Hidden Deep Into My Heart

CTF Write-Up

CTF Event:	Love at First Breach 2026 (LAFB CTF)
Platform:	TryHackMe
Challenge:	Hidden Deep Into My Heart
Category:	Web Exploitation
Difficulty:	Beginner
Points:	100
Player:	hyena11
Streak:	33 Days
Target:	10.49.172.48:5000
Date:	February 16, 2026

Overview: This write-up documents the complete solution for the "Hidden Deep Into My Heart" challenge from TryHackMe's Love at First Breach 2026 CTF event. The challenge demonstrates how sensitive information in robots.txt can lead to directory discovery and successful authentication bypass through logical credential guessing.

Flag Captured: `THM{lov3_is_in_th3_robots_txt}`

1. Reconnaissance

1.1 Initial Reconnaissance

The first step in any web application assessment is to check for standard files that might contain useful information. The robots.txt file is always a good starting point.

Command:

```
    curl -s http://10.49.172.48:5000/robots.txt
```

Output:

```
User-agent: *
Disallow: /cupids_secret_vault/*

# cupid_arrow 2026!!!
```

Key Finding: The robots.txt file revealed two critical pieces of information: a disallowed directory (/cupids_secret_vault/) and a comment that appears to be a password hint (cupid_arrow 2026!!!).

1.2 Directory Exploration

After discovering the hidden directory, I navigated to it to investigate further.

URL Visited:

```
    http://10.49.172.48:5000/cupids_secret_vault/
```

Result:

The page displayed a message: "there's more to discover" - a clear hint that additional hidden content exists within this directory.

2. Deep Enumeration

2.1 Directory Bruteforcing

Based on the hint, I used Gobuster to enumerate subdirectories within the vault directory.

Command:

```
gobuster dir -u http://10.49.172.48:5000/cupids_secret_vault/ \
            -w /usr/share/wordlists/dirb/common.txt \
            -t 50 \
            -o gobuster-vault-scan.txt
```

Result:

```
    /administrator (Status: 200)
```

Discovery: Gobuster found an administrator login page at /cupids_secret_vault/administrator

2.2 Admin Page Analysis

Accessing the administrator page revealed a standard login form with username and password fields.

3. Credential Guessing

3.1 Logical Approach

Instead of immediately resorting to brute-force tools, I applied logical reasoning based on the information gathered:

Field	Attempts	Reasoning
Username	administrator, admin, cupid	Common admin usernames
Password	cupid_arrow_2026!!!	From robots.txt comment

3.2 Login Attempts

Attempt	Username	Password	Result
1	administrator	cupid_arrow_2026!!!	Failed
2	admin	cupid_arrow_2026!!!	**SUCCESS**

Success: Using the credentials admin:cupid_arrow_2026!!! granted access to the administrator dashboard.

4. Flag Capture

Upon successful authentication, the dashboard page displayed the flag:

FLAG CAPTURED

```
THM{lov3_is_in_th3_robots_txt}
```

Challenge Completed: 100 points earned, maintaining a 33-day streak on TryHackMe.

5. Vulnerabilities Identified

ID	Vulnerability	Severity	Impact
1	Information Disclosure in robots.txt	Medium	Exposed hidden directory path and password hint
2	Weak Authentication	High	Easily guessable credentials allowed unauthorized access
3	No Rate Limiting	Low	Login form vulnerable to brute-force attacks
4	Predictable Admin Path	Low	Standard /administrator endpoint easily discovered

6. Security Recommendations

1. Remove Sensitive Information from robots.txt: Never include passwords, API keys, or sensitive hints in publicly accessible files. Use proper authentication mechanisms instead of relying on obscurity.

2. Implement Strong Authentication: Use strong, randomly generated passwords. Consider implementing multi-factor authentication for administrative accounts.

3. Add Rate Limiting: Implement rate limiting on login endpoints to prevent brute-force attacks. Lock accounts after multiple failed attempts.

4. Use Non-Standard Admin Paths: Avoid using common paths like /admin or /administrator. Implement additional authentication layers for administrative access.

5. Enable Logging and Monitoring: Log all authentication attempts and implement alerting for suspicious activities.

7. Tools and Commands

7.1 Tools Used

Tool	Version	Purpose
Gobuster	3.6	Directory and file enumeration
cURL	-	HTTP requests and testing
Web Browser	-	Manual navigation and testing

7.2 Command Reference

```
# Check robots.txt
curl -s http://10.49.172.48:5000/robots.txt

# Directory enumeration
gobuster dir -u http://10.49.172.48:5000/cupids_secret_vault/ \
            -w /usr/share/wordlists/dirb/common.txt \
            -t 50

# Test login
curl -X POST http://10.49.172.48:5000/cupids_secret_vault/administrator/login \
     -d "username=admin&password=cupid_arrow_2026!!!"
```

8. Lessons Learned

Always Check Standard Files: Files like robots.txt, sitemap.xml, and .htaccess can contain valuable information about application structure and hidden paths.

Follow the Hints: CTF challenges often provide hints through messages or comments. Pay attention to these clues as they guide you toward the solution.

Logical Thinking First: Before launching automated tools, try to understand the context and apply logical reasoning. Sometimes the simplest approach is the correct one.

Enumeration is Key: Thorough enumeration often reveals additional attack surfaces. Don't stop at the first discovery - keep exploring.

Security Through Obscurity Fails: Hiding sensitive information in comments or obscure locations does not provide real security. Proper authentication and access controls are essential.

9. Conclusion

The "Hidden Deep Into My Heart" challenge successfully demonstrated how seemingly innocuous files like robots.txt can expose critical security information. Through systematic enumeration and logical thinking, we were able to discover hidden directories, identify potential credentials, and gain unauthorized access to the administrative interface.

This challenge reinforces the importance of proper security practices: never storing sensitive information in public files, implementing strong authentication mechanisms, and applying defense-in-depth principles. For penetration testers, it highlights the value of thorough reconnaissance and the principle that sometimes the simplest approach yields the best results.

The flag `THM{lov3_is_in_th3_robots_txt}` served as a fitting reminder that valuable secrets can be hidden in plain sight, waiting to be discovered by those who know where to look.

Write-Up Author:	hyena11
Platform:	TryHackMe
Event:	Love at First Breach 2026
Date:	February 16, 2026
Points Earned:	100
Streak:	33 Days