Falcon Auth2

Federico Caselli

Jul 26, 2020

CONTENTS:

Falcon authentication middleware that supports multiple authentication schemes.

CHAPTER

ONE

USER GUIDE

1.1 Install

```
$ pip install falcon-auth2
```

1.2 Usage

This package provides a falcon middleware to authenticate incoming requests using the selected authentication backend. The middleware allows excluding some routes or method from authentication. After a successful authentication the middleware adds the user identified by the request to the `request context`.

```
import falcon
from falcon_auth2 import AuthMiddleware
from falcon_auth2.backends import BasicAuthBackend

def user_loader(attributes, user, password):
    if authenticate(user, password):
        return {"username": user}
    return None

auth_backend = BasicAuthBackend(user_loader)
auth_middleware = AuthMiddleware(auth_backend)
# use falcon.API in falcon 2
app = falcon.App(middleware=[auth_middleware])

class HelloResource:
    def on_get(self, req, resp):
        # req.context.auth is of the form:
        #
        #   {
        #       'backend': <instance of the backend that performed the authentication>
↪,
        #       'user': <user object retrieved from the user_loader callable>,
        #       '<backend specific item>': <some extra data from the backend>,
        #       ...
        #   }
        user = req.context.auth["user"]
        resp.media = {"message": f"Hello {user['username']}"}

app.add_route('/hello', HelloResource())
```

1.2.1 Override Authentication for a resource

The middleware allows each resource to customize the backend used for authentication or the excluded methods. A resource can also specify that does not need authentication.

```
from falcon_auth2 import HeaderGetter
from falcon_auth2.backends import GenericAuthBackend

class OtherResource:
    auth = {
        "backend": GenericAuthBackend(
            user_loader=lambda attr, user_header: user_header, getter=HeaderGetter(
↪"User")
        ),
        "exempt_methods": ["GET"],
    }

    def on_get(self, req, resp):
        resp.media = {"type": "No authentication for GET"}

    def on_post(self, req, resp):
        resp.media = {"info": f"User header {req.context.auth['user']}"}

app.add_route("/other", OtherResource())

class NoAuthResource:
    auth = {"auth_disabled": True}

    def on_get(self, req, resp):
        resp.media = "No auth in this resource"

    def on_post(self, req, resp):
        resp.media = "No auth in this resource"

app.add_route("/no-auth", NoAuthResource())
```

CHAPTER

TWO

API REFERENCE

2.1 Middleware

class falcon_auth2.**AuthMiddleware**(*backend: falcon_auth2.backends.base.AuthBackend*, ***, *exempt_templates: Iterable[str] = ()*, *exempt_methods: Iterable[str] = 'OPTIONS'*, *context_attr: str = 'auth'*)

Falcon middleware that can be used to authenticate a request.

The authentication backend returns an authenticated user which is then set by default in `request.context.auth["user"]`. In case of errors `falcon.HTTPUnauthorized` is raised. In addition to the `"user"`, the authenticating backend is returned in the `"backend"` key. A backend may also store additional information in this dict.

This middleware supports a global authentication configuration using provided *AuthBackend*, as well as per resource configuration. To override the authentication configuration a resource can specify an optional `auth` attribute the override properties. The `auth` attribute is a dict that can specify the keys:

- `auth_disabled` boolean. `True` disables the authentication on the resource.
- `exempt_methods` iterable that overrides the global `exempt_methods` for the resource.
- `backend` backend instace that overrides the globally configured backend used to handle the authentication of the request.

Parameters **backend** (*AuthBackend*) – The default auth backend to be used to authenticate requests. A resource can override this value by providing a `backend` key in its `auth` attribute

Keyword Arguments

- **exempt_templates** (*Iterable[str], optional*) – A list of paths templates to be excluded from the authentication. This value cannot be overridden by a resource. Defaults to `()`.
- **exempt_methods** (*Iterable[str], optional*) – A list of http methods to be excluded from the authentication. A resource can override this value by providing a `exempt_methods` key in its `auth` attribute. Defaults to `("OPTIONS",)`.
- **context_attr** (*str, optional*) – The attribute of the `req.context` object that will store the authentication information after a successful precessing. Defaults to `"auth"`.

process_resource(*req: falcon.request.Request*, *resp: falcon.response.Response*, *resource: Any*, *params: dict*)

Called by falcon when processing a resource.

It will obtain the configuration to use on the resource and, if required, call the provided backend to authenticate the request.

