

[Open in app](#)[Get started](#)

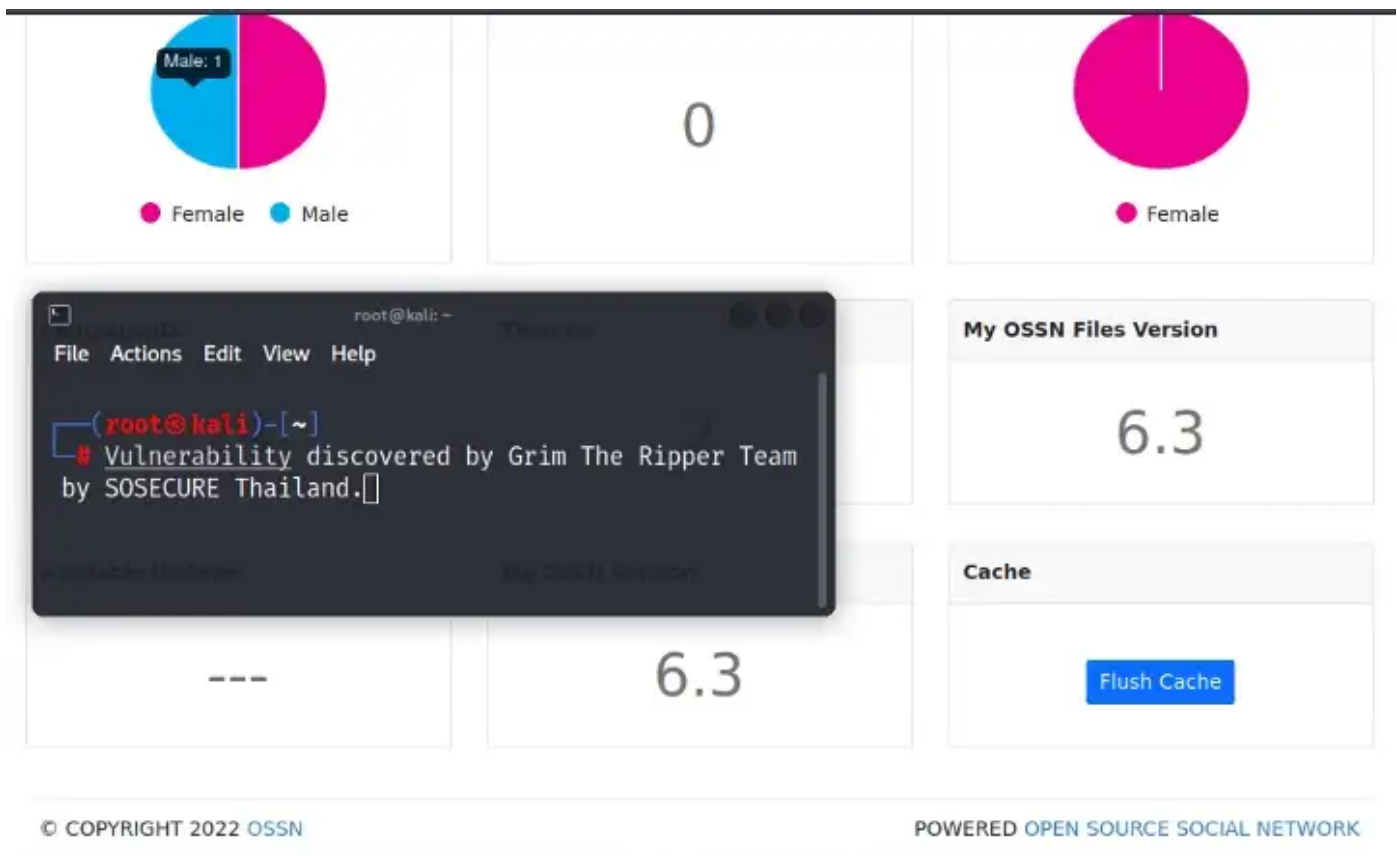
GrimTheRipper

[Follow](#)

Jul 8 · 3 min read · [Listen](#)

[Save](#)

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



## Description

#OpenTeknik LLC OSSN OPEN SOURCE | 1 ORK v6.3 LTS was discovered to contain an arbitrary file upload vulnerability via the component `/ossn/administrator/com_installer`.





