Owasp Zap test security cho Web Application và API

[Bùi Thị Yến updated 2 days ago](https://docs.lumi.vn/doc/94-owasp-zap-test-security-cho-web-application-va-api-UKVwWNLRTm/history)  • [Comment](https://docs.lumi.vn/doc/94-owasp-zap-test-security-cho-web-application-va-api-UKVwWNLRTm) • [Viewed by 8 people](https://docs.lumi.vn/doc/94-owasp-zap-test-security-cho-web-application-va-api-UKVwWNLRTm/insights)

**Owasp Zap – The Open Web Application Security Project** được hiểu là dự án mở về bảo mật ứng dụng web. **Owasp Zap** bao gồm các tính năng miễn phí và trả phí như:

* Là mã nguồn mở.
* Các công cụ đạt chuẩn về an toàn thông tin
* Thực hiện chính sách kiểm tra về bảo mật, an toàn cho mã nguồn
* Sử dụng hoàn toàn miễn phí.
* Ứng dụng đa nền tảng.
* Dễ dàng cài đặt và sử dụng.
* Cho phép triển khai sử dụng nhiều ngôn ngữ.
* Quét tự động
* Tự động cập nhật nhiều tính năng cho người dùng
* Là công cụ được nhiều người dùng tham gia sử dụng, tạo thành một cộng đồng nhiều thành viên.
* Được phát triển bởi các chuyên gia lập trình chuyên nghiệp.

**Ngoài ra, Owasp Zap cũng đưa ra 10 rủi ro mà bạn có thể gặp phải**

* Khả năng bị tiêm nhiễm mã độc. (**Lỗ hổng SQL Injection)**
* Tính sai lầm trong việc kiểm tra định danh cũng như các phiên làm việc. (**Broken Authentication)**
* Thực thi mã Scrip xấu. **(Cross Site Scripting)**
* Đối tượng tham chiếu không được an toàn tuyệt đối. (**Insecure Direct Object References)**
* Cấu hình an ninh có thể bị sai. (**Security Misconfiguration)**
* Có thể bị lộ cấu hình nhạy cảm. (**Sensitive data exposure)**
* Đôi khi còn bị mất kiểm soát mức độ truy cập chức năng. (**Missing function level access control (lỗi phân quyền))**
* Giả mạo yêu cầu. (**Cross Site Request Forgery (CSRF))**
* Bị tấn công khi sử dụng các thành phần với những lỗ hổng bảo mật. (**Using component with known vulnerabilities)**
* Chuyển hướng không an toàn. (**Unvalidated redirects and forwards)**

**Tổng hợp các công cụ quét lỗ hổng website tốt nhất**

* [Nessus-professional](https://www.tenable.com/products/nessus/nessus-professional)
* [Cystack Scan](https://web.cystack.net/) (miễn phí)
* [Burp Suite](https://portswigger.net/burp) (miễn phí/ trả phí)
* NeXpose Express/Pro/Enterprise ($2,000 – 25,000/năm)
* Net Sparker ($4,995++/website/năm)
* Accunetix ($4495++/5 website/năm)
* OpenVAS (Không công bố giá)
* [Wireshark](https://www.wireshark.org/download.html) (miễn phí)

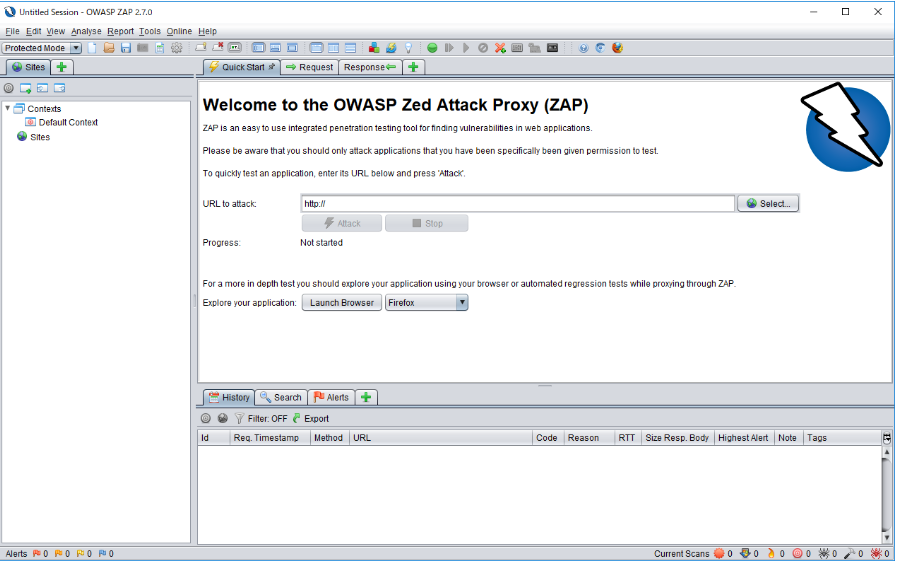
#1. Điều kiện

**Owasp Zap** chạy bằng Java chính vì vậy ta cần phải cài đặt JRE. Nếu bạn chưa cài JRE thì có thể vào [Web Site Oracle](https://docs.oracle.com/goldengate/1212/gg-winux/GDRAD/java.htm#BGBFHBEA) download và cài đặt.

#**2. Download cài đặt**

Bạn có thể download cài đặt [Owasp Zap](https://www.zaproxy.org/download/) phiên bản mới nhất ứng với môi trường làm việc của bạn

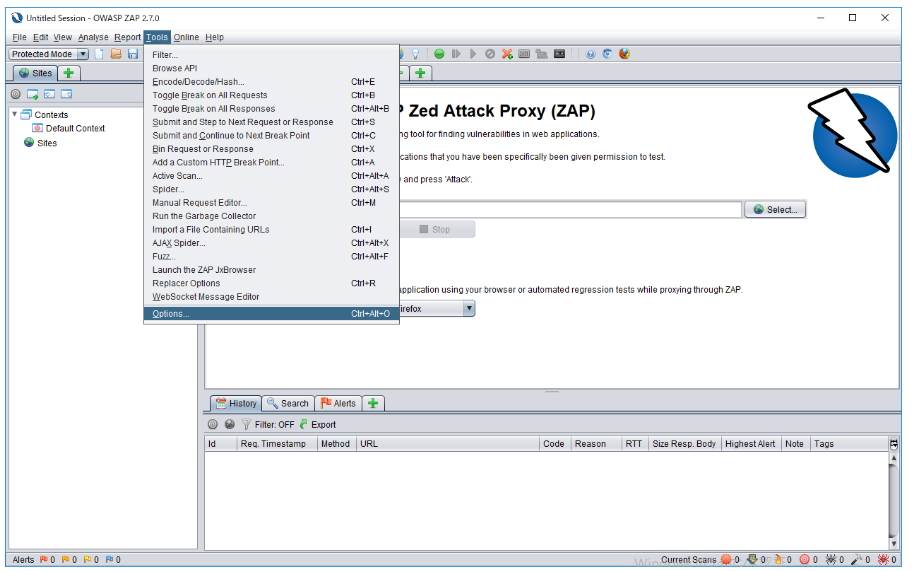
Download và cài đặt như một ứng dụng bình thường. Sau khi cài đặt xong ta khởi động ứng dụng và sẽ có giao diện sau



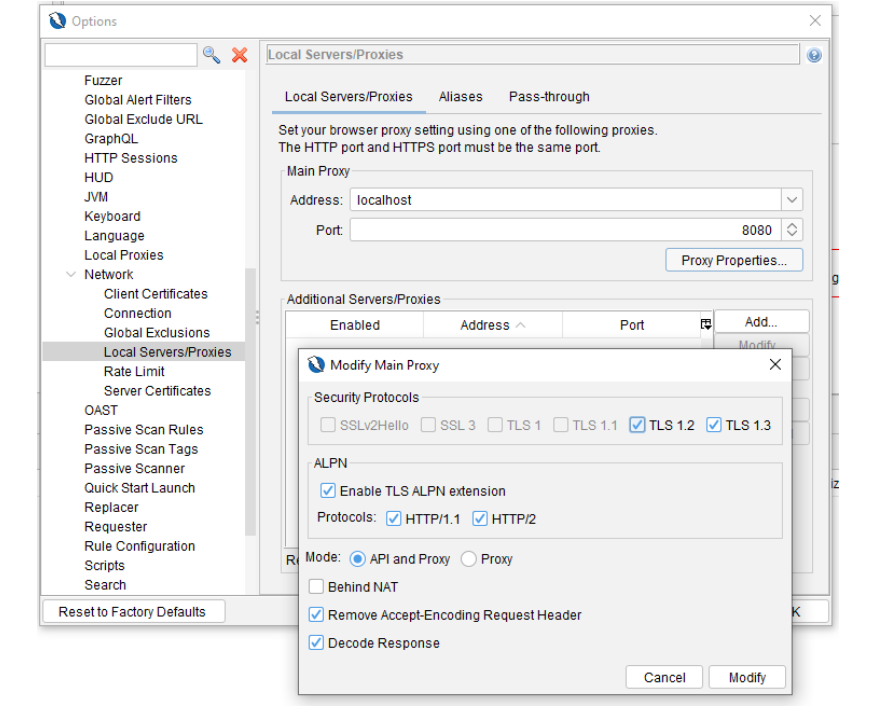
#### #**Thiết lập**

#### #**Thiết lập bên phía Owasp Zap**

OWASP ZAP có chức năng proxy cục bộ, cho phép OWASP ZAP hoạt động như một proxy cục bộ.

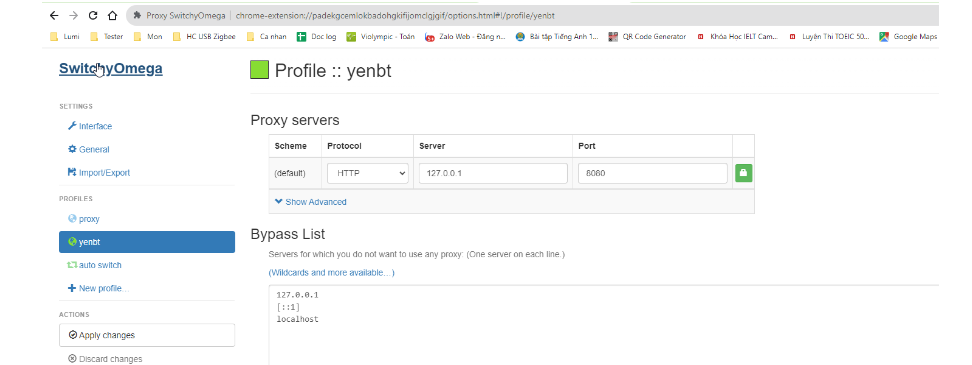


Chọn Tools -> Options, thiết lập Address và Port . Mặc đinh sẽ là localhost:8080. Trường hợp mà có ứng dụng nào khác đã chiếm dụng port 8080 thì ta có thể đổi 1 port khác tùy ý, rồi nhấn OK để lưu thiết lập.

