AS Lab 1 – Threat Modeling

Name: Vladimir Shelkovnikov

Task 1 – Decompose the application

1. Describe entry points, assets, and trust levels in form of tables

2. Select at least 3 use cases that you think are the most interesting and prepare Data Flow Diagrams (DFD) for them.

The application can be affected from and/or within the company. Therefore, I may divide the possible attackers into external and internal. For external user entry points are the web application interface and its servers. For threats within a company, it is the code of application and infrastructure that is used to deploy the application. Considering this I made the following list of entry points:

Table 1 – Entry point

ID	Name	Description	Trust level
1	External		
1.1	HTTPS Port	The web application will be available through the 443 port	Anonymous Web User (1) User with Valid Credentials (2) User with Invalid Credentials (3)
1.2	Login Page	Interface to the login function	Anonymous Web User (1) User with Valid Credentials (2) User with Invalid Credentials (3)
1.3	Login Function	Sign in and sign up	User with Valid Credentials (2) User with Invalid Credentials (3)
1.4	Content Page	Main page for all user interaction	Anonymous Web User (1) User with Valid Credentials (2) User with Invalid Credentials (3)
1.5	Search function	Query to the server and DB	Anonymous Web User (1) User with Valid Credentials (2) User with Invalid Credentials (3)
1.6	get content function	GET query to obtain content from a server	Anonymous Web User (1) User with Valid Credentials (2) User with Invalid Credentials (3)
1.7	Account page	Show information to user, web interface to manage account	User with Valid Credentials (2) Content maker (4)
1.8	manage function	Delete, upload, and edit video. Show info, give access	Content maker (4)
1.9	Moderating function	Block content	Moderator (9)

2	Internal		
2.1	Code	Code of web application and necessary algorithms for video + Dependencies that can be considered as an external threat	Devs (11) DevOps (12)
2.2	Hardware	The hardware part of the infrastructure	Staff (10) Devs(11) DevOps (12)
2.2	Infrastructure	The processes inside the company (CI/CD, etc.)	DevOps (12)

Then for the assets, I decided to divide them into three categories: User, Application, and Infrastructure as shown in Table 2.

Table 2 – Assets

ID	Name	Description	Trust Level
1	Assets related to users		
1.1	Personal Data	App stores some personal data	DB admin (5) Web server admin (6) Web server user process (7) DB user (8) Moderator (9)
1.2	Credentials	The user credentials to log into the app.	User with Valid Credentials (2) DB admin (5) Web server user process (7) DB user (8)
2	Assets related to the application		
2.1	Session		User with Valid Credentials (2)
2.2	Availability	The app should be available for users	DB admin (5) Web server admin (6)
2.3	Content (data)	Ability to manipulate the content of the app	Content maker (4) Moderator (9)
2.4	Code	Direct access to the source code	Devs (11) DevOps (12)
3	Assets related to infrastructure		
3.1	Code execution	Ability to execute source code	Web server admin (6) Web server user process (7)
3.2	Access to DB	Ability to interact with databases information	DB admin (5) DB user (8)
3.2	Access to network	Ability to interact with infrastructure within the company	DevOps (12)
3.3	Hardware	Access to the hardware part of the infrastructure	Staff (10) Devs(11) DevOps (12)

At last, I can describe the following trust levels as shown in Table 3.

Table 3 – Trust Levels

ID	Name	Description
1	Anonymous Web User	A connected user without credentials
2	User with Valid Credentials	Connected user with valid credentials
3	User with Invalid Credentials	Connected user with invalid credentials
4	Content maker	User with publisher content
5	DB admin	User with read and write access to the databases
6	Web server admin	User with the ability to configure app servers
7	Web server user process	The process used by the app server to execute code
8	DB user	User with limited read and write permission
9	Moderator	User with the ability to block the open content
10	Staff	Persons within the company without direct access to the development
11	Developer	A person with direct access to the source code
12	DevOps	Engineers who manage the software platform

Now let's move on to the data flows. I decided to describe the following processes:
1. Uploading video;
2. Getting private video
3. Getting information about account.
I started with DFD for the uploading process as shown in Figure 1.

