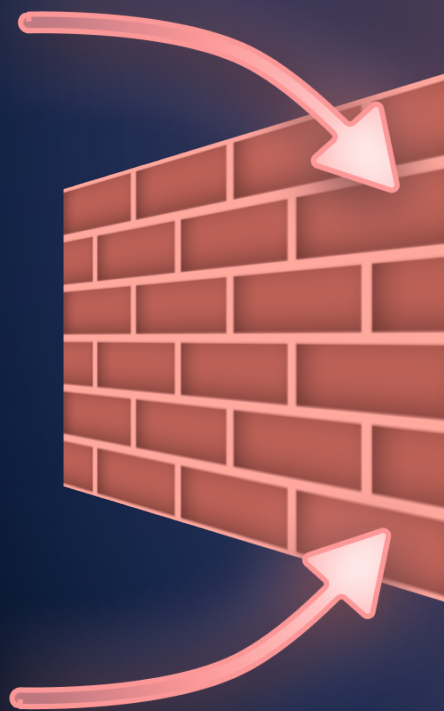


# Hydra or the Password Auditor on Pentest-Tools.com which is the best tool for brute-force attacks?

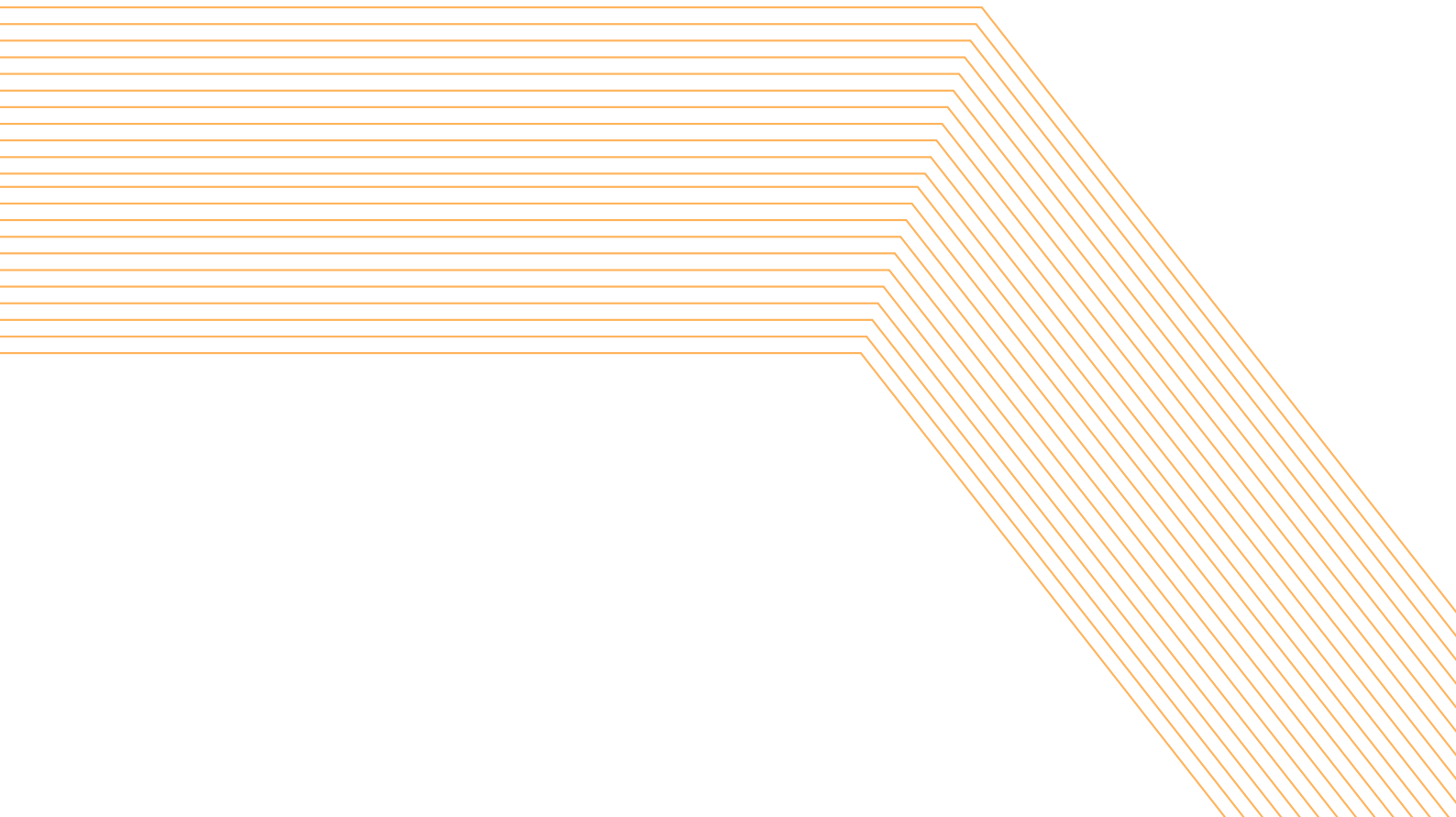


# When it comes to credential auditing, choosing the right tool can make all the difference.

This comparison puts **Hydra** and the **Password Auditor** to the test across **26 web applications** - including Microsoft Exchange, WordPress, and Joomla - to evaluate how effectively they:

