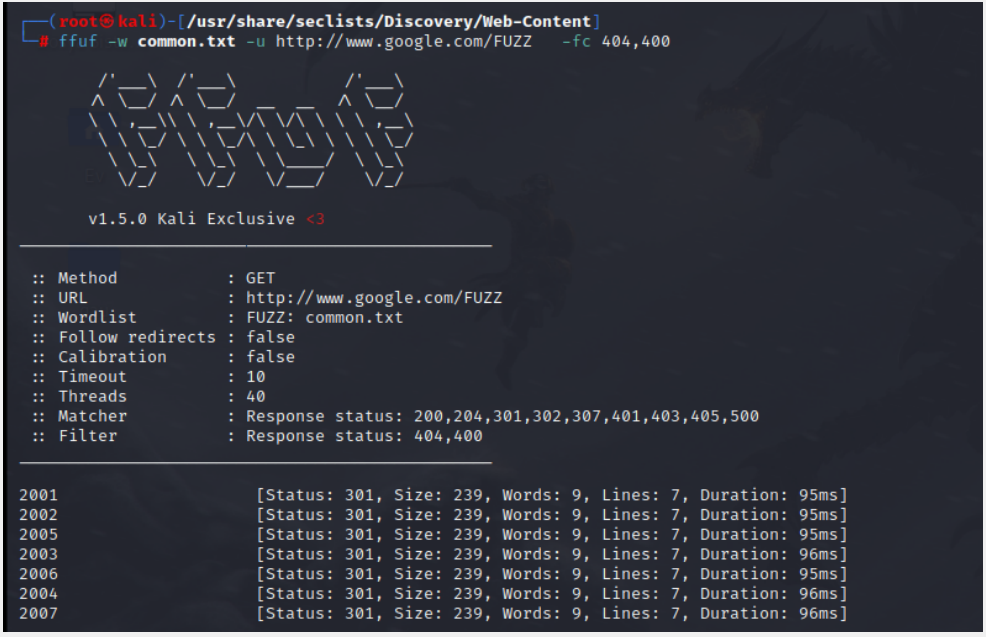
ffuf -w <path-wordlist> -u https://test-url/ -H "Host: FUZZ.site.com"



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com -H "Host:FUZZ.google.com"

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://www.google.com
 :: Wordlist         : FUZZ: common.txt
 :: Header           : Host: FUZZ.google.com
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

1                       [Status: 301, Size: 220, Words: 9, Lines: 7, Duration: 96ms]
About                   [Status: 301, Size: 218, Words: 9, Lines: 7, Duration: 136ms]
Blog                    [Status: 301, Size: 221, Words: 9, Lines: 7, Duration: 114ms]
Education               [Status: 301, Size: 220, Words: 9, Lines: 7, Duration: 98ms]
Events                  [Status: 301, Size: 223, Words: 9, Lines: 7, Duration: 100ms]
Business                [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 183ms]
Games                   [Status: 301, Size: 226, Words: 9, Lines: 7, Duration: 119ms]
Health                  [Status: 302, Size: 219, Words: 9, Lines: 7, Duration: 99ms]
```

☠️ **Durum koduna göre filtrelemek için**

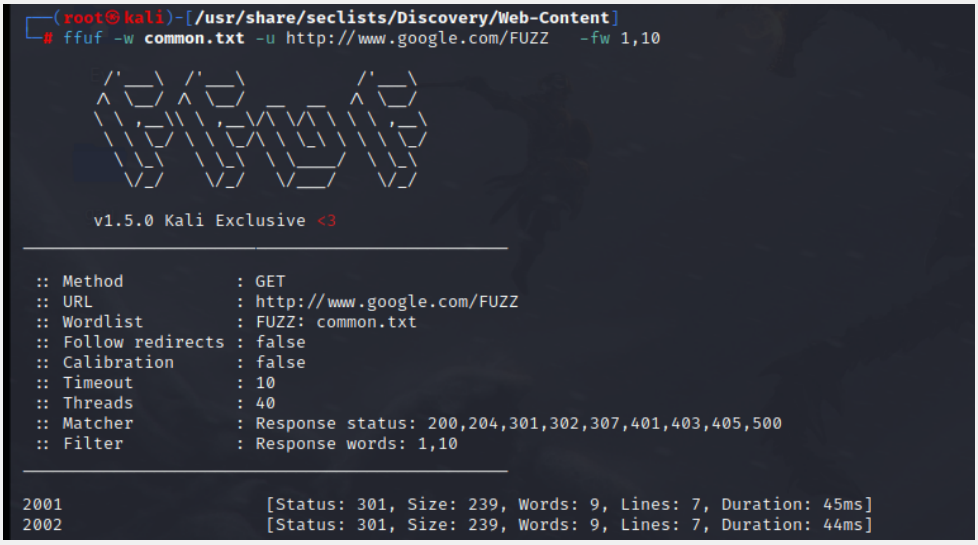
ffuf -w <path-wordlist> -u https://test-url/FUZZ -fc 404,400



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com/FUZZ   -fc 404,400

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://www.google.com/FUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response status: 404,400
________________________________________________

2001                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 95ms]
2002                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 95ms]
2005                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 95ms]
2003                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 96ms]
2006                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 95ms]
2004                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 96ms]
2007                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 96ms]
```

