Slack的$ 1.000 SSRF

156****3330 / 2019-02-24 08:20:00 / 浏览数 1129 安全技术 WEB安全 顶(0) 踩(0)

在开始之前，对于任何从BugBounty开始的人来说，我有两个重要提示。

1：始终检查以前的报告，您可能知道在这种情况下可能有效的旁路，或者您可以学习新的东西。

2：如果您喜欢有关Bug Bounty或其他黑客相关内容的内容，请注册我的频道并关注新帖子。

SLACK和SSRF：

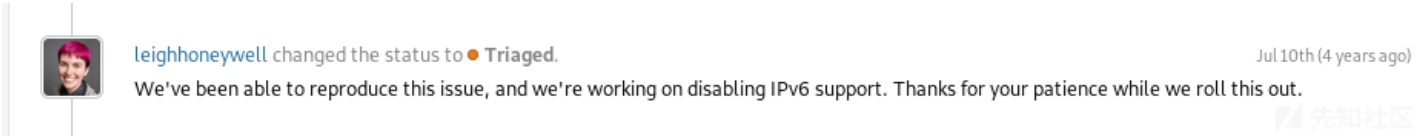
Slack是一个协作中心，它将合适的人员，信息和工具结合在一起，以完成工作。从财富100强公司到角落市场，全球数百万人使用Slack连接他们的团队，统一他们的系统，

斜杠命令 Slash Commands

“api.slack.com中的SSRF，使用斜杠命令并绕过保护措施。”

您可以在此处了解有关Slash Commands的更多信息：

“一些Slack功能，如”Integrations / Phabricator”和”Integration / Slash Commands”允许用户提交将由后端服务器访问的URL。黑名单试图禁止访问内部资源（loopback，10.0.0.0 / 8,192.168.0.0 / 24，...）。可以使用”[::]”作为主机名绕过此黑名单。只有使用该向量才能到达绑定所有接口和支持IPv6的服务。”



Slack已禁用在Slash命令中注册IPV6地址的选项。

slacka：' 我为ipv6阻止创建了一个新问题，并与我们的工程师一起升级了案例。当我们有更新时，我会通知你。'

对他们来说，一个修复，对我来说，一个旁路。

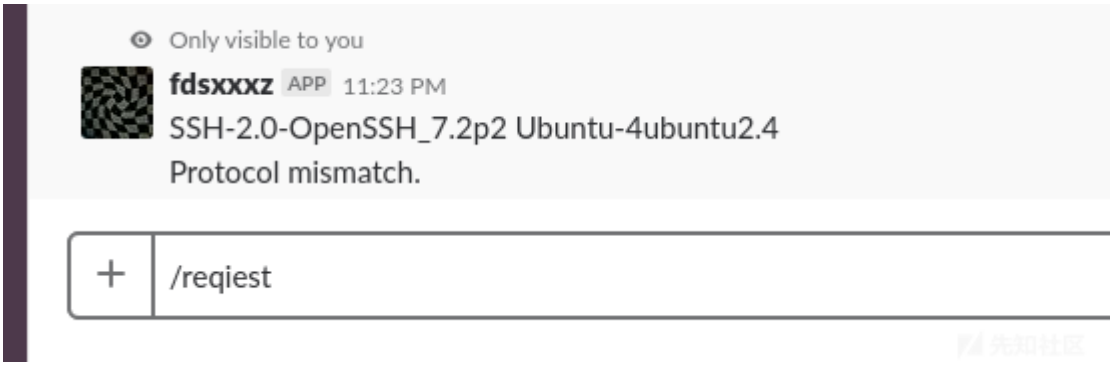
为了绕过这种新的保护，我在PHP中使用了带有“Location”标题的重定向。

在您自己的域中：index.php

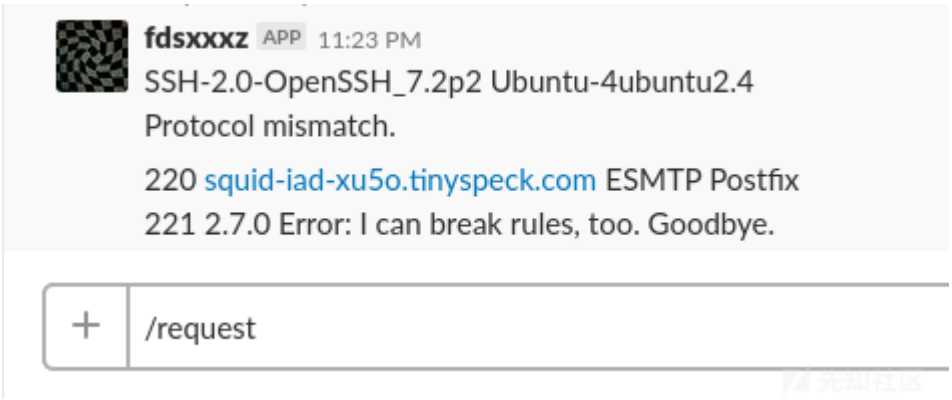
```
<?php
header("location: http://[::]:22/");
?>
```

location: http://[::]:22/
并保存。
转到你的Slack并输入/ youslash
试试我的服务器http：// hackerserver [。] com /