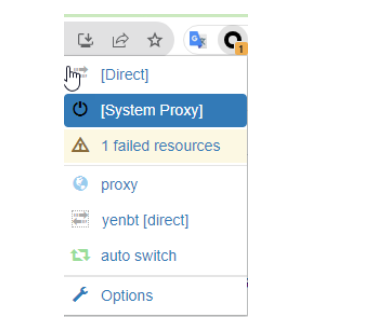


#### #**Thiết lập bên phía Browser (Chorme/Firefox**)

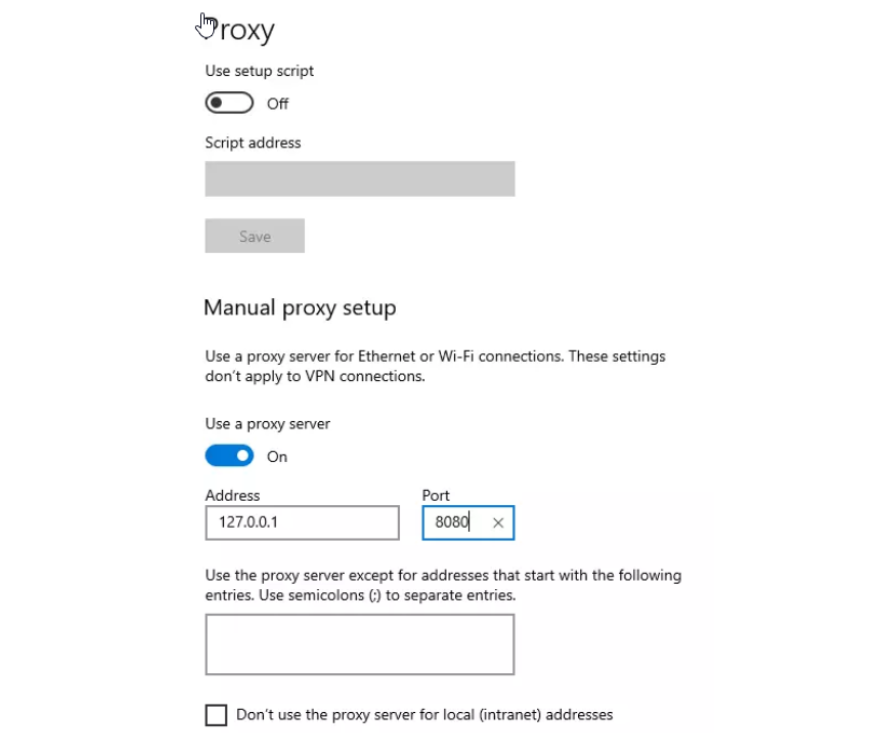
Thiết lập với Google Chorme, mục đích là để mình sử dụng được Add-on Postman của Google chorme để test API. Việc cần làm là bạn cài Add-on SwitchyOmega. Add-on này sẽ giúp bạn ON OFF việc chuyển đổi proxy 1 cách dễ dàng.



Bạn chọn New profile và điền những thông tin cần thiết , chú ý là chỗ Proxy servers bạn phải thiết lập cùng Address và cùng Port đã được thiết lập ở phía Owasp Zap. Thiết lập này sẽ giúp cho Owasp Zap bắt được những truy cập mà bạn đang truy cập phía Browser.



Sau khi thiết lập xong , nút Apply changes sẽ sáng lên, click vào để lưu thiết lập. Khi thiết lập xong Proxy cho Google – Browser rồi đó, nhìn sang góc bên phải sẽ thấy có 1 icon hình tròn hiện lên. Chọn profile bạn vừa thiết lập, để ON và click vào System Proxy để vô hiệu hóa thiết lập.



**#3. Phương pháp đánh giá rủi ro OWASP**

Phương pháp đánh giá rủi ro OWASP (Open Web Application Security Project) dựa trên các phương pháp tiêu chuẩn và được tùy chỉnh để đảm bảo tính bảo mật ứng dụng. Tiêu chuẩn xác định rủi ro như sau:

NoneBashCSSCC#ElixirErlangGoGraphQLGroovyHaskellHCLHTMLINIJavaJavaScriptJSONJSXKotlinLispLuaMermaid DiagramNixObjective-COCamlPerlPHPPowershellPythonRubyRustScalaSQLSoliditySwiftTOMLTSXTypeScriptVisual BasicYAMLZigCopy

\*\*Risk = Likelihood \\* Impact\*\*

Trong đó các yếu tố:

* Risk: Mức độ rủi ro
* Likelihood: Khả năng
* Impact: Tác động

Các bước đánh giá rủi ro được thực hiện như sau:

**Bước** **1: Xác định rủi ro**

* Xác định rủi ro cần được đánh giá. Khi đó cần thu thập đẩy đủ các thông tin như: Tác nhân, cuộc tấn công, lỗ hổng và tác động đối với đơn vị, tổ chức. Có thể có nhiều tác động và nhiều nhóm tấn công.

**Bước** **2: Ước tính khả năng dựa trên các yếu tố**

* Khi đã xác định các rủi ro tiềm ần của hệ thống, người thực hiện đánh giá cần xác định mức độ nghiệm trọng thì đầu tiên xác định khả năng xảy ra. Đây được xác định là thước đo về khả năng lỗ hổng sẽ bị phát hiện và kể tấn công có thể khai thác. Có thể chưa cần quá chính xác trong việc ước tính như trên, chỉ cần xác định mức khả năng: Thấp, trung bình, cao.
* Các yếu tố có thể dùng cho việc xác định khả năng.
* Có một số yếu tố có thể giúp xác định khả năng. Mỗi yếu tố có một bộ tùy chọn và mỗi tùy chọn được đánh số khả năng từ 0 đến 9.
* T**ác nhân đe dọa:** Yếu đố liên quan tác nhân đe dọa. Có thể ước tính khả năng tấn công thành công của nhóm tác nhân này.
* **Cấp độ kỹ năng**: Kỹ năng của nhóm tác nhân đe dọa này được xác đinh như nào?
  + 1: Không có kỹ năng
  + 3: Có một số kỹ năng
  + 5: Người dùng máy tính có kỹ năng nâng cao
  + 6: Có kỹ năng lập trình và mạng
  + 9: Có kỹ năng bảo mật xâm nhập
* **Động cơ, lý do phạm tội:** Động cơ của nhóm tác nhân đe dọa này tìm và khai thác lỗ hổng như nào?
  + 1: Phần thưởng thấp hoặc không có phần thưởng.
  + 4: Có giải thưởng.
  + 9: Giải thưởng cao.
* **Cơ hội:** Cơ hội nào cần thiết cho nhóm tác nhân đe dọa để khai thác lỗ hổng?
  + 0: Truy cập đầy đủ hoặc tài nguyên giá trị.
  + 4: Yêu cầu truy cập đặc biệt hoặc tài nguyên.
  + 7: Một số quyền truy cập hoặc tài nguyên cần thiết.
  + 9: Không cần truy cập hoặc tài nguyên cần thiết.
* **Kích thước:** Quy mô nhóm các tác nhân đe dọa này như nào?
  + 2: Nhà phát triển.
  + 2: Quản trị hệ thống.
  + 4: Người dùng nội bộ.
  + 5: Đối tác.
  + 6: Người dùng được xác thực.
  + 9: Người dùng ẩn danh.
* **Yếu tố dễ bị tổn thương:** Các yếu tố tiếp theo có liên quan đến lỗ hổng. Mục tiêu là ước tính khả năng của lỗ hổng, đặc biệt là liên quan đến việc phát hiện và khai thác lỗ hổng.
* **Dễ khám phá**: Làm thế nào nhóm các tác nhân đe dọa này có thể dễ dàng để khai thác lỗ hổng?
  + 1: Không thể.
  + 3: Khó.
  + 7: Dễ.
  + 9: Công cụ có sẵn.
* **Dễ khai thác:** Làm thế nào cho nhóm các tác nhân đe dọa dễ dàng khai thác lỗ hổng này?
  + 1: Lý thuyết.
  + 3: Khó.
  + 5: Dễ.
  + 9: Công cụ tự động có sẵn.
* **Nhận thức**: Làm thế nào cho nhóm tác nhân đe dọa này là lỗ hổng?
  + 1: Không biết.
  + 4: Ẩn.
  + 6: Hiển nhiên.
  + 9: Kiến thức công cộng.
* **Phát hiện xâm nhập:** Làm thế nào là một khai thác có thể được phát hiện?
  + 1: Phát hiện hoạt động trong ứng dụng.
  + 3: Ghi nhật ký và đánh giá.
  + 8: Ghi nhật ký mà không xem xét.
  + 9: Không đăng nhập.

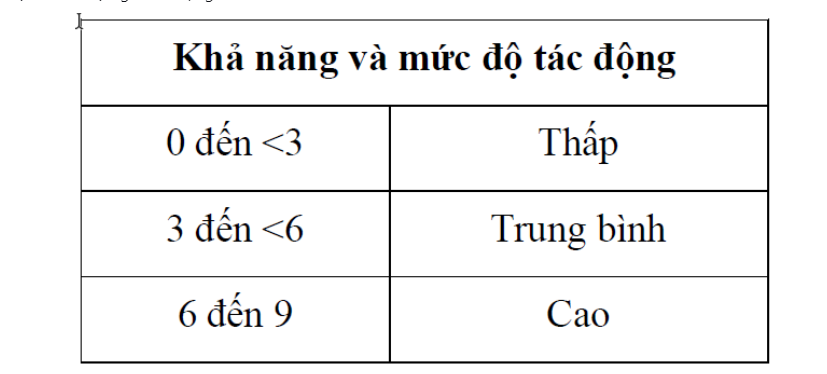
**Bước 3: Các yếu tố để ước tính tác động**

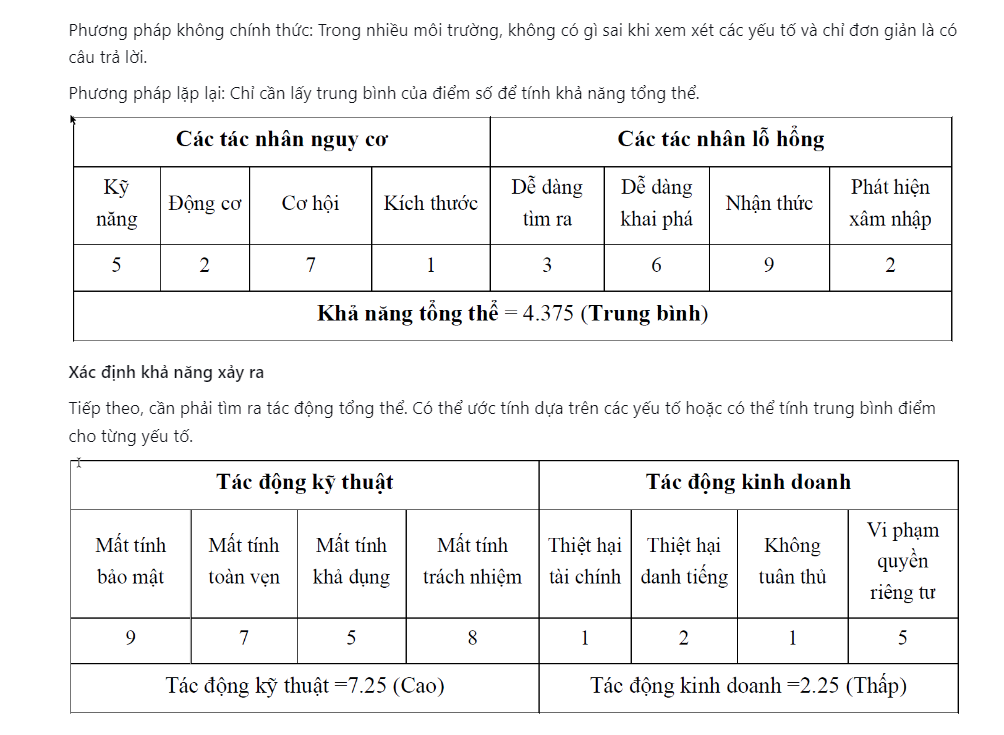
* Khi đánh giá tác động của một cuộc tấn công, cần xem xet hai loại tác động: Đầu tiên là "tác động kỹ thuật" đối với ứng dụng, dữ liệu được sử dụng và các chức năng mà đượccung cấp. Tiếp theo là "tác động nghiệp vụ" đối với đơn vị, cơ quan tổ chức vận hành ứng dụng. Trong đó, tác động nghiệp vụ là quan trọng hơn.
* Mỗi yếu tố có một tập hợp các tùy chọn và mỗi tùy chọn có xếp hạng tác động từ 0 đến 9.
* **Yếu tố tác động kỹ thuật**: Các yêu tố liên quan tác động kỹ thuật được chia ra thành: Mất tính bảo mật: Bao nhiêu dữ liệu đã bị tiết lộ và mức độ nhạy cảm?
  + 2: Dữ liệu không nhạy cảm.
  + 4: Dữ liệu quan trọng tối thiểu.
  + 6: Dữ liệu không nhạy cảm bị lộ rộng rãi.
  + 7: Dữ liệu quan trọng bi lộ.
  + 9: Tất cả dữ liệu được tiết lộ.
* **Mất tính toàn vẹn:** Bao nhiêu dữ liệu có thể bị hỏng và nó bị hư hại như thế nào?
  + 1: Dữ liệu bị hỏng nhẹ tối thiểu.
  + 3: Dữ liệu bị hỏng nghiêm trọng tối thiểu
  + 5: Dữ liệu bị hỏng nhẹ.
  + 7: Dữ liệu bị hỏng nghiêm trọng.
  + 9: Dữ liệu bị hỏng hoàn toàn.
* **Mất tính khả dụng:** Bao nhiêu dịch vụ có thể bị mất và mức độ quan trọng như thế nào?
  + 1: Các dịch vụ thứ cấp tối thiểu bị gián đoạn.
  + 5: Các dịch vụ chính tối thiểu bị gián đoạn.
  + 5: Các dịch vụ thứ cấp mở rộng bị gián đoạn.
  + 7: Các dịch vụ chính mở rộng bị gián đoạn.
  + 9: Tất cả các dịch vụ bị mất hoàn toàn.
* **Mất trách nhiệm:** Là hành động của các tác nhân đe dọa có thể ảnh hưởng đối với một cá nhân?
  + 1: Hoàn toàn có thể theo dõi.
  + 7: Có thể theo dõi.
  + 9: Hoàn toàn ẩn danh.
* **Yếu tố tác động kinh doanh:** Tác động này bắt nguồn từ tác động kỹ thuật, nhưng đòi hỏi sự hiểu biết về những gì là quan trọng đối với đơn vị. Rủi ro kinh doanh là những gì biện minh cho đầu tư trong việc khắc phục các vấn đề bảo mật.
* **Thiệt hại tài chính:** Thiệt hại tài chính là bao nhiêu từ hậu quả của một khả năng khai thác?1: Ít hơn chi phí để khắc phục lỗ hổng.
  + 3: Ảnh hưởng nhỏ đến lợi nhuận hàng năm.
  + 7: Ảnh hưởng đáng kể đến lợi nhuận hàng năm.
  + 9: Phá sản.
* **Thiệt hại danh tiếng:** Một khả năng khai thác dẫn đến thiệt hại danh tiếng gây tổn hại cho doanh nghiệp như thế nào?
  + 1: Thiệt hại tối thiểu.
  + 4: Mất tài khoản lớn.
  + 5: Mất thiện chí.
  + 9: Thiệt hại thương hiệu.
* **Không tuân thủ:** Không tuân thủ sẽ gây ra vi phạm nào?
  + 2: Vi phạm nhỏ.
  + 5: Vi phạm rõ ràng.
  + 7: Vi phạm hồ sơ cao
* **Vi phạm quyền riêng tư:** Bao nhiêu thông tin cá nhân bị tiết lộ?
  + 3: Một cá nhân.
  + 5: Hàng trăm người.
  + 7: Hàng nghìn người.
  + 9: Hàng triệu người.

