# [Toobler Blog](http://toobler.com/)

* [PORTFOLIO](http://www.toobler.com/portfolio.html)
* [SERVICES](http://www.toobler.com/services/)
* [CASE STUDIES](http://www.toobler.com/casestudy.html)
* [ABOUT](http://www.toobler.com/about.html)
* [BLOG](http://www.toobler.com/blog/)
* [CONTACT](http://www.toobler.com/#contact)

# ZAP Penetration Testing: A simple Tutorial to Detect Vulnerabilities

28th March 2016 By [Geethu Alexander](http://www.toobler.com/blog/author/geethu)

Penetration testing (otherwise known as pen testing, or the more general security testing) is the process of testing your applications for vulnerabilities, and answering a simple question: “What could a hacker do to harm my application, or organization, out in the real world?”

Recently I came across a tool, Zed Attack Proxy (ZAP). Its main goal is to allow easy penetration testing to find vulnerabilities in web applications. It is ideal for developers and functional testers as well as security experts. Let’s check out how ZAP penetration testing works.

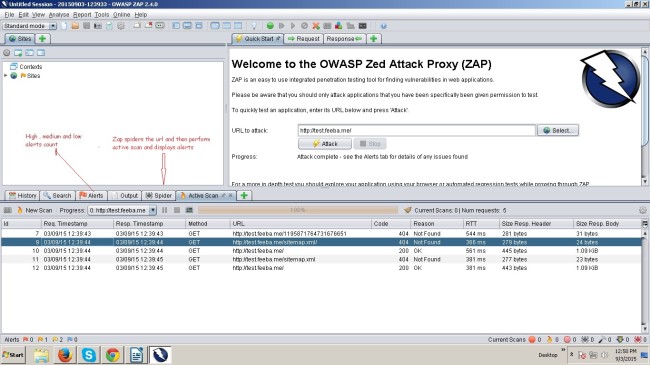
#### Installation and configuration of ZAP:

Download Link:  
<https://github.com/zaproxy/zaproxy/wiki/Downloads>

##### Step1

##### Adding a site to the testing scope

By telling ZAP what the target site is, ZAP can limit the scope of the scan and only scan the target site for vulnerabilities.  
1. Open the web application that you want to test.  
2. In Zap you will find your website/application displayed under sites.  
ZAP will spider that URL, then perform an active scan and display the results.



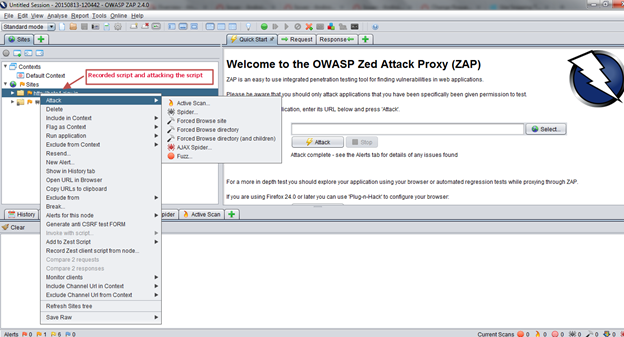
#### Zap runs on proxy, to set up the proxy in ZAP:

Close all active Firefox browser sessions  
ZAP tool -> Tools Menu -> Options -> Local Proxy -> Change Address = 127.0.0.1 Port = 8080.  
Mozilla browser -> Tools Menu -> Options -> Advanced tab -> Network -> Settings -> Select Manual Proxy configuration:- HTTP Proxy = 127.0.0.1 Port = 8080.

Now try to connect to your application using your browser.  
If you can’t connect to it then check your proxy settings again. You will need to check your browser’s proxy settings, and ZAP’s proxy settings. It’s also worth checking that the application that you are trying to test is running!

When you have successfully connected to your application you will see one or more lines in ZAP’s Sites and History tabs.  
Note that most of ZAP’s tabs provide additional functionality that could be accessed via ‘right click’ menus.

Right click on the HTML -> Attack -> Active scan  
ZAP will perform active scan on all the pages and display the results.