☠️ **Kelimelerin miktarına göre filtrelemek için**

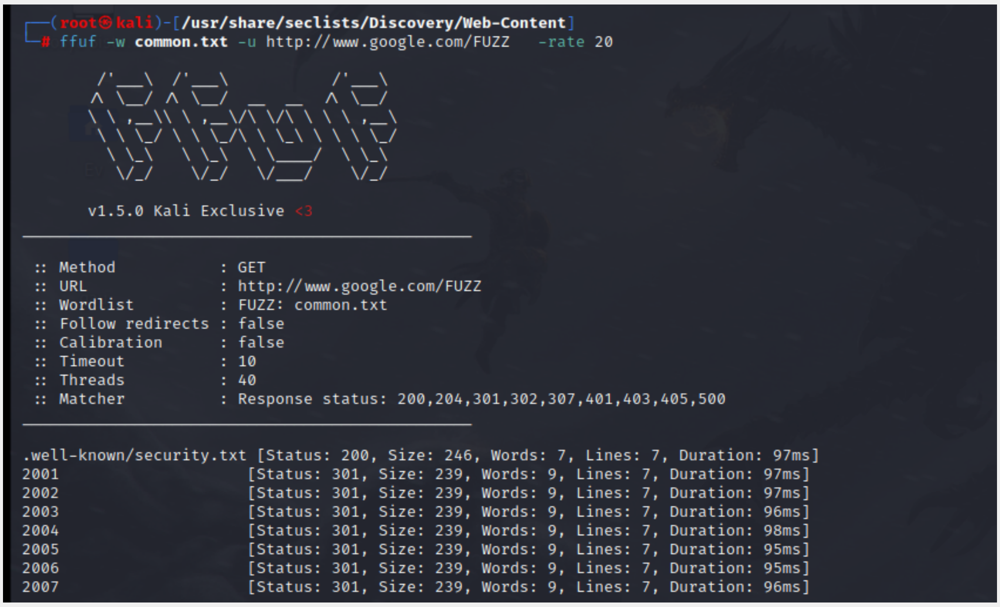
ffuf -w <path-wordlist> -u https://test-url/FUZZ -fw <amount-of-words>



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com/FUZZ   -fw 1,10

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://www.google.com/FUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response words: 1,10
________________________________________________

