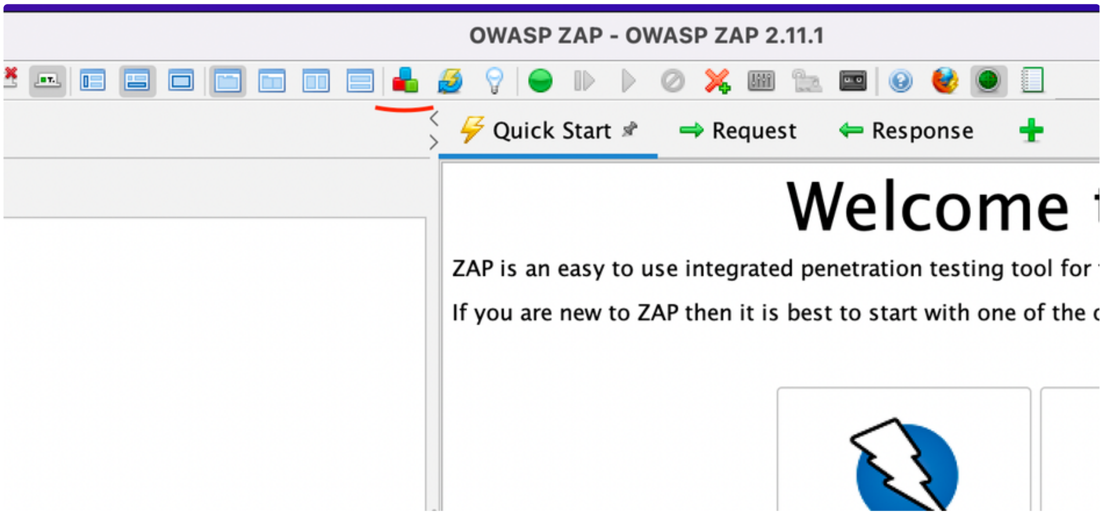
040: Hunting BAC with ZAP

OWASP ZAP is a powerful scanner but if we want to ensure we utilize its full potential, we have to configure it well. Zap has a module with which we can test for broken access control. This module is an add-on it needs to be downloaded later on we can do this from the menu. If you go to add-ons and click on that little button you can see that you can actually download the Access control module. So go ahead and download and install the module as we will be using it in this test.

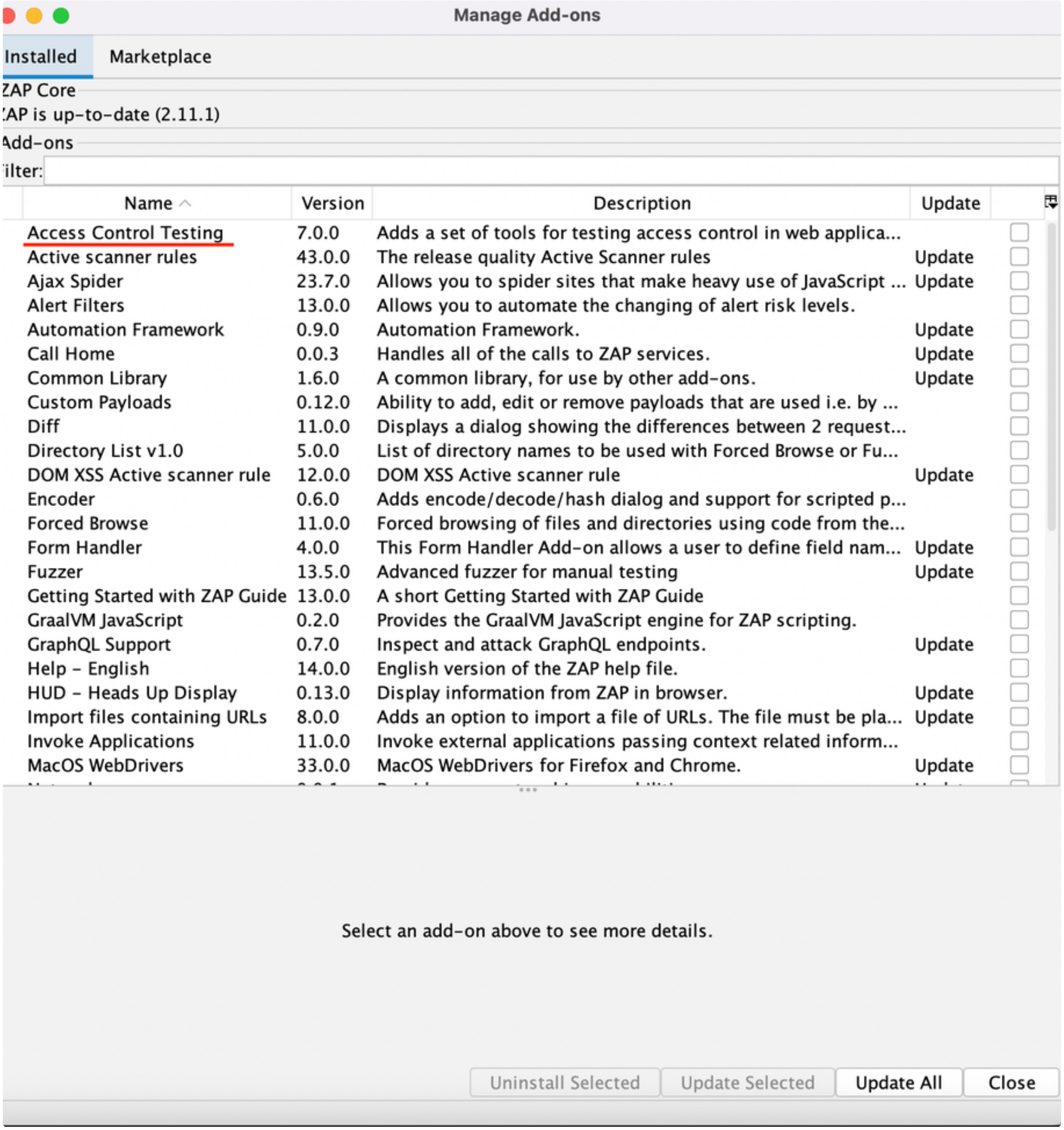


OWASP ZAP - OWASP ZAP 2.11.1

Welcome t

ZAP is an easy to use integrated penetration testing tool for

If you are new to ZAP then it is best to start with one of the o



ZAP Core

ZAP is up-to-date (2.11.1)

Add-ons

Filter:

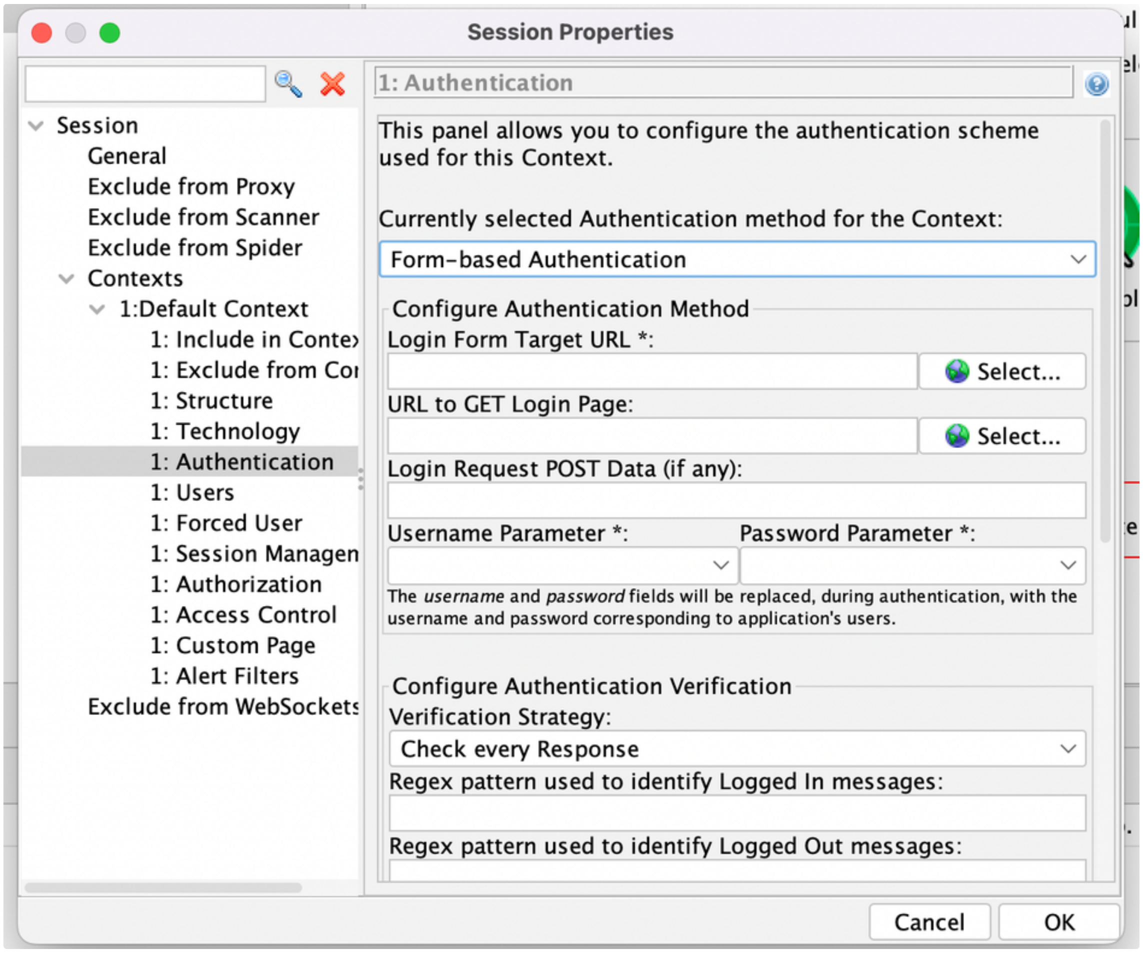
Name	Version	Description	Update	
Access Control Testing	7.0.0	Adds a set of tools for testing access control in web applica...		□
Active scanner rules	43.0.0	The release quality Active Scanner rules	Update	□
Ajax Spider	23.7.0	Allows you to spider sites that make heavy use of JavaScript ...	Update	□
Alert Filters	13.0.0	Allows you to automate the changing of alert risk levels.		□
Automation Framework	0.9.0	Automation Framework.	Update	□
Call Home	0.0.3	Handles all of the calls to ZAP services.	Update	□
Common Library	1.6.0	A common library, for use by other add-ons.	Update	□
Custom Payloads	0.12.0	Ability to add, edit or remove payloads that are used i.e. by ...		□
Diff	11.0.0	Displays a dialog showing the differences between 2 request...		□
Directory List v1.0	5.0.0	List of directory names to be used with Forced Browse or Fu...		□
DOM XSS Active scanner rule	12.0.0	DOM XSS Active scanner rule	Update	□
Encoder	0.6.0	Adds encode/decode/hash dialog and support for scripted p...		□
Forced Browse	11.0.0	Forced browsing of files and directories using code from the...		□
Form Handler	4.0.0	This Form Handler Add-on allows a user to define field nam...	Update	□
Fuzzer	13.5.0	Advanced fuzzer for manual testing	Update	□
Getting Started with ZAP Guide	13.0.0	A short Getting Started with ZAP Guide		□
GraalVM JavaScript	0.2.0	Provides the GraalVM JavaScript engine for ZAP scripting.		□
GraphQL Support	0.7.0	Inspect and attack GraphQL endpoints.	Update	□
Help - English	14.0.0	English version of the ZAP help file.		□
HUD - Heads Up Display	0.13.0	Display information from ZAP in browser.	Update	□
Import files containing URLs	8.0.0	Adds an option to import a file of URLs. The file must be pla...	Update	□
Invoke Applications	11.0.0	Invoke external applications passing context related inform...		□
MacOS WebDrivers	33.0.0	MacOS WebDrivers for Firefox and Chrome.	Update	□

Select an add-on above to see more details.

Contexts

Everything in ZAP revolves around contexts. The context is the location where you can set things like your user settings such as authorization. In this case, we will be using those authorization settings. Now to add a user we will first need to set the type of authentication as well.

For our exercise, pick the authorisation type of form based:



1: Authentication

This panel allows you to configure the authentication scheme used for this Context.

Currently selected Authentication method for the Context: Form-based Authentication

Configure Authentication Method

Login Form Target URL *:

URL to GET Login Page:

Login Request POST Data (if any):

Username Parameter *: Password Parameter *:

The *username* and *password* fields will be replaced, during authentication, with the username and password corresponding to application's users.