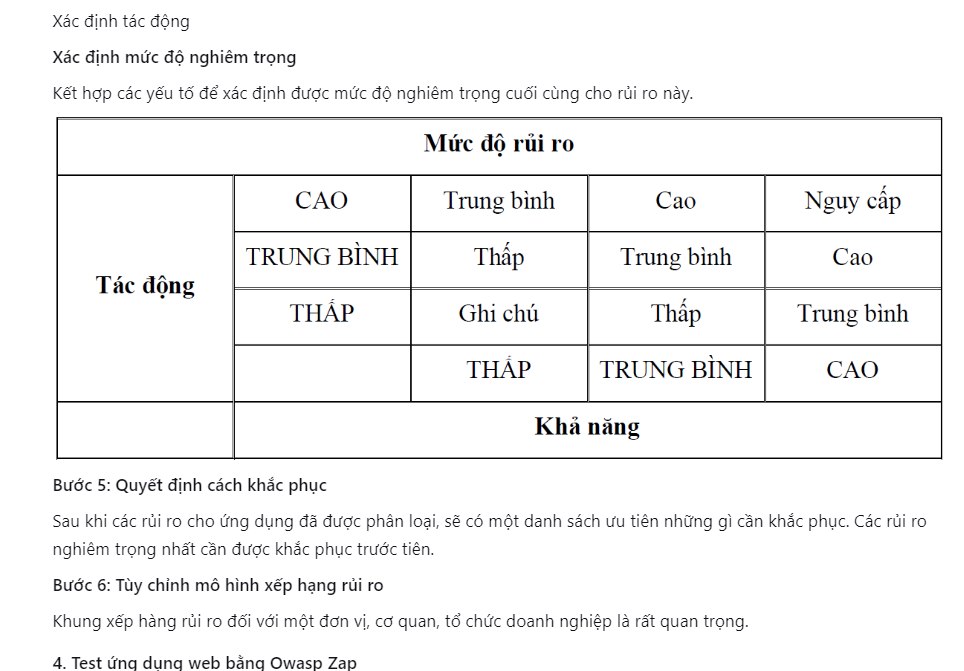
**Bước 4: Xác định mức độ nghiêm trọng**

Trong bước này, ước tính khả năng và mức độ tác động được kết hợp để tính toán mức độ nghiêm trọng chung cho rủi ro này.

Xác định mức độ nghiêm trọng của rủi ro

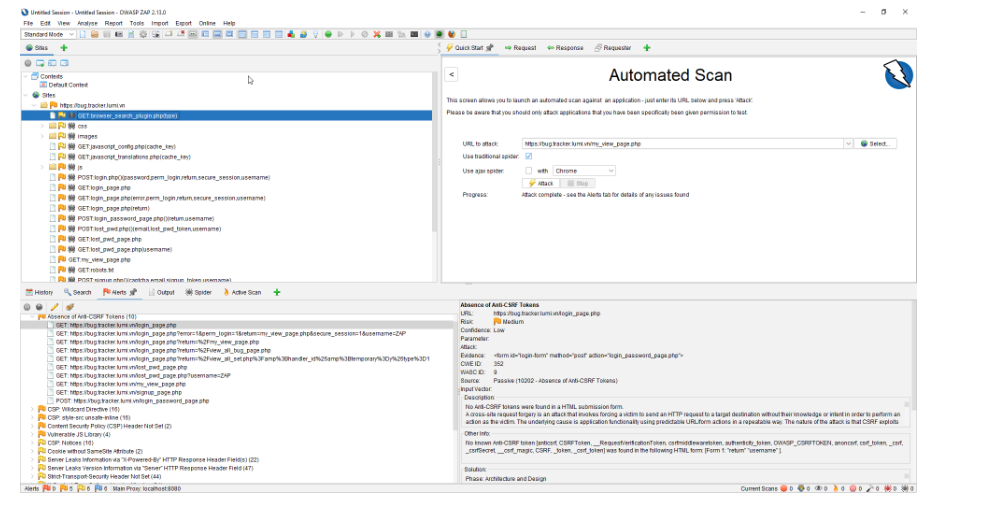






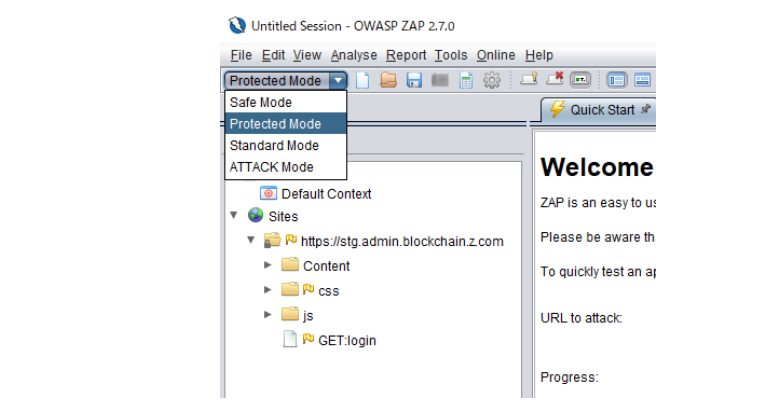
### #Test ứng dụng web bằng Owasp Zap

Sau khi thiết lập xong Proxy cho Owasp Zap và Browser, bạn có thể test những gì đã thiết lập bằng cách truy cập vào ứng dụng web bạn đang phát triển để test với các môi trường local, staging hay production.



Nếu thiết lập đúng, Owaps Zap sẽ hiện ra URL của trang web mà bạn vừa truy cập. Nếu như những bước thiết lập trước của chúng ta không sai, hãy chuyển tiếp sang phần Protected Mode.

#### #**4.1. Thiết lập protected Mode:** Owaps Zap hiện tại có 4 chế độ quét khác nhau



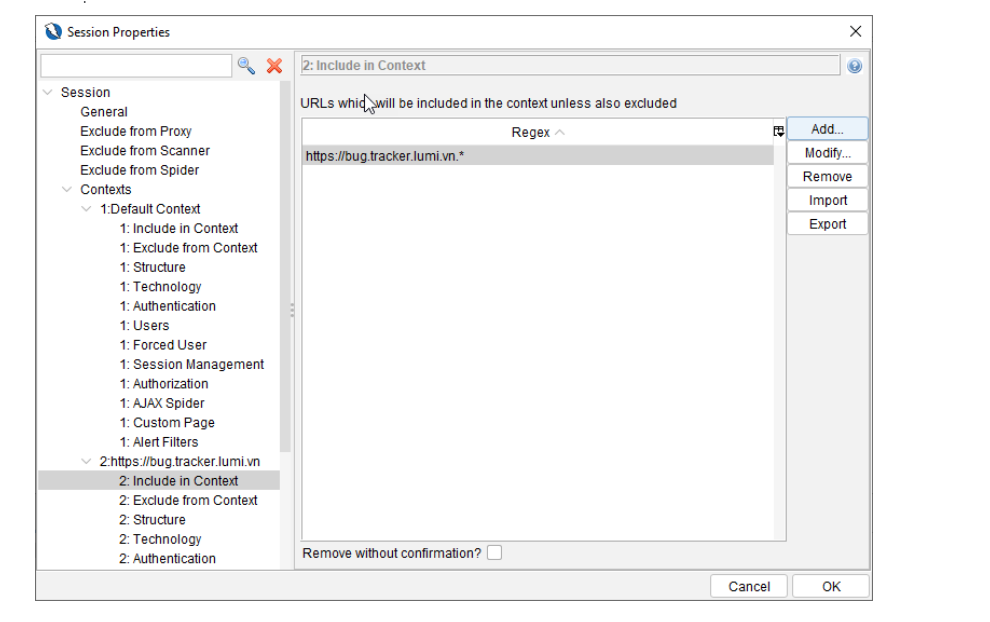
* Khi khởi động nó sẽ được đặt ở chế độ mặc định là Standard.
* Ta cần chuyển sang chế độ Protected Mode. (Lý do trọn chế độ Protected là vì, nếu trọn chế độ mặc định Standard hay là chế độ Attack thì có khả năng là nó sẽ tấn công vào các trang Web mà mình không quản lý được. Ngược lại nếu trọn chế độ Safe thì nó lại không scan được hết hoàn toàn các lỗ hổng , do đó ta trọn chế đô protected.)

