**Hidden Form Field Tampering**

**Description 1**

An attacker can exploit web app vulnerabilities and change the values in the hidden form fields to change role.

example:

The following server's answer shows a hidden field in the HTML returned to the user after a successful authentication.

HTTP/1.1 200 OK

Server: Netscape-Enterprise/6.0

Date: Wed, 1 Apr 2006 13:51:20 GMT

Set-Cookie: USER=aW78ryrGrTWs4MnOd32Fs51yDqp; path=/; domain=www.example.com

Set-Cookie: SESSION=k+KmKeHXTgDi1J5fT7Zz; path=/; domain= www.example.com

Cache-Control: no-cache

Pragma: No-cache

Content-length: 247

Content-Type: text/html

Expires: Thu, 01 Jan 1970 00:00:00 GMT

Connection: close

<form name="autoriz" method="POST" action = "visual.jsp">

<input type="hidden" name="profile" value="SysAdmin">

<body onload="document.forms.autoriz.submit()">

</td>

</tr>

An attacker can modify the value of the variable "profile" to "SysAdmin" and gain admin privilege.

References

**[1]** <https://www.owasp.org/index.php/Testing_for_Privilege_escalation_(OTG-AUTHZ-003)>