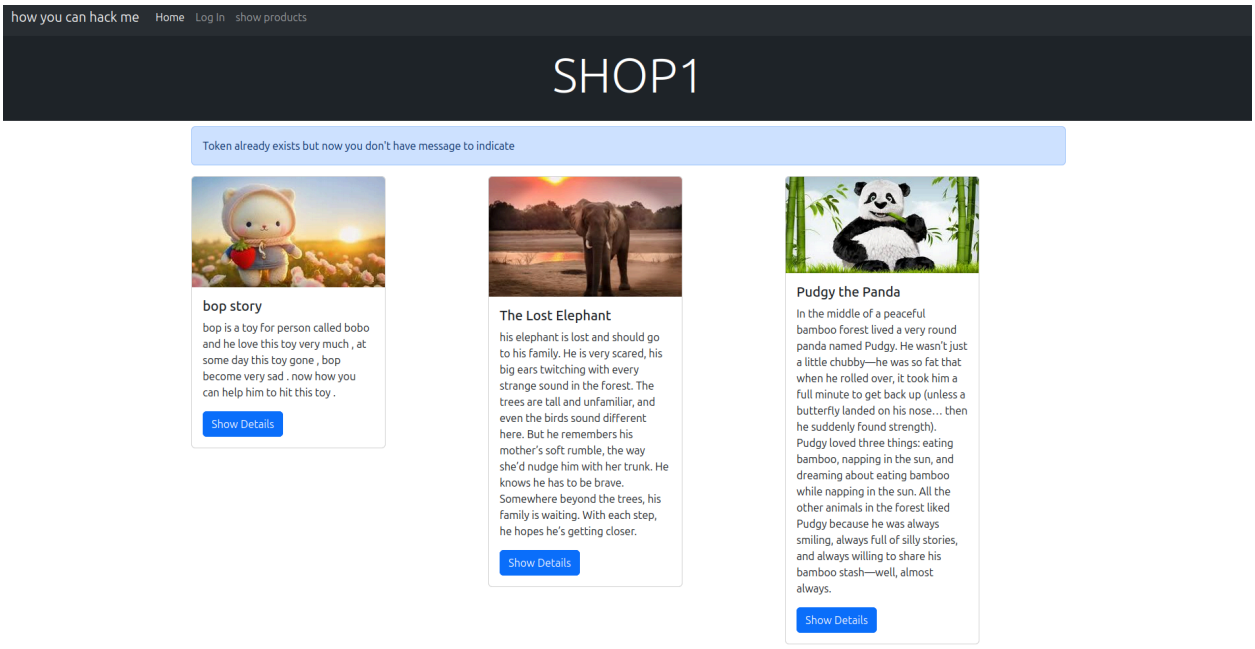
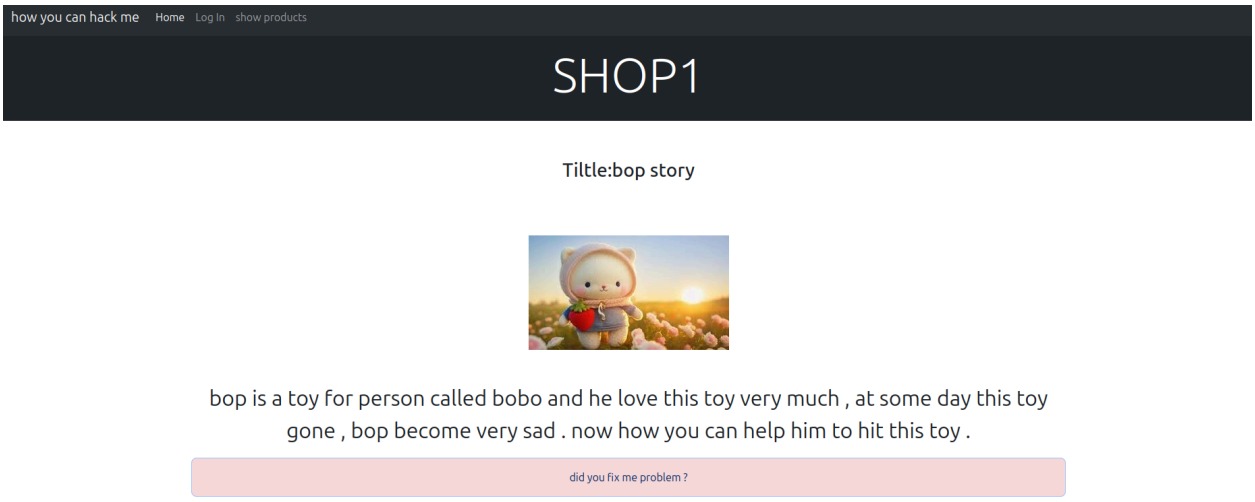
SQL_LEVEL8

