

Forum: [Hack Forums](#)

Thread: [THC-Hydra and PhpMyAdmin.](#)

N00b_n00b - October 3, 2020, 11:28 am

Hello,

I want to find a PhpMyAdmin username via THC-Hydra. The login page code is:

Code <div class="item">

<label for="input_username">Username:</label>

<input type="text" name="pma_username" id="input_username" value="" size="24"

class="textfield">

</div>

<div class="item">

<label for="input_password">Password:</label>

<input type="password" name="pma_password" id="input_password" value="" size="24"

class="textfield">I used below command:

Code \$ hydra -L /usr/share/dict/cracklib-small -p 123 192.168.56.5 http-post-form

'/phpmyadmin/index.php:pma_username=^USER^&pma_password=^PASS^:incorrect'But the result is:

Code [80][http-post-form] host: 192.168.56.5 login: agonized password: 123

[80][http-post-form] host: 192.168.56.5 login: agnomen password: 123

[80][http-post-form] host: 192.168.56.5 login: agonize password: 123

[80][http-post-form] host: 192.168.56.5 login: agreeableness password: 123

[80][http-post-form] host: 192.168.56.5 login: agreeable password: 123

[80][http-post-form] host: 192.168.56.5 login: agreed password: 123

[80][http-post-form] host: 192.168.56.5 login: agrarian password: 123

[80][http-post-form] host: 192.168.56.5 login: agrees password: 123

[80][http-post-form] host: 192.168.56.5 login: agreeably password: 123

[80][http-post-form] host: 192.168.56.5 login: agree password: 123

[80][http-post-form] host: 192.168.56.5 login: agreements password: 123

[80][http-post-form] host: 192.168.56.5 login: agricola password: 123

[80][http-post-form] host: 192.168.56.5 login: agribusiness password: 123

[80][http-post-form] host: 192.168.56.5 login: agrees password: 123

[80][http-post-form] host: 192.168.56.5 login: agreeer password: 123

[80][http-post-form] host: 192.168.56.5 login: agrimony password: 123

[80][http-post-form] host: 192.168.56.5 login: agreement password: 123

[80][http-post-form] host: 192.168.56.5 login: agreement's password: 123

[80][http-post-form] host: 192.168.56.5 login: agreeing password: 123

...Which part of my command is wrong?

Thank you.

BeggFoMercy - October 3, 2020, 4:24 pm

PHP Code

<?php

hydra -l USERHERE(ROOT/ADMIN) -P PASSWORDCRACKLIBHERE -e ns -vV IP HERE http-post-form "/phpmyadmin/index.php:pma_username=^USER^&pma_password=^PASS^&server=1:denied"

it wasnt working properly cuz " incorrect " which is the keyword that hydra looks for to determine

whether tested creds were successful or not never existed...

N00b_n00b - October 4, 2020, 8:28 am

(Oct 3, 2020 04:24 PM)BeggFoMercy Wrote: [\[CITE\]](#) PHP Code

```
<?php
```

```
# hydra -I USERHERE(ROOT/ADMIN) -P PASSWORDCRACKLIBHERE -e ns -vV IP HERE http-post-form "/phpmyadmin/index.php:pma_username=^USER^&pma_password=^PASS^&server=1:denied"
```

it wasn't working properly cuz " incorrect " which is the keyword that hydra looks for to determine whether tested creds were successful or not never existed...

Thank you, but in this stage finding password is not important for me. I just want to find usernames. Can I use a static password like "123" and just see if the username exist or not?

SIM-4845328 - October 4, 2020, 8:33 am

The tool does not tell you if the username are existing or not.

It tells you if it cracked a password for a phpmyadmin user.

I would recommend you to do this in another way, this is a long-going way to finding usernames.

If it's a big company I would actually advise you to do it by Social Engineering.

You would be surprised how many details you can get from Social Engineering.

N00b_n00b - October 4, 2020, 12:12 pm

(Oct 4, 2020 08:33 AM)s1zzel Wrote: [\[CITE\]](#) The tool does not tell you if the username are existing or not.

It tells you if it cracked a password for a phpmyadmin user.

I would recommend you to do this in another way, this is a long-going way to finding usernames.

If it's a big company I would actually advise you to do it by Social Engineering.

You would be surprised how many details you can get from Social Engineering.

Can you show me a way to find usernames?

In [this](#) tutorial, the author using THC-Hydra to find the username? Am I wrong?

SIM-4845328 - October 4, 2020, 1:02 pm

(Oct 4, 2020 12:12 PM)N00b_n00b Wrote: [\[CITE\]](#) Can you show me a way to find usernames?

