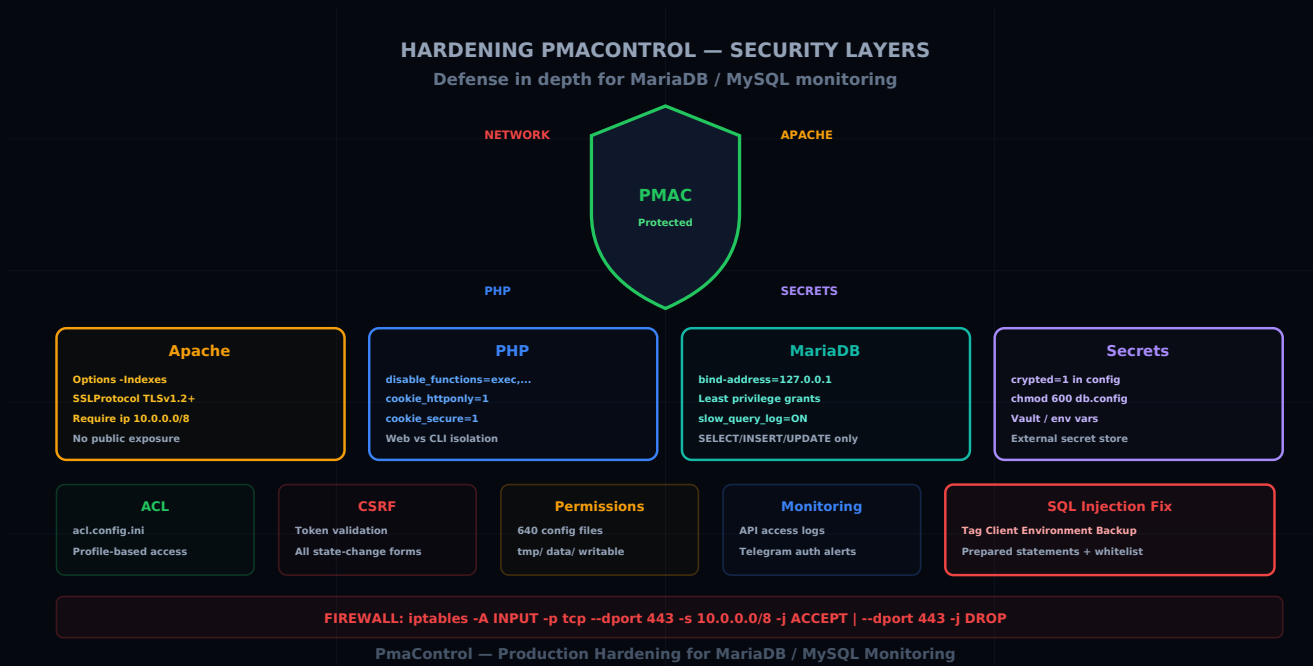


نامأل ليلد :جاتنإل ايف PmaControl بلصت لمالكال

Aurélien LEQUOY · 13 ليربأ 2026

PMACONTROL SECURITY HARDENING APACHE PHP MARIADB



ةكلمملا حيتافم هيدل PmaControl

لاصتالادامتعا تانايب نيزختب موقى MariaDB / MySQL جاتنإل مداوخ ىلع فرشي PmaControl. قارتخاب نيمجاهملا دحأ ما اذإ، تانايبلا ةدعاق ةينب وءادأل سيسي اقمو SSH حيتافمو تانايبلا ةدعاق ةيساسأل ةينبلا ىلإ لوصولاق هيدل نوكة نأ لم تحت حمل نمف لمالكال.

يف PmaControl عضو لبق اهقبي بطت بحج يتلا ةيوقتلا تاءارجإ لىصافات ليلدل اذ هوضو ACL، رارسأل، Apache، PHP، MariaDB، ةقبط لك يطغيو يلىخاد نيمأ قيقدت نم يتأي هنإ، جاتنإل ةقبط قارملاو تافلما تانودأ، CSRF.

يشتابأ: ىلوالا ةقبطلا

ليلدل ةمئاق لىطعت

تمام عمل بـرسـت اذه .سـرهـف فلم نودب لئالـدلـا تايوتـحم ضـرع Apache لـنـكمـي ،أيـضـارتـفا :

```
<Directory /srv/www/pmacontrol>
  Options -Indexes
  AllowOverride All
  Require all granted
</Directory>
```

يـلـع روثـعـلاو عورشمـلا ةيـنـب فاشـكـتـسا مجاهـمـلل نـكمـي ،اهـنـودب .ضـوافـتـلل لـباقـريغ `Indexes-
بـلـاقـمـلاو تـالـجـسـلـاو نيـوكـتـلا تـافـلم

HTTPS ضرف

مجاهـمـلل نـكمـي ،HTTPS نودب .HTTP تابلـطـي حـضـاو صـنـب دامتـعـالا تانايـب لـقـني PmaControl
اهـضـارتـعا ةـكـبـشـلا يـلـع :

```
<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

  # Modern TLS only
  SSLProtocol -all +TLSv1.2 +TLSv1.3
  SSLCipherSuite HIGH:!aNULL:!MD5:!3DES

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

ةيـلـخـادلـا ةـكـبـشـلا يـلـع رصـتـقي

ةـكـبـشـلا يـلـلـو صـولا دـيـقـت .تـنـرتـنـإـلا يـلـع هـضـرع مـتـي نـأ ادبـأ يـغـبـنيـال PmaControl
ةيـلـخـادلـا :

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

Apache ربيع قال طإلإل ىلع هفشكت ال و VPN ةكبش فلخ PmaControl عض :كلذ نم لصفألأ وأ امال.

يضرارتفالل فيضم الة لازإ

صاخ ال IP ناو نع ىلع مالعتسا يأل (000-default.conf) يضرارتفالل Apache فيضم بيحجتسي هفذح .مداخالاب:

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

نامأل س وؤر

HTTP نامأل س وؤر فضا:

```
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'"
```

PHP :ةي ناثلة قبطلال

ةرطخال فئاطوالا لي طعت

نمكي ال لجالاو .(ةومحمل، SSH) ةني عم تاي لمعل shell_exec() و exec() PmaControl مدختسي اه لئو جاتحي نذل لامعل لزع في لب ،ملاعالا ىوتسم ىلع اه لي طعت في

(ةهجالا) بيولا فيضملة بسنلاب:

```
; php.ini ou .user.ini dans le DocumentRoot
disable_functions = exec,shell_exec,system,passthru,popen,proc_open
```

```
expose_php = Off
```

(عمتسمل، ةيئابرهكلا ةسنكمل) CLI في نيلماعلل:

```
; php-cli.ini – ces workers ont besoin de shell_exec  
disable_functions =
```

ةرغث مجاهملا دج وول ىتح، ماظنلا رماو أ ذيفنت ىلع بيولا ةهجو ةردق مدع لصفلا اذه نمضي وةني.

ةنم آتاسلج

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

cookie_httponly (XSS ةيامح) ةسلجلا طابترا فيرعت فلم ىلإ لوصلو نم JavaScript عنمي.
cookie_secure CSRF نم يمحّي `cookie_samesite = Strict` طوق HTTPS ربع لاسرإلا صرفي.

ذيفنتلاو لي محتلا نم دحلا

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

موجهلا حطس ليلقتل دحلا. ةمخضتاليمحت ىلإ جاتحي ال PmaControl.

PHP ةخسن ءافخإ

```
expose_php = Off
```

HTTP تاباتسا نم X-Powered-By: PHP/8.x سار ةلازا ىلإ اذه يدؤي.

ةقبطلا 3: MariaDB

مدخات سمل ا تازا ي ت م ا دي ق ت PmaControl

ه دي ق ت . ة ل م ا ك ل ل ا ت ا ز ا ي ت م ا ل ا ب PmaControl م د خ ت س م ل ا ع ت م ت ي ا م ا ب ل ا غ ، ت ي ت ب ث ل ا د ع ب :

```
-- Révoquer les privilèges excessifs
REVOKE ALL PRIVILEGES ON *.* FROM 'pmacontrol'@'localhost';

-- Accorder uniquement ce qui est nécessaire
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;
```

ه ت د ع ا ق ي ل ل ة ب ا ت ك ل ل ا و س ي ي ا ق م ل ا ة ء ا ر ق ي ل ل ا ط ق ف ج ا ت ح ي PmaControl : ل ق ا ل ا ز ا ي ت م ا ل ا ا د ب م ة . ص ا خ ل ل

ي ل ح م ل ا ف ي ض م ل ا ب ط ب ر

ه ي ل ح م ل ا ة ه ج ا و ل ا ي ل ع ط ق ف PmaControl ت ا ن ا ي ب ل ا ة د ع ا ق ع م ت س ت ن ا ب ح ي :

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

ب ب س د ج و ي ا ل ف ، (ي ج ذ و م ن ل ا ن ي و ك ت ل ل ا) م د ا خ ل ل ا س ر ف ن ي ل ع ن ي د و ج و م ه ت د ع ا ق و PmaControl ن ا ك ا ذ ا ة . ك ب ش ل ل ا ر ب ع ع ا م ت س ل ل

ة س ا س ح ل ا ت ا ب ل ط ل ل ا ل ي ح س ت ن ي ك م ت

```
[mysqld]
general_log = OFF          # Trop verbeux en production
slow_query_log = ON
long_query_time = 1
log_error = /var/log/mysql/error.log
```

ر ي ش ت د ق ي ت ل ل ا ة ي ع ي ب ط ل ل ا ر ي غ ت ا م ا ل ع ت س ل ل ا ف ا ش ت ك ا ي ف ي ط ب ل ل ا م ا ل ع ت س ل ل ا ل ج س د ع ا س ي ة . ل غ ت س م SQL ة ن ق ح ي ل ل

ر ا ر س ا ل ا : ة ب ا ر ل ل ا ة ق ب ط ل ل ا

دامتعالا تانايب ريفشت

معددي فللملا اذه `db.config.ini.php` ي ف لوخدلا ليجسرت دامتعالا تانايب نزيخ PmaControl ريفشلتال:

```
; 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
```

حاتفم .ل.يغشلتال تقو ي ف رورملا ةم لك ريفشت ك فب PmaControl `crypted=1` ةمالعالا ربخت ن.نيوكتال فللم ن ع لصفنم ريفشلتال

اي جراخ آي رس أنزخم مدختسا

رارسلال لة جراخ رداصمب ةناعسلااب مق ،ةمهملال جاتنإلارشن تاي لمعل ةبسنلاب:

- **Vault** (HashiCorp): رارسلال ةءارق PmaControl عيطتسي
- **AWS Secrets Manager** و **GCP Secret Manager**: ةباحسلالارشن تاي لمعل
- يداعلال صنللا نم لصفأ ، قيبطتلال لباقلا يندألا دلح: **ةئيبلال تاريغتم**

```
# Exemple avec variables d'environnement
export PMAC_DB_PASSWORD="secret_value"
export PMAC_SSH_PASSPHRASE="ssh_secret"
```

نيوكتال تافل مةي امح

```
# Propriétaire : www-data (l'utilisateur Apache)
chown root:www-data /srv/www/pmacontrol/configuration/*.php

# Permissions : lecture pour le groupe, rien pour les autres
chmod 640 /srv/www/pmacontrol/configuration/*.php

# Le fichier de credentials ne doit être lisible que par www-data
chmod 600 /srv/www/pmacontrol/configuration/db.config.ini.php
```

(لوصول في مكحلتل مئاوق) ACL :ةسماخلة قةبطلا

مءارة acl.config.ini

فلم acl.config.ini فلملا دءء. ففءءءل فلم ىلع مئاوق ACL ماظن ىلع PmaControl ففءءءل. مءءءل ءءو ىلإ لوصول هءكءم فذلا ففءءل.