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

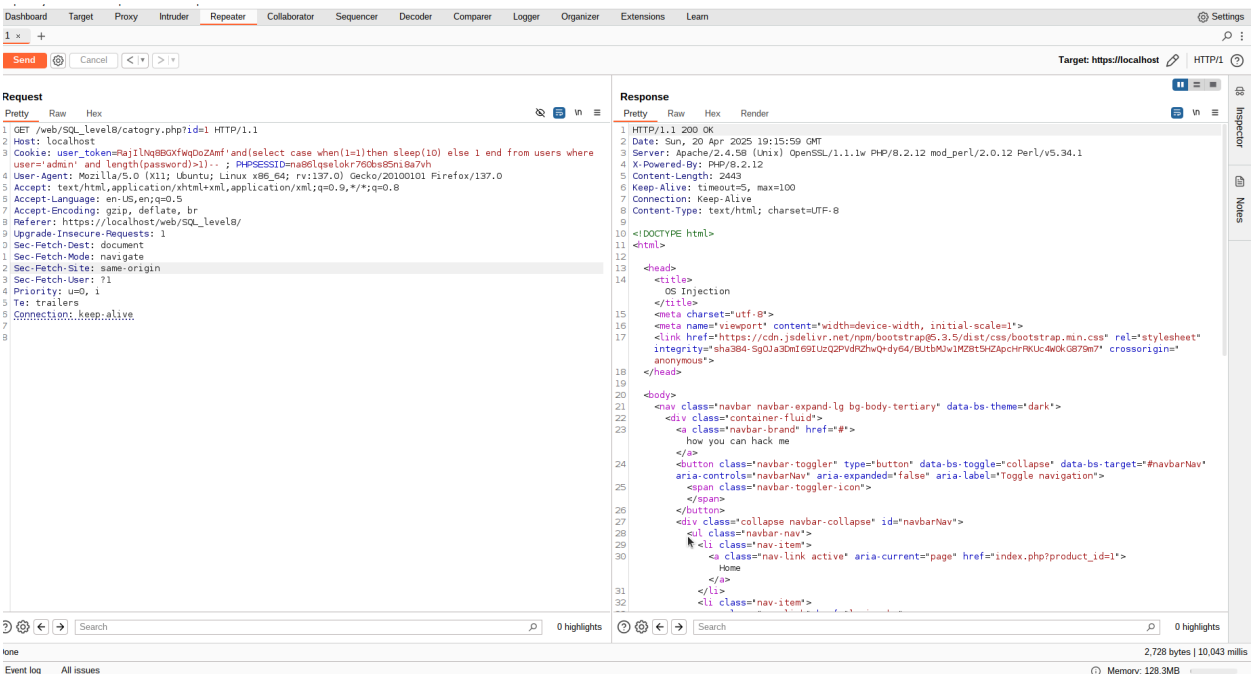
- the solution in sleeping

