BÁO CÁO ĐÁNH GIÁ KIỂM THỬ XÂM NHẬP ỨNG DỤNG (PENETRATION TESTING)

ỨNG DỤNG: TÀI LIỆU ISO

CÔNG TY CỔ PHẦN CÔNG NGHỆ AN NINH MẠNG QUỐC GIA VIỆT NAM

VIETNAM NATIONAL CYBER SECURITY TECHNOLOGY CORPORATION

info@ncsgroup.vn ncsgroup.vn 024 8588 8000

ĐỘI THỰC HIỆN DỰ ÁN

Vũng Tàu, Ngày…. Tháng…. Năm 2025

Đại diện Công ty Cổ phần Công nghệ An ninh mạng Quốc gia Việt Nam	**Đại diện LD Việt – Nga Vietsovpetro – TTCNTT&LL**
Tên & Chức vụ:	***Tên & Chức vụ:***
Trần Phú Danh – Kỹ sư	***Lê Ngọc Tân – Kỹ sư***
Chữ ký:	***Chữ ký:***
……..	……

MỤC LỤC

1. Kết quả tổng quan 3

2. Phương pháp thực hiện 3

2.1. Phân loại 3

2.2. Đánh giá kiểm thử xâm nhập ứng dụng.....6

3. Thông tin ứng dụng 7

4. Kết quả đánh giá kiểm thử ứng dụng 8

4.1. Danh sách lỗ hổng bảo mật.....8

4.2. Kết quả đánh giá chi tiết 8

4.2.1. Lỗ hổng cho phép tải lên tệp tuỳ ý trong tính năng tạo tài liệu.....8

4.2.2. Lỗ hổng thiếu kiểm tra ràng buộc trong tính năng đăng nhập 13

4.2.3. Lỗ hổng sử dụng giao thức bảo mật lỗi thời TLS 1.0 17

5. Penetration Testing Check List.....19

1. Kết quả tổng quan

- Tên ứng dụng: Tài Liệu Iso
- Thời gian thực hiện: Từ ngày .../.../2025 đến ngày .../.../2025.
- Kết quả đánh giá tổng quan:

STT	Nội dung thực hiện	Kết quả
1	Kiểm tra quản lý cấu hình & triển khai	Đạt 8/8
2	Kiểm tra quản lý định danh	Đạt 5/5
3	Kiểm tra xác thực	Đạt 9/10
4	Kiểm tra phân quyền	Đạt 4/4
5	Kiểm tra quản lý phiên	Đạt 8/8
6	Kiểm tra sàng lọc dữ liệu đầu vào	Đạt 18/18
7	Kiểm tra cơ chế xử lý lỗi	Đạt 2/2
8	Kiểm tra thuật toán mã hóa	Đạt 2/3
9	Kiểm tra logic nghiệp vụ	Đạt 8/9
10	Kiểm tra xử lý phía người dùng	Đạt 12/12

2. Phương pháp thực hiện

2.1. Phân loại

Nhóm đánh giá xác định mức độ nghiêm trọng dựa trên thang điểm CVSS của từng lỗ hổng:

Với lỗ hổng bảo mật, cán bộ thực hiện tham chiếu theo CVSS Score V3 nhằm tính điểm để xác định mức độ của một lỗ hổng bảo mật. Các chỉ số đánh giá cơ bản được chia theo Exploitability metrics, Impact metrics và Scope.

STT	Hạng mục	Chỉ số	Mô tả
1	**Khả năng khai thác** (Exploitability metrics)	**Cách thức tấn công** (Attack Vector)	Bối cảnh có thể khai thác thành công lỗ hổng bảo mật, bao gồm 4 yếu tố đánh giá là Network, Adjacent, Local, Physical

STT	Hạng mục	Chỉ số	Mô tả
2		**Độ phức tạp trong tấn công** (Attack Complexity)	Độ phức tạp tấn công phụ thuộc vào các điều kiện cần có để khai thác lỗ hổng thành công. Độ phức tạp của tấn công sẽ được đánh giá theo 2 mức là Low và High
3		**Yêu cầu về đặc quyền** (Privileges Required)	Mức độ đặc quyền mà kẻ tấn công cần có để khai thác lỗ hổng thành công, bao gồm các mức None, Low (quyền user thường) và High (quyền user cao như admin, v.v…)
4		**Tương tác từ người dùng** (User Interaction)	Mô tả quá trình khai thác lỗ hổng thành công có cần sự tương tác của người dùng hay không, bao gồm các mức None và Required
5	**Mức độ ảnh hưởng** (Impact metrics)	**Ảnh hưởng đến tính bảo mật** (Confidentiality Impact)	Mức độ tác động đến tính bảo mật thông tin, bao gồm các mức None, Low, và High
6		**Ảnh hưởng đến tính toàn vẹn** (Integrity Impact)	Mức độ tác động đến tính toàn vẹn dữ liệu, bao gồm các mức None, Low, và High
7		**Ảnh hưởng đến tính sẵn sàng** (Availability Impact)	Mức độ tác động đến tính sẵn sàng, bao gồm các mức None, Low, và High
8	**Phạm vi** (Scope)	**Phạm vi** (Scope)	Việc khai thác lỗ hổng thành công có thể làm ảnh hưởng hay

STT	Hạng mục	Chỉ số	Mô tả
			thay đổi các tài nguyên/phạm vi khác hay không, bao gồm các mức Unchanged và Changed

Sau khi hoàn thành việc tính điểm, tùy vào số điểm sẽ được phân theo các mức độ sau:

