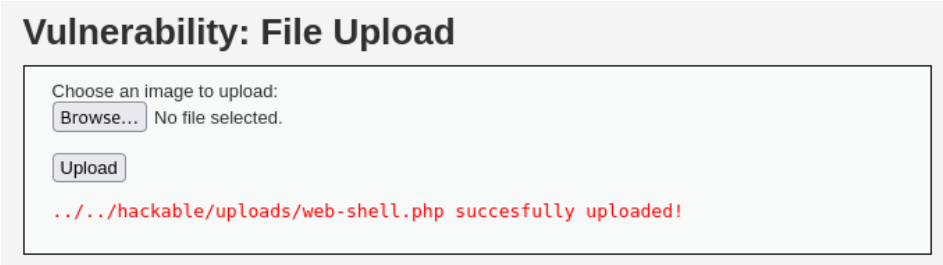
**FILE UPLOAD VULNERABILITY**

*(informazioni importanti evidenziati in rosso)*

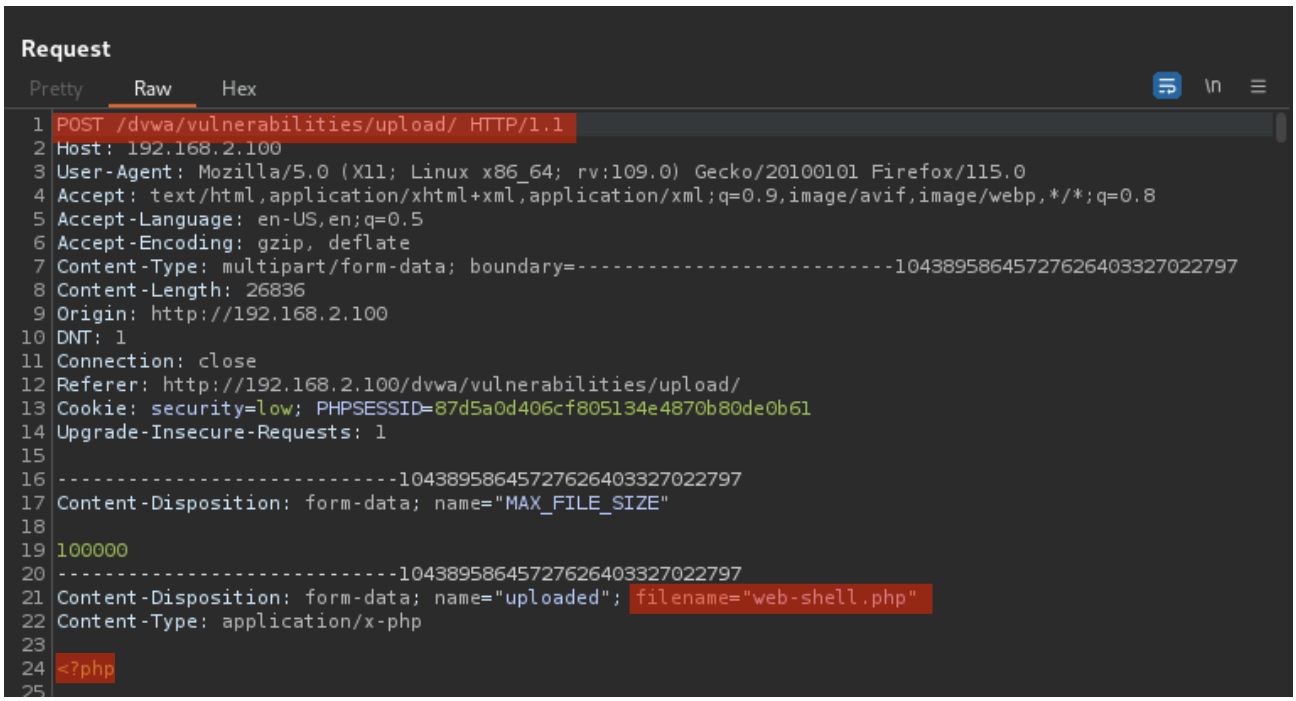
*(shell utilizzata - https://github.com/JohnTroony/php-webshells/blob/master/Collection/web-shell.php)*

