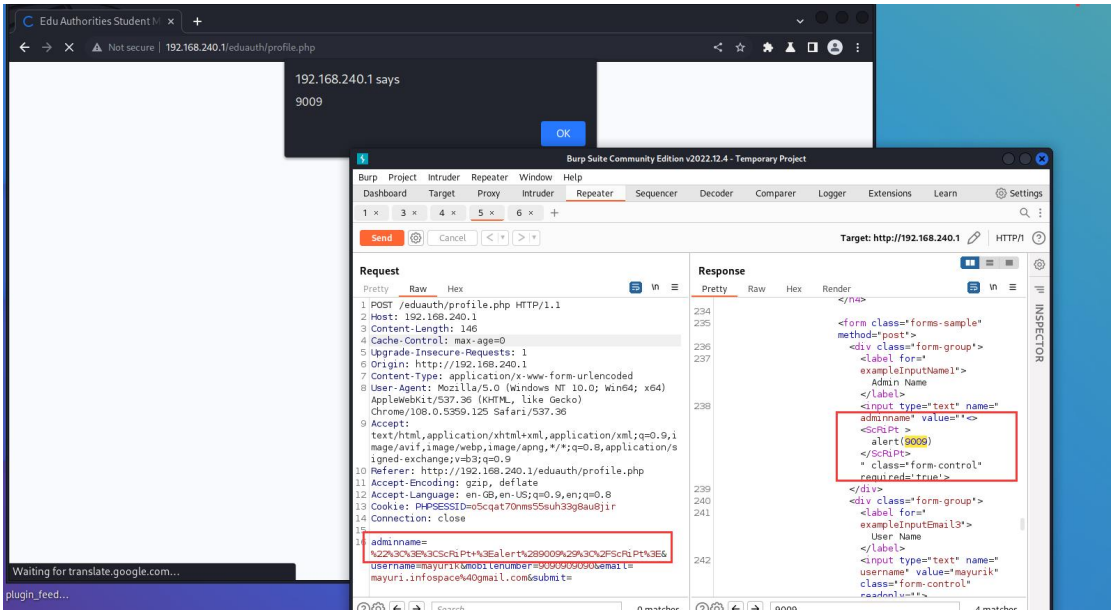
XSS injection vulnerability exists in adminname parameter of profile.php file of Online student management system

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.

```
    $AName=$_POST['adminname'];
$mobno=$_POST['mobilenumber'];
$email=$_POST['email'];
$sql="update tbladmin set AdminName=:adminname,MobileNumber=:mobilenumber,Email=:email where ID=:aid";
    $query = $dbh->prepare($sql);
    $query->bindParam(':adminname',$AName,PDO::PARAM_STR);
```

```
{          ?>
                    <div class="form-group">
                      <label for="exampleInputName1">Admin Name</label>
                      <input type="text" name="adminname" value="<?php  echo $row->AdminName;?>" class="form-control" required='true'>
                    </div>
                    <div class="form-group">
```



Payload:

adminname=%22%3C%3E%3CScRiPt+%3Ealert%289009%29%3C%2FScRiPt%3E

Source Download：

https://www.sourcecodester.com/php/16137/online-student-management-system-php-free-download.html