Challenge 1: Web App with Image-Upload

Build a web application that allows users to upload and delete pictures. You can use any public resources. The following tasks are required:

- The web application must have a function to upload and delete images.
- A GitHub project must be created for this web application, and the code must be shared.
- A whitelisting function must be implemented that allows access to the web application only from our VPN IP address:
  `20.218.226.24`

At the end, you must provide a valid URL where we can access the application and test uploading and deleting our pictures. **If there are any issues or problems with setting up the web application, please send us your application directly and we will test it locally.**

Challenge 2: Vulnerability Reporting

Your task is to analyze the provided HTTP request and response pair, which was captured during a pentest assessment of a web application. The application's purpose is to serve files like documents and images to authenticated users.

Your goal is to identify the primary security vulnerability present in this exchange and document it. While you should focus on the most critical issue, we value thoroughness and attention to detail.

The Data

Please use the following request-response pair for your analysis.

Request

```
GET /api/v1/file-viewer?filename=../../../../../etc/passwd HTTP/1.1
Host: insecure-corp-app.com
Connection: close
Accept: */*
X-Requested-With: XMLHttpRequest
Sec-CH-UA: "Google Chrome";v="125", "Chromium";v="125",
"Not.A/Brand";v="24"
Sec-CH-UA-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
    (KHTML, like Gecko) Chrome/125.0.0.0 Safari/537.36
Sec-CH-UA-Platform: "Windows"
Origin: https://qwcrzdkikcji.com
Sec-Fetch-Site: cross-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Cache-Control: no-cache
Pragma: no-cache
```

Response

```
HTTP/1.1 200 OK
Date: Mon, 23 Jun 2025 17:19:59 GMT
Server: Apache/2.4.49 (Ubuntu)
Access-Control-Allow-Origin: https://qwcrzdkikcji.com
Access-Control-Allow-Credentials: true
Vary: Origin
Cache-Control: no-store, no-cache, must-revalidate, private
Expires: 0
X-Request-ID: 7a4e6df9-a8d8-4f8a-9a0f-9e6b3c2d1b8c
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Security-Policy: default-src 'self'; object-src 'none';
Content-Type: text/plain; charset=UTF-8
Content-Length: 586
Connection: close

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
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
webadmin:x:1001:1001:Web Administrator:/home/webadmin:/bin/bash
svc_account:x:1002:1002:Service Account:/home/svc_account:/bin/sh
```

Deliverable

Please document your finding using our standard Pentest Report Finding Template provided below. Your report should be clear, concise, and professional, with actionable remediation advice.

Please submit your completed report as a single PDF document in English. We look forward to reviewing your analysis!

Good luck!

Pentest Report Finding Template

The template is explained below, which contains every detailed description of the weaknesses of this report.

This legend explains the header below.

Vulnerability title	The specific name or designation of the identified vulnerability. It is used to clearly name the vulnerability and to reference it in reports.
CVSS Risikoscore	The CVSS (Common Vulnerability Scoring System) Score Version 4 assesses the risk of a vulnerability on a scale of 0 to 10. A higher score indicates greater risk (Info to Critical). The CVSS string provides a detailed description of the individual factors that led to the calculation of the score and includes a link to the detailed calculation. See also chapter 4.2.
Inspection status	The inspection status indicates whether and to what extent a follow-up inspection by the client is necessary. We will notify you if a verification/inspection is required as a follow up action to our finding. This field either can hold the information: Verified by PCG, Verification required, Partially verified by PCG.
Solution effort	This indicates the estimated effort required to remedy the vulnerability. This is stated as low, medium or high and is an assessment without guarantee by the executing penetration testing team. This value must be verified with the client's development team, as it may differ due to the environmental characteristics.
Affected Objects	This lists the objects (systems, applications, networks, IPs, UIDs, buildings, artifacts, etc.) that are affected by the vulnerability. This helps to understand and narrow down the scope and potential impact of the vulnerability.
References	Additional information or sources provide details about the vulnerability, its impact, and possible mitigations. References point to external resources that the Penetration Testing Team has assessed as valid. Clients should check all information, as it can change constantly.

Vulnerability Template to use:

Insufficient Session Handling CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N	7,4
Inspection status	**Verified**
Solution effort	**Medium**
Affected Objects	• **IP/Application** (https://TBD.com)
References	https://TBD.com

General description

To be filled by you!

Detailed Description

To be filled by you!

Recommendations

To be filled by you!

- To be filled by you!
- To be filled by you!