### HTML 5 Storage Manipulation(DOM Based):

**Category:** Low

|  |  |
| --- | --- |
| Type |  |
| Status |  |

**Description**

DOM-based vulnerabilities arise when a client-side script reads data from a controllable part of the DOM (for example, the URL) and processes this data in an unsafe way.

HTML5 storage manipulation arises when a script stores controllable data in the HTML5 storage of the web browser (either localStorage or sessionStorage). An attacker may be able to use this behavior to construct a URL that, if visited by another application user, will cause the user's browser to store attacker-controllable data.

This behavior does not in itself constitute a security vulnerability. However, if the application later reads the data back from storage and processes it in an unsafe way, then an attacker may be able to leverage the storage mechanism to deliver other DOM-based attacks, such as cross-site scripting and JavaScript injection.

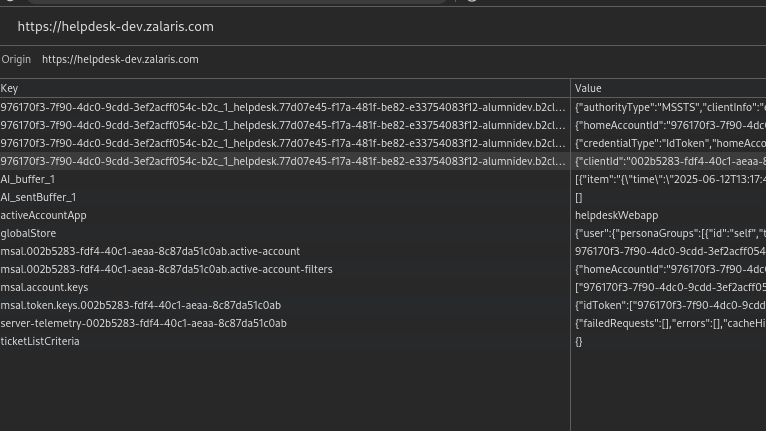
Burp Suite automatically identifies this issue using dynamic and static code analysis. Static analysis can lead to false positives that are not actually exploitable. If Burp Scanner has not provided any evidence resulting from dynamic analysis, you should review the relevant code and execution paths to determine whether this vulnerability is indeed present, or whether mitigations are in place that would prevent exploitation.

**Links Tested**

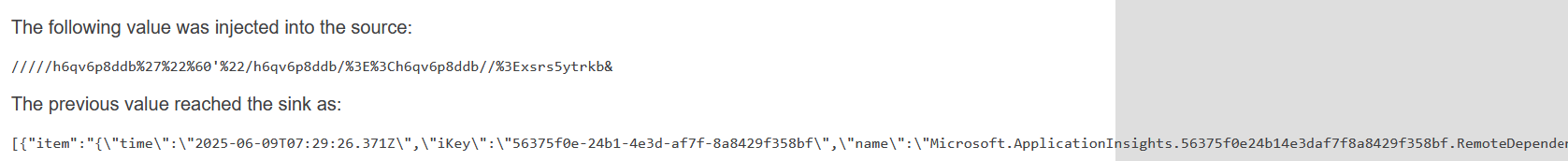
|  |
| --- |
| * / * /510 * /510/tickets/new/additional-tax-deduction * /510/tickets/new/draft-template-testing * /510/tickets/new/einstellungsbogen * /510/tickets/new/employee-transfer * /510/tickets/new/ordering-an-employment-certificate-requsition-form * /510/tickets/new/schedule-an-expert-inquiry * /777 * /777/tickets/new/additional-tax-deduction * /777/tickets/new/employee-transfer |

Steps:

* Login into helpdesk-dev.zalaris.com
* Access the browser’s local storage and check whether the application has items stored in local storage and session storage
* The screenshot below shows that the application has local storage and session storage enabled



* The value that is sent from the source to the sink is targeted to be sent to the azure insights and is not processed back by the helpdesk application . The screenshot from the automated audit is attached below [value from location.pathname passed onto sessionStorage.setItem ]



* The key value of azure insights present in the session storage is given below

|  |
| --- |
| **AI\_buffer\_1** : [{"item":"{\"time\":\"2025-06-12T14:28:10.455Z\",\"iKey\":\"56375f0e-24b1-4e3d-af7f-8a8429f358bf\",\"name\":\"Microsoft.ApplicationInsights.56375f0e24b14e3daf7f8a8429f358bf.RemoteDependency\",\"tags\":{\"ai.user.id\":\"q47P128xC9LyKIrgDpFB6t\",\"ai.session.id\":\"+tGUt703hc424qXKMLcM/y\",\"ai.device.id\":\"browser\",\"ai.device.type\":\"Browser\",\"ai.operation.name\":\"/510/tickets\",\"ai.operation.id\":\"a7f8feb9a6f34197a3076e9730ce5f7e\",\"ai.cloud.role\":\"helpdesk-webapp\",\"ai.internal.sdkVersion\":\"javascript:3.3.7\"},\"data\":{\"baseType\":\"RemoteDependencyData\",\"baseData\":{\"id\":\"|a7f8feb9a6f34197a3076e9730ce5f7e.2668600240024ee9.\",\"ver\":2,\"name\":\"GET https://helpdesk-dev.zalaris.com/api/v1/notifications?contactId=1000113\",\"resultCode\":\"200\",\"duration\":\"00:00:00.345\",\"success\":true,\"data\":\"GET https://helpdesk-dev.zalaris.com/api/v1/notifications?contactId=1000113\",\"target\":\"helpdesk-dev.zalaris.com\",\"type\":\"Ajax\",\"properties\":{\"HttpMethod\":\"GET\"},\"measurements\":{}}}}","cnt":0}] |

* The value AI\_Buffer\_1 is the key and the subsequent value after “:” is where the data from the sink goes to
* This data is not processed by the help-desk application again and has no means to alter the applications GUI or run scripts
* Therefore the reported alert can be considered as False Positive

**WORKLOG**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| When | What | Who | Recommended Action | Action plan |
| 13 June 2025 | Manually tested the HTML5 Storage Manipulation (DOM based Attack) | CSOC | No action needed | No Action Needed |