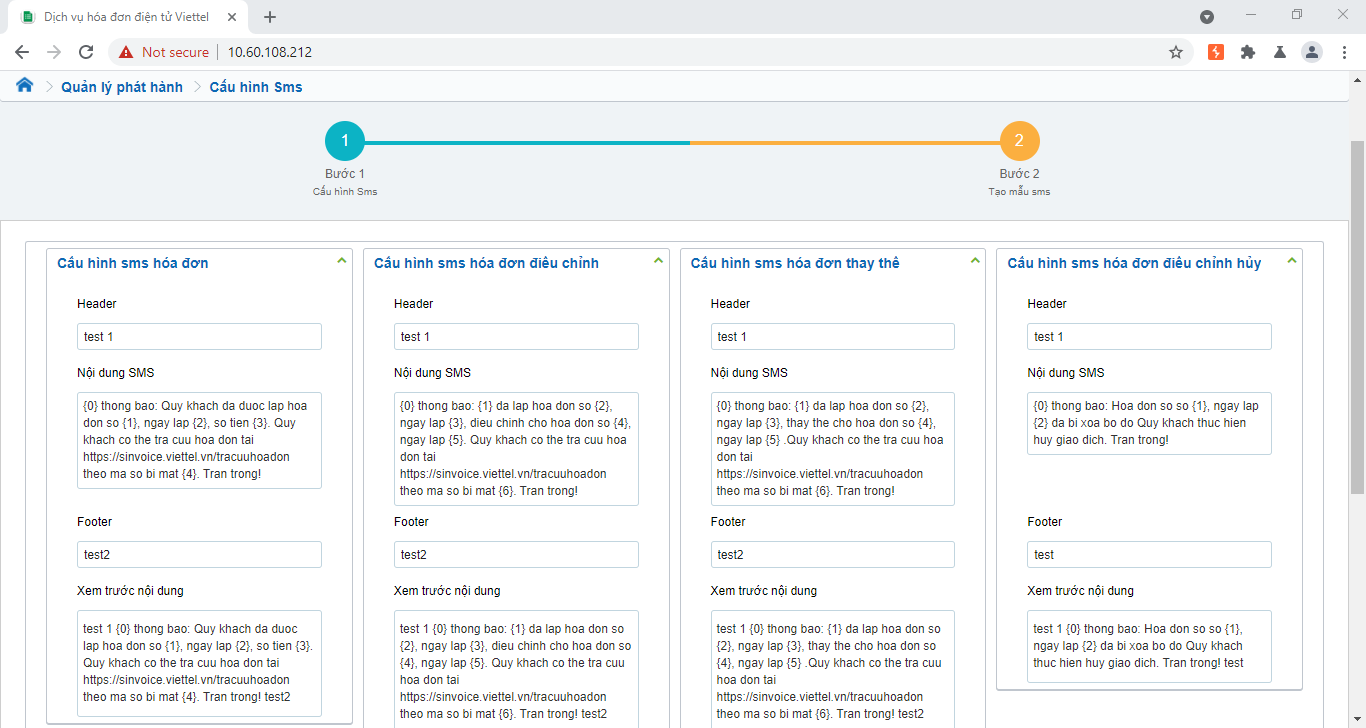
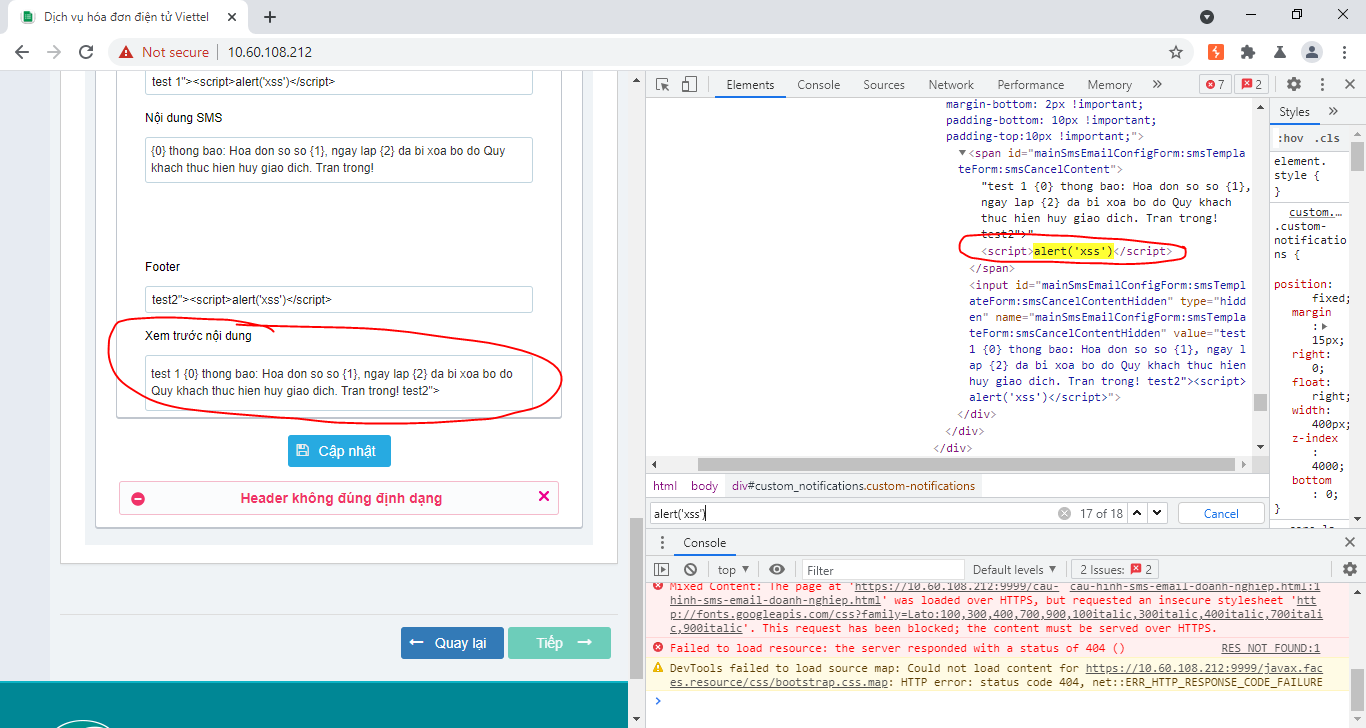
Report HDDT v1

