

Forum:[Hack Forums](#)

Thread: [\[TuT\] Finding an Admin Page \[90% GUARANTEE\]](#)

zer0pwn - April 10, 2012, 3:12 pm

Hey everyone.

There are so many people wondering how to find an admin page. I myself when I was just beginning web-hacking, started with SQL Injection. As many of you would've done as well. The problem is, you can barely ever find the proper admin page. Either you can't find it, or it won't work.

First of all, I'd like to get this through EVERYONE's head. There is a difference between a CPANEL Login, and a ADMIN Login. The cpanel login is to manage EVERYTHING on the site. You have access to FTP and everything. Unless the admin is VERY VERY VERY stupid (Which is probably likely, but still this is rare) you will not have the same credentials as the CPanel. So don't even both trying that login.

In a website, the webmaster will usually create a standard admin page, for the admins to manage everything easier.

Now. Let's start listing our possibilities.

GUESSING

This is by far the most popular way of finding an admin page. A lot of people just guess what the admin page is. Most of the time, there will either be a directory OR a file. Here is an example of a directory, and then a file:

Directory

Code `http://www.site.com/admin/`

File

Code `http://www.site.com/admin.php`

A directory can contain other files, but a file is just one thing.

A lot of the time, the admin page is simply just "Admin". So you can try adding: /admin to the end of site's URL. If you get a 404 Error (Which usually means the files does not exist) then that's not right. After I try "admin", I usually try a different method. This one is probably my favorite.

ROBOTS.TXT

What is Robots.txt? Robots.txt is a file that makes sure scanners will not be able to scan certain pages. Usually, if they don't want a scanner to find something, it's for a certain reason right? Obviously it's an important file. So sometimes they will have the admin page listed in there. This is what a Robots.txt page looks like:

Code User-Agent: *

Disallow: /moderation.php

Disallow: /ratethread.php

Disallow: /report.php
Disallow: /reputation.php
Disallow: /sendthread.php
Disallow: /usercp.php
Disallow: /usercp2.php
Disallow: /newreply.php
Disallow: /newthread.php
Disallow: /editpost.php
Disallow: /private.php
Disallow: /search.php
Disallow: /refer.php
Disallow: /myawards.php
Disallow: /stats.php
Disallow: /member.php
Disallow: /memberlist.php
Disallow: /showteam.php
Disallow: /upgrade.php
Disallow: /showratings.php

User-agent: dotbot
Disallow: /

User-agent: 008
Disallow: /

I grabbed that from HF (Don't worry, there's nothing "Top Secret" in there :P). Even if it says "Disallow" we can usually still access the files. So go ahead and add /robots.txt to your target, and see what you find!

WEB-CRAWLER

Web crawlers are, and always will be, a hackers best friend. A web-crawler will crawl a website, and list certain directories and files. I DEFINITELY recommend Acunetix. Acunetix is definitely one of the best Web-Crawlers out there, don't even bother trying to say different.

Even Robots.txt won't stop Acunetix's web-crawler (Which is very important if we actually want to get at useful files).

SUBDOMAINS

If the webmaster is smart, they will sometimes use sub-domains to hide certain admin-pages, or even files. You can tell what they may, or may not have open if you scan the ports with Nmap. Nmap will list the open ports of the website. If it has an SMTP port open, that may mean you can access an email login. Which may or may not contain valuable information.

Again, you can use Acunetix to check for subdomains. I don't have any cracks for acunetix (That I've posted) but I have seen some here on HF. I might (at some point) post a crack, and an easy one so you don't have to replace files and shit.

FTP

What is FTP? FTP stands for "File Transfer Protocol". If you have access to FTP, you can do absolutely anything you want. Unfortunately, you will not have permissions, unless you supply a username and password. But sometimes the FTP will be WIDE open for you to see. Sometimes

they'll list the admin page in there. To gain access to the FTP, you can either do:

Code ftp.site.com
or

Code http://www.site.com:21

Why did I just add a ":21" to the end of the site? Because 21 is the port for FTP. If I do :21, it'll connect to the port I have put after the ":". This is a very useful method, and I definitely recommend it.

SCANNER

Scanners are programs that will connect to the internet, and test certain pages of your website. A scanner I would recommend would be this one, by BeggFoMercy:

<https://hackforums.net/showthread.php?tid=2368870>

I vouch for his program, it is very useful.
There are other scanners out there, even web scanners.
Here's a link:
<http://tools.th3-0utl4ws.com/admin-finder/>

Just edit some stuff in Firebug, and enable the button, then you won't have to do the damn surveys.

If you're looking for another program that will scan, and you're looking for a very simple to use one, you can check out "Havij". I do not support the SQL Injection methods with it, because it's pretty "nooby". But using it to find Admin Pages is completely acceptable.

GOOGLE DORKS

Google dorks are keywords you can use to search for exact things. Like this:

Code inurl:admin.php

That will look for any site that has admin.php in it. I usually use these dorks if I'm looking for an admin page.

Code site:site.com inurl:admin
site:site.com intext:login
site:site.com intext:admin
site:site.com intitle:login
site:site.com intitle:admin
Those should help!

