

EXPLOIT

Un exploit è un software, o un insieme di istruzioni o una tecnica che sfrutta una vulnerabilità di una macchina o sistema per ottenere un accesso non autorizzato, così da poter compiere un'azione dannosa o manipolare il comportamento del sistema stesso.

Le vulnerabilità che gli exploit sfruttano possono essere errori nel software, debolezze nella configurazione di sicurezza o altri punti di debolezza nel sistema. Quando un exploit sfrutta con successo una vulnerabilità, può causare danni di vario genere, come l'accesso non autorizzato a dati sensibili, l'esecuzione di codice malevolo, la modifica di impostazioni di sistema o l'instaurazione di controllo completo sul sistema compromesso.

Per esempio qui abbiamo attaccato la macchina di meta per accedere alla cartella twiki.

```
meterpreter > ls
Listing: /var/www/twiki

Mode                Size                Type                Last modified        Name
-----
100644/rw-r--r--    1947668884941669   fil                142111537762-12-15  00:20:58 -0500   TWikiDocumentation.html
100644/rw-r--r--    225129300806849   fil                142111537899-01-21  06:49:15 -0500   TWikiHistory.html
040755/rwxr-xr-x    17592186048512    dir                142111319319-02-03  05:46:13 -0500   bin
040755/rwxr-xr-x    17592186048512    dir                181965164209-11-21  22:58:31 -0500   data
100644/rw-r--r--    3358664426254     fil                141781607365-02-06  06:09:35 -0500   index.html
040755/rwxr-xr-x    17592186048512    dir                173047578792-01-14  08:59:53 -0500   lib
100644/rw-r--r--    83494164253680    fil                142110804172-08-28  16:33:48 -0400   license.txt
040755/rwxr-xr-x    17592186048512    dir                141226543141-06-15  11:09:14 -0400   pub
100644/rw-r--r--    18614388265198    fil                142111537899-01-21  06:49:15 -0500   readme.txt
040755/rwxr-xr-x    17592186048512    dir                141491181008-10-17  17:00:33 -0400   templates

meterpreter >
[*] 192.168.1.149 - Meterpreter session 1 closed. Reason: Died
```