Configure Authentication Verification

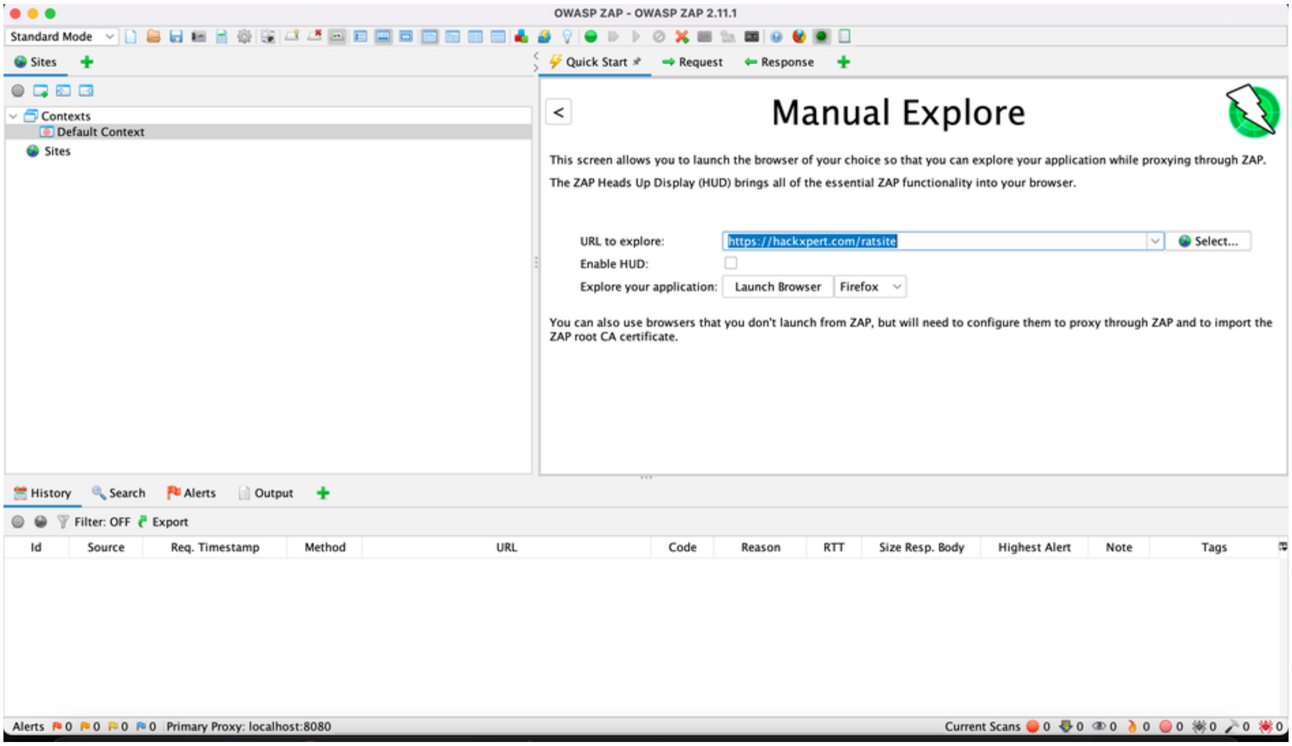
Verification Strategy: Check every Response

Regex pattern used to identify Logged In messages:

Regex pattern used to identify Logged Out messages:

It's going to ask you for a URL, on which it can't log in. to do that to, we will have to go and browse the website manually. So go ahead and browse the site manually. Make sure you actually log in with the credentials of admin and password of admin.

🔗 Welcome to RatSite!



Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

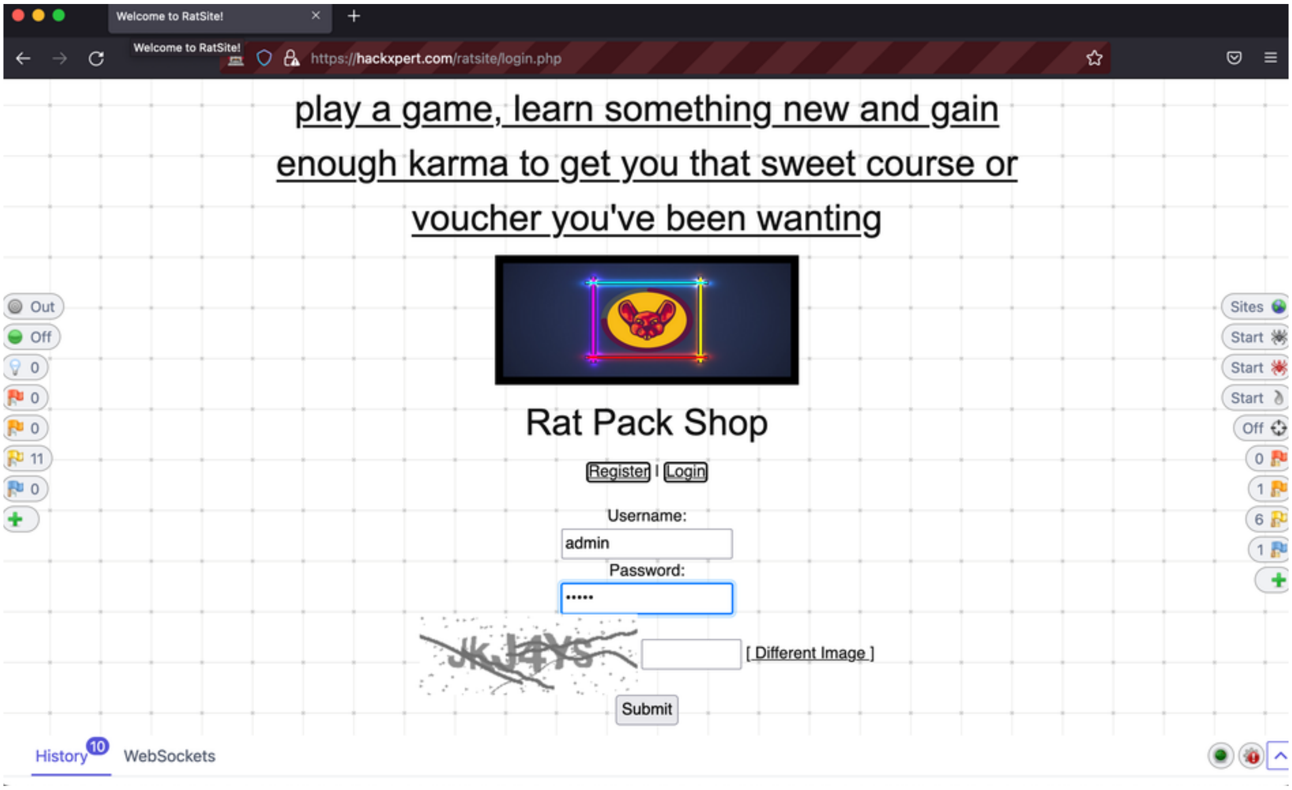
The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: https://hackxpert.com/ratsite

Enable HUD: □

Explore your application: Launch Browser Firefox

You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import the ZAP root CA certificate.



https://hackxpert.com/ratsite/login.php

play a game, learn something new and gain enough karma to get you that sweet course or voucher you've been wanting