2001                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 45ms]
2002                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 44ms]
```

☠️ **Paket gönderme hızını kontrol etmek için**

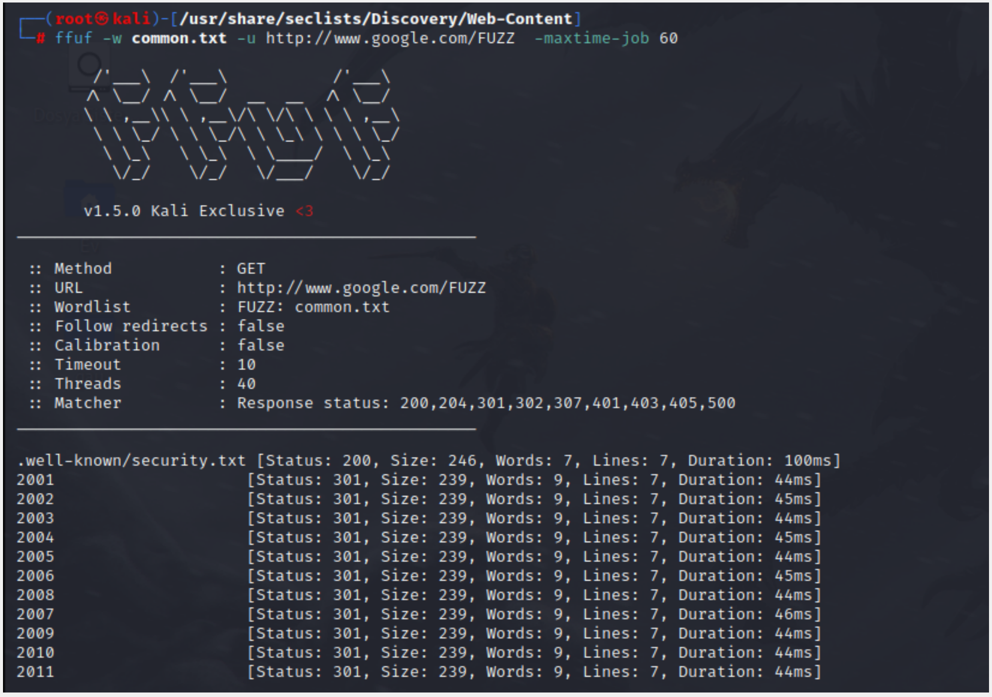
ffuf -w <path-wordlist> -u https://test-url/FUZZ -rate <rate-of-sending-packets>



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com/FUZZ  -rate 20

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://www.google.com/FUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.well-known/security.txt [Status: 200, Size: 246, Words: 7, Lines: 7, Duration: 97ms]
2001                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 97ms]
2002                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 97ms]
2003                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 96ms]
2004                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 98ms]
2005                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 95ms]
2006                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 95ms]
2007                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 96ms]
```

☠️ **Taramayı belirli bir süre veya belirli bir süreden daha kısa süre (saniye cinsinden) çalıştırmak için**

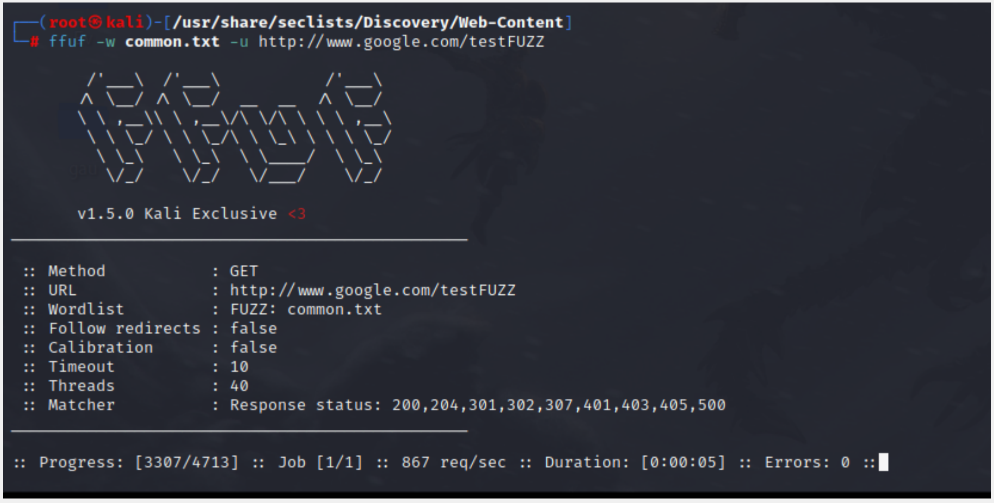
ffuf -w <path-wordlist> -u https://test-url/FUZZ -maxtime-job 60



