The Truth about Web Application Firewalls: What the vendors do NOT want you to know.

TROOPERS 09 – Munich, April 2009

$ whois WendelGH

PT Consultant at Trustwave's SpiderLabs.

Over 7 years in the security industry.

Vulnerability discovery Webmails, AP, Citrix, etc.

Spoke in YSTS 2.0, Defcon 16, H2HC and others.

Affiliated to Hackaholic team.

$ whois SandroGauci

Founder and CSO EnableSecurity.

VOIPPACK (CANVAS addon).

Security research papers.

SIPVicious and SurfJack.

Introduction

• Web Application Firewalls (WAFs) are quickly taking their place to protect web applications.

• Today WAF systems are considered the next generation product to protect websites against web hacking attacks.

• During this presentation we will show WAF systems can be identified, detected and we will introduce new attacks.

• We will show how WAF systems can be vulnerable to the same vulnerabilities that they try to protect Web Applications from.

What is WAF

• WAFs are often called 'Deep Packet Inspection Firewall'.

• Some WAFs look certain 'attack signature' while others look for abnormal behavior.

• WAFs can be either software or hardware appliance.

What is WAF

• Modern WAF systems work both with attack signature and abnormal behavior.

• WAFs can be installed as a reverse proxy, embedded or connected in a switch (SPAN or RAP).

• Nowadays many WAF products detect both inbound and outbound attacks.

Vendors

f5®

BREACH™ SECURITY LABS

eEye Digital Security®

CiTRIX®

iMPERVA®

FORTIFY® SOFTWARE

AppliCure Technologies

port80 software

armorlogic

webScurity inc.

art of defence

Who uses WAF?

- Many banks around the world.
- Companies that are very security conscious.
- Many companies in compliance with PCI DSS (Payment Card Industry - Data Security Standard).

Operation Modes:

- Negative model (blacklist based).
- Positive model (whitelist based).
- Mixed / Hybrid (mix negative and positive model protection).

Operation Mode: Negative

A negative security model detects attacks by relying on a database of attack signatures.

Example:

Do not allow in any page, any argument value (user input) which match potential XSS strings like <script>, </script>, String.fromCharCode, etc.

Operation Mode: Positive

A positive security model enforces positive behavior by learning the application logic and then building a security policy of valid known good requests.

Example:

Page news.jsp, the field "id" only accept numbers [0-9] and starting at 0 to 65535.

Common Weaknesses Brief

- Bad rules.
- Bad design.
- Bad implementation.
- Vulnerable to the same flaws they intend to protect.

Detection

WAF systems leave several signs which permit us to detect them, one of them are cookies:

Cookies: Some WAF products add their own cookie in the HTTP communication.

DEMO

Detection

WAF leave several traces that permit us to detect them, one of them are Header Rewrite:

Header Rewrite: Some WAF products allow the rewriting of HTTP headers. The most common field is "Server", this is used to try to deceive the attackers (server cloaking).

DEMO

Detection

Some WAF systems change the return codes:

• Different 404 error codes for hostile and non existent pages.

• Different error codes (404, 400, 401, 403, 501, etc) for hostile parameters (even non existent ones) in valid pages.

DEMO

Detection

Other WAF systems will simply drop the connection:

Drop Action: Immediately initiate a "connection close" action to tear down the TCP connection by sending a FIN packet.

DEMO

Detection

WAF systems leave several signs which permit us to detect them, one of them are Pre Built-in Rules:

Pre Built-in Rules: All (at least all that we know) WAF systems have a built-in group of rules in negative mode, these rules are different in each products, this can help us to detect them.