### 1. Caricamento della shell

*Browser*



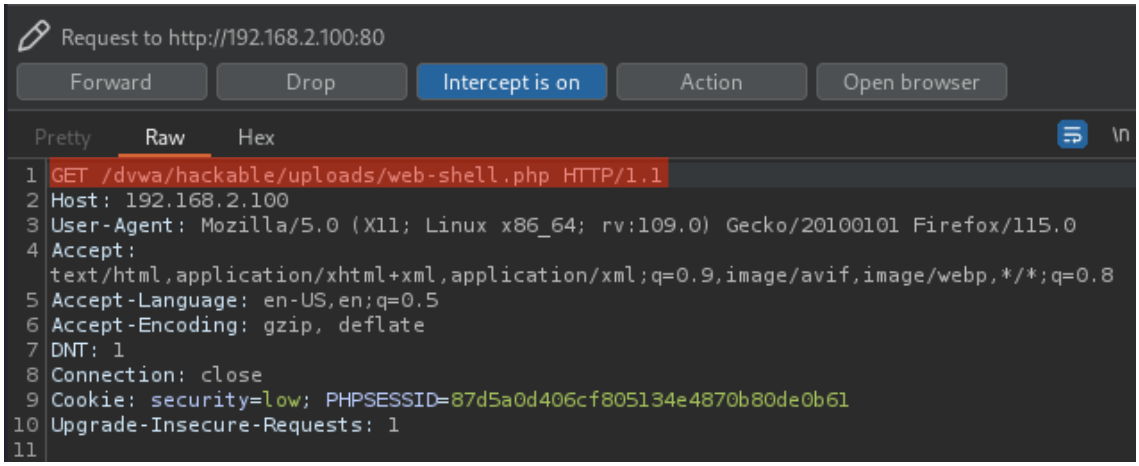

*Burpsuite*



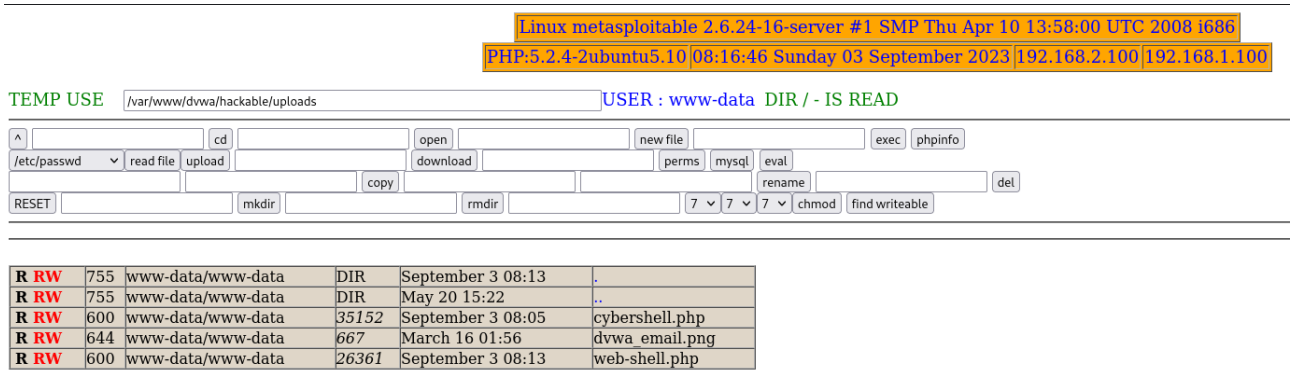
**2. Accesso alla shell appena caricata**