- identify weak credentials
- navigate complex login forms
- overcome security defenses like CAPTCHAs and IP blocking.

## Find out which tool gets you in faster, smarter, and with less hassle.

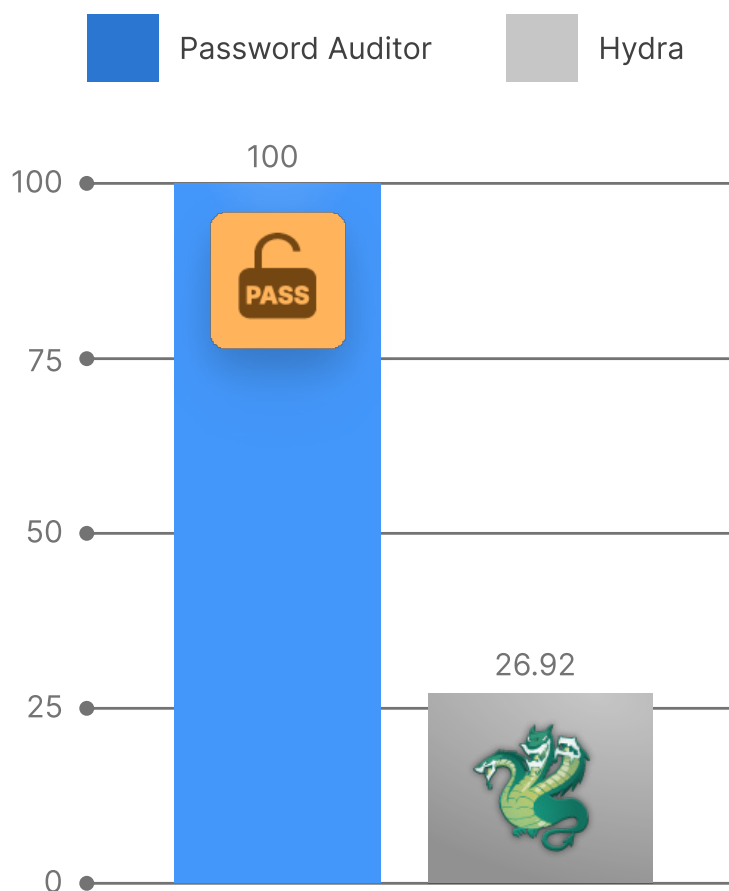


# Password bruteforcing efficiency rates

## Identifying valid credentials in a lab scenario

The **Password Auditor** on Pentest-Tools.com consistently demonstrated superior accuracy in identifying valid credentials across all 26 web applications. It achieved a **100% success rate** when tested with one valid and one invalid credential set.

**Hydra**, in contrast, identified only 7 valid credentials with a **27%** success rate for the single credential test scenario.



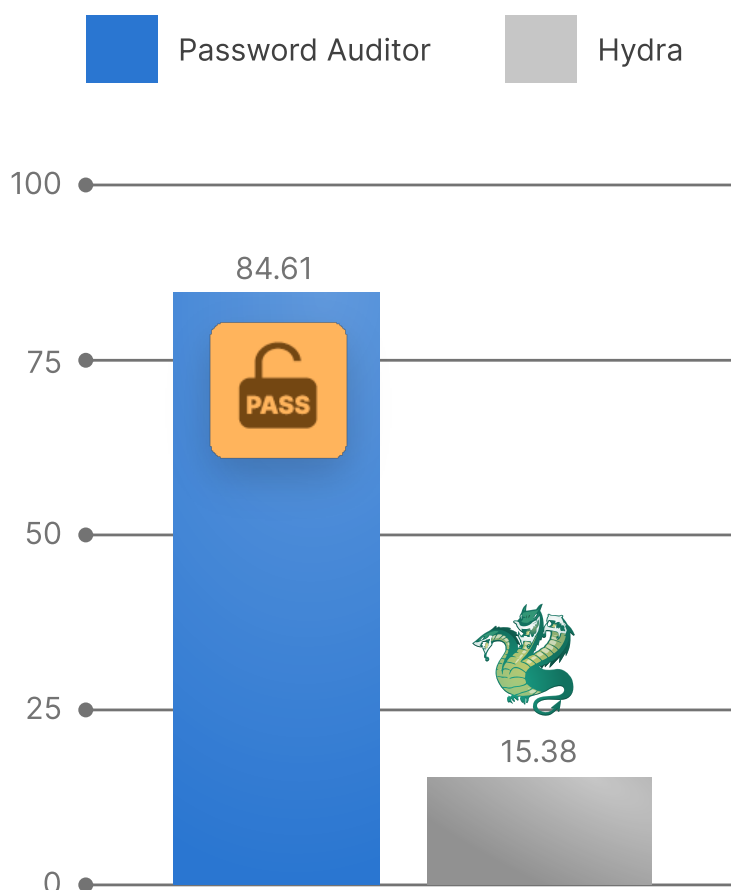
Detection % - Lab scenario  
Correctly identifying credentials

