

Forum:[Hack Forums](#)

Thread: [Hack 200 Wordpress Websites Every Day On Automation](#)

GlitchPool - November 21, 2024, 2:33 pm

What's up, legends?

You've stumbled upon a goldmine. Today, I'm going to show you how to break into WordPress admin panels like a pro without lifting a finger. No coding skills? No problem. It's all about using automation to crack weak credentials.

Here's the deal: WordPress powers over 40% of the web, and most site owners are lazy. They use default usernames like admin and passwords as bad as 123456. You're not exploiting vulnerabilities here—you're taking advantage of human stupidity.

This process is known as bruteforcing—testing thousands of username-password combinations against a WordPress login page until you find the one that works. With the right tools and a little creativity, you'll be logging into admin dashboards in no time.

Step 1: Understand the Basics

Every WordPress site has a login page located at /wp-login.php. Your goal is to find this page, use a script to try different combinations of usernames and passwords, and eventually break in.

Here's why this works:

Most site owners never change their default login credentials.

Password security is an afterthought for many small business owners.

Automated tools can try thousands of combinations in minutes, doing all the heavy lifting for you.

One of the most popular tools for bruteforcing is Hydra, which is available for free on GitHub. You can find plenty of tutorials online that explain how to set it up and use it for WordPress sites.

Step 2: Find WordPress Sites to Target

You can't hack what you can't find. Your first job is to collect a list of WordPress sites to target.

Use Google Dorks

Google is your best friend when it comes to digging up targets. Try these search queries:

`inurl:wp-login.php`

`intitle:"WordPress Admin"`

These dorks will give you direct links to WordPress login pages. Copy and save them to a text file for later.

Diversify Your Sources

Don't stop at Google. Explore smaller search engines or even forums where people list vulnerable sites.

Save everything into a list—this is your goldmine of targets.

Step 3: Automate the Bruteforce Attack

Now comes the fun part. You'll be using a tool to automatically test username-password combinations on the login pages you found.

Option 1: Use a WordPress Bruteforcing Tool

Search GitHub for "WordPress bruteforce tool," and you'll find plenty of scripts specifically designed for this purpose. Download one and follow its setup instructions.

Option 2: Use Hydra

Hydra is a more advanced tool that works across multiple platforms, including WordPress. If you're new to this, search YouTube for tutorials on using Hydra to bruteforce WordPress sites. It's straightforward once you see it in action.

Step 4: Build Your Username and Password Lists

No bruteforce attack works without solid username and password lists. These lists tell your tool which combinations to try.

Here's how to find them:

Search GitHub for "common usernames list" or "top passwords list."
Download these files and customize them if needed.

Start with obvious usernames like:

admin
editor
administrator

Pair them with common passwords like:

123456
password
admin123

This combination of usernames and passwords is your ticket in.

Step 5: Run the Attack

With your tool set up and your lists ready, it's time to run the attack. Point your script to the login pages from your target list, load your username and password files, and let it do its thing.

Here's what happens:

The tool sends login requests to each WordPress site in your list.
It tries every username-password combination in your files.
When it finds a working login, it saves the credentials for you.

Automation means you can target hundreds of websites at once, maximizing your chances of success.

Step 6: What to Do with Access

Once you're in, you've got full control over the site. What you do next is entirely up to you. You could:

Browse their admin dashboard.

Change their settings.
Upload malicious plugins.

The possibilities are endless.
Why This Works

Careless Users: Most people don't take security seriously.
Automated Tools: They save you time and effort.
Massive Targets: With so many WordPress sites online, the opportunities are endless.

Final Tips

Keep It Low-Key

Don't target big companies or government sites unless you're ready for heat. Stick to small businesses and personal blogs.

Stay Consistent

The more sites you target, the higher your chances of finding vulnerable ones.

Learn from Your Mistakes

If one method doesn't work, tweak it and try again.

That's it, folks. With a little creativity and persistence, you'll be logging into WordPress admin panels like it's child's play. Have questions or need help? Hit me up on Telegram: [deleted]

Stay shady. ? [warn]

gaush - November 21, 2024, 3:57 pm

It's a gold mine brooo

Envy - November 21, 2024, 4:00 pm

It's crazy how much a simple rewrite and login security can prevent even the most basic attacks like this, yet no one does it.

GlitchPool - November 22, 2024, 2:05 am

(Nov 21, 2024 05:00 PM)Envy Wrote: [\[CITE\]](#) It's crazy how much a simple rewrite and login security can prevent even the most basic attacks like this, yet no one does it.
YESSIR!

shipments - December 10, 2024, 2:57 pm

Newb here lol.

Is there no request limits/measures in place to prevent brute-forcing on WP sites?

AbuAbiat - December 11, 2024, 6:35 am

Nice Post dude! Thanks

Reiss0101 - December 15, 2024, 2:24 am

Thanks for the information

DarkRoot - December 15, 2024, 2:37 am

that's cool info, but I understand the forum policy blocked the telegram link.

Crabbe23 - *January 24, 2025, 3:04 pm*
how do you make money with this?

kovacicmen12 - *January 25, 2025, 2:46 pm*
ty bro.....