STT	Mức độ	Điểm số	Mức độ rủi ro
1	Nghiêm trọng – Critical	9.0 đến 10.0	Các máy chủ tồn tại lỗ hổng nghiêm trọng, cho phép kẻ tấn công thực thi mã từ xa, chiếm quyền điều khiển máy chủ. Từ đó kẻ tấn công có thể thu thập dữ liệu, tài khoản, cài đặt mã độc hoặc làm bàn đạp để tấn công các máy chủ khác trong hệ thống.
2	Cao - High	7.0 đến 8.9	Các máy chủ tồn tại lỗ hổng mức cao, cho phép kẻ tấn công có thể truy cập vào tài nguyên và dữ liệu. Lấy cắp thông tin session hoặc dữ liệu nhạy cảm từ ứng dụng hoặc máy chủ. Kẻ tấn công không thể thực thi được mã hoặc câu lệnh trên máy chủ. Mức độ rủi ro sẽ thấp hơn so với khai thác lỗ hổng mức độ Nghiêm Trọng do cần thêm một số điều kiện trong quá trình khai thác.
3	Trung bình – Medium	4.0 đến 6.9	Các máy chủ tồn tại lỗ hổng mức trung bình, cho phép kẻ tấn công có thể truy cập thông tin nhạy cảm trên ứng dụng hoặc máy chủ do thiếu sót trong quá

STT	Mức độ	Điểm số	Mức độ rủi ro
			trình cấu hình ứng dụng. Khai thác lỗ hổng mức độ trung bình cần nhiều yêu cầu hơn ví dụ như quyền truy cập vào hệ thống bị ảnh hưởng
4	Thấp – Low	0.1 đến 3.9	Các máy chủ tồn tại lỗ hổng mức thấp bao gồm các lỗi liên quan đến rò rỉ thông tin, lỗi cấu hình hay thiếu một số biện phát. Cần kết hợp với các lỗ hổng hoặc kỹ thuật mức độ cao hơn để gây ảnh hưởng nghiêm trọng hơn tới hệ thống
5	Thông tin – Information	0.0	Các máy chủ tồn tại lỗ hổng mức thông tin cung cấp thông tin về ứng dụng hoặc máy chủ giúp kẻ tấn công có thêm thông tin về công nghệ, ứng dụng hoặc các thư viện được sử dụng trên máy chủ

Tham khảo các mô tả về các metric trong CVSS V3 tại:

https://first.org/cvss/v3.1/specification-document

Tham khảo trang web tính điểm online: **https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator**

2.2. Đánh giá kiểm thử xâm nhập ứng dụng

Thực hiện kiểm thử tấn công trên hệ thống ứng dụng với tư cách là một kẻ tấn công đến từ bên ngoài hoặc bên trong hệ thống để đánh giá mức độ xâm nhập vào hệ thống khi có quyền truy cập. Việc phát hiện và xác định tất cả các lỗ hổng bảo mật có thể tồn tại trong hệ thống ứng dụng, trong phạm vi cụ thể đã được định rõ, từ đó đánh giá mức độ rủi ro của các lỗ hổng này và tác động của chúng vào thời điểm tấn công để cung cấp

các phương án khắc phục, giảm thiểu rủi ro bị khai thác đối với các lỗ hổng, điểm yếu đã xác định.

Bằng các kỹ thuật nghiệp vụ và hỗ trợ bởi các công cụ, chúng tôi đánh giá sẽ phát hiện:

- Các lỗ hổng bảo mật xuất hiện trong ứng dụng do việc code không "sạch" hoặc logic hoạt động không đảm bảo tính an toàn.
- Các lỗ hổng bảo mật đã/chưa được công bố trên toàn cầu liên quan đến framework, thư viện hoặc các modules có thể ảnh hưởng đến ứng dụng.

Theo tiêu chuẩn thực hiện, các nhóm đánh giá bao gồm:

- Thu thập thông tin
- Kiểm tra Quản lý cấu hình & triển khai
- Kiểm tra Quản lý định danh
- Kiểm tra Xác thực
- Kiểm tra Phân quyền
- Kiểm tra Quản lý phiên
- Kiểm tra Sàng lọc dữ liệu đầu vào
- Kiểm tra Cơ chế xử lý lỗi
- Kiểm tra Thuật toán mã hóa
- Kiểm tra Logic nghiệp vụ
- Kiểm tra Xử lý phía người dùng

3. Thông tin ứng dụng

Tên hệ thống	Tài liệu ISO
Loại ứng dụng	Web Application
Link truy cập	https://iso.vietsov.com.vn
Đối tượng sử dụng	Nội bộ
Hình thức kiểm tra, đánh giá	BLACKBOX
Intranet/Internet	Intranet

4. Kết quả đánh giá kiểm thử ứng dụng

4.1. Danh sách lỗ hổng bảo mật

STT	Thông tin lỗ hổng	Mức độ ảnh hưởng	Khuyến nghị khắc phục
ID-001	Lỗ hổng cho phép tải lên tệp tuỳ ý trong tính năng tạo tài liệu	Trung bình	Có
ID-002	Lỗ hổng thiếu kiểm tra ràng buộc trong tính năng đăng nhập	Trung bình	Có
ID-003	Lỗ hổng sử dụng giao thức bảo mật lỗi thời TLS 1.0	Thấp	Có

4.2. Kết quả đánh giá chi tiết

4.2.1. Lỗ hổng cho phép tải lên tệp tuỳ ý trong tính năng tạo tài liệu

Tiêu đề	Thông tin
Nhóm lỗ hổng	Business Logic Testing
CVSS	CVSS Score: 6.5 | Medium
Đường dẫn bị ảnh hưởng	/Documents_ISO/Create /Documents_ISO/Edit
Mô tả	Chức năng chọn file tải nạp trong tính năng tạo tài liệu đã thực hiện giới hạn một số đuôi mở rộng của tệp tin được tải lên. Tuy nhiên vẫn còn cho phép tải lên tệp có đuôi html và svg, dẫn đến kẻ tấn công có thể chèn mã javascript độc hại vào trong 2 loại tệp này rồi gửi lên, khi trình duyệt xử lý hiển thị các tệp này sẽ thực thi mã độc.
Tham khảo	https%3A%2F%2Fowasp.org%2Fwww-community%2Fattacks%2Fxss%2F

Hậu quả

Thực thi javascript trên trình duyệt của người dùng khác có thể gây ra 1 số hậu quả như:

- Chiếm đoạt session của người dùng.

