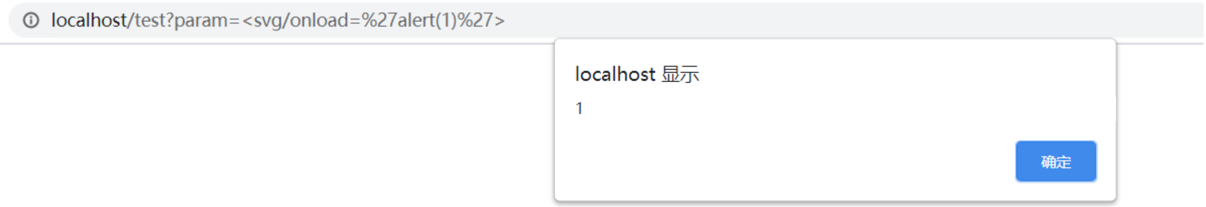
There are XSS vulnerabilities in some cases #188

Closed **HyCXSS** opened this issue on May 12, 2021 · 2 comments

HyCXSS commented on May 12, 2021 • edited

The main reason is that the controller does not filter the parameters during rendering, which leads to malicious input of users and may lead to XSS



localhost/test?param=<svg/onload=%27alert(1)%27>

localhost 显示

1

I wrote a demo:

Controller

```
@Path("/test")
public class TestController extends Controller{

    public void index() {
        String param  = getPara("param");
        System.out.println(param);
        set("param", param);
        render("test.html");
    }
}
```

test.html

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Title</title>
</head>
<body>
#(param)
</body>
</html>
```

The request parameter is "param",payload is `http://[your-ip]/test?param=<svg/onload='alert(1)'>`

If the user's input is output directly, XSS will be caused after the controller's set method is set. If the malicious parameters of controller are taken from the database, XSS vulnerability will be stored

- Repair

The `attributeValue` should be judged before the set method calls `request.setAttribute` . If it is in string format, the harmful characters should be filtered, such as `<script>`

```
public Controller set(String attributeName, Object attributeValue) {
  request.setAttribute(attributeName, attributeValue);
  return this;
}
```

OS-WS commented on Jun 27, 2021

Hi **@jfinal** **@HyCXSS** ,
This issue was assigned with CVE-2021-33348
Was this issue fixed?
If so, in what commit?

jfinal commented on Jun 27, 2021 Owner

@HyCXSS **@OS-WS** web Web framework doesn't need to filter request data. In addition to performance, it also needs to consider JS script in user business data

jfinal closed this as completed on Jun 27, 2021

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

3 participants