*Browser (URL per l'accesso)*


*Burpsuite*




*Browser - Interfaccia web della shell caricata*

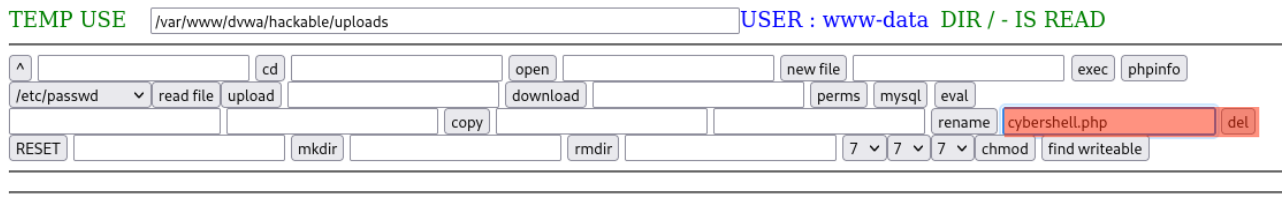



| | | | | | |
|---|---|---|---|---|---|
| R RW | 755 | www-data/www-data | DIR | September 3 08:13 | . |
| R RW | 755 | www-data/www-data | DIR | May 20 15:22 | .. |
| R RW | 600 | www-data/www-data | *35152* | September 3 08:05 | cybershell.php |
| R RW | 644 | www-data/www-data | *667* | March 16 01:56 | dvwa_email.png |
| R RW | 600 | www-data/www-data | *26361* | September 3 08:13 | web-shell.php |

### 3. Invio comandi tramite shell

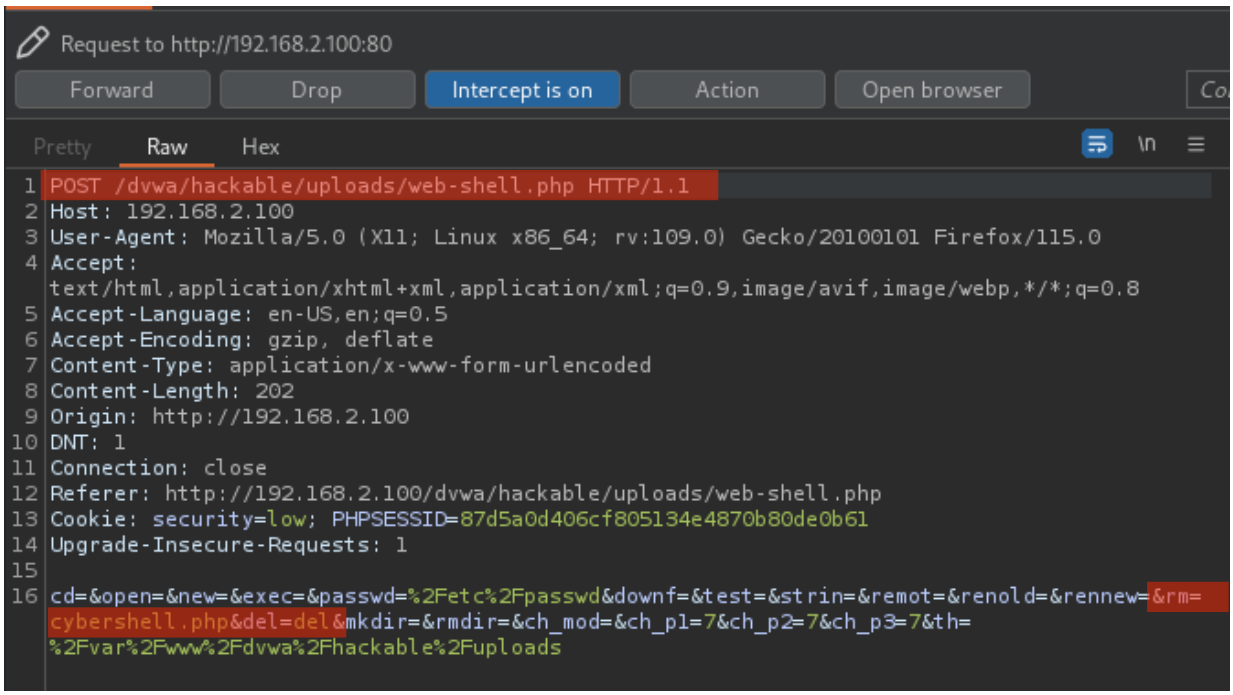
Eliminazione di un file – cybershell.php