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com/FUZZ  -maxtime-job 60

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://www.google.com/FUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.well-known/security.txt [Status: 200, Size: 246, Words: 7, Lines: 7, Duration: 100ms]
2001                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 44ms]
2002                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 45ms]
2003                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 44ms]
2004                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 45ms]
2005                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 44ms]
2006                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 45ms]
2008                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 44ms]
2007                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 46ms]
2009                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 44ms]
2010                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 44ms]
2011                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 44ms]
```

☠️ **Bellli bir urlden sonraki gelebilecek uzantıları taramak için**

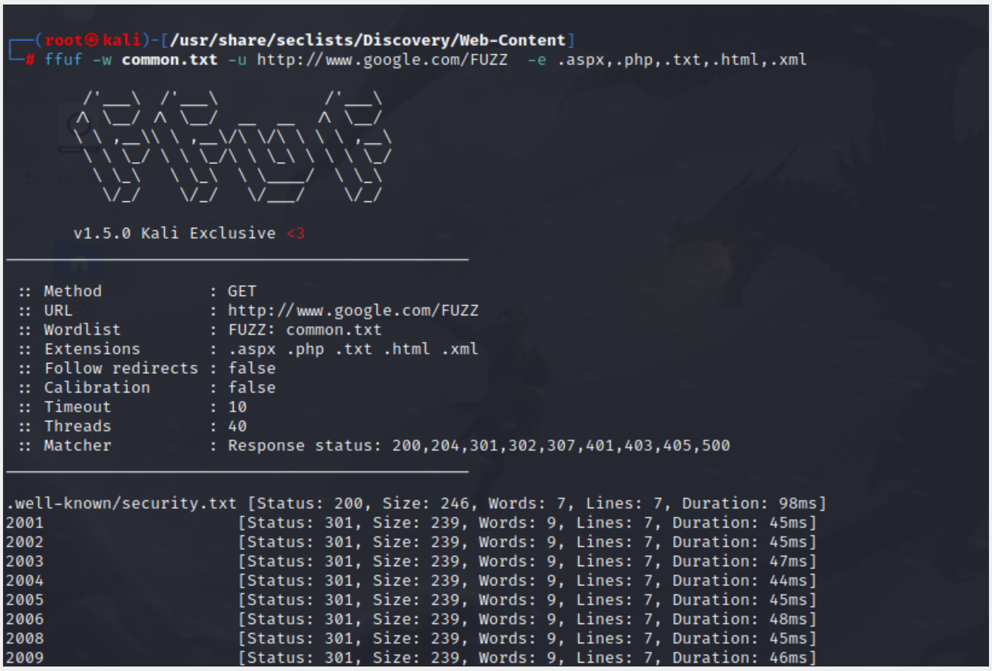
ffuf -w <path-wordlist> -u https://test-url/testFUZZ



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com/testFUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://www.google.com/testFUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

:: Progress: [3307/4713] :: Job [1/1] :: 867 req/sec :: Duration: [0:00:05] :: Errors: 0 ::
```

