

Forum:[Hack Forums](#)

Thread: [find admin page](#)

arav - August 1, 2024, 3:43 am

I can't find the admin page of a site, can someone explain to me how to find it (I'm new to website hacking)

then if someone has free time can help me also with the "next steps xD"

?Rednix™ - August 1, 2024, 3:52 am

(Aug 1, 2024 03:43 AM)arav Wrote: [\[CITE\]](#) I can't find the admin page of a site, can someone explain to me how to find it (I'm new to website hacking)

then if someone has free time can help me also with the "next steps xD"

You could try doing something like [this, click here.](#)

arav - August 1, 2024, 4:20 am

(Aug 1, 2024 03:52 AM)?Rednix™ Wrote: [\[CITE\]](#) You could try doing something like [this, click here.](#) I already tried, it doesn't work)-:

?Rednix™ - August 1, 2024, 4:21 am

(Aug 1, 2024 04:20 AM)arav Wrote: [\[CITE\]](#) I already tried, it doesn't work)-:

In that case you have to use something more advanced. Look into Github, a lot of great scripts for that.

Try this one. Very easy to setup and use, and is up to date with a large database:

<https://github.com/mlcHyAmRaNe/okadminfinder>

BiNBo - August 1, 2024, 6:27 am

What you're looking to do is web fuzzing and discovery. To get started, you'll need to use one of many tools out there (GoBuster, FFUF, RustBuster, etc.) and see if you can find it that way. Sometimes it's not so straightforward, but that should at least get you started. As for a good wordlist, just look up SecLists from Daniel Miessler. There's some great ones to get started with there.

DramaKing - August 1, 2024, 6:51 am

If a tool like dirbuster doesn't find an admin page, then the target may only be using a cPanel or is only using the server backend. You have a plan for getting a login?

arav - August 1, 2024, 7:36 am

(Aug 1, 2024 06:51 AM)DramaKing Wrote: [\[CITE\]](#) If a tool like dirbuster doesn't find an admin page, then the target may only be using a cPanel or is only using the server backend. You have a plan for getting a login?

I managed to find the page in phpMyAdmin... only now I have no idea how to access it. any advice?

DramaKing - August 1, 2024, 9:10 am

Start with learning PHP?

(Aug 1, 2024 07:36 AM)arav Wrote: [\[CITE\]](#) I managed to find the page in phpMyAdmin... only now I have no idea how to access it. any advice?

arav - August 1, 2024, 10:07 am

(Aug 1, 2024 09:10 AM)DramaKing Wrote: [\[CITE\]](#) Start with learning PHP?

I already know a minimum of it, but from knowing php to penetrating a site there's a lot of water involved.

lasvegas - August 1, 2024, 10:30 am

(Aug 1, 2024 03:43 AM)arav Wrote: [\[CITE\]](#) I can't find the admin page of a site, can someone explain to me how to find it (I'm new to website hacking)

then if someone has free time can help me also with the "next steps xD"
send the site

arav - August 1, 2024, 10:33 am

(Aug 1, 2024 10:30 AM)lasvegas Wrote: [\[CITE\]](#) send the site
<https://privnote.com/NRFW61ID#CBB2rGosW>

famedgod6 - August 1, 2024, 7:26 pm

That shits easy , just use a google dork to find an admin login page

try this basic one: inurl /admin/login.aspx

there are countless dorks for this thing.

hero hack - August 2, 2024, 7:47 am

hahaha[[color=#2ECC40](#)][[/color](#)
]

?[Video: <http://vews>][img]dfwedw[/img]wada???? [warn]

w0rd - August 2, 2024, 9:03 am

Assetfinder, dirsearch, etc. could also be a subdomain admin.domain.com. Or just use google, site:sitename "login" or site:sitename "admin". If its cPanel, have fun.