*Browser*

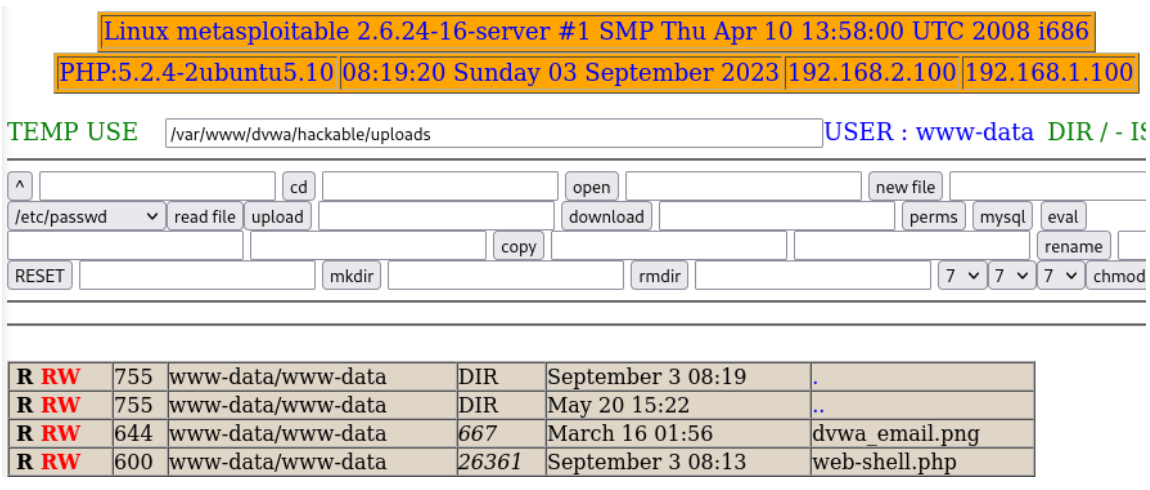



| | | | | | |
|---|---|---|---|---|---|
| R RW | 755 | www-data/www-data | DIR | September 3 08:13 | . |
| R RW | 755 | www-data/www-data | DIR | May 20 15:22 | .. |
| R RW | 600 | www-data/www-data | *35152* | September 3 08:05 | cybershell.php |
| R RW | 644 | www-data/www-data | *667* | March 16 01:56 | dvwa_email.png |
| R RW | 600 | www-data/www-data | *26361* | September 3 08:13 | web-shell.php |

*Burpsuite*



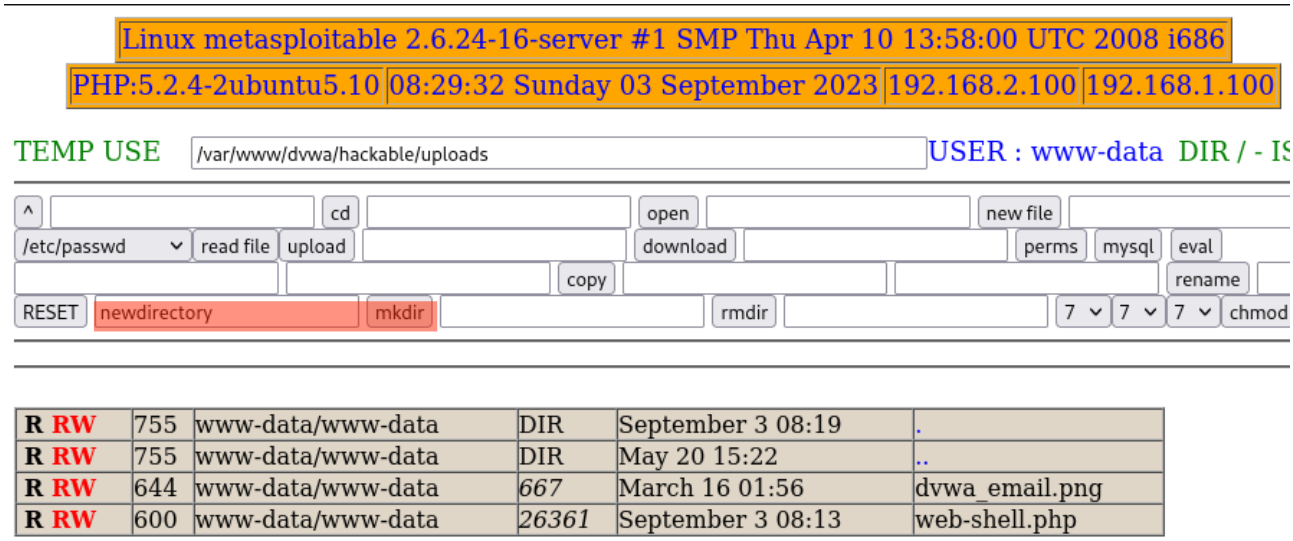

*Browser – file eliminato*




| | | | | | |
|---|---|---|---|---|---|
| R RW | 755 | www-data/www-data | DIR | September 3 08:19 | . |
| R RW | 755 | www-data/www-data | DIR | May 20 15:22 | .. |
| R RW | 644 | www-data/www-data | *667* | March 16 01:56 | dvwa_email.png |
| R RW | 600 | www-data/www-data | *26361* | September 3 08:13 | web-shell.php |