结果
:22



:25



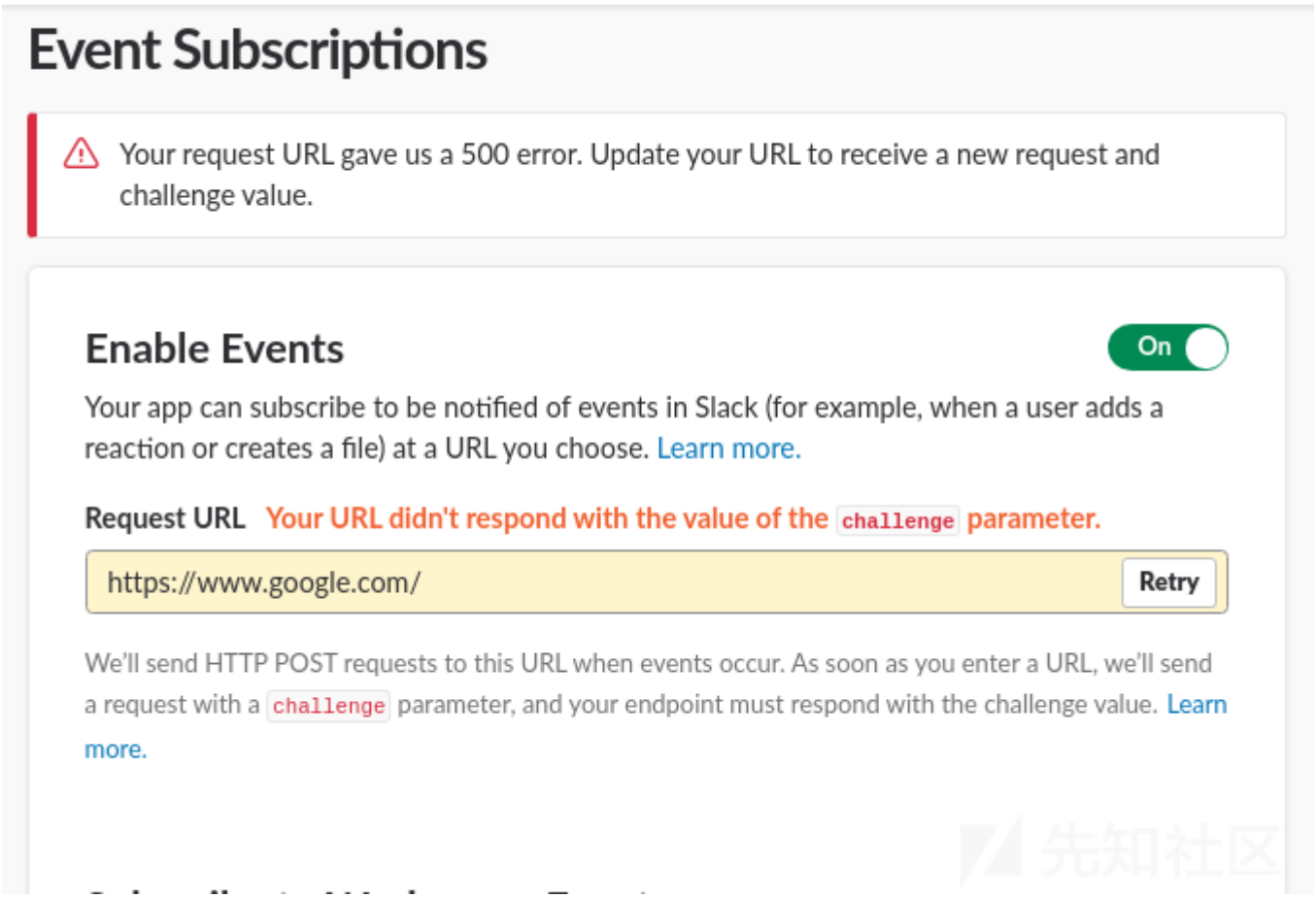
7月13日 - 第一回应
7月18日 - Tri CC
于1月23日 - Slack以500美元的奖金奖励了elber。

在找到此绕过之后，我在Slack中寻找了更多漏洞，并找到了Event Subscriptions参数。

“在事件订阅参数中绕过SSRF保护。”

该漏洞出现在“事件订阅”参数中，其中：
“ Your app can subscribe to be notified of events in Slack (for example, when a user adds a reaction or creates a file) at a URL you choose.”。
URL：https://api.slack.com/apps/YOUAPPCODE/event-subscriptions?