- Thay người dùng thực hiện các hành động tuỳ ý.
- Thay đổi các thông tin của người dùng.
- Chuyển hướng người dùng đến trang độc hại khác.

Bằng chứng tồn tại lỗi

Bước 1: Đăng nhập bằng tài khoản

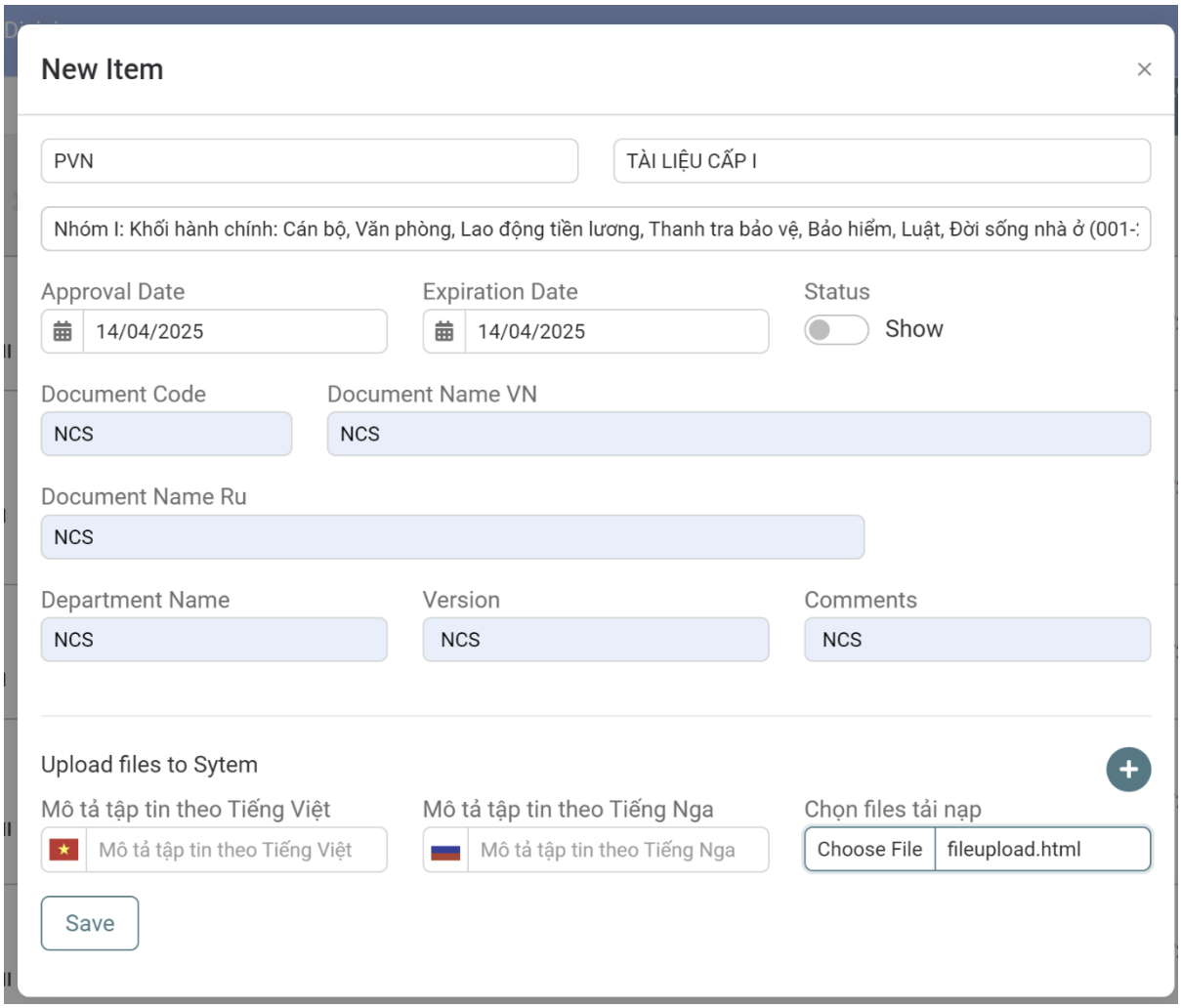
Username: admintest

Password: admin@123

Bước 2: Chọn chức năng tạo mới tài liệu.

Hình 4.2.1-1: Chọn chức năng tạo mới tài liệu

Bước 3: Nhập các thông tin yêu cầu để tạo mới và tải lên file html chứa payload khai thác