☠️ **Belirli uzantılara sahip dosya bulma**

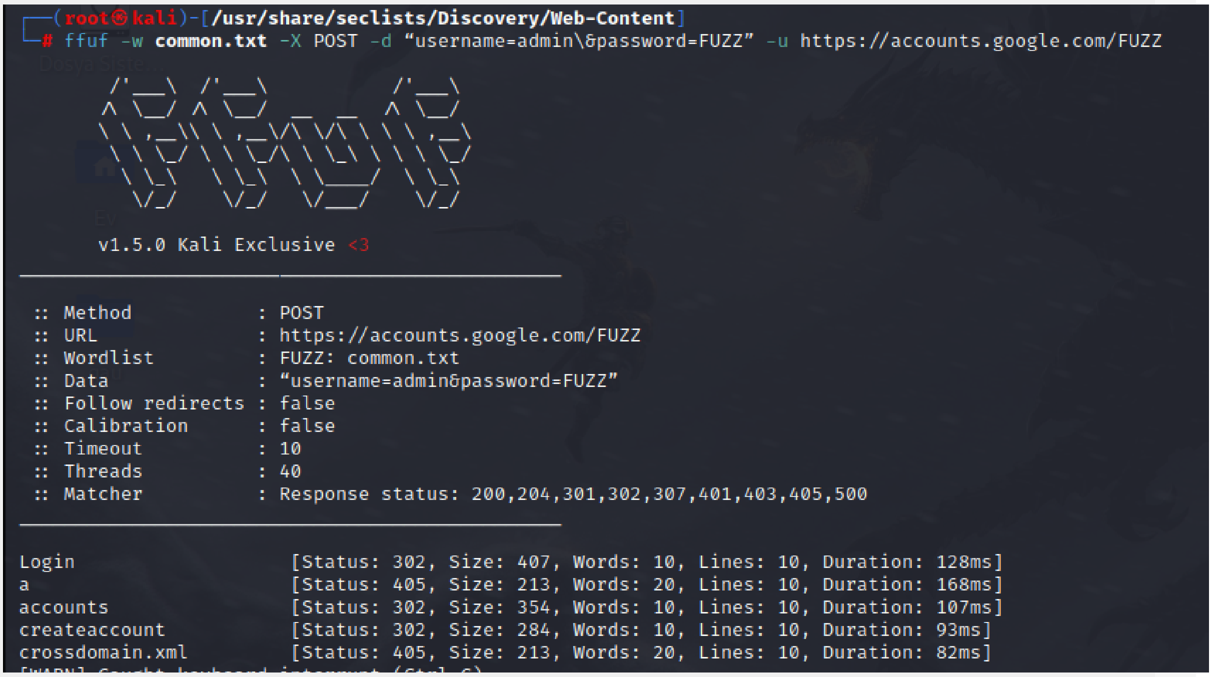
ffuf -w <path-wordlist> -u http://test-url/FUZZ -e .aspx,.php,.txt,.html



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com/FUZZ  -e .aspx,.php,.txt,.html,.xml

