

【XCTF高手进阶区】web6_ics-06 writeup

原创

Mitch311 于 2021-02-13 20:51:21 发布 92 收藏 1

分类专栏: [CTF](#)

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/Mitchell_Donovan/article/details/113803260

版权



[CTF 专栏收录该内容](#)

51 篇文章 3 订阅

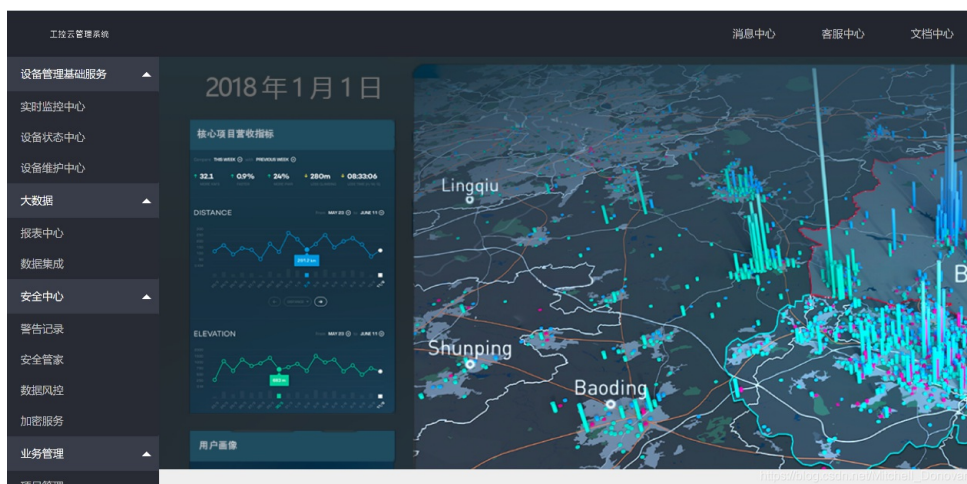
订阅专栏

web6_ics-06

[原题链接](#)

key: burpsuite 爆破 id

①环境打开后是这样的□



我把左侧导航栏里的链接试了个遍, 只有“报表中心”可以进入□



列表

日期范围

送分题

https://blog.csdn.net/Mitchell_Donovan

②这时发现地址栏多出了id=1□

我把id=1换成了id=2,3,4,5,6,7,8,9后，页面没有变化

再结合题干信息□

The screenshot shows a challenge titled 'ics-06' with a difficulty coefficient of 2.0. It is provided by Bleach and Bleachz. The source is XCTF 4th-CyberEarth. The description states: '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。'

猜测入侵者可能是想通过id来给自己创建一个后门，类似于一种密钥吧

我们的任务就是爆破出id

③burpsuite抓包，右键发送到Intruder爆破

首先确定爆破位置□

The screenshot shows the 'Payload Positions' configuration window in Burp Suite. The 'Attack type' is set to 'Sniper'. The base request is shown as: 'GET /index.php?id=§1§ HTTP/1.1'. The host is '111.200.241.244:58046'. The user agent is 'Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:85.0) Gecko/20100101 Firefox/85.0'. The accept headers are 'text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8'. The accept language is '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'. The connection is 'close'. The upgrade-insecure-requests is '1'. The cache-control is 'max-age=0'. A watermark 'https://blog.csdn.net/Mitchell_Donovan' is visible at the bottom.

随后进行payload设置□

Target Positions Payloads Options

Payload set: 1 Payload count: 1

Payload type: Numbers Request count: 1

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

To: 10000

Step: 1

How many:

https://blog.csdn.net/Mitchell_Donovan

payload类型设置为数字类型，数字类型设置为具体，范围设置为1到10000，步长设置为1

点击开始爆破

Target Positions Payloads Options

Request Headers

These settings control whether Intruder updates the configured request headers during attacks.

Update Content-Length header

Set Connection: close

Start attack

④爆破结果

Attack Save Columns

Results Target Positions Payloads Options

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length	Comment
2330	2329	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2331	2330	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2332	2331	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2333	2332	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2334	2333	200	<input type="checkbox"/>	<input type="checkbox"/>	1901	
2335	2334	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2336	2335	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2337	2336	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2338	2337	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2339	2338	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2340	2339	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	
2341	2340	200	<input type="checkbox"/>	<input type="checkbox"/>	1866	

https://blog.csdn.net/Mitchell_Donovan

返回报文长度不同的id是id=2333

直接去浏览器访问id=2333，得到flag

列表

日期范围

-

确认

cyberpeace{0e6aab5da4c9ecfb8d5589e041a18238}.in