```
; 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
```

ةسماخلة ءءوقلا

- لوصول ءوءف ءأ بءء `Config` , `Backup` , `Install` , `Api` :ةسماخلة مءءءل ءءءو ءءقءء طقف ءف لوؤسم لل آءاءم اهفءلإ
- لءءء ءوء ءراشءسا ىلإ ءوءءءءف ءف ذلا ءف روءم لل :طقف ءءءءل ففءءء فلم ءاشءل
- ACL مئاوقب ءاطغم ءفاضملا ءءءءل مءءءل ءءءو ءأ ءءءءءءل

ءماهلا ءفاهءللا طاقء ءفءءء

صاآ لكشء ءسماخلة ءفاهءللا طاقء ضءب:

```
[admin]
Install = allow ; Installation / réinstallation
Config = allow ; Modification de la configuration
Api = allow ; API REST complète
Backup = allow ; Accès aux backups (contient des données)
```

```
[dba]
Install = deny      ; JAMAIS accessible aux non-admins
Config = deny
Api = allow(read)   ; Lecture seule via API
Backup = deny
```

عقاوملا ربع تابلاطال ريزوت) CSRF: سداسلا ةقبطلا

زيمللا زومرلا دوجو نم ققحتلا

زيمللا CSRF زمر PmaControl جذوم نك نمضتي نأ بجي:

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

زيمللا زومرلا ةحص نم ققحتلا مكحتلا ةدحو ىلع بجي، مداخل بناج نم:

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

ةبولوأك ةيامحلا تاءارجإ

ةيماهه رثكأل يه ةلاحلا لدعت يتلا تاءارجإلا:

- ققيرلا فاقبي / ادب
- أطخلا يطخت
- مداخل ةلازا / ةفاصإ
- نيوكتلا ليدعت
- مدختسمللا فذح / ءاشنإ

مدخل لثامتملا خسنلا فاقبي ىلع لصتملا DBA رابجإ مجاهملا نكمي، CSRF ةيامح نودب
ههلا خخفم طبار لاسرا قيرط نع جاتنإلا.

فلمللا تانودأ: ةعباسلا ةقبطلا


```
$_SERVER['REQUEST_URI'],
http_response_code()
);
file_put_contents('/var/log/pmacontrol/api.log', $log . "\n", FILE_APPEND);
```

ةقداصملا لشرف دنع مارجي ليت تاهي بنت

للاصتالاي ف لشرف لك ل Telegram هبنت دادعإب مق

```
if (!$auth->isValid()) {
    Telegram::send(
        "☐☐ Auth failure on PmaControl\n" .
        "IP: " . $_SERVER['REMOTE_ADDR'] . "\n" .
        "User: " . $_POST['login'] . "\n" .
        "Time: " . date('Y-m-d H:i:s')
    );
}
```

تقوم رطح ثودح ل لإقئاقد 5 لال خ IP ناونع سفن نم لشرف تالاح ثال ث يدؤت نأ بجي

نيوكتلا تافل مةبقارم

اهب حرصملا ريغ تاريخيغتللا فاشتكال ةهباشم ةادأ وأ inotifywait مدختسا

```
inotifywait -m -r /srv/www/pmacontrol/configuration/ -e modify,create,delete |
while read path action file; do
    echo "[$action] $path$file" >> /var/log/pmacontrol/config_changes.log
    # Envoyer alerte Telegram
done
```

ةكبشلا : 9 ةقبطالا

ةياملال راج دعاق

