



Web Security, Network Security, Reverse Engineering - Exposed

Home	ABOUT
------	-------

Share This Blog

- Twitter
- Facebook
- Google Buzz
- Google Reader

Follow by Email

Email

Submit

Working at



Thursday, June 18, 2015

Same Origin Method Execution (SOME)



This blog post is a brief presentation of **"Same Origin Method Execution" (SOME)**. SOME is a web application attack which abuses callback endpoints (mainly **Flash** applets and **JSONP** endpoints to which OAuth dialogs often redirect to -- `redirect_uri`) by forcing a victim into executing arbitrary scripting methods of any page on the endpoint's domain. The impact of a SOME attack is similar to the impact of Cross-Site Scripting, though there are some important and distinguishing exploitation restrictions. In spite of limitations, it is vital and valid to say that the attack is not limited to a specific web functionality/page nor confined in terms of UI or HTTP response headers. In fact, using a payload of **only alphanumeric characters and a dot** will allow attackers to hijack dangerous web functionality and even exfiltrate sensitive user data such as private photos and/or videos. Popular domains like **Google**, **Yahoo**, **Microsoft** (plus.google.com, maps.yahoo.com, yammer.com and so on) along with the very popular platforms - **Wordpress** and **VideoJS** (which turned **numerous domains vulnerable** to SOME) were affected by SOME. Many were recently fixed (responsible disclosure details are mentioned below).

Paper, Demo and Slides from BlackHat

If you wish to invest your time in exploring the fascinating technical details in-depth, you are encourage to read my **white-paper** (mirror), or look at the updated Black-Hat **presentation**. The slides include a demonstration video of a SOME exploit - you can see how I used SOME to hijack Google cloud's private photo and video albums.


By the way, you can also find more details about the breach I am talking about in my previous blog post: [Stealing private photo albums from Google](#)

Attack Scenario:

To understand the SOME attack we first need to cover some general aspects,

Tweets by @BenHayak

Ben Hayak Retweeted

 **mr_me** @_mr_me_

Ok, as promised, I just released the advisory and proof of concept for CVE-2016-0140 / MS16-054 Use-After-Free RCE srcincite.io/advisories/src

25 May

Embed View on Twitter

Blog Archive

- ▼ 2015 (2)
 - June (1)
 - May (1)
- 2014 (2)
- 2013 (2)
- 2012 (5)
- 2011 (8)

Labels

- Web Application Security (12)
- Cross site Scripting (9)
- Google Security Vulnerability Reward Program (8)
- Hack (5)
- Reverse Engineering (4)
- Facebook (3)
- Gmail (3)
- Google Mail (2)
- Twitter (2)
- eBay (2)
- Cracking (1)
- Google (1)

so bear with me:

Web browsers allow execution of a variety of methods without considering the given arguments, for example: `form1.submit("ignored","ignored");` will evaluate exactly as the following natural version: `form1.submit();` will. Therefore, an external control over the prefix/padding before the parenthesis (as often given by many callback implementations) would be enough for **hijacking dangerous web functionality** regardless of the arguments.

In an environment with multiple windows and their respective documents, redirecting any of the documents will re-enforce Same Origin Policy to restrict cross-site window documents' DOM access. However, **web browsers would not delete memory references to other window objects post-redirectation**. For instance, whenever a document opens a popup window, the browser will add a memory reference pointing to this document and save it as the **window.opener** property of the new window. Regardless of any redirections this reference would continue to work unless it is explicitly deleted or destroyed.

Most callbacks endpoints are designed to only allow a limited set of characters as a callback parameter value. This is commonly done by the following regex `[a-zA-Z0-9_\.]`, or in other words, a char-set consisting of alphanumeric, a dot and an underscore. Let me add that crafting a SOME exploit requires only alphanumeric and a dot charset.

Interaction between different browsing contexts is often applied via callback execution. For instance, **Flash applets** and/or other callback endpoints (e.g. **OAuth dialogs**) commonly execute a callback function to **notify events** to a different browsing context. As a result, in cases where this callback can be controlled via a HTTP parameter, an attacker would be able to control and replace the **execution browsing context** (e.g. by redirecting the opener window document). Analogically, the **function/method** that the interpreter executes could also be controlled by the attacker.

Same Origin Method Execution abuses the nature of user agents by forging a setup of windows/frames, in turn redirecting their documents. Using references created by this setup within a callback parameter will allow replacing the execution context with a targeted document and hijacking an existing web functionality within it.

Manipulating a Surface for Method Execution

Initial steps:

Firstly, the attacker has to detect a vulnerable instance - either a plugin or a vulnerable callback endpoint document. A vulnerable instance is the one that leads the browser's interpreter towards active execution of a function name supplied by a (callback) parameter value.

Note: Instances that respond with passive mime types like `application/json` are not vulnerable when accessed directly.

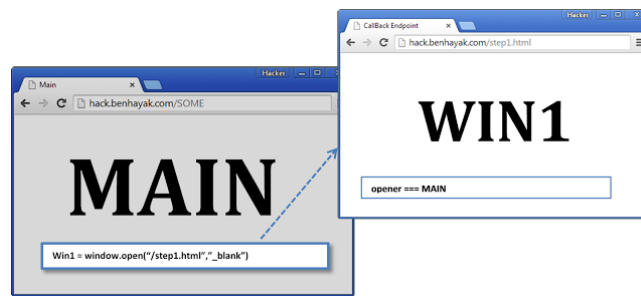
In the second preparatory step the attacker has to choose a target webpage hosted on the same domain (`http://www.vulnerable-domain.com/photoAlbums`). Aiming at hijacking a web functionality (e.g. object method, javascript function) of this target webpage, the attacker shall assemble a reference using DOM navigation or a direct reference pointing to it, for example: `document.body.privateAlbum.firstChild.nextElementSibling.submit`

Setting up the Exploit:

For setting up SOME and creating the appropriate window references, one has to create an exploitation surface/environment by opening a new browsing context (WIN1).