当我们添加不符合API标准的网站时，我们会收到以下消息：



Your request URL gave us a 500 error. Update your URL to receive a new request and challenge value.

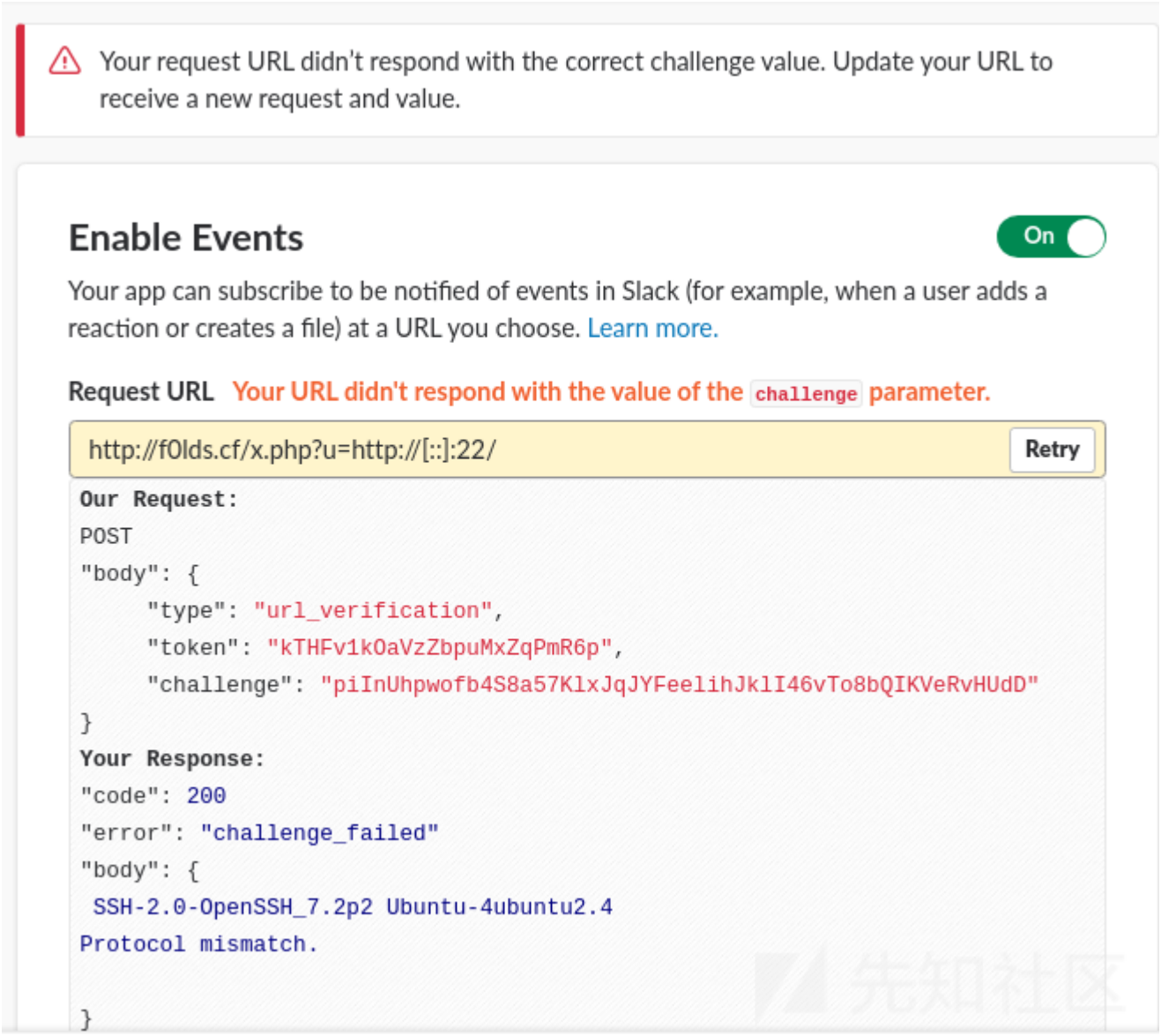
使用IPV6向量旁路[::]。

在我的host上，x.php有：

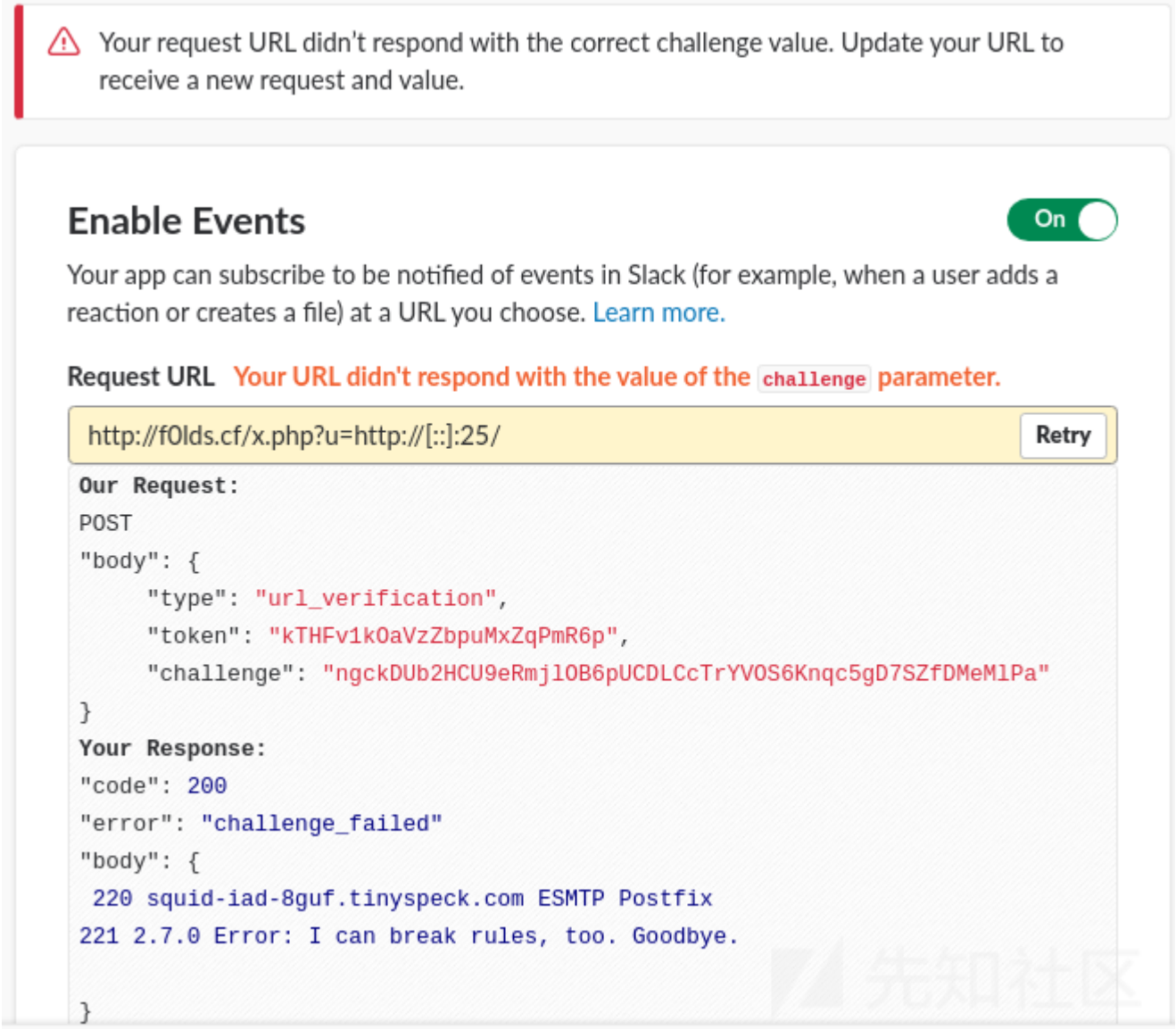
```
<?php
header("location: ".$_GET['u']);
?>
```

PoC:
http://hacker.site/x.php/?u=http://%5B::%5D:22/

Response:
SSH [::]:22



SMTP [::]:25



这份报告Slack被选为另一个SSRF的副本，我坚持说他们把我作为另一个报告的参与者。

我看到另一份报告与我的不同，所以我告诉团队他们可能是错的。

参考文献：
https://hackerone.com/reports/61312

（报告将于02/22在Hackerone上公开披露）

https://hackerone.com/reports/381129

https://hackerone.com/reports/386292

原文地址：https://medium.com/@elberandre/1-000-ssrf-in-slack-7737935d3884

目录