B1.1

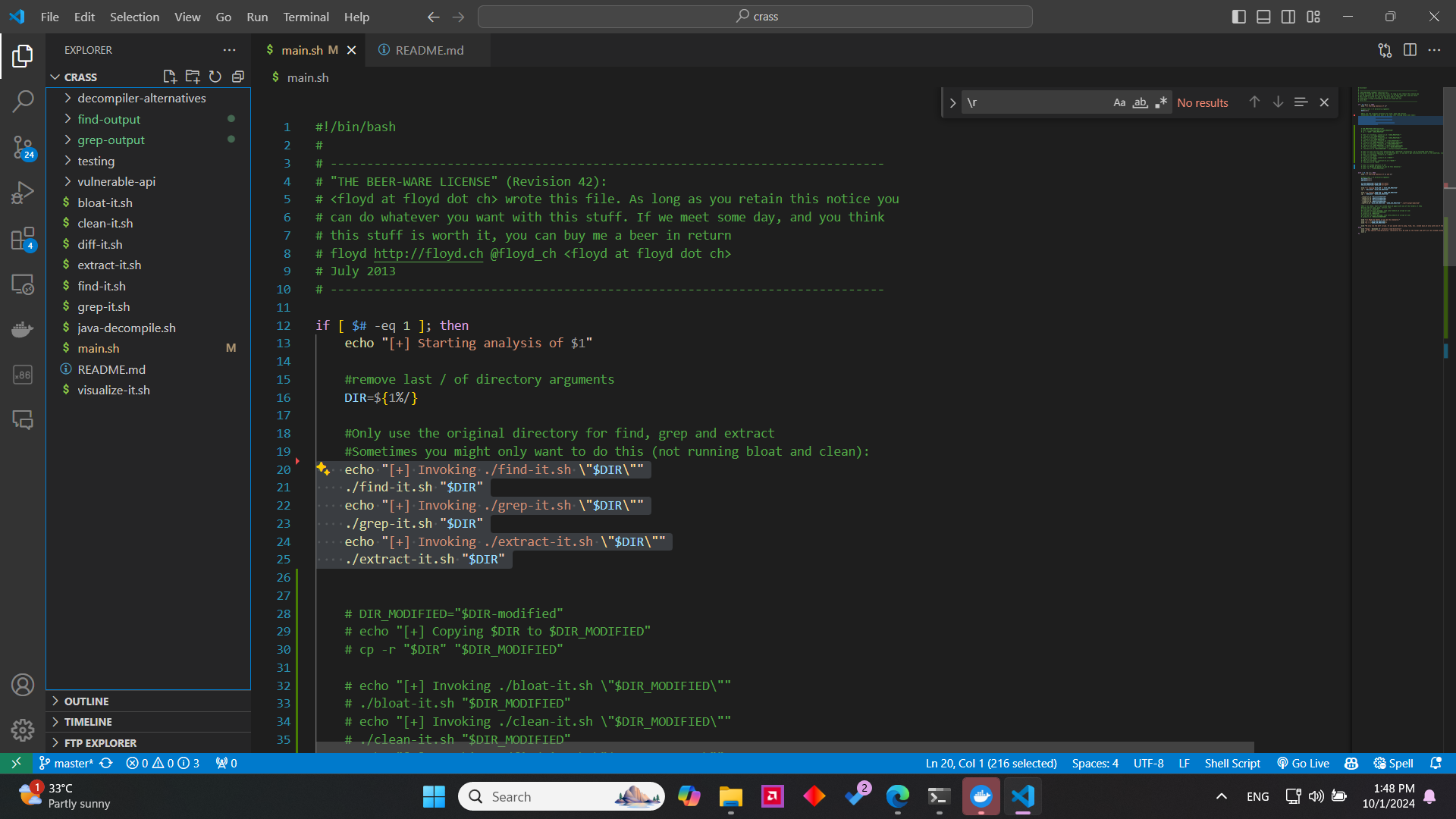


Figure 1: Đoạn code chỉnh sửa để chạy các lệnh

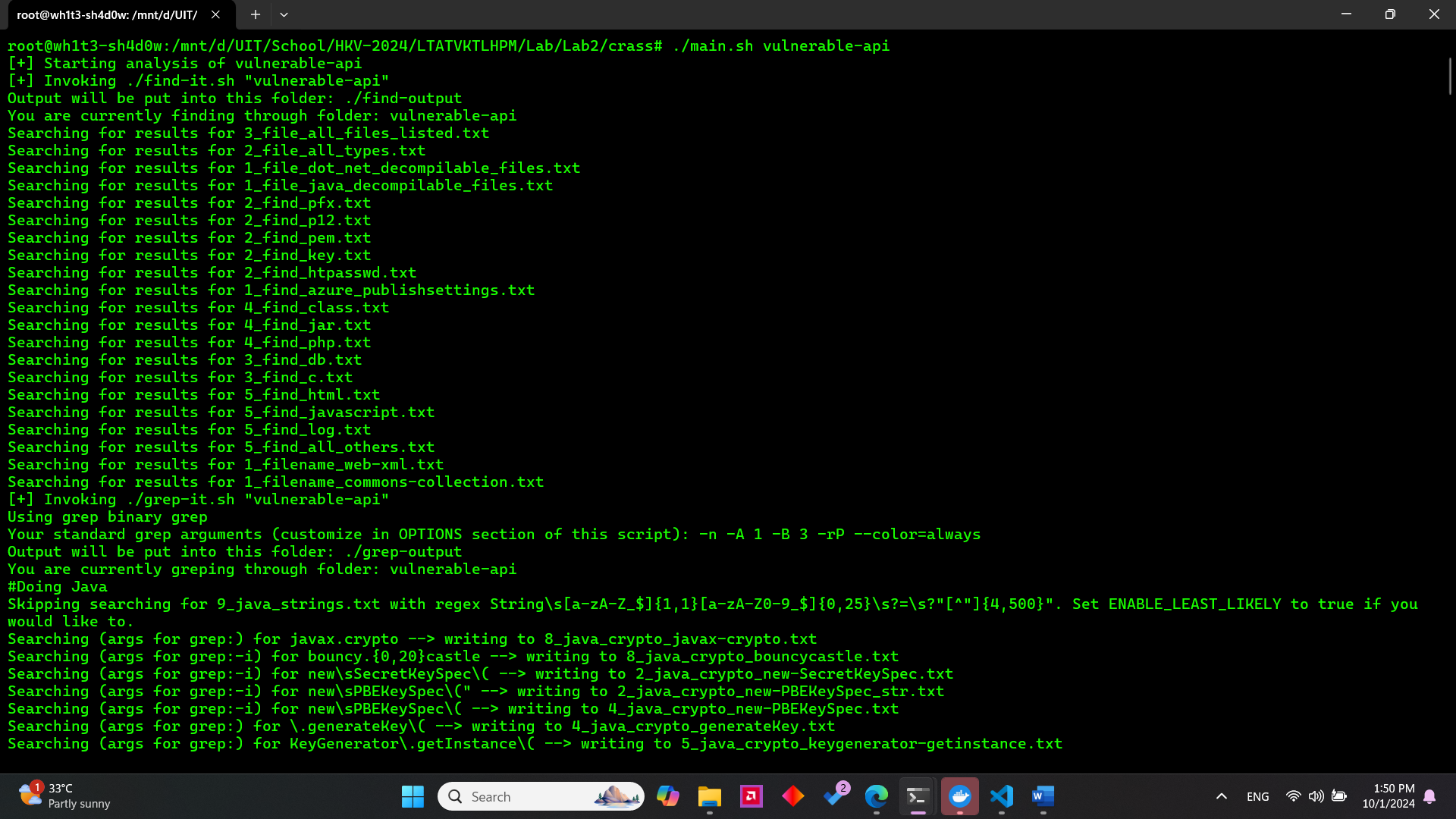


Figure 2: Màn hình chạy của bash script

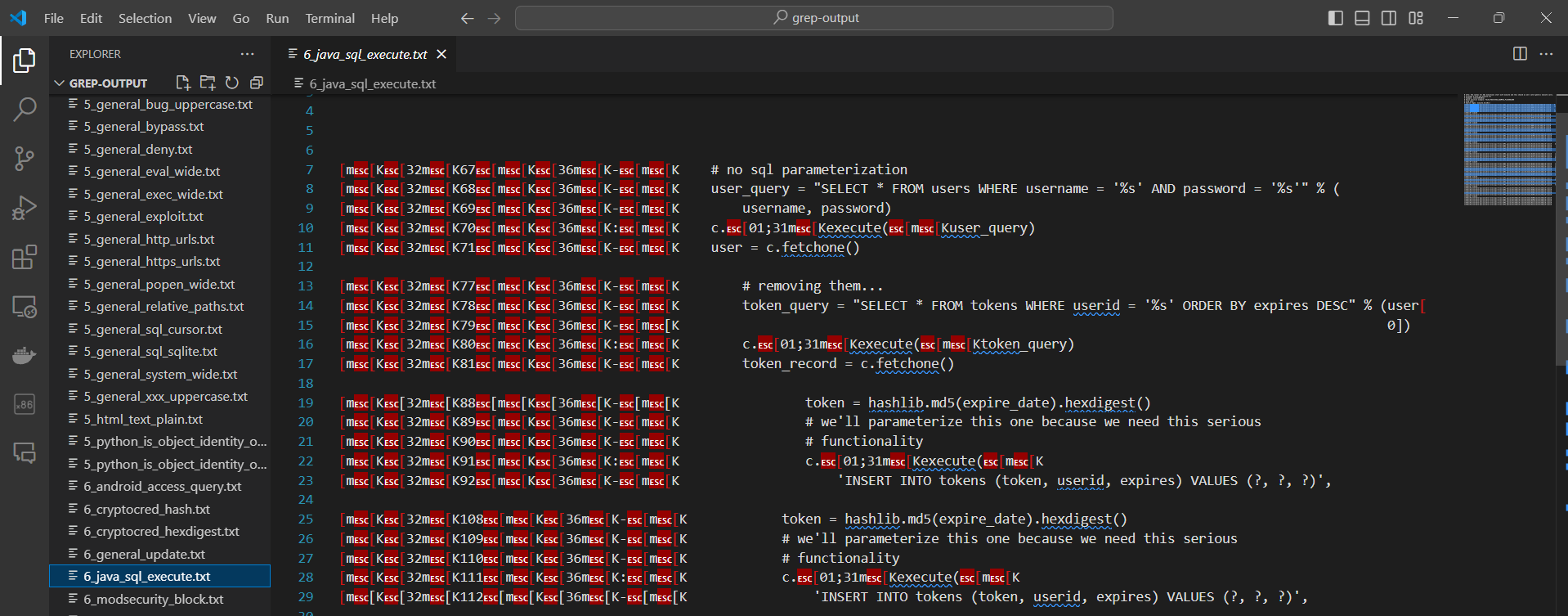


Figure 3: File output in ra lỗ hổng mà bash script tìm được

Ở đây, lỗi là do không thực hiện việc tham số hóa đầu vào truy vấn của câu lệnh SQL user\_query nên có thể xảy ra tấn công SQL Injection. Các câu lệnh truy vấn được tham số hóa bắt buộc các lập trình viên phải định nghĩa tất cả code SQL trước và sau đó mới đưa tham số vào trong câu truy vấn.

B2.2

Code **AttackerJava.java** thực hiện việc tạo ra 1 file **normalObj.serial** (có thể chứa mã độc) để cho code **MyJavaApp.java** thực hiện việc đọc vào.  
Ở đây ta thấy rằng Process p = Runtime.getRuntime().exec(this.cmd); là dòng code thực hiện chạy lệnh được deserialize từ file normalObj.serial. Vì **this.cmd** được deserialize từ **normalObj.serial** đã bị thay đổi, nên lệnh sẽ được thực hiện theo ý muốn của attacker

