

1.WAFW00F

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

ואפוף זה הוא סקריפט פיתון שמאפשר לנו לזהות איזה WAF האתר/שרת שאנו מנוטים לחדר אליו משתמש וככה אנו בטור תוקפים יכולים לתוכן את arsenel התקיפה שלנו בצורה טובה יותר וכן לדעת באיזה כלים להשתמש.

הוא ווּפּ עובד כך:

-הוא שלוח בקשה HTTP ומנסה את התשובה שלו וככה הוא מגלה האם יש לו ווּפּ
-במידה זהה לא עובד הוא שלוח מספר בקשות HTTP (יש סיכוי שהקלם זדוניות) ואז בהתאם
לtagובה הוא מחליט איזה ווּפּ זה
-במידה זהה גם לא הצליח זה מנתח את התגבותות שהוא קיבל בעבר ומשתמש באלגוריתם בשבייל
לבודק האם יש ווּפּ או מרכיב אחר שחווס את הבקשות.
בшибיל להפעיל את WAFW00F נוצרך דבר ראשון להתקין אותו
בנוסף אפשר לראות מאיפה הבקשתה נשלחה אז במידה ונרצה אונונימיות נוכל לעשות למצנו תוריפי או
להשתמש בפרוקסוי (יש אפשרות בילד אין בתוכנה)

התקנה:

בשביל להתקין אנו נכנס למכשור לינוקס שלנו ונרשום את הפקודה הבאה

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

ובמידה ופיטון לא מותקן נצטרך לרשום את הפקודה הבאה קודם

```
python setup.py install
```

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

ואז ליכת לגיט ולהתקין אותו

או במידה ואתם משתמשים בקAli לינוקס אז זה מגע בילט אין בתוך המערכת.

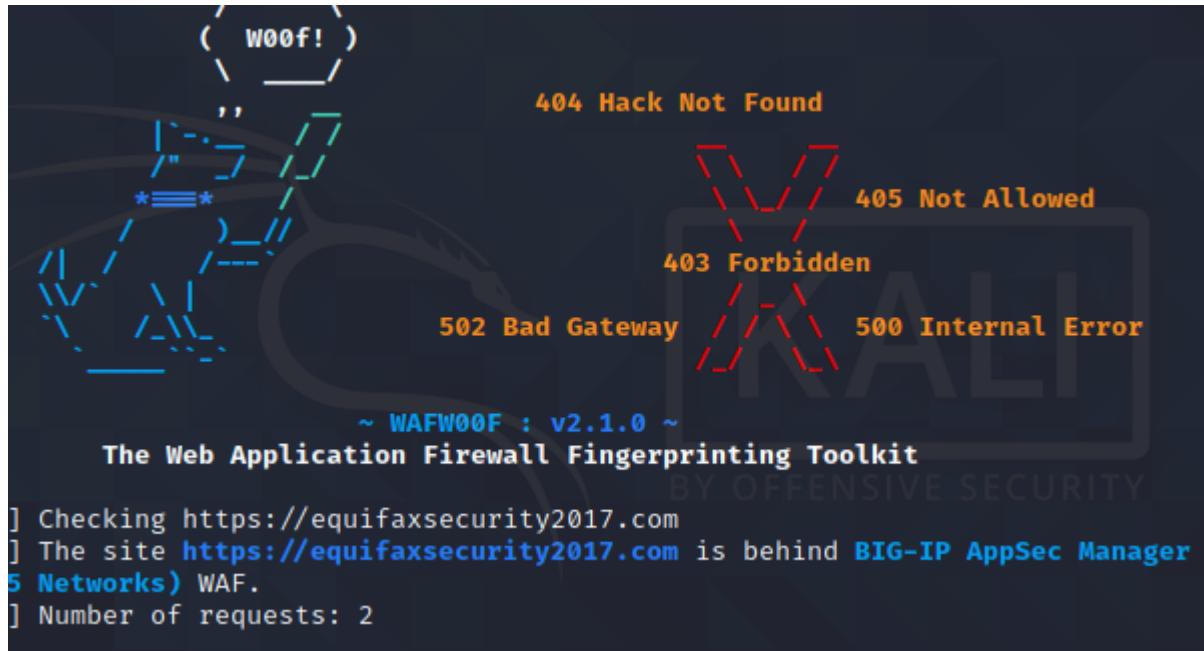
שימוש: בשביל להשתמש בוואפוף אנו פשוט נרשום wafw00f ואת הכתובת של האתר שאנו רוצים לבדוק

לדוגמא כאן אנו נבדוק את האתר [Home](#)

השתמשתי באתר זהה מכיוון שהוא כבר לא פעיל ולא מתחזק

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

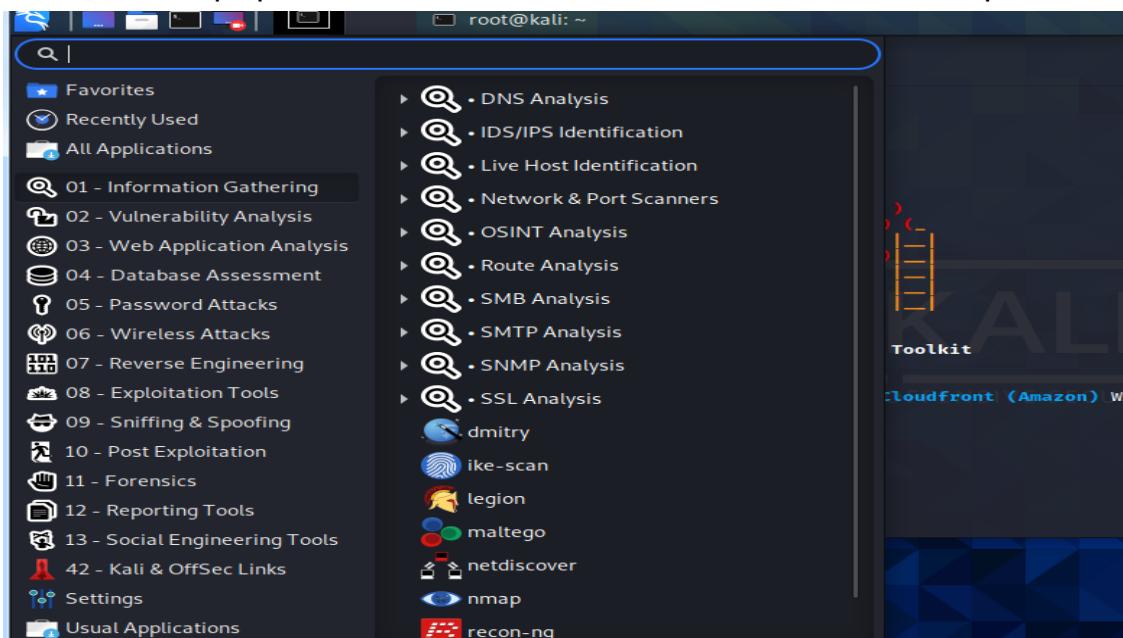
לאחר מכן אנו נלחץ אנטר ונקבל דבר דומה ל:



כמו שאפשר לראותו הוא בודק את האתר ולאחר מכן הוא אומר לנו שהאתר נמצא מאחוריו WAF מסוג ip-big של חברת 5foshlakh לו 2 רישיוטים בשביל לקבל את המידע הזה.

כמו כן אפשר לראות שחלק מהבקשות שלנו לא הצליחו ולמה הם לא הצליחו אבל הוא כן הצליח למצוא את הפירול הנדרש

כמו כן אפשר להגיע לואפוווף באמצעות לחיצה על הסימן של קאלி לעילו לאחר מכן על אינפורמצישן גattering אז על IDS/IPS IDEN ושם אפשר למצוא את זה אף וו'



במידה ונחלייט להכנס אל WAFW00F ממש זה פשוט עוזה אקסקיוט לסקריפט שמריץ את H-WAFW00F 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
r
  -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
```

בסוף חשוב לציין לפני שנעבור לשלב של הפקודות ומה הן עושות היא שואפוווף ידוע לרוחה אך ורק WAFים אשר נמצאים ברשימה שלן את הרשימה אפשר למצוא בGIT מתוך לקבצים.

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

פקודות:

כלומר עזרה ובאמצעותיו אפשר לראות אם פקודות אפשר להשתמש בהם HELP - או H הדגמה לזה אפשר לראות למעלה ^

-verbose מילים שמתארות את הוויאפ --verbose או -V

בודק את כל וואפים שנמצאים על האתר ולא מפסיק לבדוק ברגע שהוא מגיע לראשונה ומছיר -A תוצאה , בנוסף זה גם נותן מידע נוסף על השירות שאפשר ללמוד ממנו לדוגמה:

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

[*] Checking https://equifaxsecurity2017.com
[+] The site https://equifaxsecurity2017.com is behind Cloudflare (Cloudflare Inc.) WAF.
[+] Generic Detection results:
[*] The site https://equifaxsecurity2017.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
```

זה אפשר למדוד שהשרת מחזיר תגובה שונה כמשמעותו בסטרינג של תקיפה, תגובה נורמלית מחזירה קוד 200 ואילו תגובה לסתורינג של XSS זה 503.

אפשר לשלב את הפקודות -V ו-A בשבייל לבדוק אם פירוטים יש ולקבל מידע עליהם לדוגמה:

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

והתשובה שהתקבלה:

```
~ 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 השנייה אפשר לראות שהוא מצא וואפים את הסוג שלהם ואת כמות הוואפים שנמצאים על השרת .

- בשרת XXלא עוקב אחרי הקיד'ירקט שמקבלים אם יש תגובה 3 ר
- מראה לנו את הרשימה של הוואפים שוואפוף יודע למצוא תווים שלהם שמשהים איזה ואפ זה
- בדיקה אחריו ואפ ספציפי (מהרשימה) והאם הוא נמצא באתר הרלוונטי -t

לדוגמא

```

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

```

והתשובה במידה זהה ואפ 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 בפרויקט שביל לבצע את הבדיקות ד-
- שביל לדעת באיזה גרסה אתה משתמש V- ורץ' קלומר הגרסה עושים וואופ V-
- באמצעות הפקודה זו אפשר להשתמש בהادرים שהם קאוסטום מייד שביל מטרות שונות H-