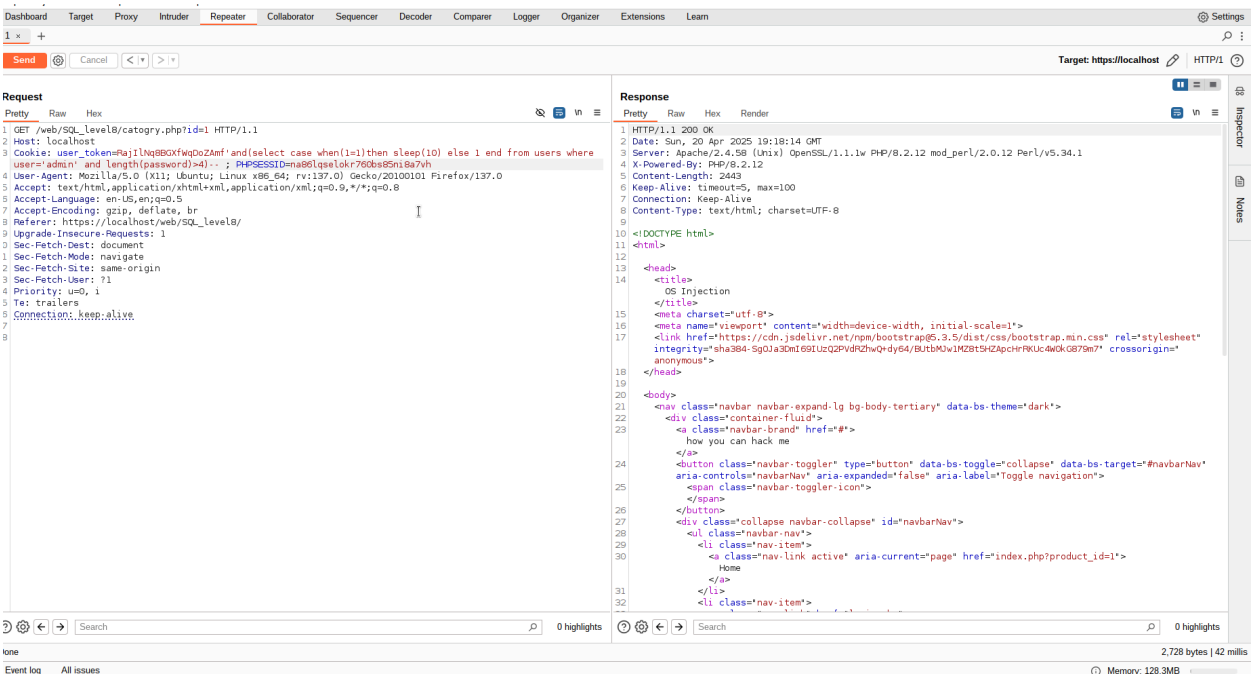


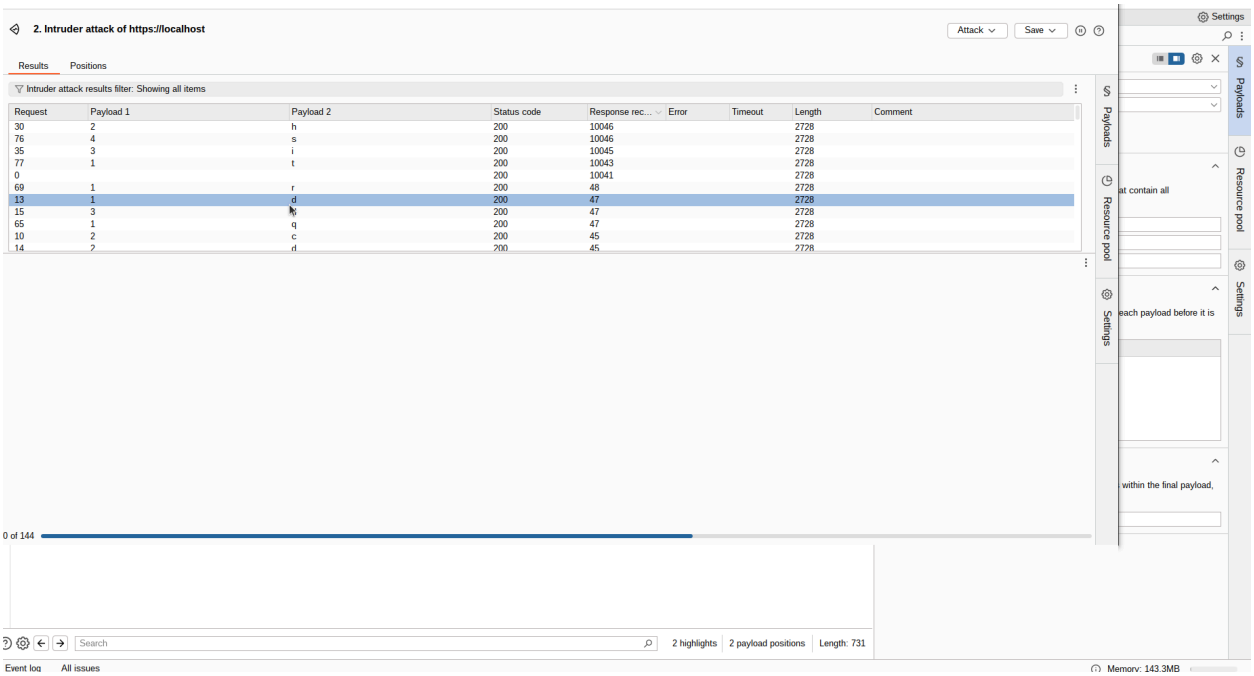
- no message is appear now or disappear what we will do