Nightshader - August 2, 2024, 6:02 pm

i have an admin panel finder from github that works pretty well for this. also its bad english makes it funny but hell of a tool and its a good addition to kali linux toolkit,
<https://github.com/C4ssif3r/admin-panel-finder>

happygonutty - August 3, 2024, 5:07 am

(Aug 1, 2024 03:43 AM)arav Wrote: [\[CITE\]](#) I can't find the admin page of a site, can someone explain to me how to find it (I'm new to website hacking)

then if someone has free time can help me also with the "next steps xD"
Simple, find out the tech stack used on your target and do some port scanning to identify your target.

Ghostboy-287 - August 4, 2024, 12:20 am

simple method:

Code # install okadminfinder
pip3 install okadminfinder

to use default wordlist
okadminfinder -u "URL"
advanced method:

```
Code # if not yet installed: sudo apt install seclists
# to list web-content wordlists
ls /usr/share/seclists/Discovery/Web-Content/
# using for example : directory-list-2.3-big.txt
okadminfinder -u "URL" -w "/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt"
usage preview
```

arav - August 4, 2024, 12:57 am

(Aug 4, 2024 12:20 AM)Ghostboy-287 Wrote: [\[CITE\]](#) simple method:

Code # install okadminfinder

pip3 install okadminfinder

to use default wordlist

```
okadminfinder -u "URL"
```

advanced method:

Code # if not yet installed: `sudo apt install seclists`

to list web-content wordlists

Is /usr/share/seclists/Discovery/Web-Content/

```
# using for example : directory-list-2.3-big.txt
```

```
okadminfinder -u "URL" -w "/usr/share/seclists/Discovery/Web-Content/directory-list-2.3-big.txt"
```

usage preview

thanks you , it worked

Ghostboy-287 - August 4, 2024, 7:55 am

(Aug 4, 2024 12:57 AM)arav Wrote: [CITE](#) thanks you , it worked

you're welcome,

if you get any issue, you're free to open an issue or asking me

ERTAN - September 21, 2024, 10:38 am

(Aug 1, 2024 03:43 AM)arav Wrote: [\[CITE\]](#) I can't find the admin page of a site, can someone explain to me how to find it (I'm new to website hacking)

then if someone has free time can help me also with the "next steps xD"

[deleted]

Link2 - September 25, 2024, 6:33 pm

But what's the purpose of finding an admin page? If it's a worthy target you won't find it anyway, because 1) it probably has an unguessable name (like /admin_p5GJyaTh8R6B9xSqXCd6FJcS) and 2) is only accessible from certain ip addresses. And even if you manage to get around that, there are still some quests waiting for ya, so what's the next step? Hacking the password? Yeah, if you try bruteforcing a website, you'll be blocked due to too many requests in like 2 seconds. But let's say with a little bit of luck your magic tool guesses the 30-character long password correctly on the first handful attempts (yes i know, in reality it would take approximately 35.700.000.000.000.000.000.000.000.000.000.000.000.000.000.000 years but let's say it's your lucky day), a valuable target will have at least one additional authentication method, maybe some code via email, sms or 2fa.

So, in summary there are quite some challenges

- Unguessable URL path, IP Whitelisting, SSL, Accessible only via VPN

- Rate Limiting, Bruteforce Prevention, Geoblocking, Useragent validation, time based access control, CSP, security headers

- Strong password (20 or more characters), MFA (email, sms, 2fa), client certificates, credential rotation

- Captcha, hidden honeypot fields
- Audit logs, Login notification alerts

I'm not sure if your supercomputer can do that^^

But the good thing is, some people are stupid af and actually hire and pay people that are even more stupid than themselves, so it's not an impossible thing, there's still a chance. Good luck :)

looser69 - September 26, 2024, 3:48 am

Thanks for thread 1!

DramaKing - September 26, 2024, 6:12 am

(Sep 25, 2024 06:33 PM)xmgr Wrote: [\[CITE\]](#) But what's the purpose of finding an admin page? If it's a worthy target you won't find it anyway, because 1) it probably has an unguessable name (like /admin_p5GJyaTh8R6B9xSqXCd6FJcS) and 2) is only accessible from certain ip addresses. And even if you manage to get around that, there are still some quests waiting for ya, so what's the next step? Hacking the password? Yeah, if you try bruteforcing a website, you'll be blocked due to too many requests in like 2 seconds. But let's say with a little bit of luck your magic tool guesses the 30-character long password correctly on the first handful attempts (yes i know, in reality it would take approximately 35.700.000.000.000.000.000.000.000.000.000.000.000.000.000.000 years but let's say it's your lucky day), a valuable target will have at least one additional authentication method, maybe some code via email, sms or 2fa.

