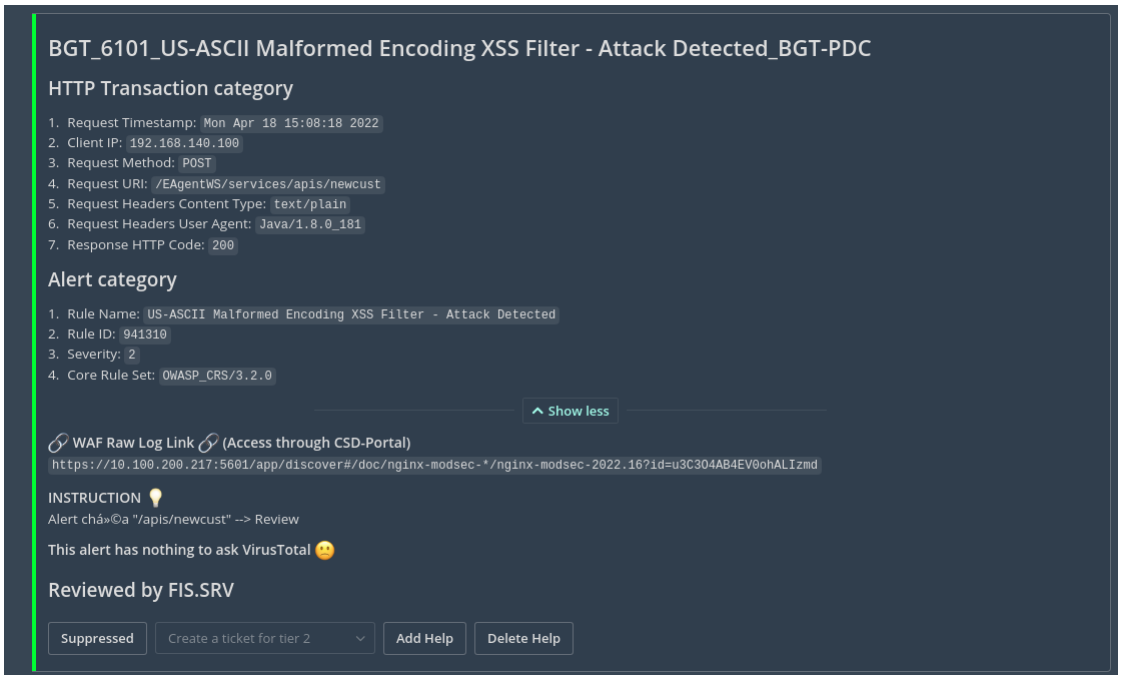
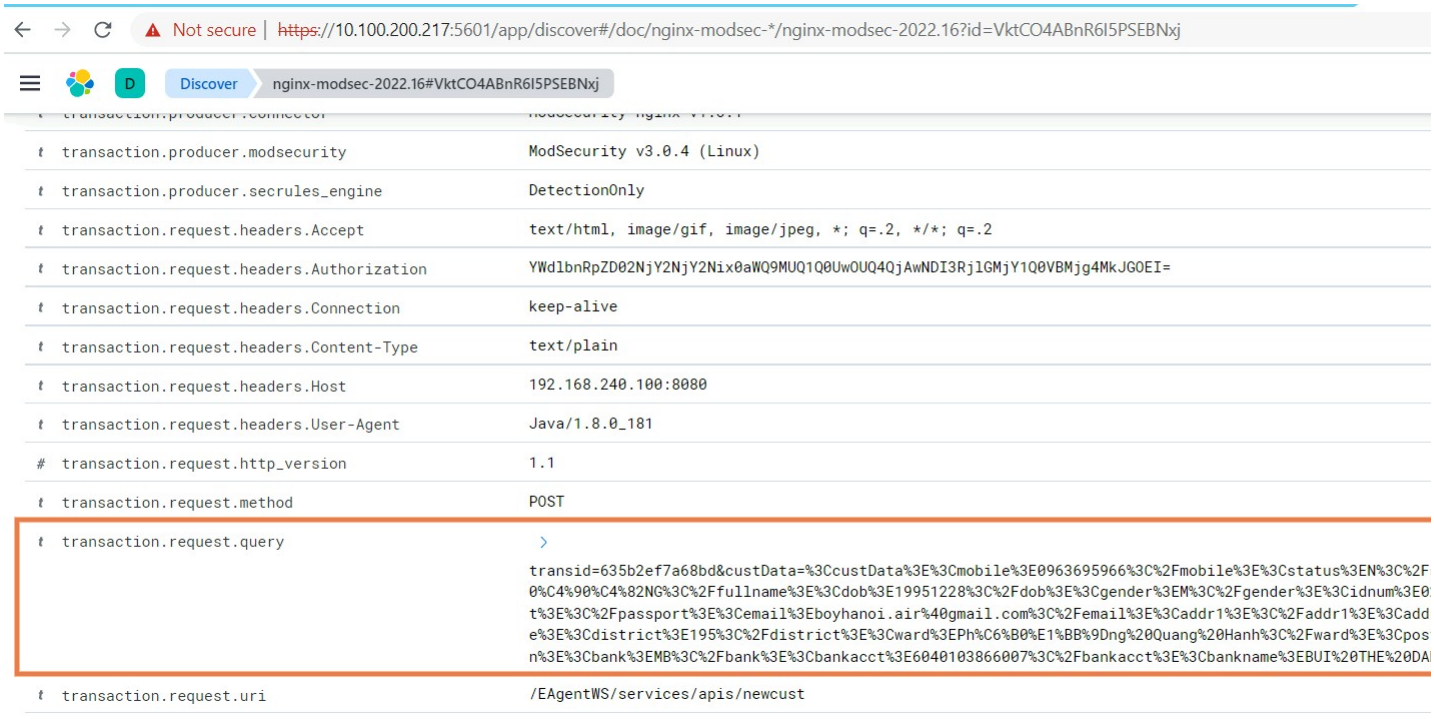
Cấu hình chỉnh sửa rule 941310: false positive

