

New issue

[Jump to bottom](#)

[Security Bug] Open Redirection Vulnerability at Login Page #5265

🔒 Closed humblelad opened this issue on Apr 19, 2020 · 3 comments · Fixed by #5375

Assignees



Labels

bug security

Milestone

📌 May 2020

humblelad commented on Apr 19, 2020

Describe the bug

It is possible to redirect a user to an attacker owned domain and trick the user. I am investigating on the potential chaining of this bug to perform other attacks.

Expected behavior

Redirection to external urls must not be allowed.

To Reproduce

This occurs at the main login page when the user enters an invalid username/password.

The url gets changed to

`http://localhost:1501/authentication/login?old=http%3A%2F%2Flocalhost%3A1501%2Fhome`

An attacker can change the url(to any attacker owned domain which may mimic submittity interface) to something like

`localhost:1501/authentication/login?old=http%3A%2F%2F1google.com`

and trick redirection to google.com users after they enter their creds.

Additional context

This can be prevented either by-

1. Adding regex checks on url and whitelisting the url.
2. Completely removing GET request based url redirection.

I am trying to fix this but thought to create this issue for others to contribute the fix if interested.

humblelad added the bug label on Apr 19, 2020

MasterOdin added the security label on Apr 19, 2020

MasterOdin added this to the Spring 2020 Priorities milestone on Apr 19, 2020

MasterOdin commented on Apr 19, 2020 • edited

Member

I think we can just insert something like:

```
if (!is_null($old) && !Utils::startsWith($old, $this->core->getConfig()->getBaseUrl())) {
    $old = null;
}
```

at <https://github.com/Submittity/Submittity/blob/master/site/app/controllers/AuthenticationController.php#L75> and

<https://github.com/Submittity/Submittity/blob/master/site/app/controllers/AuthenticationController.php#L95> as I would like to retain the behavior of redirecting the user after they login, and without making it complicated to copy/paste a URL if need be.

humblelad commented on Apr 19, 2020

Author

ok if that works. :) ILYK for any bypasses.

bmcutler modified the milestones: Spring 2020 Priorities, May 2020 on May 11, 2020

elihschiff self-assigned this on May 11, 2020

elihschiff commented on May 11, 2020

Member

Is there ever a time when we want the php to redirect users to external websites? It seems like automatically redirecting users to external websites is a bad idea anyway. There might be some way in the future where somebody finds a different way to redirect users to an external domain (other than on login) and only putting the check in the login code would not stop that. If we do want to have the ability to allow redirecting to external websites then we don't have a choice, but if we don't ever want to redirect users to external websites, I think it might be better to add that check here which will stop all redirects.

[Submittity/site/app/libraries/Core.php](#)
Line 531 in 1a6ccad

```
531     }
```


I can even have it thrown an exception so if a future developer tries an external redirect, it will let them know.

  elihschiff mentioned this issue on May 11, 2020

[Bugfix:InstructorUI] Stops submittity from being used in iframe and stops external domain redirects on login #5375

 Merged

 1 task

 bmcutler closed this as completed in #5375 on May 28, 2020

  Akokonunes mentioned this issue on Feb 7

Create CVE-2020-13121.yaml projectdiscovery/nuclei-templates#3684

 Merged

Assignees

 elihschiff

Labels


bug security

Milestone

May 2020

Development

Successfully merging a pull request may close this issue.

 [Bugfix:InstructorUI] Stops submittity from being used in iframe and stops external domain redirects on login
Submittity/Submittity

4 participants

