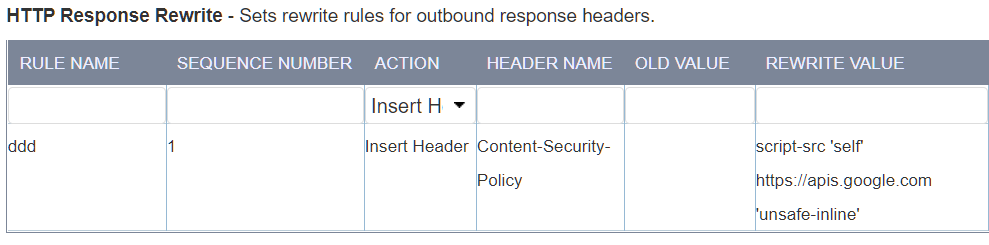
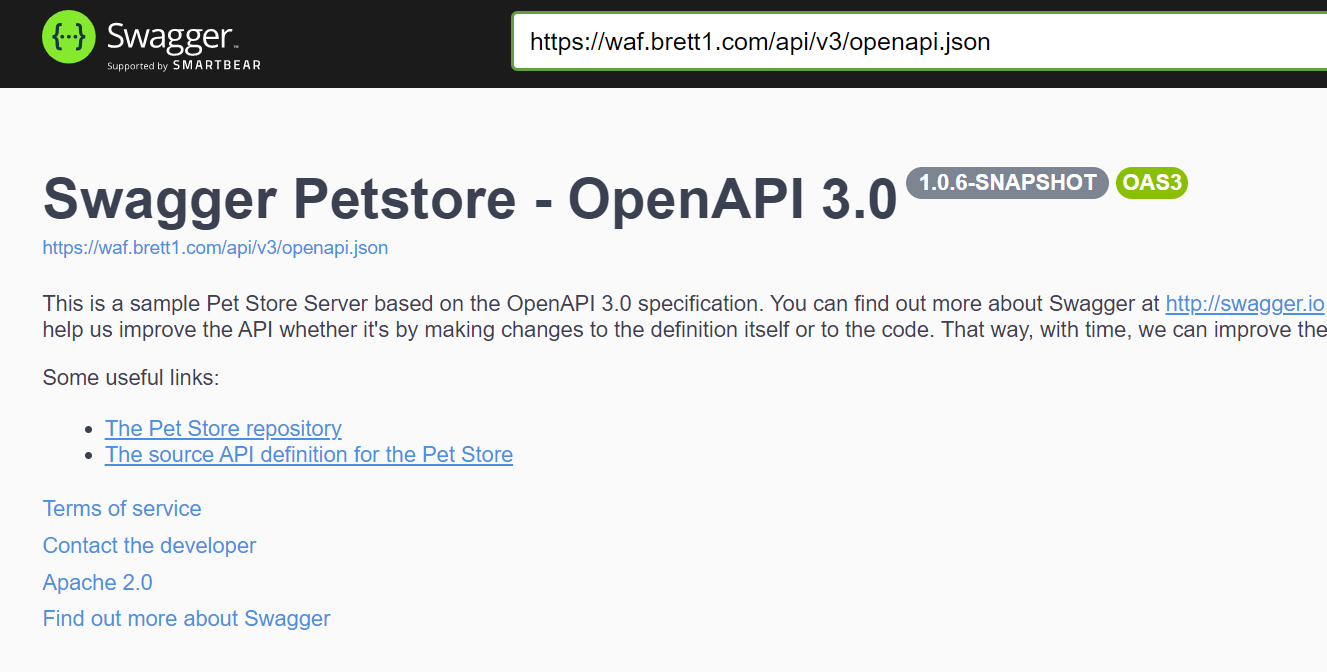
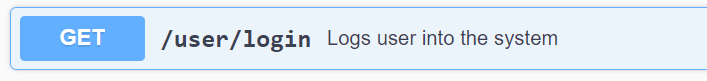
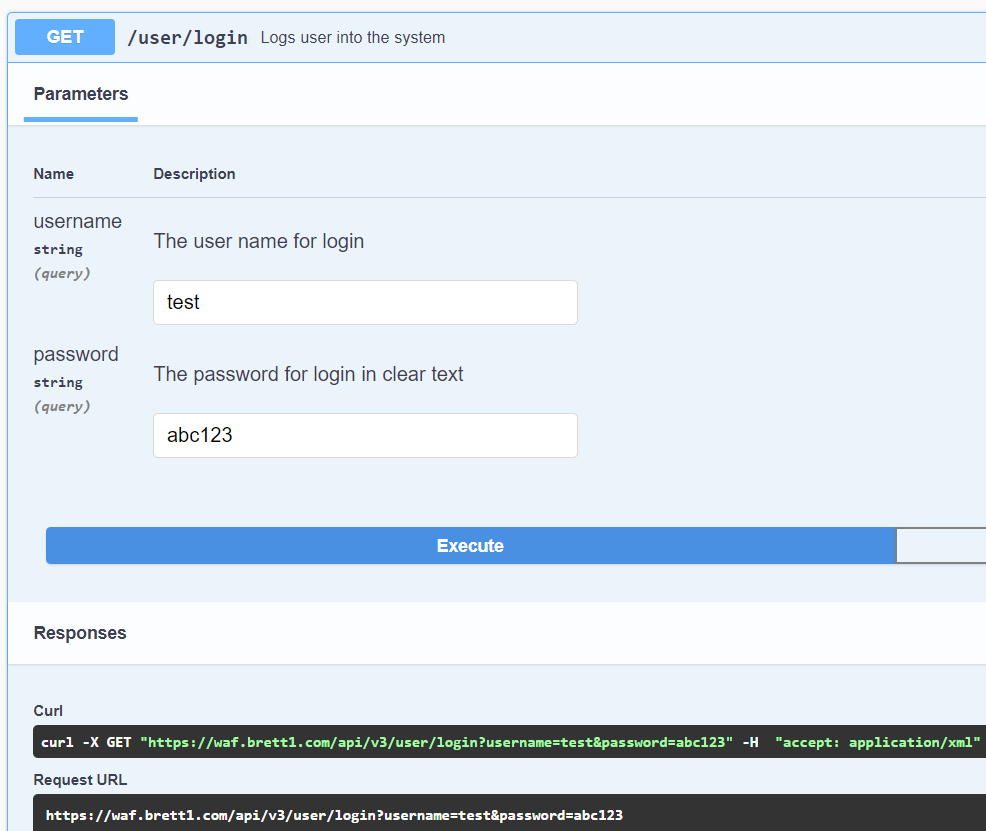
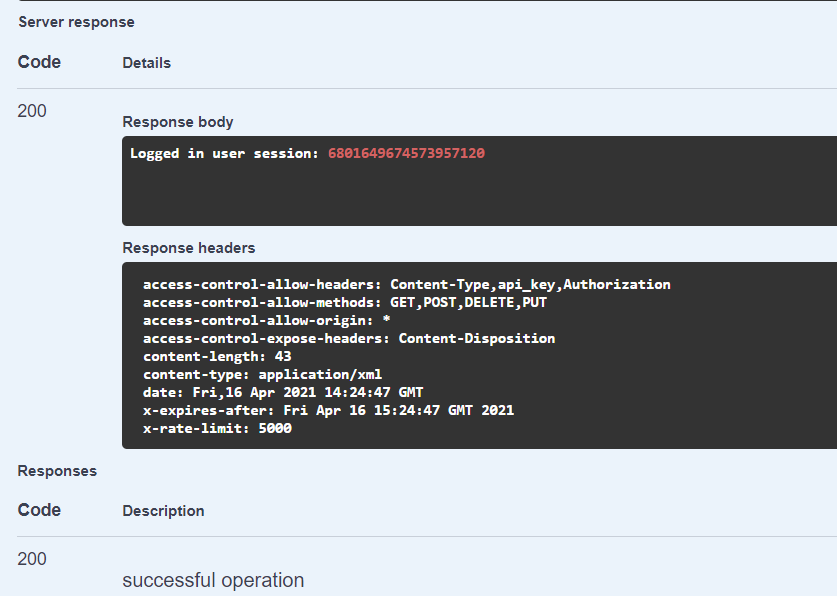
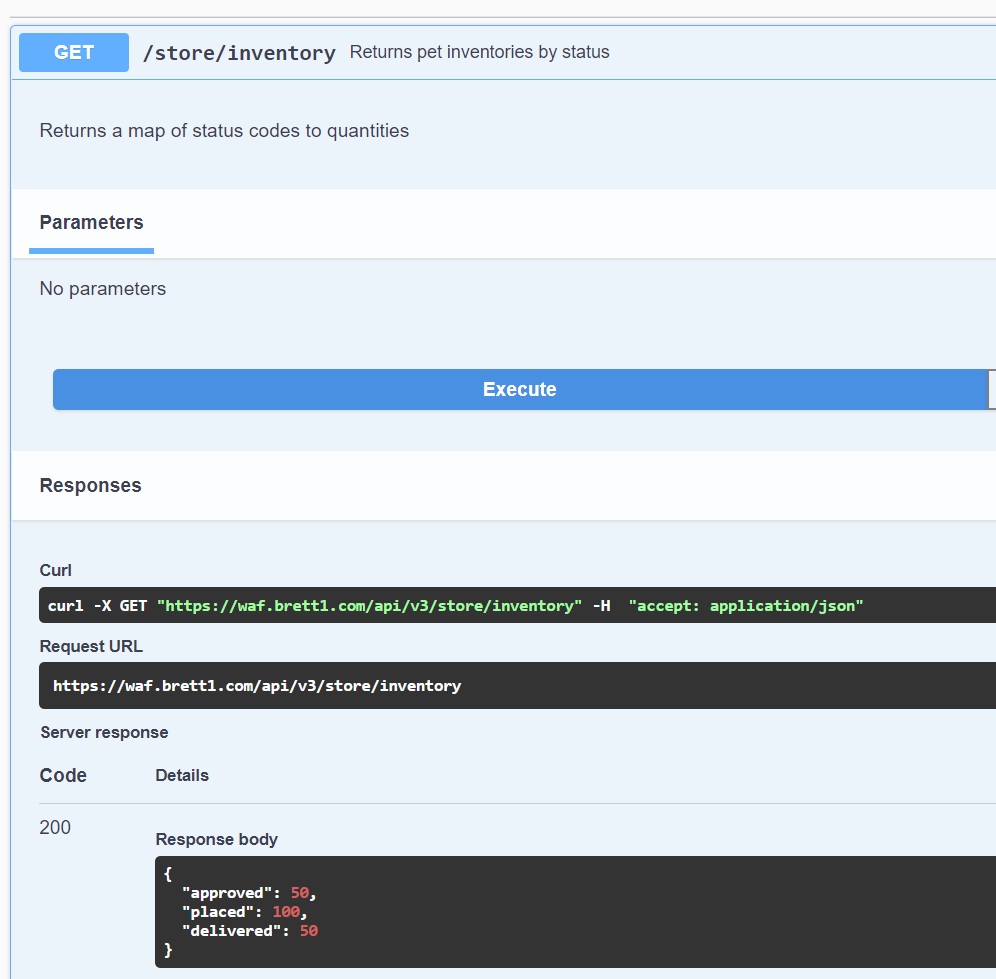
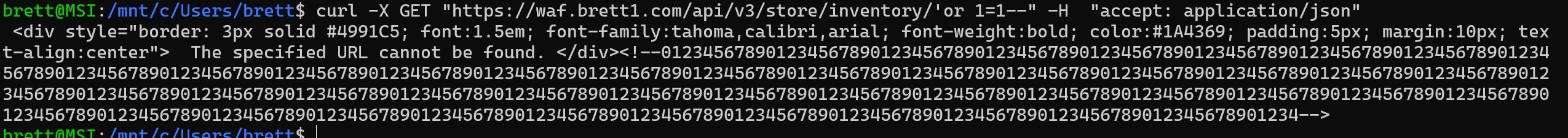
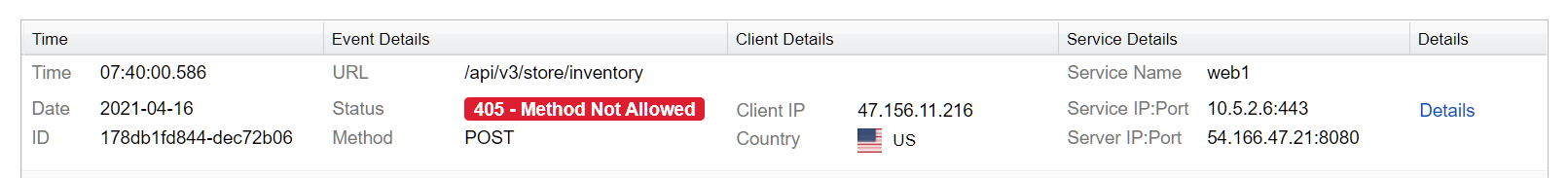
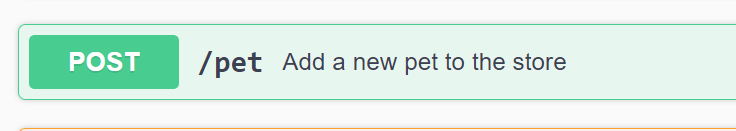
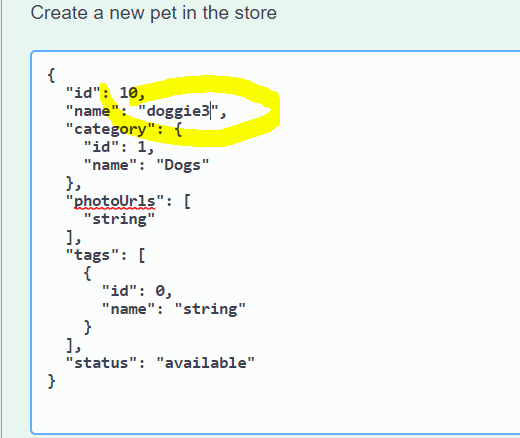
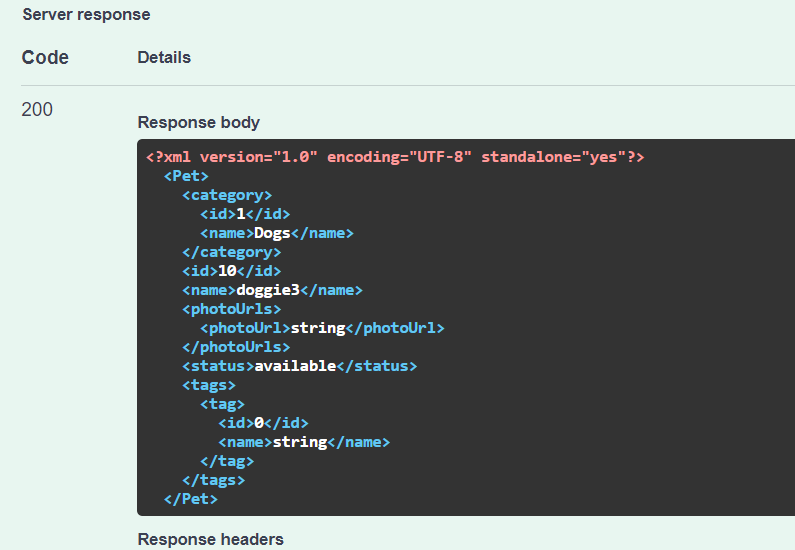


WAF Petstore API Lab Guide

