Ultimate Member <= 2.3.1 - Stored Cross-Site Scripting

Summary

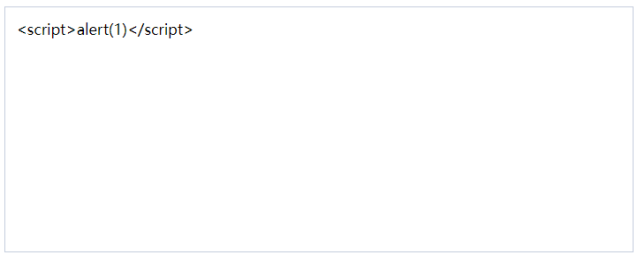
Biography component in user profile exists stored XSS vulnerability.

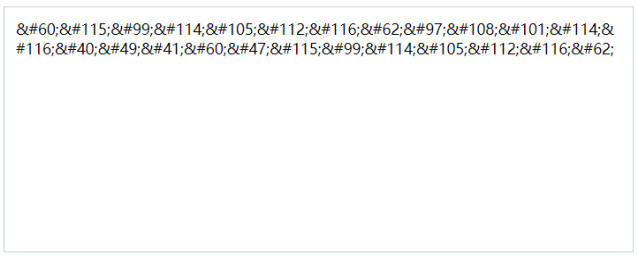
Vulnerability proof

1.Encode XSS payload by Unicode

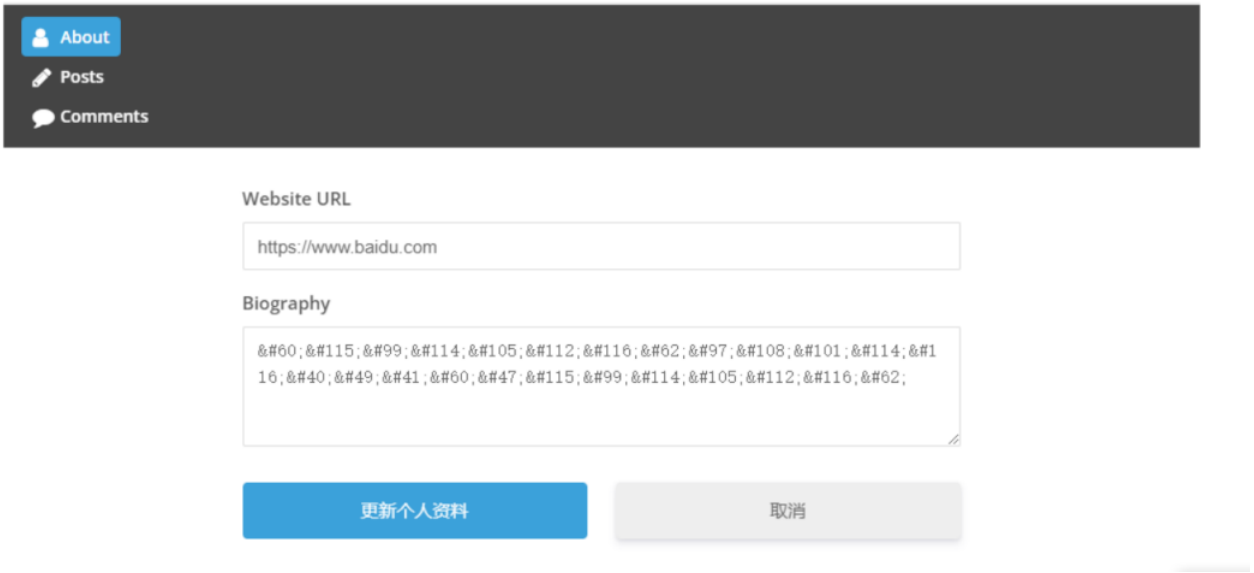
For example:

<script>alert(1)</script>





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



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