Corndel Digital.

in association with

Softwire

Workshop: Module 10

Data & Security 2

Agenda

1000 **Welcome and Register**

1015 **Part 1: STRIDE & Risk Assessments**

- Recap (20 min)
- Exercise – Risk Assessments (70 min)
- Discussion (15 min)

1200 **Lunch Break (1 hour)**

1300 **Part 2: Federated Identity Management**

- Recap (15 mins)
- Exercise – Implementing OAuth (105 mins)

1500 **Part 3: Common Vulnerabilities**

- Recap (10 min)
- Group Exercise – Vulnerable Docker Container (50 min)

Corndel Digital.

Softwire

Part 1

STRIDE & Risk Assessments

Recap

STRIDE

STRIDE categorises various types of threat:

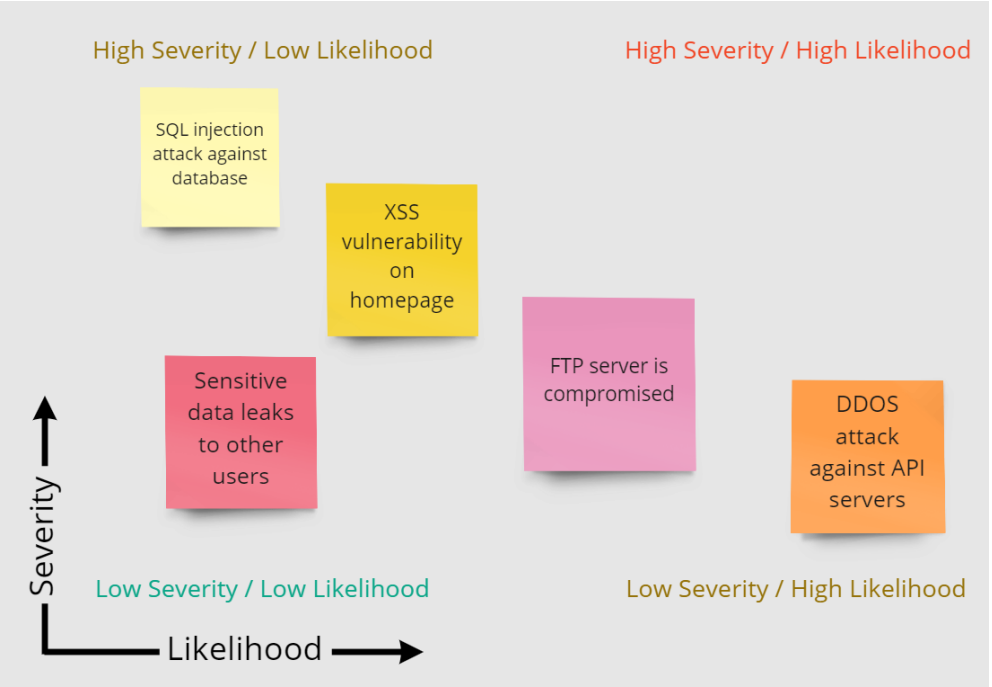
- Spoofing
- Tampering
- Repudiation
- Information Disclosure
- Denial of Service
- Elevation of Privilege

Recap

Risk Assessments

Once threats have been identified, their relative importance can be determined by by their severity & likelihood.

Risks can then be compared and prioritised (e.g. using a “Risk Storm” graph)



Exercise

Risk Assessments

Exercise

Risk Assessments

https://github.com/CorndelWithSoftwire/DevOps-Course-Workshop-Module-10-Learners/blob/main/during_workshop.md#part-1-threat-modelling

