Penetration Test Report

Pulkit Sanadhya

December 4, 2019

Contents

Executive Summary

Background

The goal of this exercise is to exploit the vulnerability in php script.

Recommendation Summary

The kali attack box will be used for this purpose .

Technical Report

Exploitation

Here , we initially went to the kali website www.m3g4c0rp.com/brian and tried to log in but it required admin credentials for the purpose.

Now , we went to the link www.m3g4c0rp.com/robots.txt are found the entry in the robot file where the link for htpasswd was defined as www.m3g4c0rp.com/brian/imgfiles/htpasswd , but we were unable to go to this link as it required admin username and password.

We opened an image file and went through the source code for that image and found that the vulnerability in php script can be exploited as by typing the following URL as :

www.m3g4c0rp.com/brian/getimage.php?raw=truefile=imgfiles /htpasswd

So we got the htpasswd file we used john the ripper against it to find that the password for the user brian was found to be swordfish , now we tried using these credentials and were able to get admin access into the system.

Now after logging into the admin panel and going through the the source code of the panel , we observed that only .jpg or .png files were allowed to be uploaded into the console. So if we can upload a file by simply renaming it to .jpg or .png we can easily upload the file, which seems to be a potential vulnerability.

We used the tool laudanum to gain shell access to the website by uploading the php file shell.php and renaming it as shell.php.jpg

Now changed the configuration file in laudanum so that after gaining the shell access the username will be admin and the password will be password .

Now , we uploaded the file shell.php.jpg and used burpsuite to capture this communication and modified the file from shell.php.jpg to shell.php and changed the content type from image/jpeg to text/html.

Now , after successfully uploading the file , we typed in the URL http://www.m3g4c0rp.com/brian/imgfiles/shell.php and were able to get access to laudanum shell and used the credentials as username as admin and password as password.

Now , as we saw the entries in robot.txt , we went to the directory /var/www/html/brian/private and changed the permission settings by using the command chmod 777 pivate , and in that directory we can see a file named ”ThisIsTheFileYouAreLookingFor” which is obviously the file that we should open and see and after opening the file we found the key19 :

KEY019:vBA+ Y/x7fG/x1cug/x7fP/x1cI/x0f//x06y@./x0a

These PHP vulnerabilities can be mitigated by carefully designing the web applications and taking preemptive precautions against such threats.

Conclusion

Hence ,we successfully were able to exfiltrate the sensitive information and find the key19.