

1.WAFW00F

git- <https://github.com/EnableSecurity/wafw00f>

וואף וואף זה הוא סקריפט פייתון שמאפשר לנו לזהות איזה WAF האתר/שרת שאנו מנסים לחדור אליו משתמש וככה אנו בתור תוקפים יכולים לתכנן את הארסנל תקיפה שלנו בצורה טובה יותר ונוכל לדעת באיזה כלים להשתמש.

הואף וואף עובד כך:

-הוא שולח בקשת HTTP ומנתח את התשובה שלו וככה הוא מגלה האם יש לו וואף
-במידה וזה לא עובד הוא שולח מספר בקשות HTTP (יש סיכוי שחלקם זדוניות) ואז בהתאם

לתגובה הוא מחליט איזה וואף זה

-במידה וזה גם לא הצליח זה מנתח את התגובות שהוא קיבל בעבר ומשתמש באלגוריתם בשביל לבדוק האם יש וואף או מרכיב אחר שחוסם את הבקשות.

בשביל להפעיל את WAFW00F נצטרך דבר ראשון להתקין אותו

בנוסף אפשר לראות מאיפה הבקשה נשלח אז במידה ונרצה אנונימיות נוכל לעשות למצנו תוריפי או להשתמש בפרוקסי (יש אפשרות בילד אין בתוכנה)

התקנה:

בשביל להתקין אנו נכנס למכשיר לינוקס שלנו ונרשום את הפקודה הבאה

```
sudo apt-get install wafw00f
```

ובמידה ופייתון לא מותקן נצטרך לרשום את הפקודה הבאה קודם

```
python setup.py install
```

במידה ונרצה להריץ את זה על וינדוס יש צורך שפייתון יהיה מותקן

ואז ללכת לגיט ולהתקין אותו

או במידה ואתם משתמשים בקאלי לינוקס אז זה מגיע בילט אין בתוך המערכת.

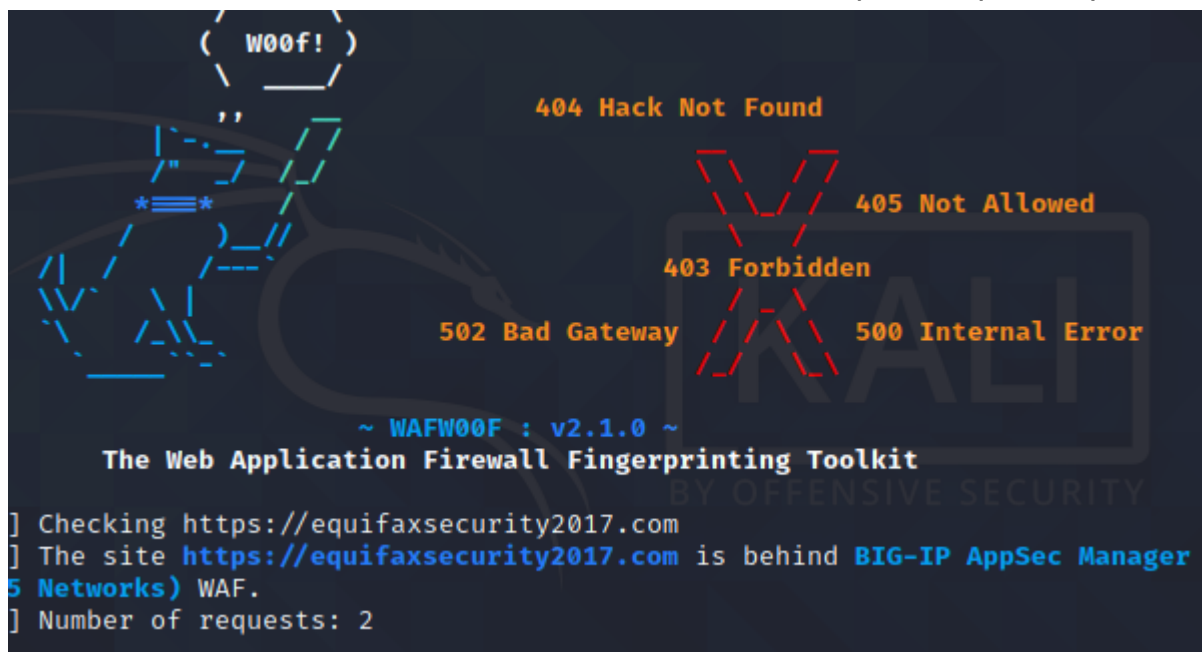
שימוש: בשביל להשתמש בוואףווף אנו פשוט נרשום wafw00f ואת הכתובת של האתר שאנו רוצים לבדוק

לדוגמא כאן אנו נבדוק את האתר [Home](https://equifaxsecurity2017.com)

השתמשתי באתר הזה מכיוון שהוא כבר לא פעיל ולא מתוחזק

```
(root@kali)-[~]  
# wafw00f equifaxsecurity2017.com
```

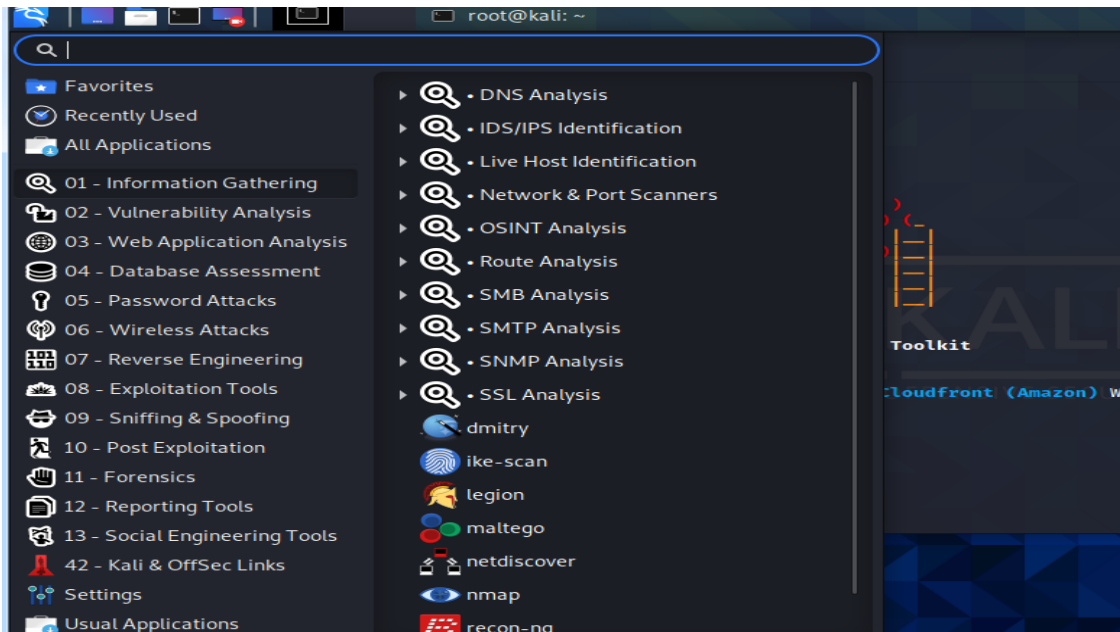
לאחר מכן אנו נלחץ אנטר ונקבל דבר דומה ל:



```
( w00f! )  
404 Hack Not Found  
405 Not Allowed  
403 Forbidden  
502 Bad Gateway  
500 Internal Error  
~ WAFW00F : v2.1.0 ~  
The Web Application Firewall Fingerprinting Toolkit  
] Checking https://equifaxsecurity2017.com  
] The site https://equifaxsecurity2017.com is behind BIG-IP AppSec Manager  
5 Networks) WAF.  
] Number of requests: 2
```

כמו שאפשר לראות הוא בודק את האתר ולאחר מכן הוא אומר לנו שהאתר נמצא מאחורי WAF מסוג big-ip של חברת 5 networks או שלקח לו 2 ריקוסטים בשביל לקבל את המידע הזה. כמו כן אפשר לראות שחלק מהבקשות שלנו לא הצליחו ולמה הם לא הצליחו אבל הוא כן הצליח למצוא את הפיירוול הנדרש

כמו-כן אפשר להגיע לוואףווף באמצעות לחיצה על הסימן של קאלי למעלה לאחר מכן על אינפורמיישן גאטרנינג ואז על IDS/IPS IDEN ושם אפשר למצוא את וואף ווף



במידה ונחליט להכנס אל WAW00F משם זה פשוט עושה אקסקיוט לסקריפט שמריץ את WAFW00F -H שבאמצעותו אנו נקבל מידע על כל הפיצרים שנמצאים לנו שם בנוסף הדגמה על איך להשתמש בתוכנה

```
root@kali: ~  
File Actions Edit View Help  
> Executing "wafw00f -h"  
Usage: wafw00f url1 [url2 [url3 ... ]]  
example: wafw00f http://www.victim.org/  
  
Options:  
-h, --help                show this help message and exit  
-v, --verbose              Enable verbosity, multiple -v options increase  
                           verbosity  
-a, --findall              Find all WAFs which match the signatures, do not stop  
                           testing on the first one  
-r, --noredirect            Do not follow redirections given by 3xx responses  
-t TEST, --test=TEST       Test for one specific WAF  
-o OUTPUT, --output=OUTPUT Write output to csv, json or text file depending on  
                           file extension. For stdout, specify - as filename.  
-i INPUT, --input-file=INPUT Read targets from a file. Input format can be csv,  
                           json or text. For csv and json, a 'url' column name o  
                           element is required.  
-l, --list                  List all WAFs that WAFW00F is able to detect  
-p PROXY, --proxy=PROXY    Use an HTTP proxy to perform requests, examples:  
                           http://hostname:8080, socks5://hostname:1080,  
                           http://user:pass@hostname:8080  
-V, --version               Print out the current version of WafW00f and exit.  
-H HEADERS, --headers=HEADERS
```

בנוסף חשוב לציין לפני שנעבור לשלב של הפקודות ומה הן עושות היא שוואףווף יודע לרחרח אך ורק WAFים אשר נמצאים ברשימה שלו את הרשימה אפשר למצוא בגיט מתחת לקבצים.

