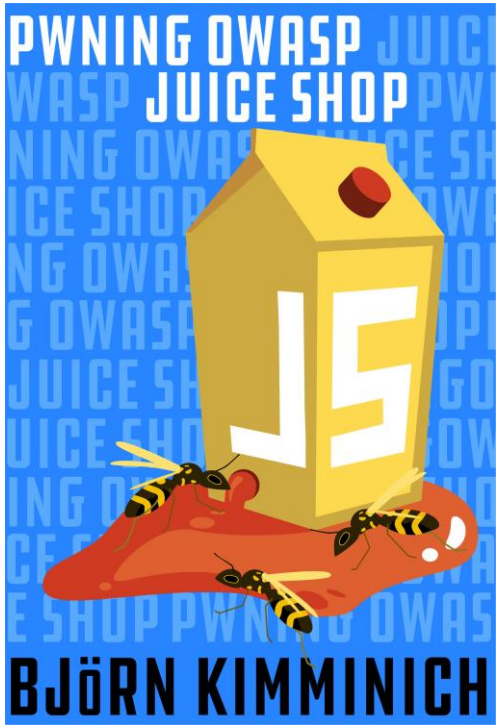
OWASP Juice Shop
Tutorial Series

Integration

Siphon juicy data in 5 different ways

Björn Kimminich

Integration specification and documentation



https://leanpub.com/juice-shop

https://pwning.owasp-juice.shop/appendix/**integration**.html

(1) Challenges API

- **/api/Challenges**
  - http://localhost:3000/api/Challenges

- Also available from centrally hosted demo instances
  - master branch / latest image: http://demo.owasp-juice.shop/api/Challenges
  - develop branch / snapshot image: http://preview.owasp-juice.shop/api/Challenges

- Sample consumers
  - https://www.npmjs.com/package/juice-shop-ctf-cli
  - http://juice-shop.github.io/juice-shop/#/5 (challenge count in slide title)

API Response (JSON Body)


```
{
   "status":"success",
   "data":[
      {
         "id":1,
         "key":"restfulXssChallenge",
         "name":"API-only XSS",
         "category":"XSS",
         "description":"Perform a <i>persisted</i> XSS attack with <code>&lt;iframe src=\"javascript:alert(`xss`)\"&gt
         "difficulty":3,
         "hint":"You need to work with the server-side API directly. Try different HTTP verbs on different entities ex
         "hintUrl":"https://pwning.owasp-juice.shop/part2/xss.html#perform-a-persisted-xss-attack-without-using-the-fr
         "solved":false,
         "disabledEnv":"Heroku",
         "createdAt":"2020-03-23T12:00:34.258Z",
         "updatedAt":"2020-03-23T12:00:34.258Z"
      },
      {
         "id":2,
         "key":"accessLogDisclosureChallenge",
         "name":"Access Log",
         "category":"Sensitive Data Exposure",
         "description":"Gain access to any access log file of the server.",
         "difficulty":4,
         "hint":"Who would want a server access log to be accessible through a web application?",
         "hintUrl":"https://pwning.owasp-juice.shop/part2/sensitive-data-exposure.html#gain-access-to-any-access-log-f
         "solved":false,
         "disabledEnv":null,
         "createdAt":"2020-03-23T12:00:34.259Z",
         "updatedAt":"2020-03-23T12:00:34.259Z"
      },
      {
        "...":"..."
      }
   ]
}
```

(2) Challenges Declaration File (YAML)

- **data/static/challenges.yml**
  - Single source of truth for all hacking challenges in the Juice Shop…
  - …which is used during server startup to populate the Challenges table…
  - …which is then exposed via the Challenges API endpoint

- Latest versions
  - master branch / latest image: https://raw.githubusercontent.com/bkimminich/juice-shop/master/data/static/challenges.yml
  - develop branch / snapshot image: https://raw.githubusercontent.com/bkimminich/juice-shop/develop/data/static/challenges.yml

- Sample consumers
  - https://owasp-juice.shop/ project website populates its *Challenge Categories* and *Hacking Instructor Tutorials* tabs from the master YAML file
  - OpenCRE importer maps challenges as training resources to then show on https://opencre.org
  - Challenge Solution Webhook (→)