In [this](#) tutorial, the author using THC-Hydra to find the username? Am I wrong?

Unfortunately, I do not have the time to help you with this.

But Google should be your friend.

N00b_n00b - October 4, 2020, 11:30 pm

Thank you.

I need someone that know how to find valid usernames by THC-Hydra.

N00b_n00b - October 6, 2020, 12:17 pm

(Oct 3, 2020 04:24 PM)BeggFoMercy Wrote: [\[CITE\]](#) PHP Code

```
<?php
```

```
# hydra -I USERHERE(ROOT/ADMIN) -P PASSWORDCRACKLIBHERE -e ns -vV IP HERE http-post-form "/phpmyadmin/index.php:pma_username=^USER^&pma_password=^PASS^&server=1:denied"
```

it wasn't working properly cuz " incorrect " which is the keyword that hydra looks for to determine whether tested creds were successful or not never existed...

I did that command and output is:

Code VERBOSE] Resolving addresses ... [VERBOSE] resolving done
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "ROOT" - 1 of 2151222 [child 0] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "" - 2 of 2151222 [child 1] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!" - 3 of 2151222 [child 2] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "! love you" - 4 of 2151222 [child 3] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!" - 5 of 2151222 [child 4] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!" - 6 of 2151222 [child 5] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!" - 7 of 2151222 [child 6] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!" - 8 of 2151222 [child 7] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!" - 9 of 2151222 [child 8] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!!" - 10 of 2151222 [child 9] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!!!" - 11 of 2151222 [child 10] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!1" - 12 of 2151222 [child 11] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!888888" - 13 of 2151222 [child 12] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!2" - 14 of 2151222 [child 13] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!1111" - 15 of 2151222 [child 14] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!123" - 16 of 2151222 [child 15] (0/0)
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=fe3f0e1d4cb13b89f0629286211b4ef3>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=ef2512677eb44cc432475b6ea462e57a>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=ba4550ea30d1031b4177cb3ee0212abb>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=5ca21e74ad5bfaaf089564ed74d444c2>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=dec221e7ae0a346ae88e635409442c71>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=f24752737dfcd76c84fb71016131e223>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=c0d22f748b3c56dc87e24bb13edd6b14>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=4af706573a7f382fa2ac693da2fc6b1d>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=d6a6ab67f7ce2d81d32f960ae69e4d87>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=3994336cc75c372f958285239e4846f8>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=873c97547103307ff1a671b2c176ee8d>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=c76bb9bbf6f2fa3b380da4edb86f832d>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=7ae7e653327a25ca2e9be2c960c684af>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=e0adc46ca96e9590b7bc221a6919c504>
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=66d96dc9c1043cd6a34f1e2b6b63d0d7>
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !
[STATUS] attack finished for 192.168.56.5 (waiting for children to complete tests)
[VERBOSE] Page redirected to
<http://192.168.56.5/phpmyadmin/index.php?token=ef6cf11622f2399e12b4cbdec17d06f5>
[80][http-post-form] host: 192.168.56.5 login: ROOT

```
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: ROOT
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!123
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!1111
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!888888
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!!!!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!1
[80][http-post-form] host: 192.168.56.5 login: ROOT password: ! love you
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!2
```

1 of 1 target successfully completed, 16 valid passwords foundWhen I want to login in PhpMyAdmin then it show me:

Code #1045 - Access denied for user 'root'@'localhost' (using password: YES)Server have below open ports:

Code Starting Nmap 7.80 (<https://nmap.org>) at 2020-10-06 15:06 EDT

Nmap scan report for 192.168.56.5

Host is up (0.00065s latency).

Not shown: 990 closed ports

PORT STATE SERVICE

22/tcp open ssh

25/tcp open smtp

80/tcp open http

110/tcp open pop3

111/tcp open rpcbind

139/tcp open netbios-ssn

143/tcp open imap

445/tcp open microsoft-ds

901/tcp open samba-swat

3306/tcp open mysqlI tried connect to MySQL via CLI:

Code # mysql -u root -p ROOT -h 192.168.56.5 -P 3306

Enter password:

ERROR 1045 (28000): Access denied for user 'root'@'192.168.56.6' (using password: YES)What is the problem?

