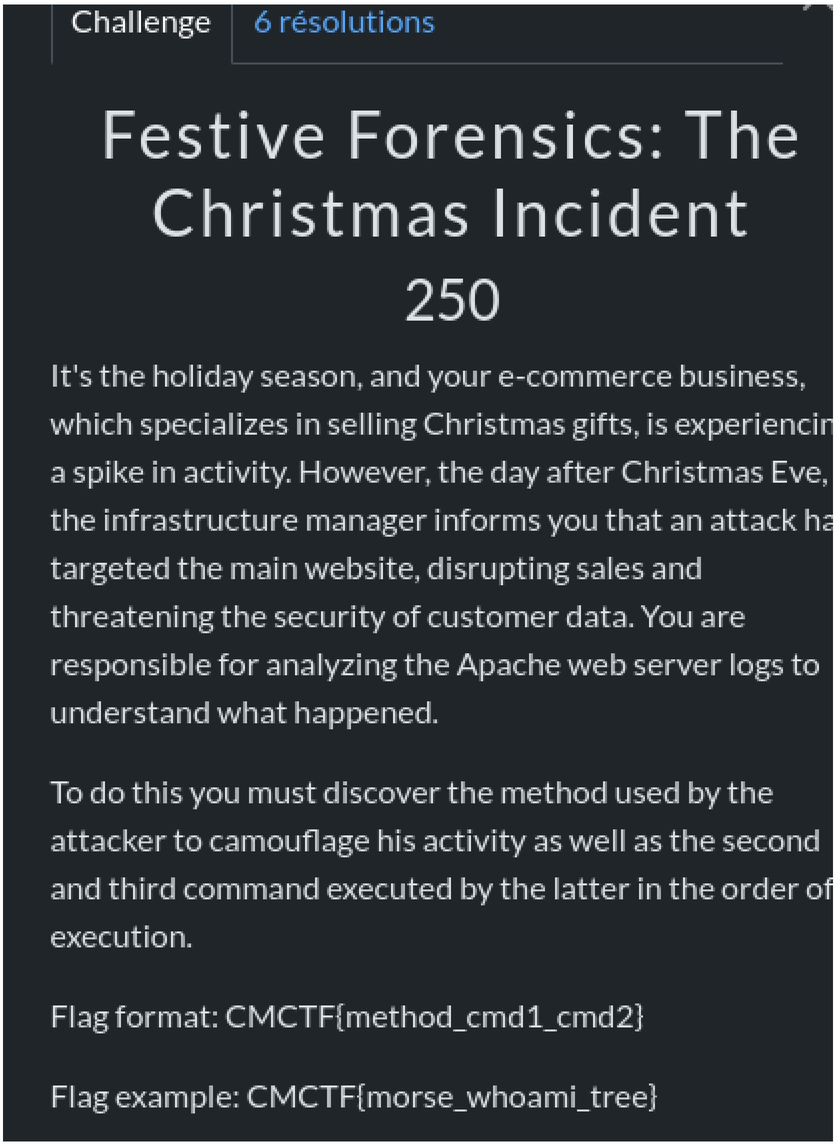
Writeup Festive Forensics: The Christmas Incident



Challenge 6 résolutions

Festive Forensics: The Christmas Incident

250

It's the holiday season, and your e-commerce business, which specializes in selling Christmas gifts, is experiencin a spike in activity. However, the day after Christmas Eve, the infrastructure manager informs you that an attack ha targeted the main website, disrupting sales and threatening the security of customer data. You are responsible for analyzing the Apache web server logs to understand what happened.

To do this you must discover the method used by the attacker to camouflage his activity as well as the second and third command executed by the latter in the order of execution.