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



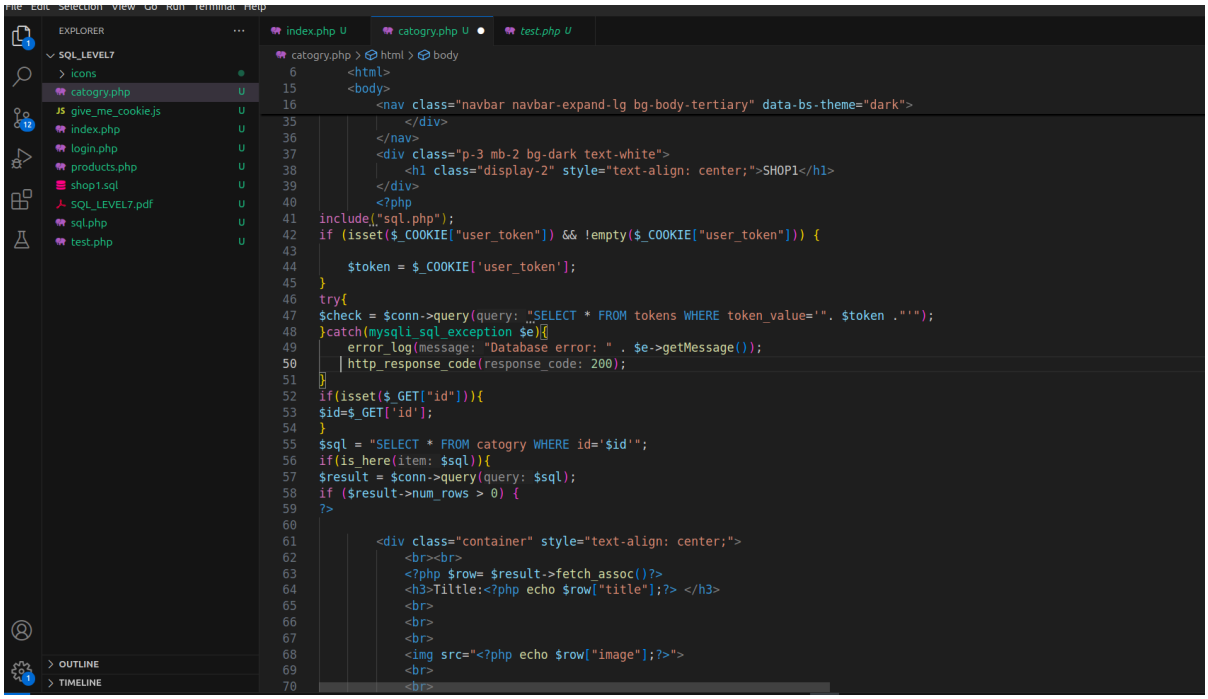




- the password is ‘this’

▼ use sample payload using Burp Suite

- let’s show that are not have any indicate


File Edit Selection View Go Run Terminal Help
EXPLORER
SQL_LEVEL7
icons
catogry.php U
give_me_cookie.js U
index.php U
login.php U
products.php U
shop1.sql U
SQL_LEVEL7.pdf U
sql.php U
test.php U
OUTLINE
TIMELINE
index.php U
catogry.php U
test.php U
catogry.php > html > body
<html>
<body>
<nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">