Hình 4.2.1-2: Nhập các thông tin cần thiết

Bước 4: Tiếp đó truy cập vào tài liệu mới tạo và chọn mở file đã tải lên

Hình 4.2.1-3: Payload XSS khai thác thành công

Request:

```
POST /Documents_ISO/Create HTTP/2
Host: iso.vietsov.com.vn
```

Cookie: .AspNetCore.Antiforgery.RQMJ5vY1_hU=CfDJ8Lrg-lDUd0xFrac9H_Zp5xp9wMklLM7eifKiKKuZIQaLP85O0ugXaW-gYfOIX80VajX9YA8EXSeZ5fQLreFAy-gedrINPMUHy1EV5CPYfjfLbp7IvpoN88pgS5SUe21sRht_0CyZ05eP_0srVkv_oIo; .AspNetCore.Culture=c%3Dvi%7Cuic%3Dvi; .AspNetCore.Identity.Application=CfDJ8Lrg-lDUd0xFrac9H_Zp5xpGg3hlxIhT2Vyo6ptBOY4szo0MM7D0Coy0JFEOkgfcmhzDAFNb8MYibWejma7ON5hTQyrVSB-Xoo17qoDn--jFA0B8Y6ZMtc8e65dpMQSNGxVMI2rLtTmc0iFkBNd9jMeXGVqpGlkEA6JKHDZp-bC_1l7ePwoRTVb70500R847SnSwsx-dLLqb3uMmR6doFwthnu3QWDc4QOLHLcOKTLb5xyVXuPDcndNHqx7Z2wKDMiQkKsJP65XDk02Tic5BxVL5tvFTd0JACJGBUgkSx620QWhVKVX6fl5Wf3aTx_QYQwrLtx6YLEhcDynfuJB2cRT9CcTvfHqr5PgGgveWRh7LHgnB0znyXcGc06PfZxc7QMW0P-yvS8NlQGIuKNNiwyHiV2eRA-eAoMuinbXoOhzCgZ1nSkb_vqBfOXx4IjOANWzRVJoMX25VI903zzA7T5awPPm38frj56cxCRM9f226yg7zrwuxmh174tKegv6FX3axyJY4rDkDcq7tqNR8Rey2ZHWNxehHTeUNXO-gc3Ntgq-J4YzD59_hNRwMtyA_y1eyu-MlXE6q9WNaVqBtTwTYuNNx5QnW2IVsPw9a06BCF_BmFnwhjh2k8UtUQHUJwNj59bWhacns-e5YxKdLLt1d1CiOCioxD_ptNhPRsLw7qDCAZnsYSb-Pz_9a73XmQ8iFJQBfZri4ILKLvtL_OtPdkzvK5bwNfxr8nBqpPoEcAxB7H1tIwVhF32h00ZoPChUCLMkQlwX8TMheeINey4s66lNTNzmbOvuKhGjg3NAYjRCEEIiPbitBjmOA4svhL5YmvMq-iMA4CySjy8n4O9EkoDftIBZ_mU08kKQBhBZomif3YDuewQ5jA3f2Cprz1H8hgN81lQWVFPXBL7mocRxITG9trkhnXxNXPnpFFWy-xc99z5PIYaL9svB81ZlZQSB5ymN0DHWR9lLbdgS781Vg65--H_zyO-bV4WNe_vUBcPn8DB-Eye1Vqn8Iv6UKBw

Content-Length: 2047

Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"

Accept-Language: en-US,en;q=0.9

Sec-Ch-Ua-Mobile: ?0

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36

Content-Type: multipart/form-data; boundary=----WebKitFormBoundarybNAAkpokHvNfAwJE

Accept: /

X-Requested-With: XMLHttpRequest

Sec-Ch-Ua-Platform: "Windows"

Origin: https://iso.vietsov.com.vn

Sec-Fetch-Site: same-origin

Sec-Fetch-Mode: cors

Sec-Fetch-Dest: empty

```
Referer: https://iso.vietsov.com.vn/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
------WebKitFormBoundarybNAAkpokHvNfAwJE
Content-Disposition: form-data; name="Divisions"
System.Collections.Generic.List`1[Microsoft.AspNetCore.Mvc.Rendering.SelectListItem]
------WebKitFormBoundarybNAAkpokHvNfAwJE
Content-Disposition: form-data; name="DivisionId"
19
------WebKitFormBoundarybNAAkpokHvNfAwJE
Content-Disposition: form-data; name="GroupsId"
1
------WebKitFormBoundarybNAAkpokHvNfAwJE
Content-Disposition: form-data; name="DocumentTypeId"
1
------WebKitFormBoundarybNAAkpokHvNfAwJE
```

Response:

```
HTTP/2 204 No Content
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=0
Date: Mon, 14 Apr 2025 09:31:07 GMT
```

Khuyến nghị:

- Sử dụng whitelist để giới hạn những đuôi tệp có thể được tải lên hệ thống, chỉ cho những loại tệp cần thiết tải lên và chặn tải lên những tệp có đuôi trùng với ngôn ngữ lập trình của trang web. Đối với ASP.NET thì những tệp không được phép tải lên là aspx, ashx, ..., và không cho phép tải lên những tệp có thể thực thi mã Javascript như html.
- Thực hiện đổi tên tệp khi đã tải lên bằng những ký tự random hoặc mã UUID, và không cho phép người dùng biết vị trí lưu tệp để tránh bị tận dụng để tải lên webshell.

4.2.2. Lỗ hổng thiếu kiểm tra ràng buộc trong tính năng đăng nhập

Tiêu đề	Thông tin
Nhóm lỗ hổng	Authentication Testing
CVSS	CVSS Score: 5.3 | Medium
Đường dẫn bị ảnh hưởng	/Account/Login
Mô tả	Ứng dụng không thực hiện giới hạn số lần thử đăng nhập không hợp lệ, cho phép kẻ tấn công thực hiện gửi hàng loạt yêu cầu đăng nhập với tên người dùng và mật khẩu khác nhau cho đến khi đoán đúng thông tin xác thực.
Tham khảo	https%3A%2F%2Fowasp.org%2Fwww-community%2Fattacks%2FBrute_force_attack

Hậu quả

Khi kẻ tấn công thực hiện khai thác thành công lỗ hổng sẽ có thể gây ra những hậu quả sau:

- Chiếm đoạt tài khoản người dùng, có thể cả tài khoản có quyền quản trị
- Truy cập trái phép vào các dữ liệu nội bộ, thực hiện các hành vi gây thiệt hại như chỉnh sửa, xóa dữ liệu.