Open in app

Get started

## Steps to attack:

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

The screenshot shows a web browser window with the address bar displaying `/ossn/administrator`. The page features the "OPENSOURCE SOCIAL NETWORK" logo at the top. Below the logo is a section titled "ADMINISTRATION" containing a login form. The form has two input fields: "Username" with the text "admin" and "Password" with masked characters. A blue "Login" button is positioned below the password field. At the bottom of the page, there is a copyright notice "© COPYRIGHT 2022 OSSN" and the text "POWERED OPEN SOURCE SOCIAL NETWORK".

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

And then we proceed towards to menu Components > installer

The screenshot shows the "COMPONENT INSTALLER" page in the OSSN administrator interface. The page has a dark header with the "OPENSOURCE SOCIAL NETWORK" logo and a navigation menu. The main content area is titled "COMPONENT INSTALLER" and contains a file upload section. It includes a "Browse..." button, a text field showing "No file selected.", and a green "Upload" button. Below these elements is a light blue message box that reads "Upload a valid .zip component package.".

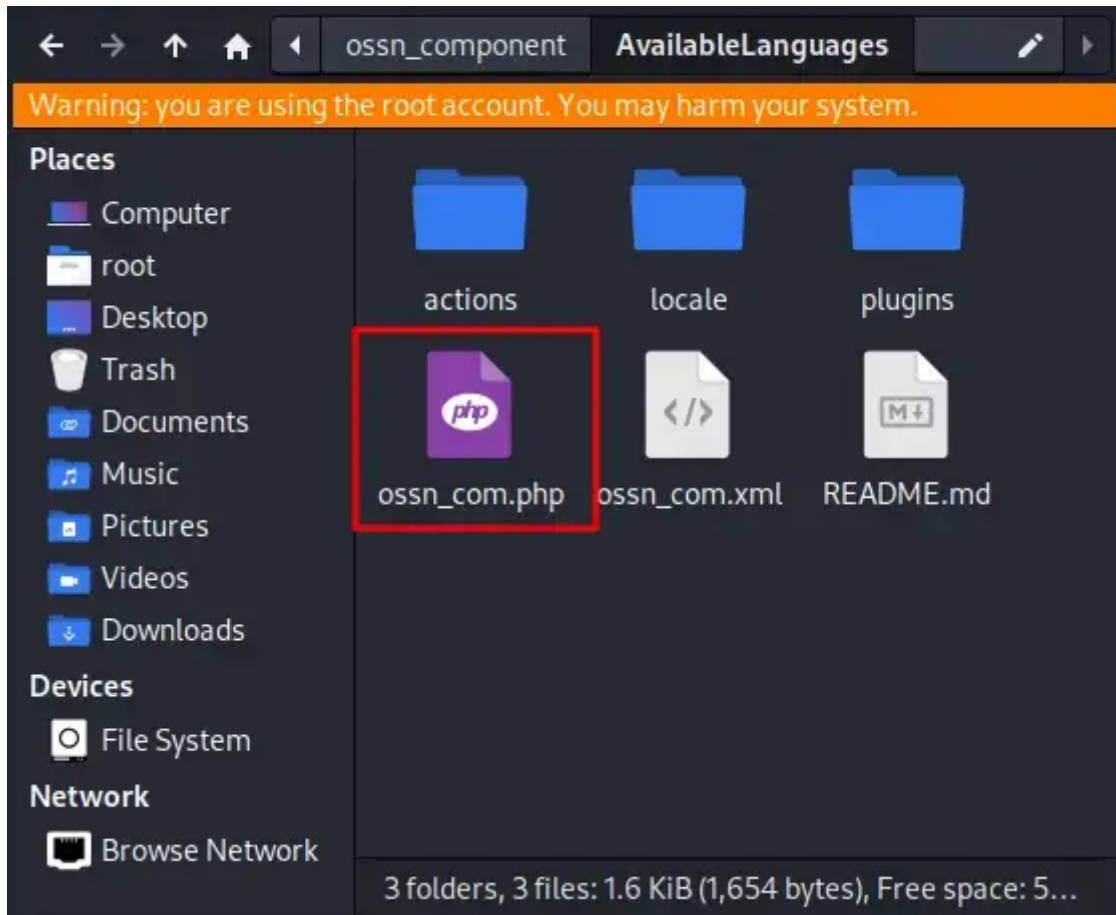
[Open in app](#)[Get started](#)

The screenshot shows the OpenSource Social Network website. The URL in the browser is <https://www.opensource-socialnetwork.org/component/view/5909/languages-list>. The page features a navigation bar with links to Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation bar, there are links to ADD DISCUSSION, SETTINGS, and a welcome message for LABIW74728@MEIDIR.COM with a LOGOUT button. The main content area is titled "Languages List" and features a post by Arsalan Shah, 3 months ago, with a 5.0 rating. The post text says: "You can enable the languages you wish to display on user profile edit page. This will help you to disable the incomplete language packs." Below the text is a list of available languages with checkboxes. To the right of the post is a "Component" sidebar with details: Developer: Arsalan, License: ossnv4, Type: Tools, Requires Ossn Version: 6.0, Latest Version: 1.2, Last Updated: 3 months ago, and Repository Url: View Repository. Below the component details are buttons for "Download v1.2" and "Download v1.1". At the bottom of the post is a "Comments" section with a "COMMENT" input field.

