GrimTheRipper Follow
Jul 8 · 3 min read · Listen

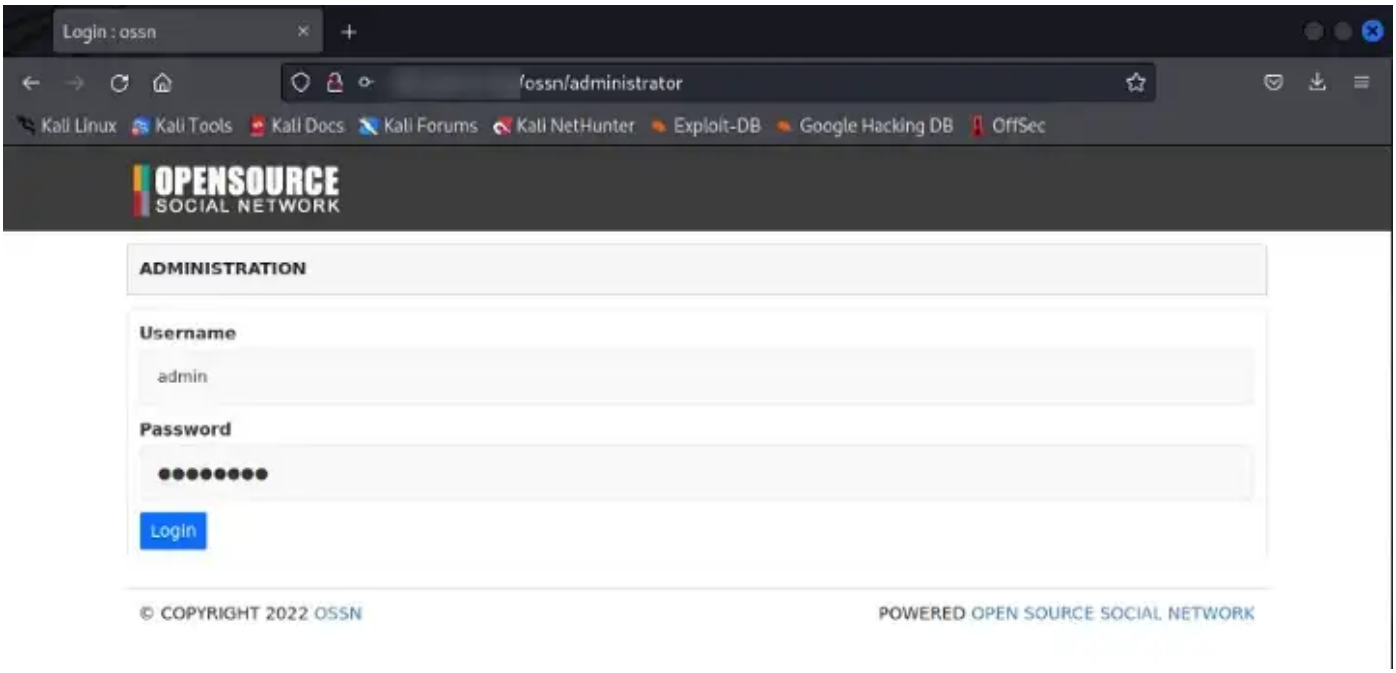
[CVE-2022–34965] Open Source Social Network 6.3 LTS— Authenticated Unrestricted File Upload (Components)

Description

#OpenTeknik LLC OSSN OPEN SOURCE SOCIAL NETWORK v6.3 LTS was discovered to contain an arbitrary file upload vulnerability via the component /ossn/administrator/com_installer.