## Identifying valid credentials in a realistic scenario

When testing the 26 target apps with multiple credentials (one valid and 10+ invalid ones), the **Password Auditor** on Pentest-Tools.com maintained a high success rate of **84%**.

In this more complex scenario, **Hydra's** success rate dropped to **15%**, correctly identifying only 4 valid credentials.

This suggests Hydra struggles more with identifying valid credentials under varying conditions.



Detection % - **Realistic scenario**  
Correctly identifying credentials

## Handling application-specific defensive mechanisms

The **Password Auditor** on Pentest-Tools.com was notably effective in recognizing various defensive mechanisms like IP blacklisting, CAPTCHA, account lockout, and rate limiting. It provided **specific feedback** and **recommendations** to bypass or handle these defenses, which is crucial for real-life penetration testing where such measures are common.

**Hydra** faced challenges with certain applications that use web CSRF tokens or dynamic form protections. Because of its inability to handle client-side JavaScript token generation or CSRF token rotation, Hydra often marked valid and invalid attempts similarly, reducing its effectiveness. Workarounds exist, but they require several tools and do not fit the scope of this benchmark.

## Ease of use and setup

The **Password Auditor** on Pentest-Tools.com is more user-friendly with a **pre-configured interface** that makes setup simple. Security practitioners just need to specify the target, select the attack type, choose ports, and enable desired services. The tool also allows **scheduling** regular scans, enhancing its usability.

**Hydra** requires a more manual setup process, including crafting specific commands to find login endpoints and parameters, which is time-consuming. This setup complexity is a disadvantage in fast-paced testing environments where time efficiency is critical.

# Methodology for this bruteforce tools comparison

Testing period: July-August 2024

Evaluated on ability to identify:

- login endpoints
- login parameters
- error messages & protection mechanisms



26

HTTP applications tested



2

replicable test scenarios



2

wordlists with valid + invalid usernames  
& passwords



7

defensive measures tested

## Ability to work around encryption and token mechanisms

The **Password Auditor** effectively managed to bypass client-side encoding and token mechanisms by using its **pre-built configurations**.

This capability is particularly valuable for auditing web apps that implement client-side protections.

**Hydra**'s performance dropped significantly on platforms that used client-side hashing or encryption. Since Hydra doesn't operate in a browser environment, it couldn't replicate JavaScript-based hashing, limiting its effectiveness against apps like Adobe ColdFusion and JetBrains TeamCity, which use advanced encryption or client-side hashing.

## Overall performance

For security specialists looking for a robust, **easy-to-use tool with high accuracy** in detecting weak credentials and handling modern web application defenses, the **Password Auditor** on Pentest-Tools.com is a recommended choice. Its high success rates, user-friendly interface, and ability to navigate advanced security mechanisms make it a more reliable option for comprehensive web app auditing.

**Hydra** remains a powerful tool, especially for scenarios where a more manual, command-line approach is suitable, or when dealing with simpler authentication mechanisms without complex client-side protections. However, for advanced, automated credential auditing across diverse environments, the **Password Auditor** offers more value and reliability.