So, in summary there are quite some challenges

- Unguessable URL path, IP Whitelisting, SSL, Accessible only via VPN
- Rate Limiting, Bruteforce Prevention, Geoblocking, Useragent validation, time based access control, CSP, security headers
- Strong password (20 or more characters), MFA (email, sms, 2fa), client certificates, credential rotation
- Captcha, hidden honeypot fields
- Audit logs, Login notification alerts

I'm not sure if your supercomputer can do that^^

But the good thing is, some people are stupid af and actually hire and pay people that are even more stupid than themselves, so it's not an impossible thing, there's still a chance. Good luck :)

Tone it down a little. 3-character password is unrealistic. Bruteforcing a cPanel or similar will probably not result in lockout after a certain number of attempts. 1 and 2 are also highly unlikely. Useragent verification will be unheard of. MFA for cPanel is an option, but I would consider it unexpected.

Null State - September 26, 2024, 5:51 pm

(Sep 25, 2024 06:33 PM)xmgr Wrote: [CITE] But what's the purpose of finding an admin page? If it's a worthy target you won't find it anyway, because 1) it probably has an unguessable name (like /admin_p5GJyaTh8R6B9xSqXCd6FJcS) and 2) is only accessible from certain ip addresses. And even if you manage to get around that, there are still some quests waiting for ya, so what's the next step? Hacking the password? Yeah, if you try bruteforcing a website, you'll be blocked due to too many requests in like 2 seconds. But let's say with a little bit of luck your magic tool guesses the 30-character long password correctly on the first handful attempts (yes i know, in reality it would take approximately 35.700.000.000.000.000.000.000.000.000.000.000.000.000.000.000 years but let's say it's your lucky day), a valuable target will have at least one additional authentication method, maybe some code via email, sms or 2fa.

So, in summary there are quite some challenges

- Unguessable URL path, IP Whitelisting, SSL, Accessible only via VPN

- Rate Limiting, Bruteforce Prevention, Geoblocking, Useragent validation, time based access control, CSP, security headers
- Strong password (20 or more characters), MFA (email, sms, 2fa), client certificates, credential rotation
- Captcha, hidden honeypot fields
- Audit logs, Login notification alerts

I'm not sure if your supercomputer can do that^^

But the good thing is, some people are stupid af and actually hire and pay people that are even more stupid than themselves, so it's not an impossible thing, there's still a chance. Good luck :)
You obviously have SOME idea of what you're describing, but you've also likely had zero actual experience with the subject...

There's no reason to go off the way you did, at all. You also assume way too much perfection from the humans configuring stuff. Why do you think stuff gets hacked? Oversights, improper implementations, etc. You saying it's extremely unlikely OP will accomplish anything with this is about the same odds as OP or anyone else trying to get in WOULD find a way. Go look at Bugcrowd or HackerOne, and let me know how many wtf bugs you see.

To add for OP: <https://github.com/carpdm20/awesome-hacking?tab=readme-ov-file#tutorials>

I don't like spoonfeeding knowledge, it shows zero initiative and honestly isn't a good look for a person wanting to learn Cybersecurity, especially offensive side. Read the tutorials that interest you there, and see what you don't understand/need help with. Then use Google. After, PM if you're actually stuck and getting nowhere.

Link2 - September 28, 2024, 2:16 pm

(Sep 26, 2024 05:51 PM)HOS7 187 Wrote: [\[CITE\]](#) [...your whole post..]

Thanks for writing your opinion :) I pointed out some of the challenges that might get in the way, even tho i may have exaggerated a lil bit, but what I wrote is not a list of "all security mechanisms that you will definitely face" but more like "just so you know, THAT exists and if some clever person cared about security, you'll for sure have a hard time". Unfortunately I can't understand what is making you so upset about that. I did not even offend anyone, I re-read my post again and yeah, couldn't find any insults.

