关于视频课

- 目的：在实际项目中，我们学习的知识是如何被使用的
- 涉及到代码的部分，建议在 PC 上收看

极客时间

22. 从 CVE-2018-9230 说起

关于 CVE-2018-9230

极客时间

CVE-2018-9230 Detail

Current Description

** DISPUTED ** In OpenResty through 1.13.6.1, URI parameters are obtained using the ngx.req.get_uri_args and ngx.req.get_post_args functions that ignore parameters beyond the hundredth one, which might allow remote attackers to bypass intended access restrictions or interfere with certain Web Application Firewall (ngx_lua_waf or X-WAF) products. NOTE: the vendor has reported that 100 parameters is an intentional default setting, but is adjustable within the API. The vendor's position is that a security-relevant misuse of the API by a WAF product is a vulnerability in the WAF product, not a vulnerability in OpenResty.

Source: MITRE
Description Last Modified: 04/20/2018

- 影响面：很多开源的 WAF 是基于 OpenResty 开发的
- 存在争议：并非 OpenResty 的安全漏洞

学习目的

极客时间

- 获取用户上传参数相关 API 介绍
- 如何正确阅读 OpenResty 文档
- 代码中如何做安全防护
- OpenResty 如何看待和处理安全隐患

攻击手段

极客时间

- OpenResty 中的 ngx.req.get_uri_args、ngx.req.get_post_args 和 ngx.req.get_headers，默认返回前 100 个参数

- 参数溢出：攻击者可以填入 100 个无用参数，把 payload 放在第 101 个参数中，借此绕过 WAF 的检测

为什么不是 OpenResty 的漏洞?

- 以 ngx.req.get_uri_args 为例，旧版本的文档如下：

```
ngx.req.get_uri_args
--------------------
-**syntax:** *args = ngx.req.get_uri_args(max_args?)*

-Note that a maximum of 100 request arguments are parsed by default (including those with the same name) and that
 additional request arguments are silently discarded to guard against potential denial of service attacks.
```

```
50
51  - local args = ngx.req.get_uri_args(0)
52   ```
53
54   Removing the `max_args` cap is strongly discouraged.
```

- 提供了可选的 max_args 参数，来控制返回参数的个数，设置为 0 即全部返回

- 但强烈不建议设置为 0，这会带来更严重的安全漏洞：拒绝服务攻击。攻击者构造包含海量参数的请求，可以导致 worker 进程 CPU 满载

OpenResty 的处理方式

极客时间

- 第一时间响应
- 保持向下兼容
- 不能引入新的安全和性能问题
- 不做为安全漏洞处理，增加错误提示

升级后的 API


```
 ngx.req.get_uri_args
 --------------------
+**syntax:** *args, err = ngx.req.get_uri_args(max_args?)*

 +Note that a maximum of 100 request arguments are parsed by default (including those with the same name) and that
  additional request arguments are silently discarded to guard against potential denial of service attacks. Since
  `v0.10.13`, when the limit is exceeded, it will return a second value which is the string `"truncated"`.

+ local args, err = ngx.req.get_uri_args(10)
+ if err == "truncated" then
+     -- one can choose to ignore or reject the current request here
+ end
```

- 恰当的平衡：超过 100 个参数的请求，WAF 可以选择拒绝
- 我们永远都需要错误处理

如何避免?

- 仔细阅读 OpenResty 文档，每句话都是有含义的
- 转换安全防护思路，黑名单永远都会有漏网之鱼

被动和主动安全防护模式

- negative：黑名单规则，非黑即白
- positive：身份认证，非白即黑

```
if is_hacker():
    deny()
else:
    access_db()


if is_admin():
    access_db()
else:
    deny()
```

极客时间

Q&A