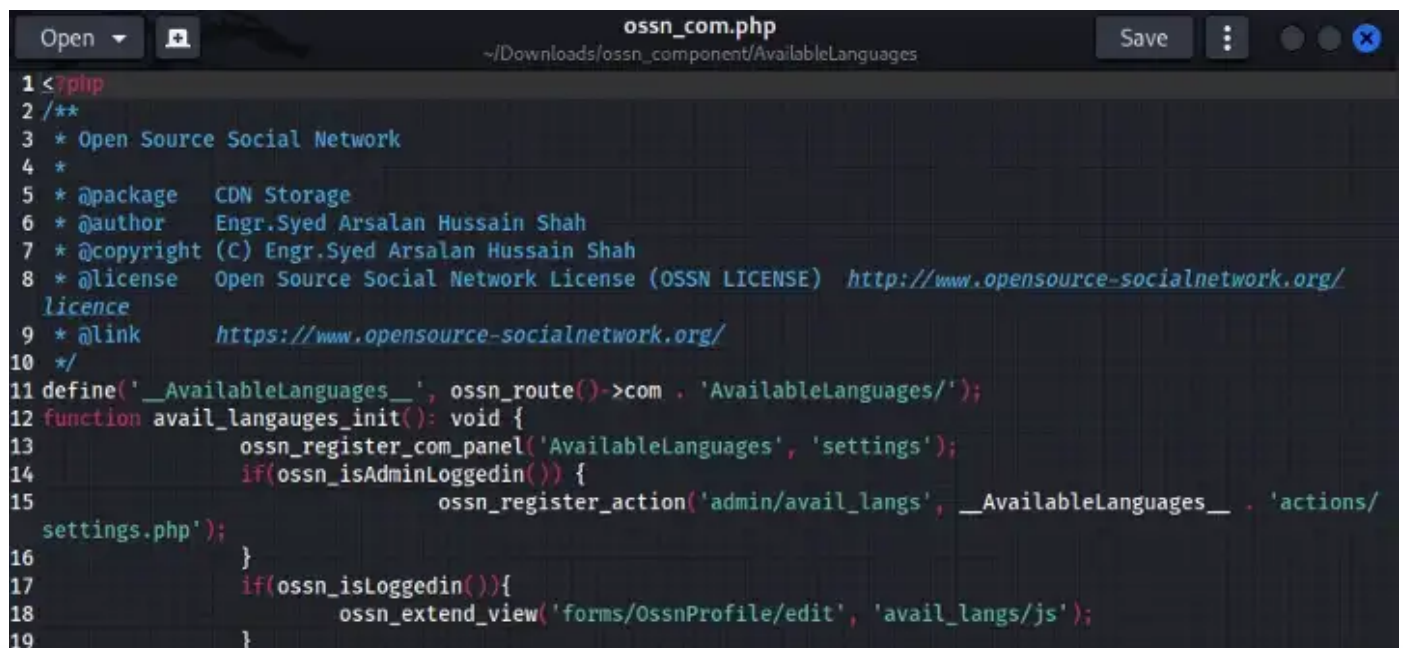
<https://www.opensource-socialnetwork.org/component/view/5909/languages-list>

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



[Open in app](#)[Get started](#)

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





Open in app

Get started

Edit content of ossn\_com.php to PHP reverse shell.





[Open in app](#)

Get started

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

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





Open in app

Get started

`http://<IP>/osn/administrator/com_installer`

Choose the archive that we create.

Choose the archive that we create.





Open in app

Get started

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

Using netcat to listen for TCP connections on port 443.





[Open in app](#)[Get started](#)

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

`http://<IP>/osn/components/AvailableLanguages/osn_com.php`

`http://<IP>/osn/components/AvailableLanguages/osn_com.php`

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





Open in app

Get started

### 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>





[Open in app](#)

[Get started](#)

[About](#) [Help](#) [Terms](#) [Privacy](#)

Get the Medium app

