jsEncrypter/README.md at master · c0ny1/jsEncrypter

jsEncrypter

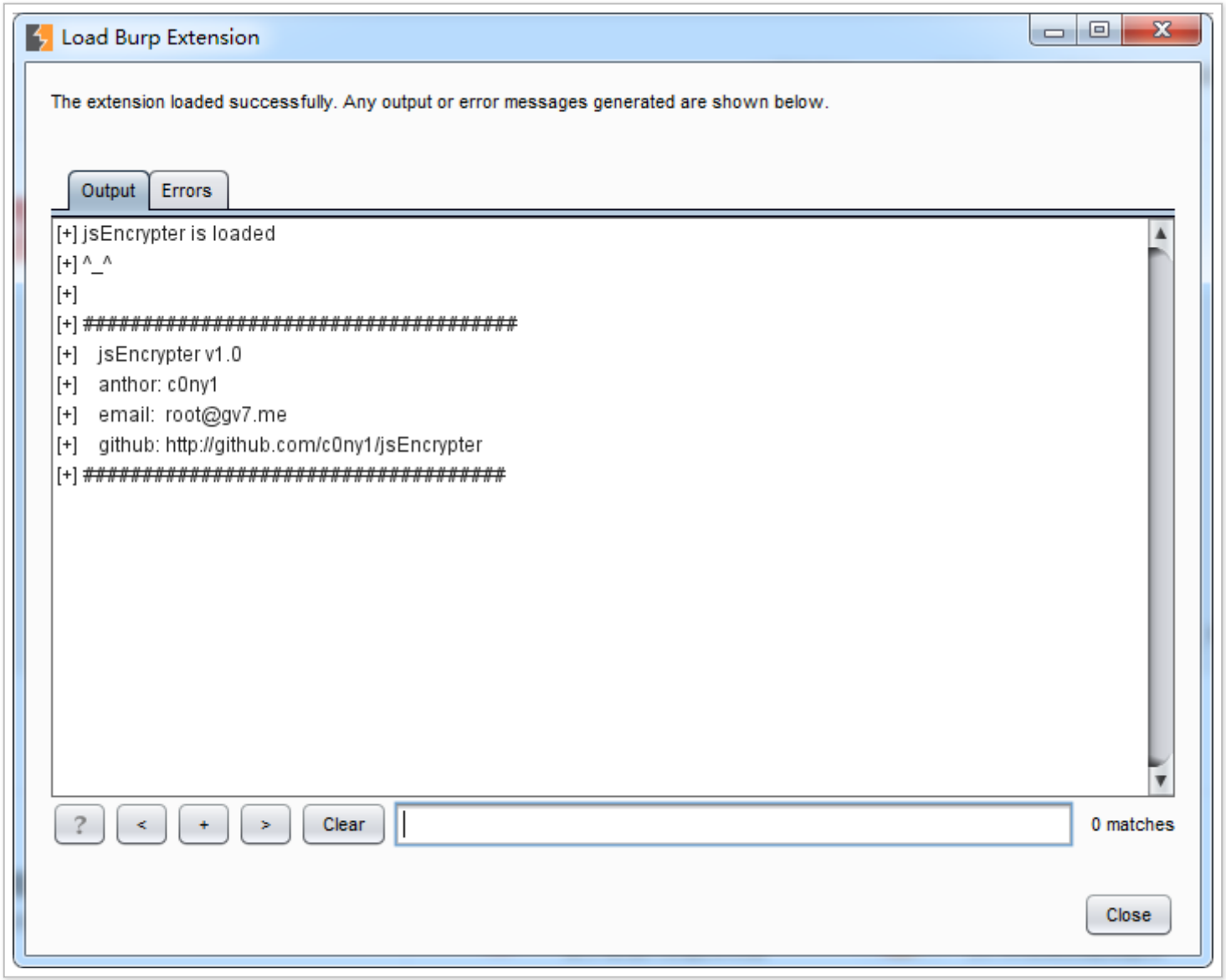
本插件使用 phantomjs 调用前端加密函数对数据进行加密，方便对加密数据输入点进行 fuzz。