(Sep 26, 2024 06:12 AM)DramaKing Wrote: [\[CITE\]](#) 3-character password is unrealistic. Bruteforcing a cPanel or similar will probably not result in lockout after a certain number of attempts. 1 and 2 are also highly unlikely. Useragent verification will be unheard of. MFA for cPanel is an option, but I would consider it unexpected

I assume you mean the 30 that i mentioned before, and yes, that is actually totally realistic. I and many other programmers I know use up to 64 chars-long (different, of course, lul) passwords for every single account or login. What you consider "unexpected", "unlikely" or "unrealistic" is totally fine, no problem with that at all, what I do not understand is, what's even the point of telling me that? I listed a bunch of security mechanisms and some made up scenarios, just for the sake of information and completeness and to give a rough example of things that can happen. I did not talk about "likeliness" or "probability". This is for OP to decide, don't you think so?

And yes, you are both totally right, I'm not some super hacker or whatever thing (in fact, I can not find the place where I claimed or pretended to be so). What I CAN do and what I am also allowed to do, is talking about things that come to my mind. Knowing THAT a security mechanism like, let's say, "Bruteforce prevention" exists and what it roughly means, does not imply that I am an expert in the "Bruteforce prevention" topic, and not being an expert does not prohibit me talking about things, does it? I am a senior php developer, my specialty is NOT the security topic, although of course I

know a lil bit here and there, XSS, SQL Injection, CSRF, session hijacking .. blahblah so mostly only all that kinda things related to web and php and ssh and linux servers, and that's already where my knowledge ends. I did never do things like bruteforce attacks or tried cracking passwords with rainbow tables or whatever tools the cool kids use nowadays, but I should be free to talk about everything I want, shouldn't I?

DramaKing - September 28, 2024, 4:24 pm

(Sep 28, 2024 02:16 PM)Link2 Wrote: [\[CITE\]](#) Thanks for writing your opinion :) I pointed out some of the challenges that might get in the way, even tho i may have exaggerated a lil bit, but what I wrote is not a list of "all security mechanisms that you will definitely face" but more like "just so you know, THAT exists and if some clever person cared about security, you'll for sure have a hard time". Unfortunately I can't understand what is making you so upset about that. I did not even offend anyone, I re-read my post again and yeah, couldn't find any insults.

I assume you mean the 30 that i mentioned before, and yes, that is actually totally realistic. I and many other programmers I know use up to 64 chars-long (different, of course, lul) passwords for every single account or login. What you consider "unexpected", "unlikely" or "unrealistic" is totally fine, no problem with that at all, what I do not understand is, what's even the point of telling me that? I listed a bunch of security mechanisms and some made up scenarios, just for the sake of information and completeness and to give a rough example of things that can happen. I did not talk about "likeliness" or "probability". This is for OP to decide, don't you think so?

And yes, you are both totally right, I'm not some super hacker or whatever thing (in fact, I can not find the place where I claimed or pretended to be so). What I CAN do and what I am also allowed to do, is talking about things that come to my mind. Knowing THAT a security mechanism like, let's say, "Bruteforce prevention" exists and what it roughly means, does not imply that I am an expert in the "Bruteforce prevention" topic, and not being an expert does not prohibit me talking about things, does it? I am a senior php developer, my specialty is NOT the security topic, although of course I know a lil bit here and there, XSS, SQL Injection, CSRF, session hijacking .. blahblah so mostly only all that kinda things related to web and php and ssh and linux servers, and that's already where my knowledge ends. I did never do things like bruteforce attacks or tried cracking passwords with rainbow tables or whatever tools the cool kids use nowadays, but I should be free to talk about everything I want, shouldn't I?

