echo

> Author : disam | 王松億 | B06705049

Problem Description

https://eductf.zoolab.org:49007 Difficulty: medium

題目的網站是由express+ejs建構而成，而允許的動作就只有POST給根目錄，然後網站會把text的paramater值渲染到一個網頁並回傳。

Solution

> 並沒有解出此題，寫下我的解題過程

查看原始html發現/echo.zip可以下載source code，在本地端先架了一個server測試，發現只要在POST request的body設定複數個text的值，text就會變成json或array，且我們也可以任意的控制裡面的key和value值，因此第一個想到的辦法是prototype pollution，因為如果要把text印出來，就必須呼叫text.toString()這個內建的function，而經過測試結果可以知道如果我們把text的型態變成一個json且裡面有一個key為toString，那網站就會噴error，原因是toString不是一個function而是我們傳進來的字串，所以只要有辦法將text[toString]這個值改成一個function，就可以任意執行我們想要的函式，但最後還是沒找到。 後來又往ejs的source code看，楊皓丞發現 https://www.xmsec.cc/prototype-pollution-notes/ 這個網站有寫到某個ejs的漏洞，但最後我們沒實作出來。