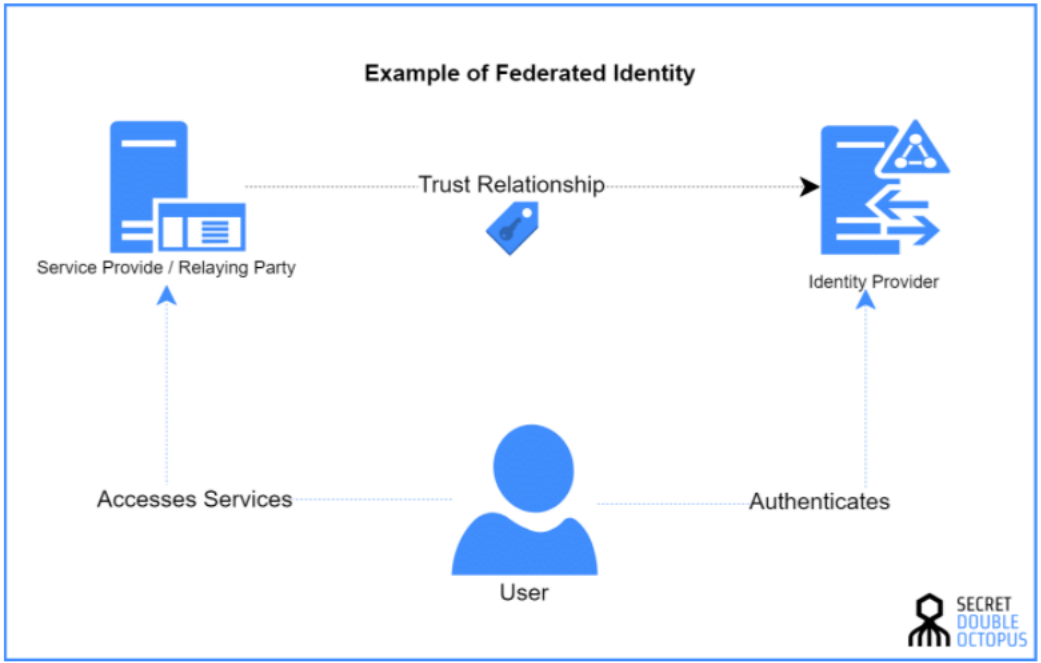
Part 2

Federated Identity Management

Recap

Federated Identity / Single Sign On (SSO)

Essentially acts as a gatekeeper or bastion to your system, requiring only one login rather than needing separate passwords for different applications within the same organisation.



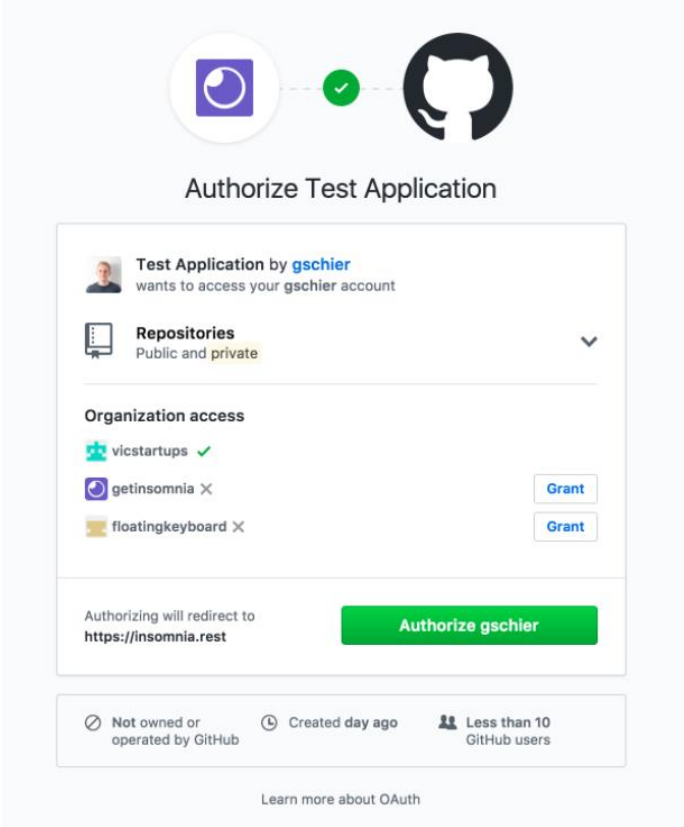
Recap

OAuth

Allows a ***provider*** to handle authentication for a system.

