

★ Get unlimited access to the best of Medium for less than \$1/week. [Become a member](#)



# TryHackMe — LDAP Injection — Writeup



embossdotar · Follow

Published in System Weakness

2 min read · May 29, 2024



Listen



Share



More

**Key points: LDAP | Lightweight Directory Access Protocol | LDAP Injection | Authentication Bypass | Unauthorized Data Access | Data Manipulation | Tautology-Based Injection | Wildcard Injection | Blind LDAP Injection | Boolean Exploitation | Error-Based Inference. LDAP Injection by awesome TryHackMe! 🎉**

Hi All.

First, quick introduction. Mentioned Room is *Premium* type.

It's worth considering being a premium user, more info here:

<https://tryhackme.com/why-subscribe>

**My referral link** 🎁 (“When someone uses your referral link to sign up for a premium membership within 7 days, you both earn \$5 credit towards premium access!”):

<https://tryhackme.com/signup?referrer=655bf0dd7cb6fa588c31d1a3> “It’s a win-win for you and your friends!” 🚀

(Steps: TryHackMe THM — sign up and become a premium user)

If you want to support my work, you can also take a look here:

<https://referral.hackthebox.com/mz824lP> — HTB, thanks! ✨

(Steps: Register on HackTheBox)

It would be great for you to be more familiar with these topics, so please visit the Room <https://tryhackme.com/r/room/ldapinjection> to get more details. ✨ I encourage you to do the tasks on your own.

These tasks are well-prepared, so I will try to not repeat the content. You have there what you need, but I want to share some additional helpful and useful resources.

*Tip: if you stuck with some task — please take your time, don't be in hurry. Let's be a more familiar with mentioned tools, make steps again etc.*

## Task 1 — Introduction

Get ready! 🚀

## Task 2 — Structure

No answer needed

(make sure you have read the chapter's content)

*Additional sources:*

[https://en.wikipedia.org/wiki/Lightweight\\_Directory\\_Access\\_Protocol](https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol)

<https://www.okta.com/uk/identity-101/what-is-ldap/>

<https://www.redhat.com/en/topics/security/what-is-ldap-authentication>

<https://learn.microsoft.com/en-us/previous-versions/windows/desktop/ldap/lightweight-directory-access-protocol-ldap-api>

<https://www.digitalocean.com/community/tutorials/understanding-the-ldap-protocol-data-hierarchy-and-entry-components>

## Task 3 — Search Queries

No answer needed

(make sure you have read the chapter's content)

*Additional sources:*

<https://confluence.atlassian.com/kb/how-to-write-ldap-search-filters-792496933.html>

<https://learn.microsoft.com/en-us/windows/win32/adsisearch-filter-syntax>

## Task 4 — Injection Fundamentals

No answer needed

(make sure you have read the chapter's content)

*Additional sources:*

[https://owasp.org/www-community/attacks/LDAP\\_Injection](https://owasp.org/www-community/attacks/LDAP_Injection)

[https://cheatsheetseries.owasp.org/cheatsheets/LDAP\\_Injection\\_Prevention\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/LDAP_Injection_Prevention_Cheat_Sheet.html)

## Task 5 — Exploiting LDAP

Flag

LDAP Injection Lab

# Normal LDAP Injection

Welcome, THM{!b451c\_ld4p\_inj3ct1ON!}!

LDAP Query: (&(uid=f\*)(userPassword=\*))

Username:

Password:

Login

Flag, source: THM —LDAP Injection

Q: What is the flag?

A: THM{!b451c\_ld4p\_inj3ct1ON!}

## Task 6 — Blind LDAP Injection

No answer needed

(make sure you have read the chapter's content)

## Task 7 — Automating the Exploitation



# THM{!!bl1nDLd4P1nj3ct10n!!}

You can now exploit blind LDAP injection!

Flag, source: THM — LDAP Injection

## ▶ Flag

Q: What is the flag in the dashboard?

A: THM{!!bl1nDLd4P1nj3ct10n!!}

*Additional sources:*

[https://owasp.org/www-project-web-security-testing-guide/latest/4-Web\\_Application\\_Security\\_Testing/07-Input\\_Validation\\_Testing/06-Testing\\_for\\_LDAP\\_Injection](https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/07-Input_Validation_Testing/06-Testing_for_LDAP_Injection)  
<https://capec.mitre.org/data/definitions/136.html>

I hope you enjoy! 🍀

#LDAP #LightweightDirectoryAccessProtocol #LDAPInjection  
#AuthenticationBypass #UnauthorizedDataAccess #DataManipulation #Tautology-  
BasedInjection #WildcardInjection #BlindLDAPInjection #BooleanExploitation  
#Error-BasedInference #writeup #hacking #ITsecurity #THM #TryHackMe

Best wishes,

Tryhackme

Tryhackme Walkthrough

Tryhackme Writeup

Cybersecurity

Cybersecurity Awareness

[Follow](#)

## Published in System Weakness

5.9K Followers · Last published 3 days ago

System Weakness is a publication that specialises in publishing upcoming writers in cybersecurity and ethical hacking space. Our security experts write to make the cyber universe more secure, one vulnerability at a time.