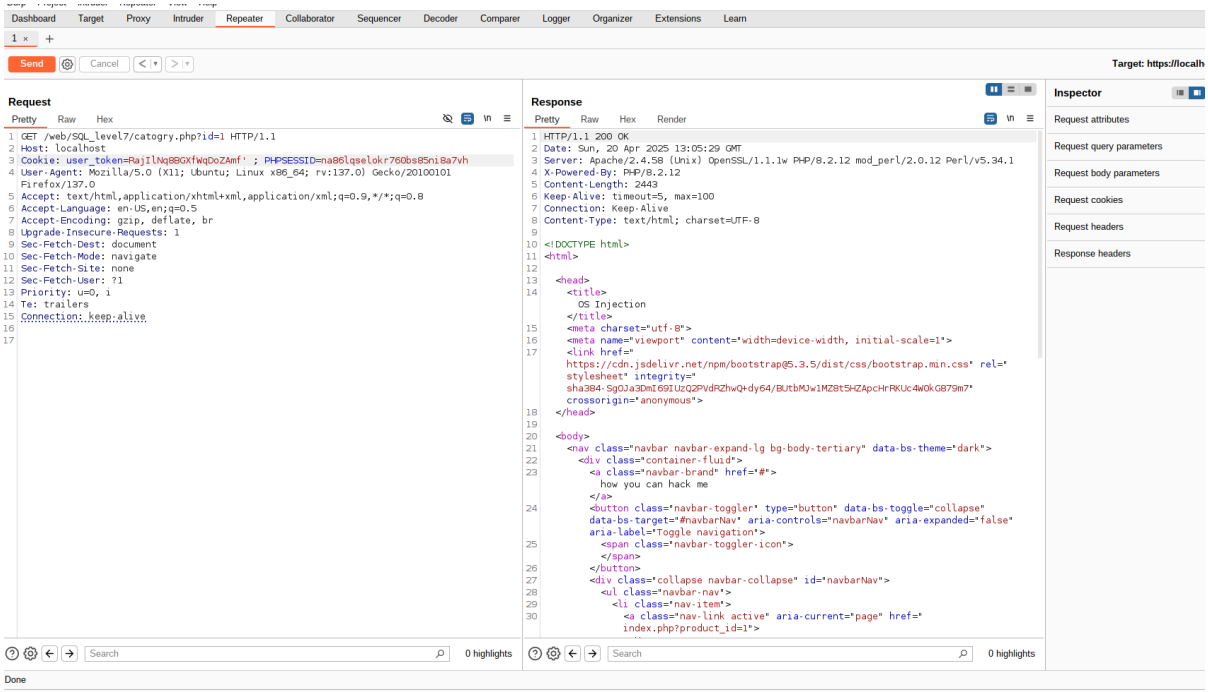
</nav>

<h1 class="display-2" style="text-align: center;">SHOP1</h1>

<?php
include("sql.php");
if (isset($_COOKIE["user_token"]) && !empty($_COOKIE["user_token"])) {
$token = $_COOKIE['user_token'];
}
try{
$check = $conn->query(query: "SELECT * FROM tokens WHERE token_value='". $token ."'");
}catch(mysqli_sql_exception $e){
error_log(message: "Database error: " . $e->getMessage());
http_response_code(response_code: 200);
}
if(isset($_GET["id"])){
$id=$_GET['id'];
}
$sql = "SELECT * FROM catogry WHERE id='$id'";
if(is_here(item: $sql)){
$result = $conn->query(query: $sql);
if ($result->num_rows > 0) {
?>

<?php $row= $result->fetch_assoc()?>
<h3>Tiltle:<?php echo $row["title"];?> </h3>