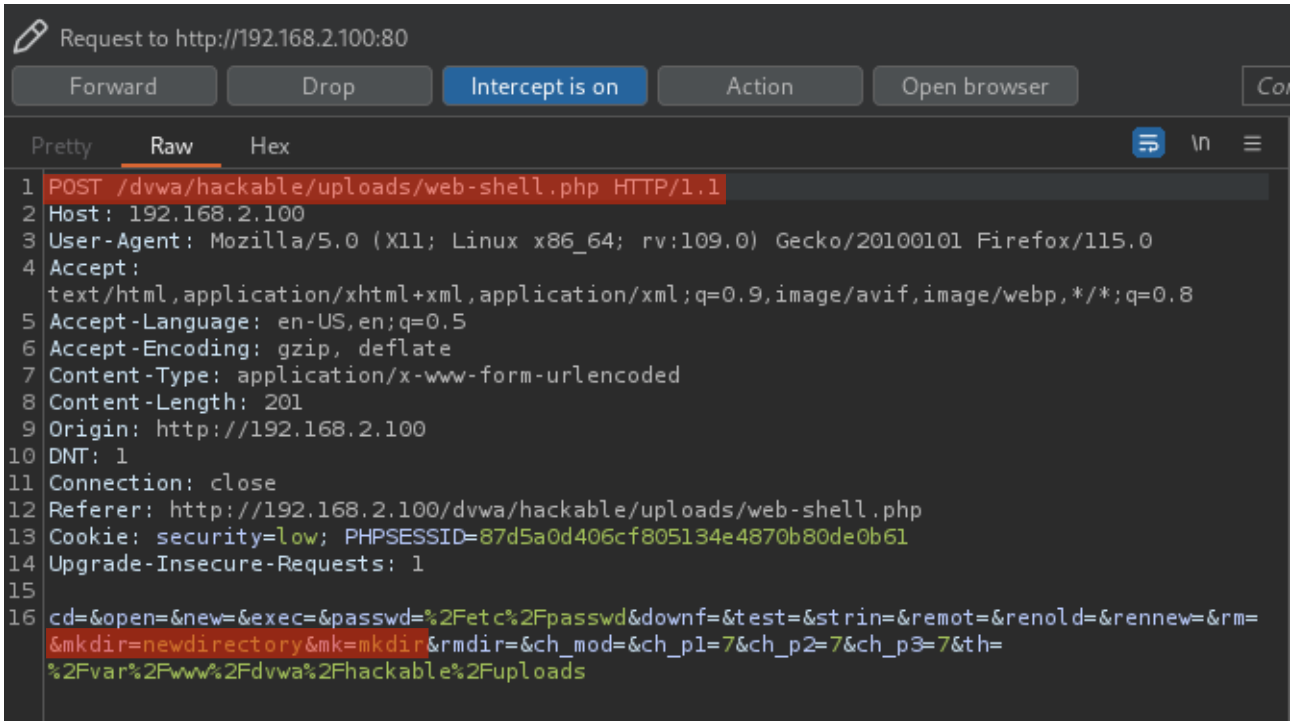
Creazione nuova directory

*Browser*

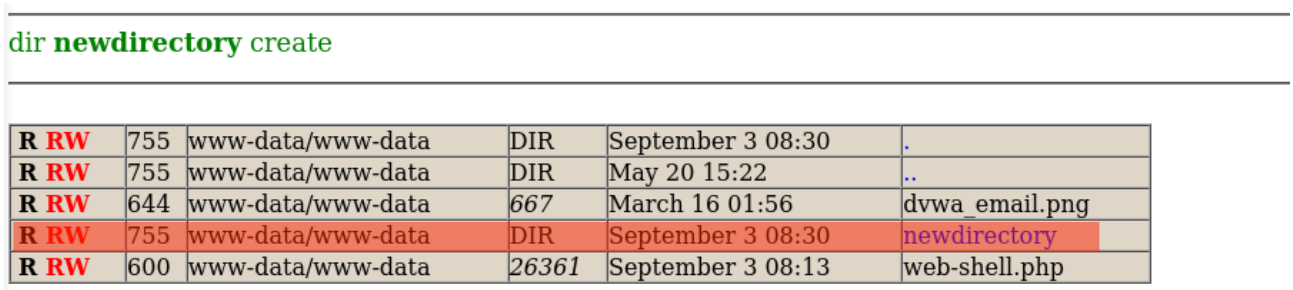



| | | | | | |
|---|---|---|---|---|---|
| R RW | 755 | www-data/www-data | DIR | September 3 08:19 | . |
| R RW | 755 | www-data/www-data | DIR | May 20 15:22 | .. |
| R RW | 644 | www-data/www-data | *667* | March 16 01:56 | dvwa_email.png |
| R RW | 600 | www-data/www-data | *26361* | September 3 08:13 | web-shell.php |

