CVE-2021-24830

Advanced Access Manager < 6.8.0 - Admin+ Stored Cross-Site Scripting

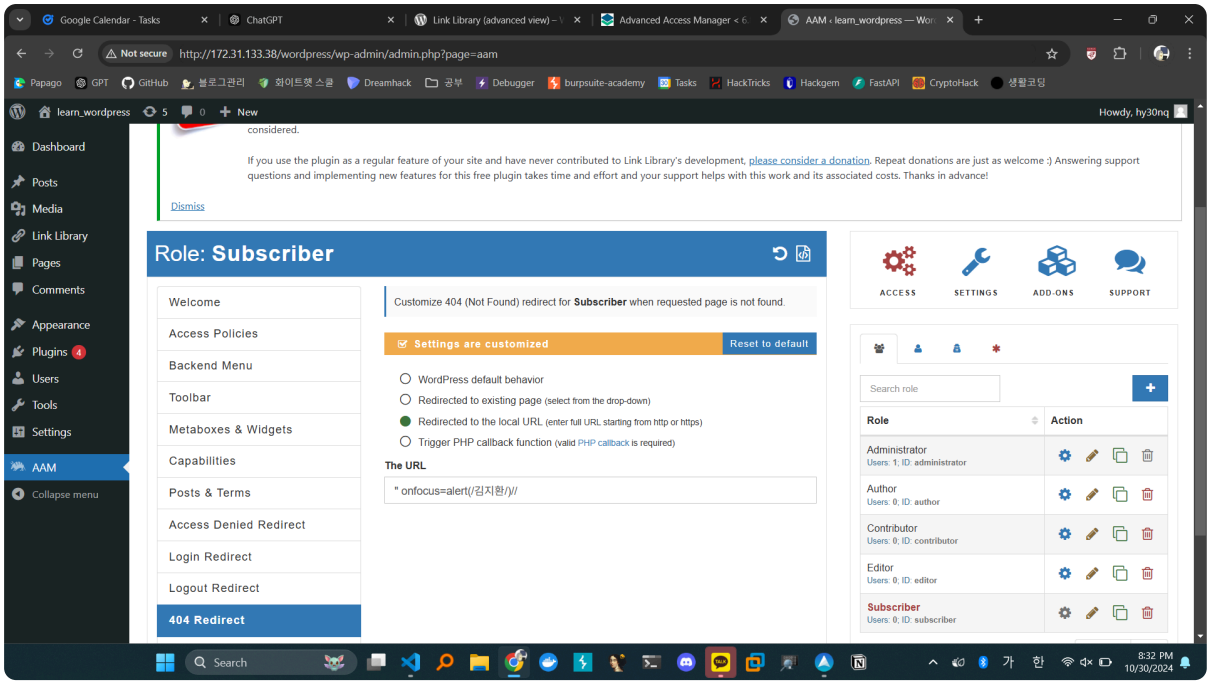
```
                    <input type="text" class="form-control"
name="logout.redirect.url" placeholder="https://" value="<?php echo
$this->getOption('logout.redirect.url'); ?>" />
```

