SWAPP: A New Programmable Playground for Web Application Security

Phakpoom Chinprutthiwong, Jianwei Huang, and Guofei Gu, *SUCCESS Lab, Texas A&M University*

https://www.usenix.org/conference/usenixsecurity22/presentation/chinprutthiwong

This artifact appendix is included in the Artifact Appendices to the Proceedings of the 31st USENIX Security Symposium and appends to the paper of the same name that appears in the Proceedings of the 31st USENIX Security Symposium.

August 10–12, 2022 • Boston, MA, USA

978-1-939133-31-1

A Artifact Appendix

A.1 Abstract

This artifact is provided to help validate two goals of our proposed platform SWAPP: compatibility (changes needed to work with legacy code or other existing libraries); and fast-prototyping (easiness to program a new app and its effectiveness). Consequently, the artifact contains two major components corresponding to each goal. First, we provide clean SWAPP and its app source codes. This will be used in conjunction with Wordpress and Workbox to show how to encapsulate Workbox as a SWAPP app and run SWAPP in a popular web app (Wordpress) as discussed in Section 6.2. Second, we provide four demo (pre-configured SWAPP and its apps) that illustrates how four of the apps discussed in the paper can work to prevent the corresponding attacks. To run this artifact, we provide Docker images with shell scripts that will help set up the environment automatically.

A.2 Artifact check-list (meta-information)

- **Run-time environment:** Ubuntu 18.04+ and Docker.
- **Metrics:** Compatibility with legacy code. Vulnerabilities mitigated.
- **Output:** Web page. Console. Measured characteristics.
- **Experiments:** Manual steps by users.
- **How much disk space required (approximately)?:** 1GB.
- **How much time is needed to prepare workflow (approximately)?:** 10 minutes.
- **How much time is needed to complete experiments (approximately)?:** 30 minutes
- **Publicly available (explicitly provide evolving version reference)?:** Yes. https://github.com/successlab/swapp
- **Archived (explicitly provide DOI or stable reference)?:** Yes. https://doi.org/10.5281/zenodo.6860277

A.3 Description

A.3.1 How to access

SWAPP is publicly available at https://github.com/successlab/swapp. The artifact is available at https://doi.org/10.5281/zenodo.6860277.

A.3.2 Hardware dependencies

N/A

A.3.3 Software dependencies

Ubuntu 18.04+. Docker.

A.3.4 Data sets

N/A

A.3.5 Models

N/A

A.3.6 Security, privacy, and ethical concerns

N/A

A.4 Installation

We have provide docker images with two shell scripts to help install Docker (install.sh) and setup the environment (deploy.sh). Users only need to execute these scripts in an Ubuntu system as required.

A.5 Experiment workflow

There are two metrics to validate our artifact: compatibility (M1), and programmability (M2). The workflow of this experiment is split into two sections correspondingly.

Section M1 showcases the compatibility of SWAPP. There are two steps in this section.

1. Setup Wordpress. Simply visit http://localhost using a web browser and follow the page instruction.
2. Interact with SWAPP. The installed Wordpress is already equipped with SWAPP. Four apps are also enabled. Interact with the website and see the browser console to observe the interaction and performance of SWAPP.

Section M2 showcases the programmability of SWAPP. We provide four demonstrating web pages corresponding to each of the four apps discussed in the paper: DOM Guard, Cache Guard, Autofill Guard, and Data Guard. The demo should also illustrate the effectiveness of each apps in responding to the corresponding attacks.

DOM Guard's effectiveness in preventing DOM-XSS attacks can be observed. Visit http://localhost/demo/domguard/index.html using a web browser to access DOM Guard's demo web page. Further instructions are provided in the web page.

Cache Guard's effectiveness in preventing side-channel attacks can be observed. To validate Cache Guard, simply visit http://localhost/demo/cacheguard/index.html using a web browser. Further instructions are provided in the web page.

Autofill Guard's effectiveness in preventing XSS attackers from accessing user's form input can be observed. Visit http://localhost/demo/autofillguard/ using a web browser to access Autofill Guard's demo web page. The website is installed with phpBB and the following credentials need to be used to correctly set up the demo.

- Database server hostname: mysql
- Database username: wp_user
- Database password: wp_password
- Database name: wordpress

After the set up is done, remove the /public_html/demo/autofillguard/install folder. Then, click "Take me to the ACP" and click "Logout" of the admin account. Next, revisit http://localhost/demo/autofillguard/. There should be a login form within an iFrame. In the case the iFrame does not show up, try refreshing the web page. Interact with the login form using the admin credentials to see if Autofill Guard works.

Data Guard's effectiveness in preventing Indirect Object Reference attacks can be observed. To validate Data Guard, simply visit http://localhost/demo/data_guard/index.html and follow the instruction given in the web page.

A.6 Evaluation and expected results

There are two goals of SWAPP that this artifact aims to validate.

SWAPP requires minimal changes to legacy and existing code (Compatibility). In section M1 workflow, we demonstrate that SWAPP can be easily installed on a popular web app like Wordpress. For instance, SWAPP only requires one line of code change to work with WordPress. Furthermore, encapsulating Workbox, a popular caching library, as a SWAPP app only requires a few lines of code change. The specific files that we change are located at public_html/wp-content/themes/twentytwentyone/footer.php (line 13) and public_html/apps/workbox-sw.js (lines 88-124). By observing the console while using Wordpress, there should not be any fatal errors from SWAPP.

SWAPP apps can be easily developed and are effective (Fast-prototyping). In section M2 workflow, we provide several demonstrating web pages for testing four SWAPP apps. Interacting with the demo should show that SWAPP and the apps are effective.

A.7 Version

Based on the LaTeX template for Artifact Evaluation V20220119.