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

```php
<?php
function encrypt($data, $key)
{
    $key = md5('ISCC');
    #print $key;
    $x = 0;
    $len = strlen($data);
    $klen = strlen ($key);
    #print $len;
    for($i=0; $i < $len; $i++){
        if($x == $klen)
            $x = 0 ;
        $char .= $key[$x];
        $x += 1;
        #print $key[$x];
```

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

6.5.2自定义解密算法

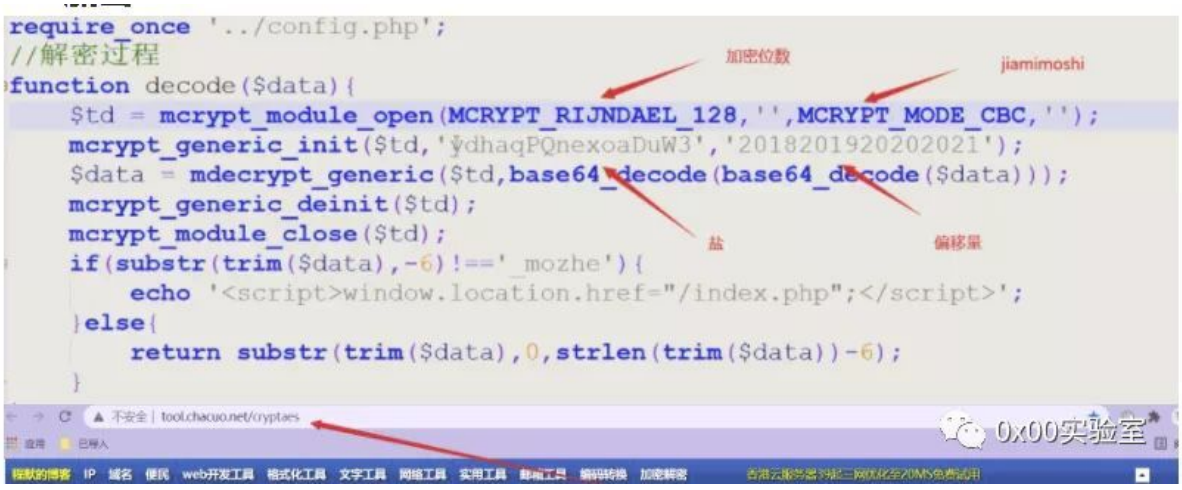
```
<?php
function decrypt($str){
    $mkey = md5('ISCC');
    $klen = strlen($mkey);
    $tmp = $str;
    $tmp = base64_decode($tmp);          //解密base64
    $md_len = strlen($tmp);              //获取输入加密字符长度
    $x = 0;
    $char = "";                          //临时数组

    for ($i=0; $i<$md_len; $i++){
        if ($x == $klen){                //当加密字符串长度超出key
            $x = 0;                      //的长度时查重头开始和获取
        }
```

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

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

> 带盐加密：md5(md5(pass).salt)

6.6 AES加密



资源

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