* Tên lỗi: XSS stored
* Mức độ: Cao.
* Endpoint ảnh hưởng: /cau-hinh-tin-nhan
* Miêu tả: Khi người dùng vào mục cấu hình sms. Nhập một đoạn mã javascript vào các trường "Header", "Nội dung sms"hoặc "Footer" và lưu lại. Đoạn mã javascript đó sẽ được đưa vào trường "xem trước nội dung" và thực thi code javascript.
* Cách fix: Endcode dữ liệu ở trường “Xem trước nội dung”trước khi trả về cho client.
* PoC:





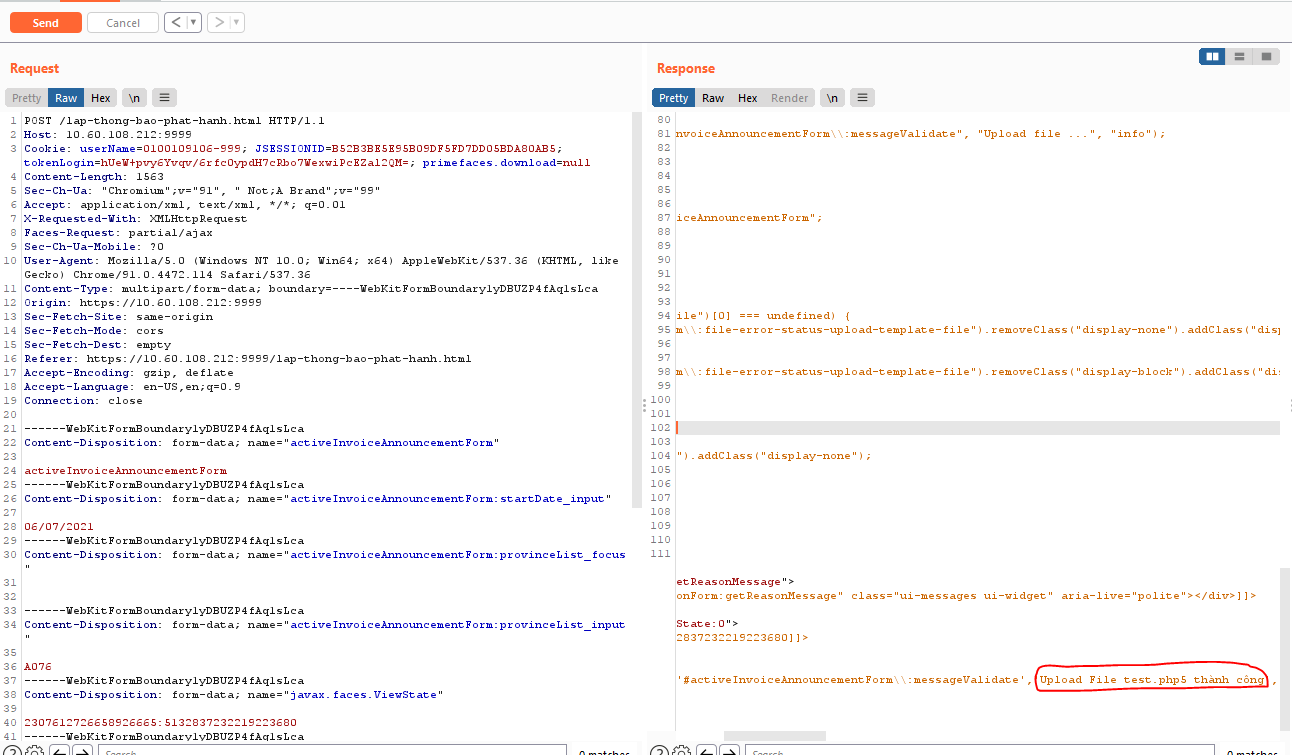
1. Tên lỗi: upload file tùy ý.

Mức độ: yếu.

Endpoint ảnh hưởng: /lap-thong-bao-phat-hanh.html

Miêu tả lỗi: Ở mục “quản lý phát hành”, người dùng chọn “lập thông báo phát hành” và chọn mục “thêm mới” sau khi hoàn thành việc thêm mới thì thực hiện “gửi yêu cầu phê duyệt” một thoại sẽ hiện ra và yêu cầu người dùng chọn một file pdf. Với nội dung file được bắt đầu bằng ký hiệu nhận dạng của file pdf va nội dung do người dùng viết(tùy ý). Thì sever vẫn xử lý kể cả khi đó là file php.

Fix: kiểm tra nội dung file trước khi thực hiện upload lên máy chủ.



1. Tên lỗi: Reflected xss(self).

Mức độ: Yếu.

Endpoint ảnh hưởng: /lap-thong-bao-phat-hanh.html

Miêu tả: khi người dùng thực hiện upload một file với tên là một đoạn mã javascript ở hành động “Gửi yêu cầu phê duyệt” sau đó server sẽ trả lại tên file do người dùng upload mà không encode.

Fix: encode tên file trước khi trả về cho người dùng, hoặc chỉ đưa ra thông báo “upload file thành công”.

PoC:

