How to Protect phpMyAdmin Using Nginx?

written by sysadmin | 31 December 2025

The previous article explained how to install phpMyAdmin with the nginx web server. This article will explain how to protect phpMyAdmin from unauthorized users using nginx.

Problem

How to protect phpMyAdmin using nginx?

Solution

There are several methods to protect phpMyAdmin using nginx:

1. Allowing certain IPs

The phpMyAdmin application can only be accessed by users who have certain IP addresses. For example, you want the IP localhost, and only 192.168.56.1 to be able to access phpMyAdmin. Then add the script below to the **/etc/nginx/sites-available/default** file in the **location /phpmyadmin** section:

```
allow 127.0.0.1;
allow 192.168.56.1;
deny all;
```

For more details, take a look at the image below:

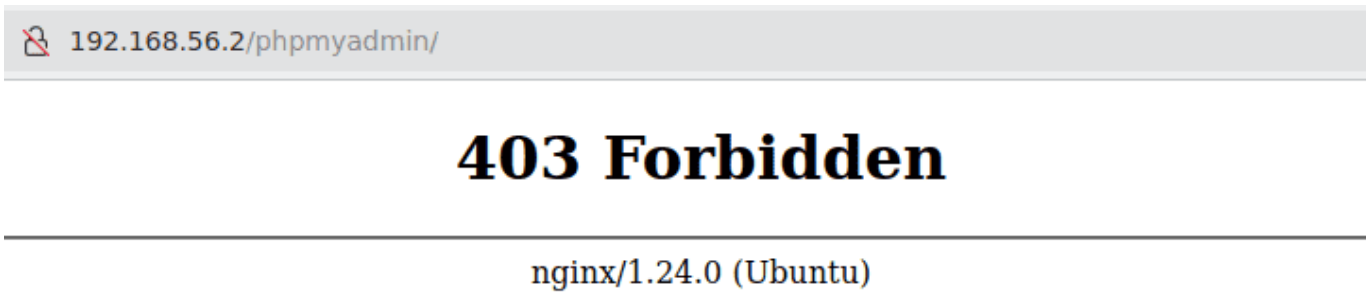
```
location /phpmyadmin {
    root /usr/share/;
    index index.php;

    allow 127.0.0.1;
    allow 192.168.56.1;
    deny all;

    location ~ ^/phpmyadmin/(.+\.php)$ {
        try_files $uri =404;
        root /usr/share/;
        fastcgi_pass unix:/run/php/php8.3-fpm.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        include fastcgi_params;
    }

    location ~* ^/phpmyadmin/(.+\.(css|js|jpg|jpeg|gif|png|ico|html|xml|txt))$ {
        root /usr/share/;
    }
}
```

Allowing certain IPS

After that, use the command below to reload nginx:

```
sudo nginx -t
sudo systemctl reload nginx
```

If any user who uses an IP other than the localhost and 192.168.56.1 wants to access phpMyAdmin, then that user will not be able to access phpMyAdmin, as shown in the image below:



```
Forbidden access
```

2. Add a password

To make it safer, phpMyAdmin should be given additional HTTP Auth so that users who want to access the application must enter a password. Use the command below to install HTTP auth:

```
sudo apt install apache2-utils
sudo htpasswd -c /etc/nginx/.phpmyadmin admin
```

Enter the password that you want, and then in the **/etc/nginx/sites-available/default** file, add the script below:

```
auth_basic 'Restricted';
auth_basic_user_file /etc/nginx/.phpmyadmin;
```

So the default file will look like the image below:

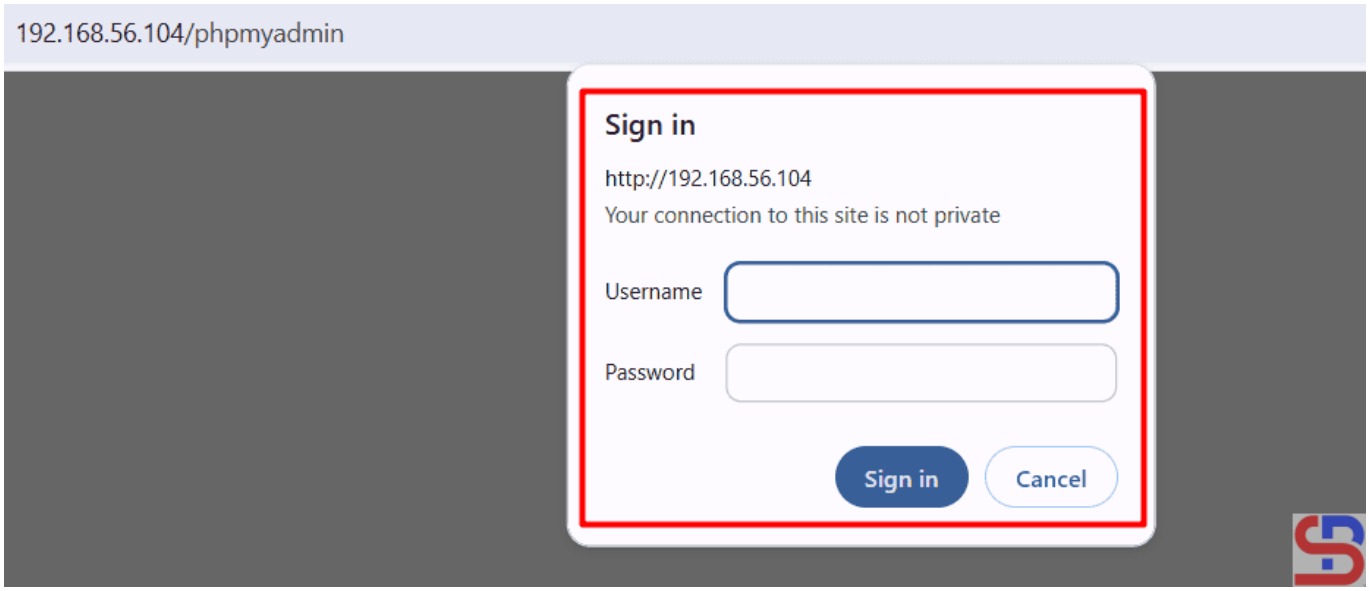
```
location /phpmyadmin {
    root /usr/share/;
    index index.php;

    allow 127.0.0.1;
    allow 192.168.56.1;
    deny all;

    auth_basic "Restricted";
    auth_basic_user_file /etc/nginx/.phpmyadmin;


    location ~ ^/phpmyadmin/(.+\.php)$ {
        try_files $uri =404;
        root /usr/share/;
        fastcgi_pass unix:/run/php/php8.3-fpm.sock;
        fastcgi_index index.php;
        fastcgi_param SCRIPT_FILENAME $document_root$fastcgi_script_name;
        include fastcgi_params;
    }

    location ~* ^/phpmyadmin/(.+\.(css|js|jpg|jpeg|gif|png|ico|html|xml|txt))$ {
        root /usr/share/;
    }
}
```

Adding HTTP Auth in Nginx

After that, use the command below to reload nginx:

```
sudo nginx -t
sudo systemctl reload nginx
```

Open the browser, and when you access phpMyAdmin, it should be there should be a display like below:



Enter username and password when accessing phpMyAdmin

Enter the username: **admin** and the password you created previously. If there are no errors, you can access phpMyAdmin.

3. Change the URL

By default, if you want to access phpMyAdmin, then you type the command below:

```
http://ip_server/phpmyadmin
```

However, for security reasons, it is best to replace the word phpMyAdmin with another word, for example, **pma,** so that the site address changes to:

```
http://ip_server/pma
```

Therefore, in the default file, change the file by deleting the **/phpmyadmin** section with the script below:

```
location /pma {
        alias /usr/share/phpmyadmin/;
        index index.php;

        allow 127.0.0.1;
```

```
        allow 192.168.56.1;
        deny all;

        auth_basic "Restricted";
        auth_basic_user_file /etc/nginx/.phpmyadmin;

        location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.3-fpm.sock;
        fastcgi_param SCRIPT_FILENAME $request_filename;
        }

        location ~* \.(css|js|jpg|jpeg|gif|png|ico|html|xml|txt)$ {
        expires 30d;
        access_log off;
        }
    }
```

so that the default file changes to look like the image below:

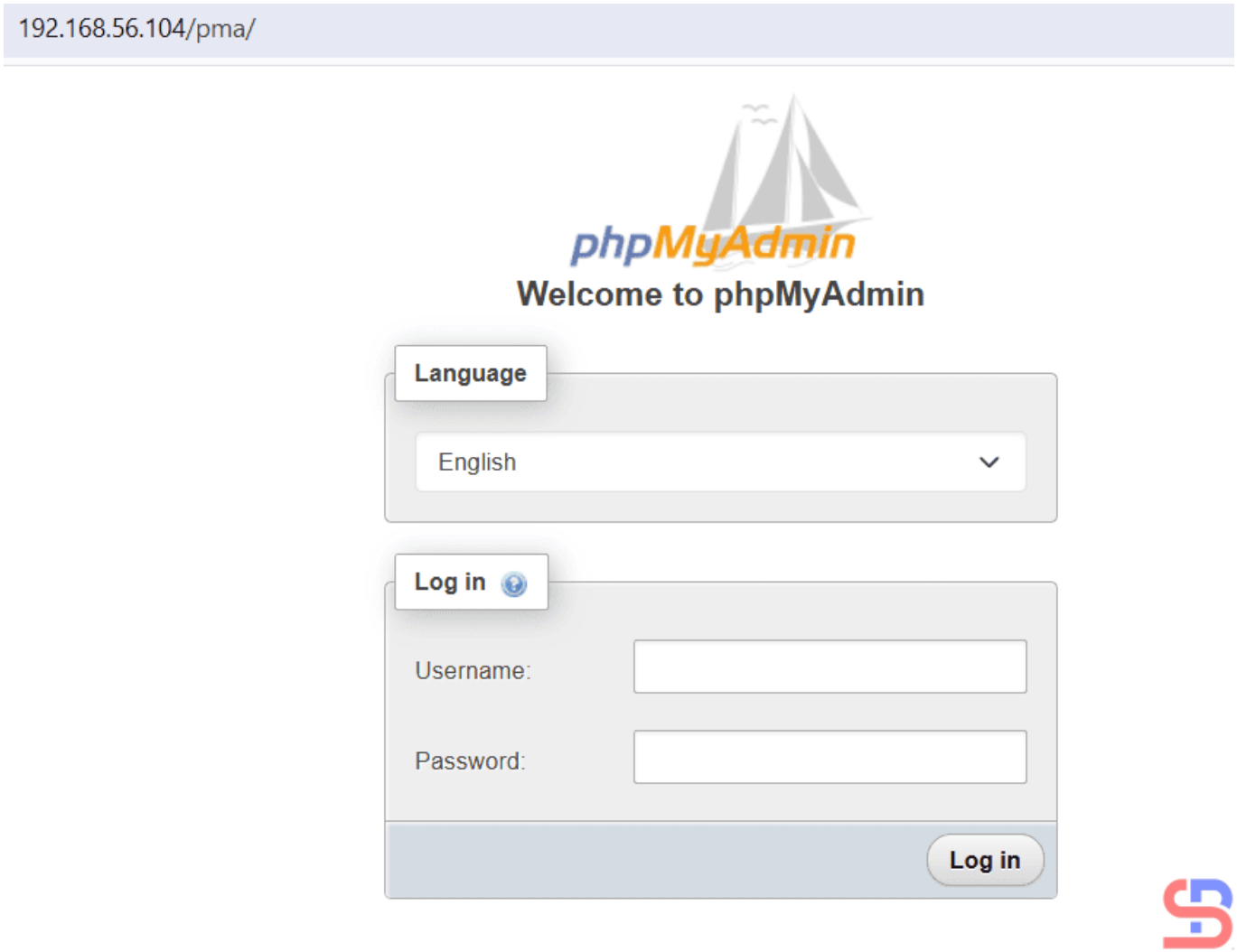
```
server {
    listen 80;
    server_name _;
    root /var/www/html;
    index index.php index.html;

    location / {
        try_files $uri $uri/ =404;
    }

    location /pma {
        alias /usr/share/phpmyadmin/;
        index index.php;

        allow 127.0.0.1;
        allow 192.168.56.1;
        deny all;

        auth_basic "Restricted";
        auth_basic_user_file /etc/nginx/.phpmyadmin;

        location ~ \.php$ {
        include snippets/fastcgi-php.conf;
        fastcgi_pass unix:/run/php/php8.3-fpm.sock;
        fastcgi_param SCRIPT_FILENAME $request_filename;
        }

        location ~* \.(css|js|jpg|jpeg|gif|png|ico|html|xml|txt)$ {
        expires 30d;
        access_log off;
        }
    }
}
```

Change the URL in Nginx

Use the command below to reload nginx:

```
sudo nginx -t
sudo systemctl reload nginx
```

Open **http://ip_server/pma** in your browser, then you should be able to access phpMyAdmin as in the image below:



Change the URL

Note

There is one more method so that your phpMyAdmin application can be secure, namely, using SSL. You can use a Let’s Encrypt SSL certificate for your phpMyAdmin site because the certificate is free. However, if you want the phpmyadmin application not to be accessed by the public, I think, then there is no need to use SSL.

References

digitalocean.com
serverfault.com
httpd.apache.org