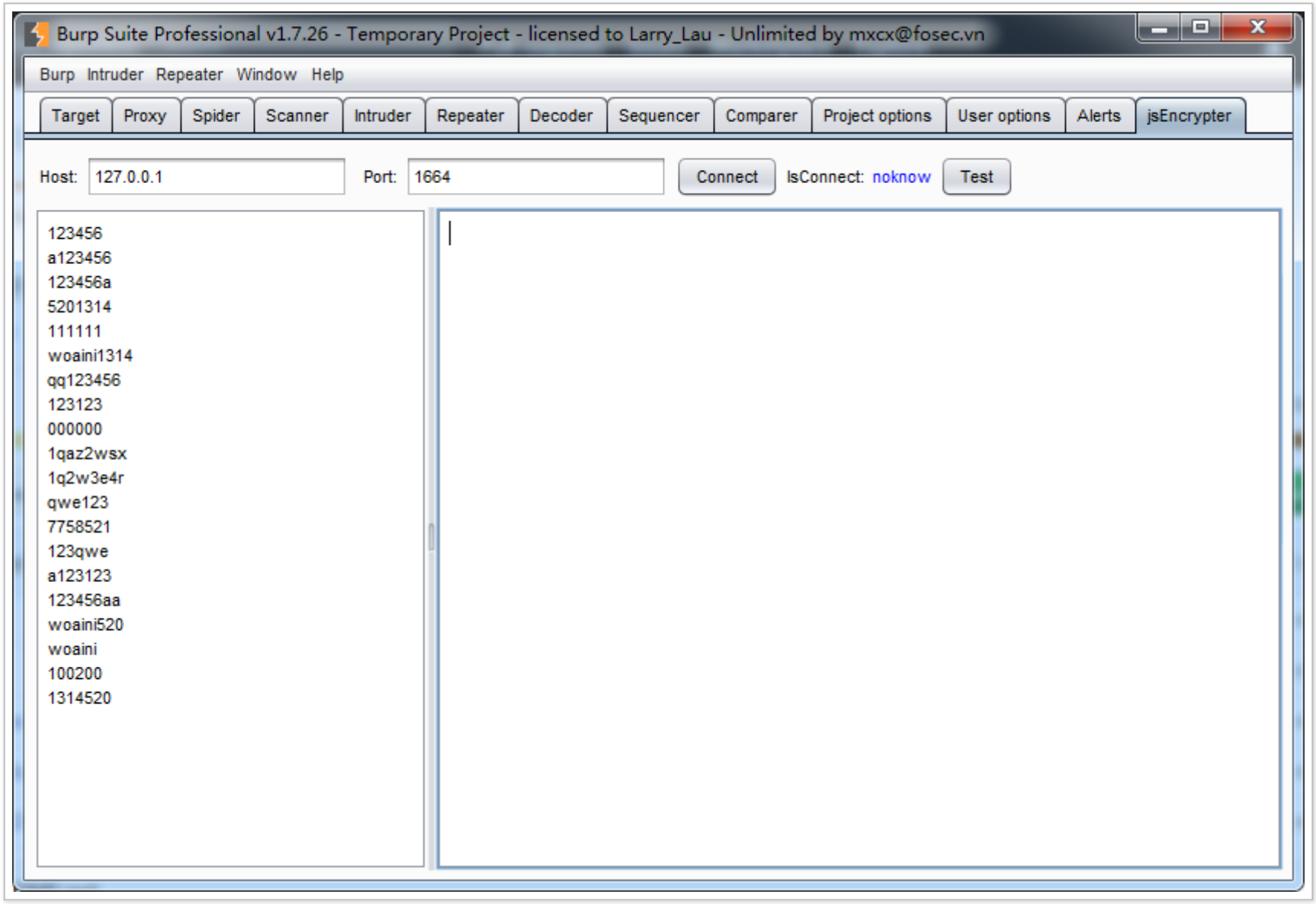
0x01 插件编译

安装好 maven，然后执行以下命令即可编译成功:

```
mvn package
```

0x02 插件安装


Load Burp Extension
The extension loaded successfully. Any output or error messages generated are shown below.
Output
Errors
[+] jsEncrypter is loaded
[+] ^_^
[+]
[+] ####################################
[+] jsEncrypter v1.0
[+] anthor: c0ny1
[+] email: root@gv7.me
[+] github: http://github.com/c0ny1/jsEncrypter
[+] ####################################
?
<
+
>
Clear
0 matches
Close


Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Decoder Sequencer Comparer Project options User options Alerts jsEncrypter
Host: 127.0.0.1
Port: 1664
Connect
IsConnect: noknow
Test
123456
a123456
123456a
5201314
111111
woaini1314
qq123456
123123
000000
1qaz2wsx
1q2w3e4r
qwe123
7758521
123qwe
a123123
123456aa
woaini520
woaini
100200
1314520

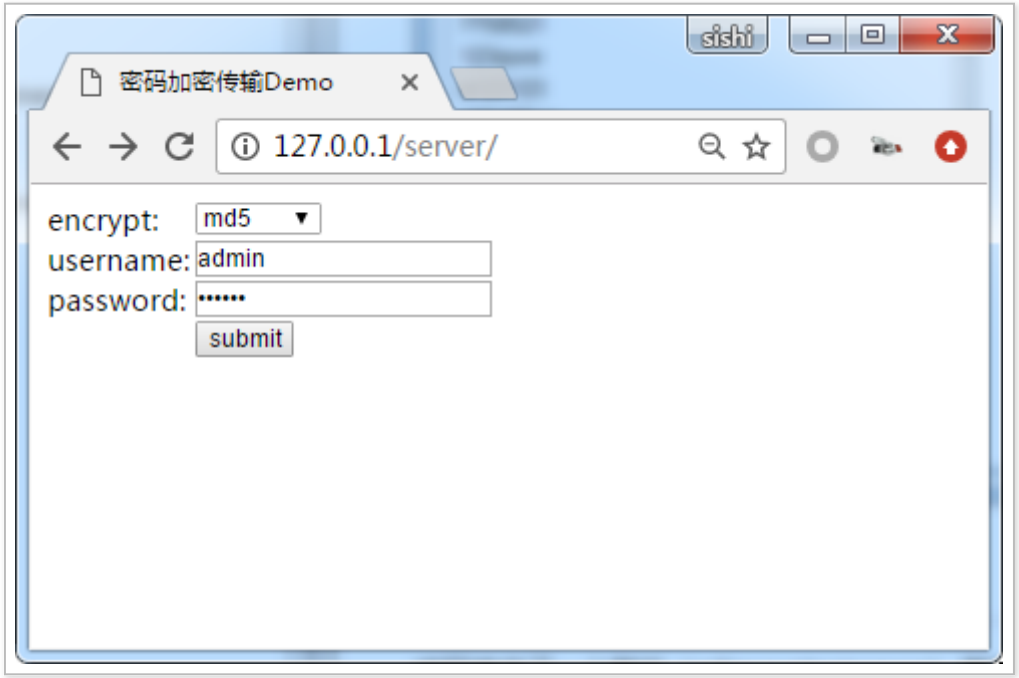
0x03 插件使用

3.1 运行靶机

项目提供了一个用 php 编写的靶机（jsEncrypter/server），靶机提供了 7 个算法对密码进行加密后传输，后台解密，最后进行密码匹配。

- base64
- md5
- sha1
- sha254
- sha384

- sha512
- RSA



3.2 编写 phantomJS 运行脚本

`jsEncrypter/js/jsEncrypter_base.js` 为插件 phantomJS 脚本模板。我们只需要将实现加密算法的 js 文件引入模板脚本，并在模板脚本的 js_encrypt 函数体中完成对加密函数的调用。

```
.......
.......
.......
// 加载实现加密算法的js脚本
var wasSuccessful = phantom.injectJs('xxx.js');/*引入实现加密的js文件*/

// 处理函数
function js_encrypt(payload){
        var newpayload;
        /**********在这里编写调用加密函数进行加密的代码************/

        /*********************************************************/
        return newpayload;
}
.......
.......
.......
```