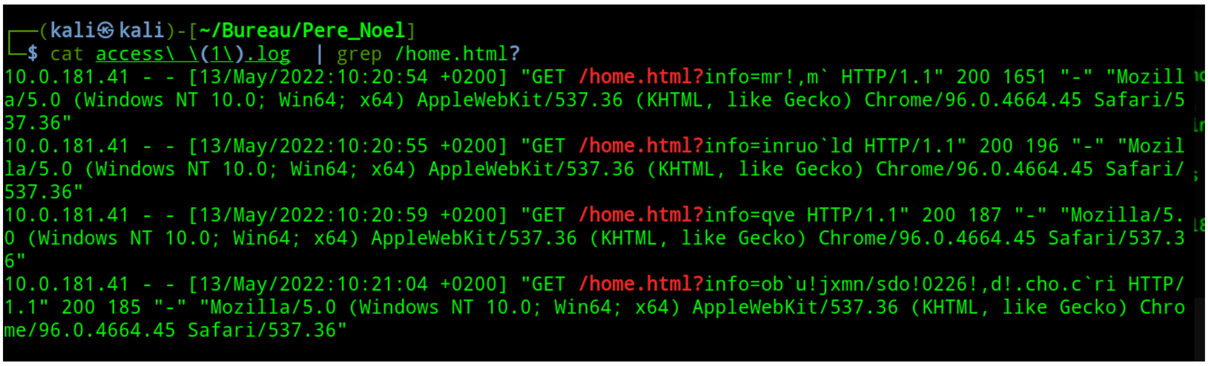
Flag format: CMCTF{method_cmd1_cmd2}

Flag example: CMCTF{morse_whoami_tree}

J ai ouvrir le fichier pour l analyse

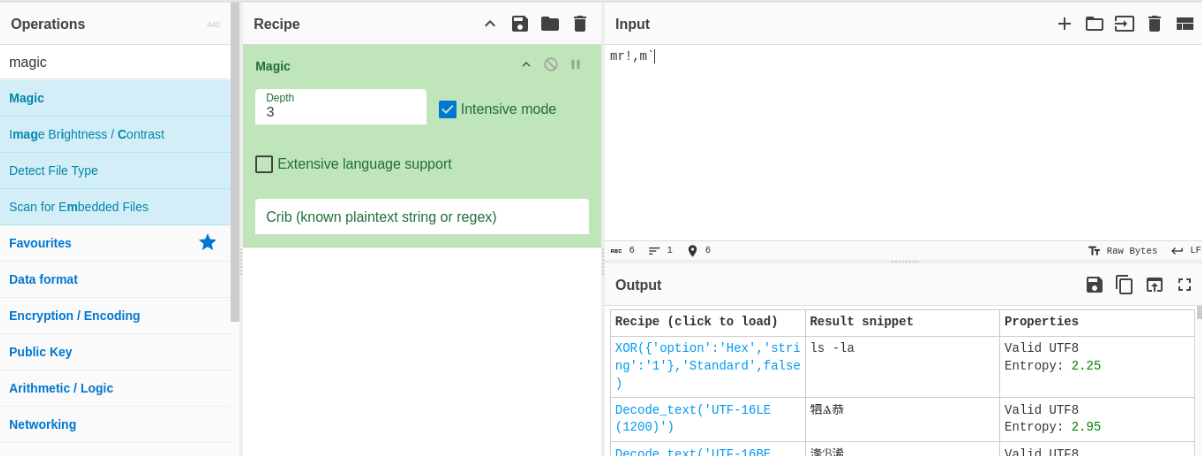
Si l'on analyse attentivement, on constate que seules les données des requêtes utilisant la méthode GET sont visibles. En effet, avec la méthode GET, les données sont transmises directement dans l'URL. Comme le fichier journal enregistre les chemins ou URLs, nous pouvons y voir ces données. En revanche, les données envoyées via les méthodes POST ou PUT restent invisibles, car elles sont transmises dans le corps de la requête, lequel n'est pas consigné dans le fichier journal.

j ai utuliser du grep



```
┌──(kali㉿kali)-[~/Bureau/Pere_Noel]
└─$ cat access\ \(1\).log  | grep /home.html?
10.0.181.41 - - [13/May/2022:10:20:54 +0200] "GET /home.html?info=mr!,m` HTTP/1.1" 200 1651 "-" "Mozill
a/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/5
37.36"
10.0.181.41 - - [13/May/2022:10:20:55 +0200] "GET /home.html?info=inruo`ld HTTP/1.1" 200 196 "-" "Mozil
la/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/
537.36"
10.0.181.41 - - [13/May/2022:10:20:59 +0200] "GET /home.html?info=qve HTTP/1.1" 200 187 "-" "Mozilla/5.
0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.3
6"
10.0.181.41 - - [13/May/2022:10:21:04 +0200] "GET /home.html?info=ob`u!jxmn/sdo!0226!,d!.cho.c`ri HTTP/
1.1" 200 185 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chro
me/96.0.4664.45 Safari/537.36"
```