YAML Schema

```yaml
-
  name: 'Some Name'
  category: 'Category of the challenge'
  tags: # (optional) for grouping by aspects beyond category-level
    - Brute Force
    - Code Analysis
    - Contraption
    - Danger Zone
    - Good Practice
    - Good for Demos
    - OSINT
    - Prerequisite
    - Shenanigans
    - Tutorial
  description: 'Here the actual task for the attacker is described.'
  difficulty: 1 # a number between 1 and 6
  hint: 'A text hint to display on the Score Board when hovering over the challenge'
  hintUrl: 'https://pwning.owasp-juice.shop/part2/<category>.html#<shortened description>'
  mitigationUrl: 'https://cheatsheetseries.owasp.org/cheatsheets/<corresponding cheat sheet>.html' # will be empty if n/a
  key: someNameChallenge
  disabledEnv: # (optional) to disable challenges dangerous or incompatible in certain environments
    - Docker
    - Heroku
    - Gitpod
    - Windows
  tutorial: # (optional) present only on challenges with a Hacking Instructor tutorial
    order: 1 # a unique number to specify the recommended order of tutorials
```

(3) Direct Links into Juice Shop and its official guide

Description	Link composition	Condition	Examples
Scroll to a specific challenge on the Score Board *(unless hidden by a filter)*	`/#/score-board/challenge=<name>`		http://localhost:3000/#/score-board?challenge=Score%20Board
Link to official hints for a specific challenge	`<hintUrl>`		https://pwning.owasp-juice.shop/part2/score-board.html#find-the-carefully-hidden-score-board-page or https://pwning.owasp-juice.shop/part2/xss.html#perform-a-dom-xss-attack
Link to official step-by-step solution for a specific challenge	`https://pwning.owasp-juice.shop/appendix/solutions.html#<hash part of hintUrl>`		https://pwning.owasp-juice.shop/appendix/solutions.html#find-the-carefully-hidden-score-board-page or https://pwning.owasp-juice.shop/appendix/solutions.html#perform-a-dom-xss-attack
Direct link to a Hacking Instructor tutorial for a specific challenge	`/#/hacking-instructor?challenge=<name>`	Only for challenges where `tutorial` is defined.	http://localhost:3000/#/hacking-instructor?challenge=Score%20Board or http://preview.owasp-juice.shop/#/hacking-instructor?challenge=DOM%20XSS

Sample consumer:
https://opencre.org

(4) Challenge Solution Webhook

- Juice Shop can notify a specified webhook when a hacking challenge is solved
- Possible use cases include notifying a company‘s/university‘s learning management system about progress of training/lecture participants

Environment variable	Expected value	Recommendations
`SOLUTIONS_WEBHOOK`	URL of the webhook Juice Shop is supposed to call whenever a challenge is solved.	The webhook URL should be bound to the user who solved the challenge and allow its provider to verify the Juice Shop origin instance. In most cases **the webhook URL should be treated as sensitive information and not be published or transmitted unencrypted!**

- Sample consumers:
  - https://github.com/juice-shop/multi-juicer team scoreboard

Webhook Payload

```
{ "solution":
  { "challenge": "<'key' of the solved challenge from ./data/static/challenges.yml>",
    "cheatScore": "<probability of 0..1 that this solution has been cheated>",
    "totalCheatScore": "<average probability of 0..1 that solutions up until now have been cheated>",
    "issuedOn": "<yyyy-MM-ddThh:mm:ssZ>"
  },
  "ctfFlag": "<CTF flag code of the solved challenged based on the injected (or default) 'CTF_KEY'>",
  "issuer": {
    "hostName": "<server os hostname>",
    "os": "<server os type (and release)>",
    "appName": "<'application.name' from loaded YAML configuration in ./config folder>",
    "config": "<name of the loaded configuration>",
    "version": "<version from ./package.json>"
  }
}
```

Webhook Payload (Example)


```
▼ "root":
  ▼ "solution":
      "challenge": "key"
      "cheatScore": 0
      "totalCheatScore": 0
      "issuedOn": "2023-05-17T21:51:02.168Z"
    "ctfFlag": "b0d70dce6cadadb85882ea498fac6785dba2349b"
  ▼ "issuer":
      "hostName": "fv-az319-950"
      "os": "Windows_NT (10.0.20348)"
      "appName": "OWASP Juice Shop"
      "config": "default"
      "version": "15.0.0-SNAPSHOT"
```