Rat Pack Shop

Register | Login

Username: admin

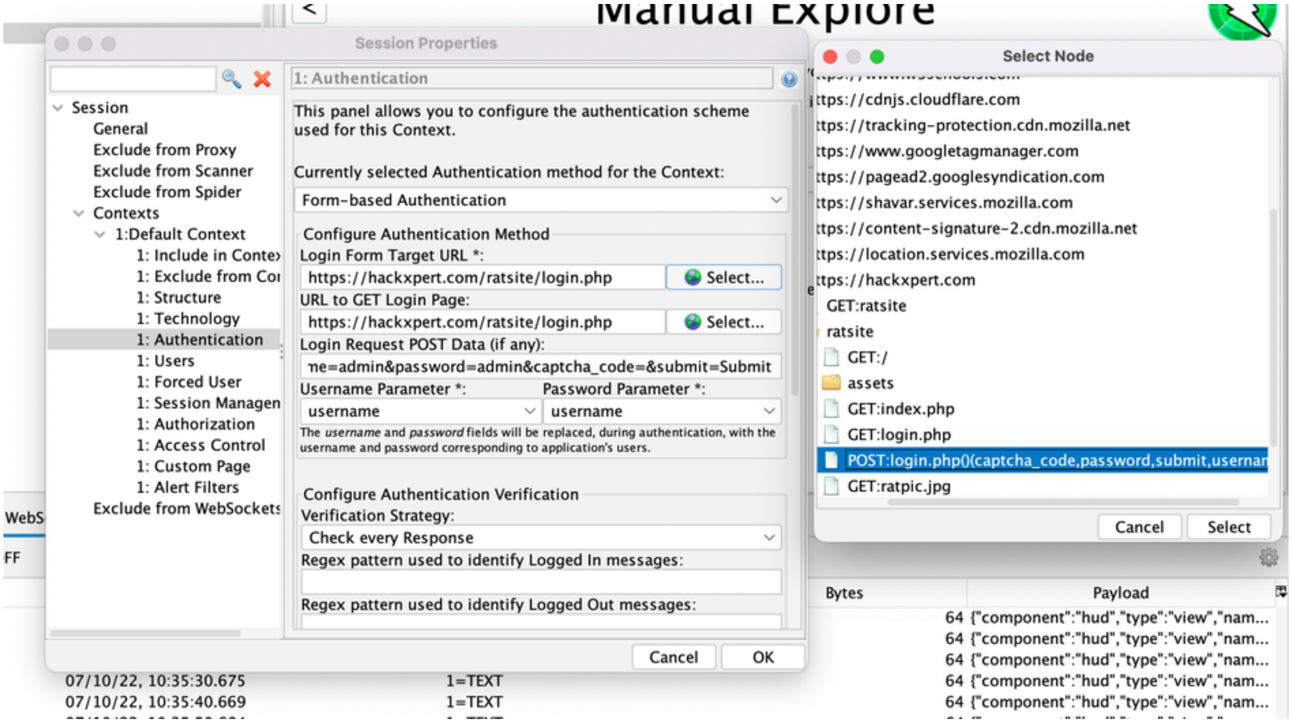
Password: •••••

[Different Image]

Submit

After logging in we can return to our context to set the authorization type.

Set it to login form based. And then the first selection box makes sure you select the POST request to login.php.



1: Authentication

This panel allows you to configure the authentication scheme used for this Context.

Currently selected Authentication method for the Context: Form-based Authentication

Configure Authentication Method

Login Form Target URL *: https://hackxpert.com/ratsite/login.php

URL to GET Login Page: https://hackxpert.com/ratsite/login.php

Login Request POST Data (if any): ne=admin&password=admin&captcha_code=&submit=Submit

Username Parameter *: username

Password Parameter *: username

The *username* and *password* fields will be replaced, during authentication, with the username and password corresponding to application's users.

Configure Authentication Verification

Verification Strategy: Check every Response

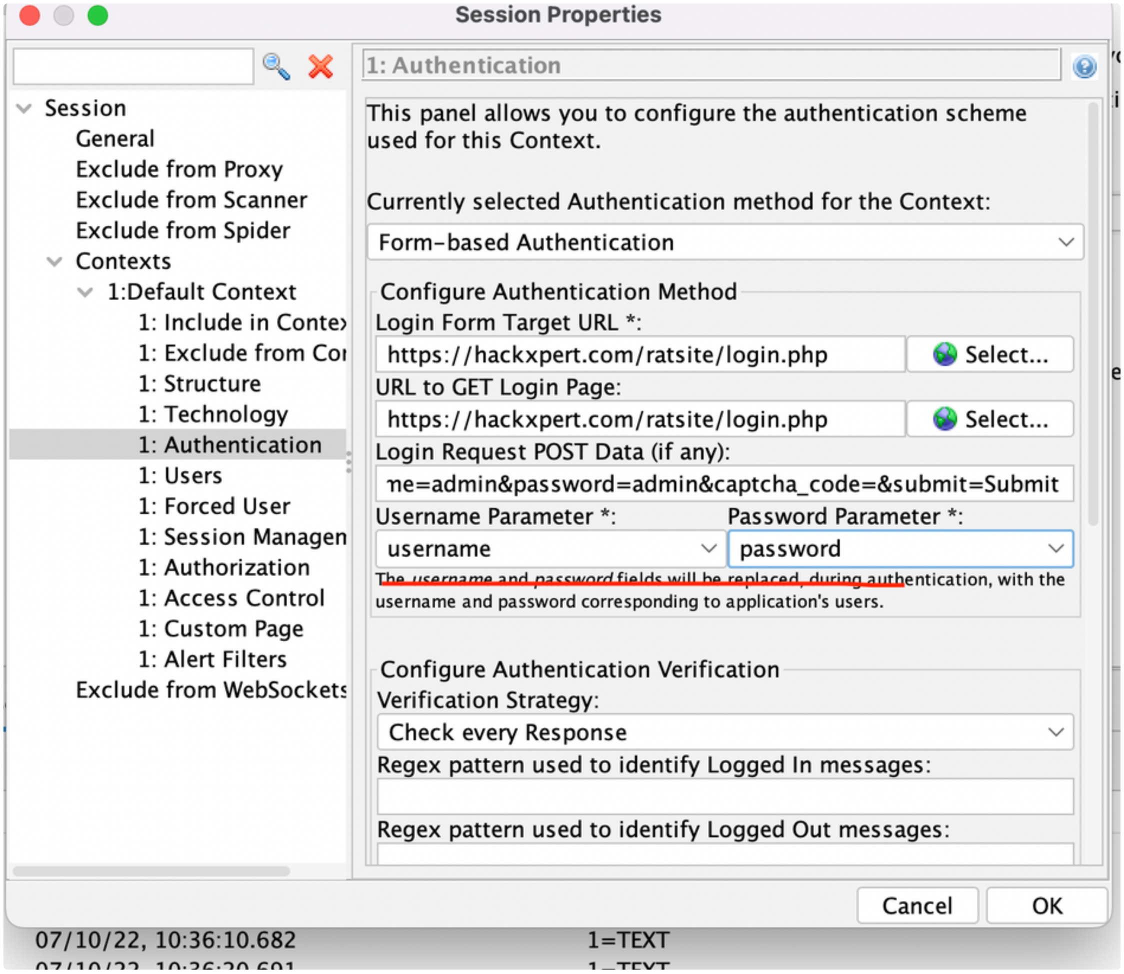
Regex pattern used to identify Logged In messages:

Regex pattern used to identify Logged Out messages:

```
ttps://cdnjs.cloudflare.com
ttps://tracking-protection.cdn.mozilla.net
ttps://www.googletagmanager.com
ttps://pagead2.googlesyndication.com
ttps://shavar.services.mozilla.com
ttps://content-signature-2.cdn.mozilla.net
ttps://location.services.mozilla.com
ttps://hackxpert.com
  GET:ratsite
  ratsite
    GET:/
    assets
    GET:index.php
    GET:login.php
    POST:login.php()(captcha_code,password,submit,usernan
    GET:ratpic.jpg
```

```
07/10/22, 10:35:30.675    1=TEXT    64 {"component":"hud","type":"view","nam...
07/10/22, 10:35:40.669    1=TEXT    64 {"component":"hud","type":"view","nam...
```

Make sure you match the two parameters of username and password.



Session Properties

1: Authentication

This panel allows you to configure the authentication scheme used for this Context.

Currently selected Authentication method for the Context: Form-based Authentication

Configure Authentication Method

Login Form Target URL *: https://hackxpert.com/ratsite/login.php

URL to GET Login Page: https://hackxpert.com/ratsite/login.php

Login Request POST Data (if any): ne=admin&password=admin&captcha_code=&submit=Submit

Username Parameter *: username

Password Parameter *: password

The username and password fields will be replaced, during authentication, with the username and password corresponding to application's users.

Configure Authentication Verification

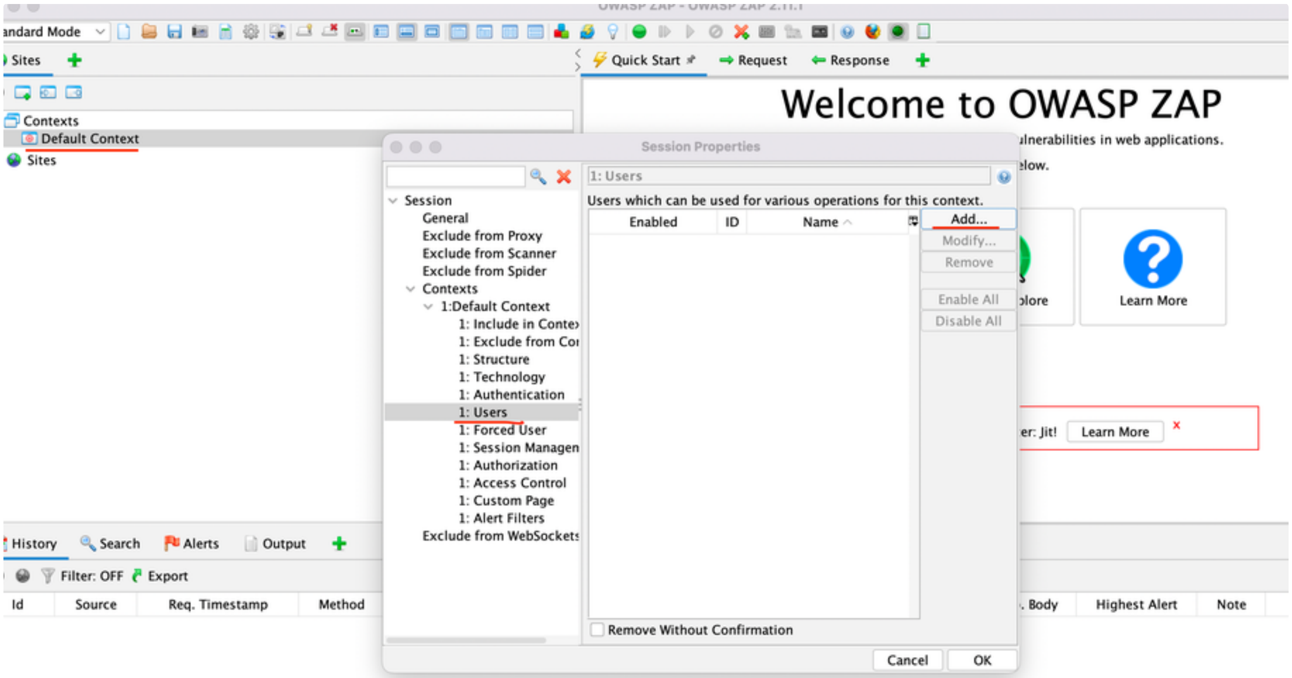
Verification Strategy: Check every Response

Regex pattern used to identify Logged In messages:

Regex pattern used to identify Logged Out messages:

07/10/22, 10:36:10.682 1=TEXT

Now go ahead and open the default context so we can add a user to it:



Session Properties

1: Users

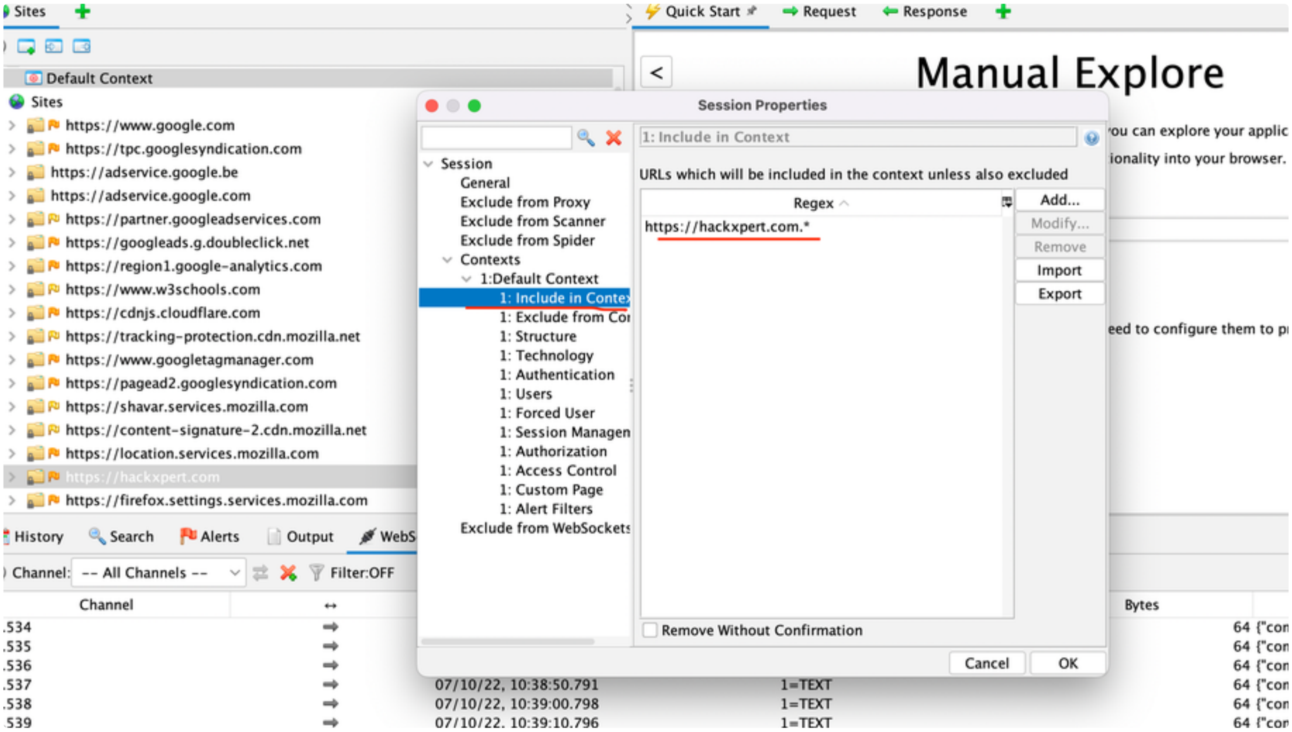
Users which can be used for various operations for this context.

Enabled	ID	Name

☐ Remove Without Confirmation

Add the two users with username admin and password admin and also at the user with username test and password test.

Lastly make sure that your Scope is set correctly:


Sites
Default Context
Sites
https://www.google.com
https://tpc.googlesyndication.com
https://adservice.google.be
https://adservice.google.com
https://partner.googleadservices.com
https://googleads.g.doubleclick.net
https://region1.google-analytics.com
https://www.w3schools.com
https://cdnjs.cloudflare.com
https://tracking-protection.cdn.mozilla.net
https://www.googletagmanager.com
https://pagead2.googlesyndication.com
https://shavar.services.mozilla.com
https://content-signature-2.cdn.mozilla.net
https://location.services.mozilla.com
https://hackxpert.com
https://firefox.settings.services.mozilla.com
History
Search
Alerts
Output
WebS
Channel: -- All Channels --
Filter:OFF
Channel
Quick Start
Request
Response
Manual Explore
Session Properties
Session
General
Exclude from Proxy
Exclude from Scanner
Exclude from Spider
Contexts
1:Default Context
1: Include in Contex
1: Exclude from Co
1: Structure
1: Technology
1: Authentication
1: Users
1: Forced User
1: Session Managen
1: Authorization
1: Access Control
1: Custom Page
1: Alert Filters
Exclude from WebSockets
Add...
Modify...
Remove
Import
Export
Cancel
OK
Bytes

1: Include in Context

URLs which will be included in the context unless also excluded

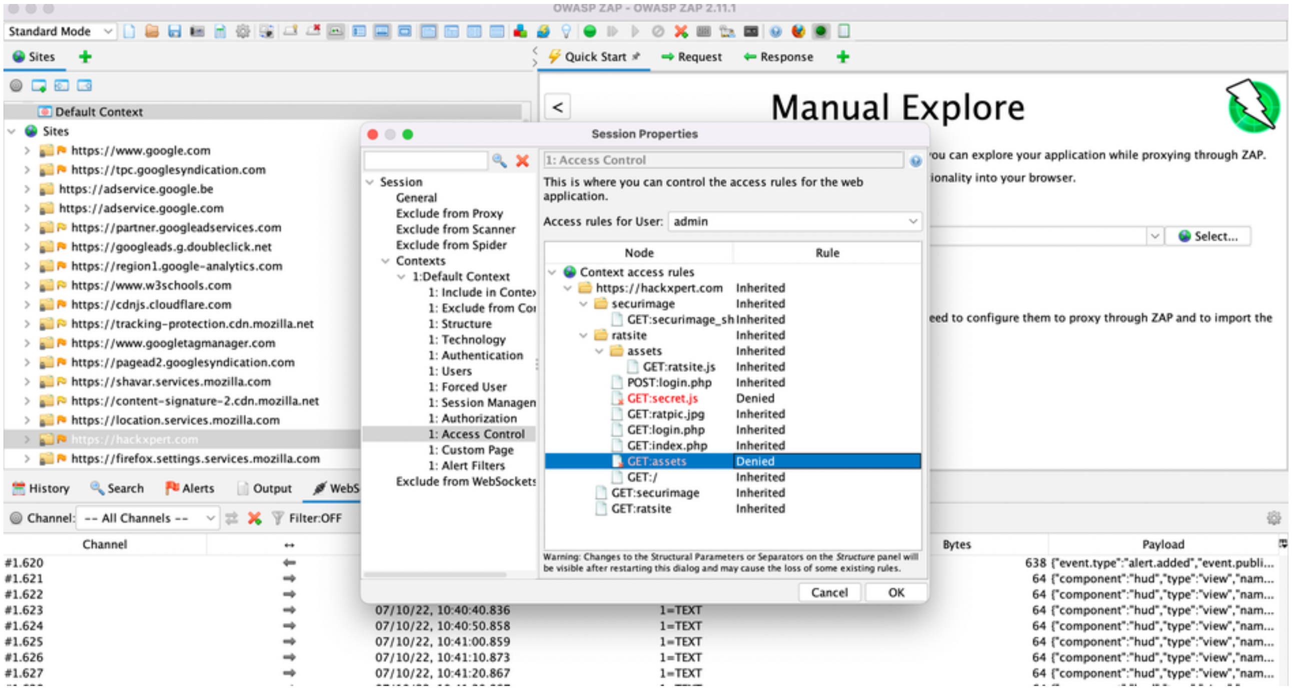
Regex
https://hackxpert.com.*

□ Remove Without Confirmation

```
.534    ➡                                                   64 {"con
.535    ➡                                                   64 {"con
.536    ➡                                                   64 {"con
.537    ➡  07/10/22, 10:38:50.791        1=TEXT             64 {"con
.538    ➡  07/10/22, 10:39:00.798        1=TEXT             64 {"con
539     ➡  07/10/22, 10:39:10.796        1=TEXT             64 {"con
```

And if you did everything well you should be able to set per specific Endpoint what a user can and cannot see this also is valid for an unauthenticated user.