So everyone uses the password practices that you and the developers you know use? I know people at my office that use dictionary words, communal passwords, and their names for passwords. One of these is the 'webmaster'. My supervisor criticizes me for using long, unique passwords (long being 18-19 character phrases). My point is that most people like to use passwords that they remember. If password policy says 16 characters with upper- and lowercase letters, numbers, and symbols, they'll keep near the minimum. If they need to enter strings that are 30-64 characters, they'll write it onto a sticky note and still complain.

Link2 - September 29, 2024, 2:10 am

Thanks for your reply.

(Sep 28, 2024 04:24 PM)DramaKing Wrote: [\[CITE\]](#) So everyone uses the password practices that you and the developers you know use?

What, no, where did I say that? But using secure passwords is important, or is that not a thing anymore? I mean, this forum is about hacking things and stuff, but security is a quite nearby topic, isn't it? If there are not any defense and security mechanisms, then it isn't "hacking" anymore, but just like going through an open door .. ? I don't know who you are and what you know about the topic, but in real world, a person (e.g. a software developer or sysadmin) that is building a platform or website or application or network that is somehow accessible or available from the outside, will do

everything to protect it from improper use. And that is not an opinion, that is facts, I'm not arguing about that, this is basic common sense. And yes, using (and forcing to use) secure passwords is one of the steps to make things more secure. For passwords, it is more important that they are secure than whether or not they are easy to remember. That's what password managers are built for, to use secure passwords you do not have to remember (and I'm talking about secure, local password manager applications like KeePass, not about online password manager websites that get magically hacked and leaked every once in a while).

I mean, ok, you "could" lower the password security requirements if there is an additional authentication factor enabled. But, tbh, if you're used to password managers, it's really not such a big effort, speaking from my experience. Or, if the service provides authentication via Passkeys, that would also be an option (as much as I know about this, it's some passwordless authentication thing where you can use biometrics via your local device, I did not have time to have a closer look at that yet, maybe it's a good alternative).

(Sep 28, 2024 04:24 PM)DramaKing Wrote: [\[CITE\]](#) My supervisor criticizes me for using long, unique passwords (long being 18-19 character phrases).
That is your problem. lul

(Sep 28, 2024 04:24 PM)DramaKing Wrote: [\[CITE\]](#) My point is that most people like to use passwords that they remember.

First, this is not a point. Point. Most people also do not like to get hacked, but you cannot have two things at the same time that are mutually exclusive. What most people do is not automatically the right thing to do.

Null State - October 2, 2024, 1:57 am

(Sep 28, 2024 02:16 PM)Link2 Wrote: [\[CITE\]](#) Thanks for writing your opinion :) I pointed out some of the challenges that might get in the way, even tho i may have exaggerated a lil bit, but what I wrote is not a list of "all security mechanisms that you will definitely face" but more like "just so you know, THAT exists and if some clever person cared about security, you'll for sure have a hard time". Unfortunately I can't understand what is making you so upset about that. I did not even offend anyone, I re-read my post again and yeah, couldn't find any insults.

I assume you mean the 30 that i mentioned before, and yes, that is actually totally realistic. I and many other programmers I know use up to 64 chars-long (different, of course, lul) passwords for every single account or login. What you consider "unexpected", "unlikely" or "unrealistic" is totally fine, no problem with that at all, what I do not understand is, what's even the point of telling me that? I listed a bunch of security mechanisms and some made up scenarios, just for the sake of information and completeness and to give a rough example of things that can happen. I did not talk about "likeliness" or "probability". This is for OP to decide, don't you think so?

And yes, you are both totally right, I'm not some super hacker or whatever thing (in fact, I can not find the place where I claimed or pretended to be so). What I CAN do and what I am also allowed to do, is talking about things that come to my mind. Knowing THAT a security mechanism like, let's say, "Bruteforce prevention" exists and what it roughly means, does not imply that I am an expert in the "Bruteforce prevention" topic, and not being an expert does not prohibit me talking about things, does it? I am a senior php developer, my specialty is NOT the security topic, although of course I know a lil bit here and there, XSS, SQL Injection, CSRF, session hijacking .. blahblah so mostly only all that kinda things related to web and php and ssh and linux servers, and that's already where my knowledge ends. I did never do things like bruteforce attacks or tried cracking passwords with rainbow tables or whatever tools the cool kids use nowadays, but I should be free to talk about everything I want, shouldn't I?