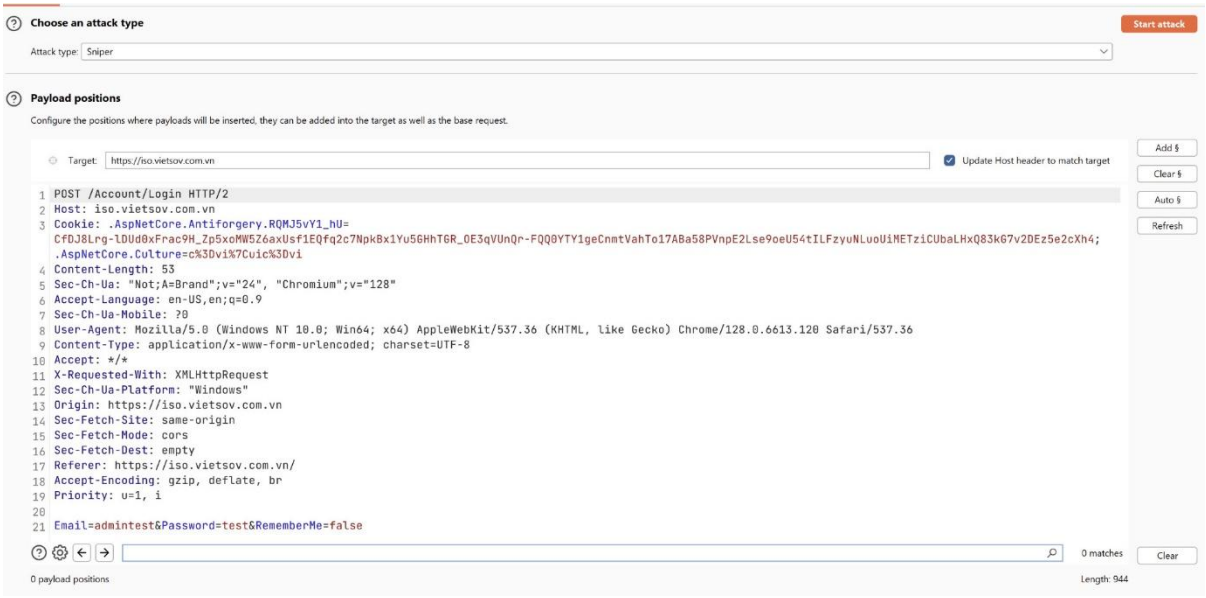
Bằng chứng tồn tại lỗi

Bước 1: Truy cập vào chức năng đăng nhập của ứng dụng và nhập tên người dùng đã biết, mật khẩu tuỳ ý, sau đó bấm nút đăng nhập

Username: adminTest

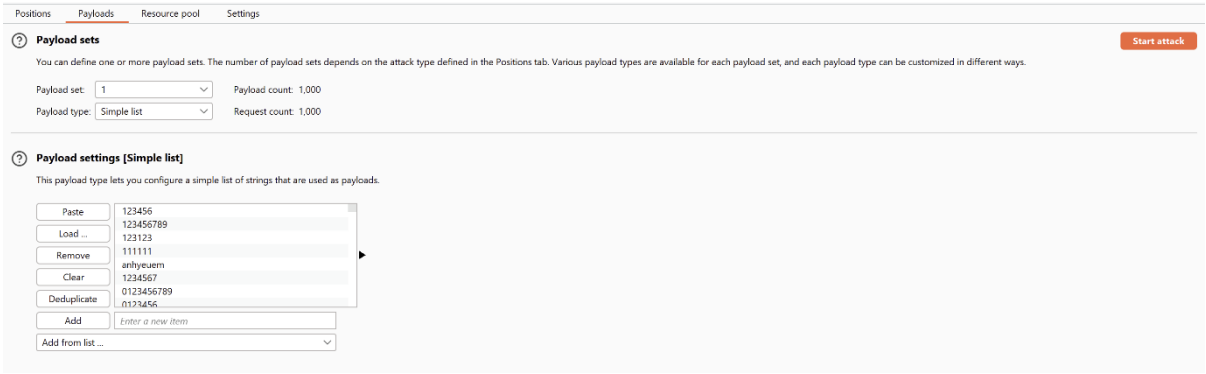
Password: test

Bước 2: Chặn request đăng nhập và gửi đến tab intruder của ứng dụng burpsuite



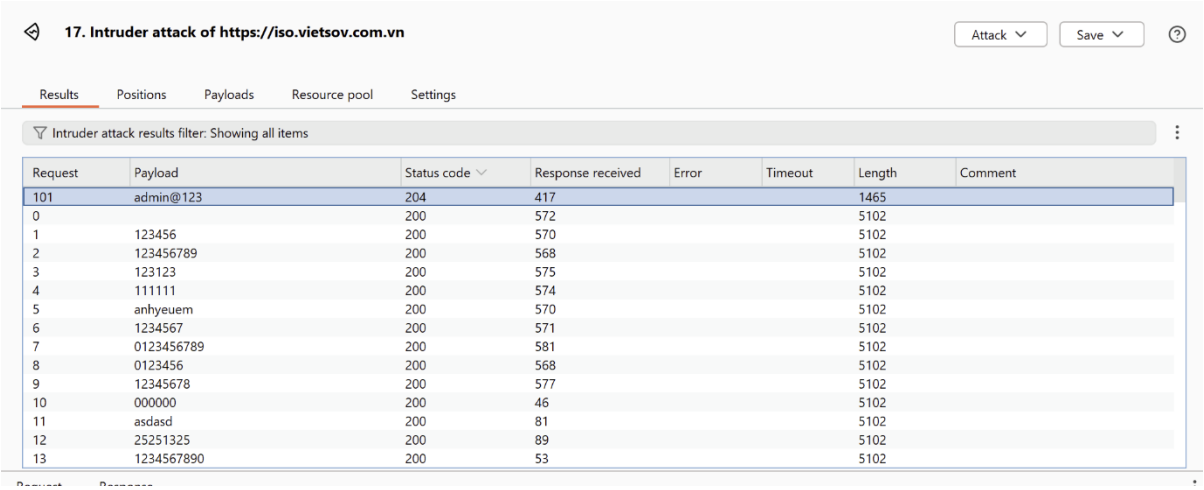
Hình 4.2.2-1: Request yêu cầu đăng nhập

Bước 3: Chọn biến mật khẩu là biến sẽ được thay thế, chuyển sang tab payload. Sau đó nhập danh sách mật khẩu vào mục payload settings



Hình 4.2.2-2: Nhập danh sách mật khẩu brute force

Bước 4: Bấm start attack, ứng dụng burpsuite sẽ tự động gửi yêu cầu đăng nhập với danh sách mật khẩu đã cung cấp. Nếu thông tin đăng nhập chính xác, response sẽ trả về status là 204.