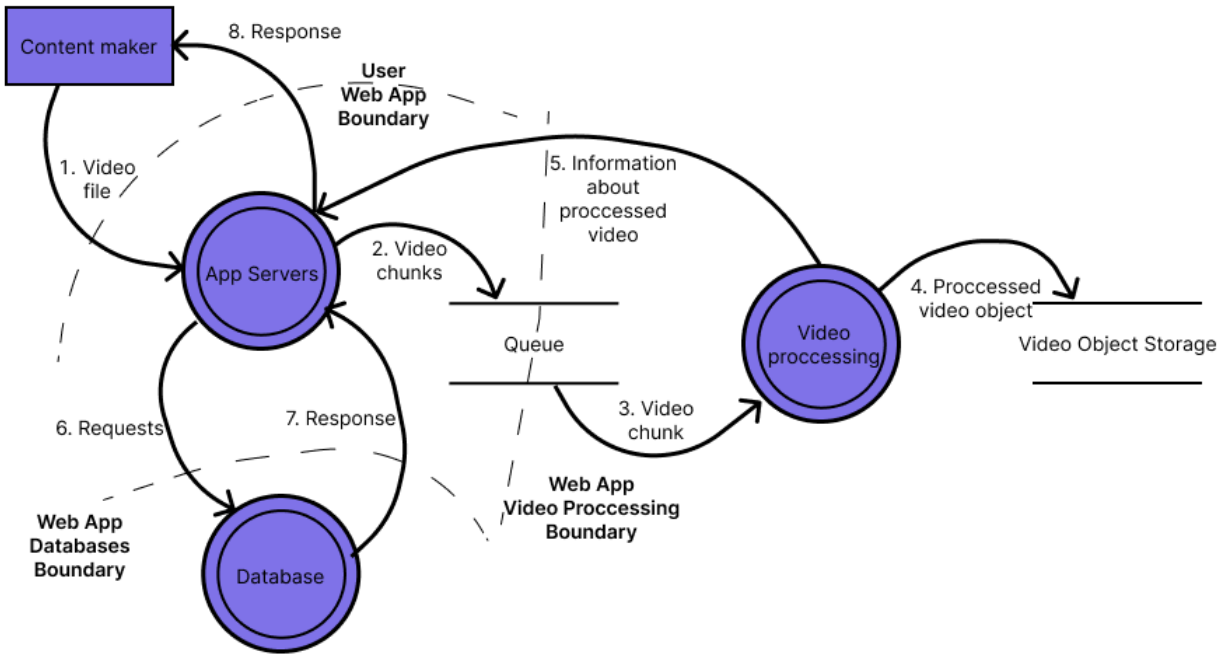

Figure 1 – Uploading video

It started with the user uploading content to the application server. The server should perform validation and sends video chunks to the video processing queue. Each chunk goes through video processing and is stored in Video Objects Storage. After that app servers received information about processed video and update the databases.

Figure 2 shows the data flow diagram for getting private video.

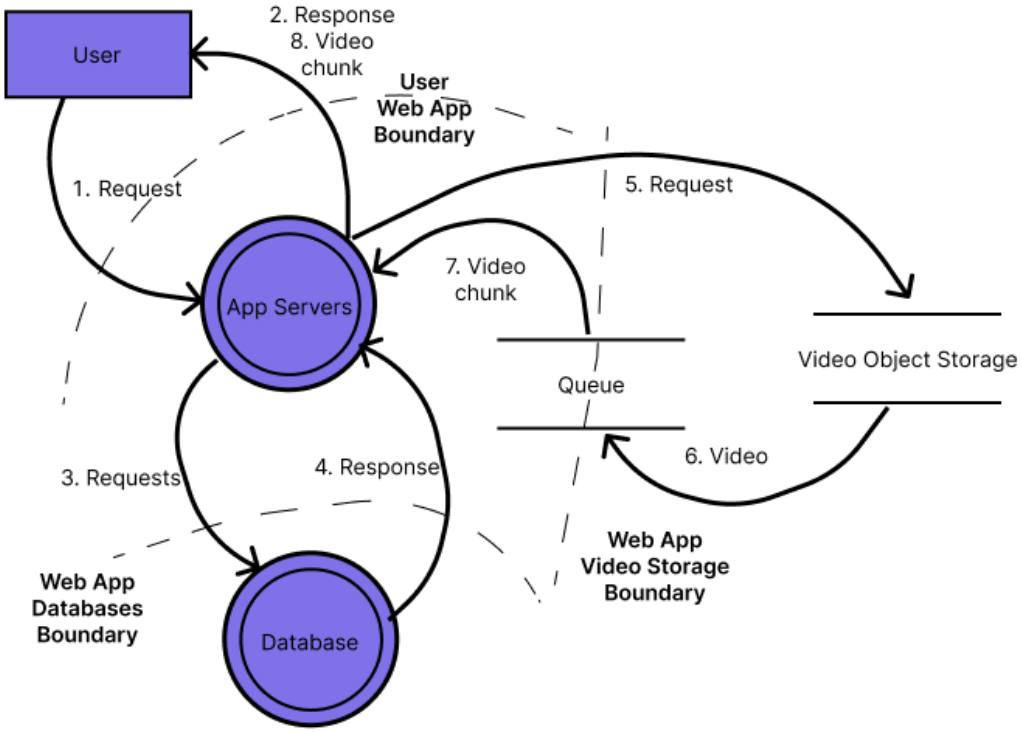

Figure 2 – Get a private video

The user makes a request for a private video. Then server should check if there is such a video and if this user has permission to access it. It may ask for user credentials, which will lead to a repeat of 1-2-3-4 requests. If everything is okay it will ask Video Objects Storage for the file. It will send chunks to the server via the queue. Figure 3 shows the third diagram.