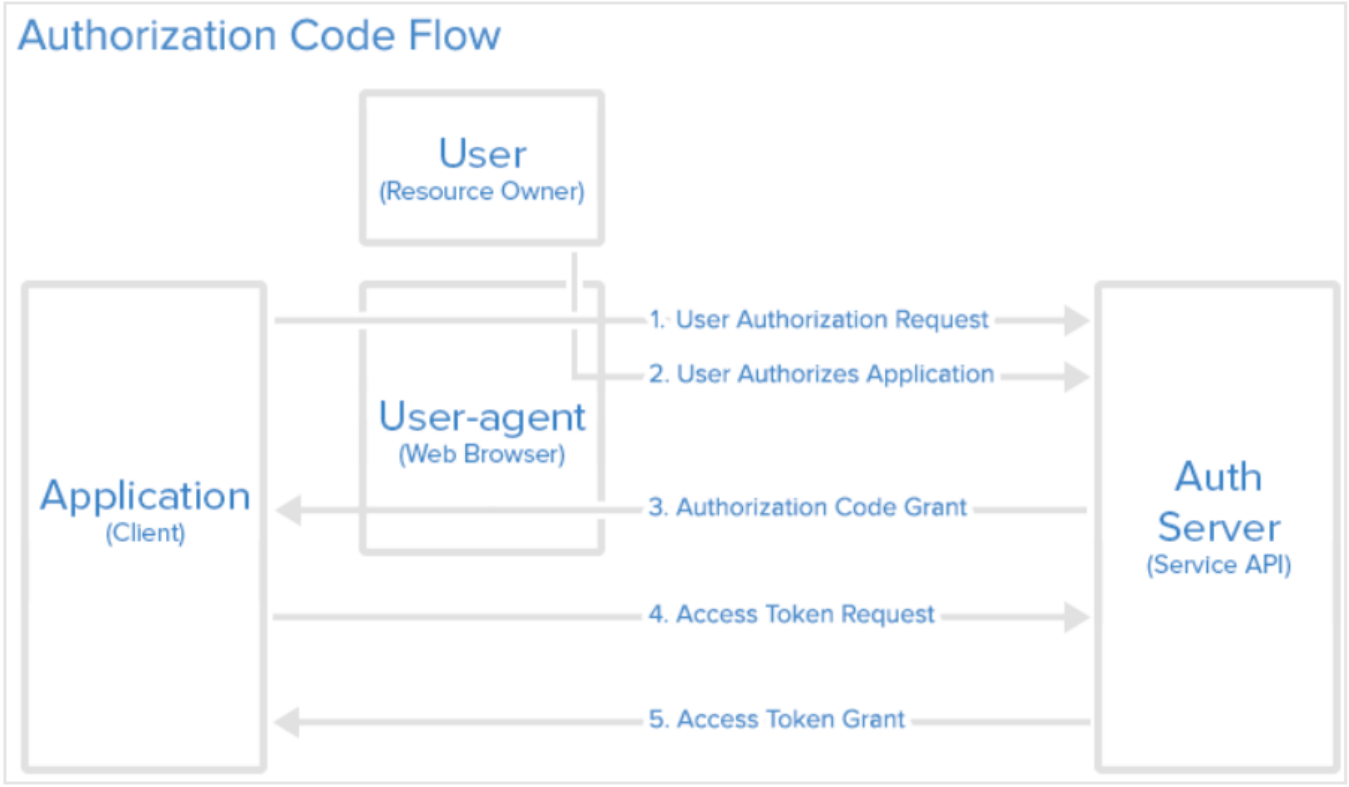
Can be convenient for users as they don't need to create a new password.

However keep in mind that users need to have a account from a supported provider to use your system!



Recap

How Does OAuth2 Actually Work?



Exercise

Auth Setup Exercise

https://github.com/CorndelWithSoftwire/DevOps-Course-Workshop-Module-10-Learners/blob/main/part_2.md

Corndel Digital.

Softwire

Part 3

Common Vulnerabilities

Recap

SQL Injection

This vulnerability typically arises when user provided data is used to generate raw SQL queries:

```
String query = "INSERT INTO Students (name) VALUES ('" + name + "')";
```

In this case the attacker can easily inject a `DROP TABLE` statement using the `name` variable:

```
INSERT INTO Students (name) VALUES ('Robert'); DROP TABLE Students; --')
```

Recap

Cross Site Scripting XSS

Cross site scripting covers a variety of attacks where external code is injected into a website and then run in a user's browser unexpectedly.

What makes these attacks particularly powerful is that it only requires a poorly designed website and cannot be protected by good architectural design

Exercises

Vulnerable Docker Box

https://github.com/CorndelWithSoftwire/DevOps-Course-Workshop-Module-10-Learners/blob/main/during_workshop.md#part-3-vulnerable-docker-box-optional

XSS Game

https://xss-game.appspot.com/?utm_source=webopsweekly&utm_medium=email

Corndel Digital.

Softwire

Thank You!