

Forum:[Hack Forums](#)

Thread: [When Columbia Uni tries to 1337haxxor you](#)

Ralkage - April 12, 2015, 11:36 am

Yeah, I'm being totally serious. I did a reverse lookup on the IP address and it showed something quite shocking. Apparently someone tried to brute force into my groups gaming ftp server and failed miserably as they tried to use the username "FTP" with no password. Is this how they conduct classes at the CUIT department or something? I feel the need to dig deeper but I don't know where to start, so far I found out that the server or machine that the IP traces back to is using XAMPP and anonymous ftp is open as well as phpMyadmin. Tried the default values but no luck with root and no password lol.

Any guidance to where I need to start is helpful, or am I in the wrong place or something?

Oh wise potato chip users....guide me...

P.S. I don't want to DDOS, I just want to get into the hidden places where the cool kids hang out in the server room there.

Edit: Found this error from the root directory....

Code Warning: require_once(C:\xampp\htdocs\includes\errors.inc): failed to open stream: No such file or directory in C:\xampp\htdocs\opa\includes\bootstrap.inc on line 2237 Fatal error: require_once(): Failed opening required 'C:\xampp\htdocs\includes\errors.inc' (include_path='.;C:\xampp\php\PEAR') in C:\xampp\htdocs\opa\includes\bootstrap.inc on line 2237
Network ID exposed, hosts listed and half of them using XAMPP and wordpress lol

Edit 2: I know that no one will read this bit I got access into phpMyadmin....wat do?

Coftek - April 12, 2015, 4:51 pm

I would think that someone could just be using their servers as a proxy, not necessarily someone at the school trying to bruteforce a game server.

Ralkage - April 12, 2015, 5:04 pm

(Apr 12, 2015 04:51 PM)Coffey™ Wrote: [\[CITE\]](#) I would think that someone could just be using their servers as a proxy, not necessarily someone at the school trying to bruteforce a game server.

This could be true, but one random host out of probably 500+? And when I got into phpmyadmin and guessed the credentials in 5 tries I was like really? That easy? lol

I kept the same Network ID and changed the host number and I've found some pretty weird stuff. Even found a jenkins page filled with CUIT private projects. ?

Coftek - April 12, 2015, 5:25 pm

(Apr 12, 2015 05:04 PM)Ralkage Wrote: [\[CITE\]](#) This could be true, but one random host out of probably 500+? And when I got into phpmyadmin and guessed the credentials in 5 tries I was like really? That easy? lol

I kept the same Network ID and changed the host number and I've found some pretty weird stuff. Even found a jenkins page filled with CUIT private projects. ?

More often then not, it's someone that either doesn't like someone on the server, or just downloaded loic and wants to try out his hacker skills.

Either way, that sounds pretty interesting. Mind sharing something cool?

Ralkage - April 12, 2015, 5:33 pm

(Apr 12, 2015 05:25 PM)Coffey™ Wrote: [\[CITE\]](#) More often then not, it's someone that either doesn't like someone on the server, or just downloaded loic and wants to try out his hacker skills.

Either way, that sounds pretty interesting. Mind sharing something cool?

I have no problem with that ? First I wanna keep searching, see if there are any vulnerabilities and then you'll be the first person I'll share my findings with over PM.

Maybe we can discuss? I'm afraid that one of the script kiddies on here might ruin the fun....

sluggerz - April 12, 2015, 6:22 pm

(Apr 12, 2015 05:04 PM)Ralkage Wrote: [\[CITE\]](#) This could be true, but one random host out of probably 500+? And when I got into phpmyadmin and guessed the credentials in 5 tries I was like really? That easy? lol

I kept the same Network ID and changed the host number and I've found some pretty weird stuff. Even found a jenkins page filled with CUIT private projects. ?

Interesting, I wonder what they are up to.

Ralkage - April 12, 2015, 6:53 pm

(Apr 12, 2015 06:22 PM)sluggerz Wrote: [\[CITE\]](#) Interesting, I wonder what they are up to. I'll keep poking around and post some screenshots of my findings. ?