Request	Payload	Status code	Response received	Error	Timeout	Length	Comment
101	admin@123	204	417			1465	
0		200	572			5102	
1	123456	200	570			5102	
2	123456789	200	568			5102	
3	123123	200	575			5102	
4	111111	200	574			5102	
5	anhyeuem	200	570			5102	
6	1234567	200	571			5102	
7	0123456789	200	581			5102	
8	0123456	200	568			5102	
9	12345678	200	577			5102	
10	000000	200	46			5102	
11	asdasd	200	81			5102	
12	25251325	200	89			5102	
13	1234567890	200	53			5102	

Hình 4.2.2-3: Danh sách yêu cầu đăng nhập tương ứng với mật khẩu

Request:

```
POST /Account/Login HTTP/2
Host: iso.vietsov.com.vn
Cookie: .AspNetCore.Antiforgery.RQMJ5vY1_hU=CfDJ8Lrg-lDUd0xFrac9H_Zp5xoMW5Z6axUsf1EQfq2c7NpkBx1Yu5GHhTGR_OE3qVUnQr-FQQ0YTY1geCnmtVahTo17ABa58PVnpE2Lse9oeU54tILFzyuNLuoUiMETziCUbaLHxQ83kG7v2DEz5e2cXh4; .AspNetCore.Culture=c%3Dvi%7Cuic%3Dvi
Content-Length: 51
Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
Accept-Language: en-US,en;q=0.9
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.6613.120 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Accept: /
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Platform: "Windows"
Origin: https://iso.vietsov.com.vn
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://iso.vietsov.com.vn/
Accept-Encoding: gzip, deflate, br
Priority: u=1, i
```

```
Connection: keep-alive
Email=admintest&Password=admin@123&RememberMe=false
```

Response:

```
HTTP/2 204 No Content
Cache-Control: no-cache,no-store
Pragma: no-cache
Expires: Thu, 01 Jan 1970 00:00:00 GMT
Server: Microsoft-IIS/10.0
Strict-Transport-Security: max-age=0
Set-Cookie: .AspNetCore.Identity.Application=CfDJ8Lrg-lDUd0xFrac9H_Zp5xqqJ0Ovz95-XJqFz6EGUV_8Aw9pwbfHhbBfKt6WKpB_8twcXAAHcDtmICnNSq583C1NGD8qq7D_DAqrTLPBlPrG9bmfW8AxKTUg57jylA4xy_td9SpdKYnzPp_gx1IgtMh80dPOErREnlS22fZVAZyh_0CTLuihNBtJFVFjIYFrIMcz9pVhNA80lrw15IfpgYItS-x-Ihtz4jyqmbZlAQNJPul7uEXtDvdV58xFOh0t-6UoZJkY5S_Swm4GTikhbOtY4W-2AyWOKyGEYjohtN0EXct75ZLEOXFGKWsIiPhgO5Evuu2-MMiCUEqhQfLpS9CjFEqtxC-CfvpILqB5xhHN6OSbxByqLNEPX5U1wrVLo6b_PUrdtxlfhMjngDJK6YilvWUDcRko-JZn80-yiQQgBp0Ohs07lYLyEajpSuuGNyujQuMjuYDZSHJ-ov2uE8pgXDHXzTWgwLCL81-vxKxZJDPaW-E3fOcj3IQxdNAlo9uDNKwBKjg_DCO27v5suLPNiolVAmHppQGfhCY9jdTFOi82icANui3psQyvksNOGK-6BVERwxgvc2AzS-A9iO4GlBYvfRAscBNrWd6oltoPAYtSAoq49disoVWuhSwh9kzcO3BE9ynCx16i279RynEX0sEkIAUvhWEOQrmuqX1MyVhqfzsddgl5sNdbLTsW1P5fEYqouTrYq4y5frhO2jixBdaW7FYvcmgr6bf4sMBOWrQv9zmz80RybA15FGN3eqCw6652u0qgWGCjHfXyKkq5NJsZheop1evKjf_7UN2Frm9mIOKd0nRQFN9LE43yDz7teeWLOKJLf6lsxxzyW6meFFgnaDaPzi1M5jz87szH_kZ0NUH58XNRK203Dow7tt6bAtgYYFfiYNTpZIm7aibck55JYc6Q1lTvJTugWnu2jSwf9WgbxxAMPBlzYIiXe8JY_XJXZu5Ug2V-yTlVwqTiVLXyM43llLmHnRll5J7BMXBNFcEIZj8iKn5RoRx1rOfFcSY_8ly-CthPIniwtWxvOeCj3PkKG3jaM7zCdBCdkn7FUarxYxNHbQNq8AIMsmXvwLUcHYg2_NfVoSVAI_TL1GHHDWfKzDE8FqCROQH0kg0qBKFow9-S1aJ7hwLNPg; path=/; secure; samesite=lax; httponly
Date: Sat, 19 Apr 2025 03:21:06 GMT
```

Khuyến nghị:

- Hệ thống nên triển khai cơ chế giới hạn số lần đăng nhập sai trong một khoảng thời gian ngắn (ví dụ: khóa tạm thời sau 5 lần sai liên tiếp trong 5 phút). Cơ chế này được cấu hình bằng thuộctính IdentityOptions có sẵn trong ASP.NET Core Identity

- Kết hợp cùng các kỹ thuật như xác minh CAPTCHA sau một số lần đăng nhập thất bại hoặc yêu cầu xác thực hai lớp (2FA) để tăng cường bảo mật. Việc xác thực CAPTCHA có thể được thực hiện thông qua phương thức .PostAsync trong thư viện reCAPTCHA của ASP.NET.

