Mình đã khai thác được lỗi của website : https://dx.thuathienhue.gov.vn

trong lúc học ở VNcert vào đầu năm 2024.

Chức năng : Đăng ký sự kiện

Dưới đây là một form đăng ký sự kiện mà khi nhìn vào ta có thể thấy được có rất nhiều trường có thể injection.

Ở đây mình sẽ khai thác 2 lỗi đó là XSS và File Inclusion

A screenshot of a computer

Description automatically generated

Mình sẽ inject payload XSS vào cả 3 trường : - “tên sự kiện, tóm tắt và nội dung” với cùng 1 payload JS đó là hiển thị thông báo cookie của người dùng ra khi họ nhìn thấy form sự kiện này.

Sau khi lưu, ứng dụng web sẽ thoát ra bên ngoài danh sách các event sắp diễn ra. Và có một event của mình vừa tạo, được thông báo với nội dung cookie của user, với 3 thông báo được hiển thị cùng 1 lúc. Ta có thể hiểu được rằng payload ở cả 3 trường đều đã tác động vào hệ thống.

A screen shot of a computer

Description automatically generated

Sau khi nhấn nút OK, event sẽ đựợc hiển thị dưới tên như dưới đây :   
A close up of a screen

Description automatically generated

Ta có thể thấy tên sự kiện chỉ còn đọng lại “phucduuu”, phần JS còn lại đã đi đâu?

Câu trả lời là nó vẫn ở đó, vẫn ở phía sau chữ “phucduuu”, nhưng nó đang được thực thi và hiển thị.

Một câu hỏi nữa, đó là : Nếu như user thấy được cookie của chính bản thân họ thì chẳng phải là một chuyện bình thường hay sao ?

Câu trả lời sẽ là : Mình có thể xài payload khác, có thể user sẽ không có hiển thị gì cả. Mà ngầm gửi một gói tin đến một trang web mà “mình” host. Gói tin đó sẽ bao gồm cookie của user, kèm theo đó là trường `referer`để biết chính xác user đó đến từ trang web nào. Nhưng đây là một trang web gov, bạn có thể hình dung sẽ ra sao nếu mình khai thác một trang web gov rồi đấy.

\*Nội dung của bài này chỉ dừng lại ở việc phục vụ mục đích học tập.

Trong lúc sử dụng thử trang web, mình đã biết được rằng site này sử dụng .NET. Tiếp theo mình sẽ khai thác với lỗi File Inclusion, trong lúc gửi gói tin ở phía trên, mình đã bắt lại bằng burp suite, sau đó chèn payload bằng một đoạn mã .aspx với nội dung như sau :

A screenshot of a computer screen

Description automatically generated

Đoạn code này sẽ tạo một kết nối TCP đến ip và port được chỉ định, sau đó mình sẽ listen trên cổng đã được IP public forwarding.

Sau khi đã gửi gói tin đến ứng dụng web, nhìn response để thấy được phản ứng của ứng dụng web là đã nhận file vừa được upload.

Tiếp theo set up listen trên port 80, và truy cập url mà site đã trả về.

A screenshot of a computer

Description automatically generated

Ở đây mình đã check user của folder upload, và xem một số thông tin cơ bản.

Mình đã dừng việc khai thác tại đây, vì lý do như trên.

Khai thác như thế này chỉ là khai thác lỗi file upload. Theo phỏng đoán của mình, nếu mình khai thác bằng lỗi file inclusion thì có lẽ là một user khác có quyền cao hơn.

* TimoMangCut