Low Balancer

> Author : weibig | 陳惟中 | B06705014

Problem Description

http://eductf.zoolab.org:18787 Difficulty: medium

題目的網站是由jQuery建構而成，會將字串轉倒轉，並在下方印出。另外空格會變轉成"+"號，有些字串受限制而不會被印出(e.g. 輸入 >?php?< 倒轉後的 不會印在下方)。

Solution

> 並沒有解出此題，寫下我的解題過程

一開始看到此題，先想辦法實作js alert(1)，首先bypass空格限制，我用 "" 分割 attribute ，也就是利用 `<img\onerror="">` 的倒轉放入js payload，的確讓網站作出 alert(1)。之後觀察原始碼，與組員討論可能可以怎樣存取到目錄下的 flag.txt，認為光靠js不是一個能有效找出 flag 的方法，但又無法在空格裡實作 `<?php ?>` 的 php code，我覺得這題應該跟用 "," 分隔字串有關，因為字串中有 "," 會被分成兩個 `<div>` ，如果可以存取到 `<div>` 裡面的資料，可能有辦法做一些繞過處理，但最後因為沒有時間繼續琢磨而沒能取到 flag。