

This document lists all the ABAC tests performed on the generated engine described in our paper "A Low-Code Platform for Generating Secure by Design Enterprise Services" and the corresponding results. Both of them are listed in a tests-per-resource fashion. For all the following cases, the Response Code 200 is the standard HTTP "200 OK" response, the Response Code 401 is the "401 UNAUTHORIZED" one and 403 is the standard "403 FORBIDDEN" HTTP code.

Account Resource Tests

Table 1 Account Resource Tests

Test Nr.	HTTP Verb	Test Description	Response Code
1	POST	Create a user account as guest Subject and account role set to "customer".	200
2	POST	Create a user account as guest Subject and account role set to "manager".	403
3	POST	Create a user account as authenticated Subject and account role set to "customer".	200
4	POST	Create a user account as authenticated Subject and account role set to "manager".	403
5	POST	Create a user account as Subject that provides wrong credentials.	401
6	GET	Get the list of all user accounts as guest.	401
7	GET	Get personal user account data.	200
8	GET	Get a specific user account as guest Subject.	401
9	GET	Get the list of all user accounts as authenticated Subject with role "customer".	200
10	GET	Get the list of all user accounts as authenticated Subject with role "manager".	200
11	GET	Get as authenticated manager Subject the user account of another user.	200
12	GET	Get as authenticated customer Subject the user account of another user.	403
13	PUT	Update a user account as Subject that provides wrong credentials.	401
14	PUT	Update a user account as Subject that provides non-existing credentials.	401
15	PUT	As an authenticated manager Subject update another user's account.	403
16	PUT	Update personal user account data and account role property is set to "customer".	200
17	PUT	Update a user account as a guest Subject.	401
18	PUT	Update as authenticated customer Subject the personal account and set the role property to "manager".	403
19	PUT	Update as authenticated manager Subject the personal account data and set the role property (again) to "manager".	200

20	DEL	Delete as authenticated customer Subject the user account of another user.	403
21	DEL	Delete as authenticated customer Subject the personal user account.	403
22	DEL	Delete as guest Subject the account of a user.	401
23	DEL	Delete as authenticated manager Subject the account of another user.	200
24	DEL	Delete as authenticated manager Subject the personal account.	200

Table 2 Hypermedia links provided for Account Resource Tests with HTTP OK 200 code

Test Nr.	HTTP Verb	Hypermedia Links
1	POST	POST new account
3	POST	POST new account, GET account list
7	GET	GET/PUT personal account, POST new account, POST new order (customer case), GET personal account's orders, GET account's products (manager case), POST new Product (manager case)
9	GET	GET account list, POST new account, GET personal account
10	GET	GET account list, POST new account, GET personal account, GET account (one link for each other user)
11	GET	GET/DELETE specific user's account, GET all products of the account, POST new product, GET all account's orders, POST new account, GET account list.
16	PUT	PUT personal account, GET products list, GET orders list, POST new order, GET account list, POST new account.
19	PUT	GET/PUT/DELETE personal account, GET products list, POST new product, GET orders list, GET accounts list, POST new account.
23	DEL	POST new account, GET account list.
24	DEL	POST new account, GET account list.

Product Resource Tests

Table 3 Product Resource Tests

Test Nr.	HTTP Verb	Test Description	Response Code
1	POST	Create a product as guest Subject	401
2	POST	Create a product as customer Subject	403
3	POST	Create a product as manager Subject	200
4	GET	Get a draft product as guest Subject	403
5	GET	Get a draft product as customer Subject	403
6	GET	Get a draft product as manager Subject	200
7	GET	Get an available product as guest Subject	200
8	GET	Get an available product as customer Subject	200

9	GET	Get an available product as manager Subject	200
10	GET	Get list of products as guest Subject	200
11	GET	Get list of products as customer Subject	200
12	GET	Get list of products as manager Subject	200
13	PUT	Update a draft product as guest Subject	401
14	PUT	Update a draft product as customer Subject	403
15	PUT	Update a draft product as manager Subject	200
16	PUT	Update an available product as guest Subject	401
17	PUT	Update an available product as customer Subject	403
18	PUT	Update an available product as manager Subject	200
19	DEL	Delete a product (regardless its status) as guest Subject	401
20	DEL	Delete a product (regardless its status) as customer Subject	403
21	DEL	Delete a product (regardless its status) as manager Subject	200

Table 4 Hypermedia links provided for Product Resource Tests with HTTP OK 200 code

Test Nr.	HTTP Verb	Hypermedia Links
3	POST	GET products list, POST a new product, GET/PUT/DELETE the created product, GET/PUT/DELETE owned account
6	GET	GET/PUT/DELETE the draft product, GET this product's reviews list, POST a new product, GET owned account products list, GET/PUT/DELETE owned account.
7	GET	GET the same product, GET this product's reviews list, GET the products list of the related account.
8	GET	GET the same product, GET this product's reviews list, POST a review for this product, GET the products list of the related account.
9	GET	GET/PUT/DELETE the same product, GET reviews list for this product, POST a new product, GET products list of owned account, GET/PUT/DELETE owned account
10	GET	GET products list of the related account, one GET link for every product with status available.
11	GET	GET products list of the related account, one GET link for every product with status available.
12	GET	GET products list of owned account, POST a new product, one GET link for every product regardless its status
15	PUT	GET/PUT/DELETE the same product, GET reviews list of this product, POST a new product, GET products list of owned account.
18	PUT	GET/PUT/DELETE the same product, GET reviews list of this product, POST a new product, GET products list of owned account.
21	DEL	POST a new product, GET products list of owned account.