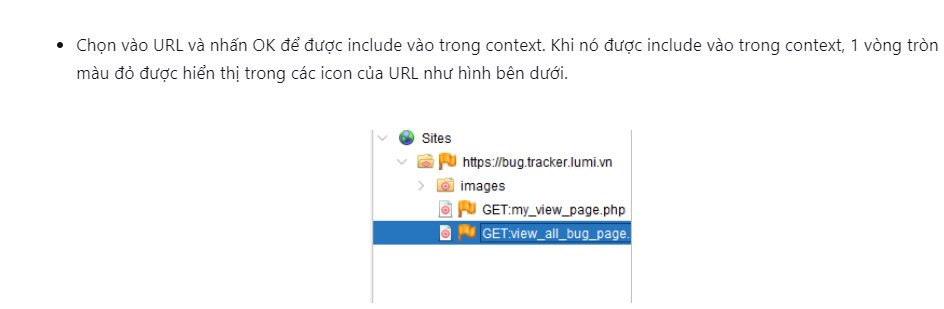
#### #**4.2. Tiến hành Test**

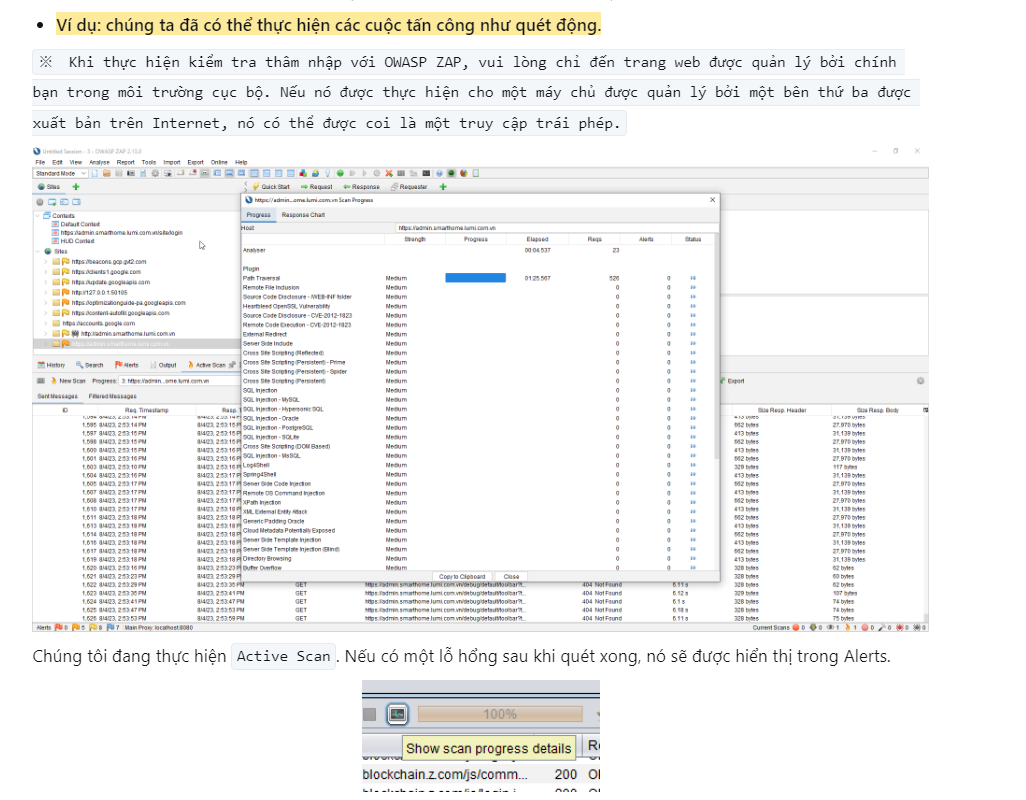
Click chuột phải vào link URL ở phía tab Sites, sẽ thấy mục Attack hiện lê nhưng không kích hoạt được bởi chưa Include in Context. Nhiệm vụ của bạn lúc này là Include URL cần được kiểm tra trong Context.

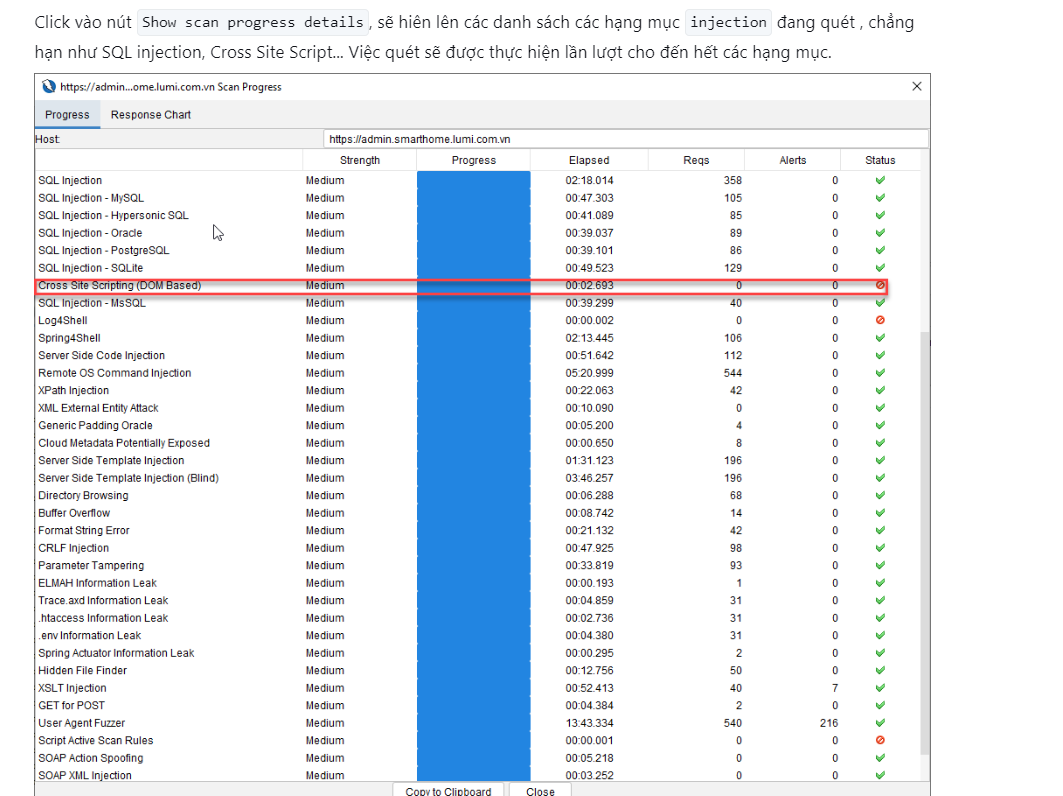
#### #**Include in Context**

* Click chuột phải vào Link và chọn Include in Context và chọn New Context. Khi đó, màn hình session property sẽ xuất hiện.



