Injections

LDAP Injection

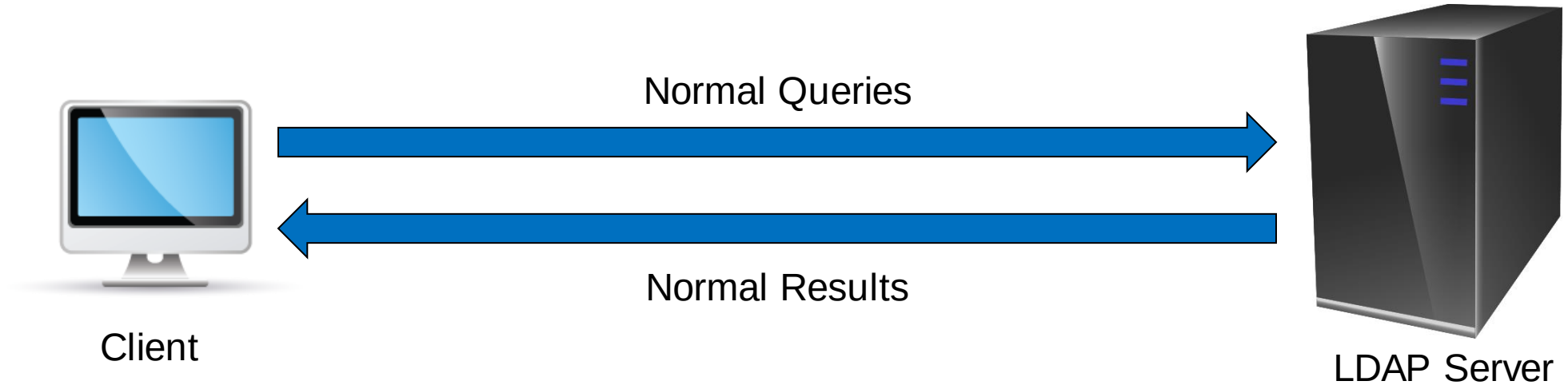
LDAP

- LDAP is Lightweight Directory Access Protocol
- It is used to access and update information in a directory which is built on the X.500 model
- It includes the operations used to establish and disconnect a session from the server.

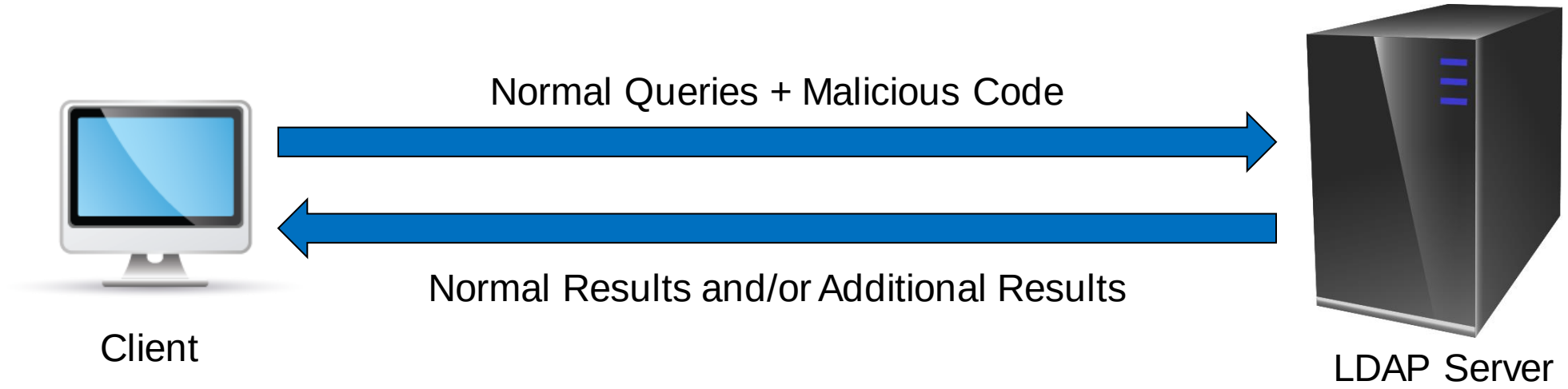
LDAP Injection

- LDAP Injection is an Injection based attack similar to SQL Injection, where in the attack is based to exploit the web application that constructs LDAP statements that are based on user input.
- The LDAP Injection generally occurs when there is a faulty input sanitization, which an attacker could use to modify the LDAP statements using local proxy, hence leading to execution of arbitrary commands.

Normal LDAP Operation:



Operation done with LDAP Injection



Example Vulnerable Code

```
<?php
ldap_search($ds, $dn,
"(&(sn=userid)(userid=".$_GET["userid"]."))");
?>
```

Request Sent by an Attacker:

```
http://www.site.com/user.php?userid=*
```

Impact

- The Impact of this attack generally depends on the vulnerable application and its functionality.
- It is possible for an attacker to gain access to sensitive information, and further modify or delete the data or could even perform privilege escalation.

Mitigations

- Proper Input Validations must be implemented at the Front-end Application.
- Using of Regular Expressions by developers would be a better option to validate untrusted input.
- Appropriate permissions on user objects should be set.
- Disabling the Anonymous access to the directory objects.
- Filtering of the data that is going out is also an important mitigation step that could be taken.
- Implementation of proper access control mechanism on data that is within the LDAP Directory.