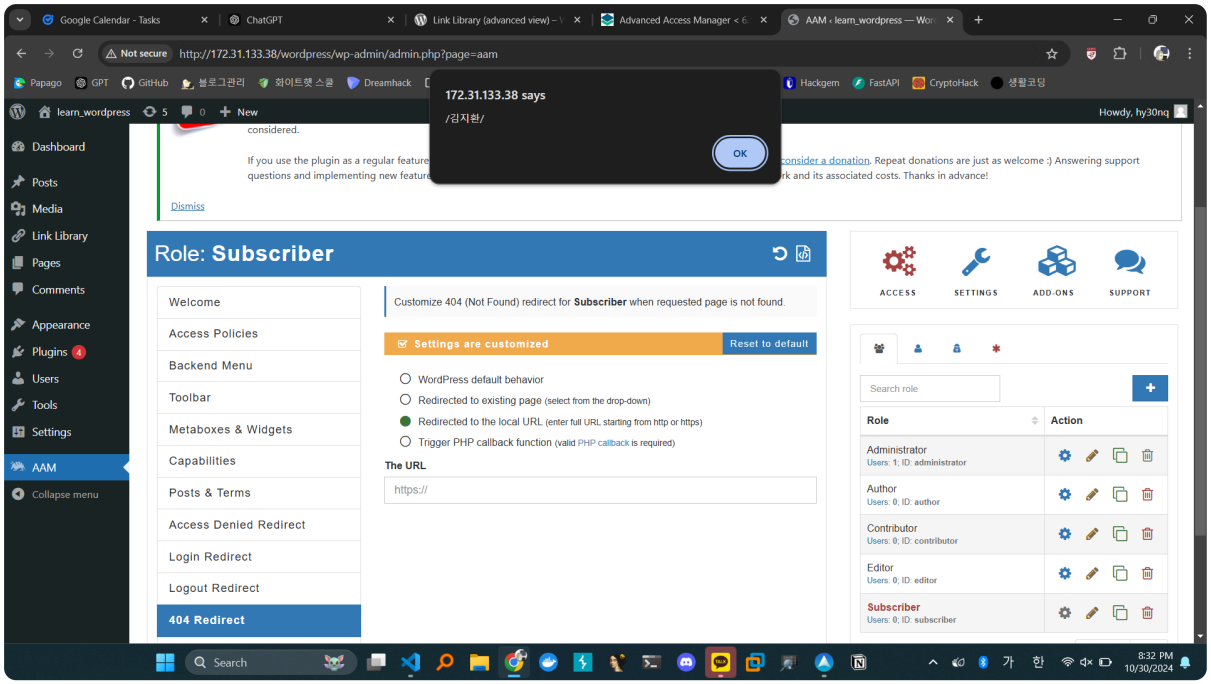
해당 부분에서 입력을 받은 후 value에 저장

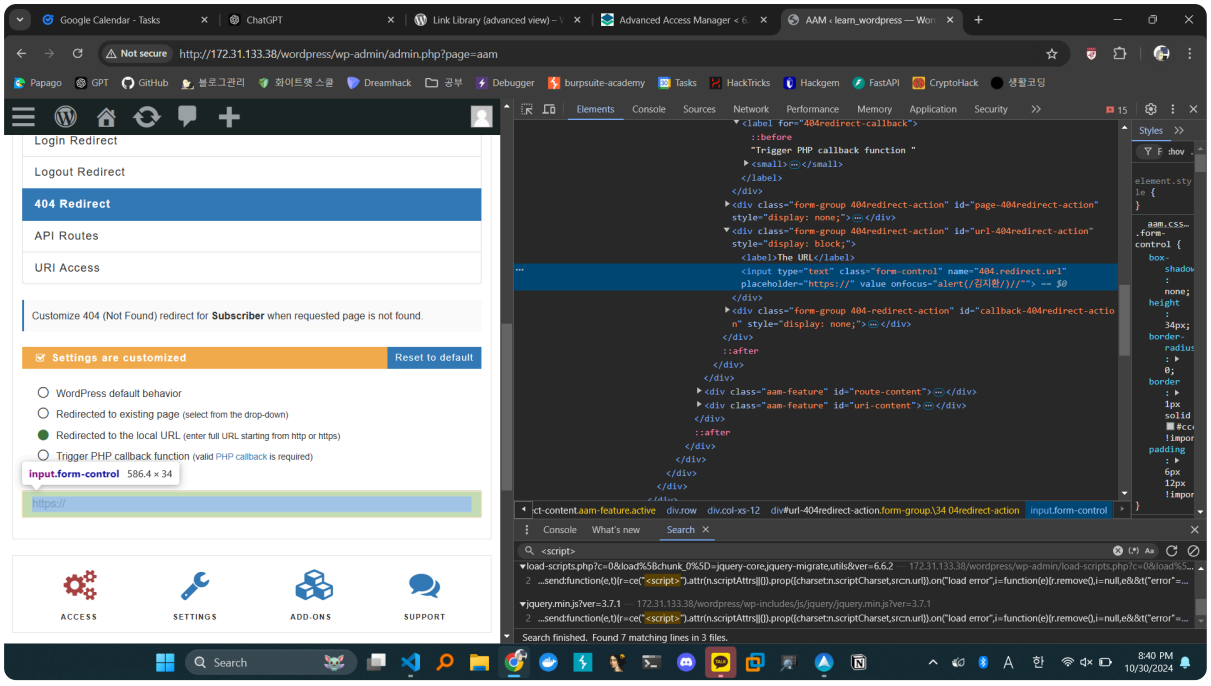
여기서 값을 가져올 때 검증 없이 가져옴

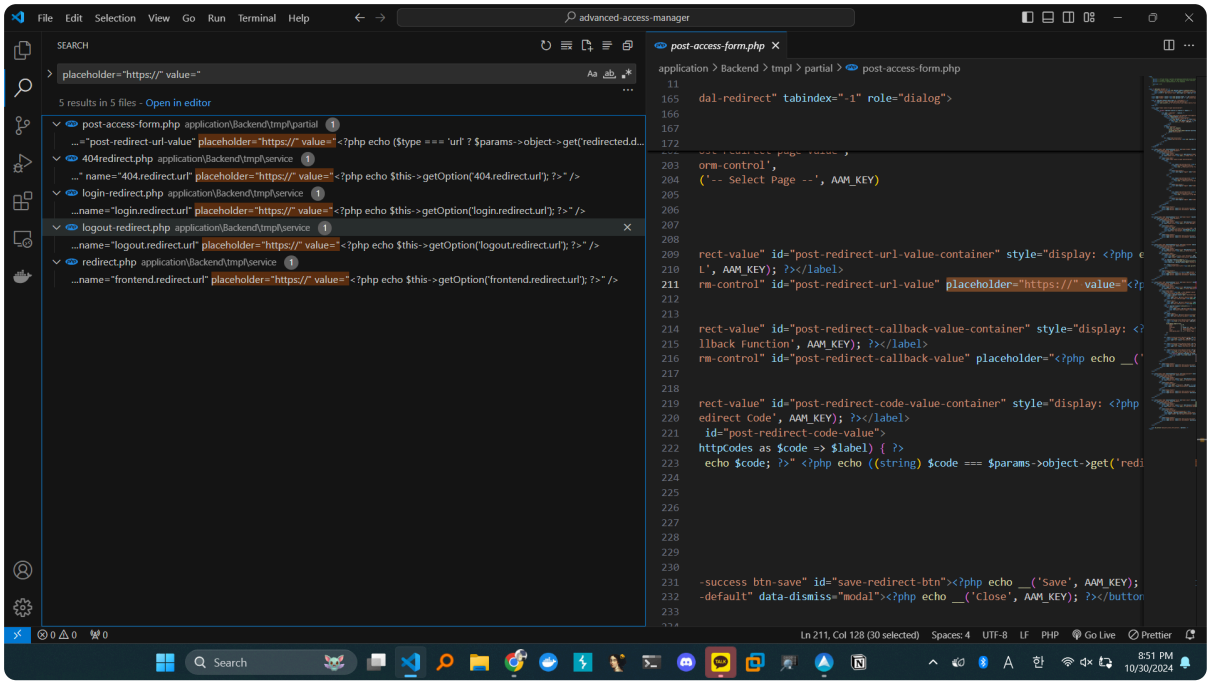
```
payload : " onfocus=alert(/XSS/) autofocus a=" //
```

Redirected to the local URL이 있는 모든 부분에 대해서 xss가 발생 할 수 있음


Google Calendar - Tasks
ChatGPT
Link Library (advanced view) – \
Advanced Access Manager < 6
AAM ‹ learn_wordpress — Wor
Not secure
http://172.31.133.38/wordpress/wp-admin/admin.php?page=aam
learn_wordpress
New
Howdy, hy30nq
Dashboard
Posts
Media
Link Library
Pages
Comments
Appearance
Plugins
Users
Tools
Settings
AAM
Collapse menu
considered.
If you use the plugin as a regular feature of your site and have never contributed to Link Library's development, please consider a donation. Repeat donations are just as welcome :) Answering support questions and implementing new features for this free plugin takes time and effort and your support helps with this work and its associated costs. Thanks in advance!
Dismiss
Role: Subscriber
Welcome
Access Policies
Backend Menu
Toolbar
Metaboxes & Widgets
Capabilities
Posts & Terms
Access Denied Redirect
Login Redirect
Logout Redirect
404 Redirect
Customize 404 (Not Found) redirect for Subscriber when requested page is not found.
Settings are customized
Reset to default
WordPress default behavior
Redirected to existing page (select from the drop-down)
Redirected to the local URL (enter full URL starting from http or https)
Trigger PHP callback function (valid PHP callback is required)
The URL
" onfocus=alert(/김지환/)//
ACCESS
SETTINGS
ADD-ONS
SUPPORT
Search role
