Writeup: Secrets in Source 2 - HackerDNA Cybersecurity Lab

Introduction

In the world of web security, client-side protections often give developers a false sense of security. Labs like *Secrets in Source 2* from HackerDNA expose just how fragile these measures can be. Hosted on HackerDNA, this very easy challenge (rated for beginners) simulates a corporate website from "SecureVault Technologies"—a fictional company boasting "enterprise cybersecurity solutions" with cutting-edge features like disabled right-click menus, blocked developer tools, and even detection scripts to scare off curious users. But as any ethical hacker knows, what happens in the browser stays in the browser, and true secrets can't hide forever.

Objective: Launch the lab environment, access the target website, and uncover the hidden flag(s) by bypassing superficial client-side defenses. This lab emphasizes reconnaissance and basic web inspection skills, teaching why source code comments (and other overlooked areas) are a goldmine for attackers.

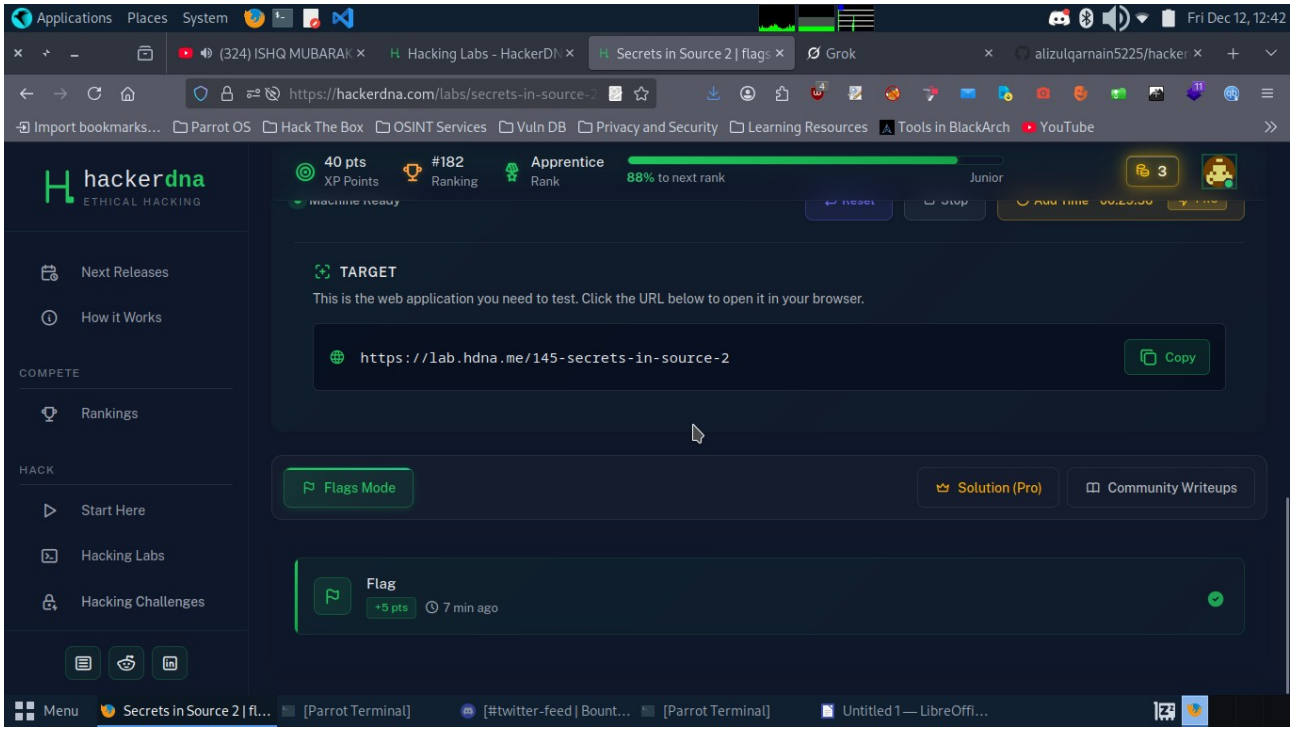
Difficulty: Very Easy
Points: 5 (1 flag worth +5 pts)
Success Rate: ~71% (as of December 2025)
Estimated Time: 5-10 minutes
Skills Tested: Web source inspection, bypassing basic UI restrictions, HTML parsing

No prior setup is needed beyond a modern browser—HackerDNA provides a private, ephemeral lab instance with an industry-standard server. It's a perfect entry point for newcomers to web pentesting, reminding us that 90% of "secure" sites leak info through sheer laziness.