*Burpsuite*



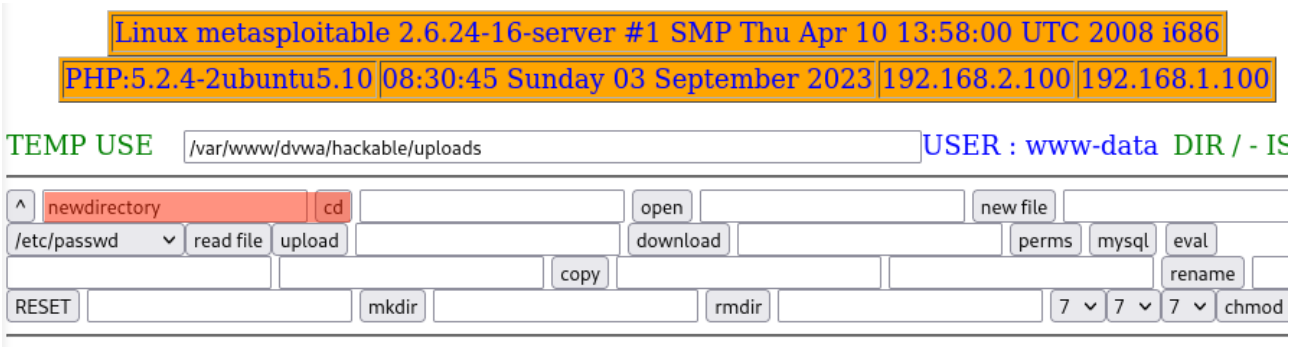

*Browser – directory creata*



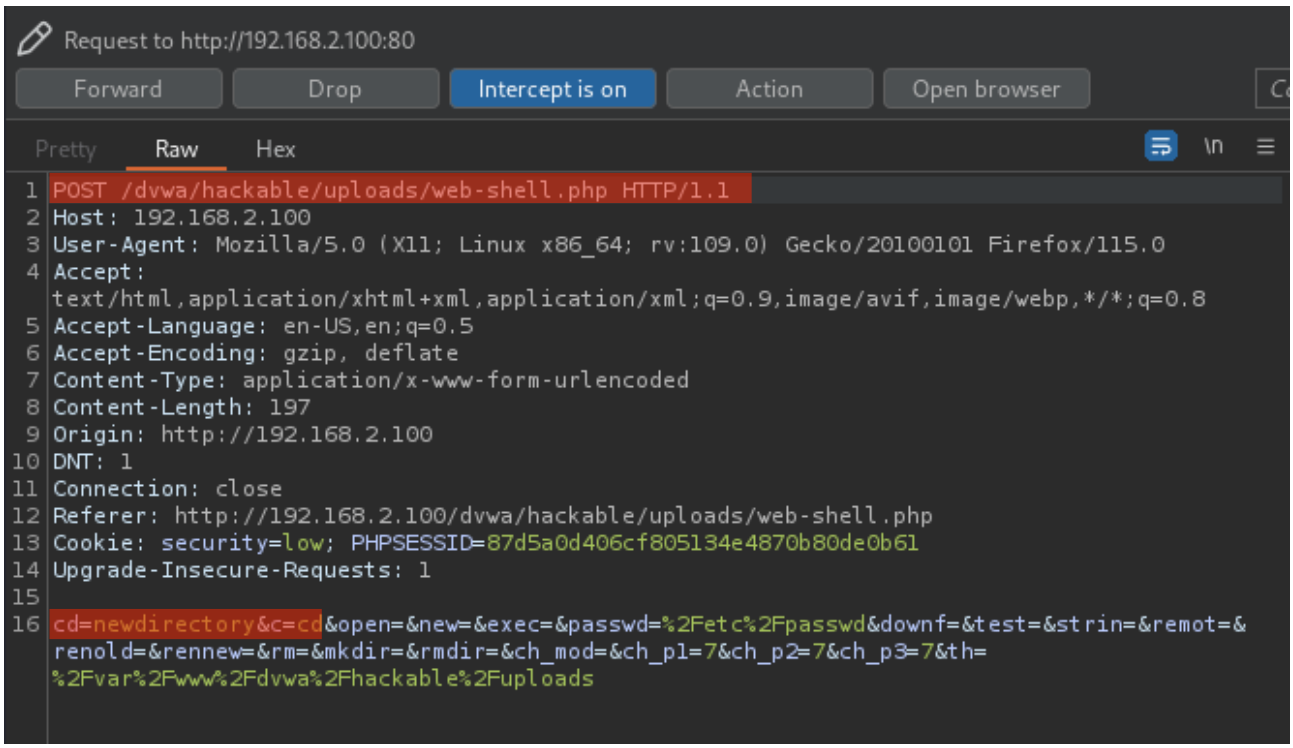

| | | | | | |
|---|---|---|---|---|---|
| R RW | 755 | www-data/www-data | DIR | September 3 08:30 | . |
| R RW | 755 | www-data/www-data | DIR | May 20 15:22 | .. |
| R RW | 644 | www-data/www-data | *667* | March 16 01:56 | dvwa_email.png |
| R RW | 755 | www-data/www-data | DIR | September 3 08:30 | newdirectory |
| R RW | 600 | www-data/www-data | *26361* | September 3 08:13 | web-shell.php |