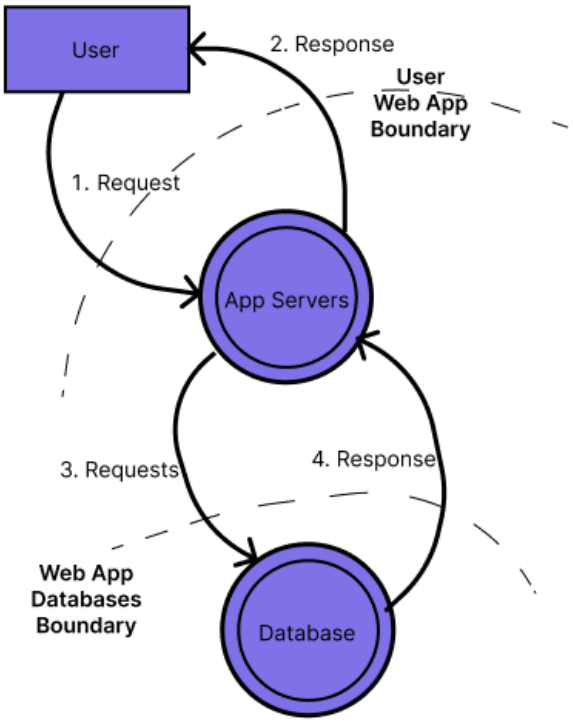

Figure 3 – Get info about the account/video

Here everything is simple. The user makes a request. The server may ask him for credentials. Then it will ask DB for information and provide it to the user or give an exception.

Task 2 – Determine threats

1. Now when you have decomposed the system you can determine possible threats. Categorizations such as STRIDE allow identifying threats in the application in a structured and repeatable manner.

Table 4 – Threats

Asset	Category	Threat	Vulnerability	Score	Countermeasure
Personal Data	Spoofing	Personal data can be obtained by the attacker	Personal information is stored openly and can be accessed	5.3	Hide confidential info about a person
Credentials	Spoofing Tampering	The credentials can be spoofed by an attacker	The insecure transition of credentials Insecure storage of credentials Insecure credentials configuration	7.2	Configure secure options and ciphers for TLS. Encryption Validation
Session	Spoofing Tampering	Session can be hijacked	absence/weakness of identity token validation Bypass authorization	8.2	Configuring the appropriate safety options for token and authorization process Sensitive cookies are encrypted and expired after logout Extra authentication with important actions
Availability	Denial of Service	An attacker can affect the work of the application	Network layer flood Domain hijacking	6.8	Applying restrictions depending on the frequency of requests
Content (data)	Information Disclosure	Attacker can get access to confidential content	Saving content in browser Misconfiguration Spoofing the private content	5.8	Sensitive info does not store Applying appropriate configuration for exceptions and errors Encryption for content with safe ciphers.
Code	Tampering Information	Code may contain known	Vulnerable dependencies	9.3	DAST, SAST, configure logging,

	Disclosure	vulnerabilities. Its dependencies can also be affected by the attacker	Exposed data in open code Disclosure of sensitive information in errors or logs '- Nonrepudiation SCA		secret scanning, backup data Integrity check Train information security developers
Code execution	Elevation of Privelege	An attacker can execute commands	Lack of regular patching could lead to remote code execution Injection	9.6	Patching the vulnerability Principle of least privileges for processes Forced validation for input Input filtering Encoding
Access to DB	Spoofing Tampering	Databases contain a lot of information that should be securely stored	Data can be modified by external user Data can be accessed by external user	9.6	Principle of least privileges for processes Validation Encryption HMAC
Access to network		Infrastructure within the company can be exposed	Exposed port Misconfiguration Exposed environment Exposed confidential information into open sources Exposed services	8.0	ACL configuration for logs Configuration of environment Secret scanning Least privilege
Hardware	DoS Information Disclosure	The hardware part of the infrastructure can be affected	Damaged by person Stealed Was modified Damaged by events (flood, earthquake, etc.)	6.8	Backup Mitigation Creation of protected premises Development of physical security procedures Distributed infrastructure