4.2.3. Lỗ hổng sử dụng giao thức bảo mật lỗi thời TLS 1.0

Tiêu đề	Thông tin
Nhóm lỗ hổng	Configuration and Deployment Management Testing
CVSS	CVSS Score: 3.7 | Low
Đường dẫn bị ảnh hưởng	Tất cả đường dẫn trong ứng dụng
Mô tả	Hệ thống hiện vẫn cho phép sử dụng giao thức TLS 1.0 – một giao thức mã hóa đã lỗi thời và không còn đảm bảo an toàn theo các tiêu chuẩn bảo mật hiện đại (như PCI-DSS, NIST, HIPAA,…). TLS 1.0 dễ bị khai thác bởi các cuộc tấn công như BEAST, Padding Oracle hoặc các downgrade attack.
Tham khảo	https%3A%2F%2Fcheatsheetseries.owasp.org%2Fcheatsheets%2FTransport_Layer_Security_Cheat_Sheet.html

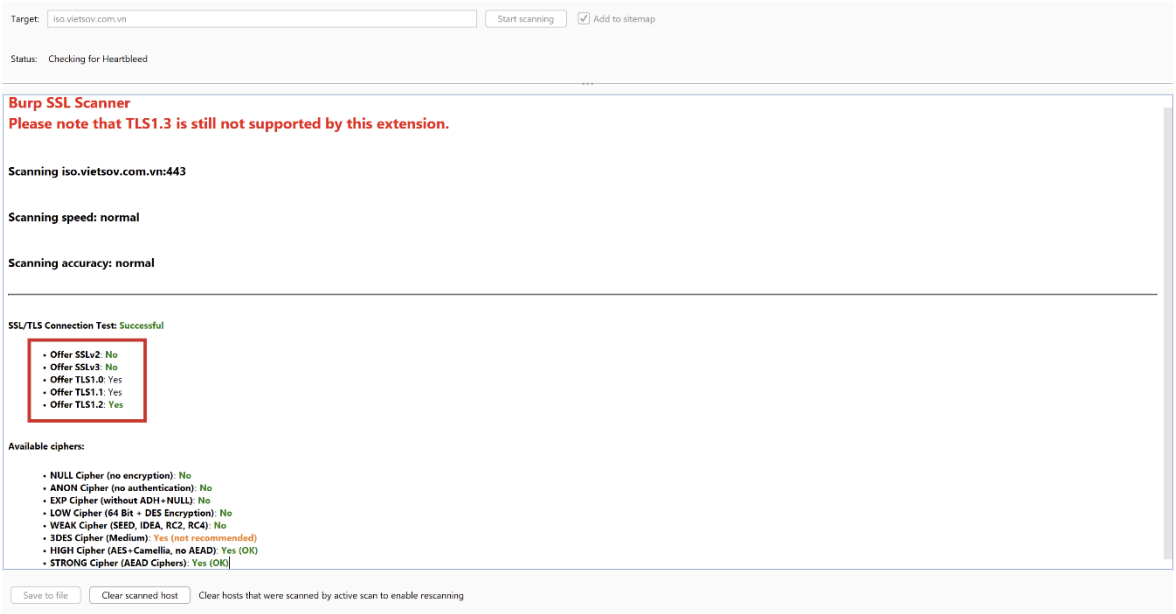
Hậu quả

Nếu kẻ tấn công thành công khai thác lỗ hổng sẽ có thể gây ra những hậu quả sau:

- Những thông tin truyền qua mạng có thể bị chặn, giải mã rồi chỉnh sửa dữ liệu do sử dụng thuật toán mã hóa yếu
- Ép chuyển client và server xuống phiên bản giao thức cũ kém an toàn như TLS 1.0, từ đó khai thác các lỗ hổng đã biết.

Bằng chứng tồn tại lỗi

Trong kết quả quét các giao thức hệ thống sử dụng, có kiểm tra ra hệ thống có hỗ trợ giao thức TLS1.0.



Hình 4.2.3-1: Thông tin các giao thức ứng dụng hỗ trợ

Khuyến nghị: Vô hiệu hóa hoàn toàn giao thức TLS 1.0 và 1.1 trên toàn bộ hệ thống, bao gồm: máy chủ web (Apache, Nginx, IIS), load balancer, API gateway, reverse proxy, và các dịch vụ khác có hỗ trợ SSL/TLS.

5. Penetration Testing Check List

STT	Test case đánh giá	Kết quả
1	**Kiểm tra quản lý cấu hình & triển khai**	
1.1	Kiểm thử Cấu hình Mạng/Hạ tầng	**Đạt**
1.2	Kiểm thử Cấu hình Nền tảng Ứng dụng	**Đạt**
1.3	Kiểm thử Xử lý Phần mở rộng Tệp tin đối với Thông tin Nhạy cảm	**Đạt**
1.4	Sao lưu và Tệp tin không được tham chiếu cho Thông tin Nhạy cảm	**Đạt**
1.5	Liệt kê Giao diện Quản trị Hạ tầng và Ứng dụng	**Đạt**
1.6	Kiểm thử Phương thức HTTP	**Đạt**
1.7	Kiểm thử HSTS	**Đạt**
1.8	Kiểm thử Chính sách vượt qua miền RIA	**Đạt**
2	**Kiểm tra quản lý định danh**	
2.1	Kiểm thử Định nghĩa Vai trò	**Đạt**
2.2	Kiểm thử Quy trình Đăng ký Người dùng	**Đạt**
2.3	Kiểm thử Quy trình Cấp tài khoản	**Đạt**
2.4	Kiểm thử Đối với Liệt kê Tài khoản và Tài khoản Người dùng dễ đoán được	**Đạt**
2.5	Kiểm thử Đối với Chính sách tên người dùng yếu hoặc không được áp dụng	**Đạt**
3	**Kiểm tra xác thực**	
3.1	Kiểm thử cho Việc Truyền tải Chứng thực qua Kênh được Mã hóa	**Đạt**
3.2	Kiểm thử cho Chứng thực Mặc định	**Đạt**