2.2 Backends implementations

2.2.1 Base classes

class falcon_auth2.backends.**AuthBackend**

Base class that defines the signature of the *authenticate()* method.

Backend must subclass of this class to be used by the *AuthMiddleware* middleware.

abstract authenticate(*attributes: falcon_auth2.utils.RequestAttributes*) → dict

Authenticates the request and returns the authenticated user.

If a request cannot be authenticated a backed should raise:

- *AuthenticationFailure* to indicate that the request can be handled by this backend, but the authentication fails.
- *BackendNotApplicable* if the provided request cannot be handled by this backend. This is usually raised by the *Getter* used by the backend to process the request.
- *UserNotFound* when no user could be loaded with the provided credentials.

Parameters **attributes** (RequestAttributes) – The current request attributes. It's a named tuple which contains the falcon request and response objects, the activated resource and the parameters matched in the url.

Returns *dict* – A dictionary with a required `"user"` key containing the authenticated user. This dictionary may optionally contain additional keys specific to this backend. If the `"backend"` key is specified, the middleware will not override it.

class falcon_auth2.backends.**BaseAuthBackend**(*user_loader: Callable*, *, *challenges: Optional[Iterable[str]] = None*)

Utility class that handles calling a provided callable to load an user from the authentication information of the request in the *load_user()* method.

Parameters **user_loader** (*Callable*) – A callable object that is called with the *RequestAttributes* object as well as any relevant data extracted from the request by the backend. The arguments passed to `user_loader` will vary depending on the *AuthBackend*. It should return the user identified by the request, or `None` if no user could be not found.

Note: Exception raised in this callable are not handled directly, and are surfaced to falcon.

Keyword Arguments **challenges** (*Optional[Iterable[str]], optional*) – One or more authentication challenges to use as the value of the `WWW-Authenticate` header in case of errors. Defaults to `None`.

load_user(*attributes: falcon_auth2.utils.RequestAttributes*, **args*, ***kwargs*) → Any

Invokes the provided `user_loader` callable to allow the app to retrieve the user record. If no such record is found, raises a *UserNotFound* exception.

Parameters

- **attributes** (RequestAttributes) – The request attributes.
- ***args** – Positional arguments to pass to the `user_loader` callable.
- ****kwargs** – Keyword arguments to pass to the `user_loader` callable.

Returns *Any* – The loaded user object returned by `user_loader`.

2.2.2 Authentication Backends

class falcon_auth2.backends.**GenericAuthBackend**(*user_loader: Callable*, *getter: falcon_auth2.getter.Getter*, **, payload_key: Optional[str] = None*, *challenges: Optional[Iterable[str]] = None*)

Generic authentication backend that delegates the verification of the authentication information retried from the request by the provided `getter` to the `user_loader` callable.

This backend can be used to quickly implement custom authentication schemes or as an adapter to other authentication libraries.

Depending on the `getter` provided, this backend can be used to authenticate the an user using a session cookie or using a parameter as token.

Parameters

- **user_loader** (*Callable*) – A callable object that is called with the *RequestAttributes* object and the information extracted from the request using the provided `getter`. It should return the user identified by the request, or `None` if no user could be not found.

  Note: Exception raised in this callable are not handled directly, and are surfaced to falcon.

- **getter** (`Getter`) – Getter used to extract the authentication information from the request. The returned value is passed to the `user_loader` callable.

Keyword Arguments

- **payload_key** (*Optional[str], optional*) – It defines a key in the dict returned by the `authentication()` method that will contain data obtained from the request by the `getter`. Use `None` to disable this functionality. Defaults to `None`.
- **challenges** (*Optional[Iterable[str]], optional*) – One or more authentication challenges to use as the value of the `WWW-Authenticate` header in case of errors. Defaults to `None`.

authenticate(*attributes: falcon_auth2.utils.RequestAttributes*) → dict

Authenticates the request and returns the authenticated user.

class falcon_auth2.backends.**BasicAuthBackend**(*user_loader: Callable*, **, auth_header_type: str = 'Basic'*, *getter: Optional[falcon_auth2.getter.Getter] = None*)

Implements the 'Basic' HTTP Authentication Scheme.