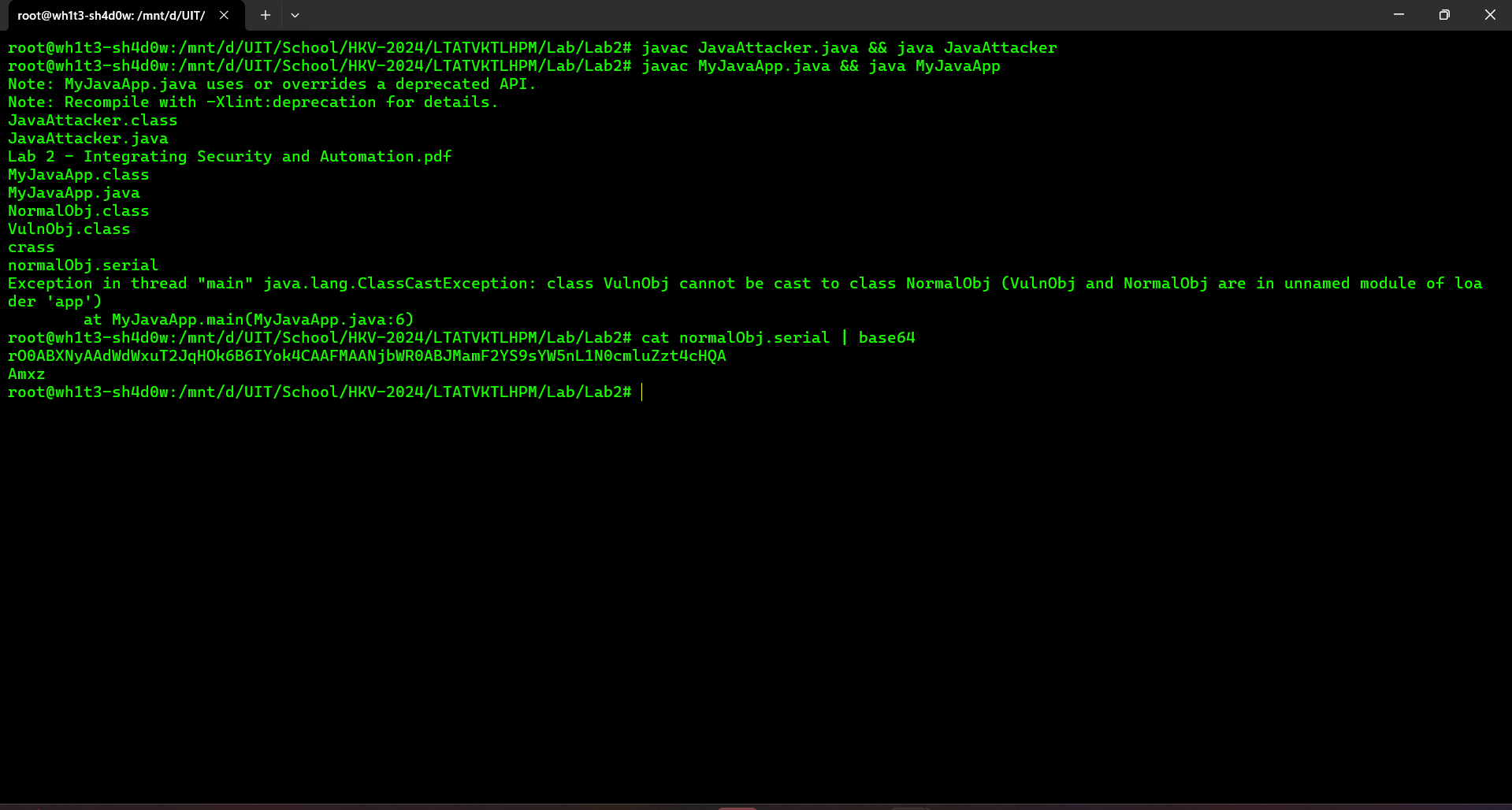


Figure 4: Màn hình sau khi thực hiện Attack và chuyển nội dung trong file normalObj.serial sang chuỗi base64.

Phần mở đầu của chuỗi ký tự base64 là r0OAB, cho ta biết rằng