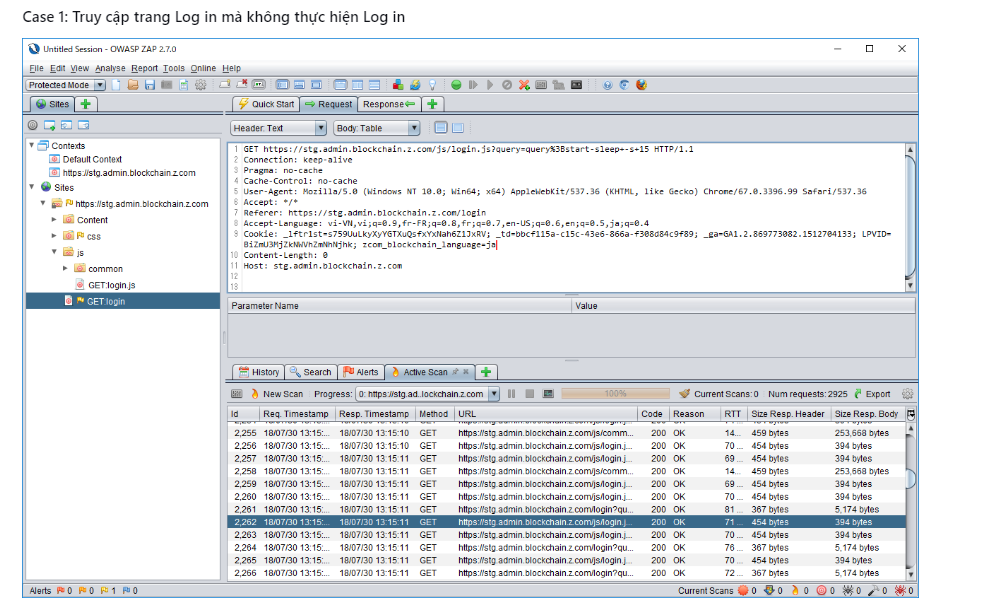




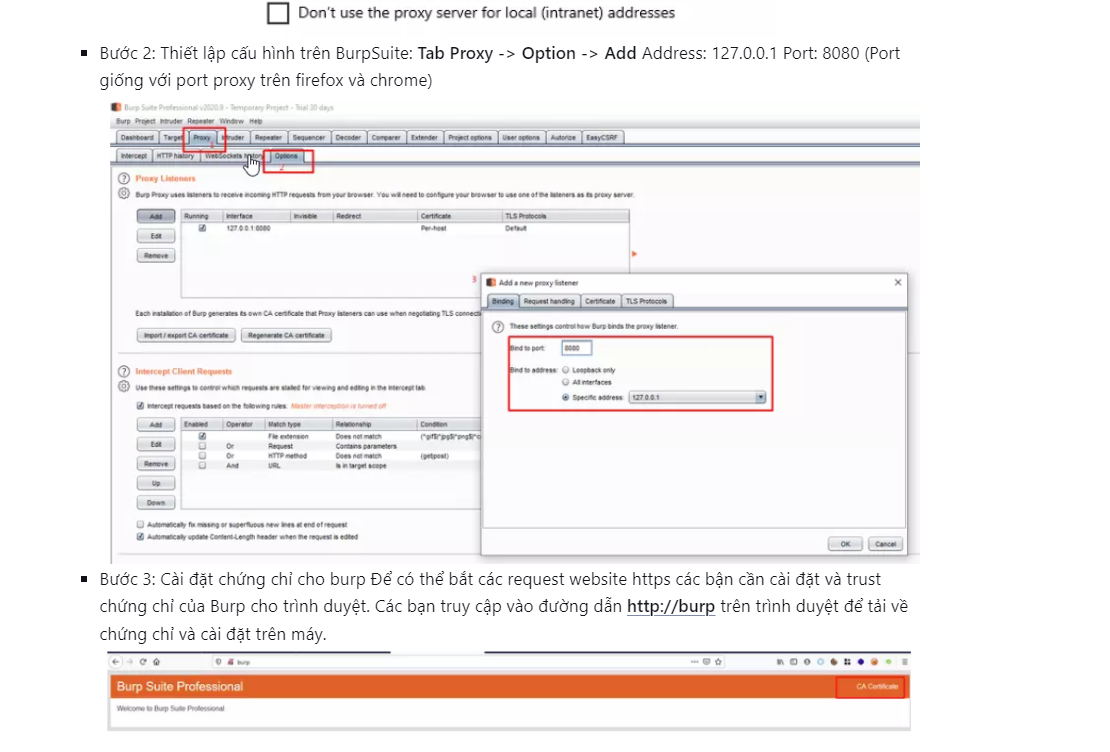
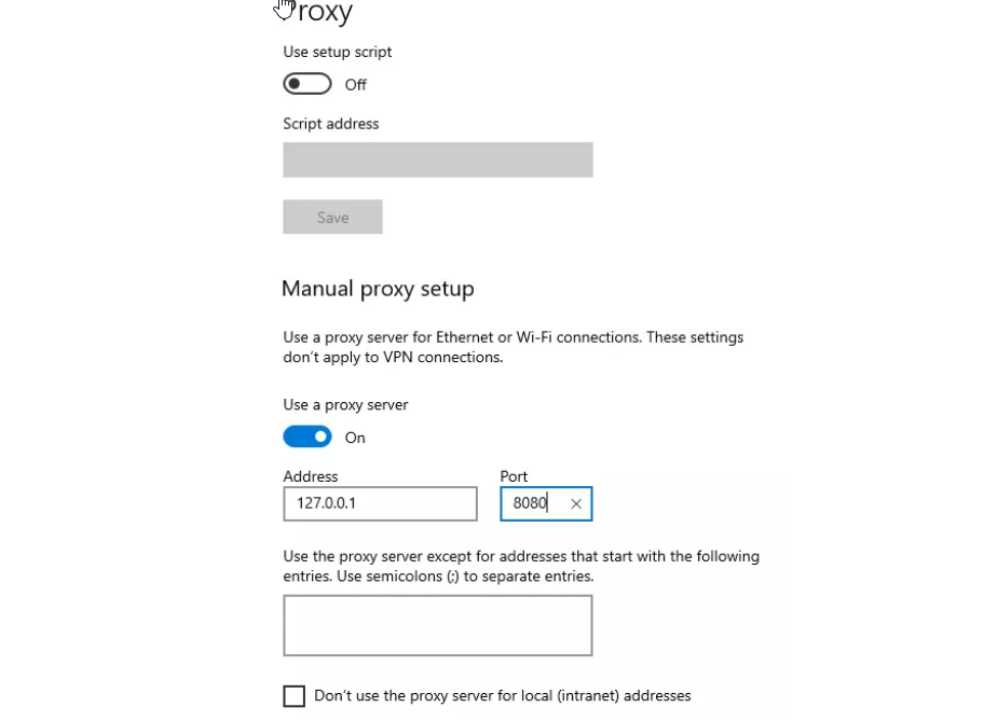
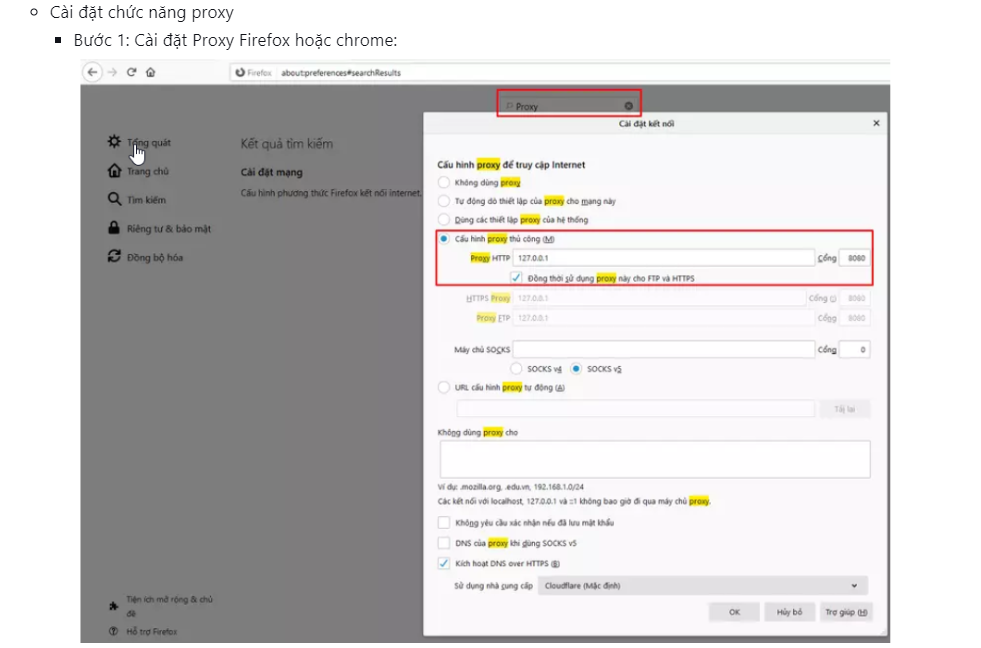
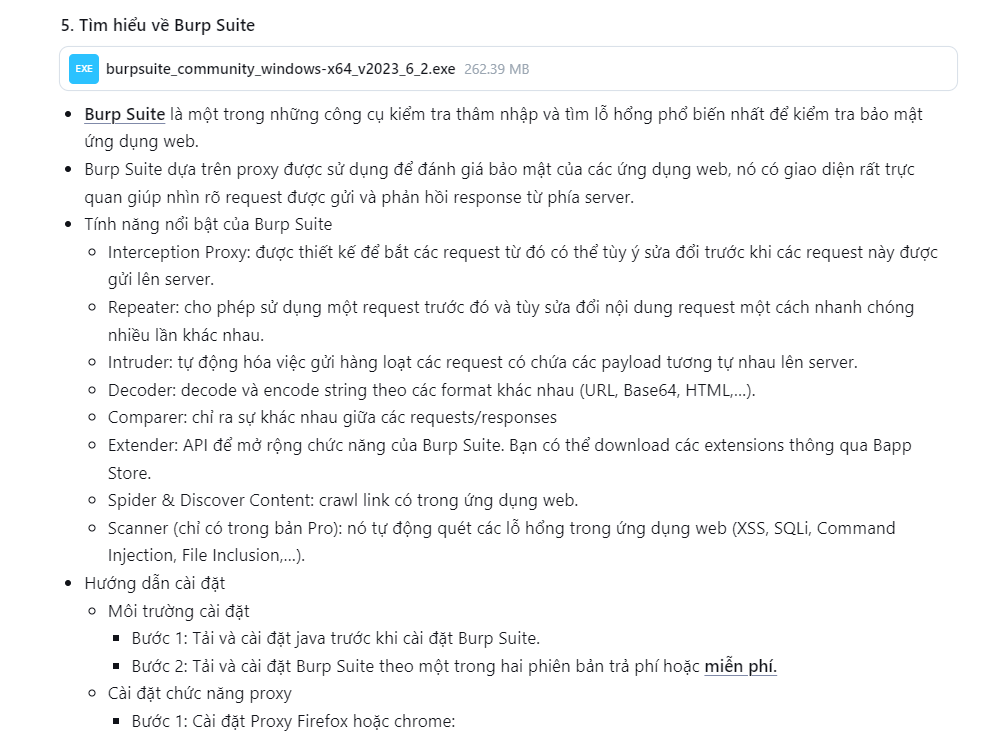
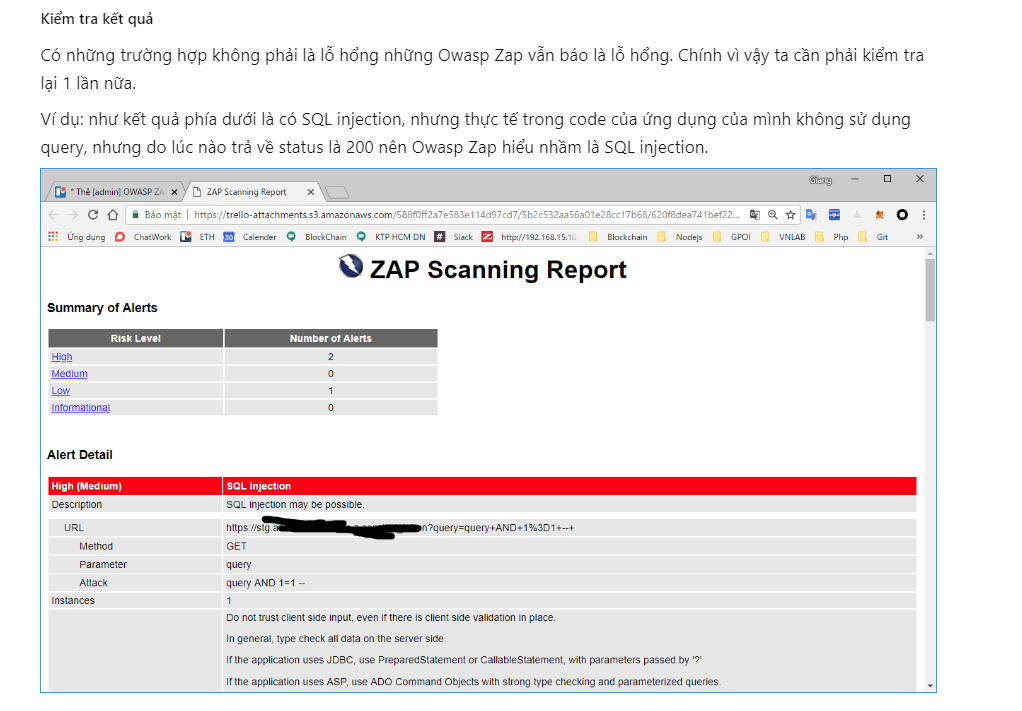
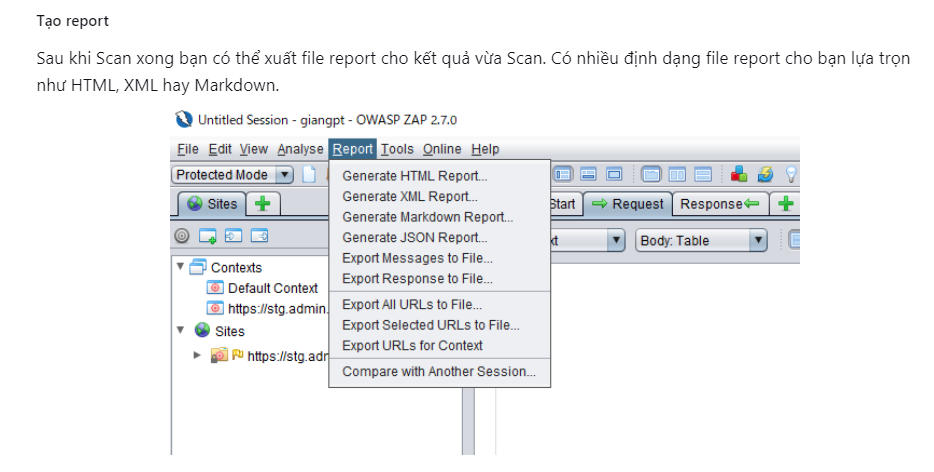
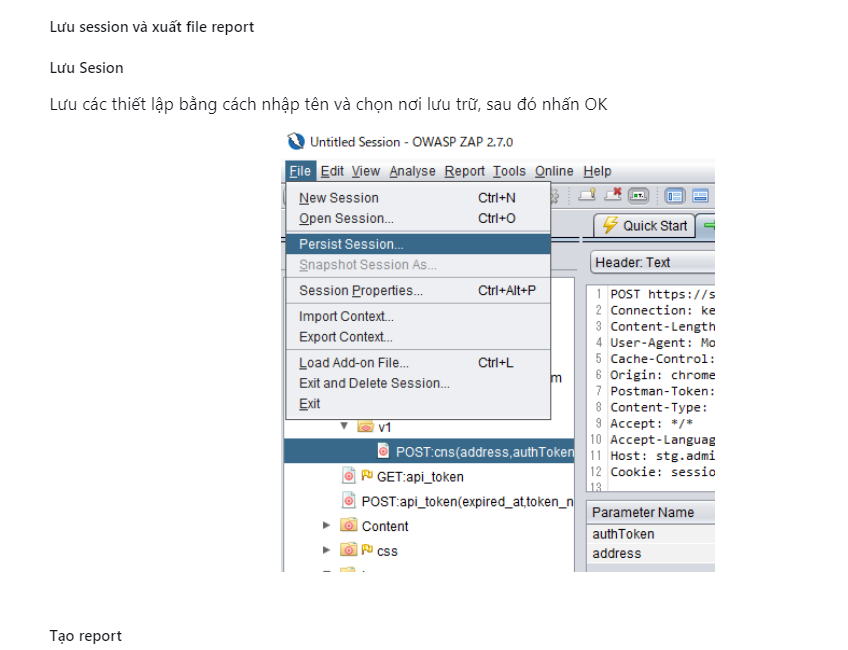
