

Forum:[Hack Forums](#)

Thread: [\[Behind The Scenes\] Boolean Based Blind Injection \(Blind SQLi\)](#)

-DownFall - April 24, 2012, 11:25 am

Hey niggas and hoes of HF....so I'm bored as fuck on my iPod so I'd thought I should share some more of my knowledge with you guys. This time it's just a basic explanation on Boolean Based Blind Injection, or "Blind SQLi". For those of you that know how it works, good for you - this is for those who don't. There's a couple important factors that I'm going to go over. First thing first is how it works.

Explanation

Blind Injection is more than "and 1=1 , and 1=2". Yeah you might remember the queries to a blind injection attack, but the question is - what the fuck is going on behind the scenes? Here is how it works. There's always a query behind a page, selecting content to be displayed on a page. Now, when this query becomes false, it selects nothing. Basically we use true and false statements along with visible data on the page to determine our data that's being withdrawn. Here's an example.

Code `http://www.site.com/news.php?article_id=1`

Now, the query behind the page here would look something like this.

Code `SELECT * FROM news WHERE article_id=1`

Makes sense right? Now if this site was vulnerable to SQL Injection, here's how the query would look with a blind attack.

Code `http://www.site.com/news.php?article_id=1 AND 1=1--`

`SELECT * FROM news WHERE article_id=1 AND 1=1`

Nothing would be missing from the page, because the query is true, therefore it selects the content from the database. Now if I did something like this....

Code `http://www.site.com/news.php?article_id=1 AND 1=2--`

`SELECT * FROM news WHERE article_id=1 AND 1=2`

Now this brings us back to basic math...does 1=2? No it does not, so the query here becomes false and selects nothing. It's the same thing as this.

Code `SELECT * FROM news WHERE article_id=1 AND FALSE`

It would select nothing...

Functions Behind A Blind Attack

So now that you know how blind attacks work, I'm going to explain how we draw data using functions that are known in SQL.

AND - Common Sense -- ("The AND operator displays a record if both the first condition and the second condition is true.")

ASCII - Converts your selected value to ascii characters. ("Returns the ASCII code value of the leftmost character of a character expression.")

SELECT - Selects something ("The SELECT statement is used to select data from a database.")

SUBSTRING - Selects a part of something. ("The Substring function in SQL is used to grab a portion of the stored data. ")

These functions are huge in blind injection. Using these, you could create powerful queries that get you the data you want. Here's a few examples on how they look in action.

Code `http://site.com/news.php?article_id=1 AND SUBSTR((SELECT username FROM users WHERE is_admin='y' LIMIT 0,1),1,1)='x'`

If the first letter of the first admin account is "x", the query would return true and nothing would come up missing from the page. If it wasn't, the query would return false...get it?

You can create your own queries, use your imagination. Boolean Based Blind Injection is a really useful method of web application exploiting and there WILL be times when you need it. Here's my tutorial on it, read up and learn.

[\[Detailed\] Boolean Based Blind Injection \[Tutorial\]](#)

Have fun guys,

-DownFall

xx 0x0 xx - April 24, 2012, 12:32 pm

so nice and simple and short good work dude sure i learned from it thx alot

torque59 - April 24, 2012, 12:34 pm

Excellent Downfall ?

I have Always used knowledge in reference to your tuts

Gr8 Work there

HATS OFF ?

BeggFoMercy - April 24, 2012, 12:35 pm

Ofc u wont get much attention , HF is full of skids atm ;)

JoinSeventh - April 24, 2012, 12:37 pm

(Apr 24, 2012 12:35 PM)BeggFoMercy Wrote: [\[CITE\]](#) Ofc u wont get much attention , HF is full of skids atm ;)

Atm? HF has been full of skids as long as I can remember...

Anyway, for all you "h4xX0rs" out there: Try to read through this and learn something.

Good tutorial.

Bacardi - April 24, 2012, 12:38 pm

Interesting. Got a bookmarked, going to read it soon.