*Accesso alla nuova directory*

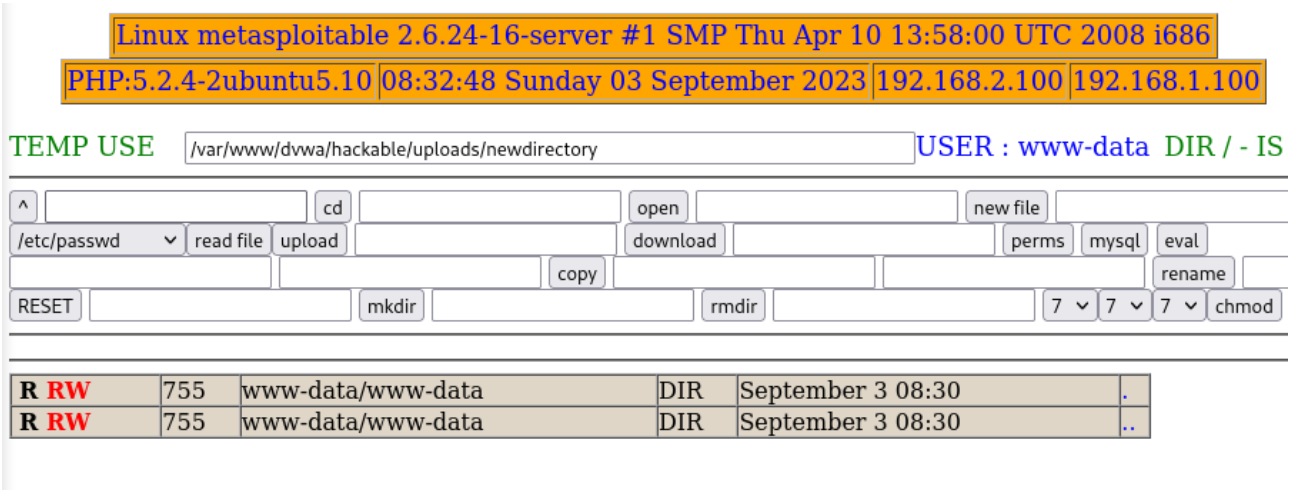
*Browser*



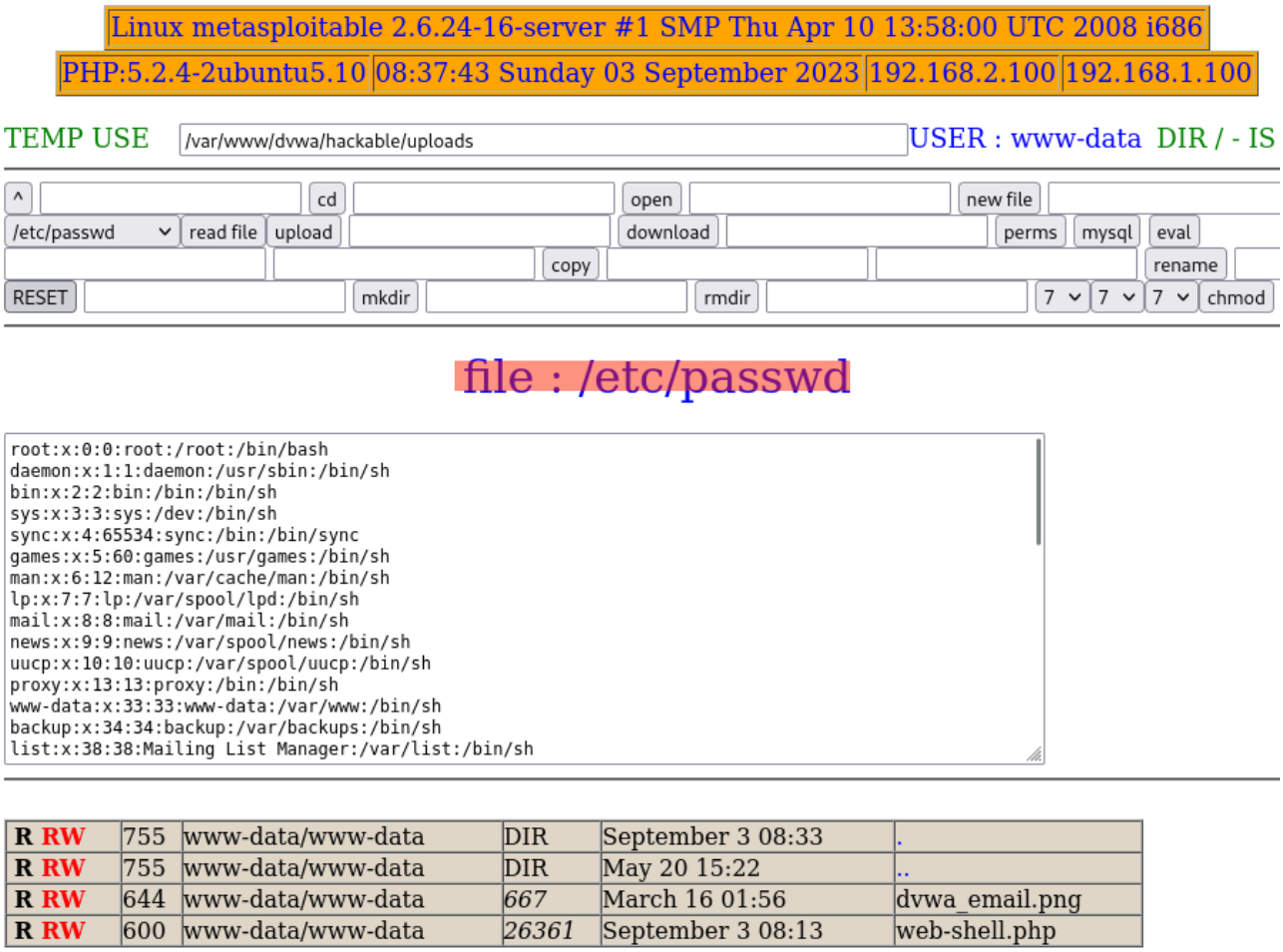

*Burpsuite*




*Browser*



Accesso remoto al file “passwd” della macchina server




| | | | | | |
|---|---|---|---|---|---|
| R RW | 755 | www-data/www-data | DIR | September 3 08:33 | . |
| R RW | 755 | www-data/www-data | DIR | May 20 15:22 | .. |
| R RW | 644 | www-data/www-data | *667* | March 16 01:56 | dvwa_email.png |
| R RW | 600 | www-data/www-data | *26361* | September 3 08:13 | web-shell.php |