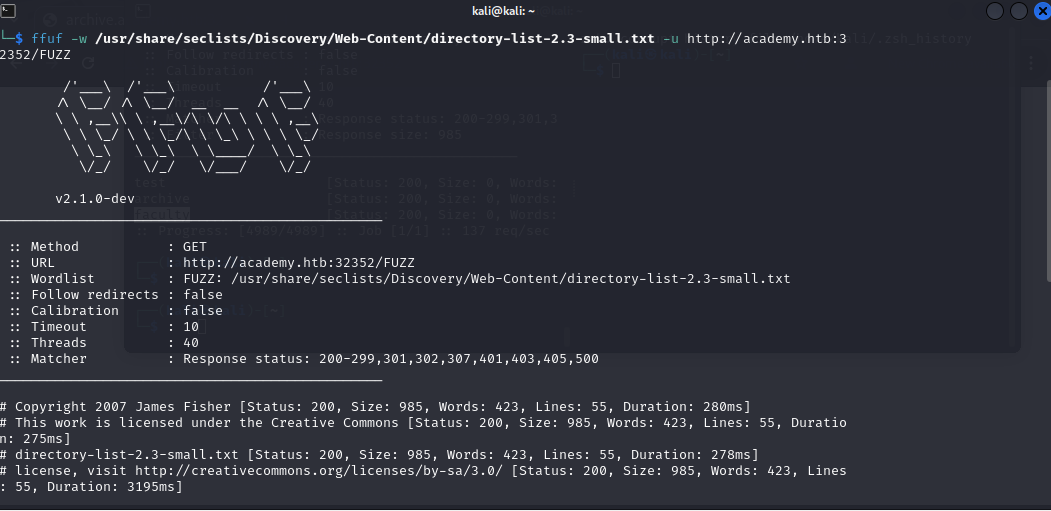
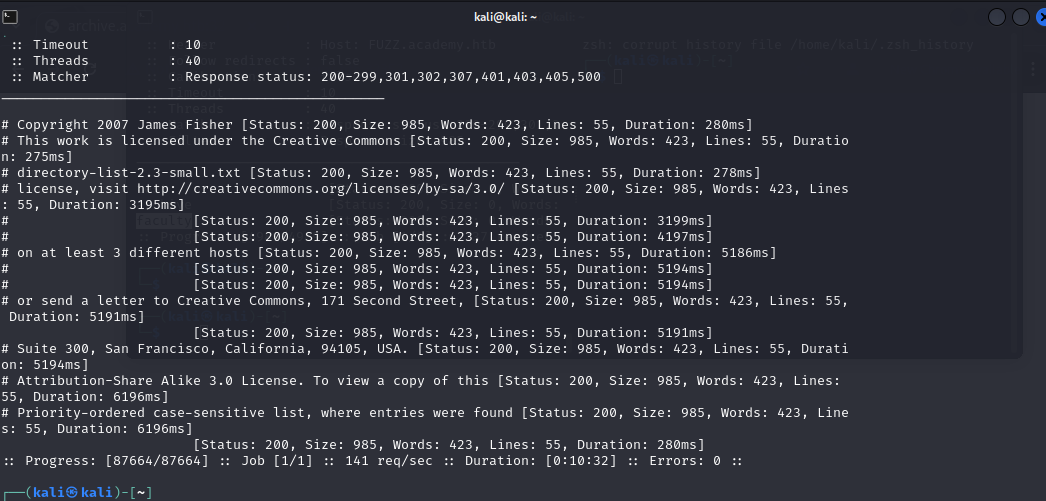
IP: 94.237.51.209:32352

Đầu tiên chúng ta cùng burp force directory của web này xem coi có gì thú vị hông nha



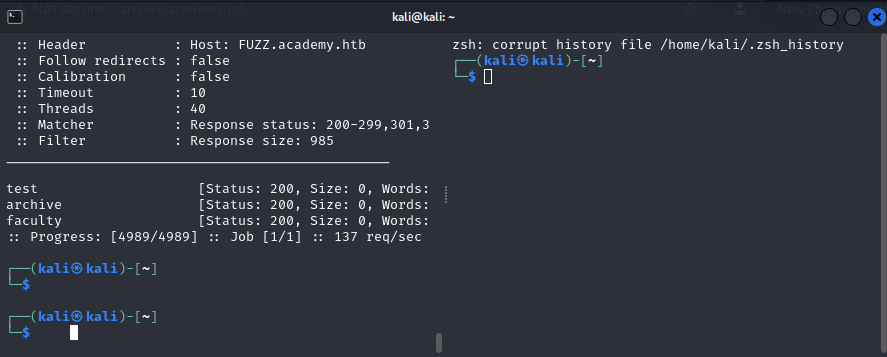
Đáng tiếc là không có gì xuất hiện



Kế tiếp chúng ta thử tìm kiếm sub-domain của web này với câu lệnh:

*ffuf -w /opt/useful/seclists/Discovery/DNS/subdomains-top1million-5000.txt:FUZZ -u http://academy.htb:PORT/ -H 'Host: FUZZ.academy.htb'*

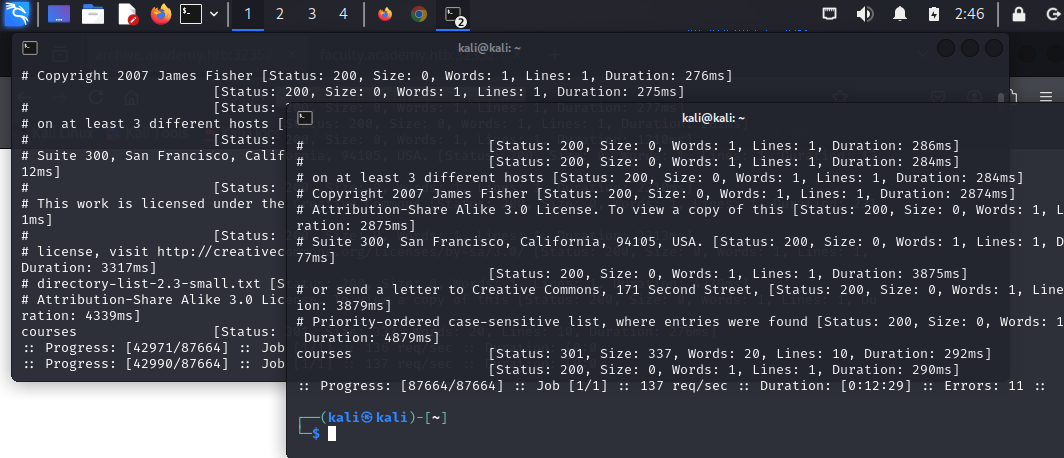
(vì có gợi ý ip này là của web academy.htb nên chúng ta có thể viết thẳng vào etc/hosts local bằng câu lệnh sudo ‘echo “IP\_SERVER name\_web” >> /etc/hosts’ để nó phân giải tên miền trong trường hợp mình thử truy cập web browers mà hong ra nha)



Quá đã lần này tìm ra 3 thư mục mới *(đáp án 1)*

Nào chúng ta tiếp tục burp force thì chỉ tìm được trong 2 thư mục archive faculty đều có source

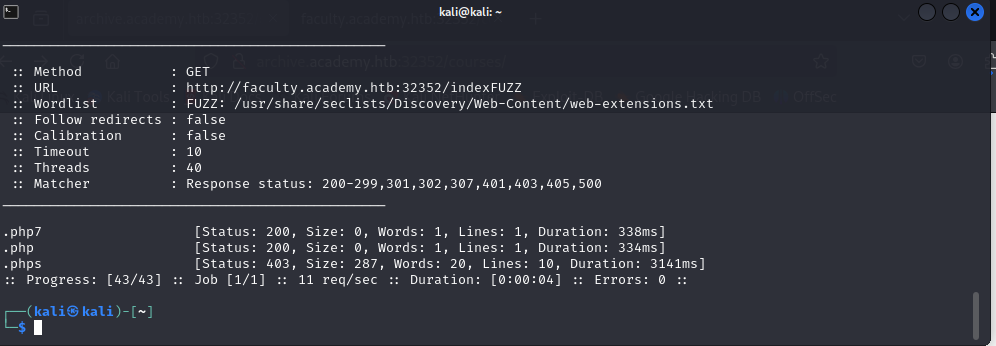
1 tín hiệu tốt



Tiếp tục tới bước tìm extension mà web sử dụng là loại nào?