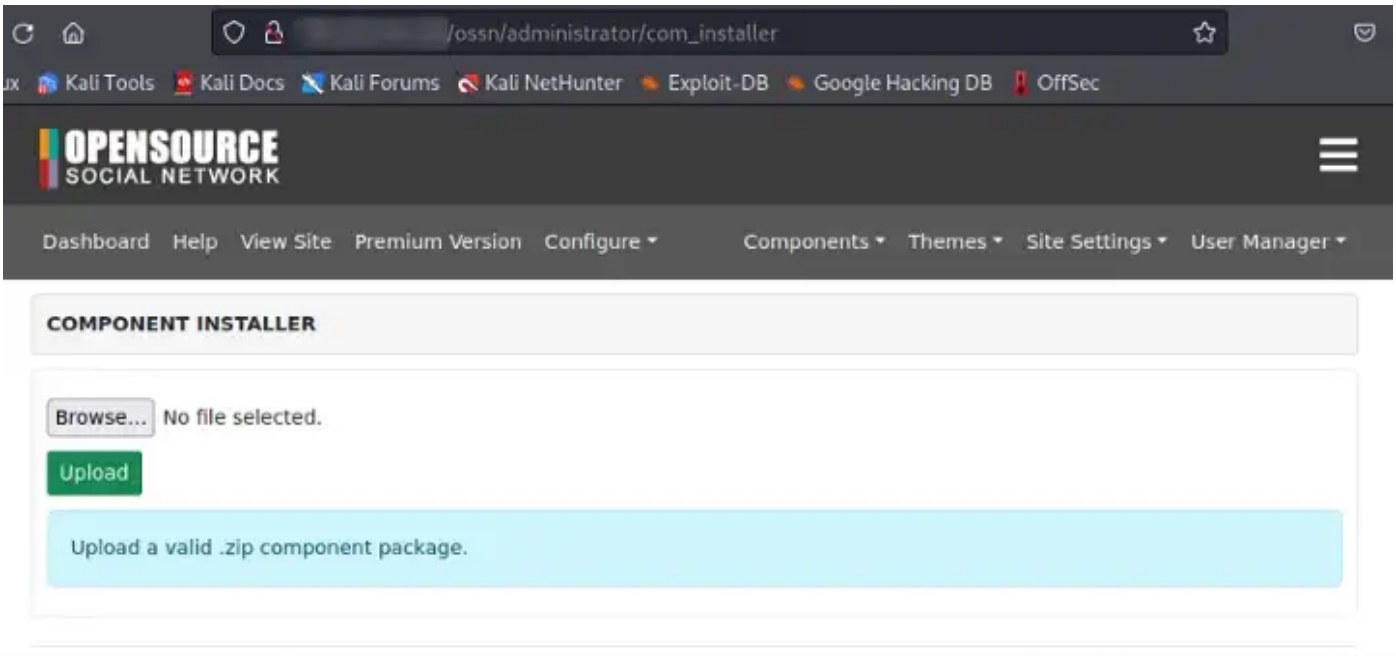
Steps to attack:

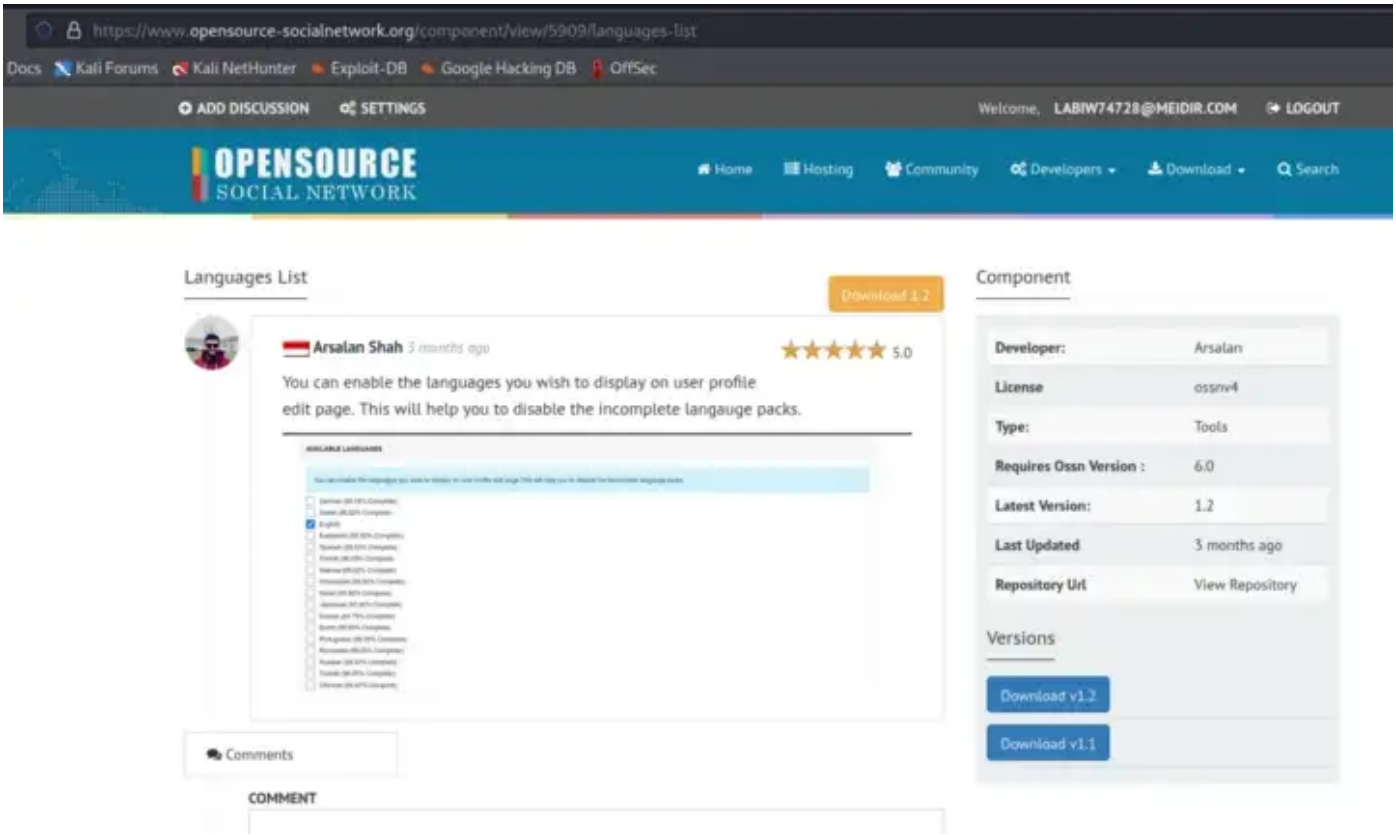
First, we log in to the OSSN 6.3 as the admin privileges on the administrator page.