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://www.google.com/FUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Extensions       : .aspx .php .txt .html .xml
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.well-known/security.txt [Status: 200, Size: 246, Words: 7, Lines: 7, Duration: 98ms]
2001                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 45ms]
2002                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 45ms]
2003                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 47ms]
2004                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 44ms]
2005                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 45ms]
2006                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 48ms]
2008                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 45ms]
2009                    [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 46ms]
```

☠️ **Fuzz verileriyle POST isteği göndermek için**

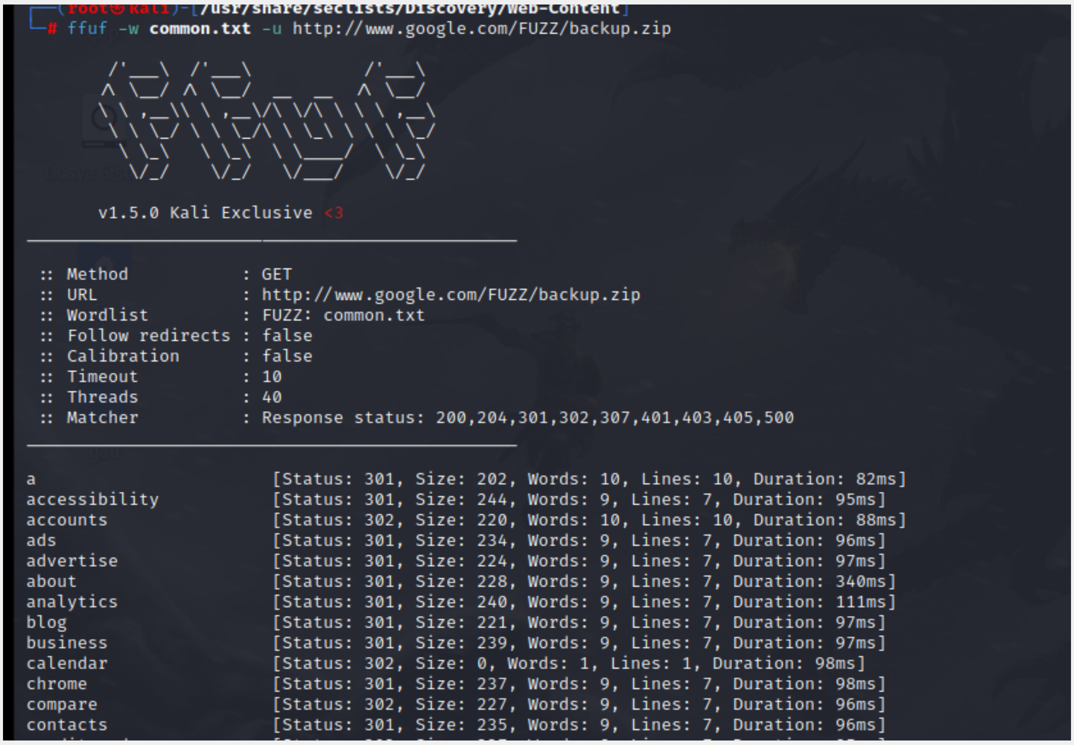
ffuf -w <path-wordlist> -X POST -d “username=admin\&password=FUZZ” -u http://test-url/FUZZ



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -X POST -d “username=admin\&password=FUZZ” -u https://accounts.google.com/FUZZ

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : POST
 :: URL              : https://accounts.google.com/FUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Data             : “username=admin&password=FUZZ”
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

Login                   [Status: 302, Size: 407, Words: 10, Lines: 10, Duration: 128ms]
a                       [Status: 405, Size: 213, Words: 20, Lines: 10, Duration: 168ms]
accounts                [Status: 302, Size: 354, Words: 10, Lines: 10, Duration: 107ms]
createaccount           [Status: 302, Size: 284, Words: 10, Lines: 10, Duration: 93ms]
crossdomain.xml         [Status: 405, Size: 213, Words: 20, Lines: 10, Duration: 82ms]
[WARN] Caught keyboard interrupt (Ctrl-C)
```

☠️ **Dizinden sonra belirli formattaki dosyayı taramak için**

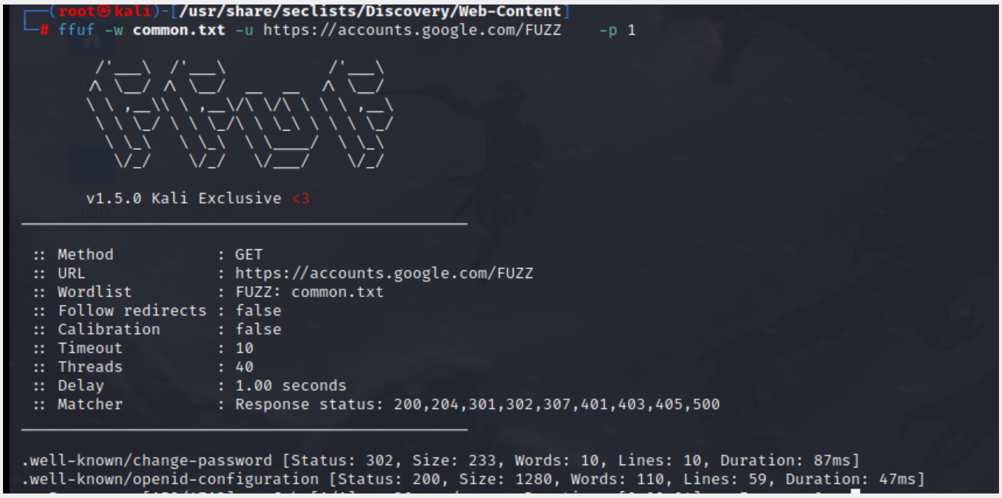
ffuf -w <path-wordlist> -u http://test-url/FUZZ/backup.zip



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u http://www.google.com/FUZZ/backup.zip

