
Blind OS command injection with output redirection

1. This lab contains a blind OS command injection vulnerability in the feedback function.
2. The application executes a shell command containing the user-supplied details. The output from the command is not returned in the response. However, you can use output redirection to capture the output from the command. There is a writable folder at: /var/www/images/
The application serves the images for the product catalog from this location. You can redirect the output from the injected command to a file in this folder, and then use the image loading URL to retrieve the contents of the file.
3. First, I think to pass the output of the command to /var/www/images/ and read it because the bug is blind and this file is writable.
4. I do same steps as the previous lab and I detect that the email variable is vulnerable. So, the payload is same plus a little something new.
Payload: || whoami > /var/www/images/test.txt ||
The response is 200 OK. So, Maybe the injection success.
5. The next step, I open any product's image and the URL is:
<https://0ad800f804d2d2608027a8bd00b1008a.web-security-academy.net/image?filename=54.jpg>
I changed it to:
<https://0ad800f804d2d2608027a8bd00b1008a.web-security-academy.net/image?filename=test.txt>
and I got it. The current user is **peter-QokVqk**