```
# Autoriser HTTP/HTTPS uniquement depuis le réseau interne
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
```

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

مَاع ضَرَعَم دَجْوِي ال

نإف، ةقداصملا عم ىتح .تترتنإلا ربع هيلإ لوصولا أحاتم نوكتي نأ أدبأ يغبنني ال PmaControl
أدج ري ب ك موحهلا حطس:

- فارشإلل ةعضاخلا مداوخلا دامتعا تاناي ب نيزخت متي
- SSH حيتافم نيزخت متي
- جاتنإلا مداوخ ىلع تاءارجإلا ذيفنت ةهجاولا كل حيتت

SSH، قفن وأ VPN (WireGuard، OpenVPN) مدختساف، أبولطم دعب نع لوصولا ناك اذا

جالعلا - SQL نقحلا :10 ةقبطلا

مكحت تادجوع برأ في SQL نقحلا رطاخم انيدل يلخادلا قيقدتلا دج:

جالع	رطخ	يلاملا بقارملا
تاملعم تاذ تامالعسا	WHERE ةلمجل يكيما نيديلا انبلا	Tag.php
تاملعم تاذ تامالعسا	تاحش رمل في لسلسلا	Client.php
دومعلل ءاضيبلا ةمئاقلا	BY بيترتلاب ريغتملا ءافيتسالا	Environment.php
تاملعم تاذ تامالعسا	LIKE في اهؤاغلا متي مل ةلمعم	Backup.php

(ةفيعضلا) لبق:

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

(نم) دعب:

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

ديحولاً نم آلا ل حلأ هه ءاضي بلأ ةمئاقلا نإف، ORDER BY تارابع ل ةبسنلاب

```
$allowed_columns = ['name', 'created_at', 'id'];
$sort = in_array($_GET['sort'], $allowed_columns) ? $_GET['sort'] : 'name';
$sql = "SELECT * FROM tags ORDER BY " . $sort;
```

بلصتلا ةعجارم ةمئاق

ةطقن لك ةحص نم ققحت، جاتنإل في PmaControl عضو لب

- [] نكمم -Indexes :يشتابأ
- [] یرسقل HTTPS :يشتابأ
- [] ةيلخادلا ةكبشلا لىل إ دقم لوصو :يشتابأ
- [] يضارتفال فيضملا ةلازإ تم :يشتابأ
- [] بولأ فيضم لىل ةريطخل فئاطولا ليطعت م : PHP
- [] PHP: session.cookie_httponly = 1
- [] PHP: session.cookie_secure = 1
- [] PHP: expose_php = 0ff
- [] تازايمالا نم یندألا دلابل ءتمت تي مدختسم : MariaDB
- [] MariaDB: bind-address = 127.0.0.1
- [] ةرفشملا دامتعالا تاناي ب : رارسألا (crypted=1)
- [] 640 تانوذألا :نيوكتلا تافل م
- [] ةدقم ةساسحل مكحتلا تادحو : ACL
- [] تاءارجلال لكشأ عيمجل ةزيمملا زومرلا : CSRF
- [] ةباتكلل ةلباقلا تادلجملا طقف /data/ و /tmp/ :تانوذألا
- [] API لوصولو لجلس :ةبقارملا
- [] ةقداصملا لشف دنع تاهي بنت :ةبقارملا
- [] دوجوم ةيامحل رادج :ةكبشلا
- [] ماع ضرع دجوي ال :ةكبشلا
- [] يطايتحالأ خسنلاو ةئيبللاو لي مغلأو ةمعالأ في اهنيوكت مت يتلا تامالعئسالا : SQL

ةصالخا

مداوخ ىلى لوصولا ةينامإب ةادألا عتمتت .مازتلا وه لب - افرت سىل PmaControl نىمأت نإ
SSH ربع رماوألا ذىفنت اهنكمىو ،دامتعالا تانايب نىزختو ،MariaDB / MySQL جاتنإلا

،تانودأ،Apache, PHP, MariaDB, Secrets, ACL, CSRF) ةقبط لك :تاقبط يف بلصتلا ةيلمع متت
مجاهملا ئطبت ىرخألا تاقبطلال نإف ،تاقبطلال ىدحإ قارتخا مت اذإ .أزجاج فىضت (ةكبش

ال ةفلكتلا .دحاو لمع موى فى قىببطلل ةلباقو ةىساق رىبادتلا هذه لك :راسلا ربخلالو
كب ةصاخلا تانايبالا ةدعاقل ةىتحتلا ةىنبلاب ساسملا رطاخمب ةنراقم ركذت