SOME (1)

XFraming (1)



Once the environment is ready, the initiating page (MAIN) shall redirect its document to any desired target page on the endpoint's domain (http://www.vulnerable-domain.com/target_document).

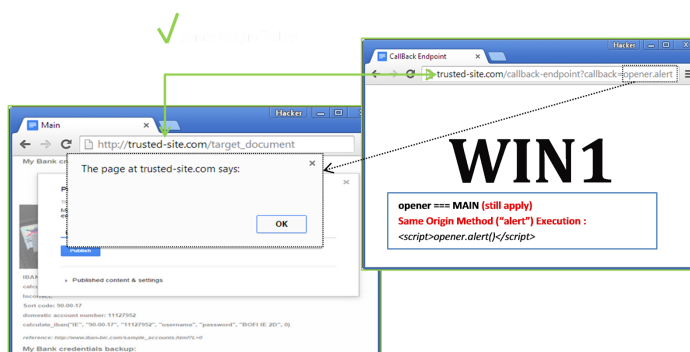
Following the redirection, the new browsing context (WIN1) shall wait for the targeted document's DOM loading completion.

Once ready, for hijacking a method execution, the new browsing context (WIN1) would **redirect its document to the vulnerable instance** set with an arbitrary callback parameter, for example:

<http://www.vulnerable-domain.com/flash-plugin.swf?>

callback=opener.document.body.privateAlbum.firstChild.nextElementSibling.submit

Demo of designating the execution context for executing an alert:



PoC:

@Main Page:

```
<script>
function startSOME() {
  window.open("step1.html");
  location.replace("http://www.vulnerable-domain.com/privateAlbum");
}
document.body.addEventListener("click",startSOME); //Popup Blocker trick
</script>
```

@step1.html:

```
opener.document.body.privateAlbum.firstChild.nextElementSibling.submit");
```

Mitigation and Fix

Static Callbacks - Exploiting Same Origin Method Execution relies on abusing a callback parameter. Many web applications can actually maintain their same existing functionality without having to dynamically

set callbacks. Thus, when applicable, websites should use fixed callback values as opposed to externalizing the callback control.

White-list approach – In cases where the web application is designed for supporting more than a single callback per endpoint, or, alternatively, where maintaining a high flexibility is highly important (common in Flash plugins), it is better to set a white-list and match the given callback parameter value against it. This would enforce and verify that only legitimate callback functions can execute. UPDATE: I am working on a JavaScript defense library aiming to serve as a generic and easy to deploy solution.

Cross-Domain Messaging – Use postMessage for notifying events and interacting to and from cross-domains as an alternative to javascript callback execution (if applicable).

Responsible Disclosure:

Oct 30, 2014: Google fixed a vulnerable instance – Google Plus.

Nov 06, 2014: Microsoft fixed a vulnerable instance – Yammer.

April 21, 2015: Wordpress fixed a vulnerable instance – Plupload.

(Kudos to @zoczus for finding yammer and plupload instances)

The issue of callback exploitation is known to a certain level in the infosec community, although until recently the attack did not catch enough attention. For that reason website owners, including the leading players, still rely on developers' habits and experience. More importantly, no 'best practice' or standard was published as of now. Thus I chose to shed some light on Same Origin Method Execution and callback endpoints during the BlackHat conference. Several aspects of Same Origin Method Execution have been discovered by top researchers namely Google's Aleksandr Dobkin and LinkedIn's Roman Shafigullin. They both certainly deserve credit here.

It is noteworthy that Google Bug Bounty deemed this attack's impact similar to that of cross-site scripting.

Microsoft Bug Bounty deemed this attack's impact similar to that of cross-site scripting.

Wordpress classified this attack like "XSS" in their critical security release (Apr. 2015 - [WordPress 3.9-4.1.1 - Same-Origin Method Execution](#)).

The Same Origin Method Execution attack can lead to ugly and critically severe consequences for its targeted victims. Keep in mind that the attack's risk is considered as high as the risk of Cross-site scripting, rated the "third most risky attack" in OWASP top 10 project - that is A3 Cross-site scripting (XSS). To conclude, it is really important to abandon the misconception that a narrow set of characters somehow guarantees safety and security, of your web applications. Further, we should strive to raise the developers' awareness of SOME.

Posted by [Ben Hayak] at 6:03 PM

 +4 Recommend this on Google

5 comments:

 **Unknown** December 1, 2015 at 5:41 AM

The link to your white paper is broken...

[Reply](#)

[Replies](#)



[Ben Hayak] December 1, 2015 at 2:39 PM

Thank you for letting me know! Meanwhile you can use the mirror link (<https://www.blackhat.com/docs/eu-14/materials/eu-14-Hayak-Same-Origin-Method-Execution-Exploiting-A-Callback-For-Same-Origin-Policy-Bypass-wp.pdf>)

The server will be back up soon.



[Ben Hayak] December 1, 2015 at 3:23 PM

Update: the server is up

[Reply](#)

Anonymous March 15, 2016 at 12:18 AM

Is the SOME exploit dependent on JSONP? Of is the SOME attack dependent on poor control over the implementation of callback?

[Reply](#)



[Ben Hayak] March 15, 2016 at 1:21 PM

I would say, the first could happen, however, the second is really the issue.

[Reply](#)

Enter your comment...

Comment as: Lyleaks Zero (C ▼)

Sign out

Publish

Preview

☐ Notify me

[Home](#)

[Older Post](#)

Subscribe to: [Post Comments \(Atom\)](#)