http://<IP>/ossn/administrator

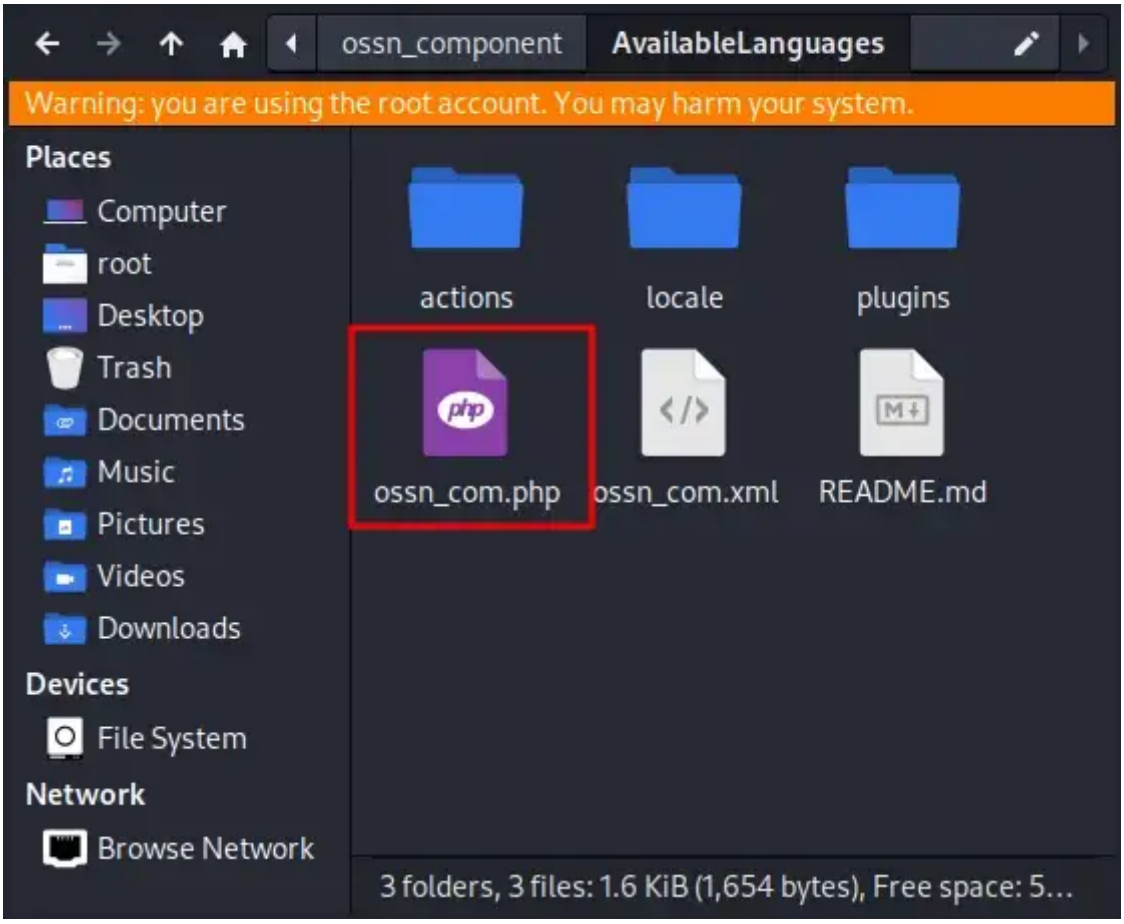
And then we proceed towards to menu Components > installer