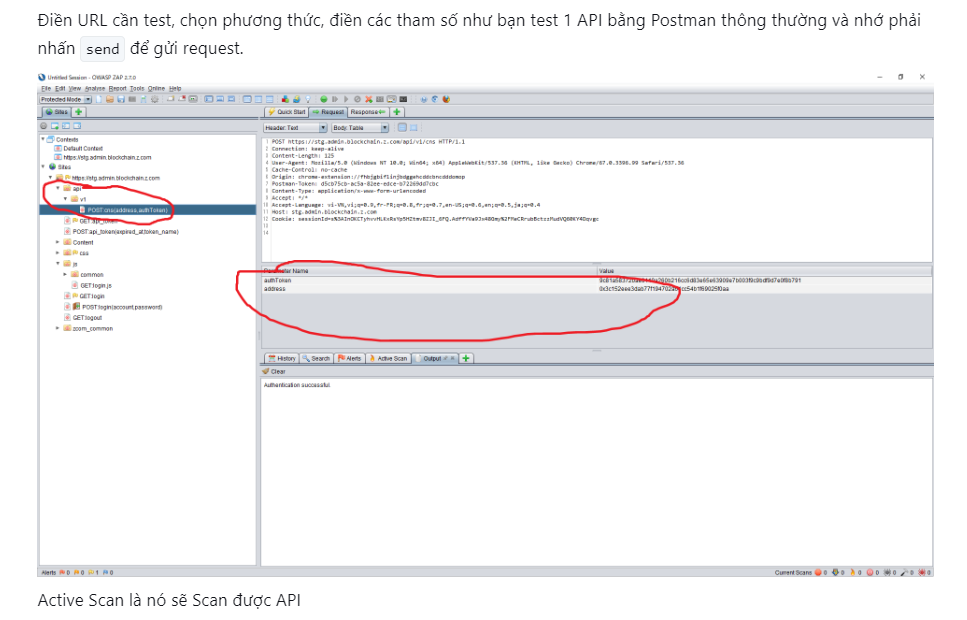
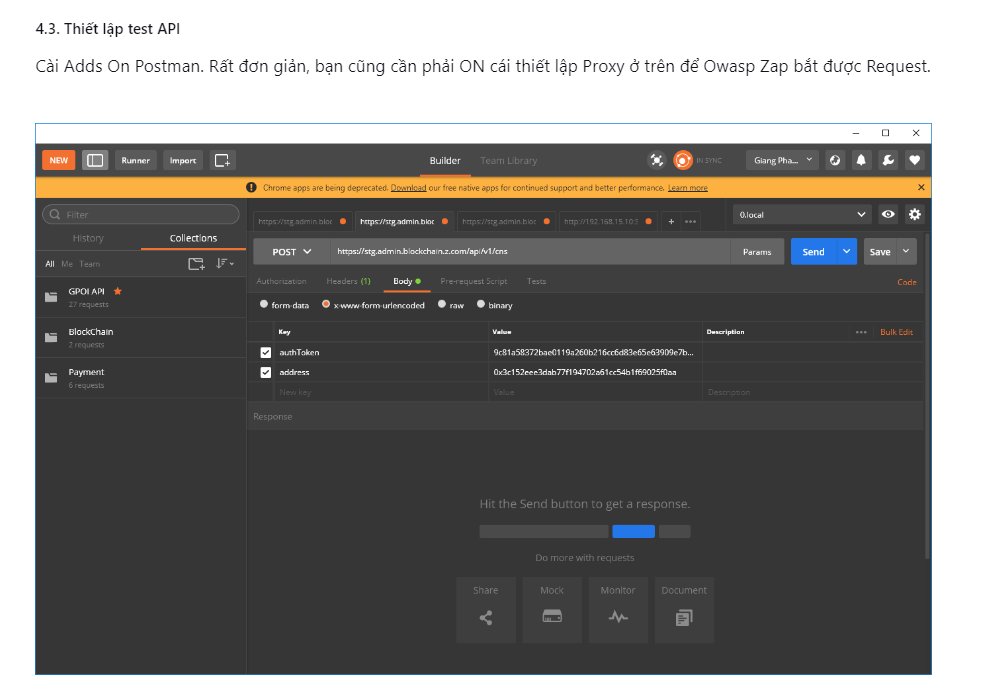
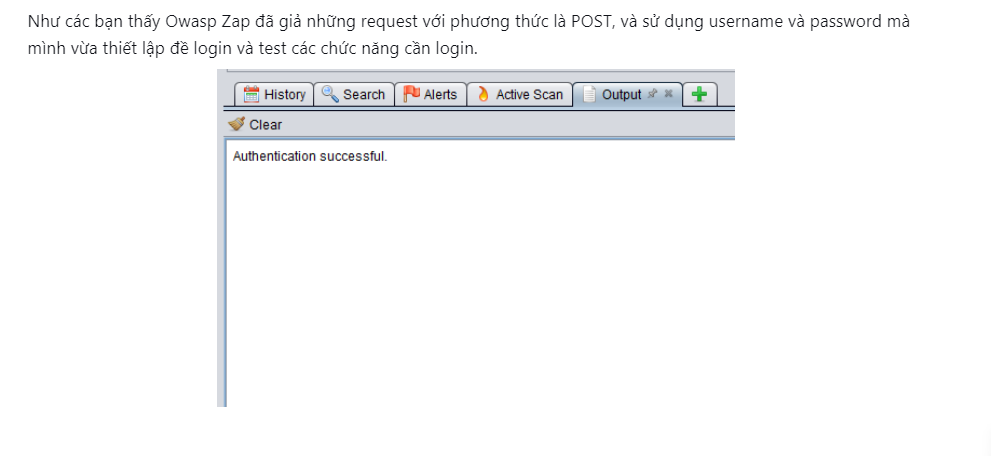
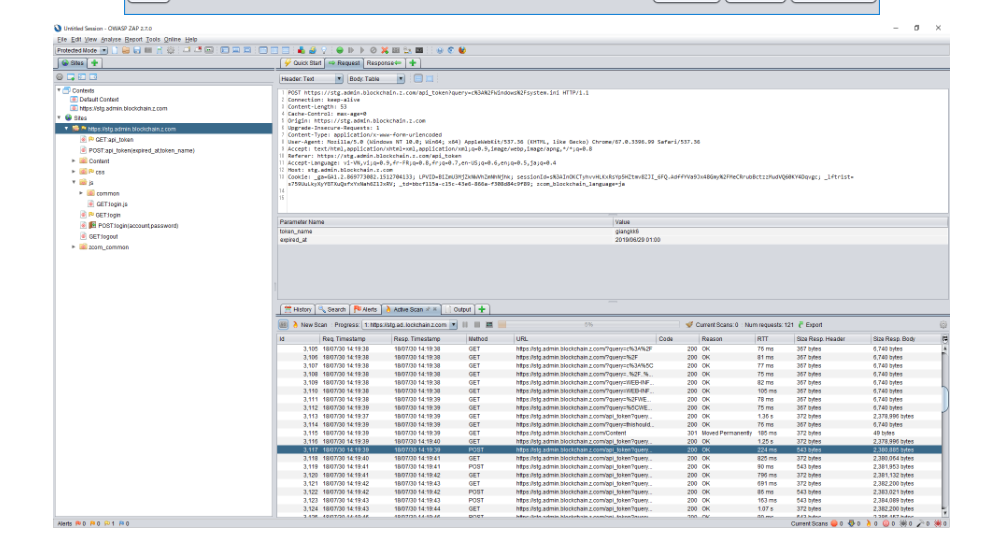
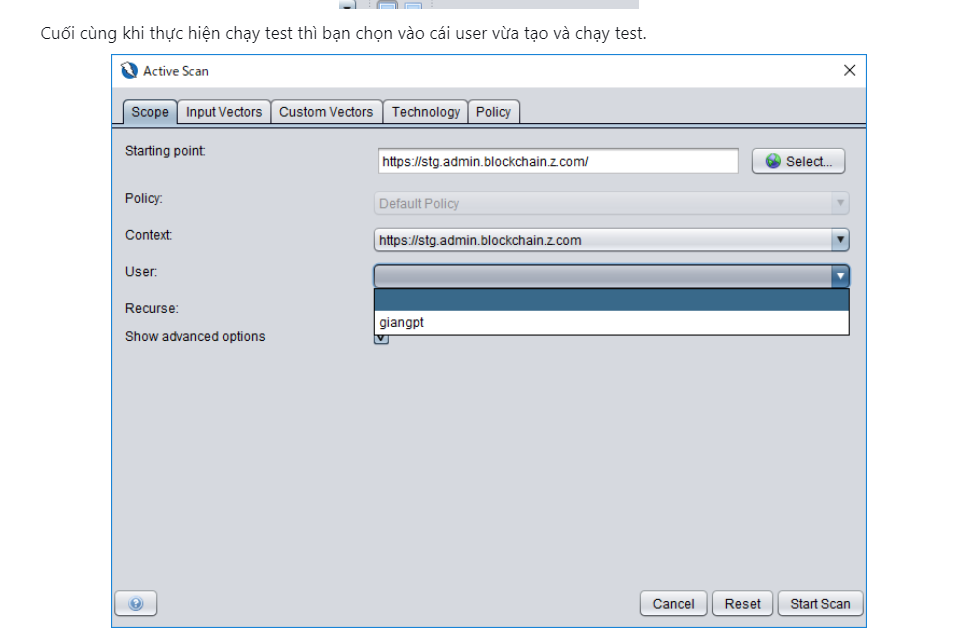
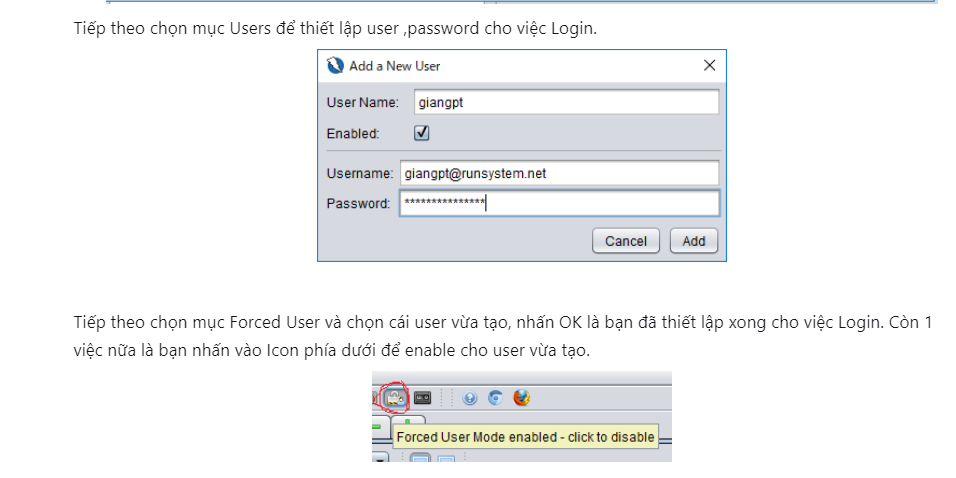
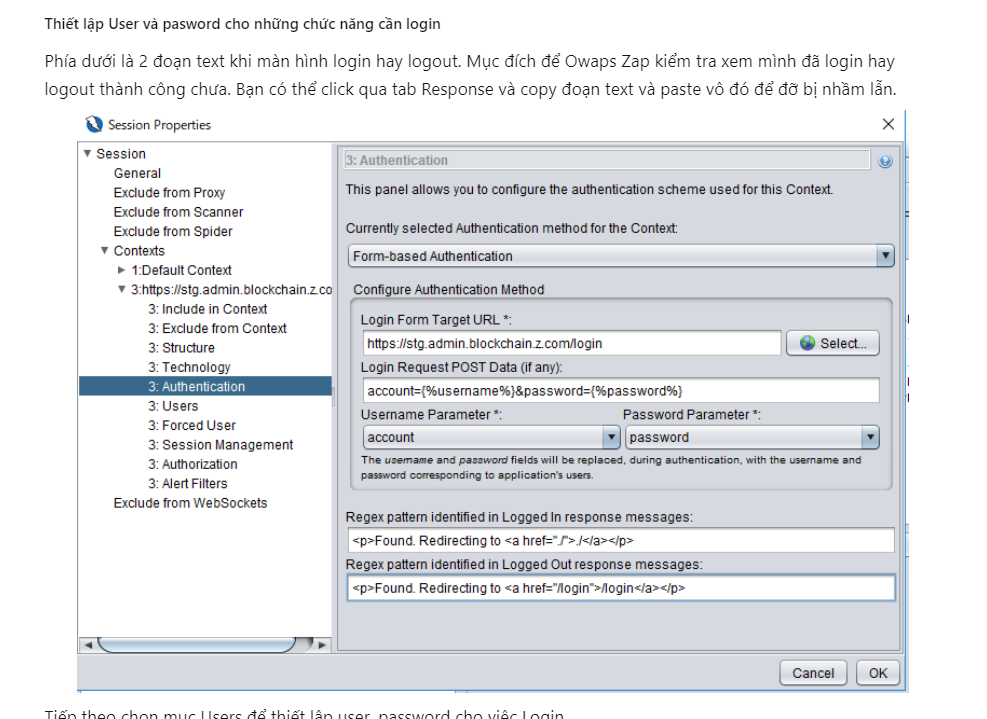
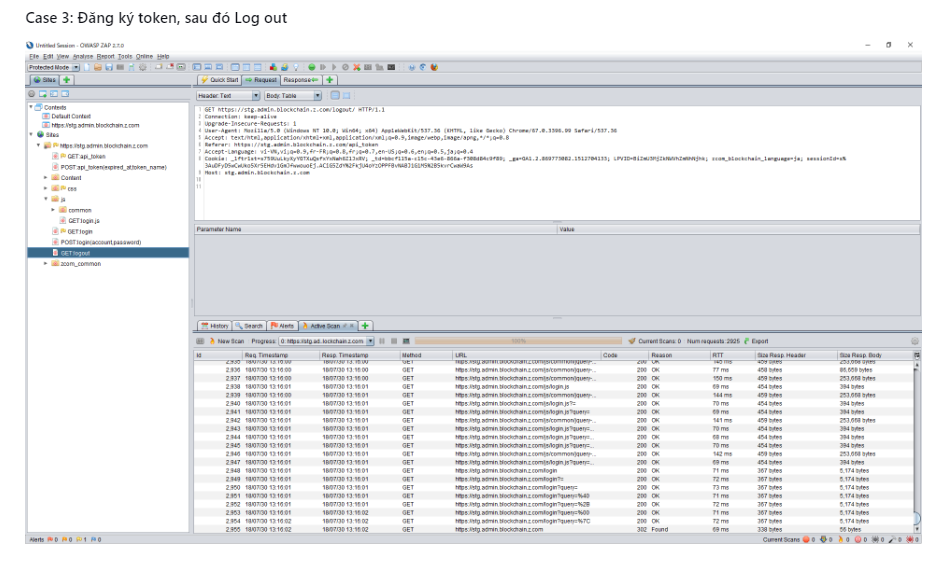