Lab Setup

1. **Access the Lab**: Head to HackerDNA Labs and search for "Secrets in Source 2." If you're logged in, click "Start Lab" to spin up a dedicated VM (takes ~1-2 minutes). This gives you an isolated environment with tools like a terminal, browser, and Burp Suite pre-configured if needed.
2. **Retrieve the Target URL**: Once the machine is running, the HackerDNA dashboard will display the target application URL (something like http://<lab-ip>:port). Copy it—it's your gateway to SecureVault's "impenetrable" site. Pro tip: Bookmark the dashboard for easy flag submission later.

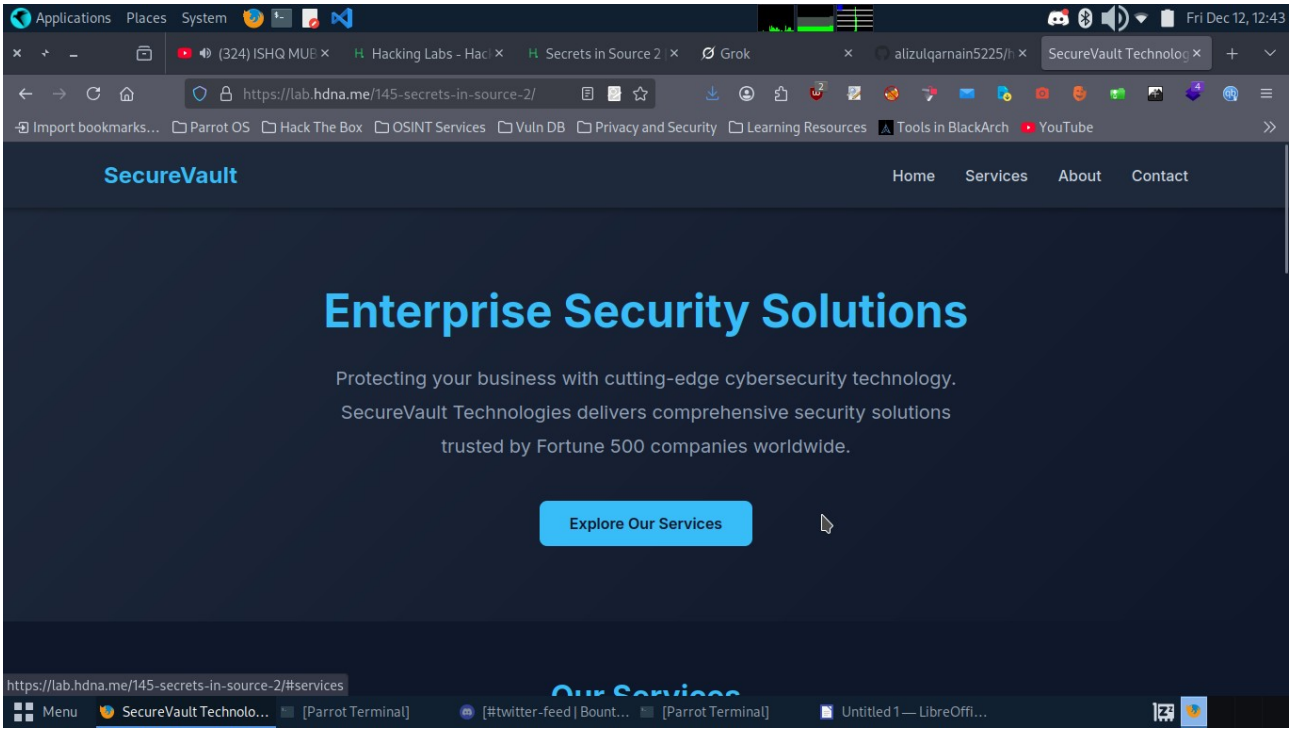
HackerDNA Lab Dashboard



Step 1: Launch the Target Website

- Paste the provided URL into your browser (e.g., Firefox or Chrome—avoid Edge if it auto-blocks dev tools).
- You'll land on the SecureVault homepage: a sleek blue-themed site proclaiming "Enterprise Security Solutions" trusted by "Fortune 500 companies worldwide." There's a big "Explore Our Services" button and navigation for Home, Services, About, and Contact. It feels legit... almost too legit.

SecureVault Homepage

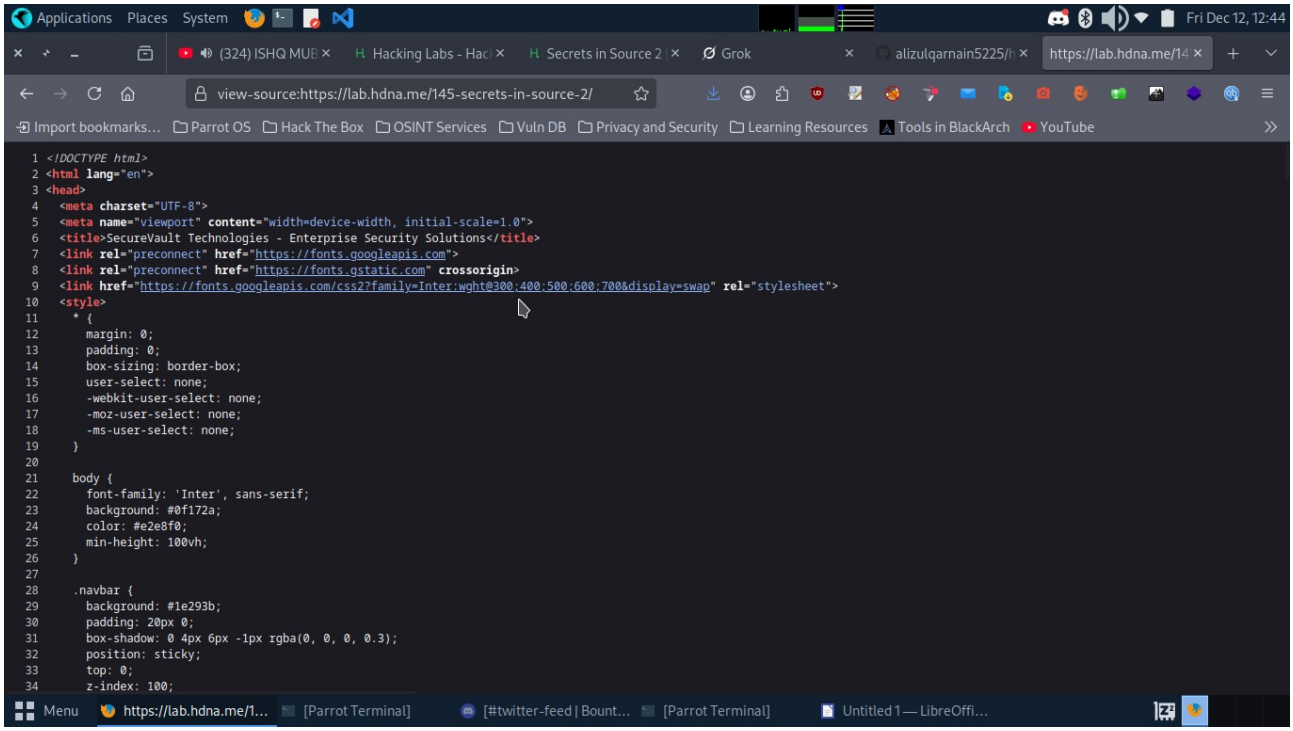


Step 2: Bypass Restrictions and Inspect the Source

- **Quick Bypass**: Hold Ctrl+U (or Cmd+U on Mac) to force-view the page source. Alternatively, if dev tools are nagging you, launch a new incognito window or use a browser extension like "Disable JavaScript" temporarily.
- The HTML source loads up, revealing the raw guts of the page. No encryption, no obfuscation—just plain, readable code.

Step 3: Hunt for the Flag

- Scroll through the <head> or <body> sections. Amid the <script> tags and CSS links, your eyes will catch something suspicious: HTML comments (<!-- -->).
- Buried in one of them? The flag itself, casually embedded as if the devs forgot to strip it out during deployment. It's a classic rookie mistake—comments are invisible to users but fully exposed to anyone who peeks under the hood.



Congratulation flag is found