đây là Serialized Object của Java.

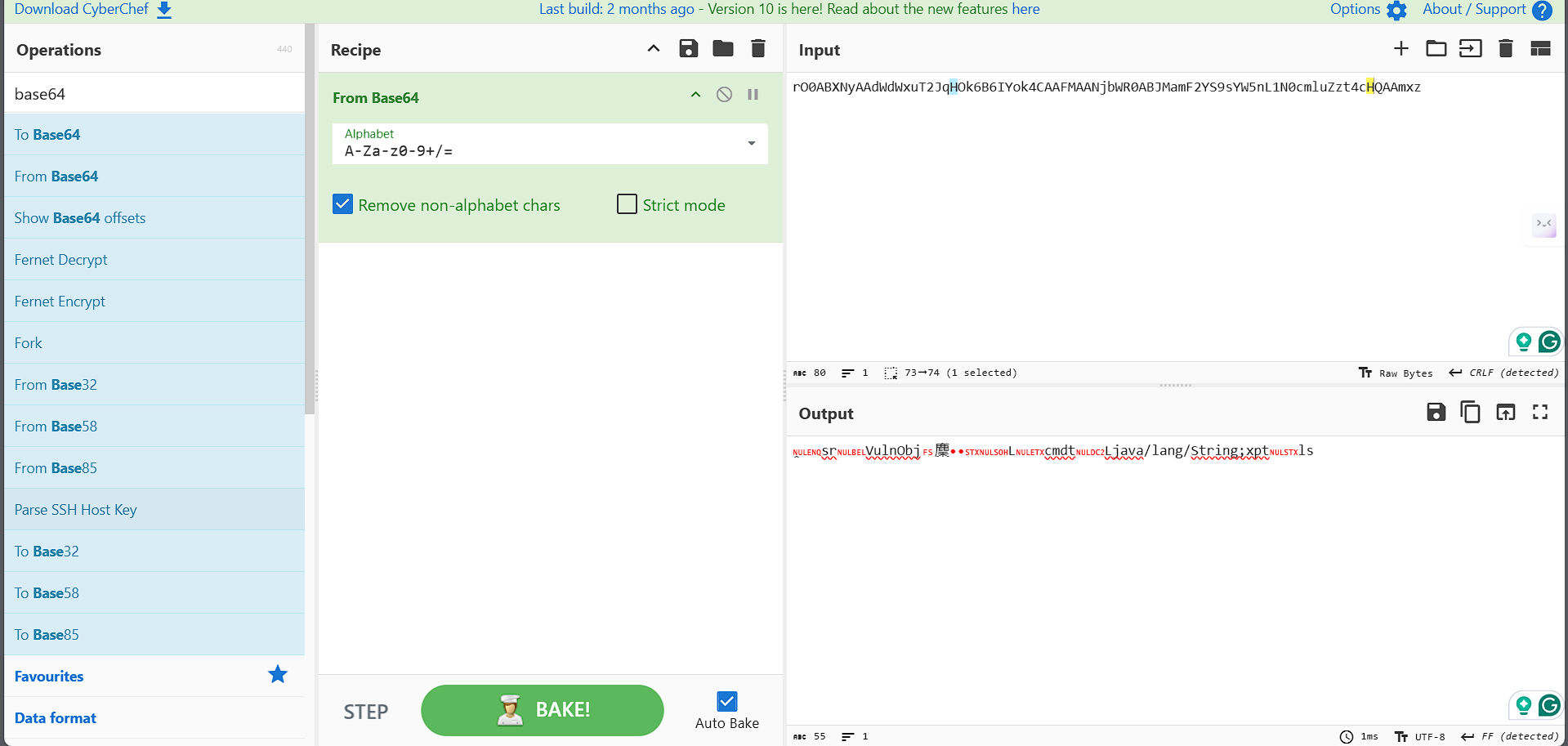


Figure 5: Decode chuỗi base64 được tạo ra

Thử decode mã base64 của **normalObj.serial**, ta thấy có **VulnObj** và **java/lang/String**

B2.4

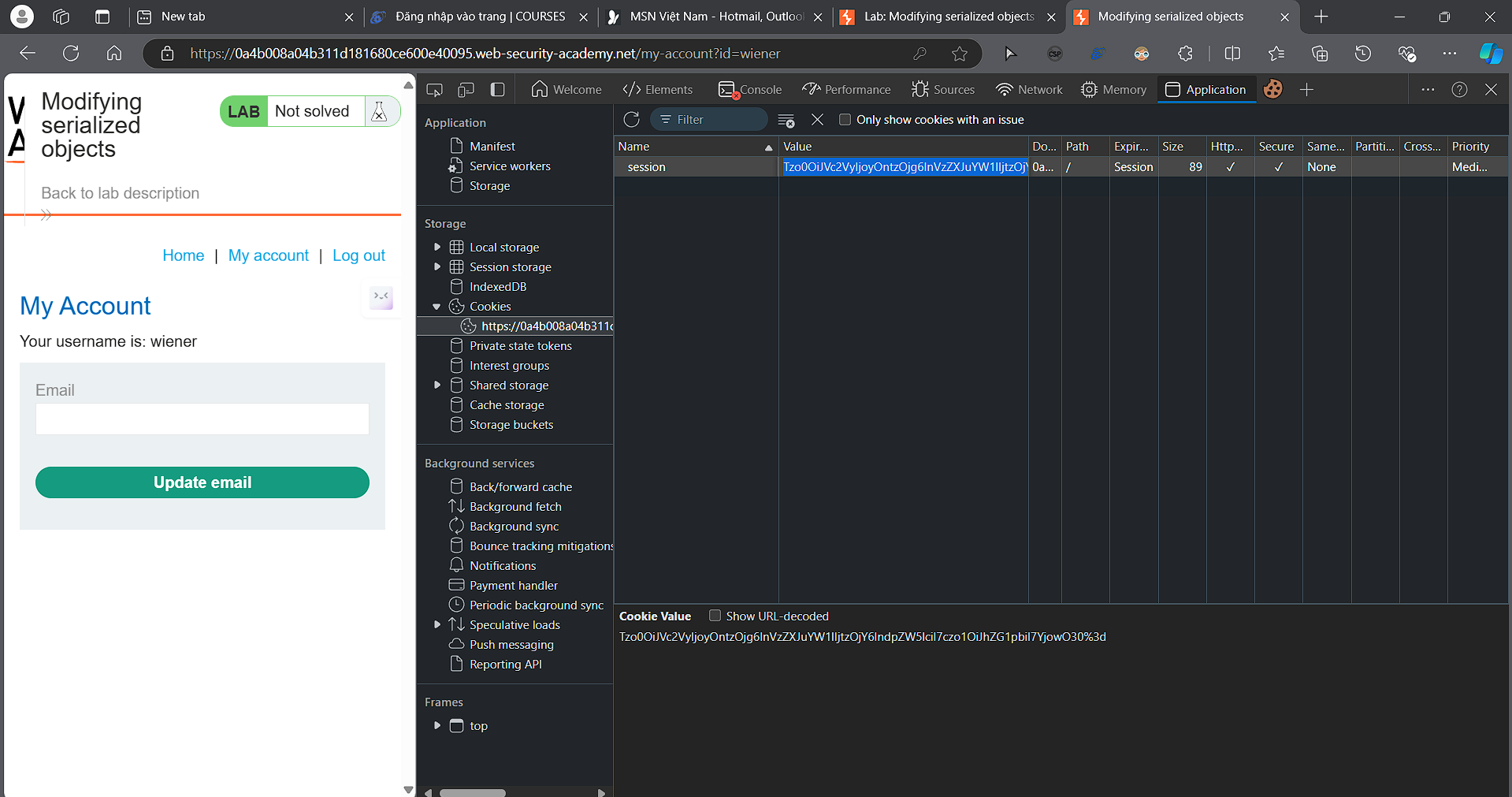


Figure 6: Value của session

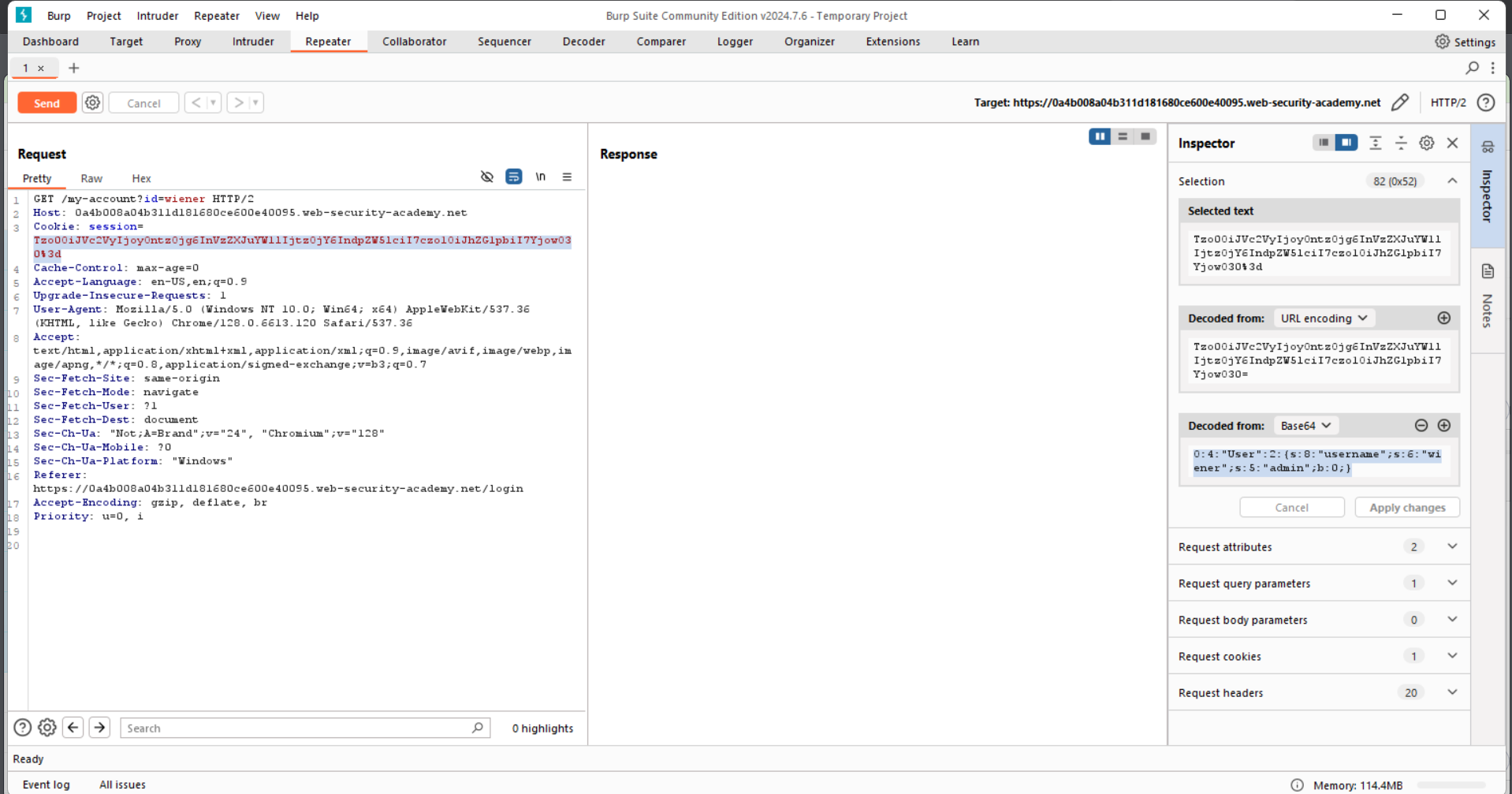


Figure 7: Deocde base64 value của session

Ta thấy rằng value của session khi decode từ base64 sẽ cho ta một Serialized object của PHP là: **O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:0;}**.

Ở đây thì giá trị của admin đang là 0 (false) nên nếu muốn thay đổi quyền sang admin sẽ đổi thành 1 (true) và sẽ có được chuỗi mới là **O:4:"User":2:{s:8:"username";s:6:"wiener";s:5:"admin";b:1;}** và tiến hành mã hóa chuỗi này sang base64

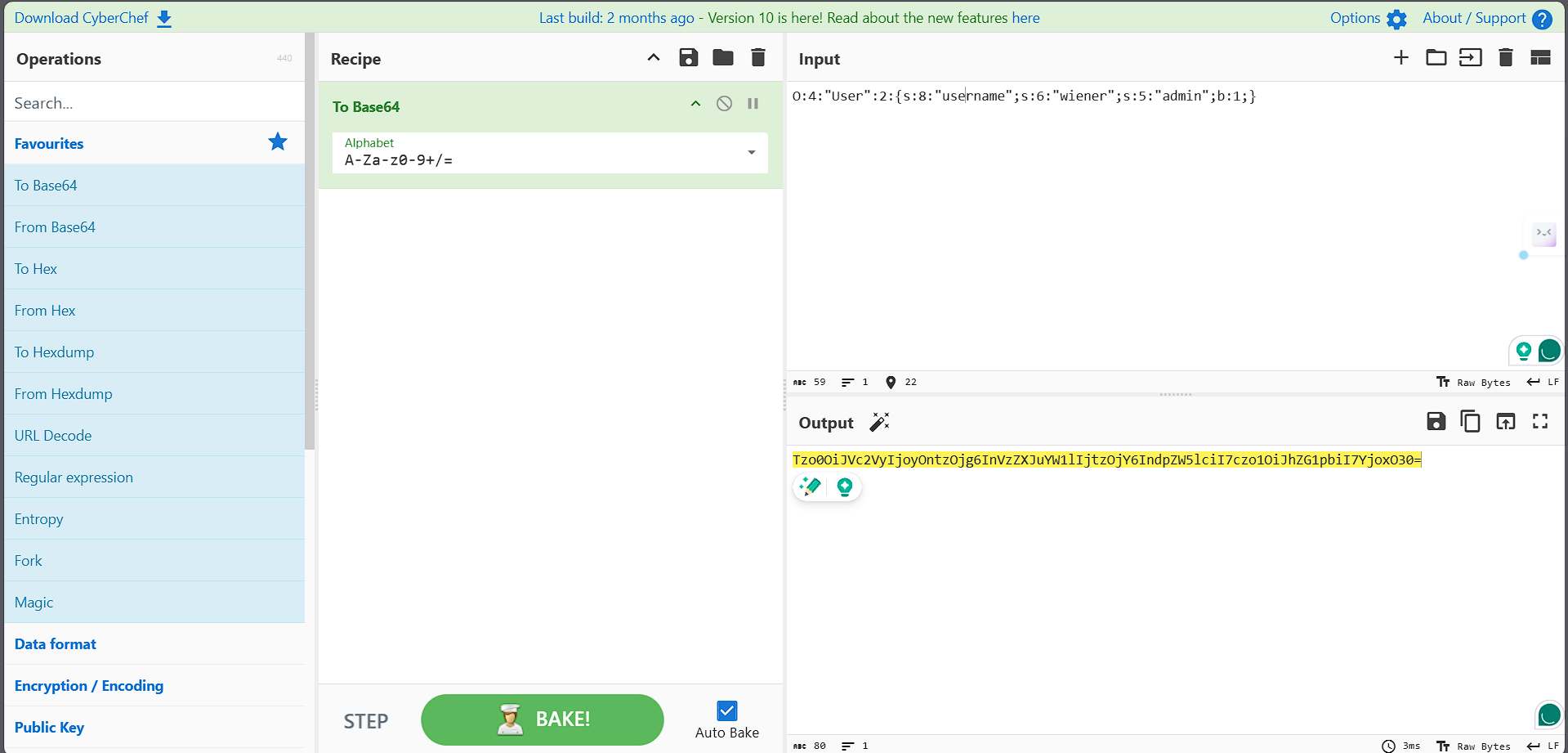


Figure 8: Mã hóa chuỗi mới sang base64

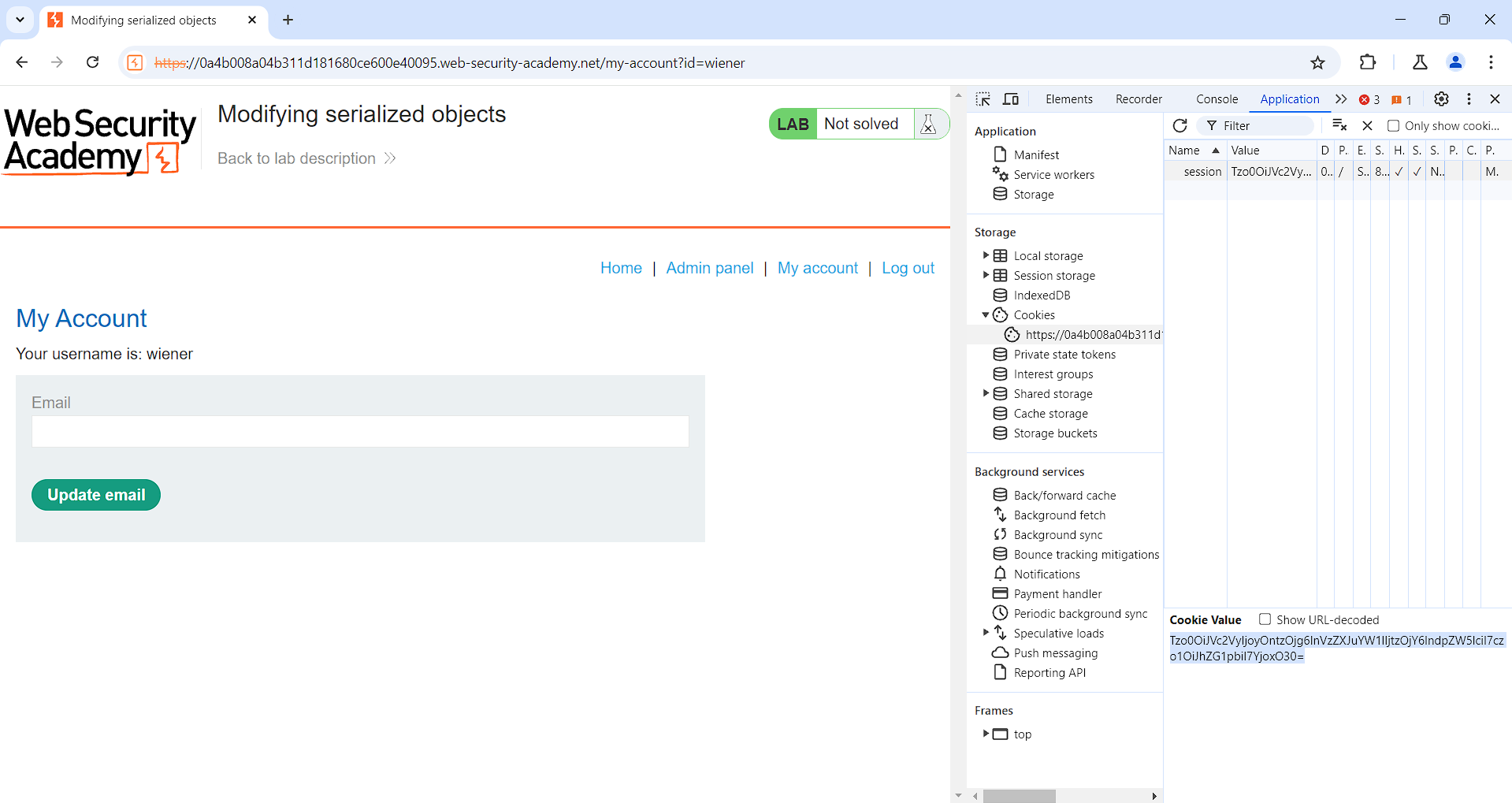
Giá trị mới của cookie sẽ là **Tzo0OiJVc2VyIjoyOntzOjg6InVzZXJuYW1lIjtzOjY6IndpZW5lciI7czo1OiJhZG1pbiI7YjoxO30=**  
  