1. Login to your WAF, then create a service listening on 443 with a server named badstore-origin.cudathon.com listening on 8080
2. WAF->Websites -> Website Translations add the following 
3. Download the Petstore API Swagger file from <https://petstore.swagger.io/v2/swagger.json> to your computer
4. WAF->Websites->JSON Security-JSON Security->Import API Spec and choose the swagger.json you downloaded
5. Browse to the Service and verify you see the web page 
6. Scroll down and click on GET user/login 
7. Click “Try it Out” and fill in username and passsword as test/abc123 then click execute 
8. Verify you see the following response ( session id will be different ) 
9. Scroll to STORE -> /store/inventory click Try it out, then execute, and it looks like this 
10. Copy the CURL command and try it out on your computer, make sure it works.
11. Then change the method to a POST and try that, and verify the WAF blocks the POST because POST is not allowed in the JSON Schema that you imported for the /store/inventory endpoint
12. Go back to doing a GET but add a SQL injection to the end of the GET verify the WAF blocks this  
13. Back in the browser, scroll to PET -> add pet to store and click it, then click try it out 
14. Give your pet a unique name and click execute 
15. Verify you get a json response similar to this 
16. Copy the CURL command Change the name to ‘or 1=1— which is s SQL injection and execute 
17. Verify the WAF blocked this 