

Forum:[Hack Forums](#)

Thread: [Xpath Injection Help](#)

raylex02 - July 30, 2018, 6:40 pm

Hello, i'm trying to extract a website's database using xpath injection and i was able to get the admin username and password but i have a little problem when trying to extract the password column. The password isn't plain text it's a hash so when i try to extract it the Xpath result doesn't display the full hash, is there a way to view the complete password hash using xpath injection?

Gee4rce - July 31, 2018, 6:07 am

It is hard to rate this remotely,
but you could try fetching one hash in two outputs with the "substring" function.

So you go and define a start and endpoint to split your output into two.
After you have the output of both requests, you just put it back together again.
But not considered to be an elegant solution if you are dealing with larger db's.

Example:

Let's say complete hash is 20 chars long.

1. request: ...substring(passhash,1,10)...

2. request: ...substring(passhash,11,20)...

So you fetch the first half (1 - 10 characters of hash),
and then the other half (character 11 - 20).

If this doesn't help, you may go and ask in the SQLi sub-section
of the Website and Forum hacking section.

Cheers, Gee.

Hooded Robin - July 31, 2018, 7:52 am

FYI more explanation on why this occurs as I helped push the fix for sqlmap to correct this issue a while back ;)

The length restriction on xpath functions (extractvalue/updatesxml) are limited to 26 chars due to the fact that it is expecting a floating point result and thus the value is trimmed to 26 chars as this is limit on the default precision value returned for floating point values. This is why you need to check the length of the value you want, then extract the result in chunks using a substring/mid approach as explained above to work around the length limitations.

raylex02 - July 31, 2018, 1:53 pm

(Jul 31, 2018 06:07 AM)Gee4rce Wrote: [\[CITE\]](#) It is hard to rate this remotely,
but you could try fetching one hash in two outputs with the "substring" function.

So you go and define a start and endpoint to split your output into two.
After you have the output of both requests, you just put it back together again.
But not considered to be an elegant solution if you are dealing with larger db's.

Example:

Let's say complete hash is 20 chars long.

1. request: ...substring(passhash,1,10)..
2. request: ...substring(passhash,11,20)..
So you fetch the first half (1 - 10 characters of hash),
and then the other half (character 11 - 20).

If this doesn't help, you may go and ask in the SQLi sub-section
of the Website and Forum hacking section.

Cheers, Gee.

Thanks man, can you make an example of how i can add this to my injection string? i
'm new to this

Gee4rce - August 2, 2018, 8:07 am

(Jul 31, 2018 07:52 AM)Hooded Robin Wrote: [\[CITE\]](#) FYI more explanation on why this occurs as I
helped push the fix for sqlmap to correct this issue a while back ;)

I see i forgot about Mid() function ?

Good job on the SQLmap fix, i wasn't aware of the details behind that cut-off problem,
but i faced it in the past too. Good to know, makes sense now, thanks!

(Jul 31, 2018 01:53 PM)raylex02 Wrote: [\[CITE\]](#) Thanks man, can you make an example of how i can
add this to my injection string? i

'm new to this

No problem,

but for helping you with full PoC you would have to share the target with me,
as otherwise i could only make wild guesses. If you decide to do so, then best
send it via private message, wouldn't post it publically in this forum, or your
target may get raped by others.

Other than that, it would probably look something like this:
(spaces added or otherwise i couldn't post)

SQL like'ish:

Code ' and sele ct substr ing(passwdhash,4,3)--
or

XSLT like'ish:

Code ' and substr ing(/some/path/@passwdhash, string-length(/some/path/@passwdhash)-10)
Thats all i can tell from remote.

Cheers, Gee.