LDAP injection prevention

By Vincent VAUBAN

Summary

- LDAP
- LDAP Injection
- OWASP recommendation
- Coding demo

What is LDAP?

Introduction to LDAP (Lightweight Directory Access Protocol)

- LDAP stands for Lightweight Directory Access Protocol
- used to access and manage directory information over a network.
- Think of it like a digital phone book ☎️📙—but much more versatile and scalable.

What is LDAP Used For?

LDAP is commonly used in IT environments for:

- 👌 Authentication
- 🔐 Authorization
- Centralized User Management

For example, when you log into a corporate network

How Does LDAP Work?

Imagine LDAP as a tree 🌳:

- 🌱 The roots (e.g., dc=example, dc=com).
- 🌿 Branches (like departments).
- 🍃 Leaves are entries like users, printers, or shared resources.

➡️ LDAP organizes data hierarchically, making it easy to query and retrieve specific information efficiently.

Why is LDAP Important?

- LDAP simplifies user management 💋
- LDAP provides one source of truth.

What is LDAP Injection?

LDAP Injection 💉

- Is a type of injection using user input. ⌨️

- If the input is not properly validated, attackers can access unauthorized data 😱

How Does LDAP Injection Work? 🤔

- You input a filter habitually like this cn=readers

- If the input is cn=*, you get access to all the data 😱

How to Prevent LDAP Injection?

- Sanitize User Input 🧼

- Escape special LDAP characters 🫸 like *, (,), and \.

OWASP recommendation

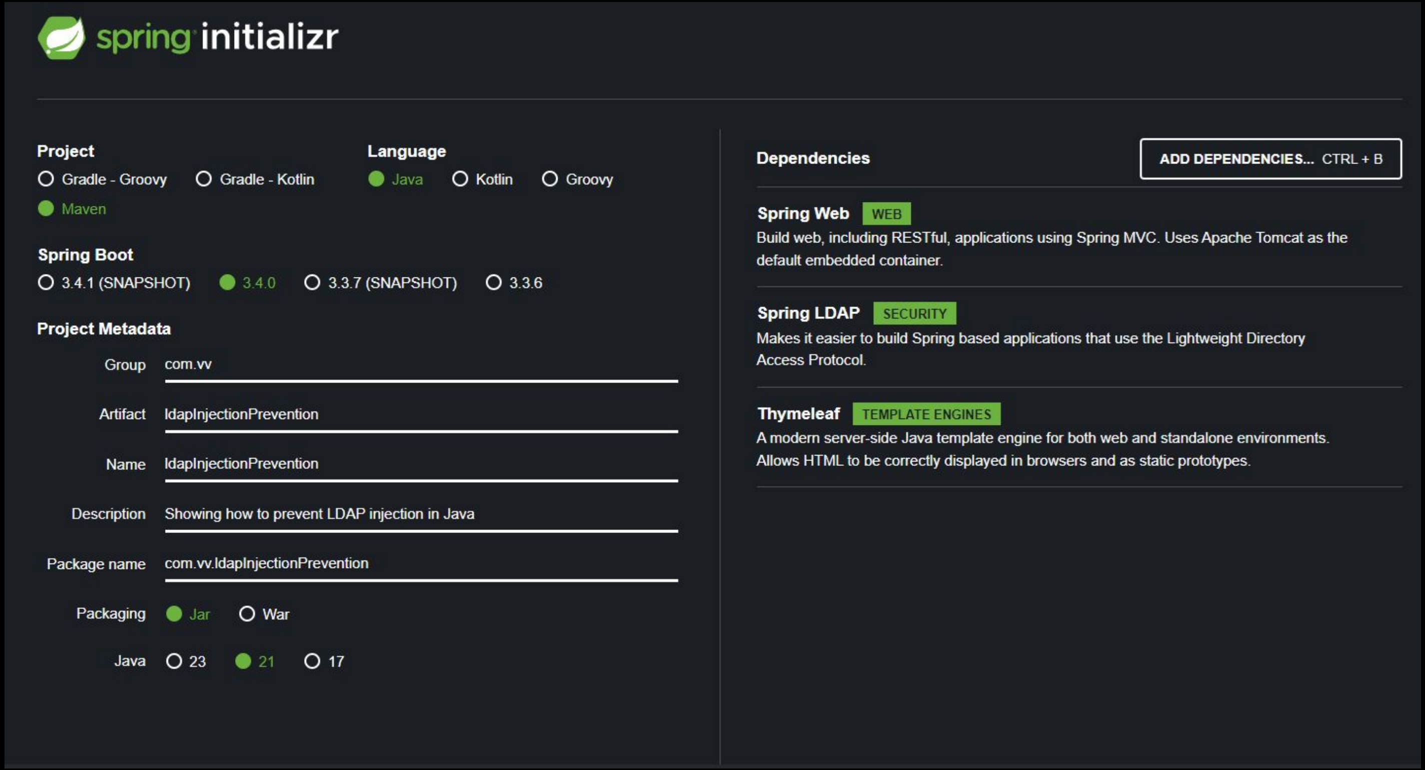
https://wiki.owasp.org/index.php/Preventing_LDAP_Injection_in_Java

- Both the distinguished name (DN) and the search filter have their own sets of meta-characters.
- Escape them

Coding Demo

https://github.com/vinny59200/java-ldap-prevention

Sprint init



Project

○ Gradle - Groovy ○ Gradle - Kotlin ● Maven

Language

● Java ○ Kotlin ○ Groovy

Spring Boot

○ 3.4.1 (SNAPSHOT) ● 3.4.0 ○ 3.3.7 (SNAPSHOT) ○ 3.3.6

Project Metadata

Group: com.vv

Artifact: ldapInjectionPrevention

Name: ldapInjectionPrevention

Description: Showing how to prevent LDAP injection in Java

Package name: com.vv.ldapInjectionPrevention

Packaging: ● Jar ○ War

Java: ○ 23 ● 21 ○ 17

Dependencies

Spring Web WEB

Build web, including RESTful, applications using Spring MVC. Uses Apache Tomcat as the default embedded container.

Spring LDAP SECURITY

Makes it easier to build Spring based applications that use the Lightweight Directory Access Protocol.

Thymeleaf TEMPLATE ENGINES

A modern server-side Java template engine for both web and standalone environments. Allows HTML to be correctly displayed in browsers and as static prototypes.

Add of escaping methods and demo of their actions.

Starting the LDAP

```
docker run --detach --rm --name openldap5 -p 1389:1389  --env
LDAP_ADMIN_USERNAME=admin --env
LDAP_ADMIN_PASSWORD=adminpassword --env
LDAP_USERS=customuser --env
LDAP_PASSWORDS=custompassword --env
LDAP_ROOT=dc=example,dc=org --env
LDAP_ADMIN_DN=cn=admin,dc=example,dc=org
bitnami/openldap:latest
```

Testing the LDAP 👨‍💻

🚣‍♂️Navigate to the database files folder to view the various database files:

```
cd /bitnami/openldap/slapd.d/cn\=config/
```

👓View the OpenLDAP database :

```
cat /bitnami/openldap/slapd.d/cn\=config/olcDatabase\=\{2\}mdb.ldif
```

🕵️Verify entries:

```
ldapsearch -x -H ldap://localhost:1389 -D "cn=admin,dc=example,dc=org"
-W -b "dc=example,dc=org" -s sub "(objectclass=*)"
adminpassword
```

Thanks for watching!