Well, that's pretty much it. Thanks for reading the tutorial, and I hope this helps you out! These methods are extremely useful, I find admin pages A LOT with these methods, don't doubt them until you try them.

Thanks!

joomlafkr - April 10, 2012, 3:14 pm

Actually i was writing on the same subject but you did fine !

i had like 1 other way to find the admin panel that will make finding it to be 100% :p

Nice job there dude !

TwinBlade - April 10, 2012, 3:18 pm

Nice, am downloading it now..

and btw, does every website must have an admin login page?
cuz some doesnt seem to have any..

and btw, great text designs..

Exploithero - April 10, 2012, 3:20 pm

Niceeee!! Very helpfull thread! Bookmarked;) :D thanks

zer0pwn - April 10, 2012, 3:26 pm

(Apr 10, 2012 03:14 PM)joomlafkr Wrote: [\[CITE\]](#) Actually i was writing on the same subject but you did fine !

i had like 1 other way to find the admin panel that will make finding it to be 100% :p

Nice job there dude !

Haha, thanks a lot :P

If you want, I can add your method (Obviously giving you credit)?

Volim te - April 10, 2012, 3:26 pm

Nice thread to bad some people don't use robots.txt to disallowed admin pages been indexed)-; and why use [ftp.site.com](ftp://site.com) or site.com:21? Just try <ftp://site.com>

Keif - April 10, 2012, 3:27 pm

Stop being so HQ man you're killing me xD

zer0pwn - April 10, 2012, 3:27 pm

(Apr 10, 2012 03:26 PM)Slen Wrote: [\[CITE\]](#) Nice thread to bad some people don't use robots.txt and why use [ftp.site.com](ftp://site.com) or site.com:21 just try <ftp://site.com>

If you do

Code ftp.site.com

It'll automatically change to "ftp://site.com" or "ftp://ftp.site.com". I thought it'd be easier for people to understand, so just did the "ftp.site.com".

Volim te - April 10, 2012, 3:29 pm

(Apr 10, 2012 03:18 PM)TwinBlade Wrote: [\[CITE\]](#) Nice, am downloading it now..

and btw, does every website must have an admin login page?
cuz some doesnt seem to have any..

and btw, great text designs..No lots of people just use CPanel or something unless it's a user login kind of site.

zer0pwn - April 10, 2012, 3:32 pm

(Apr 10, 2012 03:29 PM)Slen Wrote: [\[CITE\]](#) No lots of people just use CPanel or something unless it's a user login kind of site.

That's not completely true.

If you're a good webmaster (Which people really try to be, because they want money) they'll add a User Admin Login, so that they can actually understand what they're doing.

But yeah, not ALL sites will have custom admin pages, but if you find Admin Credentials, obviously

there's one hidden somewhere right?

OH YEAH! I forgot to add that you can check the normal user login aswell.

BeggFoMercy - April 10, 2012, 3:39 pm

Ahaha awesomest tutorial about admin page finding , Thanks for adding my tool though :D !

Volim te - April 10, 2012, 3:40 pm

(Apr 10, 2012 03:32 PM)Zer0Pwn Wrote: [\[CITE\]](#) That's not completely true.

If you're a good webmaster (Which people really try to be, because they want money) they'll add a User Admin Login, so that they can actually understand what they're doing.

But yeah, not ALL sites will have custom admin pages, but if you find Admin Credentials, obviously there's one hidden somewhere right?

OH YEAH! I forgot to add that you can check the normal user login aswell. Very true but the admin credentials might not even be for that script Say the page /index.php?id=xyz is vul I select the DBs that MySQL user is using and bam I find mybb_database etc if you get what I mean.

Anyway I find mass file checking works well if there is not allowed files in robots.

zer0pwn - April 10, 2012, 3:45 pm

(Apr 10, 2012 03:40 PM)Slen Wrote: [\[CITE\]](#) Very true but the admin credentials might not even be for that script Say the page /index.php?id=xyz is vul I select the DBs that MySQL user is using and bam I find mybb_database etc if you get what I mean.

Anyway I find mass file checking works well if there is not allowed files in robots.

That's also true.

When you said Mass File Checking I thought of Google Dorks (Because it checks for keywords). So I added that in the tut.

Thanks for the posts though.

Zhen. - April 10, 2012, 7:28 pm

Nice tutorial brah.

Would be pretty useful for everyone searching for admin.

Keep up the good work! <3

zer0pwn - April 10, 2012, 7:37 pm

(Apr 10, 2012 07:28 PM)-Zer0Freak- Wrote: [\[CITE\]](#) Nice tutorial brah.

Would be pretty useful for everyone searching for admin.

Keep up the good work! <3

Thanks :D

-notices how we look so epic with our sigs matching-

Zhen. - April 10, 2012, 7:46 pm

(Apr 10, 2012 07:37 PM)Zer0Pwn Wrote: [\[CITE\]](#) Thanks :D

-notices how we look so epic with our sigs matching-

-notices the same thing and fuck yea it's damn epic!-

Anytime bro <3