Go re-read again, your first paragraph. Literally the entire thing is worded in a sarcastic tone. If you can't see that, can't really help you.

your last paragraph literally implied OP was really stupid lmao.
To quote:

I'm not sure if your supercomputer can do that^^

But the good thing is, some people are stupid af and actually hire and pay people that are even more stupid than themselves, so it's not an impossible thing, there's still a chance. Good luck :)

You're insinuating OP's pc of unknown spec is too shit to accomplish something that isn't really necessarily resource intensive. You also flat out said, on the positive side for you OP, some interviewers are stupid as fuck, and might actually hire and pay you more than your worth so there's a chance. Good luck :)

Before you say you meant just in general, you were clearly talking directly to OP lmao.

Link2 - October 2, 2024, 3:17 pm

Thanks for your reply. As said I was exaggerating a bit, and the supercomputer thing was sarcastic and meant to be funny, the trailing "^^" indicates that. Obviously I messed that one up.. My message was clearly not condescending or offending and certainly not insulting. However, it's nearly impossible to choose words in a way that there is not any room left for interpretation, but that's not on me then. From my side, I already clarified the open questions (more than necessary), if you still do not like my post, that's okay, I can't change that :) I definitely appreciate the effort of hacking, which doesn't mean tho that I am not allowed to point out the difficulties that may come in the way. It's okay when not everyone can understand my intention or sense of humour, if there's a question about it, just ask (as some of you already did). Despite that, in my opinion we already wasted enough time with more or less unproductive off topic stuff, but you can still reach out to me via PM if you want to further express your displeasure about my style of writing, not a problem at all. In return, next time I promise to "tone it down a little" (as suggested) to spread a little bit more positive vibes ;)

PS: as a non-native English speaker, I hope my posts are understandable good enough^^

GovernmentGradeGlow - October 3, 2024, 9:31 pm

(Aug 1, 2024 03:43 AM)arav Wrote: [CITE](#) I can't find the admin page of a site, can someone explain to me how to find it (I'm new to website hacking)

then if someone has free time can help me also with the "next steps xD"

The first step is simple, there's plenty of tools you can use to find a "/Admin" Directory or other hidden directories on a host or server, first things first is to run a NMAP scan to find open ports and what kind they are once you have your http/https port you can find out what kind of server it is running on and OS, and if there's any other open ports on the IP target you have to remember these because you may be able to exploit one of these ports to access the target.

Now we have our Target's IP and ports, we can run a tool like gobuster to find hidden directories and then use different wordlists payloads to bruteforce & sniff out hidden directories like "/admin, /wp-admin, /login, /assets, /admin.php, /login.php, etc.. now if you end up finding the /admin page, you should be checking out everything the page has to offer, use your Browser's Developer Tools to look at the /admin pages source code and components. Find out what kind of Server the site is on or what was used to create the website, once you know these details you should be googling exploits and vulns.

You can also run the tool nikto which is pretty simple, just run the nikto -h url and it will show you all of the possible exploits can be used on the Target URL you gave it, or you can use Metasploit to find out other possible exploits for the Target URL

Lastly, depending on what kind of elements your website has, there's all types of other ways to test the /admin page like XSS, sql injection, SSRF, or use a tool like burpsuite to test http requests and a bunch of other stuff. Hope this helps a bit, Honestly if I can give anyone advice if you wanna learn hacking you have to start from the beginning, learn the fundamentals, don't skip steps and eventually you'll come across exactly what you wanna learn and you'll have the experience and knowledge to learn it the right way.

7 - October 3, 2024, 9:34 pm

This thread developed quite hard and strong.

He wants to find an admin page

<https://github.com/C4ssif3r/admin-panel-finder>

let him do one step at a time..

also check dns using emulation and records

JACC_1997 - October 5, 2024, 6:58 am

escanea tu ip publica, encontraras muchos administradores de paginas