Day06 基础入门—加密算法

6.1 常见加密编码等算法解析

MD5, SHA, ASC, 进制, 时间戳, URL,
 BASE64, Unescape, AES, DES 等

6.2 常见加密形式算法解析

• 直接加密,带 salt,带密码,带偏移,带位数,带模式,带干扰,自定义组合等

6.3 常见解密方式

• 枚举,自定义逆向算法,可逆向

6.4 了解常规加密算法的特性

• 长度位数,字符规律,代码分析,搜索获取等

6.5 工具



6.5.1自定义加密算法

```
1
    <?php
 2
    function encrypt($data, $key)
    {
        $key = md5('ISCC');
 4
        #print $key;
 6
        x = 0;
        $len = strlen($data);
 8
        $klen = strlen ($key);
 9
        #print $len;
        for($i=0; $i < $len; $i++){
10
            if(x == klen)
11
12
                 x = 0:
            char = key[x];
13
14
            x += 1:
            #print $key[$X];
15
```

```
16
        }
       #print $char[0].$char[1].$char[2];
17
     for ($i=0;$i<$len; $i++){
18
            $str .= chr ((ord ($data[$i]) + ord
19
    ($char[$i]))%128);
20
        }
        return base64_encode ($str);
21
22 }
   echo encrypt('helloword');
23
24
   ?>
```

6.5.2自定义解密算法

```
1 <?php
   function decrypt($str){
2
       $mkey = md5('ISCC');
      $klen = strlen($mkey);
      $tmp = $str;
       $tmp = base64_decode($tmp); //解密
6
   base64
       $md_len = strlen($tmp);
                            //获取输入
   加密字符长度
       x = 0;
      $char = "";
9
                                      //临时数组
10
   for ($i=0; $i<$md_len; $i++){
11
          if (x == klen)
12
   符串长度超出key
              x = 0;
                                      //的长度时
13
   查重头开始和获取
          }
14
```

```
15
                                             //.= 累积
            char = \mbox{mkey}[\mbox{$x$};
    函数
16
            x += 1;
17
        }
18
19
        $md_data = array();
                                             //获取加密
    字符中的ASCII数据
        for ($i=0; $i<$md_len; $i++){
20
            array_push($md_data,ord($tmp[$i]));
21
        }
22
23
24
        $md_data_source = array();
        $data1 = "":
25
        $data2 = "";
26
        foreach ($md_data as $key => $value){//最终还
27
            i = key;
28
            if($i >= strlen($mkey)){
29
                $i = $i - strlen($mkey);
30
            }
31
            $dd = $value:
32
           $od = ord($mkey[$i]);
33
            array_push($md_data_source,$dd);
34
            $data1 .=chr(($dd+128)-$od);
35
    数据加key的Ascii大于128
            $data2 .=chr($dd-$od);
36
                                                 //原
    数据加key的Ascii小于128
37
        }
38
        print "data1 =>".$data1."<br>\n";
39
        print "data2 =>".$data2."<br>\n";
40
41
   }
```

```
42
43  $str = 'HxclIiEqIiUY';
44  decrypt($str);
45  ?>
```

带盐加密: md5(md5(pass).salt)

6.6 AES加密

```
require once '../config.php';
//解密过程
                                                              加密位数
                                                                                      jiamimoshi
function decode ($data) {
    $td = mcrypt module open(MCRYPT RIJNDAEL 128,'', MCRYPT MODE CBC,'');
    mcrypt_generic_init($td,'\dhaqPQnexoaDuW3','2018201920202021');
    $data = mdecrypt_generic($td,base64_decode(base64_decode($data)));
    mcrypt_generic_deinit($td);
    mcrypt_module_close($td);
                                                                                 偏総景
     if(substr(trim($data),-6)!==' mozhe'){
          echo '<script>window.location.href="/index.php";</script>';
     else
          return substr(trim($data),0,strlen(trim($data))-6);
→ C 🔺 不安全 | tool.chacuo.net/cryptaes 🐗
                                                                                 (产) 0x00实验室。
控制的博客 IP 域名 便民 web开发工具 格式化工具 文字工具 网络工具 实用工具 翻辑工具 编码转换 加密转密
加密解密工具 在线AES加密解密、AES在线加密解密、AES encryption and decryption
対称性加速解度
          AES,原规则是标准(连进:Advanced Encryption Standard、报告:AES),在更好学中艾斯的内容的研究。是美国联开朗南采用的一种艾尔加度的唯一,这个标准用来替让原产的EES,已经被多方分析因为"分处世界所使用。严格地说,AES的原则在各位即选择不完全一样(网络西国斯克斯中一者可以与助),因为阿内西亚加密法可以及为进入范围的政策的政策,AES的政策上海国际"为128比例,更明已被明可以是128、192或256比例,而和ndard使用的密钥据的影响和医技术使用以及对自由。256比例为上面,它经太阳不正常是不正常是EECRAES CEC, AES CTRAES OF BAES CEI
 3DES加度解度AESID密解度
                                                                华纳云、香港服务器减400 香港云18/月 全球服务器支持虚拟市 免费试用可天付
 常
■ Twofish加速解

■ Twofish加速解
* Serpent加坡縣
被
* Gost加密解密
* Rijndae加密解
和对称性加密解密
 ■ RSA控制对
■ RSA私钥密码言
           1 将你电脑文件直接拖入试试^-^
                                                   AESTER AESTER
除
* RSA私詞獻妈修
                                                                                 (C) 0x00实验室
改
■ PKCS#1转 AES加密,解密转换指率(base647); ● ■ ■
```

资源

```
1 https://www.mozhe.cn
2 https://www.cmd5.com
3 http://tool.chacuo.net/cryptaes
4 https://ctf.bugku.com/challenges
```