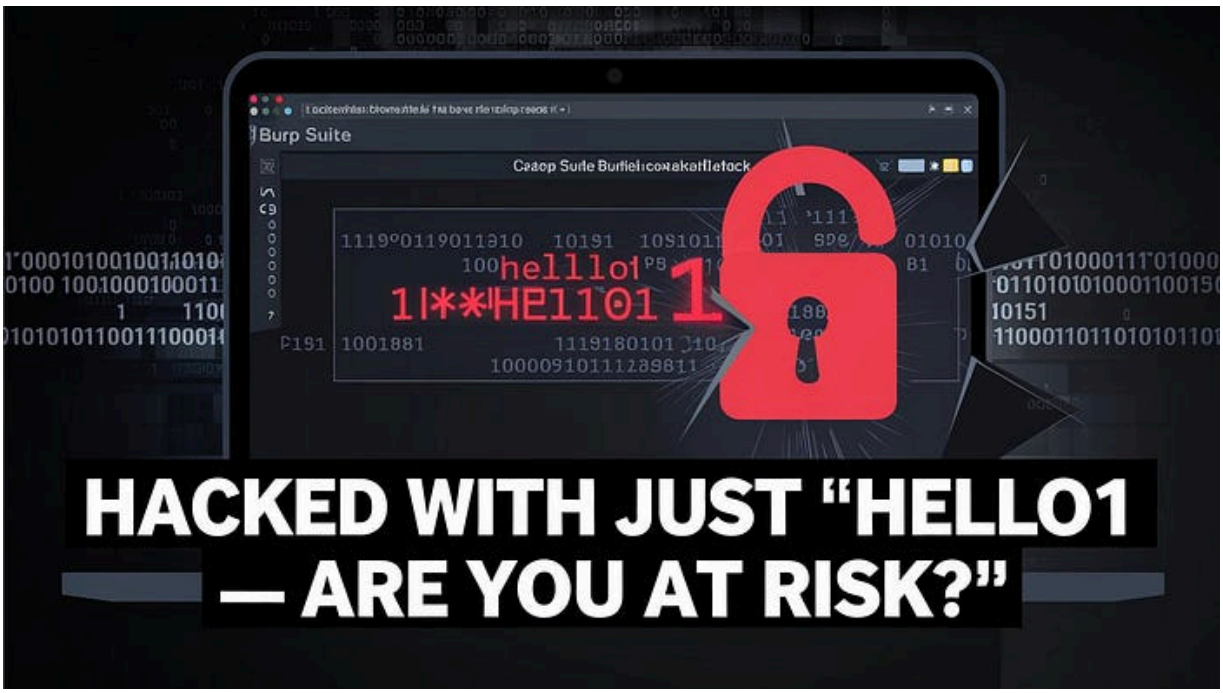
< Go to the original



How I Hacked an Admin Panel with Just a Weak Password (and Why You're at Risk Too)

I never thought a password as simple as 'hello1' could unlock an admin dashboard controlling millions of user records.

Ibtissam hammadi

Follow

androidstudio · July 12, 2025 (Updated: July 12, 2025) · Free: No

But there it was — a single click away from disaster.

This wasn't a sophisticated cyberattack. No zero-day exploits, no advanced malware.

Just **a weak password** and a security oversight that could've exposed **10 million users' data.**

Reconnaissance: The Hunt for Weak Points

Before any hack comes **reconnaissance** — the art of finding cracks in the armor.

Step 1: Subdomain Discovery

I started with SecurityTrails and Google Dorks, searching for:

```
Copy

site:*.company.com admin
site:*.company.com login
```

Within minutes, I found:

```
Copy

admin.company.com
dashboard.company.com
```

Most companies hide admin panels behind these URLs. The problem? Many never change the default access rules.

Step 2: Testing for Entry Points

I fired up **Burp Suite**, the Swiss Army knife of hackers, and probed the login page.

- **User Enumeration Flaw:** The page leaked valid usernames when I entered **fake credentials**. A classic mistake.
- **Default Credentials Attempt:** I tried **admin:admin**, **admin:password123**, and then… **admin:hello1**.

Exploitation: The 5-Second "Hack"

This wasn't a brute-force attack with **10,000 passwords per second.** Just **a short list of common weak passwords:**

```
Copy

admin
password
123456
hello1
companyname2023
```

Burp Suite Intruder automated the process, but **anyone with patience could've done it manually.**

The real shock? The password wasn't even hidden — just plaintext in the HTTP request.

Impact: What Could've Happened

Once inside, I had **full control.** I could've:

✔ **Downloaded all user databases** (emails, passwords, credit cards)

✔ **Deleted entire production tables** (bye-bye, customer data)

✔ **Sold access on the dark web** (for **$5,000+**, based on similar breaches)

The worst part? **No alerts were triggered.** No rate limits. No **Multi-Factor Authentication (MFA).**

This wasn't hacking. It was walking through an unlocked door.

For Companies:

- **Enforce 12+ character passwords** (with numbers + symbols)
- **Enable MFA** (SMS or authenticator apps)
- **Monitor failed logins** (block IPs after 5 attempts)
- **Never expose admin panels to the public** (IP whitelist them)

For Ethical Hackers:

- Always test default credentials (You'd be surprised how often they work)
- **Use Burp Suite Intruder** for brute-force testing (legally, on bug bounty programs)
- **Report responsibly** (Don't touch data — just prove the flaw)

Would Your Admin Panel Survive a 'hello1' Test?

If I — a random researcher — could break in with **a toddler's password**, imagine what a **real hacker** could do.

This isn't about fear-mongering. It's a wake-up call.

Tag a developer who needs to see this. 👏 Clap if you learned something. 💬R Comment if you've seen worse passwords!

#cybersecurity #hacking #bug-bounty #tech #password-security