ecureApp_FileUploadPortal_ThreatMode

Owner: Zainab Qureshi and Irum Imtiaz
Reviewer:
Contributors:
Date Generated: Fri Oct 24 2025

OWASP Threat Dragon

Executive Summary

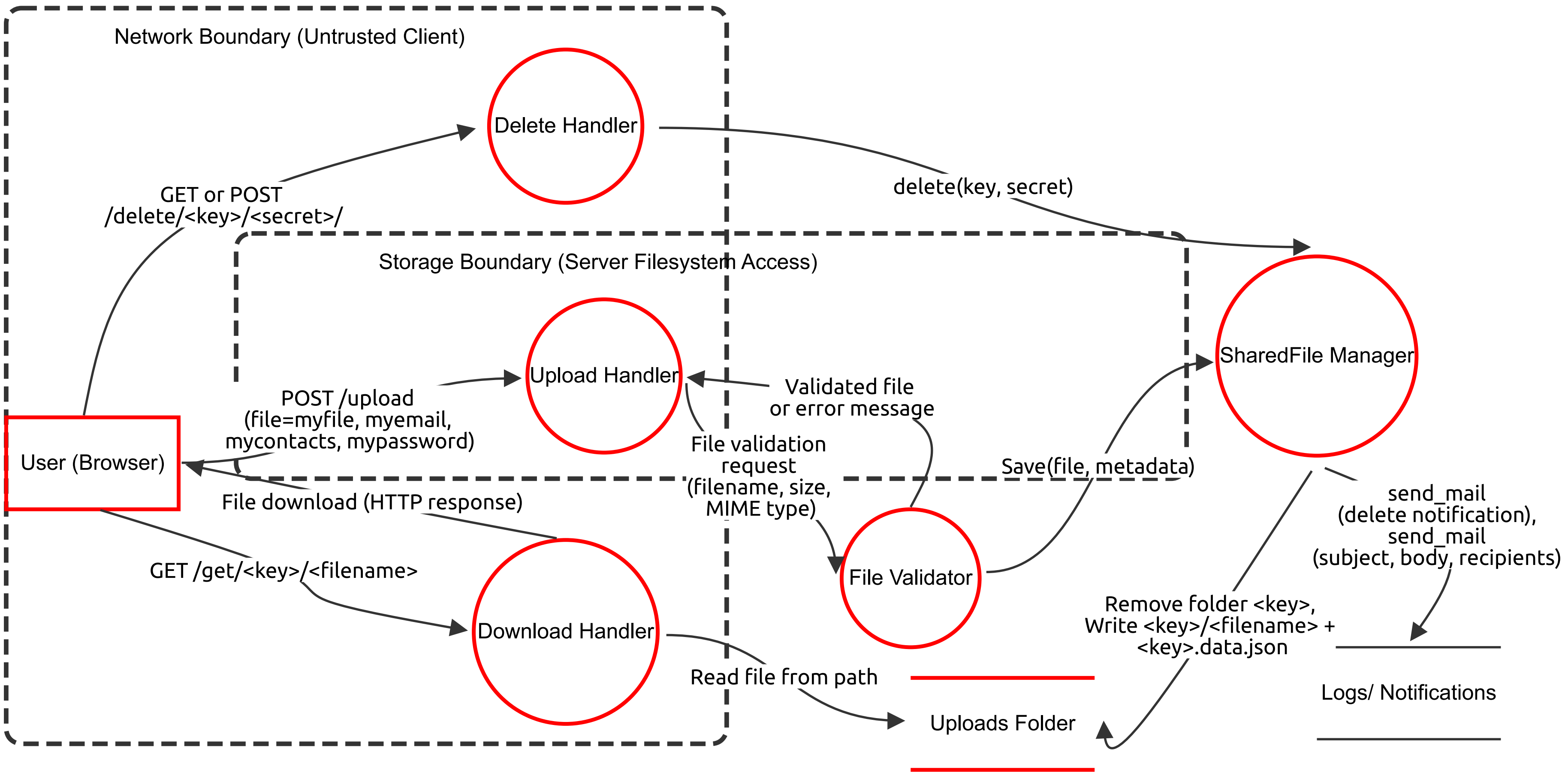
High level system description

Threat model for Flaskup-based Secure File Upload Portal

Summary

Total Threats	10
Total Mitigated	0
Total Open	10
Open / Critical Severity	0
Open / High Severity	4
Open / Medium Severity	5
Open / Low Severity	1