Click vào nút Show scan progress details, sẽ hiên lên các danh sách các hạng mục injection đang quét , chẳng hạn như SQL injection, Cross Site Script... Việc quét sẽ được thực hiện lần lượt cho đến hết các hạng mục.

**Dưới đây là ví dụ 3 case Log in, đăng ký token, Log out**







**#6. Bài tập thực hành test chức năng bảo mật.**

Demo website: <http://testphp.vulnweb.com/userinfo.php>

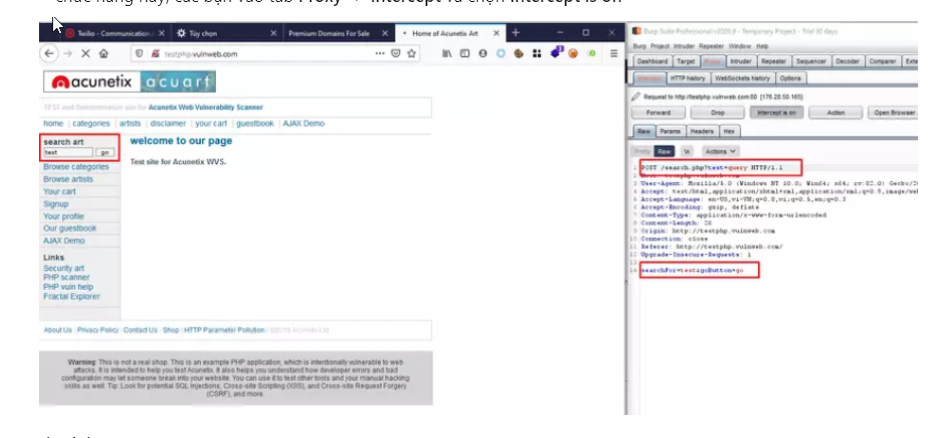
Tài khoản:

* Username: test
* Password: test

Công cụ hỗ trợ sử dụng

**Control toàn bộ request**

* Kiểm soát được dữ liệu được gửi lên server từ client, kiểm tra phía client bằng java script hay html5. Để sử dụng chức năng này, các bạn vào tab **Proxy -> Intercept** và chọn **Intercept is on**



**Các chức năng**

* **Intercept is on**: Request trước khi được gửi lên server sẽ được chặn lại tại đây để sửa đổi Nếu không on thì request sẽ đi thẳng lên server (Request vẫn được lưu lại tại tab **Proxy -> Proxy history** . Nếu không muốn bắt request thì các bạn chỉ cần click vào để tắt đi.
* **Drop**: Request bị drop và không gửi lên server
* **Forward**: Request được gửi lên server sau khi sửa đổi (hoặc không). Các bạn có thể thấy ró request được gửi lên bao gồm header, body... Và có thể sửa đổi thoải mái.
* \***LƯU Ý**: Vì khi các bạn chọn "Intercept is on" Burpsuite sẽ bắt toàn bộ request gửi từ trình duyệt nên nó có thể có cả request từ các website khác không phải request mình cần. Gặp trường hợp vậy các bạn cứ chọn forward cho tới khi nào có thể bắt được đúng request của website mình muốn.

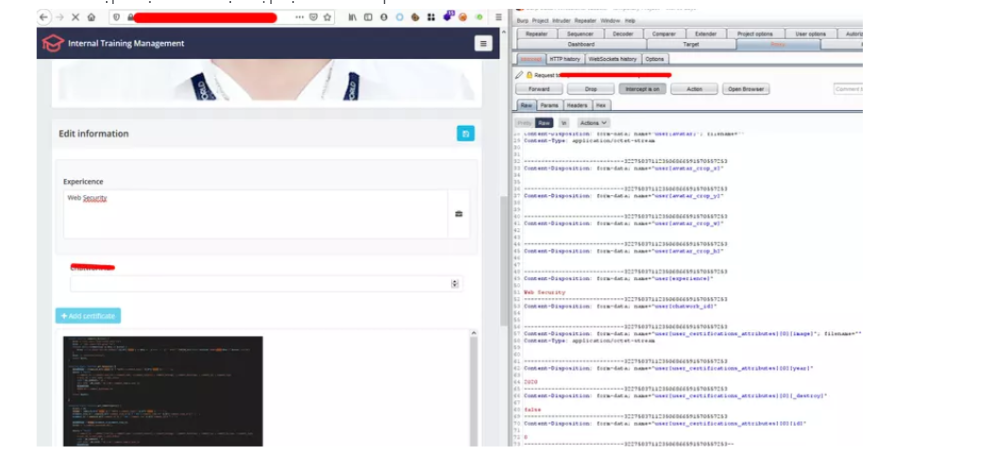
**Bypass client validation**

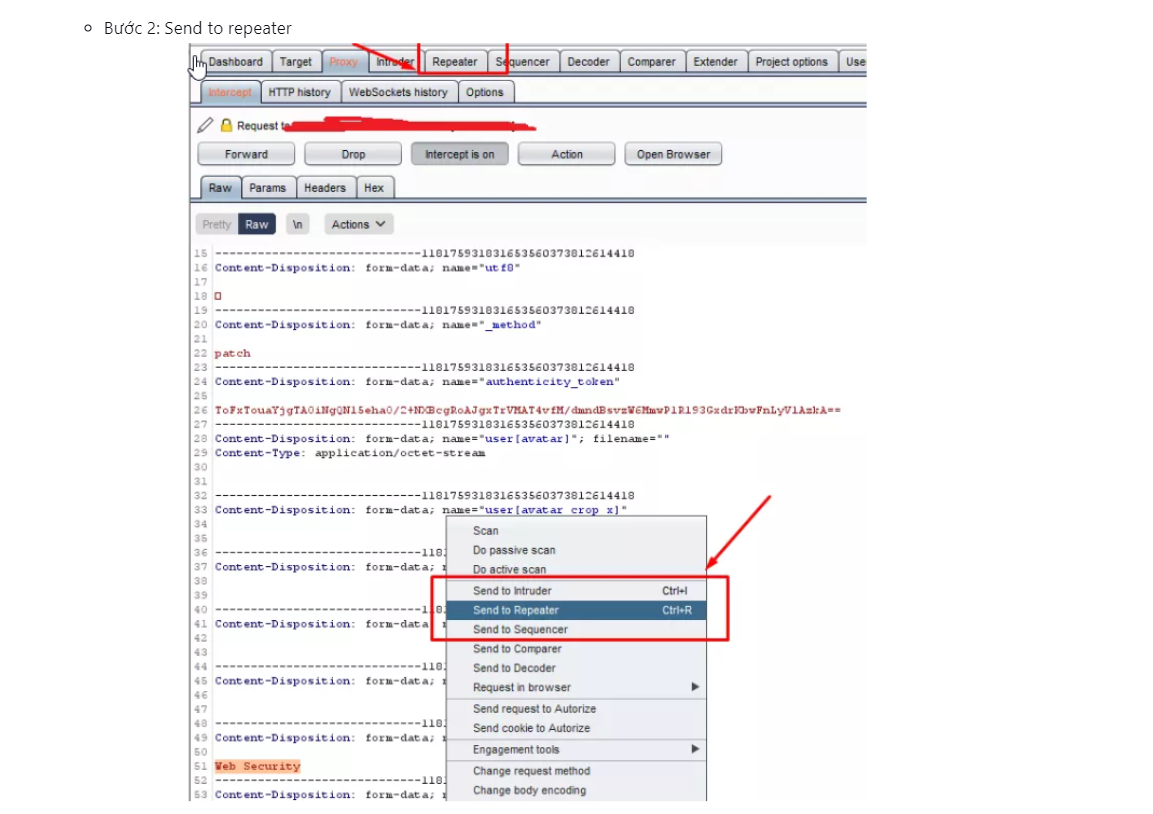
* VD: Phía client cho nhập 1 số, chặn nhập số âm và 1 số quá lớn. Hoặc website có chức năng upload ảnh và sử dụng javascript để kiểm tra đuôi file có phải .png, .jpg không. Bạn cần upload 1 file ảnh hợp lệ, sau đó sửa đuôi ảnh theo ý mình muốn như .html, .php, .image.
* **Demo tham khảo**
  + Bước 1: Upload 1 file php không thành công

