

Burpsuit中文处理及暴力破解应用

邑安科技 邑安全 2020-06-16 11:10:52

更多全球网络安全资讯尽在邑安全
www.eansec.com

BURPSUIT

目前我们在渗透测试中，经常会用到密码爆破这个功能项，常用的密码爆破的工具之一是BURPSUIT。遇到中文用户名的时候，很多同学不清楚需要转换字符编码的操作。下面我来演示下中文用户名的密码爆破，先贴2段测试用的代码。

```
<!-- Login.html -->
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8" />
    <title></title>
  </head>
  <body>
    <form action="login.php" method="post">
      账号: <input name="uname" /><br />
      密码: <input name="pwd" /><br />
      <input type="submit" />
    </form>
  </body>
</html>
```

```
<!-- login.php -->
<!DOCTYPE html>
<html>
  <head>
    <meta charset="utf-8" />
    <title></title>
  </head>
  <body>
    <?php
      /*接收用户输入*/
      $uname = $_POST['uname'];
      $pwd = $_POST['pwd'];

      if($uname == "管理员" && $pwd == "123456"){
        echo '登录成功';
      }
      else{
        echo '账号或密码错误';
      }
    ?>
  </body>
</html>
```

登录页面

账号：

密码：

提交查询



抓包并发送到intruder模块

Burp Project Intruder Repeater Window Help

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project

Intercept HTTP history WebSockets history Options

Request to http://[REDACTED]

Forward Drop Intercept is on Action

Raw Params Headers Hex

POST /login/login.php HTTP/1.1
Host: [REDACTED]
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 42
Origin: http://[REDACTED]
Connection: close
Referer: http://[REDACTED]/login/login.html
Upgrade-Insecure-Requests: 1

uname=%E7%AE%A1%E7%90%86%E5%91%98&pwd=2312

| | |
|--------------------|--------|
| Scan | |
| Send to Intruder | Ctrl+I |
| Send to Repeater | Ctrl+R |
| Send to Sequencer | |
| Send to Comparer | |
| Send to Decoder | |
| Request is blocked | |



选择Pitchfork

Burp
Project
Intruder
Repeater
Window
Help

Dashboard

Target

Proxy

Intruder

Repeater

Sequencer

Decoder

Comparer

Extender

Project options

2 x

...

Target

Positions

Payloads

Options

?

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the details.

Attack type:

Sniper

Sniper

Battering ram

Pitchfork

Cluster bomb

POST /login

Host:

User-Agent:

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: zh-CN,zh;q=0.8,en;q=0.6

Accept-Encoding: gzip, deflate

Content-Type: application/x-www-form-urlencoded

Content-Length: 42

Origin: http://

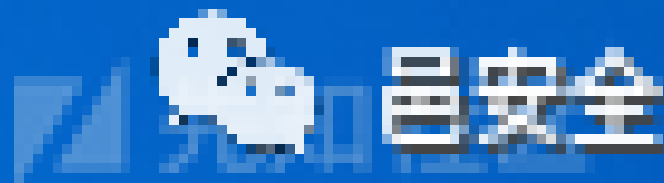
Connection: close

Referer: http:// /login/login.html

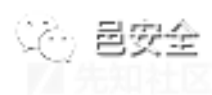
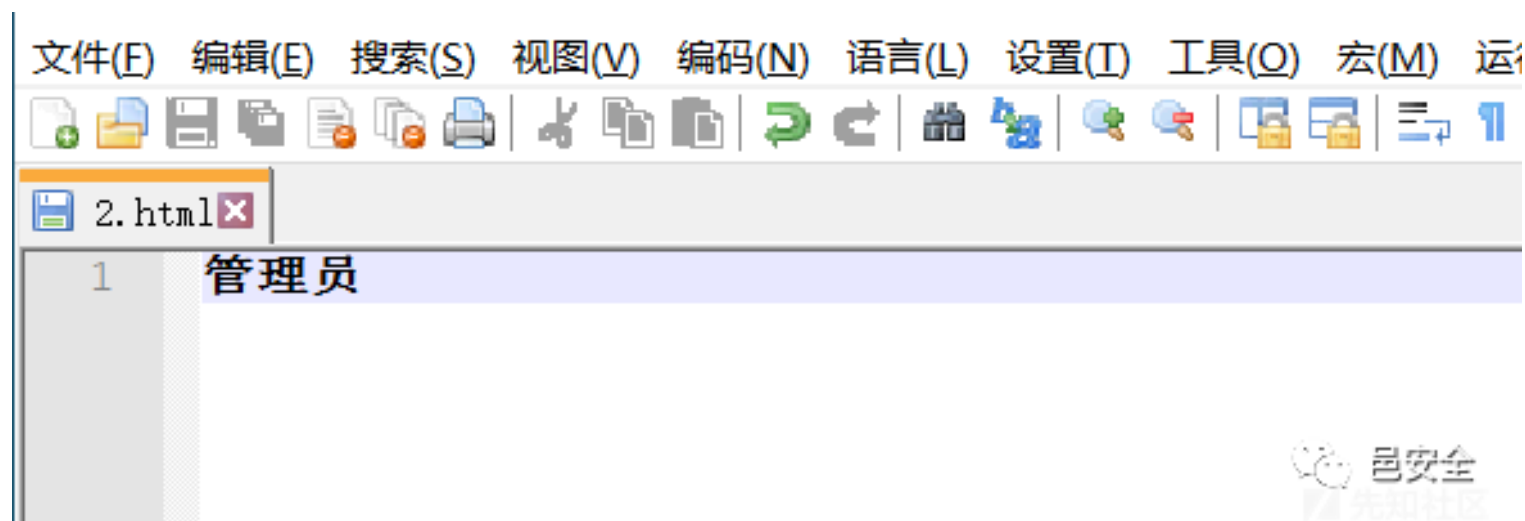
Upgrade-Insecure-Requests: 1