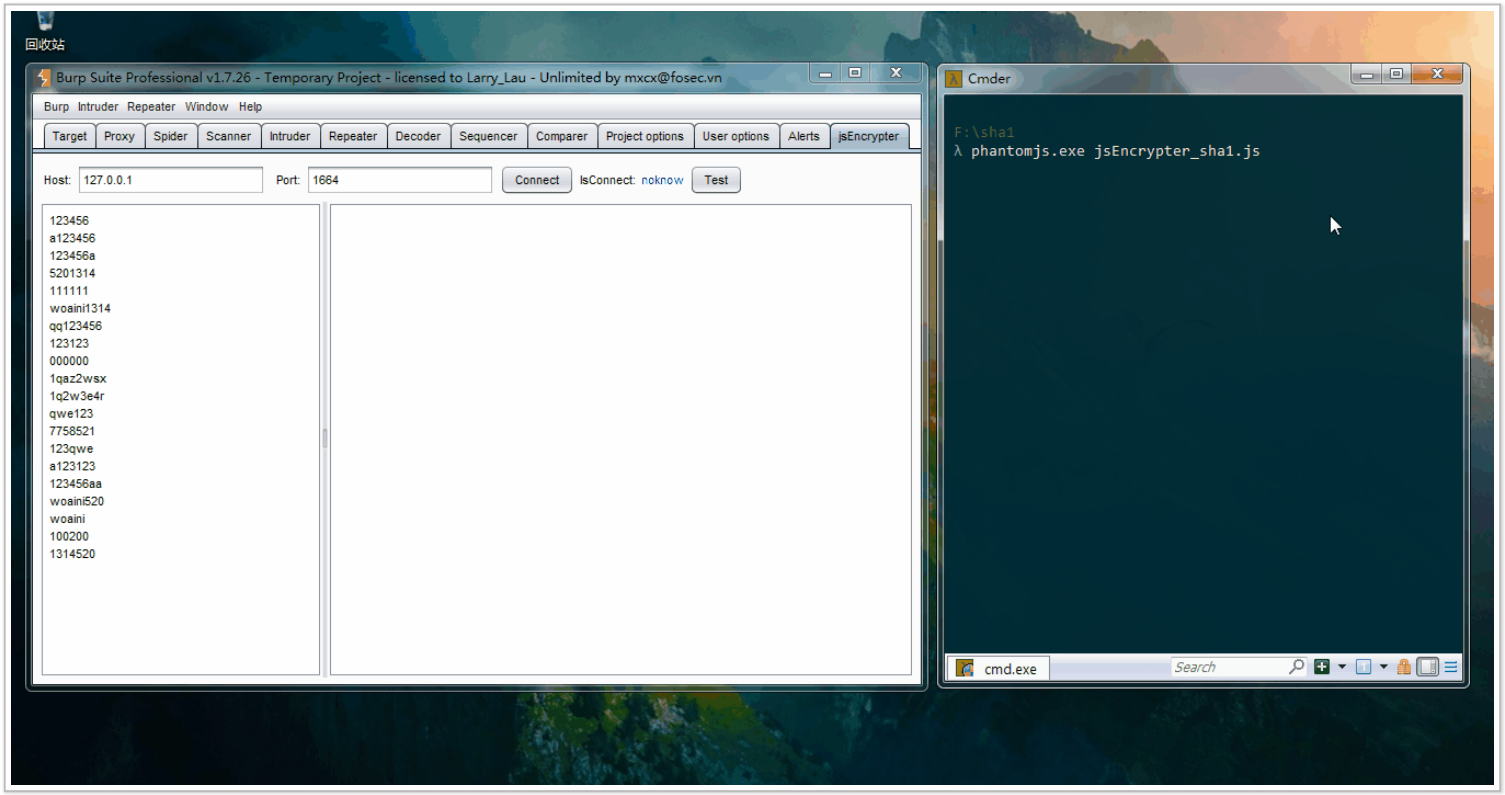
项目 jsEncrypter/server/TestScript 目录下是编写好的对应靶机各个加密算法的 phantomJS 脚本，可以参考！

