Cyber Youth Singapore

Instagrain

horizontal line

**Creator Name: Kok Rui**

# Setup:

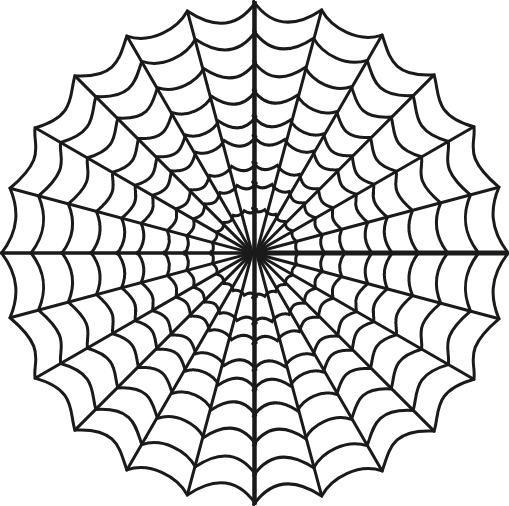
## **Static Files:**

* 1. grain.php
  2. flag\_bhjabd1iu23bkjsad.txt

## **Usage:**

* 1. Put grain.php in html folder
  2. Create an uploads directory, full permissions granted to all users (chmod 777)
  3. Make sure directory listing is banned
  4. Make sure php file uploads are allowed
  5. Attach the source code in chall desc

# Description:

* **Description:**
  + The Singapore Farmers’ Association has launched a new social media platform to rival Instagram - where farmers can proudly flaunt pictures of their latest grain harvests. You’ve been invited to beta-test - can you find a secret file in their servers?
* **Hints:**
  + Look closely at what php functions are carrying out the “checks”, and how they work
  + This challenge draws inspiration from both Web and Forensics categories!
  +  a simple one will do

# Solution

1. Notice that the challenge lets you access (and hence run) the file you uploaded
2. Google and figure out that php’s getimagesize() checks for file signatures
3. Craft payload, either
   1. add a jpeg signature then immediately follow by php backdoor,
   2. or take a normal jpeg, edit one of the exif fields to your php backdoor
4. Upload payload, access it and get web shell access, cat the flag file