קישור לגיט: <https://github.com/EnableSecurity/wafw00f>

פקודות:

כלומר עזרה ובאמצעותו אפשר לראות איזה פקודות אפשר להשתמש בהם -HELP או -H
הדגמה לזה אפשר לראות למעלה ^

מכיל יותר מילים שמתארות את הוואף --verbose או -V
בודק את כל וואפים שנמצאים על האתר ולא מפסיק לבדוק ברגע שהוא מגיע לראשון ומחזיר -A
תוצאה, בנוסף זה גם נותן מידע נוסף על השרת שאפשר ללמוד ממנו לדוגמא:

```
~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://www.cloudflare.com
[+] The site https://www.cloudflare.com is behind Cloudflare (Cloudflare Inc.) WAF.
[+] Generic Detection results:
[*] The site https://www.cloudflare.com seems to be behind a WAF or some sort of security solution
[~] Reason: The server returns a different response code when an attack string is used.
Normal response code is "200", while the response code to cross-site scripting attack is "503"
[~] Number of requests: 5
```

מזה אפשר ללמוד שהשרת מחזיר תגובה שונה כשמנסים להשתמש בסטרינג של תקיפה, תגובה נורמאלית מחזירה את הקוד 200 ואילו תגובה לסטרינג של XSS זה 503.
אפשר לשלב את הפקודות -V ו-A בשביל לבדוק איזה פיירוולים יש ולקבל מידע עליהם לדוגמא:

```
(root@kali)-[~]
# wafw00f -a https://equifaxsecurity2017.com -vv
```

והתשובה שהתקבלה:

```
( Woof! )

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit

INFO:wafw00f:The url https://equifaxsecurity2017.com should start with http:// or https:// .. fixing (might make this unusable)
[*] Checking https://equifaxsecurity2017.com
INFO:wafw00f:starting wafw00f on https://equifaxsecurity2017.com
INFO:wafw00f:Request Succeeded
INFO:wafw00f:Request Succeeded
INFO:wafw00f:Checking for ACE XML Gateway (Cisco)
INFO:wafw00f:Checking for aeSecure (aeSecure)
INFO:wafw00f:Checking for AireeCDN (Airee)
INFO:wafw00f:Checking for Airlock (Phion/Ergon)
INFO:wafw00f:Checking for Alert Logic (Alert Logic)
```

```

INFO:wafw00f:Checking for ZScaler (Accenture)
INFO:wafw00f:Identified WAF: ['BIG-IP AppSec Manager (F5 Networks)', 'Instart
DX (Instart Logic)']
[+] The site https://equifaxsecurity2017.com is behind BIG-IP AppSec Manager
(F5 Networks) and/or Instart DX (Instart Logic) WAF.
[+] Generic Detection results:
INFO:wafw00f:Request Succeeded
INFO:wafw00f:Request Succeeded
INFO:wafw00f:Request Succeeded
INFO:wafw00f:Request Succeeded
INFO:wafw00f:Request Succeeded
[-] No WAF detected by the generic detection
[-] Number of requests: 7
INFO:wafw00f:Found: 3 matches.

```

בתמונה השניה אפשר לראות שהוא מצא וואפים את הסוג שלהם ואת כמות הוואפים שמגנים על השרת.

- בשרת XX לא עוקב אחרי הקידיירקט שמקבלים אם יש תגובה 302
- מראה לנו את הרשימה של הוואפים שוואף יודע למצוא תווים שלהם שמזהים איזה וואף זה
- בדיקה אחרי וואף ספציפי (מהרשימה) והאם הוא נמצא באתר הרלוונטי

לדוגמא

```

(root@kali)-[~]
# wafw00f -t BitNinja https://equifaxsecurity2017.com

```

והתשובה במידה וזה וואף לא מהרשימה :

```

~ WAFW00F : v2.1.0 ~
The Web Application Firewall Fingerprinting Toolkit
[*] Checking https://equifaxsecurity2017.com
[-] WAF BitNinja was not found in our list

```

- משתמש בפרוקסי בשביל לבצע את הבקשות
- בשביל לדעת באיזה גרסא אתה משתמש -V ורז'ן כלומר הגרסא עושים וואף -V
- באמצעות הפקודה הזו אפשר להשתמש בהאדרים שהם קאסטום מייד בשביל מטרות שונות -H