Figure 9: Chèn cookie mới vào

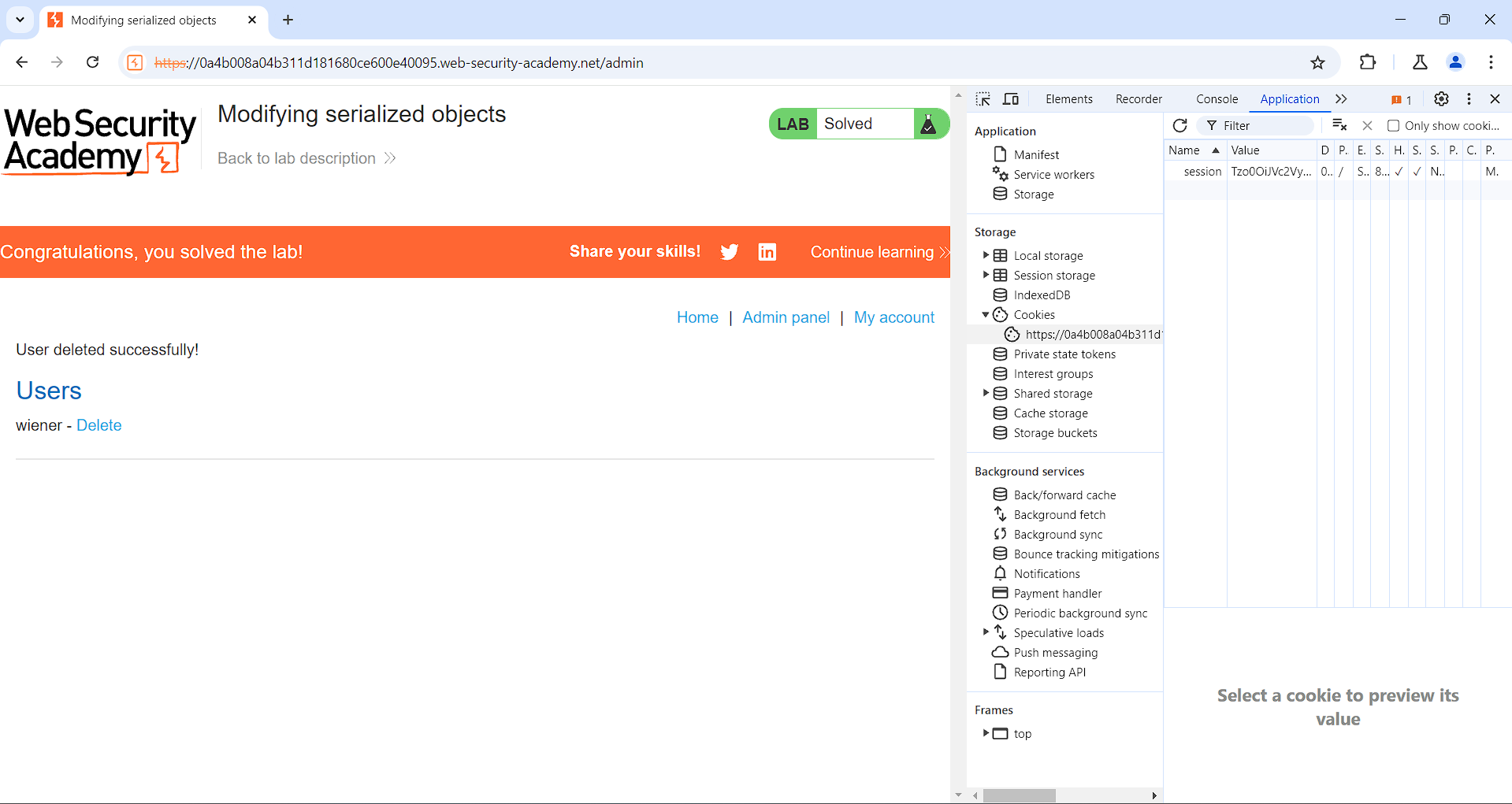


Figure 10: Bài lab hoàn thiện sau khi đã xóa user Carlos