<img src="<?php echo $row["image"];?>">

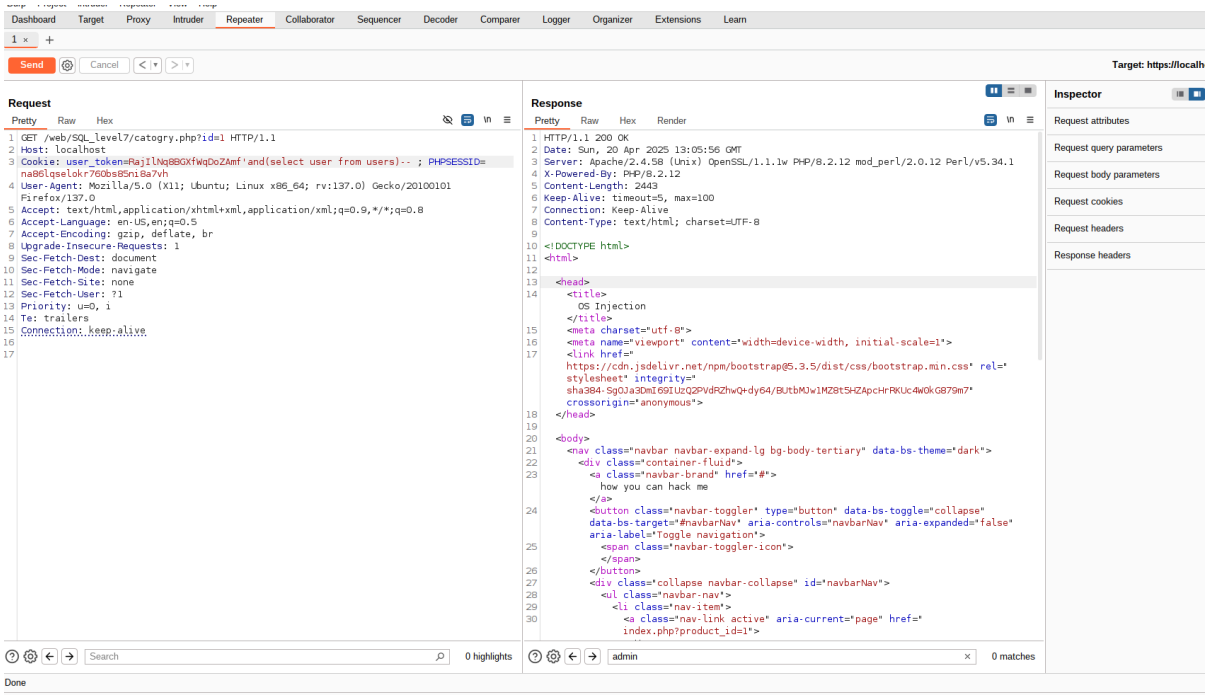

Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Organizer Extensions Learn
Send Cancel
Target: https://localh
Request
Pretty Raw Hex
GET /web/SQL_level7/catogry.php?id=1 HTTP/1.1
Host: localhost
Cookie: user_token=RajIlNqBBGXfWqDoZAmf' ; PHPSESSID=na86lqselokr760bs85ni8a7vh
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101 Firefox/137.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Te: trailers
Connection: keep-alive
Response
Pretty Raw Hex Render
HTTP/1.1 200 OK
Date: Sun, 20 Apr 2025 13:05:29 GMT
Server: Apache/2.4.58 (Unix) OpenSSL/1.1.1w PHP/8.2.12 mod_perl/2.0.12 Perl/v5.34.1
X-Powered-By: PHP/8.2.12
Content-Length: 2443
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: text/html; charset=UTF-8
<!DOCTYPE html>
<html>
<head>
<title>
OS Injection
</title>
<meta charset="utf-8">
<meta name="viewport" content="width=device-width, initial-scale=1">
<link href="
https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel="
stylesheet" integrity="
sha384-SgOJa3DmI69IUzQ2PVdRZhwQ+dy64/BUtbMJw1MZ8t5HZApcHrRKUc4W0kG879m7"
crossorigin="anonymous">
</head>
<body>
<nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">