uname= \$ %E7%AE%A1%E7%90%86%E5%91%98 \$ &pwd= \$ 2312 \$

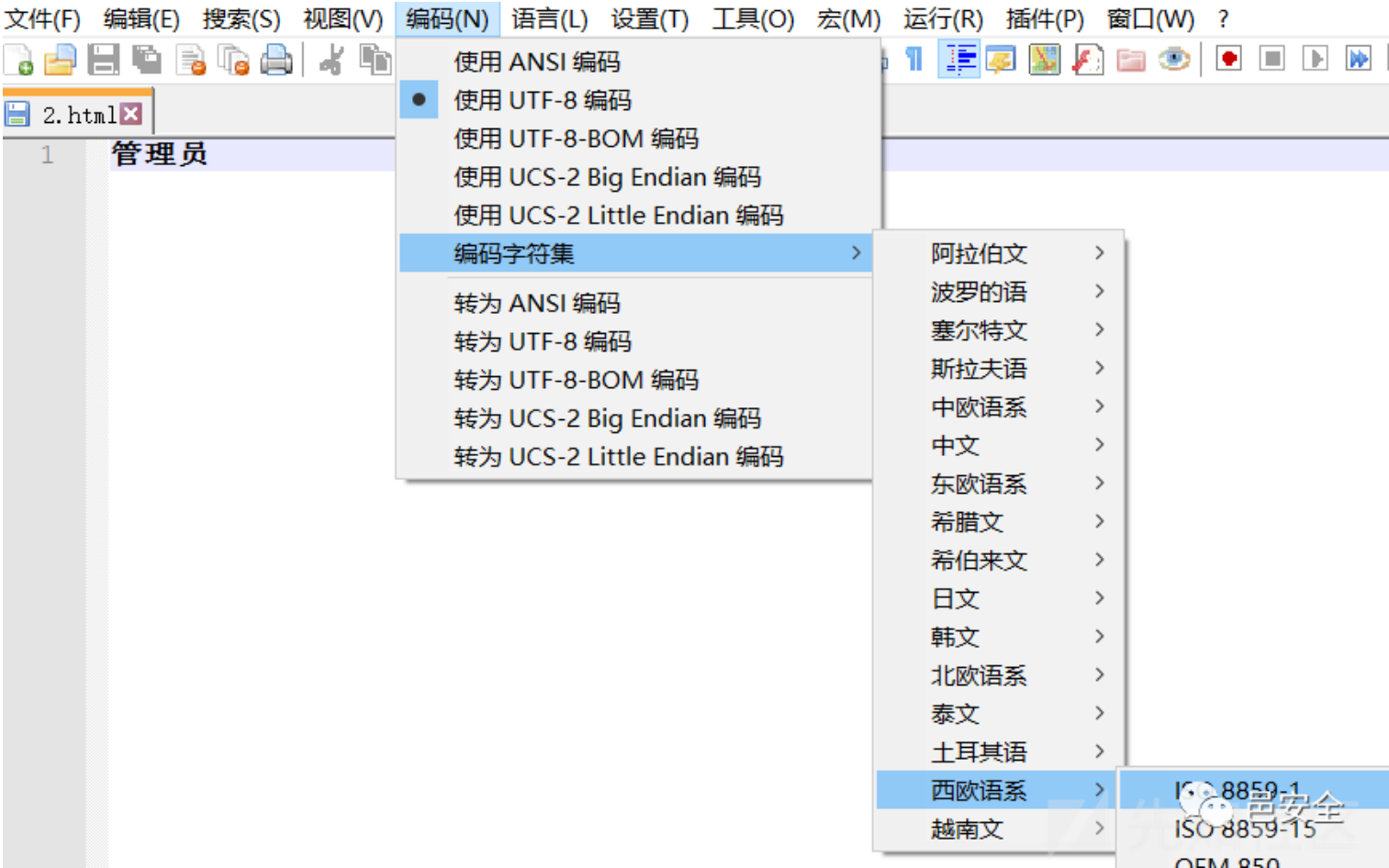
新建一个html文件



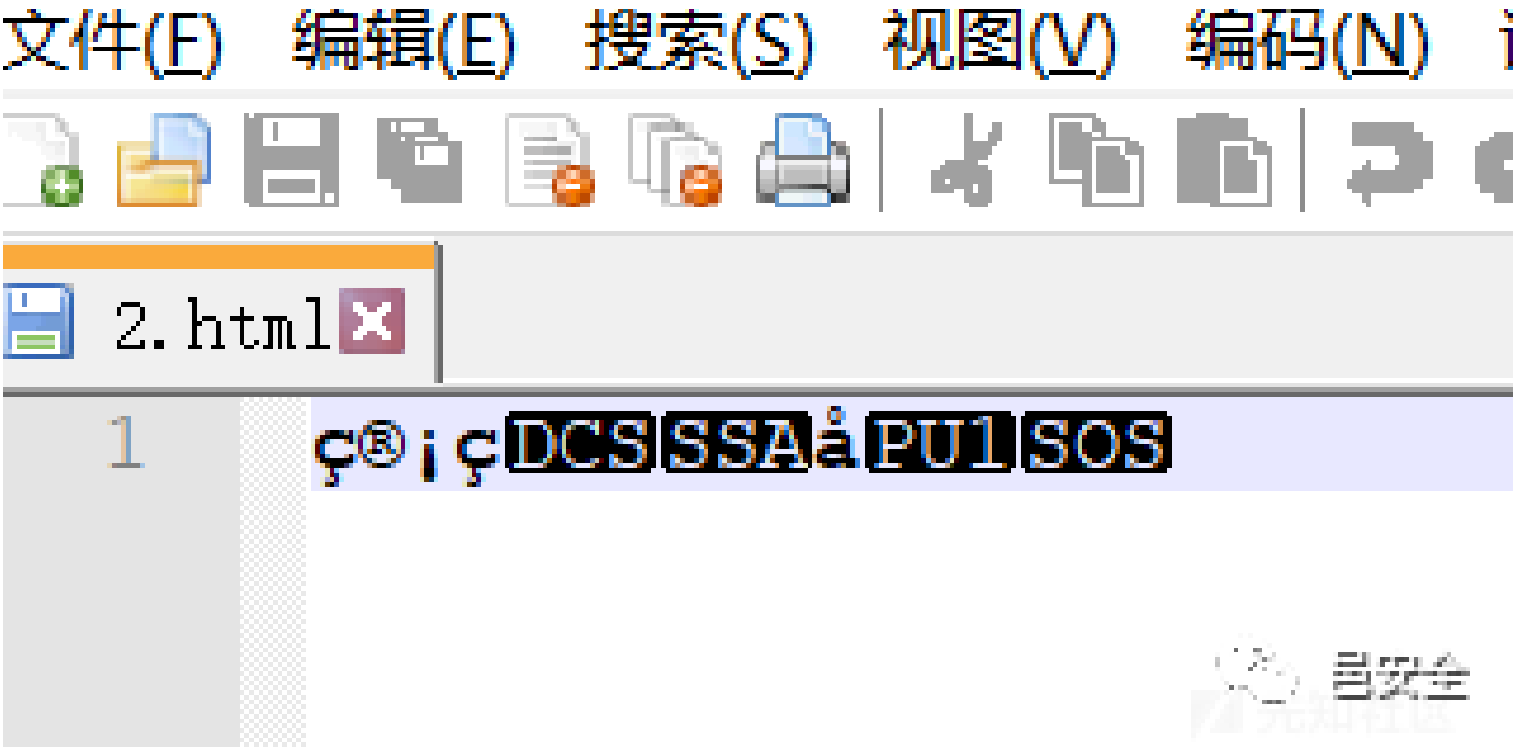
用文本编辑器打开，写入“管理员”三个字



转换字符



转换后的“管理员”字符



将转换过的字符复制进列表

② Payload Sets

You can define one or more payload sets. The number of payload sets and each payload type can be customized in different ways.

Payload set: Payload count: 2

Payload type: Simple list Request count: 2

② Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are

Paste

admin

Load ...

32432

Remove

Clear

Add

© 2013 Pearson Education, Inc. or its affiliate(s). All rights reserved.

Add from list ...

Attack Save Columns

ResultsTargetPositionsPayloadsOptions

Filter: Showing all items

| Request | Payload1 | Payload2 | Status | Error | Timeout | Length | Comment |
|---------|-----------|----------|--------|--------------------------|--------------------------|--------|---------|
| 0 | | | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 382 | |
| 1 | admin | 6 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 382 | |
| 2 | 32432 | password | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 382 | |
| 3 | ç@iç ¢â'~ | 123456 | 200 | <input type="checkbox"/> | <input type="checkbox"/> | 373 | |

RequestResponse

RawParamsHeadersHex

POST /login/login.php HTTP/1.1
Host:
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://
Connection: close
Referer: http:///login/login.html
Upgrade-Insecure-Requests: 1

uname=纓\$慙鍛 &pwd=123456

0 matches

Finished

转自先知社区

欢迎收藏并分享朋友圈，让五邑人网络更安全



欢迎扫描关注我们，及时了解最新安全动态、学习最潮流的安全姿势！

推荐文章

- 1 新永恒之蓝？微软SMBv3高危漏洞（CVE-2020-0796）分析复现
- 2 重大漏洞预警：ubuntu最新版本存在本地提权漏洞（已有EXP）u3000