(5) Prometheus Metrics

- **/metrics**
  - http://localhost:3000/metrics

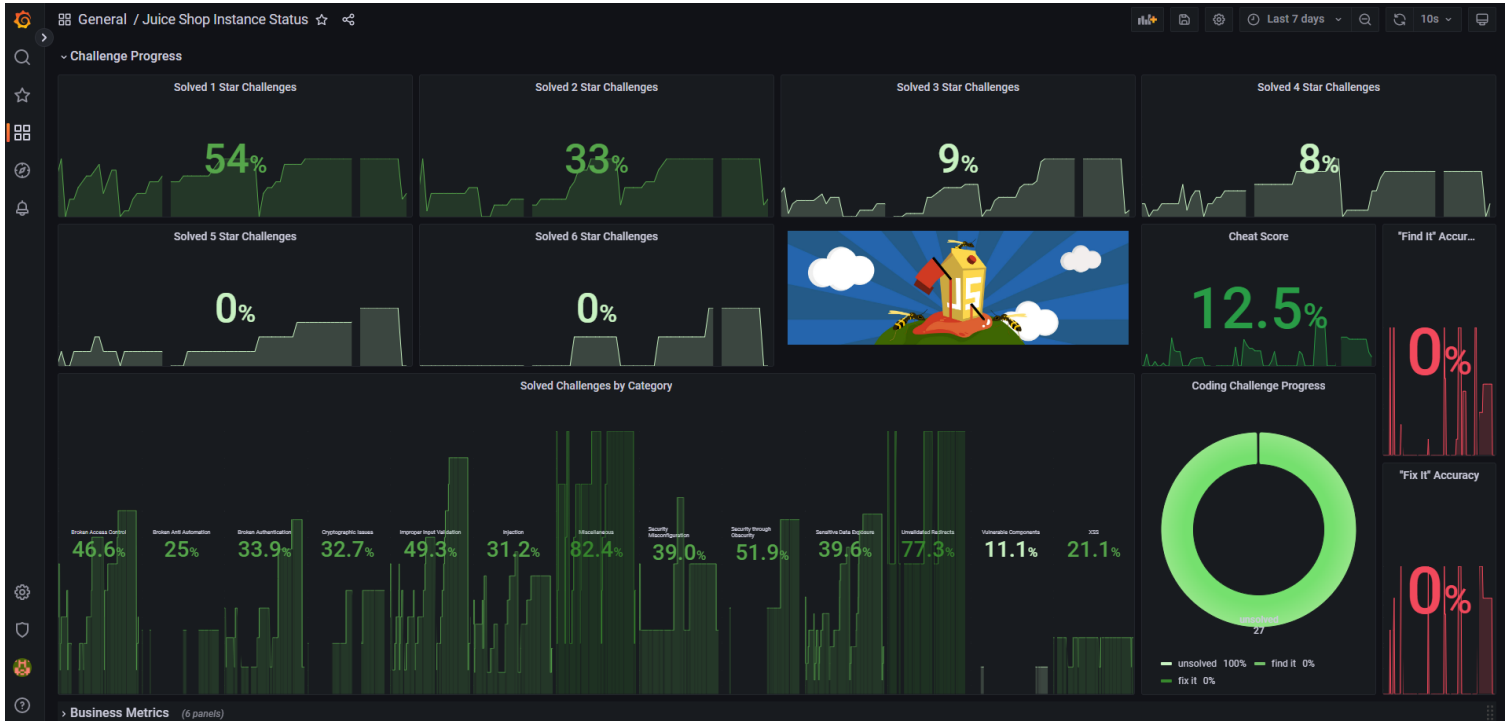
- Simple configuration

```
scrape_configs:
  - job_name: 'juiceshop_local'
    scrape_interval: 30s
    scrape_timeout: 10s
    static_configs:
    - targets: ['localhost:3000']
```

- Sample consumers
  - https://github.com/juice-shop/multi-juicer provides a Grafana dashboard to the admin for team progress tracking and troubleshooting instances
  - A RaspberryPi under Björn‘s desk scrapes http://demo.owasp-juice.shop/metrics and hosts a Grafana dashboard

Grafana Dashboard based on Prometheus metrics

- **monitoring/grafana-dashboard.json**
  - https://github.com/bkimminich/juice-shop/blob/master/monitoring/grafana-dashboard.json



Feedback? Questions? Ideas?