MrWebSecure Pvt.Ltd.

|  |  |
| --- | --- |
| DESCRIPTION | Malicious actors can use direct request manipulation using Burp Suite tool to modify the total payable amount when the order is processed. |
| IMPACT | By using this attack, attacker can reduce the price and 0 and join that event in free |
| Vulnerability Name | Price Response Manipulation Vulnerability |
| Vulnerable url | <https://mrwebx.com/event/#/event/registration/form> |
| REMEDIAL | the client-side JavaScript validation was removed the application was not accepting any user value to the response and manipulating the response gave us an error message. |
| REFERENCE | <https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/11-Client-side_Testing/06-Testing_for_Client-side_Resource_Manipulation> |
| POC | First I open vulnerable url    Then I click on apply coupon and then enter the sql injection query: admin'or'1'='1 and capture that request from Burpsuite      And then I intercept that request by right clicking on the page.    because of that sql injection query, the response will show you the discount code and how much discount you got.    Now increase the amount of discount as per your requirement. And forward the request    Now you have received your discount, now you can view the payment. |