how you can hack me

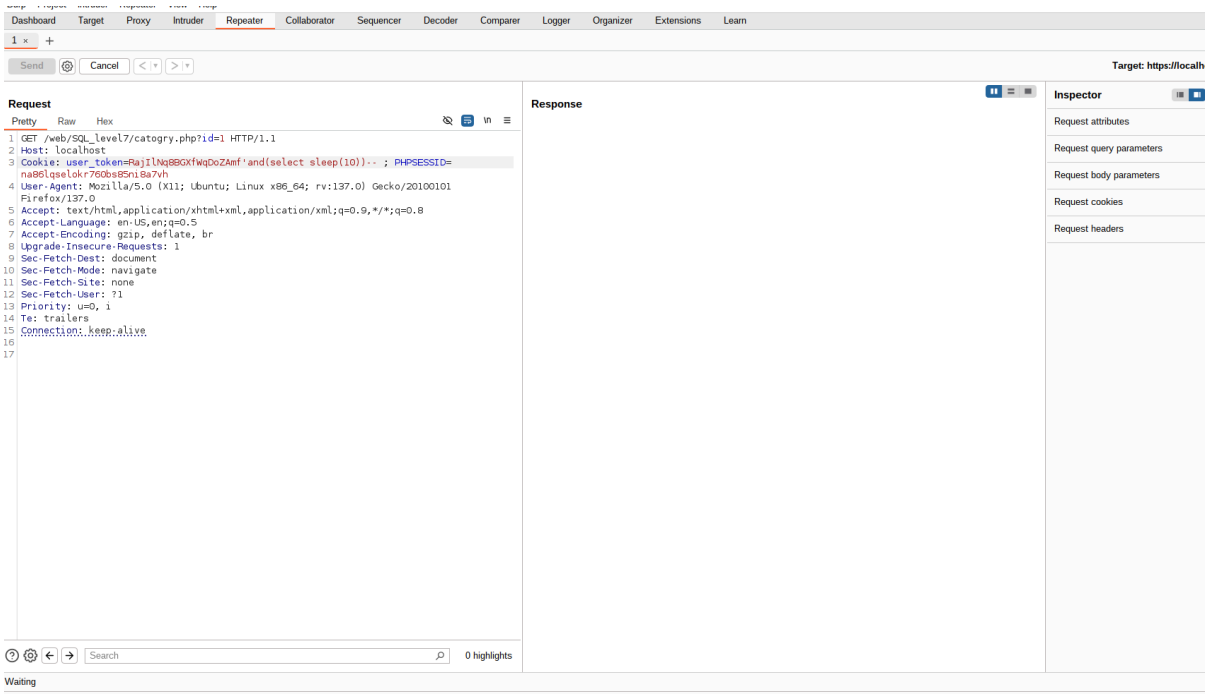
<button class="navbar-toggler" type="button" data-bs-toggle="collapse"
data-bs-target="#navbarNav" aria-controls="navbarNav" aria-expanded="false"
aria-label="Toggle navigation">