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://www.google.com/FUZZ/backup.zip
 :: Wordlist         : FUZZ: common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

a                       [Status: 301, Size: 202, Words: 10, Lines: 10, Duration: 82ms]
accessibility           [Status: 301, Size: 244, Words: 9, Lines: 7, Duration: 95ms]
accounts                [Status: 302, Size: 220, Words: 10, Lines: 10, Duration: 88ms]
ads                     [Status: 301, Size: 234, Words: 9, Lines: 7, Duration: 96ms]
advertise               [Status: 301, Size: 224, Words: 9, Lines: 7, Duration: 97ms]
about                   [Status: 301, Size: 228, Words: 9, Lines: 7, Duration: 340ms]
analytics               [Status: 301, Size: 240, Words: 9, Lines: 7, Duration: 111ms]
blog                    [Status: 301, Size: 221, Words: 9, Lines: 7, Duration: 97ms]
business                [Status: 301, Size: 239, Words: 9, Lines: 7, Duration: 97ms]
calendar                [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 98ms]
chrome                  [Status: 301, Size: 237, Words: 9, Lines: 7, Duration: 98ms]
compare                 [Status: 302, Size: 227, Words: 9, Lines: 7, Duration: 96ms]
contacts                [Status: 301, Size: 235, Words: 9, Lines: 7, Duration: 96ms]
```

☠ -p kullanarak gecikmeyi saniye türünden ayarlayabiliriz

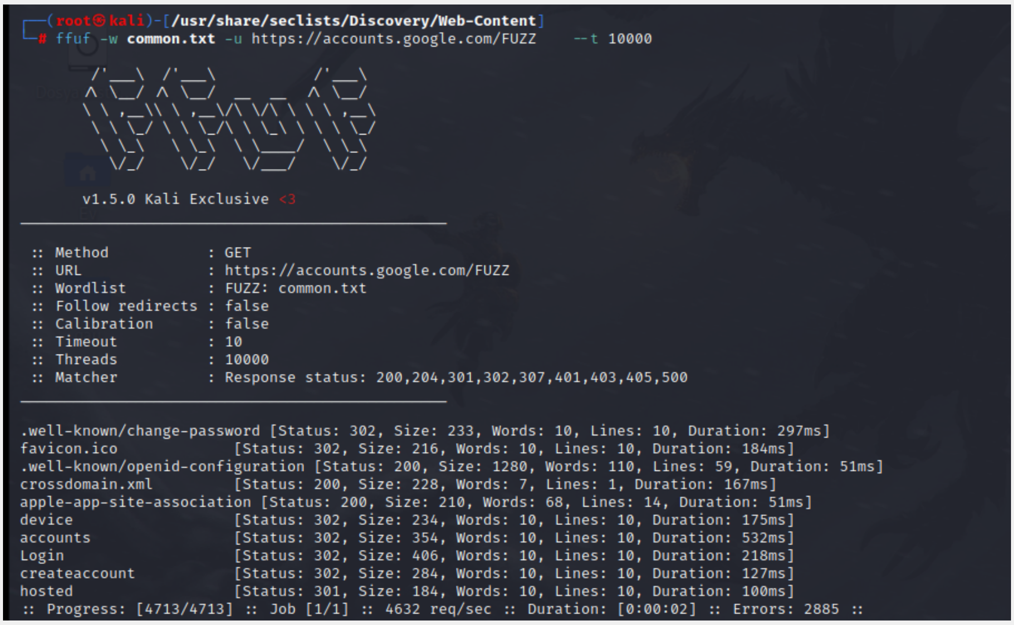
ffuf -u http://test-url/FUZZ/ -w <path-wordlist> -p 1



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u https://accounts.google.com/FUZZ    -p 1

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : https://accounts.google.com/FUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Delay            : 1.00 seconds
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.well-known/change-password [Status: 302, Size: 233, Words: 10, Lines: 10, Duration: 87ms]
.well-known/openid-configuration [Status: 200, Size: 1280, Words: 110, Lines: 59, Duration: 47ms]
```

☠ -T kullanarak taramayı hızlandırmak veya yavaşlatmak (default değer 40'tır)