And now it's all up to you because you'll have to set what a specific user is allowed to see and what you're not allowed to see. Make sure you set this up correctly before running because otherwise, your report will not be correct.


OWASP ZAP - OWASP ZAP 2.11.1
Standard Mode
Sites
Default Context
Sites
https://www.google.com
https://tpc.googlesyndication.com
https://adservice.google.be
https://adservice.google.com
https://partner.googleadservices.com
https://googleads.g.doubleclick.net
https://region1.google-analytics.com
https://www.w3schools.com
https://cdnjs.cloudflare.com
https://tracking-protection.cdn.mozilla.net
https://www.googletagmanager.com
https://pagead2.googlesyndication.com
https://shavar.services.mozilla.com
https://content-signature-2.cdn.mozilla.net
https://location.services.mozilla.com
https://hackxpert.com
https://firefox.settings.services.mozilla.com
History
Search
Alerts
Output
WebS
Channel: -- All Channels --
Filter:OFF
Channel
Quick Start
Request
Response
Manual Explore
Select...
Session Properties
Session
General
Exclude from Proxy
Exclude from Scanner
Exclude from Spider
Contexts
1:Default Context
1: Include in Contex
1: Exclude from Co
1: Structure
1: Technology
1: Authentication
1: Users
1: Forced User
1: Session Managen
1: Authorization
1: Access Control
1: Custom Page
1: Alert Filters
Exclude from WebSockets
Cancel
OK
Bytes
Payload

1: Access Control

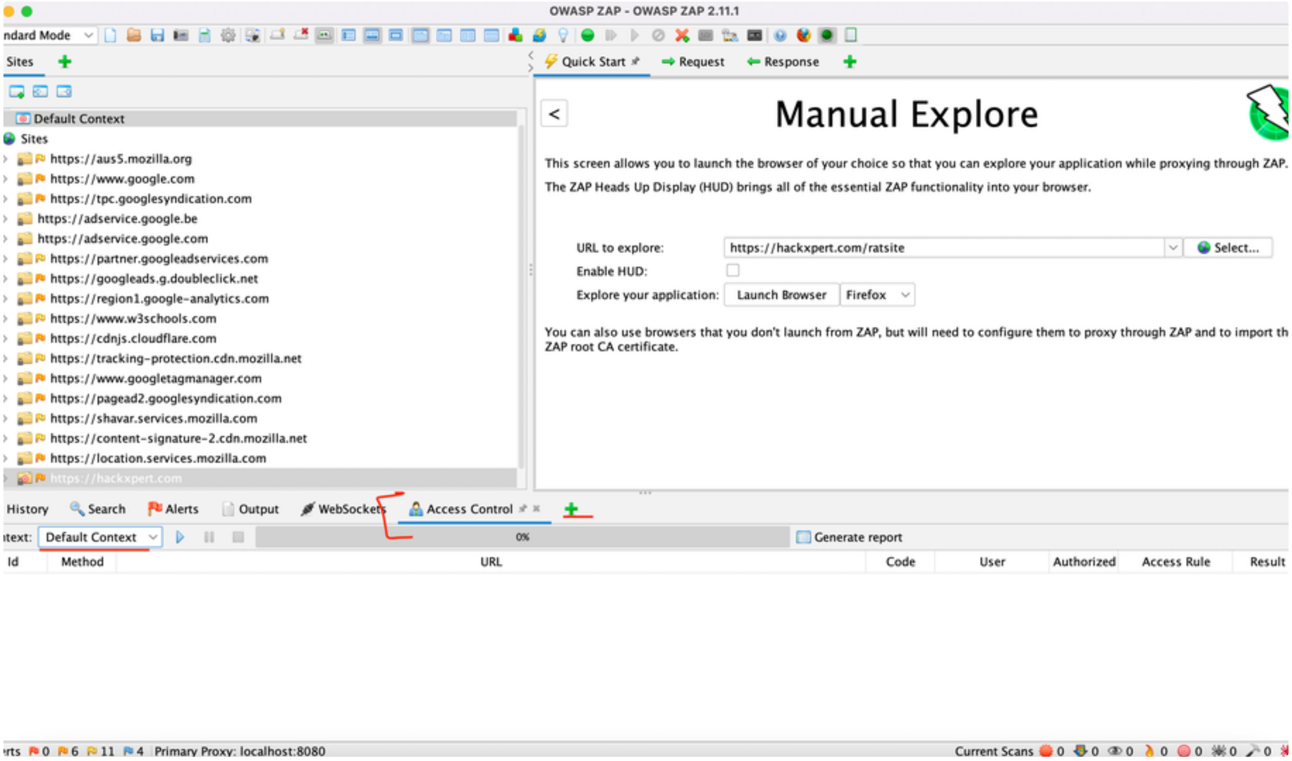
This is where you can control the access rules for the web application.

Access rules for User: admin

Node	Rule
Context access rules	
https://hackxpert.com	Inherited
securimage	Inherited
GET:securimage_sh	Inherited
ratsite	Inherited
assets	Inherited
GET:ratsite.js	Inherited
POST:login.php	Inherited
GET:secret.js	Denied
GET:ratpic.jpg	Inherited
GET:login.php	Inherited
GET:index.php	Inherited
GET:assets	Denied
GET:/	Inherited
GET:securimage	Inherited
GET:ratsite	Inherited

Warning: Changes to the Structural Parameters or Separators on the *Structure* panel will be visible after restarting this dialog and may cause the loss of some existing rules.

```
#1.620  ⬅                                          638 {"event.type":"alert.added","event.publi...
#1.621  ➡                                           64 {"component":"hud","type":"view","nam...
#1.622  ➡                                           64 {"component":"hud","type":"view","nam...
#1.623  ➡  07/10/22, 10:40:40.836      1=TEXT       64 {"component":"hud","type":"view","nam...
#1.624  ➡  07/10/22, 10:40:50.858      1=TEXT       64 {"component":"hud","type":"view","nam...
#1.625  ➡  07/10/22, 10:41:00.859      1=TEXT       64 {"component":"hud","type":"view","nam...
#1.626  ➡  07/10/22, 10:41:10.873      1=TEXT       64 {"component":"hud","type":"view","nam...
#1.627  ➡  07/10/22, 10:41:20.867      1=TEXT       64 {"component":"hud","type":"view","nam...
```



Default Context

Sites

- https://aus5.mozilla.org
- https://www.google.com
- https://tpc.googlesyndication.com
- https://adservice.google.be
- https://adservice.google.com
- https://partner.googleadservices.com
- https://googleads.g.doubleclick.net
- https://region1.google-analytics.com
- https://www.w3schools.com
- https://cdnjs.cloudflare.com
- https://tracking-protection.cdn.mozilla.net
- https://www.googletagmanager.com
- https://pagead2.googlesyndication.com
- https://shavar.services.mozilla.com
- https://content-signature-2.cdn.mozilla.net
- https://location.services.mozilla.com
- https://hackxpert.com

Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: https://hackxpert.com/ratsite Select...