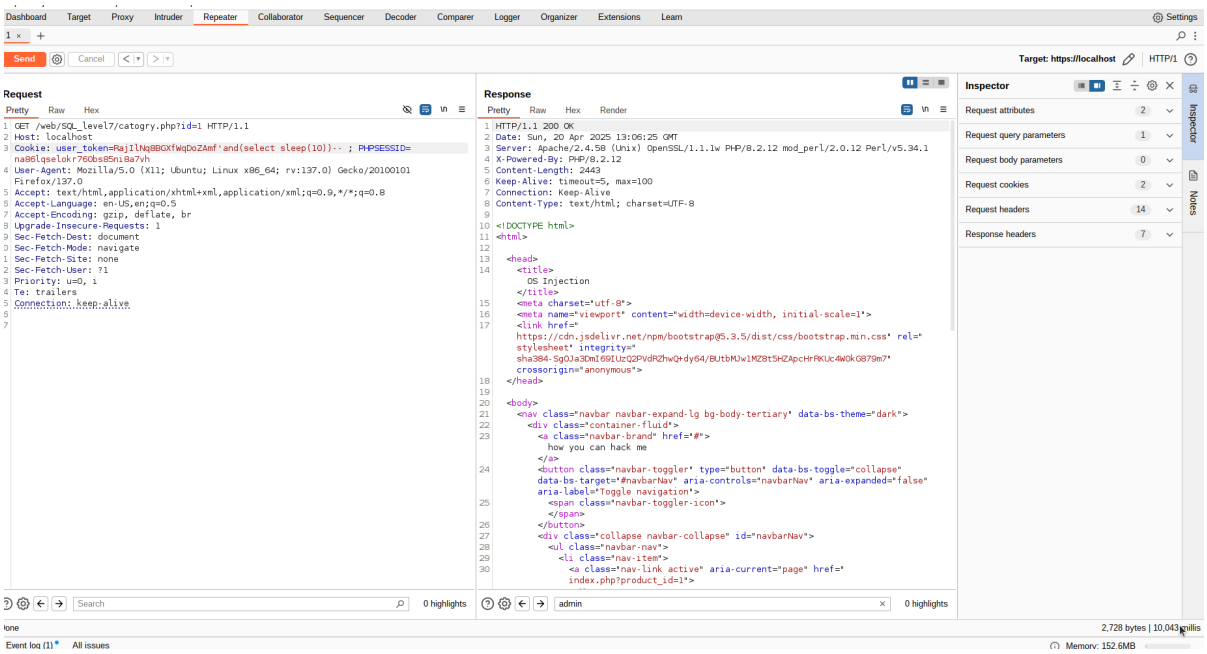
</button>

<ul class="navbar-nav">
<li class="nav-item">
<a class="nav-link active" aria-current="page" href="
index.php?product_id=1">
Inspector
Request attributes
Request query parameters
Request body parameters
Request cookies
Request headers
Response headers
Search
0 highlights
Search
0 highlights
Done



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



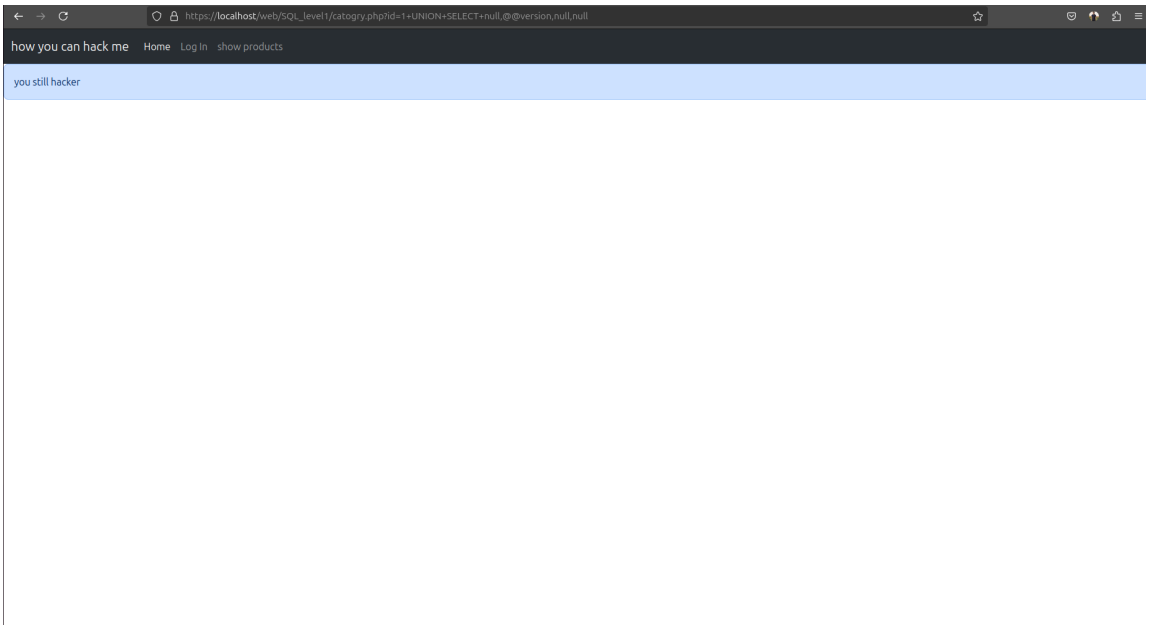


- the response will come back after 10sec
- you will show that the time in the bottom of the right is ⇒ 10.043 ms

---

▼ 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.