STT	Test case đánh giá	Kết quả
3.3	Kiểm thử cho Cơ chế Khóa yếu	**Không đạt**
3.4	Kiểm thử cho Việc Bỏ qua Phương thức Xác thực	**Đạt**
3.5	Kiểm thử Chức năng Ghi nhớ Mật khẩu	**Đạt**
3.6	Kiểm thử cho Yếu điểm của Bộ nhớ đệm Trình duyệt	**Đạt**
3.7	Kiểm thử cho Chính sách Mật khẩu yếu	**Đạt**
3.8	Kiểm thử cho Câu hỏi/Trả lời Bảo mật yếu	**Đạt**
3.9	Kiểm thử cho Chức năng Thay đổi hoặc Đặt lại Mật khẩu yếu	**Đạt**
3.10	Kiểm thử cho Xác thực yếu trong Kênh Thay thế	**Đạt**
4	**Kiểm tra phân quyền**	
4.1	Kiểm thử Traversal Thư mục/Chứng nhận Tệp tin	**Đạt**
4.2	Kiểm thử Việc Bỏ qua Phương thức Phân quyền	**Đạt**
4.3	Kiểm thử Nâng cao Quyền hạn	**Đạt**
4.4	Kiểm thử Các Tham chiếu Đối tượng Trực tiếp không An toàn	**Đạt**
5	**Kiểm tra quản lý phiên**	
5.1	Kiểm thử Bỏ qua Phương thức Quản lý Phiên	**Đạt**
5.2	Kiểm thử Thuộc tính Cookies	**Đạt**
5.3	Kiểm thử Session fixation	**Đạt**
5.4	Kiểm thử Session variable	**Đạt**
5.5	Kiểm thử CSRF	**Đạt**
5.6	Kiểm thử Chức năng Đăng xuất	**Đạt**
5.7	Kiểm thử Thời gian Chờ Phiên	**Đạt**

STT	Test case đánh giá	Kết quả
5.8	Kiểm thử Đối với Việc Làm rối Phiên	**Đạt**
6	**Kiểm tra sàng lọc dữ liệu đầu vào**	
6.1	Kiểm thử Reflected Cross Site Scripting	**Đạt**
6.2	Kiểm thử Stored Cross Site Scripting	**Đạt**
6.3	Kiểm thử HTTP Verb Tampering	**Đạt**
6.4	Kiểm thử HTTP Parameter pollution	**Đạt**
6.5	Kiểm thử SQL Injection	**Đạt**
6.6	Kiểm thử LDAP Injection	**Đạt**
6.7	Kiểm thử ORM Injection	**Đạt**
6.8	Kiểm thử XML Injection	**Đạt**
6.9	Kiểm thử SSI Injection	**Đạt**
6.10	Kiểm thử XPath Injection	**Đạt**
6.11	Kiểm thử IMAP/SMTP Injection	**Đạt**
6.12	Kiểm thử Code Injection	**Đạt**
6.13	Kiểm thử Local File Inclusion	**Đạt**
6.14	Kiểm thử Remote File Inclusion	**Đạt**
6.15	Kiểm thử Command Injection	**Đạt**
6.16	Kiểm thử Buffer overflow	**Đạt**
6.17	Kiểm thử incubated vulnerabilities	**Đạt**
6.18	Kiểm thử HTTP Splitting/Smuggling	**Đạt**
7	**Kiểm tra cơ chế xử lý lỗi**	
7.1	Phân tích Error Codes	**Đạt**
7.2	Phân tích Stack Traces	**Đạt**

STT	Test case đánh giá	Kết quả
8	**Kiểm tra thuật toán mã hóa**	
8.1	Kiểm thử cho Ciphers SSL/TSL Yếu, Bảo vệ Lớp Truyền không Đủ	**Không đạt**
8.2	Kiểm thử cho Padding Oracle	**Đạt**
8.3	Kiểm thử cho Thông tin Nhạy cảm được gửi qua các kênh không được mã hóa	**Đạt**
9	**Kiểm tra logic nghiệp vụ**	
9.1	Kiểm thử Logic Doanh nghiệp và Xác nhận Dữ liệu	**Đạt**
9.2	Kiểm thử Khả năng Làm giả yêu cầu	**Đạt**
9.3	Kiểm thử Kiểm tra Tính toàn vẹn	**Đạt**
9.4	Kiểm thử Thời gian Xử lý Quy trình	**Đạt**
9.5	Kiểm thử Giới hạn Số lần một Chức năng có thể Sử dụng	**Đạt**
9.6	Kiểm thử cho Việc Lách luật Quy trình công việc	**Đạt**
9.7	Kiểm thử Phòng thủ chống Sử dụng sai Ứng dụng	**Đạt**
9.8	Kiểm thử Tải lên các Loại Tệp tin không Được Mong đợi	**Không đạt**
9.9	Kiểm thử Tải lên các Tệp tin Độc hại	**Đạt**
10	**Kiểm tra xử lý phía người dùng**	
10.1	Kiểm thử DOM based Cross Site Scripting	**Đạt**
10.2	Kiểm thử JavaScript Execution	**Đạt**
10.3	Kiểm thử HTML Injection	**Đạt**
10.4	Kiểm thử Client-Side URL Redirect	**Đạt**
10.5	Kiểm thử CSS Injection	**Đạt**

STT	Test case đánh giá	Kết quả
10.6	Kiểm thử Client-Side Resource Manipulation	**Đạt**
10.7	Kiểm thử Cross Origin Resource Sharing	**Đạt**
10.8	Kiểm thử Cross Site Flashing	**Đạt**
10.9	Kiểm thử Clickjacking	**Đạt**
10.10	Kiểm thử Web Sockets	**Đạt**
10.11	Kiểm thử Web Messaging	**Đạt**
10.12	Kiểm thử lưu trữ cục bộ	**Đạt**