[Follow](#)

## Written by embossdotar

232 Followers · 219 Following

Security researcher. VDP enthusiast - and similar solutions like bounty <https://github.com/mbiesiad>

[Open in app](#) ↗

Medium



Search



What are your thoughts?

[Respond](#)

## More from embossdotar and System Weakness





In MeetCyber by embossdotar

## How I Found 3x XSS in 6 Seconds! Without Automated Tools

XSS discoveries using manual way—found really quick



Dec 6, 2024



133



1



In System Weakness by AbhirupKonwar

## The best way to find private Bug-Hunting programs



Recon process to find private programs



Dec 25, 2024



236



8





In System Weakness by AbhirupKonwar

## Exposed Git Directory P1 Bug

Story of P1 Bug that turned out to be ?



Dec 11, 2024



313



3



```
/language      (Status: 301) [Size: 335]
/components    (Status: 301) [Size: 337]
/api           (Status: 301) [Size: 330]
/cache         (Status: 301) [Size: 332]
/libraries     (Status: 403) [Size: 287]
/tmp           (Status: 301) [Size: 330]
/layouts       (Status: 301) [Size: 334]
```



embossdotar

## TryHackMe—Gobuster: The Basics—Writeup

Key points: Recon | Enumeration | Gobuster. Gobuster: The Basics by awesome TryHackMe! 🎉

🌟 Oct 23, 2024 🖱️ 1



- See all from embossdotar
- See all from System Weakness

Recommended from Medium



ents

	⌵	User Name	⌵	Name	⌵	Surname	⌵	Email
3		student1		Student1				studi
4		student2		Student2				studi
5		student3		Student3				studi
9		anatacker		Ana Tacker				
10		THM{Got.the.User}		X				
11		qweqwe		qweqwe				

⏪ ⏩ 1 ⏪ ⏩

embossdotar

TryHackMe—Session Management—Writeup

Key points: Session Management | Authentication | Authorisation | Session Management Lifecycle | Exploit of vulnerable session management...

🌟 Aug 7, 2024 🖱️ 27







CyferNest Sec

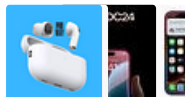
## CSRF | TryHackMe Walkthrough

CSRF: The Art of Sneaky Online Mischief

Jan 3 🖱️ 1

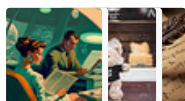


### Lists



#### Tech & Tools

22 stories · 384 saves



#### Medium's Huge List of Publications Accepting Submissions

377 stories · 4364 saves



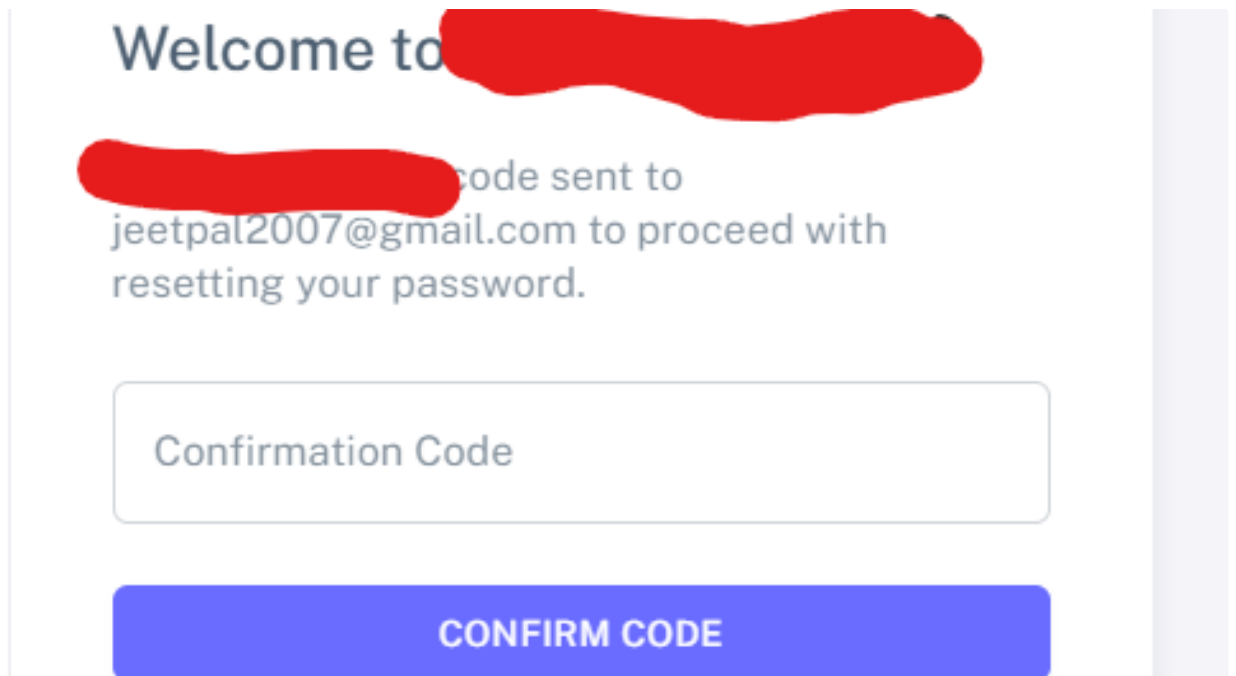
#### Staff picks

797 stories · 1564 saves



#### Natural Language Processing

1887 stories · 1535 saves



 In InfoSec Write-ups by JEETPAL

## How I Discovered an Email Disclosure Vulnerability

FREE ARTICLE

★ Jan 4 🖱 293 💬 5




**Disclosed** July 24, 2023, 9:12pm UTC

**Severity**  Medium (4 ~ 6.9)

**Weakness** Server-Side Request Forgery (SSRF)

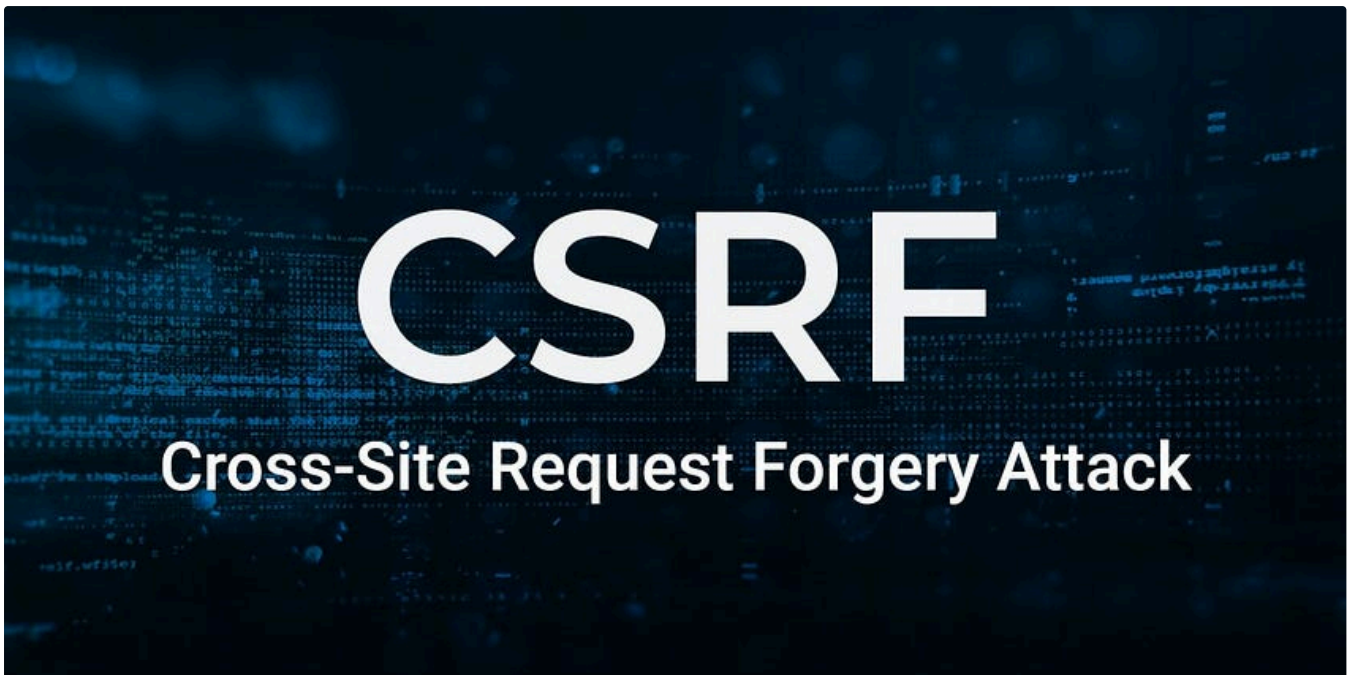
**Bounty** \$3,000

 Oday stories

### This Simple GraphQL SSRF Bug Earned \$3,000 (3/30 DAYS)

I'm a security researcher, and I've taken on the challenge of explaining one bug bounty report every day for the next 30 days—30 days...

★ Jan 1 🖱 271 💬 2



Abhijeet kumawat

## Day 30 of 30 Day — 30 Vulnerabilities | Cross-Site Request Forgery (CSRF)

Day 30: Mastering Account Takeover through CSRF Token Reuse — Essential Tricks & Techniques Based on Personal Experience and Valuable POCs

★ Sep 8, 2024 🖱 60



@SOCALLEDHACKER



\$BLIND\$  
**SSRF**

[HTTPS://NEXGUARDIANS.COM](https://nexguardians.com)

In T3CH by socalledhacker

## Server-Side Request Forgery \$(SSRF)\$ allows internal ports scanning

Read For Free- <https://nexguardians.com/blind-ssrf-allows-internal-ports-scanning/>

★ Nov 15, 2024 🖱 149



See more recommendations