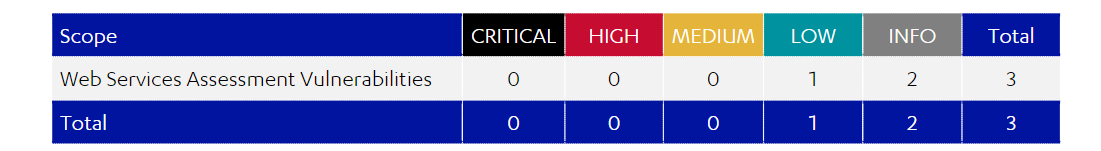
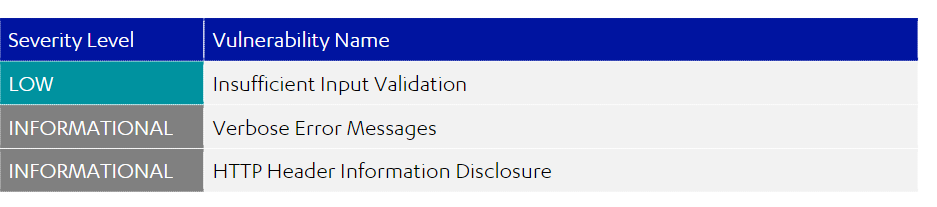
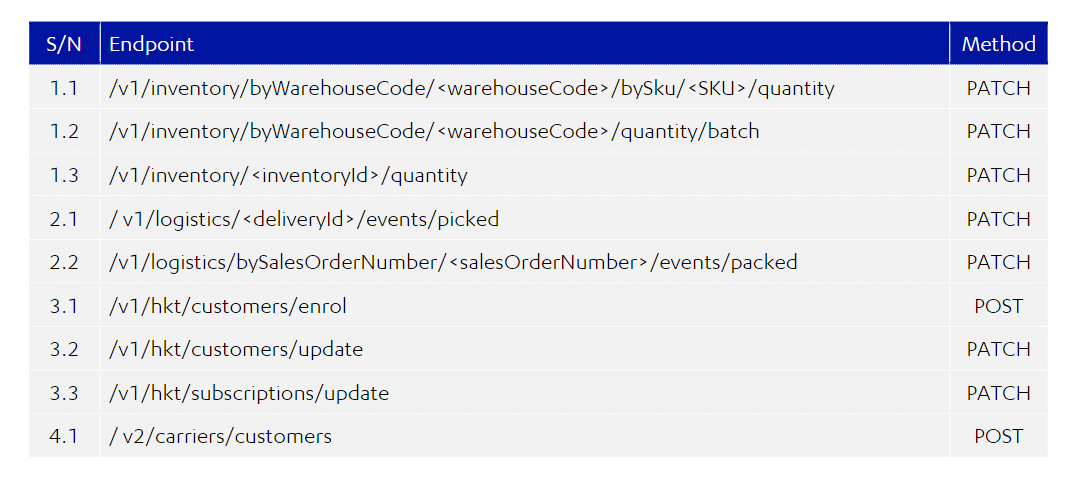
Real Sample – From Org





Provided



**Sample**

Request

PATCH /v1/inventory/byWarehouseCode/habbitzz/bySku/200085/quantity HTTP/1.1X-API-Key: AoaRVcXQ7o80MnW8TYjpndAkOgozZ7qlpOPvbvgckH4mQSkoIkT25qMpSAcS2rWdOnmContent-Type: application/gobiUser-Agent: PostmanRuntime/7.24.1Accept: \*/\*Postman-Token: e43ebc27-60c8-4846-a3e8-ae62d9f46353Host: api.uat-hk.eagle-tech.ioAccept-Encoding: gzip, deflateConnection: closeContent-Length: 81Cookie: GCLB=CLm\_neiyvM34ZQ{"type": "relative","quantity": -1000000,"stockLocation": "new"

Response

HTTP/1.1 200 OKContent-Type: application/gobiContent-Length: 223x-powered-by: Undertow/1Server: WildFly/10Date: Tue, 2 Aug 2022 08:10:30 GMTX-Kong-Upstream-Latency: 51X-Kong-Proxy-Latency: 6

Via: kong/1.0.3, 1.1 googleAlt-Svc: h3-Q050=":443"; ma=2592000,h3-Q046=":443"; ma=2592000,h3-Q043=":443"; ma=2592000,quic=":443"; ma=2592000; v="46,43"Connection: close{"id":"5ea1744126b75a15570516df","warehouseCode":"habbitzz","quantity":-999999, "quantityReserved":1,"sku":"200085","stockLocation":"new","createdA

Impact

When input validation is ineffective, the application is exposed to an increased risk from input driven attacks such as SQL Injection and Cross Site Scripting (XSS). Furthermore, there is an increased risk that exploitable attack vectors could be realised at a future date, for example, when a new functionality is added, which can be leveraged to exploit weak validation routines.For this application, the use of negative warehouse stock, negative retail device prices, long in the future subscription dates or the storage of XSS payloads could negatively affect the application.

Remedial Action

It is recommended to modify server-side input validation functions to ensure that comprehensive validation is performed for all input. Validation should be based on strictly defined white-lists of permitted characters appropriate for each of the expected inputs (e.g. contact number fields should not contain alphabet or special characters). Validation functions should also include minimum and maximum length restrictions.Input that does not match the white list of permitted characters or length restrictions should be rejected. Where a business case justifies the inclusion of special characters within a specific white-list, a risk assessment should be performed that includes threat modelling, to determine the significance within the context of all possible data flows, andthe effect on backend processing and interpreters. This process will help to determine the most appropriate method to safely handle the input.Input that requires special characters should also be properly escaped before use or storage by the application.A stable and mature library which protects against XSS attacks and should be utilised to safely encodeinformation which is to be included as part of HTML output to the browser. The OWASP Enterprise Security API (ESAPI) provides protection against common XSS attacks and can be retrofitted into the majority of web applications.