Enable HUD: □

Explore your application: Launch Browser Firefox

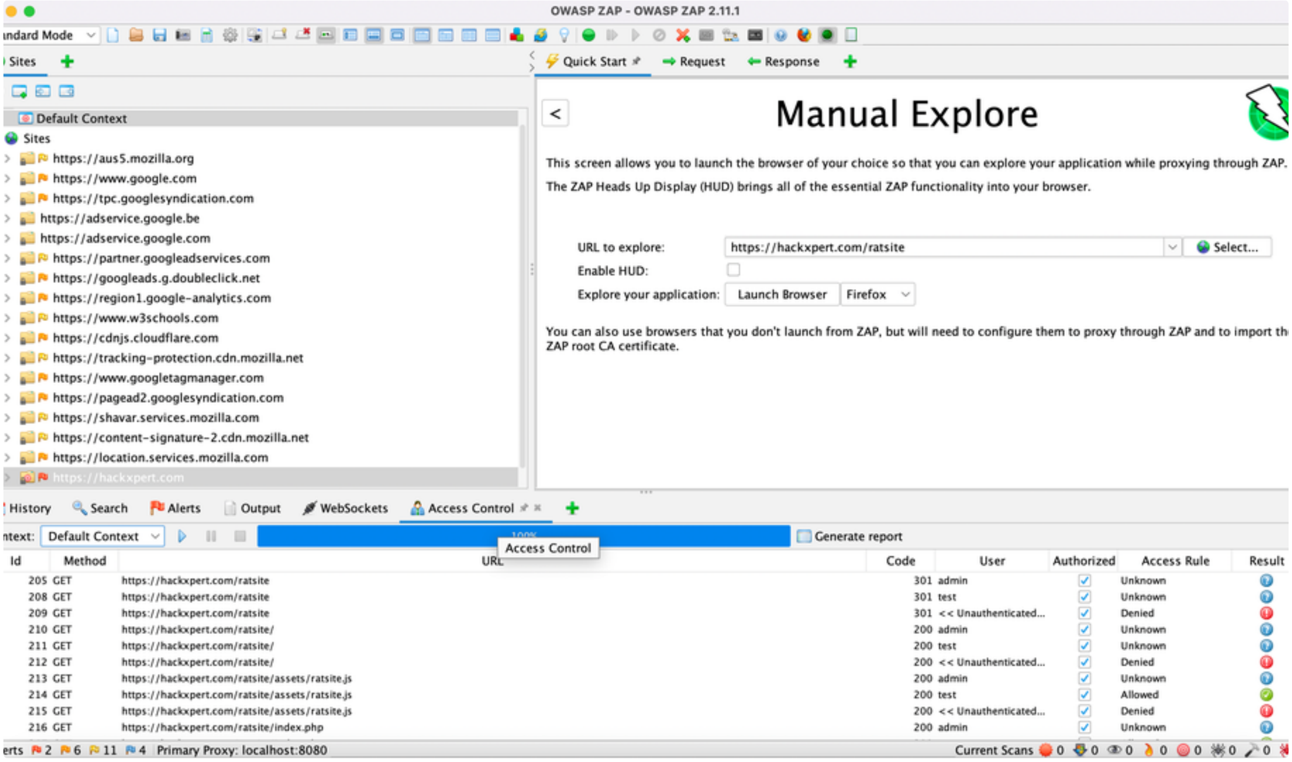
You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import th ZAP root CA certificate.

ntext: Default Context 0% □ Generate report

Id	Method	URL	Code	User	Authorized	Access Rule	Result

rts 0 6 11 4 Primary Proxy: localhost:8080

If you set everything up correctly you should now be able to run access control on a specific context. You should really know that every single context can be different and can have a different user set in them. This is important because we can separate it for example and broken access control testing and IDOR testing. Even with IDORs we can have a specific context for every user type.



Default Context

Sites

- https://aus5.mozilla.org
- https://www.google.com
- https://tpc.googlesyndication.com
- https://adservice.google.be
- https://adservice.google.com
- https://partner.googleadservices.com
- https://googleads.g.doubleclick.net
- https://region1.google-analytics.com
- https://www.w3schools.com
- https://cdnjs.cloudflare.com
- https://tracking-protection.cdn.mozilla.net
- https://www.googletagmanager.com
- https://pagead2.googlesyndication.com
- https://shavar.services.mozilla.com
- https://content-signature-2.cdn.mozilla.net
- https://location.services.mozilla.com
- https://hackxpert.com

Manual Explore

This screen allows you to launch the browser of your choice so that you can explore your application while proxying through ZAP.

The ZAP Heads Up Display (HUD) brings all of the essential ZAP functionality into your browser.

URL to explore: https://hackxpert.com/ratsite Select...

Enable HUD: □

Explore your application: Launch Browser Firefox

You can also use browsers that you don't launch from ZAP, but will need to configure them to proxy through ZAP and to import th ZAP root CA certificate.

ntext: Default Context 100% Access Control □ Generate report

Id	Method	URL	Code	User	Authorized	Access Rule	Result
205	GET	https://hackxpert.com/ratsite	301	admin	☑	Unknown	?
208	GET	https://hackxpert.com/ratsite	301	test	☑	Unknown	?
209	GET	https://hackxpert.com/ratsite	301	<< Unauthenticated...	☑	Denied	!
210	GET	https://hackxpert.com/ratsite/	200	admin	☑	Unknown	?
211	GET	https://hackxpert.com/ratsite/	200	test	☑	Unknown	?
212	GET	https://hackxpert.com/ratsite/	200	<< Unauthenticated...	☑	Denied	!
213	GET	https://hackxpert.com/ratsite/assets/ratsite.js	200	admin	☑	Unknown	?
214	GET	https://hackxpert.com/ratsite/assets/ratsite.js	200	test	☑	Allowed	✓
215	GET	https://hackxpert.com/ratsite/assets/ratsite.js	200	<< Unauthenticated...	☑	Denied	!
216	GET	https://hackxpert.com/ratsite/index.php	200	admin	☑	Unknown	?

erts 2 6 11 4 Primary Proxy: localhost:8080

So as you can see this is a really powerful tool that you can run over and over and over again but you really have to take the time to set this up correctly. Every single build can now easily be tested.