#### Save the ZAP session

Once you have manually explored the application it would be a good time to save the ZAP session so that you can look at it again.  
If your application has multiple roles then you should explore it with each role and save the sessions in separate files.

#### Generating a Report:

ZAP tool -> Report -> Generate HTML report (Any other options listed) -> Save and share the report.

##### Authentication , session and User management using ZAP

1) Context: Represents a Web application  
2) Session Management Method: How are the web Sessions identified by the server and handle requests

Example: cookie based using query parameters  
3) Authentication Method: How is a new session established?  
It could be either Form based authentication method, HTTP based or oath methods.  
4) User Management: Handling users of web application that could be used for executing actions  
Example: user name/password pair

##### Steps to follow:

1) Set proxy in local browser/access url: [https://pr-uat.iptquote.com](https://pr-uat.iptquote.com/)  
Now include web app in context.

#### Context includes:

(i)Authentication  
(ii)Session management  
(iii)Users management

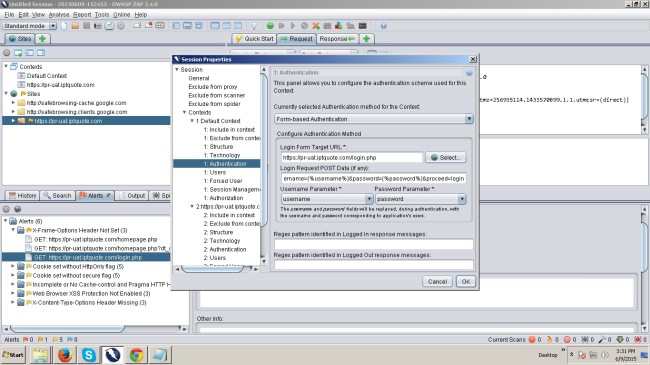
#### Context: Form based authentication

(I) log-in from target url: https://pr-uat.iptquote.com/login.php

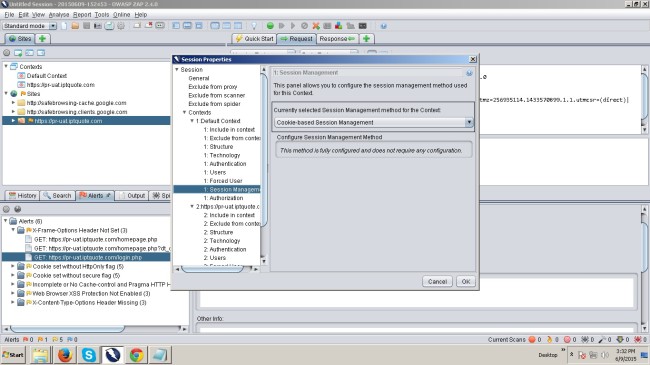
(ii) Login Request POST Data: username={%username%}&password={%password%}&proceed=login

(iii) Set params as: username =password

(iv) Include regex pattern for logged in or logged out response  
Regex pattern for logged in response :- \Qa href=”https://pr-uat.iptquote.com/login.php?proceed=logout\E