Nous avions un paramètre info qui prends des valeur bizarre, ceux sont les cmd



magic

Magic

Depth 3

☑ Intensive mode

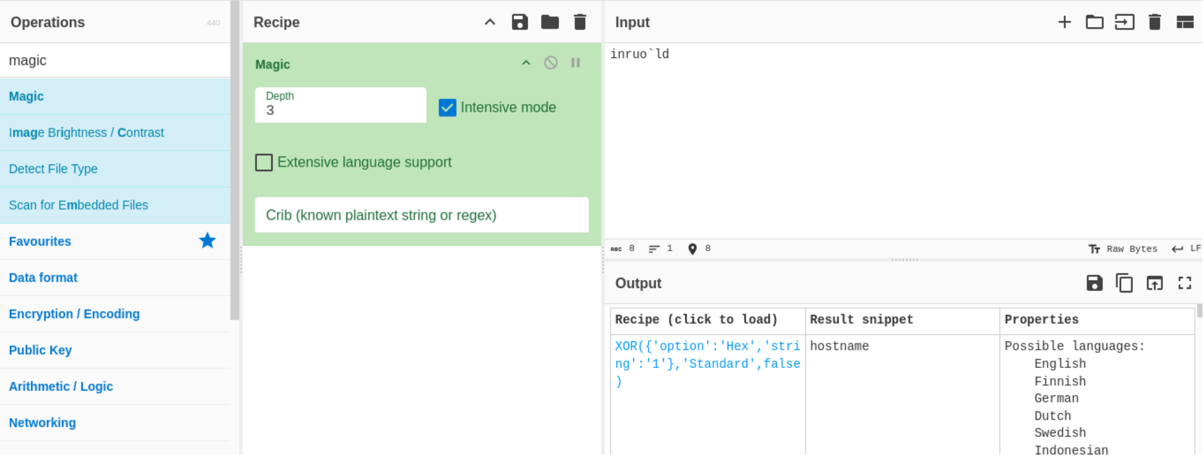
□ Extensive language support

Input:

```
mr!,m`
```

6 1 6

Recipe (click to load)	Result snippet	Properties
XOR({'option':'Hex','string':'1'},'Standard',false)	ls -la	Valid UTF8 Entropy: 2.25
Decode_text('UTF-16LE (1200)')	栒ⵡ恭	Valid UTF8 Entropy: 2.95
Decode_text('UTF-16BE	潲ⱡ湬	Valid UTF8



magic

Magic

Depth 3

☑ Intensive mode

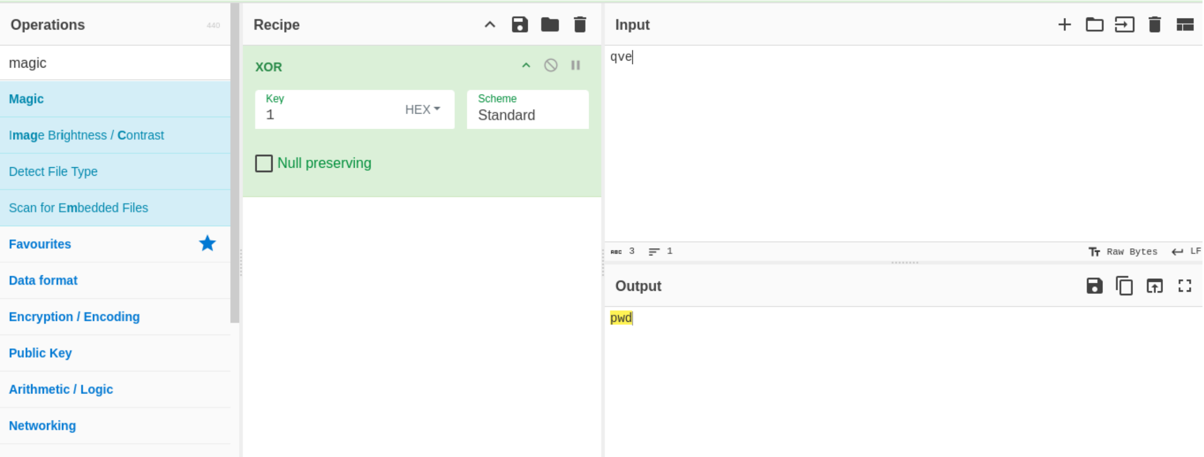
□ Extensive language support

Input:

```
inruo`ld
```

8 1 8

Recipe (click to load)	Result snippet	Properties
XOR({'option':'Hex','string':'1'},'Standard',false)	hostname	Possible languages: English Finnish German Dutch Swedish Indonesian



XOR

Key 1 HEX

Scheme Standard

□ Null preserving

Input: qve

Output: pwd

CMCTF{xor_hostname_pwd}

Writeup overhack