Heat - October 6, 2020, 12:23 pm

(Oct 6, 2020 12:17 PM)N00b_n00b Wrote: [CITE](#) I did that command and output is:

Code VERBOSE] Resolving addresses ... [VERBOSE] resolving done

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "ROOT" - 1 of 2151222 [child 0] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "" - 2 of 2151222 [child 1] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!" - 3 of 2151222 [child 2] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "! love you" - 4 of 2151222 [child 3] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!" - 5 of 2151222 [child 4] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!" - 6 of 2151222 [child 5] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!" - 7 of 2151222 [child 6] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!" - 8 of 2151222 [child 7] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!" - 9 of 2151222 [child 8] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!!" - 10 of 2151222 [child 9] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!!" - 11 of 2151222 [child 10] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!!" - 12 of 2151222 [child 11] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!!!888888" - 13 of 2151222 [child 12] (0/0)

[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!2" - 14 of 2151222 [child 13] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!!1111" - 15 of 2151222 [child 14] (0/0)
[ATTEMPT] target 192.168.56.5 - login "ROOT" - pass "!!!123" - 16 of 2151222 [child 15] (0/0)
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=fe3f0e1d4cb13b89f0629286211b4ef3
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=ef2512677eb44cc432475b6ea462e57a
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=ba4550ea30d1031b4177cb3ee0212abb
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=5ca21e74ad5bfaaf089564ed74d444c2
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=dec221e7ae0a346ae88e635409442c71
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=f24752737dfcd76c84fb71016131e223
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=c0d22f748b3c56dc87e24bb13edd6b14
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=4af706573a7f382fa2ac693da2fc6b1d
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=d6a6ab67f7ce2d81d32f960ae69e4d87
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=3994336cc75c372f958285239e4846f8
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=873c97547103307ff1a671b2c176ee8d
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=c76bb9bbf6f2fa3b380da4edb86f832d
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=7ae7e653327a25ca2e9be2c960c684af
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=e0adc46ca96e9590b7bc221a6919c504
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=66d96dc9c1043cd6a34f1e2b6b63d0d7
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !
[STATUS] attack finished for 192.168.56.5 (waiting for children to complete tests)
[VERBOSE] Page redirected to
http://192.168.56.5/phpmyadmin/index.php?token=ef6cf11622f2399e12b4cbdec17d06f5
[80][http-post-form] host: 192.168.56.5 login: ROOT
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: ROOT
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!123
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!1111
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!888888
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!1
[80][http-post-form] host: 192.168.56.5 login: ROOT password: ! love you
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!
[80][http-post-form] host: 192.168.56.5 login: ROOT password: !!!!!2
1 of 1 target successfully completed, 16 valid passwords foundWhen I want to login in PhpMyAdmin

then it show me:

Code #1045 - Access denied for user 'peter'@'localhost' (using password: YES)Server have below open ports:

Code Starting Nmap 7.80 (<https://nmap.org>) at 2020-10-06 15:06 EDT

Nmap scan report for 192.168.56.5

Host is up (0.00065s latency).

Not shown: 990 closed ports

PORT STATE SERVICE

22/tcp open ssh

25/tcp open smtp

80/tcp open http

110/tcp open pop3

111/tcp open rpcbind

139/tcp open netbios-ssn

143/tcp open imap

445/tcp open microsoft-ds

901/tcp open samba-swat

3306/tcp open mysql tried connect to MySQL via CLI:

Code mysql -u root -p ROOT -h 192.168.56.5 -P 3306

Enter password:

error 1045 (28000): Access denied for user 'root'@'192.168.56.6' (using password: YES)What is the problem?

password is wrong is issue

N00b_n00b - October 6, 2020, 12:30 pm

(Oct 6, 2020 12:23 PM)Heat Wrote: [\[CITE\]](#) password is wrong is issue

Then why THC-Hydra tell me that it found password???

Heat - October 6, 2020, 3:29 pm

(Oct 6, 2020 12:30 PM)N00b_n00b Wrote: [\[CITE\]](#) Then why THC-Hydra tell me that it found password???16 valid passwords found

lol u got it all messed up

N00b_n00b - October 7, 2020, 12:44 am

(Oct 6, 2020 03:29 PM)Heat Wrote: [\[CITE\]](#) 16 valid passwords found

lol u got it all messed up

Nothing is working.

korona33 - October 8, 2020, 11:19 am

my phone is 567 876 986 543 87 call me please ? ple ple ple ple ple ple ple ple pe

N00b_n00b - October 8, 2020, 12:49 pm

(Oct 8, 2020 11:19 AM)korona33 Wrote: [\[CITE\]](#) my phone is 567 876 986 543 87 call me please ? ple ple ple ple ple ple ple ple pe
Sorry, I can't.