Role
Action
Administrator
Users: 1; ID: administrator
Author
Users: 0; ID: author
Contributor
Users: 0; ID: contributor
Editor
Users: 0; ID: editor
Subscriber
Users: 0; ID: subscriber
Search
8:32 PM
10/30/2024


Google Calendar - Tasks
ChatGPT
Link Library (advanced view) – \
Advanced Access Manager < 6
AAM ‹ learn_wordpress — Wor
Not secure
http://172.31.133.38/wordpress/wp-admin/admin.php?page=aam
172.31.133.38 says
/김지환/
OK
learn_wordpress
New
Howdy, hy30nq
Dashboard
Posts
Media
Link Library
Pages
Comments
Appearance
Plugins
Users
Tools
Settings
AAM
Collapse menu
considered.
consider a donation. Repeat donations are just as welcome :) Answering support
rk and its associated costs. Thanks in advance!
Dismiss
Role: Subscriber
Welcome
Access Policies
Backend Menu
Toolbar
Metaboxes & Widgets
Capabilities
Posts & Terms
Access Denied Redirect
Login Redirect
Logout Redirect
404 Redirect
Customize 404 (Not Found) redirect for Subscriber when requested page is not found.
Settings are customized
Reset to default
WordPress default behavior
Redirected to existing page (select from the drop-down)
Redirected to the local URL (enter full URL starting from http or https)
Trigger PHP callback function (valid PHP callback is required)
The URL
https://
ACCESS
SETTINGS
ADD-ONS
SUPPORT
Search role
Role
Action
Administrator
Users: 1; ID: administrator
Author
Users: 0; ID: author
Contributor
Users: 0; ID: contributor
Editor
Users: 0; ID: editor
Subscriber
Users: 0; ID: subscriber
Search
8:32 PM
10/30/2024





위에 나오는 부분에서 다 xss 발생함

참고자료

https://wpscan.com/vulnerability/1c46373b-d43d-4d18-b0ae-3711fb0be0f9/