3.3 运行 phantomJS 并测试

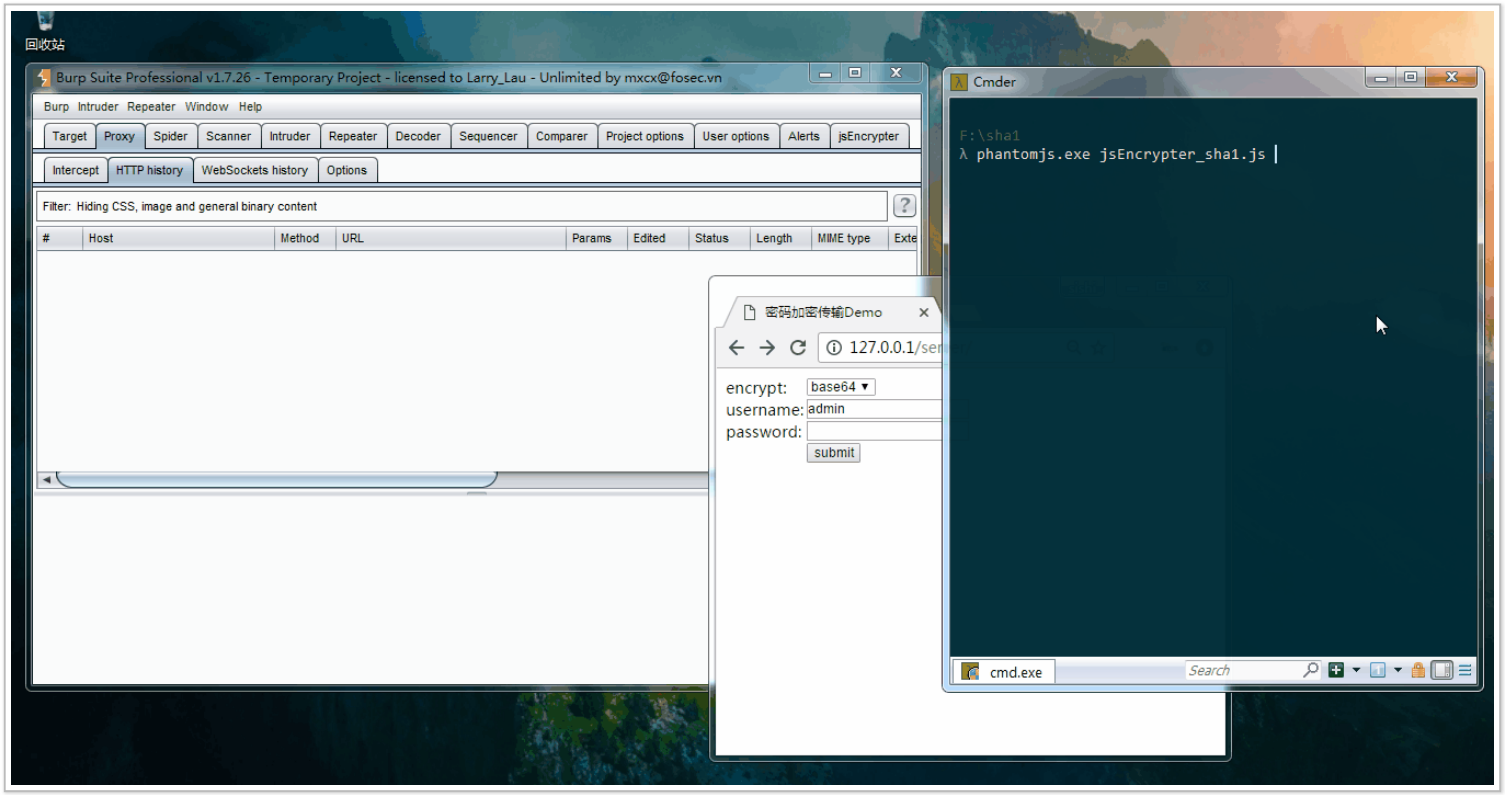
运行 phantomJS

```
>phantomJS.exe jsEncrypter_sha1.js
```

测试的目的是为了确保我们编写的 phantomJS 脚本能够正常加密 payload。


回收站
Burp Suite Professional v1.7.26 - Temporary Project - licensed to Larry_Lau - Unlimited by mxcx@fosec.vn
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Decoder Sequencer Comparer Project options User options Alerts jsEncrypter
Host: 127.0.0.1
Port: 1664
Connect
IsConnect: noknow
Test
123456
a123456
123456a
5201314
111111
woaini1314
qq123456
123123
000000
1qaz2wsx
1q2w3e4r
qwe123
7758521
123qwe
a123123
123456aa
woaini520
woaini
100200
1314520
Cmder
F:\sha1
λ phantomjs.exe jsEncrypter_sha1.js
cmd.exe
Search

3.4 抓包暴力破解



0x04 相关文章

- 编写加密传输爆破插件 jsEncrypter

- 快速定位前端加密方法

- 解决 jsEncrypter 脚本错误代码不报错问题

- jsEncrypter 的 Node.js 版 server 脚本

全文完