## Comparison results: the most accurate brute forcing tool

Curious how the detection percentages translate to the roster of web apps tested in this benchmark? **Take a look:**

# Overview of this bruteforce tools comparison

Application	The Password Auditor on Pentest-Tools.com		Hydra	
	Lab setup	Real-life setup	Lab setup	Real-life setup
WordPress	✓	✓	✓	✗
Drupal	✓	✓	✓	✓
Joomla login	✓	✓	✗	✗
Joomla administrator login	✓	✓	✗	✗
cPanel login	✓	✓	✗	✗
cPanel WHM	✓	✓	✗	✗
phpMyAdmin	✓	✓	✗	✗
Jira	✓	✓	✓	✗
Bitbucket	✓	✓	✓	✓
Confluence	✓	✓	✓	✓
Exchange	✓	✓	✗	✗
Plesk web pro	✓	✓	✗	✗
Jenkins	✓	✓	✗	✗
Grafana	✓	✗	✗	✗
Webmin	✓	✓	✗	✗
Kibana	✓	✓	✗	✗
Adobe Coldfusion	✓	✓	✗	✗
Zabbix	✓	✗	✓	✓
Weblogic	✓	✗	✓	✗
Gitlab CE	✓	✗	✗	✗
PrestaShop	✓	✓	✗	✗
JetBrains TeamCity	✓	✓	✗	✗
F5 BIG-IP	✓	✓	✗	✗
Magento	✓	✓	✗	✗
Roxy-WI	✓	✓	✗	✗
CloudPanel	✓	✓	✗	✗



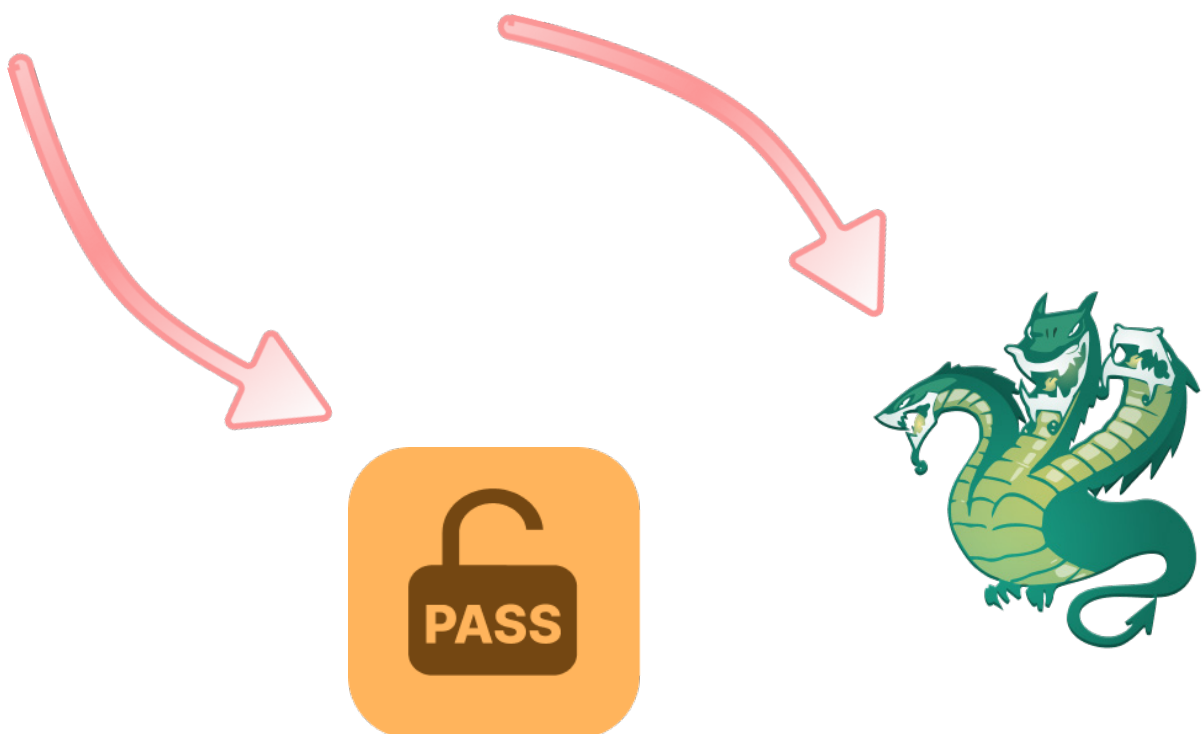
# How to bruteforce web apps with Hydra and the Password Auditor

Tinkering with security tools is fun, but it can quickly become frustrating if it takes too long.

The most demanding part of this comparison was setting up Hydra correctly. Crafting the right command is time-consuming, so we're sharing **the detailed steps for identifying parameters and configuring Hydra to test all 26 web apps**.

Alongside it you'll see how to use our **Password Auditor** - and what results it gets you.

Get the technical comparison details and **see the full configurations steps** on [pentest-tools.com/vs/hydra](https://pentest-tools.com/vs/hydra)



Europe, Romania, Bucharest  
48 Bvd. Iancu de Hunedoara

[support@pentest-tools.com](mailto:support@pentest-tools.com)  
[pentest-tools.com](https://pentest-tools.com)

Join our community of ethical hackers!