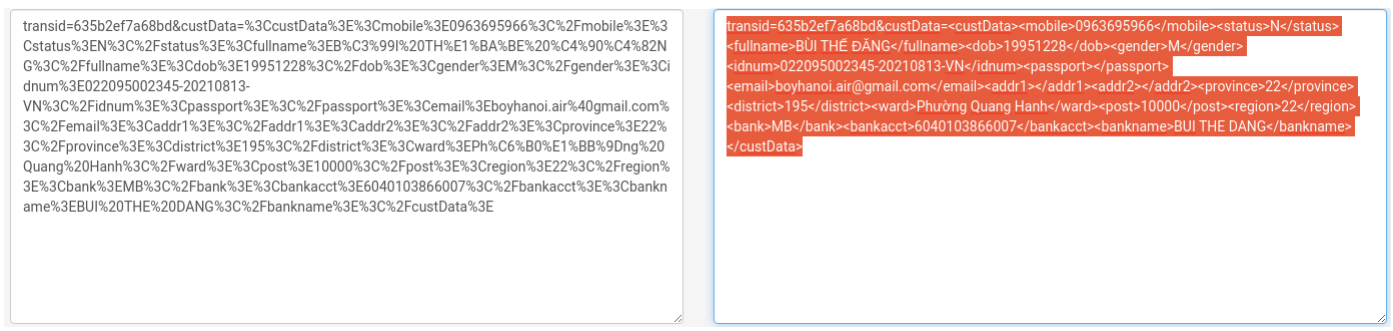
1. Tuning



1.1. Kiểm tra request.



1.2. Decode URL thành text để kiểm tra dấu hiệu tấn công XSS




```
transid=635b2ef7a68bd&custData=<custData><mobile>0963695966</mobile><status>N</status><fullname>BÙI THẾ ĐĂNG</fullname><dob>19951228</dob><gender>M</gender><idnum>022095002345-20210813-VN</idnum><passport></passpo
```

Sau khi kiểm tra kết luận Query an toàn không chưa ký tự dấu hiệu tấn công XSS => **False positive**

2. Fixing ### 2.1. Nguyên nhân Với rule XSS này vấn đề gây ra cảnh báo sai là do **Query**. Request có chứa các ký tự **UTF-8** trong XML data của **Query** cụ thể là `<fullname>BÙI THẾ ĐĂNG</fullname>` , trong rule phát hiện XSS áp dụng với US-ASCII khi thực hiện match sẽ có những ký tự đặc biệt được quy đổi thành " hoặc **>** dẫn đến cảnh báo kích hoạt sai.

2.2. Cấu hình chỉnh sửa rule

Tại thư mục lưu trữ rule: `rules/` Chỉnh sửa tại file : `REQUEST-941-APPLICATION-ATTACK-XSS.conf` Ở Rule id: **941310** - Trước khi sửa

```
SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm/|REQUEST_COOKIES_NAMES|ARGS_NAMES|ARGS|XML:/* "@rx \xbc[^\xbe>]*[\xbe>]|<[^\xbe]*\xbe" \
"id:941310,\
phase:2,\
block,\
capture,\
t:none,t:urlDecodeUni,t:lowercase,t:urlDecode,t:htmlEntityDecode,t:jsDecode,\
msg:'US-ASCII Malformed Encoding XSS Filter - Attack Detected',\
logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}',\
```

- Sau khi thêm `t:utf8toUnicode`

```
SecRule REQUEST_COOKIES|!REQUEST_COOKIES:/__utm/|REQUEST_COOKIES_NAMES|ARGS_NAMES|ARGS|XML:/* "@rx \xbc[^\xbe>]*[\xbe>]|<[^\xbe]*\xbe" \
  "id:941310,\
  phase:2,\
  block,\
  capture,\
  t:none,t:utf8toUnicode,t:urlDecodeUni,t:lowercase,t:urlDecode,t:htmlEntityDecode,t:jsDecode,\
  msg:'US-ASCII Malformed Encoding XSS Filter - Attack Detected',\
  logdata:'Matched Data: %{TX.0} found within %{MATCHED_VAR_NAME}: %{MATCHED_VAR}'"
```

Preferences

- github
- Modsec-NginX