2 Sensitive Clickjacking on admin login page.

Share:

State	Resolved (Closed)
Disclosed	**April 22, 2019 9:31am +0530**
Reported To	Shipt
Asset	admin.shipt.com (Domain)
Weakness	UI Redressing (Clickjacking)
Bounty	$100
Severity	Low (0.1 ~ 3.9)
Participants	
Visibility	Disclosed (Full)

Collapse

TIMELINE

mdspr99 submitted a report to **Shipt**. Aug 1st (9 months ago)

Hi There

I got a Clickjacking bug
Heres the all details :

Vulnerable link : https://staging-admin.shipt.com/

Then open notepad and paste the following code :

```
<html>
<head>
<title>Clickjack test page</title>
</head>
<body
<p>This website is vulnerable to clickjacking!</p>
<iframe src="https://staging-admin.shipt.com/" width="1247" height="800"></iframe>
</body>
</html>
```

As far as i know this data is enough to prove that your site is vulberable to Clickjacking..
according to OWASP its more than enough..
https://www.owasp.org/index.php/Testing_for_Clickjacking_(OWASP-CS-004)

Solution:
https://www.owasp.org/index.php/Clickjacking_Defense_Cheat_Sheet
check this out..here is the solution for that..
I also submit some screenshot as a prove :)

Impact

To carry out this type of technique the attacker has to create a seemingly harmless web page that loads the target application through the use of an iframe (suitably concealed with CSS code). Once this is done, the attacker could induce the victim to interact with his fictitious web page by other . Like other attacks, a common prerequisite is that the victim is authenticated against the attacker's target website.

1 attachment:
F327088: Screenshot_1.png

joystick HackerOne staff closed the report and changed the status to ○ **Informative**. Aug 2nd (9 months ago)

The lack of X-Frame-Options does not always indicate that a security vulnerability is present. This is an optional header that is only necessary on endpoints where there UI is rendered to invoke state changing actions. We recommend reading this informative post by David Ross: https://plus.google.com/u/0/+DavidRossX/posts/jVrtTRd5yKP

shiptsecurity1 **reopened** this report. Aug 2nd (9 months ago)

joystick HackerOne staff closed the report and changed the status to ○ **Not Applicable**. Aug 2nd (9 months ago)

Based on your initial description, there do not appear to be any security implications as a direct result of this behavior. If you disagree, please reply with additional information describing your reasoning. Including a working proof-of-concept can be incredibly helpful in our assessment of these claims.

shiptsecurity1 **reopened** this report. Aug 2nd (9 months ago)

shiptsecurity1 changed the status to ○ **Triaged**. Aug 2nd (9 months ago)

mdspr99 posted a comment. Aug 6th (9 months ago)

Any update ?

Shipt rewarded mdspr99 with a **$100** bounty. Aug 7th (9 months ago)

Thank you for your report @mdspr99. I have validated the issue, and due to the criticality of this asset and because it is on the login page (fyi, after login, future pages are unable to be framed), we will be addressing this immediately. I will update the report once it has been resolved. Thank you for helping keep Shipt safe!

mdspr99 posted a comment. Aug 7th (9 months ago)

Many many thanks :)

shiptsecurity1 changed the scope from **staging-admin.shipt.com** to **admin.shipt.com**. Aug 9th (9 months ago)

shiptsecurity1 posted a comment. Sep 7th (8 months ago)

Update: @mdspr99, this resolution is still being developed and tested by our engineering team(s). I will update when it has been resolved.

mdspr99 posted a comment. Sep 7th (8 months ago)

OKay :) many many thanks :)

shiptsecurity1 posted a comment. Mar 23rd (about 1 month ago)

@mdspr99 , I believe we've implemented the necessary changes to resolve this. Can you verify?

mdspr99 posted a comment. Mar 23rd (about 1 month ago)

Hi there
It's already been resolved :)

Thanks

shiptsecurity1 closed the report and changed the status to ○ **Resolved**. Mar 23rd (about 1 month ago)

mdspr99 requested to disclose this report. Mar 23rd (about 1 month ago)

This report has been disclosed. Apr 22nd (about 1 hr ago)