DFD


Network Boundary (Untrusted Client)
Delete Handler
GET or POST
/delete/<key>/<secret>/
delete(key, secret)
Storage Boundary (Server Filesystem Access)
SharedFile Manager
Upload Handler
Validated file
or error message
POST /upload
(file=myfile, myemail,
mycontacts, mypassword)
User (Browser)
File validation
request
(filename, size,
MIME type)
Save(file, metadata)
File download (HTTP response)
send_mail
(delete notification),
send_mail
(subject, body, recipients)
GET /get/<key>/<filename>
File Validator
Remove folder <key>,
Write <key>/<filename> +
<key>.data.json
Download Handler
Read file from path
Uploads Folder
Logs/ Notifications

DFD

User (Browser) (Actor)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
3	Spoofing identity via forged headers or fake email	Spoofing	Medium	Open		Provide a description for this threat	Require login or token authentication; verify sender emails before notifications

Upload Handler (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
1	Tampering - Path traversal / Filename tampering	Tampering	High	Open		Attacker submits filename with ../ to write outside intended folder or replaces files	Use werkzeug.utils.secure_filename(), enforce storage folder, no user-controlled path writes
6	File error messages leak internal paths	Information disclosure	Medium	Open			Sanitize error messages
7	Anyone can upload and share link (no auth)	Elevation of privilege	High	Open		Provide a description for this threat	Add access tokens or password-protected uploads

File Validator (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
8	Validation errors leak information	Information disclosure	Medium	Open		Provide a description for this threat	Generic error messages; logging only on server

SharedFile Manager (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
9	No audit trail for changes	Repudiation	Medium	Open		Provide a description for this threat	Maintain audit log
10	Plaintext .data.json exposes sensitive info	Information disclosure	High	Open		Provide a description for this threat	Encrypt or restrict permissions

Download Handler (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
11	Repeated download requests flood server	Denial of service	Medium	Open		Provide a description for this threat	Add rate-limiting

Delete Handler (Process)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
12	Delete confirmation leaks file presence	Information disclosure	Low	Open		Provide a description for this threat	Respond generically regardless of validity

Uploads Folder (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations
13	Manual modification of uploaded files	Tampering	High	Open		Provide a description for this threat	Use checksums; limit write permissions

Logs/ Notifications (Store)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

POST /upload (file=myfile, myemail, mycontacts, mypassword) (Data Flow)

Description: The user submits the upload form via HTTP POST, including the file and optional email fields.

Number	Title	Type	Severity	Status	Score	Description	Mitigations

File validation request (filename, size, MIME type) (Data Flow)

Description: Upload handler sends the uploaded file object to the validation process for checking.

Number	Title	Type	Severity	Status	Score	Description	Mitigations

GET /get/<key>/<filename> (Data Flow)

Description: Browser requests file download using the unique key.

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Read file from path (Data Flow)

Number	Title	Type	Severity	Status	Score	Description	Mitigations

GET or POST /delete/<key>/<secret>/ (Data Flow)

Description: User requests deletion using the secret key.

Number	Title	Type	Severity	Status	Score	Description	Mitigations

delete(key, secret) (Data Flow)

Description: Validates secret key and calls delete method.

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Remove folder <key>, Write <key>/<filename> + <key>.data.json (Data Flow)

Description: Writes both the actual file and metadata JSON file to disk.
Physically deletes folder and contents.

Number	Title	Type	Severity	Status	Score	Description	Mitigations

send_mail (delete notification), send_mail (subject, body, recipients) (Data Flow)

Description: Sends optional notification emails using Flask-Mail.
Sends admin or uploader notification on delete.

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Save(file, metadata) (Data Flow)

Description: Passes validated file and metadata for saving and assigning unique keys.

Number	Title	Type	Severity	Status	Score	Description	Mitigations

Validated file or error message (Data Flow)

Description: Returns confirmation or error after filename/size validation using secure_filename().

Number	Title	Type	Severity	Status	Score	Description	Mitigations

File download (HTTP response) (Data Flow)

Description: Sends the requested file via Flask send_file().

Number	Title	Type	Severity	Status	Score	Description	Mitigations