FadedCow - April 13, 2015, 12:22 am

(Apr 12, 2015 06:53 PM)Ralkage Wrote: [\[CITE\]](#) I'll keep poking around and post some screenshots of my findings. ?

When I get home I'll see if I can try and help you out. Just pm your skype to me and I'll hit you up in a few hours.

The_J0k3r - April 13, 2015, 12:44 am

Upload shell through phpMyAdmin + Add user with administrator rights and enable Remote Desktop = Profit? :3

Ralkage - April 13, 2015, 5:49 am

(Apr 13, 2015 12:22 AM)FadedCow Wrote: [\[CITE\]](#) When I get home I'll see if I can try and help you out. Just pm your skype to me and I'll hit you up in a few hours.

Ralkage, I'm on once in a while.

(Apr 13, 2015 12:44 AM)The_J0k3r Wrote: [\[CITE\]](#) Upload shell through phpMyAdmin + Add user with administrator rights and enable Remote Desktop = Profit? :3

Root looks to either be disabled or has a custom password. Though I found two users with no passwords, just no rights to add databases lol. I can add tables to the test database this person has up but I can't import anything until I get root. It's probably a simple password. How does one start his journey into uploading shell?

Ralkage - April 14, 2015, 5:35 pm

Can anyone help me out? I have access to the PMA user, no password.

EXPLICIT CONTENT - April 15, 2015, 2:33 am

Do you got FILE Privilege under that username ? You could try to shell it with a INTO OUTFILE statement

Ralkage - April 16, 2015, 8:24 am

(Apr 15, 2015 02:33 AM)Codah Wrote: [\[CITE\]](#) Do you got FILE Privilege under that username ? You could try to shell it with a INTO OUTFILE statement

Tried SELECT * INTO OUTFILE "C:\xampp\htdocs\shell.php" in the SQL Query tab but it just loads and does nothing, even checked for the file.

The reason how I found the directory because the index showed:

Code Warning: require_once(C:\xampp\htdocs\includes\errors.inc): failed to open stream: No such file or directory in C:\xampp\htdocs\opa\includes\bootstrap.inc on line 2237 Fatal error: require_once(): Failed opening required 'C:\xampp\htdocs\includes\errors.inc' (include_path='.;C:\xampp\php\PEAR') in C:\xampp\htdocs\opa\includes\bootstrap.inc on line 2237

cla55ified - April 16, 2015, 9:23 am

try this see if the root password is located in the config file...

LOAD DATA LOCAL INFILE 'C:/xampp/phpmyadmin/config.inc.php' INTO TABLE pma_bookmark (dbase)

If its not in C:/ use the variables page in phpmyadmin to see what drive its installed on.

Try 'C://xampp/filezillaftp/filezilla server.xml' to get the filezilla passwords.

Also if you dont have access to pma_bookmark just use another table you have access to. I'm gussing you will have the pma user though.

Ralkage - April 16, 2015, 4:21 pm

(Apr 16, 2015 09:23 AM)cla55ified Wrote: [\[CITE\]](#) try this see if the root password is located in the config file...

LOAD DATA LOCAL INFILE 'C:/xampp/phpmyadmin/config.inc.php' INTO TABLE pma_bookmark (dbase)

If its not in C:/ use the variables page in phpmyadmin to see what drive its installed on.

Try 'C://xampp/filezillaftp/filezilla server.xml' to get the filezilla passwords.

Also if you dont have access to pma_bookmark just use another table you have access to. I'm gussing you will have the pma user though.

The thing is that I run any SQL and it just shows the yellow loading box and fades away :(

I have access to this though through pma:

Code pma_bookmark
pma_column_info
pma_designer_coords
pma_history
pma_pdf_pages
pma_relation
pma_table_coords
pma_table_info
pma_tracking
pma_userconfig
I can edit these btw

and pma_userconfig shows me the lists of users and something called blob.

