IT UNIVERSITY OF COPENHAGEN

DevOps: Software Evolution and Software Maintenance Security Assessment

Group F
Adam Hvitsted Rose (adjr@itu.dk)
Danielle Marie Dequin (ddeq@itu.dk)
Danyal Yorulmaz (dayo@itu.dk)
Jakob Henriksen (jarh@itu.dk)
Sabrina Fonseca Pereira (sabf@itu.dk)

6th Semester, Spring 2023
Data Science/Software Development BSc

BSDSESM1KU

Security Analysis

A: Risk Identification

Identify Assets

Technologies

- Go, Gin & Gorm
- PostgreSQL
- Grafana, Prometheus, Loki & Promtail
- GitHub Actions
- Docker
- Cypress
- Docker Hub
- Discord
- Vagrant

Infrastructure Our infrastructure is hosted by Digital Ocean. Droplets are VM's running on Digital Ocean's infrastructure.

- Webserver droplet
- Database server droplet
- Monitoring droplet

We started our security assessment by identifying threats against our website.

Identify Threat sources	Construct Risk scenarios
SSH into droplet	Attacker knows IP address, computer name for a droplet, and can add their own private key to gain access.
SQL injection	Attacker performs SQL injection on web application to download sensitive user data.
Hacking Digital Ocean account	Attacker using brute force or some other way to hack into our Digital Ocean account, giving them access to our whole application.
XSS Attack	XSS attack into HTML forms to inject malicious JavaScript
Connect to PostgreSQL remotely	Attacker uses PSQL to access our stuff.
Access .env file in webserver container	Hacker accesses the .env file inside the webserver docker container (which contains credentials to the database)
DDoS attack	Attacker uses a DDoS attack, causing application to shutdown.

Table 1: Identified risks and set up scenarios for each risk

Construct Risk scenarios

- Attacker knows IP address, computer name for a droplet, and can add their own private key to gain access.
- Attacker performs SQL injection on web application to download sensitive user data.
- Attacker using brute force or some other way to hack into our Digital Ocean account, giving them access to our whole application.
- XSS attack into HTML forms to inject malicious JavaScript
- Attacker uses PSQL to access our stuff.
- Hacker accesses the .env file inside the webserver docker container (which contains credentials to the database)
- Attacker uses a DDOS attack, causing application to shutdown.

B: Risk Analysis

Likelihood & Impact

Likelihood e.g., Rare, Unlikely, Possible, Likely, Almost Certain Impact. e.g., Insignificant, Minor, Moderate, Major, Severe

Name	Likelihood	Impact
SSH into droplet	Possible	Major
SQL injection	Likely	Major
Hacking Digital Ocean account	Rare	Severe
XSS Attack	Likely	Severe
Connect to PostgreSQL	Rare	Moderate
Access .env file in webserver	Possible	Severe
DDOS attack	Likely	Minor

Risk Matrix

After identifying the risks, we analysed how big of a deal it would be, if they were to happen. We visualised this with a Risk Matrix.

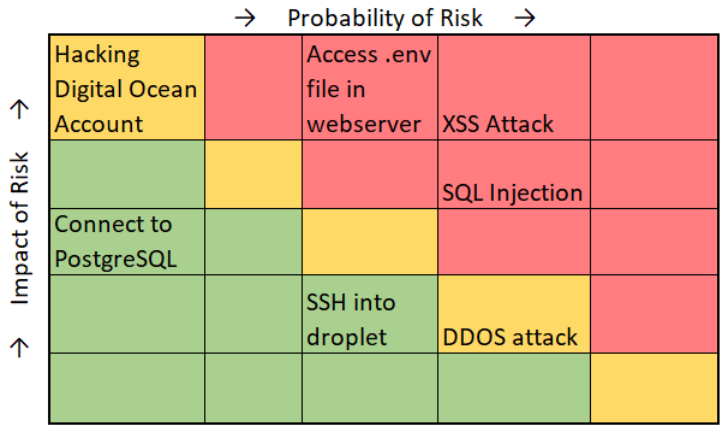

Figure 1: Risk Assessment

C: Pen-test Your System

Vulnerability scanning

We used OWASP ZAP to scan our system for vulnerabilities. The results from the scan showed us that we had several threats against our website, including SQL injections and XSS attacks as we had predicted from our analysis.

Vulnerability fixing

A vulnerability from our early analysis, that we decided to get rid of, was the access to our .env files in the web server.