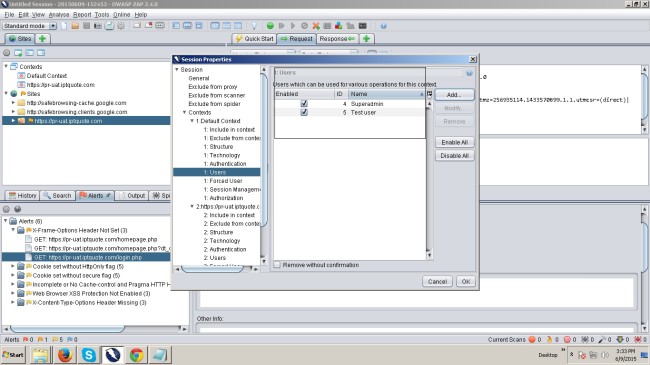


#### Context: Session Management



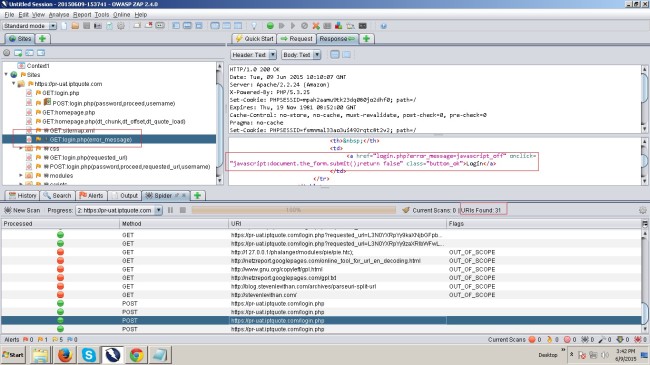
#### Context: User management

For user management, we can add 2 users, one valid user let it be the “Existing user” here “superadmin” in our example and other is “Test User” invalid user.

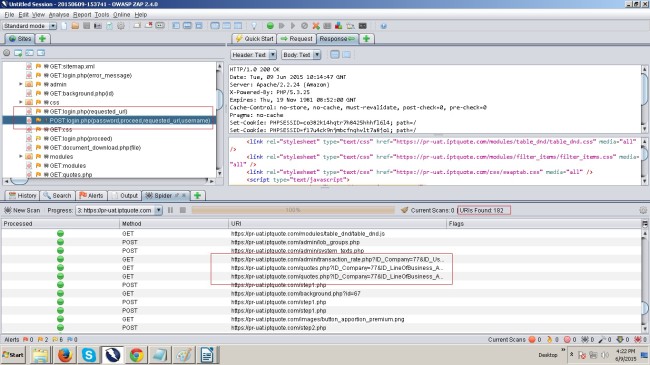


#### Spider url attack applied to “Test user”

If spider url attack applied to the Test user returns get\_login.php (error\_message), also once spider attack completed “Test User” accesses home url only. uri’s covered: 31 is shown in the screenshot, where as only scan through https://pr-uat.iptquote.com



#### Spider url attack for existing valid user “Superadmin”



Here spider url attack applied to the Existing valid user. That is user with super admin logged in credentials. In the attached screenshots returns “POST login.php ( request \_url) if selected, returns Uri’s covered 182 for the valid user. He can access all sites.

If you have any interest in application security then you should download ZAP and try it out.

##### Links:

OWASP [https://www.owasp.org](https://www.owasp.org/)  
Zed Attack Proxy, <https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project>

* [OWASP](http://www.toobler.com/blog/tag/owasp)

* [PENETRATION TESTING](http://www.toobler.com/blog/tag/penetration-testing)

* [QA](http://www.toobler.com/blog/tag/qa)

* [QUALITY ASSURANCE](http://www.toobler.com/blog/tag/quality-assurance)

* [SECURITY TESTING](http://www.toobler.com/blog/tag/security-testing)

* [ZAP](http://www.toobler.com/blog/tag/zap)

### RECENT ARTICLES

##### [Finally !!! CSS Variable has arrived.](http://www.toobler.com/blog/finally-css-variables-arrived)

25th October 2016[->](http://www.toobler.com/blog/finally-css-variables-arrived)

##### [THE MOST USEFUL CSS3 FEATURES](http://www.toobler.com/blog/the-most-useful-css3-features)

19th October 2016[->](http://www.toobler.com/blog/the-most-useful-css3-features)

##### [Does it make sense deploying Swift instead of Java...](http://www.toobler.com/blog/swift-for-android)

19th April 2016[->](http://www.toobler.com/blog/swift-for-android)

http://www.toobler.com/blog/wp-content/themes/tbl_2016/images/needHelp.pnghttp://www.toobler.com/blog/wp-content/themes/tbl_2016/images/chat-face.png

Top of Form





Bottom of Form

[**Older Post**](http://www.toobler.com/blog/google-accelerated-mobile-pages)[**Newer Post**](http://www.toobler.com/blog/how-to-migrate-from-parse-to-mongodb-and-aws)