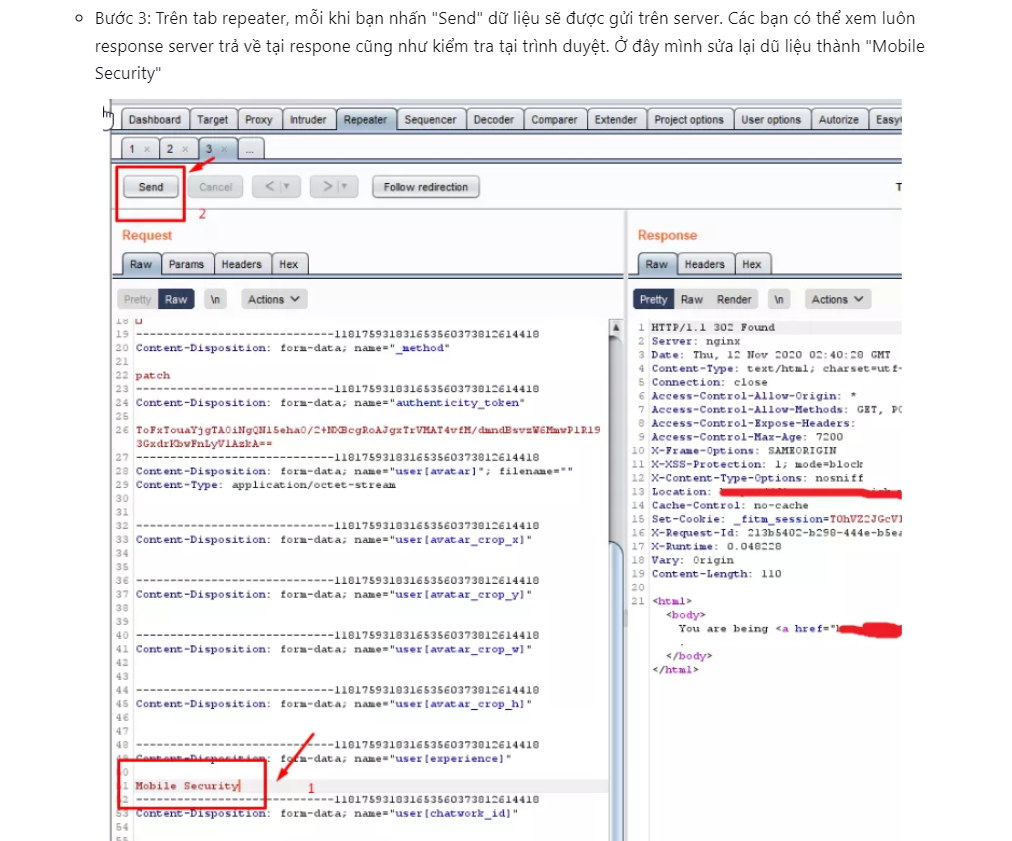


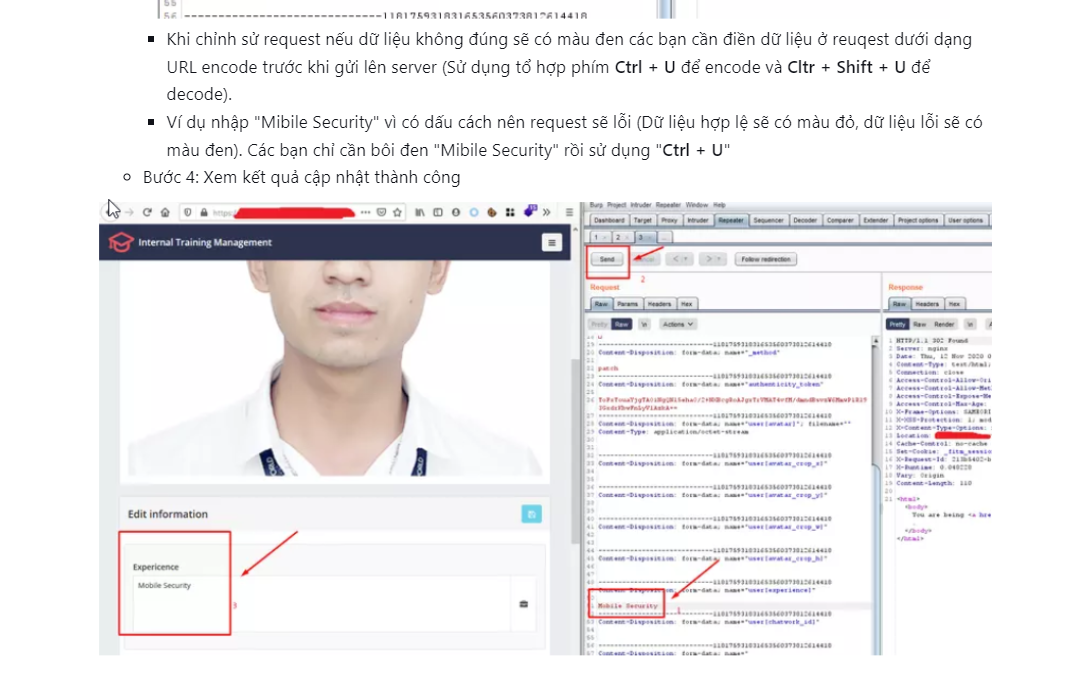
**Test các trường dữ liệu**

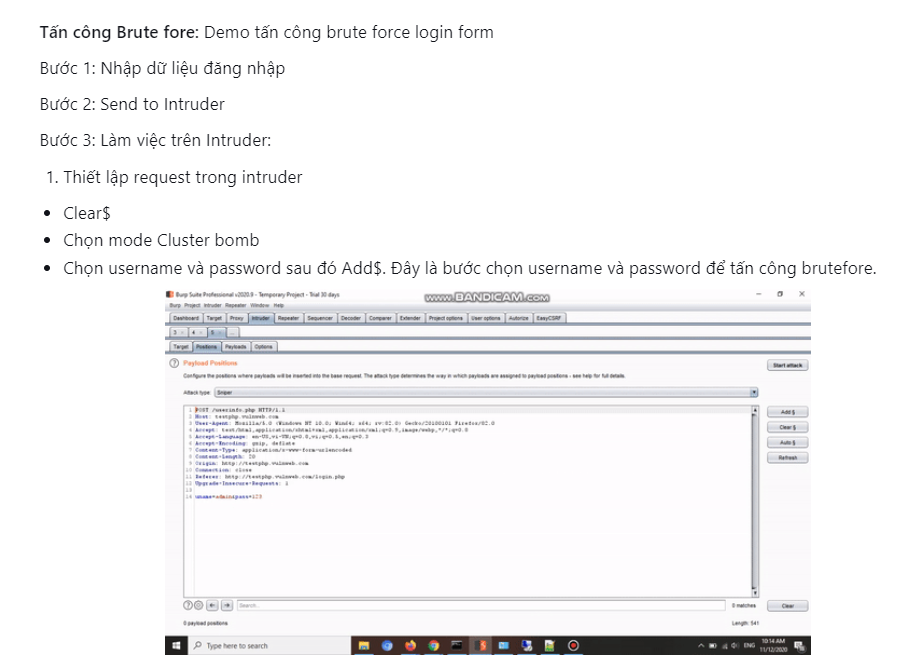
* Chỉ với 1 request hợp lệ được "**Intercept is on**" sau đó là click chuột phải và "**Send to repeater**" là các bạn có thể thoải mái test và không cần nhập liệu lại nhiều lần khác nhau.
* Demo chức năng cập nhật profile user
  + Bước 1: Cập nhật với dữ liệu hợp lệ và "Intercept"

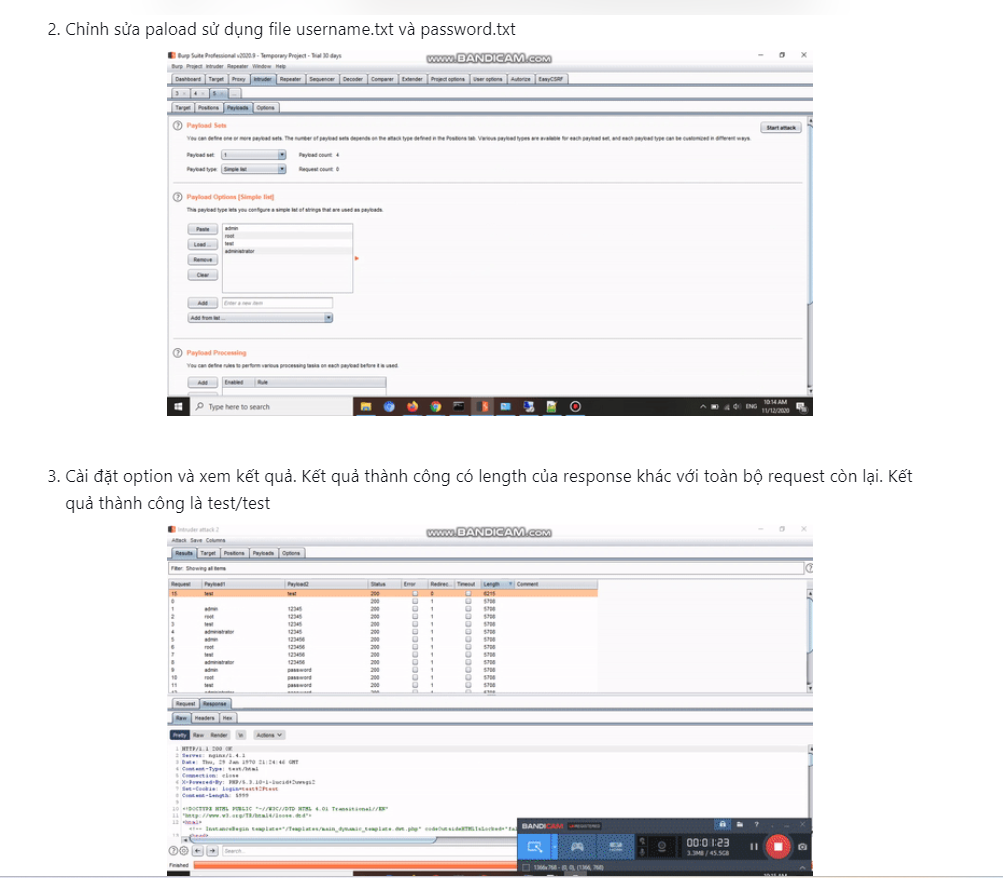












**Ngoài ví dụ các chức năng trên, còn rất nhiều các case thực tế cần được kiểm thử. Ví dụ về “Các kịch bản kiểm thử để kiểm tra tính bảo mật” :**

* Xác minh trang web có chứa dữ liệu quan trọng như mật khẩu, số thẻ tín dụng, câu trả lời bí mật cho câu hỏi bảo mật, vv phải được gửi qua HTTPS (SSL).
* Xác minh thông tin quan trọng như mật khẩu, số thẻ tín dụng, v.v. sẽ hiển thị ở định dạng được mã hóa.
* Xác minh quy tắc mật khẩu được thực hiện trên tất cả các trang xác thực như Đăng ký, quên mật khẩu, thay đổi mật khẩu.
* Xác minh nếu mật khẩu được thay đổi, người dùng sẽ không thể đăng nhập bằng mật khẩu cũ.
* Xác minh các thông báo lỗi sẽ không hiển thị bất kỳ thông tin quan trọng nào.
* Xác minh nếu người dùng đăng xuất khỏi hệ thống hoặc phiên người dùng đã hết hạn, người dùng sẽ không thể điều hướng trang web.
* Xác minh việc truy cập trực tiếp vào các trang web được bảo mật và không được bảo mật mà không cần đăng nhập.
* Xác minh tùy chọn “Xem mã nguồn” bị tắt và không hiển thị với người dùng.
* Xác minh tài khoản người dùng bị khóa nếu người dùng nhập sai mật khẩu nhiều lần.
* Xác minh các cookie không nên lưu trữ mật khẩu.
* Xác minh nếu, bất kỳ chức năng nào không hoạt động, hệ thống sẽ không hiển thị bất kỳ thông tin ứng dụng, máy chủ hoặc cơ sở dữ liệu nào. Thay vào đó, nó sẽ hiển thị trang lỗi tùy chỉnh.
* Xác minh các cuộc tấn công SQL injection.
* Xác minh vai trò người dùng và quyền của họ. Ví dụ người dùng bình thường không thể truy cập trang quản trị.
* Xác minh các hoạt động quan trọng được ghi trong các tệp nhật ký và thông tin đó sẽ được theo dõi.
* Xác minh các giá trị phiên trong định dạng được mã hóa trong thanh địa chỉ.
* Xác minh thông tin cookie được lưu trữ ở định dạng được mã hóa.
* Xác minh ứng dụng tấn công Brute Force

### #7. Tham khảo file báo cáo kiểm thử bảo mật

Sau khi hoàn thành kiểm thử bảo mật, bạn hãy lập file báo cáo kiểm thử để thực hiện báo cáo công việc.

* Sử dụng file báo cáo kết quả có sẵn của tool
* Hoặc dựng file báo cáo kết quả, phân tích lỗi