Another nice thread Downfall! :)

-DownFall - April 24, 2012, 12:47 pm

Thanks everyone...waited a good 20 minutes before I got a reply lol. My question is, how many of you knew this? Those that learned SQL should know why things come up missing in a blind injection, but did anyone who learned SQLi without learning SQL first know why?...this is why hacking is no fun unless you know what's really going on..

As for "HF is full of skids", true but we all start somewhere. Not knowing much has nothing to do with being lazy and not leaving a comment on a thread you just read lol.

Mx. - April 24, 2012, 12:54 pm

Have read / used this kind before, i swear hacking years ago was a bitch with mysql, there where no tutorials at all, well never this well written, so all you skids better take it with you, as its valueble for later.

Well done DownFall.

noober1001 - April 24, 2012, 12:59 pm

really very good.
thank you so much bro for sharing this.
keep sharing.

-DownFall - April 24, 2012, 1:11 pm

(Apr 24, 2012 12:54 PM)Mx. Wrote: [\[CITE\]](#) Have read / used this kind before, i swear hacking years ago was a bitch with mysql, there where no tutorials at all, well never this well written, so all you skids better take it with you, as its valueble for later.

Well done DownFall.

Thanks, means alot...if anyone else reads this just post what you think of it and whether you learned something or not...also take a look at my tutorial I linked down at the bottom if you want to learn how to use blind.

Bacardi - April 24, 2012, 1:15 pm

I'm on of the people that learned SQLi before knowing SQL. Although, I'm started a new year at school which comes with a class in SQL.

With that, this will help me understand how SQLi is possible :)

-zerocool - April 24, 2012, 1:24 pm

(Apr 24, 2012 12:37 PM)JoinSeventh Wrote: [\[CITE\]](#) Atm? HF has been full of skids as long as I can remember...

Anyway, for all you "h4xX0rs" out there: Try to read through this and learn something.

Good tutorial.
Agree with him. .

Good tut for learner.

-DownFall - April 24, 2012, 10:09 pm

(Apr 24, 2012 01:24 PM)-zerocool Wrote: [\[CITE\]](#) Agree with him. .

Good tut for learner.
Thanks, please keep the comments coming....

Px5 - April 25, 2012, 7:50 am

Nice one downfall.
Great tutorial :-)

dhrubo11 - April 25, 2012, 9:10 am

you are best man .. i like your tutorials

Hooded Robin - April 25, 2012, 10:12 am

i learned to hack first then learned syntax and meaning later (still learning in fact, constantly). I wish I had done the other way around as understanding things make a world of difference in increasing your chances of success as you learn how to adapt better to the oddities which break standard tutorial based syntaxes, and thus stopping most skiddies in tracks. School is cool, but its not the only place you can learn :p

Nice write up as usual -DownFall!

-DownFall - April 25, 2012, 9:14 pm

(Apr 25, 2012 10:12 AM)Hooded Robin Wrote: [\[CITE\]](#) i learned to hack first then learned syntax and meaning later (still learning in fact, constantly). I wish I had done the other way around as understanding things make a world of difference in increasing your chances of success as you learn how to adapt better to the oddities which break standard tutorial based syntaxes, and thus stopping most skiddies in tracks. School is cool, but its not the only place you can learn :p

Nice write up as usual -DownFall!

We must be long lost brothers, this was the reply I was waiting for. Thanks HR c:

Phizo - April 25, 2012, 11:13 pm

Nice tutorial, like always :).
Keep up the good work man!

-DownFall - April 25, 2012, 11:16 pm

Hehe....everyone keeps saying tutorial, this is just an explanation on how it works >.<
The tutorial is at the bottom lol , thanks though for the feedback ^.^

c3970r - January 10, 2015, 2:08 am

Hlo! I tried to understand the working of website but when i add ' (quote) the whole web page which is loaded after this is a blank Then i tried to confirm thee blind SQLi by using True and false query but again the page loaded is blank everytime .

I know there is Blind sqli how can i go further plz help and guide me.
Thanks in advance!

WitchKing - January 10, 2015, 2:10 am

i like this tutorial..bookmarked..keep on sharing

Root_x7 - April 16, 2015, 5:35 am

Awesome :D Thanks a lot for sharing <3 it