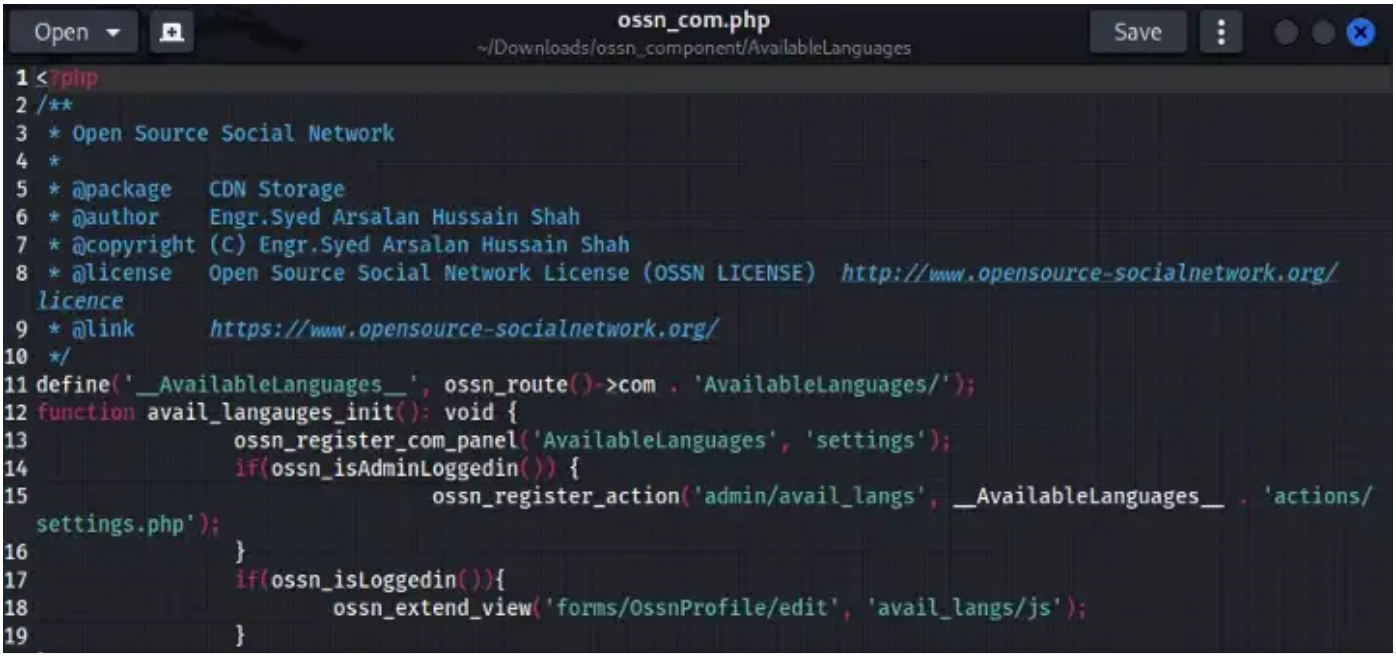


https://www.opensource-socialnetwork.org/component/view/5909/languages-list

When unzipping the theme that we download, we will find the ossn_com.php file in the directory of the theme.



It looks like we can change the content of the ossn_com.php file to PHP reverse shell.



Edit content of ossn_com.php to PHP reverse shell.


Create an archive in type zip that contains the directory of components.

Proceed towards to menu Components > installer and click on the Browse button.

http://<IP>/ossn/administrator/com_installer

Choose the archive that we create.

Choose the archive that we create.

Now, our component with the malicious files is all ready to use.

Using netcat to listen for TCP connections on port 443.


Direct access to ossn_com.php file that we edit the content to PHP reverse shell via the link following.

http://<IP>/ossn/components/AvailableLanguages/ossn_com.php

http://<IP>/ossn/components/AvailableLanguages/ossn_com.php

Bravo!, We get the system shell on the web server which uses Open Source Social Network 6.3.


Discoverer:

Grim The Ripper Team by SOSECURE Thailand

Reference:

1. https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34965
2. https://www.opensource-socialnetwork.org/
3. https://github.com/opensource-socialnetwork/opensource-socialnetwork/releases/tag/6.3
4. https://www.openteknik.com/contact?channel=ossn