DEMO

Detection

You should be thinking…

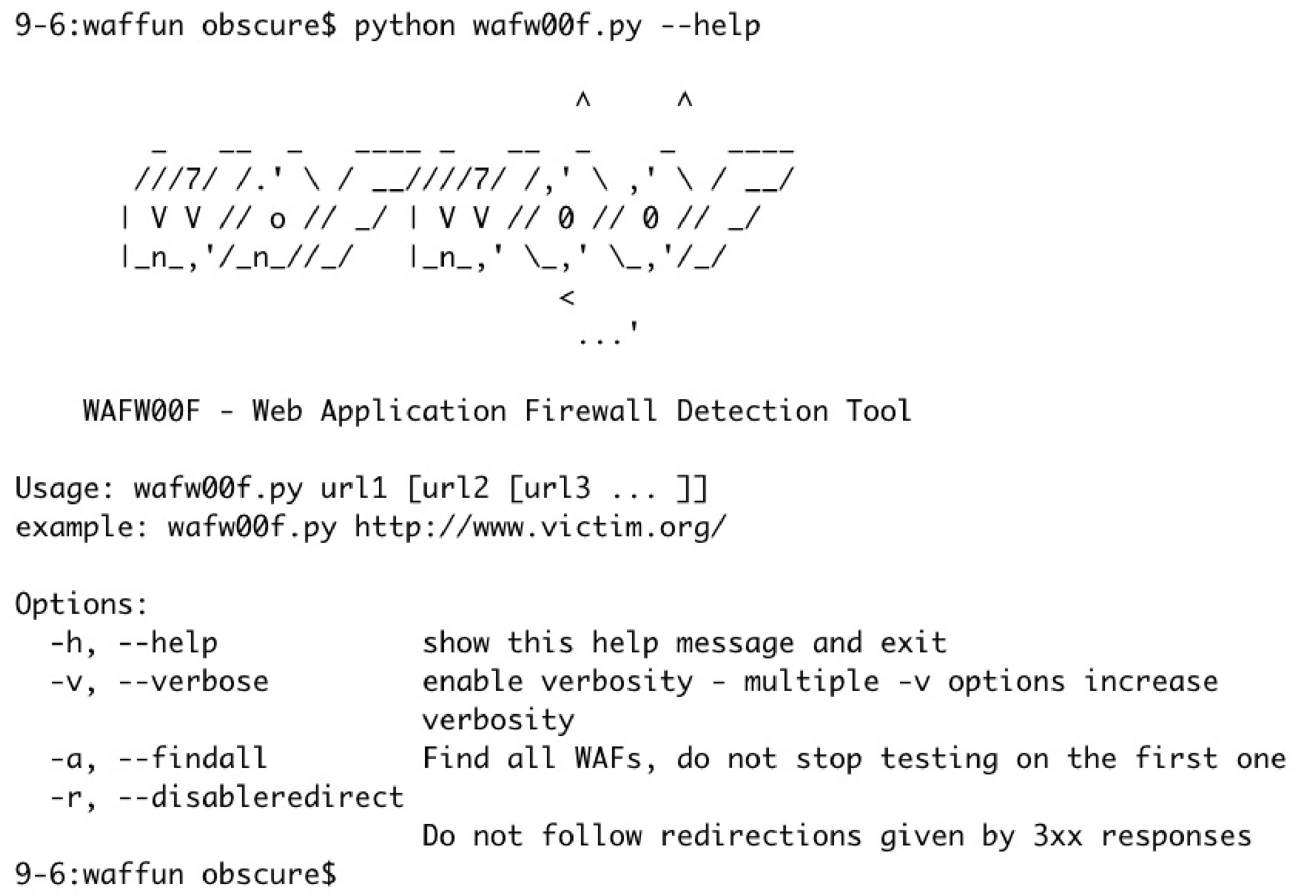
- It’s so boring.
- We have to have good knowledge of various products to identify them correctly.
- What about a tool that does all this?

WAFW00F

That’s our answer for your prayers:

- Detect 10 different WAF products.
- Generic detection.
- Supports Windows and Unix.
- Much more coming soon.

WAFW00F



```
9-6:waffun obscure$ python wafw00f.py --help

                                 ^     ^
        _   __  _   ____ _   __  _    _   ____
       ///7/ /.' \ / __////7/ /,' \ ,' \ / __/
      | V V // o // _/ | V V // 0 // 0 // _/
      |_n_,'/_n_//_/   |_n_,' \_,' \_,'/_/
                                <
                                 ...'

    WAFW00F - Web Application Firewall Detection Tool

Usage: wafw00f.py url1 [url2 [url3 ... ]]
example: wafw00f.py 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, do not stop testing on the first one
  -r, --disableredirect
                        Do not follow redirections given by 3xx responses
9-6:waffun obscure$
```

WAFW00F

DEMO

Bypassing

WAF systems can be bypassed in various ways. We can modify our attack to still be effective and not match the WAF rules:

- Detect allowed / good strings.
- Detect denied / bad strings.
- Detect sequences of good and bad strings together.
- Modify your attack to match the good rules.

DEMO

Bypassing

WAF systems can be bypassed in various ways. Another way is to use encoding and language support:

- Unicode.
- Homographic attacks.

DEMO

Bypassing

WAF systems can be bypassed in various ways. Web languages are very flexible:

- HTML and JS is very flexible.
- XSS Case.

DEMO

Bypassing

WAIT!

- What about positive model?
- They are really secure?
- If we find a positive model we should give up?

DEMO

Bypassing

There are many other ways to bypass WAF systems…

Coming soon!

Bypassing

You should be thinking…

- It’s so boring.
- It’s time consuming.
- The are so many different techniques to remember.
- There are so many specific techniques that are product dependent.
- How about a tool which does all of the above?

WAFFUN

That's our answer for your prayers:

- Test the target and point weakness in the WAF system.
- Use with WAFW00F for better results.
- Supports Windows and Unix.
- Alpha version! We need the community help!
- Much more coming soon.

WAFFUN

DEMO

Show Time: 0day

DEMOS

WAF - Other problems

- Backdoors.
- DoS.
- Overflows.

Thank you!

Do you have access to a commercial WAF system?
Do you have ideas to improve our tools?
Don't have anyone to talk to?

Contact us!

wsguglielmetti [em] gmail [ponto] com
sandro [em] enablesecurity [ponto] com