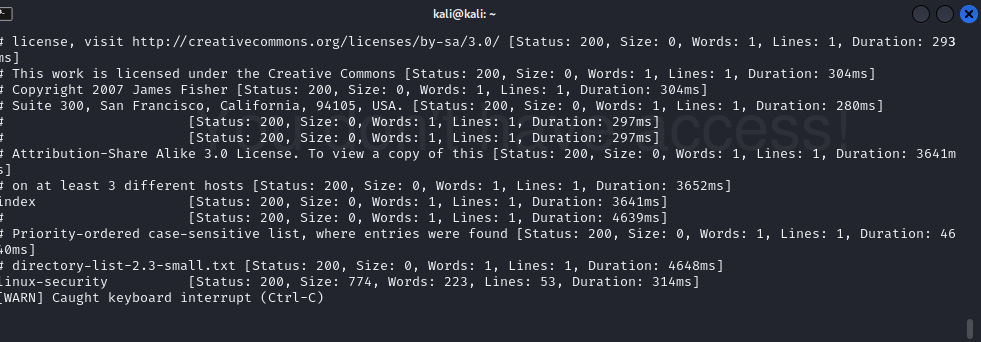
Ta dùng lệnh:

*ffuf -w /usr/share/seclists/Discovery/Web-Content/web-extensions.txt:FUZZ -u* [*http://faculty.academy.htb:32352/indexFUZZ*](http://faculty.academy.htb:32352/indexFUZZ)

**

Sau khi burp force cả 3 url ta lấy được 3 kết quả như hình trên. *(đáp án 2)*

Vậy là ta đã biết được đuôi extension của web này dùng là gì rồi tiếp theo ta sẽ thử burp force tệp xem coi có gì không?

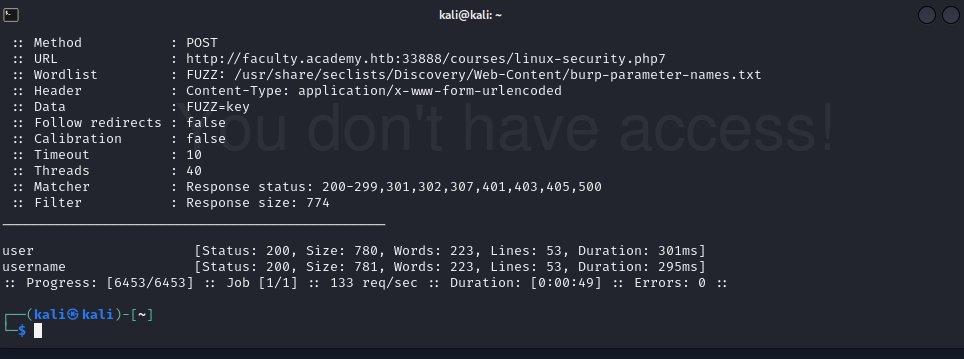


Phát hiện được 1 file khá nhạy cảm và không được acess *(đáp án 3)*

Sau đó sử dụng câu lệnh

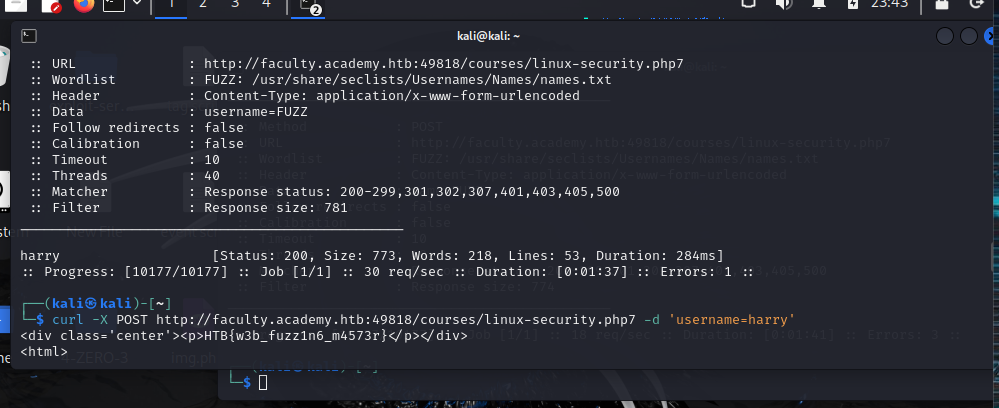
*ffuf -w /usr/share/seclists/Discovery/Web-Content/burp-parameter-names.txt:FUZZ -u http://faculty.academy.htb:33888/courses/linux-security.php7 -X POST -d 'FUZZ=key' -H 'Content-Type: application/x-www-form-urlencoded' -fs 774*

để burpforce parameter của trang bị chặn đó



ở đây ta thấy được 2 parameter hoạt động trên web đó. Đoán chừng user là dạng số id cho username tên của người dùng.

Tiếp tục tìm kiếm value của username ta thấy được tên của harry



Sau đó ta thử xem trang web với giá trị username=harry thì ta kiếm được flag cuối cùng.