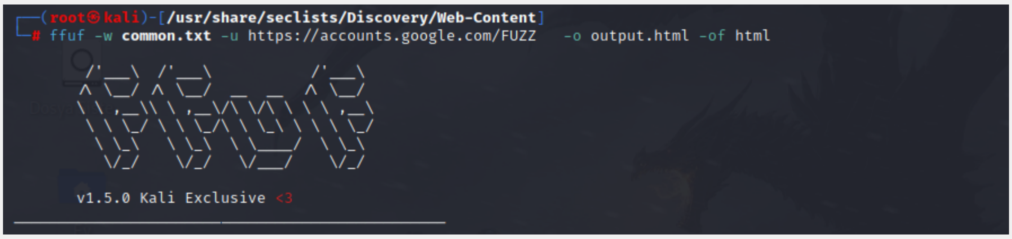
ffuf -u http://test-url/FUZZ/ -w <path-wordlist> -t 1000



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u https://accounts.google.com/FUZZ    --t 10000

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : https://accounts.google.com/FUZZ
 :: Wordlist         : FUZZ: common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 10000
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

.well-known/change-password [Status: 302, Size: 233, Words: 10, Lines: 10, Duration: 297ms]
favicon.ico             [Status: 302, Size: 216, Words: 10, Lines: 10, Duration: 184ms]
.well-known/openid-configuration [Status: 200, Size: 1280, Words: 110, Lines: 59, Duration: 51ms]
crossdomain.xml         [Status: 200, Size: 228, Words: 7, Lines: 1, Duration: 167ms]
apple-app-site-association [Status: 200, Size: 210, Words: 68, Lines: 14, Duration: 51ms]
device                  [Status: 302, Size: 234, Words: 10, Lines: 10, Duration: 175ms]
accounts                [Status: 302, Size: 354, Words: 10, Lines: 10, Duration: 532ms]
Login                   [Status: 302, Size: 406, Words: 10, Lines: 10, Duration: 218ms]
createaccount           [Status: 302, Size: 284, Words: 10, Lines: 10, Duration: 127ms]
hosted                  [Status: 301, Size: 184, Words: 10, Lines: 10, Duration: 100ms]
:: Progress: [4713/4713] :: Job [1/1] :: 4632 req/sec :: Duration: [0:00:02] :: Errors: 2885 ::
```

☠ Çıktıyı -o ve format -of kullanarak kaydetmek için

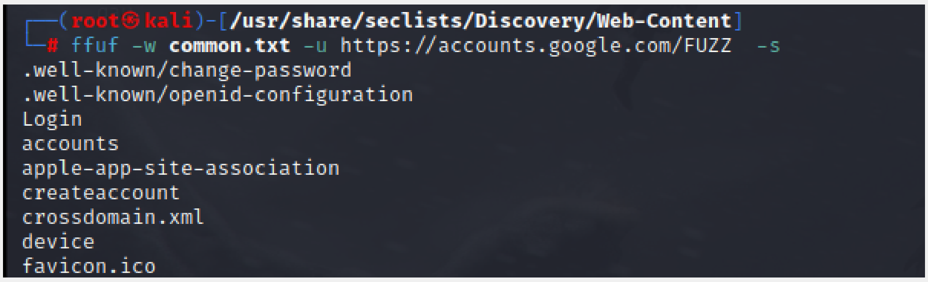
ffuf -u https://test-url/FUZZ/ -w <path-wordlist> -o output.html -of html



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u https://accounts.google.com/FUZZ    -o output.html -of html

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.5.0 Kali Exclusive <3
________________________________________________
```

☠️ **Taramayı sessiz modda çalıştırmak için**

ffuf -u https://test-url/FUZZ -w <path-wordlist> -s



```
┌──(root㉿kali)-[/usr/share/seclists/Discovery/Web-Content]
└─# ffuf -w common.txt -u https://accounts.google.com/FUZZ  -s
.well-known/change-password
.well-known/openid-configuration
Login
accounts
apple-app-site-association
createaccount
crossdomain.xml
device
favicon.ico
```