

-Indexes [redacted]

[redacted] HTTPS

PmaControl [redacted] HTTP [redacted] HTTPS [redacted]

```
<VirtualHost *:80>
    ServerName pmacontrol.internal.company.com
    Redirect permanent / https://pmacontrol.internal.company.com/
</VirtualHost>

<VirtualHost *:443>
    ServerName pmacontrol.internal.company.com
    SSLEngine On
    SSLCertificateFile /etc/ssl/certs/pmacontrol.pem
    SSLCertificateKeyFile /etc/ssl/private/pmacontrol.key

    # [redacted] TLS
    SSLProtocol -all +TLSv1.2 +TLSv1.3
    SSLCipherSuite HIGH:!aNULL:!MD5:!3DES

    DocumentRoot /srv/www/pmacontrol
</VirtualHost>
```

[redacted]

PmaControl [redacted]

```
<Location />
    Require ip 10.0.0.0/8
    Require ip 172.16.0.0/12
    Require ip 192.168.0.0/16
</Location>
```

[redacted] PmaControl [redacted] VPN [redacted] Apache [redacted]

[redacted]

Apache [redacted] default.conf [redacted] IP [redacted]

```
a2dissite 000-default.conf
systemctl reload apache2
```

⏏

⏏ HTTP ⏏

```
Header always set X-Content-Type-Options "nosniff"
Header always set X-Frame-Options "SAMEORIGIN"
Header always set X-XSS-Protection "1; mode=block"
Header always set Referrer-Policy "strict-origin-when-cross-origin"
Header always set Content-Security-Policy "default-src 'self'; script-src 'self' 'unsafe-
inline'; style-src 'self' 'unsafe-inline'"
```

2 ⏏ PHP

⏏

PmaControl ⏏ exec() ⏏ shell_exec() ⏏

⏏ Web ⏏

```
; php.ini ⏏ DocumentRoot ⏏ .user.ini
disable_functions = exec,shell_exec,system,passthru,popen,proc_open
expose_php = Off
```

⏏ CLI ⏏ Aspirateur⏏Listener⏏

```
; php-cli.ini - ⏏ shell_exec
disable_functions =
```

⏏ Web ⏏

⏏

```
session.cookie_httponly = 1
session.cookie_secure = 1
session.cookie_samesite = Strict
session.use_strict_mode = 1
session.name = PMACSESSID
```

cookie_httponly JavaScript Cookie XSS Secure HTTP Strict SameSite = Strict CSRF

```
upload_max_filesize = 2M
post_max_size = 8M
max_execution_time = 30
max_input_time = 60
memory_limit = 256M
```

PmaControl

PHP

```
expose_php = Off
```

HTTP Powered-By: PHP/8.x

3 MariaDB

PmaControl

PmaControl

```
-- 
REVOKE ALL PRIVILEGES ON *.* FROM 'pmacontrol'@'localhost';

-- 
GRANT SELECT, INSERT, UPDATE, DELETE ON pmacontrol.* TO 'pmacontrol'@'localhost';
GRANT SELECT ON performance_schema.* TO 'pmacontrol'@'localhost';
GRANT REPLICATION CLIENT ON *.* TO 'pmacontrol'@'localhost';
GRANT PROCESS ON *.* TO 'pmacontrol'@'localhost';

FLUSH PRIVILEGES;
```

PmaControl

Localhost

PmaControl

```
[mysqld]
bind-address = 127.0.0.1
```

[[PmaControl [REDACTED]

[REDACTED]

```
[mysqld]
general_log = OFF          # [REDACTED]
slow_query_log = ON
long_query_time = 1
log_error = /var/log/mysql/error.log
```

[REDACTED] SQL [REDACTED]

4 [REDACTED]

[REDACTED]

PmaControl [db]config.ini.php [REDACTED]

```
; configuration/db.config.ini.php
[default]
driver = mysql
host = 127.0.0.1
port = 3306
login = pmacontrol
password = "ENCRYPTED_VALUE_HERE"
database = pmacontrol
crypted = 1
```

crypted=1 [REDACTED] PmaControl [REDACTED]

[REDACTED]

[REDACTED]

- **Vault** [HashiCorp] PmaControl [REDACTED] API [REDACTED]
- **AWS Secrets Manager** [GCP Secret Manager] [REDACTED]
- [REDACTED]

```
# 设置环境变量
export PMAC_DB_PASSWORD="secret_value"
export PMAC_SSH_PASSPHRASE="ssh_secret"
```

设置权限

```
# 设置 www-data 用户对 Apache 文件的权限
chown root:www-data /srv/www/pmacontrol/configuration/*.php

# 设置 www-data 用户对 Apache 文件的权限
chmod 640 /srv/www/pmacontrol/configuration/*.php

# 设置 www-data 用户对数据库配置文件的权限
chmod 600 /srv/www/pmacontrol/configuration/db.config.ini.php
```

5 ACL 配置

acl.config.ini

PmaControl 的 ACL 配置文件

```
; configuration/acl.config.ini
[admin]
* = allow

[dba]
Slave = allow
Server = allow
Dashboard = allow
Backup = deny
Config = deny

[readonly]
Slave = allow
Server = allow(show)
Dashboard = allow
* = deny
```

设置

- `Config Backup Install Api` `XXXXXXXXXX`
- `XXXXXXXXXXXXXXXXXXXX`
- `XXXXXXXXXXXX` ACL `XX`

`XXXXXX`

`XXXXXXXXXX`

```
[admin]
Install = allow      ; XX/XX
Config = allow      ; XXXX
Api = allow          ; XX REST API
Backup = allow       ; XXXXXXXX

[dba]
Install = deny       ; XXXXXXXX
Config = deny
Api = allow(read)   ; XX API XXXX
Backup = deny
```

6 `XX` CSRF `XXXXXXXXXX`

`XXXXXX`

`XX` PmaControl `XXXXXXXXXX` CSRF `XX`

```
<form method="POST" action="/slave/start/42/">
  <input type="hidden" name="csrf_token" value="<?= $csrf_token ?>">
  <button type="submit">Start Slave</button>
</form>
```

`XXXXXXXXXXXXXXXXXXXX`

```
if ($_POST['csrf_token'] !== $_SESSION['csrf_token']) {
  throw new SecurityException('Invalid CSRF token');
}
```

`XXXXXXXXXX`

`XXXXXXXXXXXXXXXXXXXX`

iptables

```
# 配置 HTTP/HTTPS
iptables -A INPUT -p tcp --dport 80 -s 10.0.0.0/8 -j ACCEPT
iptables -A INPUT -p tcp --dport 443 -s 10.0.0.0/8 -j ACCEPT
iptables -A INPUT -p tcp --dport 80 -j DROP
iptables -A INPUT -p tcp --dport 443 -j DROP

# 配置 localhost MySQL
iptables -A INPUT -p tcp --dport 3306 -s 127.0.0.1 -j ACCEPT
iptables -A INPUT -p tcp --dport 3306 -j DROP
```

配置

PmaControl 配置

- 配置
- 配置 SSH
- 配置

配置 VPN、WireGuard、OpenVPN、SSH

10 SQL 注入

配置 SQL 注入

文件	配置	效果
Tag.php	WHERE	
Client.php		
Environment.php	ORDER BY	
Backup.php	LIKE	

配置

```
// Tag.php - 配置
$sql = "SELECT * FROM tags WHERE name LIKE '%" . $_GET['search'] . "%'";
$results = $db->query($sql);
```