Order Resource Tests

Table 5 Order Resource Tests

Test Nr.	HTTP Verb	Test Description	Response Code
1	POST	Create an order as guest Subject	401
2	POST	Create an order as manager Subject	403
3	POST	Create an order as customer Subject	200
4	PUT	Update an order as guest Subject	401
5	PUT	Update an order as manager Subject	403
6	PUT	Update an order as customer Subject who is not the owner of the order.	403
7	PUT	Update an order as customer Subject who is the owner of the order.	200
8	GET	Get an order as guest Subject	401
9	GET	Get an order as customer Subject who is not the owner of the order	403
10	GET	Get an order as guest Subject who is the owner of the order	200
11	GET	Get an order as manager Subject	200
12	DEL	Delete an order as guest Subject	401
13	DEL	Delete an order as customer Subject who is not owner of the order	403
14	DEL	Delete an order as customer Subject who is the owner of the order	403
15	DEL	Delete an order as manager Subject	200

Table 6 Hypermedia links provided for Order Resource Tests with HTTP OK 200 code

Test Nr.	HTTP Verb	Hypermedia Links
3	POST	GET orders list of owned account, POST a new order, GET/PUT the created order, GET/PUT owned account
7	PUT	GET/PUT the same order, GET products list of this order, POST a new order, GET orders list of owned account
10	GET	GET/PUT the same order, GET products list of this order, POST a new order, GET orders list of owned account, GET/PUT owned account
11	GET	GET/DELETE the same order, GET products list of this order, GET orders list of the related account, GET/DELETE the related account.
15	DEL	GET orders list of the related account

Review Resource Tests

Table 7 Review Resource Tests

Test Nr.	HTTP Verb	Test Description	Response Code
1	POST	Create a review as guest Subject for a draft product	401
2	POST	Create a review as customer Subject for a draft product	403
3	POST	Create a review as manager Subject for a draft product	403
4	POST	Create a review as guest Subject for an available product	401
5	POST	Create a review as manager Subject for an available product	403
6	POST	Create a review as customer Subject for an available product	200
7	GET	Get a review as guest Subject for a draft product	403
8	GET	Get a review as customer Subject who is not the owner of the review for a draft product	403
9	GET	Get a review as customer Subject who is the owner of the review for a draft product	200
10	GET	Get a review as manager Subject for a draft product	200
11	GET	Get a review as guest Subject for an available product	200
12	GET	Get a review as customer Subject who is not the owner of the review for an available product	200
13	GET	Get a review as customer Subject who is the owner of the review for an available product	200
14	GET	Get a review as manager Subject for an available product	200
15	PUT	Update a review as guest Subject for a draft product	401
16	PUT	Update a review as customer Subject who is not the owner of the review for a draft product	403
17	PUT	Update a review as customer Subject who is the owner of the review for a draft product	200
18	PUT	Update a review as manager Subject for a draft product	403
19	PUT	Update a review as guest Subject for an available product	401
20	PUT	Update a review as customer Subject who is not the owner of the review for an available product	403
21	PUT	Update a review as customer Subject who is the owner of the review for an available product	200
22	PUT	Update a review as manager Subject for an available product	403
23	DEL	Delete a review as guest Subject regardless the product's status	401
24	DEL	Delete a review as customer Subject who is not the owner of the review, regardless the product's status	403
25	DEL	Delete a review as customer Subject who is the owner of the review, regardless the product's status	200
26	DEL	Delete a review as manager Subject, regardless the product's status	200

Table 8 Hypermedia links provided for Review Resource Tests with HTTP OK 200 code

Test Nr.	HTTP Verb	Hypermedia Links
6	POST	GET reviews list of this product, POST a new review, GET/PUT/DELETE the same review, GET the related product
9	GET	GET/PUT/DELETE the same review, GET reviews list of this product
10	GET	GET/DELETE the same review, Get reviews list of this product, GET/PUT/DELETE the related product.
11	GET	GET the same review, GET reviews list of this product, GET related product
12	GET	GET the same review, POST a new review for the related product, GET reviews list of the related product, GET the related product
13	GET	GET/PUT/DELETE the same review, POST a new review for the related product, GET reviews list of the related product, GET the related product
14	GET	GET/DELETE the same review, GET reviews list of the related product, GET/PUT/DELETE related product
17	PUT	GET/PUT/DELETE the same review, GET reviews list of the related product
21	PUT	GET/PUT/DELETE the same review, POST a new review for this product, GET reviews list for the related product
25	DEL	GET reviews list for the related product
26	DEL	GET reviews list for the related product