Clients should authenticate by passing the credential in the format `username:password` encoded in `base64` in the `Authorization` HTTP header, prepending it with the type specified in the setting `auth_header_type`. For example, the user `"Aladdin"` would provide his password, `"open sesame"`, with the header:

```
Authorization: Basic QWxhZGRpbjpvcGVuIHNlc2FtZQ==
```

Parameters **user_loader** (*Callable*) – A callable object that is called with the `RequestAttributes` object and the username and password credentials extracted from the request using the provided `getter`. It should return the user identified by the request, or `None` if no user could be not found.

Note: Exception raised in this callable are not handled directly, and are surfaced to falcon.

Keyword Arguments

- **auth_header_type** (*string, optional*) – The type of authentication required in the `Authorization` header. This value is added to the `challenges` in case of errors. Defaults to `"Basic"`.

  Note: When passing a custom getter this value is only used to generate the `challenges`, since the getter will be used to obtain the credentials to authenticate.

- **getter** (*Optional[Getter]*) – Getter used to extract the authentication information from the request. When using a custom getter, the returned value must be a `base64` encoded string with the credentials in the format `username:password`. Defaults to *AuthHeaderGetter* initialized with the provided `auth_header_type`.

authenticate(*attributes: falcon_auth2.utils.RequestAttributes*) → dict
Authenticates the request and returns the authenticated user.

class falcon_auth2.backends.**NoAuthBackend**(*user_loader: Callable, *, challenges: Optional[Iterable[str]] = None*)
No authentication backend.

This backend does not perform any authentication check. It can be used with the *MultiAuthBackend* in order to provide a fallback for an unauthenticated user or to implement a complitely custom authentication workflow.

Parameters **user_loader** (*Callable*) – A callable object that is called with the *RequestAttributes* object and returns a default unauthenticated user (alternatively the user identified by a custom authentication workflow) or `None` if no user could be not found.

Note: Exception raised in this callable are not handled directly, and are surfaced to falcon.

Keyword Arguments **challenges** (*Optional[Iterable[str]], optional*) – One or more authentication challenges to use as the value of the `WWW-Authenticate` header in case of errors. Defaults to `None`.

authenticate(*attributes: falcon_auth2.utils.RequestAttributes*) → dict
Authenticates the request and returns the authenticated user.

2.2.3 Meta Backends

class falcon_auth2.backends.**CallBackBackend**(*backend: falcon_auth2.backends.base.AuthBackend, *, on_success: Optional[Callable] = None, on_failure: Optional[Callable] = None*)
Meta-Backend used to notify when another backend has success and/or fails to authenticate a request.

This backend delegates all the authentication actions to the provided `backend`.

Parameters **backend** (*AuthBackend*) – The backend that will be used to authenticate the requests.

Keyword Arguments

- **on_success** (*Optional[Callable], optional*) – Callable object that will be invoked with the *RequestAttributes*, the `backend` and the authentication result (the dict that will be placed in the request context by the middleware) after a successful request authentication. Defaults to `None`.
- **on_failure** (*Optional[Callable], optional*) – Callable object that will be invoked with the *RequestAttributes*, the `backend` and the raised exception after a failed request authentication. Defaults to `None`.

Note: This method cannot be used to suppress the exception raised by the `backend` that will be propagated after the invocation ends, but the callable can choose to raise a different exception instead.

---

authenticate(*attributes: falcon_auth2.utils.RequestAttributes*) → dict
Authenticates the request and returns the authenticated user.

class falcon_auth2.backends.**MultiAuthBackend**(*backends: Iterable[falcon_auth2.backends.base.AuthBackend]*, *, *continue_on: Optional[Callable] = None*)
Meta-Backend used to combine multiple authentication backends.

This backend successfully authenticates a request if one of the provided backends can authenticate the request or raises *BackendNotApplicable* if no backend can authenticate it.

This backend delegates all the authentication actions to the provided `backends`.

Parameters **backends** (*Iterable[AuthBackend]*) – The backends to use. They will be used in order.

Keyword Arguments **continue_on** (*Callable*) – A callable object that is called when a backend raises an exception. It should return `True` if processing should continue to the next backend or `False` if it should stop by re-raising the backend exception. The callable takes the backend and the raised exception as parameters. The default implementation continues processing if any backend raises a *BackendNotApplicable* exception.

Note: This callable is only invoked if a backend raises an instance of `HTTPUnauthorized` or one of it's subclasses. All other exception types are propagated.

---

authenticate(*attributes: falcon_auth2.utils.RequestAttributes*)
Authenticates the request and returns the authenticated user.

2.3 Getter

A "Getter" is an instance used by a backend to extract the authentication information from a falcon `Request`.

class falcon_auth2.**Getter**
Represents a class that extracts authentication information from a request.

abstract load(*req: falcon.request.Request*, *, *challenges: Optional[Iterable[str]] = None*) → str
Loads the specified attribute from the provided request.

If a getter cannot be used with the current request, a *BackendNotApplicable* is raised. The `challenges`, when provided, will be added to `WWW-Authenticate` header in case of error.

Parameters **req** (*Request*) – The current request.

Keyword Arguments **challenges** (*Optional[Iterable[str]], optional*) – One or more authentication challenges to use as the value of the WWW-Authenticate header in case of errors.

Returns *str* – The loaded data, in case of success.

class falcon_auth2.**HeaderGetter**(*header_key: str*)

Returns the specified header from a request.

Parameters **header_key** (*str*) – the name of the header to load.

load(*req: falcon.request.Request*, *, *challenges: Optional[Iterable[str]] = None*) → str

Loads the header from the provided request

class falcon_auth2.**AuthHeaderGetter**(*auth_header_type: str*, *, *header_key: str = 'Authorization'*)

Returns the auth header from a request, checking that it in the form `<auth_header_type> value`.

Parameters **auth_header_type** (*str*) – The type of the auth header. Common values are "Basic", "Bearer".

Keyword Arguments **header_key** (*str, optional*) – The name of the header to load. Defaults to "Authorization".

load(*req: falcon.request.Request*, *, *challenges: Optional[Iterable[str]] = None*) → str

Loads the auth header from the provided request

class falcon_auth2.**ParamGetter**(*param_name: str*)

Returns the specified parameter from the request.

If the parameter appears multiple times an error will be raised.

Note: When the falcon Request option RequestOptions.auto_parse_form_urlencoded is set to True, this getter can also retrieve parameter in the body of a form-urlencoded request.

Parameters **param_name** (*str*) – the name of the param to load.

load(*req: falcon.request.Request*, *, *challenges: Optional[Iterable[str]] = None*) → str

Loads the parameter from the provided request

class falcon_auth2.**CookieGetter**(*cookie_name: str*)

Returns the specified cookie from the request.

If the cookie appears multiple times an error will be raised.

Parameters **cookie_name** (*str*) – the name of the cookie to load.

load(*req: falcon.request.Request*, *, *challenges: Optional[Iterable[str]] = None*) → str

Loads the cookie from the provided request

class falcon_auth2.**MultiGetter**(*getters: Iterable[falcon_auth2.getter.Getter]*)

Combines multiple getters. This is useful if a value can be passed in multiple ways to the server, like using an header or a query parameter.

Will use the first value successfully returned, ignoring all *BackendNotApplicable* exceptions raised by the previously tried getters. If no getter can return a valid value an exception will only be raised.

Parameters **getters** (*Iterable[Getter]*) – The getters to use. They will be tried in order and the first value successfully returned is used.

load(*req: falcon.request.Request*, *, *challenges: Optional[Iterable[str]] = None*) → str
Loads the value from the provided request using the provided getters

2.4 Exceptions

All exceptions are subclasses of falcon `HTTPUnauthorized`.

class falcon_auth2.**AuthenticationFailure**(*title=None*, *description=None*, *challenges=None*, *headers=None*, ***kwargs*)
Raised when an authentication backend fails to authenticate a syntactically correct request.

This will terminate the request with status 401 if no other logic is present.

class falcon_auth2.**BackendNotApplicable**(*title=None*, *description=None*, *challenges=None*, *headers=None*, ***kwargs*)
Raised when a request is not understood by an authentication backend. This may indicate that the request is intended for another backend.

This will terminate the request with status 401 if no other logic is present.

class falcon_auth2.**UserNotFound**(*title=None*, *description=None*, *challenges=None*, *headers=None*, ***kwargs*)
Raised when the `user_loader` callable of an authentication backend cannot load an user with the received payload. This may indicate that the request is intended for another backend.

This will terminate the request with status 401 if no other logic is present.

2.5 Utils

class falcon_auth2.**RequestAttributes**(*req: falcon.request.Request*, *resp: falcon.response.Response*, *resource: Any*, *params: dict*)
Named tuple that is passed to the backend *`authenticate()`* when a request is performed.

params: dict
The parameters of passed in the url.

req: falcon.request.Request
The falcon request.

resource: Any
The falcon responder resource.

resp: falcon.response.Response
The falcon response.

INDEX