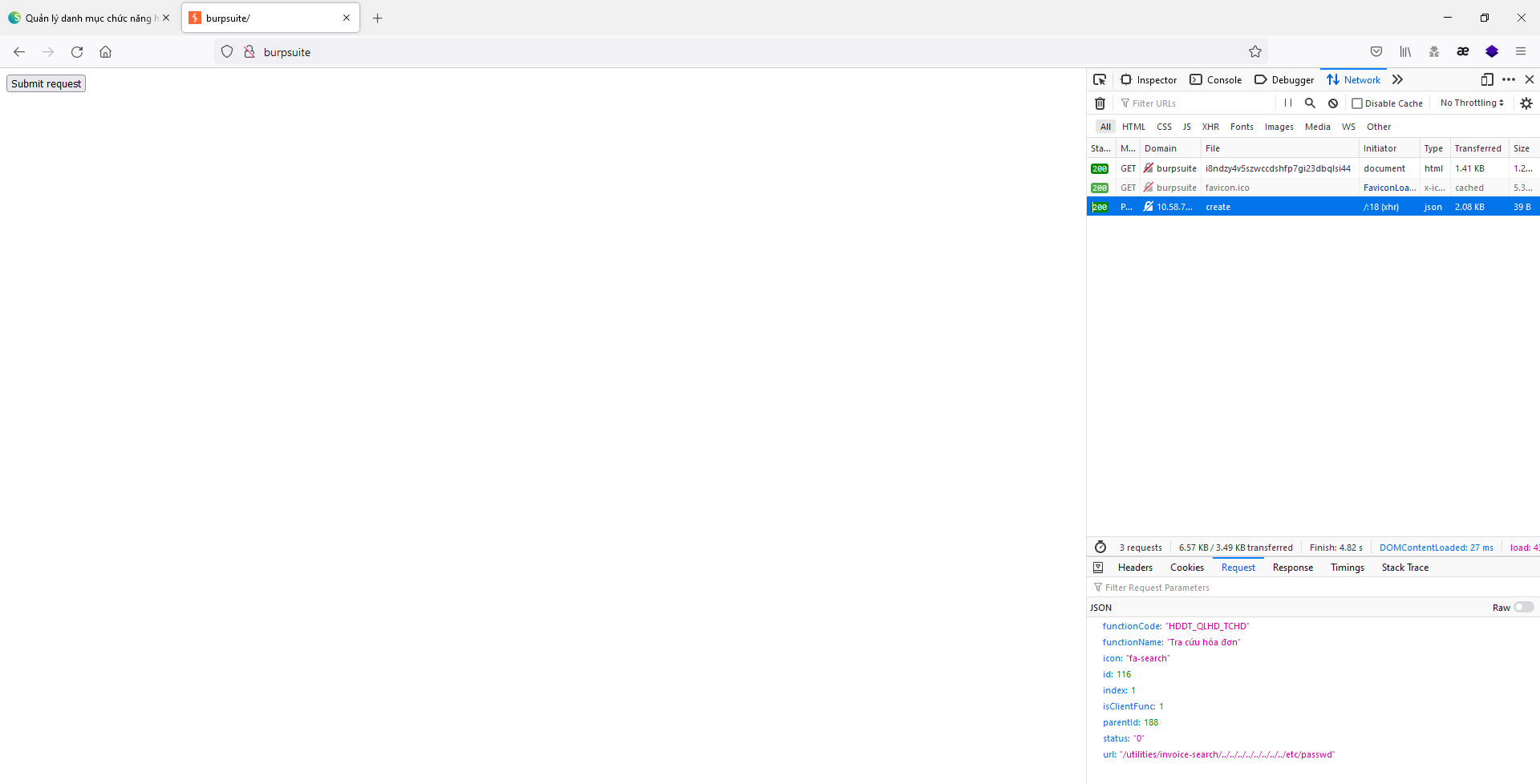
Report hóa đơn điện tử version 2.

* **Số lỗi: 2**
* **Mức độ: Cao**

1. Lỗi CSRF

* Mức độ: Cao
* Phạm vi ảnh hưởng:
  + - http://10.255.61.16/hddt2
    - http://10.255.61.16/hddt2-admin
  + Miêu tả lỗi: Sau khi người dùng đăng nhập vào ứng dụng, người dùng truy cập vào đường dẫn do kẻ tấn công cung cấp. Kẻ tấn công có thể thao tác, thay đổi thông tin trên trang của người dùng mà người dùng không hay biết.
  + Ảnh hưởng: Kẻ tấn công có thể thao tác như người dùng.
  + Cách fix: thêm csrf token vào mỗi bước submit của người dùng.
  + POC



1. Lỗi phân quyền.

* Mức độ: Cao.
* Phạm vi ảnh hưởng:
* /hddt2-admin/api/services/einvoiceadminapplication/api/tenant-branch/delete
* /hddt2-admin/api/services/einvoiceadminapplication/api/tenant-branch/update
* /hddt2-admin/api/services/einvoiceadminapplication/api/currency/create-currency
* /hddt2-admin/api/services/einvoiceadminapplication/api/app-params/update
* /hddt2-admin/api/services/einvoiceadminapplication/api/invoice-clusters
* Miêu tả lỗi: người dùng bình thường có thể thao tác được với quyền của admin.
* Ảnh hưởng: người dùng bình thường có thể thay đổi thông số trên trang của admin mà không bị ngăn chặn.
* Cách fix: phân quyền người dùng.
* PoC: