

WEB APPLICATION PENETRATION TESTING REPORT for Microweber

Prepared by: GrozdniyAndy of XSS.is

20/11/2023



Table Of Contents

Table Of Contents

Executive Summary

1.1 Grading Criteria1.2 Project Objectives1.3 Methodology1.4 Summary of Findings

Findings

2.Broken Access Control2.1 Files or Directories Accessible to External Parties2.2 Cross-Site Request Forgery (CSRF)

3.Injection

3.1 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Executive Summary

This report presents the results of the Black Box penetration testing for the Microweber Open-Source CMS. The recommendations provided herein are structured to facilitate the remediation of the identified security risks. This document serves as a formal letter of attestation for the recent Microweber CMS penetration testing. Evaluation ratings compare information gathered during the engagement to "best in class" criteria for security standards. We believe that the statements made in this document provide an accurate assessment of Microweber's current security as it relates to Microweber data. We highly recommend reviewing the Summary section for business risks and High-Level Recommendations to better understand the risks and discovered security issues.

Grading Criteria

The penetration test for Microweber utilized the Common Weakness Enumeration (CWE) and the OWASP Top 10 as key grading criteria. The CWE framework was employed to identify and categorize specific vulnerabilities, while the OWASP Top 10 served as a guide to focus on critical web application security risks. The Common Vulnerability Scoring System (CVSSv3) was applied to quantify the severity of identified vulnerabilities, aiding in prioritizing remediation efforts based on potential impact.

Project Objectives

The overarching goal of the penetration test was to assess the security posture of Microweber, uncovering vulnerabilities in line with the CWE and OWASP Top 10 frameworks. Specific objectives included the identification and validation of security weaknesses, the quantification of risk using CVSSv3, and the provision of actionable recommendations to enhance the overall security of Microweber.

Methodology

The penetration test followed a black-box approach. The methodology included:

- 1. Vulnerability Assessment: Applying automated tools and manual techniques based on CWE and OWASP Top 10 to discover and validate vulnerabilities.
- 2. Exploitation: Ethical exploitation of identified vulnerabilities to assess impact, with severity quantified using CVSSv3.
- 3. Post-Exploitation: Analyzing the extent of compromise and determining potential risks associated with successful exploitation.
- 4. Reporting: Documenting findings, including identified vulnerabilities, their CWE categorization, OWASP Top 10 relevance, and CVSSv3 scores, with actionable recommendations for remediation.

Public

This report is made as effort to increase security in open source projects.

Summary of Findings

Vulnerability #	Score
1	5.3 <u>AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N</u>
2	5.3 <u>AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N</u>
3	3.8 <u>AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N</u>
4	8.1 <u>AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:N</u>
5	4.6 <u>AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N</u>
6	3.5 <u>AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:N</u>

Public This report is made as effort to increase security in open source projects.



Findings

2. Broken Access Control

Broken Access Control refers to a security vulnerability that occurs when an application or system fails to properly enforce restrictions on what authenticated users are allowed to do. This vulnerability arises when access controls, such as permissions and restrictions, are not effectively implemented or are easily bypassed. It allows unauthorized users to access sensitive data, perform actions they shouldn't be allowed to, or exploit functionalities that should be restricted.

The consequences of Broken Access Control can be severe, as it can lead to unauthorized access to confidential information, unauthorized modification of data, and other security breaches. Common examples include a user being able to view or modify another user's data, gaining access to privileged functionalities without proper authorization, or manipulating URLs or parameters to access restricted areas of a website or application.

Reference: https://owasp.org/Top10/A01_2021-Broken_Access_Control/

2.1 Files or Directories Accessible to External Parties

Description:

The product makes files or directories accessible to unauthorized actors, even though they should not be.

Location:

http://microweber.local/userfiles/install_log.txt http://microweber.local/api/image-generate-tn-request/{Number}?saved

Impact:

Some files are accessible to unauthenticated users and this may lead to sensitive data leakage.

Reference: https://cwe.mitre.org/data/definitions/552.html

Vulnerability Detail [1]

File install_log.txt has logs stored and they can be viewed with anyone who knows the right value of parameter '_'. Those logs store installed modules and other debug information which may be considered as sensitive.

Proof of Vulnerability [1]

Install the microweber and check both requests (client-side) and request logs (server-side).

Public



Image [1]



Image [2]

Image number 2 shows only partial logs, full logs to be seen we should open URL as in Image [1]. This file is stored in the server and not deleted. When I googled inurl:install_log.txt



Image [3]

Public



Vulnerability Detail [2]

It is possible to view images uploaded by administration but not used.

Proof of Vulnerability [2]

Upload any image in any way, but don't use it anywhere. To see uploaded images you can use Media Libary.

-	-		Category name							
_		Selec	t image				×			
			My computer	URL	Uploaded	Media library				
							,			
-										
				A	dd file					
Cantor				or drop f	iles to upload	- Q -				
			775			Ye				
		Cance	1				ОК			
,										
Sugar.			(the online)							

Image [4]

						Burp	Suite Cor	nmunity	Edition V202	3.7.3 - Te	mporary P	roject							
Dashboard	Target	Proxy	Intruder	Repeater	Collaborator	Se	equencer	Decode	er Compare	er Logg	er Orga	inizer Le	arn Ext	tensions	InQL			0	Settings
Intercept	HTTP history	Web	Sockets history	() P	roxy settings														
√ Filter: Sho	wing all items																		?
# ^	Host		Method		URL		Params	Edited	Status code	Length	MIME type	Extension		Title		Comment	TLS	IP	
05 http://1	72.16.241.132:	8080	GET /a	api/image-gene	rate-tn-request/4	1?sav	. 🗸		200	4319	XML							172.16.241.13	\$2
													-		Inspect	or] ∓ ∸ (® ×
Request						=	Respo	nse					B 10	-					~ ~
1 GET /ani	aw Hex	rate_tr-	-request/41	rsaved HTT	P/1.1	-	1 HTTP	Haw 2/1.1 200	OK Hex H	ender				-	Request	attributes		2	~
2 Host: 172 3 User-Ager	2.16.241.13 nt: Mozilla	2:8080 /5.0 (W:	indows NT 1	0.0; Win64	x64)		2 Date 3 Serv	: Sun, 1 rer: Apac	9 Nov 2023 he/2.4.57 (13:43:04 Debian)	GMT				Request	query parameter	'S	1	~
Safari/53 4 Accept:	37.36	(KHIML,	LIKE GECKO) Chrome/1	15.0.5/90.1/1		5 Cont 6 Conn	ent-Leng	th: 4135 close						Request	cookies		6	~
image/avi 8 5 Referen:	if,image/we	bp,image	e/apng,imag	e/svg+xml,	image/*,*/*;c	q=0 .	7 Cont 8 9 <7xm	ent-Type	: image/svg	+xml	F-8"?>				Request	headers		8	~
http://17 ge_id=3	72.16.241.1	32:8080	/admin/shop,	/category/	create?parent	_pa	10 <svg http</svg 	xmlns="	http://www. /3.org/1999/	w3.org/20 xlink" ve	00/svg" xr rsion="1.1	mlns:xlink 1" id="Lay	=" er_1" x="	өрх	Respons	e headers		6	~
6 Accept-Er 7 Accept-Le 8 Cookie: 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 1977/2014 19	ncoding: gz anguage: en isGditModem wwb.SthaStay0X8 WydStASU9X8 Vala0X20U laravel_se caYY2ndK5ul 10%303; XS 10%CVCY2 WZ3FhSklC03 MrwMZ0NArz HrTH04dkxk YmMAD0dkmw xIiwidGFnIj on: close	ip, def i-GB,en-I- itrue; la iddc2b2 XalDvkbu klJ0Vq11 swP4yOU .132%3A8 KF-TOKE mTXJIY2 Z1MIpyd SJUR2OW VGQ3d0NL IMZg5ZDI oiIn0%3D	Late 15; q=0-9, en ang=en_US; 99401580fd1; 52gbB0cJe9y 10; LzrREXQomi Markon 1402pna2lyT 1980xkpPME1 1402pna2lyT 1980xkpPME1 1960aU; 1350M 1960aU; 1350M 196	;q=0.8 4c7f58ea4e ncmxafAy6b 50R2YtTgV7 tmR; back_ shop/categ EE9PSISInZI M0dtb0MzdEI SRUpKVkpUM M1LC3YTWHI xdkZTdjNjRI	30989d= cx) 0La0Carfpi 07%r500p.vtC to_admin= pry/create%31 hbW/LipickUlt 104Mr20Bu%2 LidMr20Bu%2 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidMr22Ev%3 LidM	-3fs JSy0 Par -V1N -22H EVS DTUW M2Y	"y= enab 11 <sty 12 .s 13 .s 14 .s 15 16 <rec 0.7- c-1. -0.6 c0-1 3-1. c2.7 7,44. c-1. .8c3 c1.6 c0-2 c-1. c-1. c2.7 c-1. c-1. c2.7 c-1. c-1. c2.7 c-1. c-1. c2.7 c-1. c-1. c2. c2. c2. c2. c2. c2. c2. c2. c2. c2</rec </sty 	<pre>"'0px" vj le=backg /le type= t0{fill: t1{fill: t2{fill: tyle> <path d="<br">.2,101.5 .2,101.5 .2,101.5 .2,11-23 .5,2.8-1.5 .2,4-0.3 .5,2.8-1.5 .2,6-1.2 .5,0,5.4,6 .5,1,2-2 .5,2,1,2-4 .8,0,7.1 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4 .2,1,2-4</path></pre>	LevBox" 0 0 "text/css"> 0 "text/css"> none;ströke: rule:evenod: #FFFFF;} 1.3" y="-128 " hb.lcl.7,0, 1-3.6c9-2: 5-1.7-6-1.7; 3.7-2.7c0: (.5-0.8-3.5c) 3.37.9,05.9,9,11: (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.4,8c) (.4.8,2.8,8c) (.4.8,	796.9 218 0 796.9 #000000; d;clip-ru 6.5" clas 3.1-0.3,4 -0.7-3.8 -0.7-3.8 -0.7-1.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.2 -0.	.6" style: 218.6;" xr stroke-mil le:evenodd s="st0" wr 2.2-4.9 h7.4c1.9, -2.7.8,1.3- 2.7.8,1.3- 2.1.8-2.2; .3V104h11. 7-0.9,6.8 1-6.9,1: 1,2.6,6.5; 5.3-2.4; 2014		preserve" a;} (#SVGID_1 " height= 1.3,2.9-2 ,5.2-0.8c 0.7-2-1.2 3,3.6,2.9 h-20V79.3 -3.8,3.6-	<pre>> .3c 1.6 -3. ,4. h18 6.7</pre>					
	→ Search				0 ma	tches	0.63	$\left(\leftrightarrow \right)$	dmin-dashboa	rd-contact-fe	rm		0 mat	ches					

Image [5]

Public



I was able to view image 46 as unauthenticated user even though I shouldn't be.



Image [6]

Remediation

remove the log file after installation and restrict access to view images only to authorised users.

Public This report is made as effort to increase security in open source projects.

2.2 Cross-Site Request Forgery (CSRF)

Description:

The web application does not, or can not, sufficiently verify whether a well-formed, valid, consistent request was intentionally provided by the user who submitted the request.

Location:

http://microweber.local/livewire/message/admin::edit-user.update-profile-form

Impact:

The consequences will vary depending on the nature of the functionality that is vulnerable to CSRF. An attacker could effectively perform any operations as the victim. If the victim is an administrator or privileged user, the consequences may include obtaining complete control over the web application - deleting or stealing data, uninstalling the product, or using it to launch other attacks against all of the product's users. Because the attacker has the identity of the victim, the scope of CSRF is limited only by the victim's privileges.

Reference: https://owasp.org/www-community/attacks/csrf

Vulnerability Detail [3]

When uploading an image, for example a profile photo, it gets stored in the server and when saving it the full URL is used to save it. Attacker can put URL from external source. It may be intended when adding a category image, but not when uploading a profile photo. Vulnerability exists in uploading profile photo. Also there is a check for extension, which can be bypassed

Proof of Vulnerability [3]

In Image [7] we put external URL, for example some random image from github and in the Image [8] we can see that it is in source attribute. Application would allow me to add URLs that end only with .jpg, so I used #.jpg, it will comment .jpg and I would be able to add any URL I want, which will allow me to make anyone viewing the profile send any malicious request I want. As you can see in Image [9], I added # before the .jpg and in Image [10], the request was sent without #.jpg, as it is a comment. This way we bypassed the security implemented.

Public

This report is made as effort to increase security in open source projects.





Image [7]



Image [8]

Public





Image [9]



Image [10]

Remediation Use relative paths when adding an image instead of using full URLs.

Public



3. Injection

An application is vulnerable to attack when:

- User-supplied data is not validated, filtered, or sanitized by the application.
- Dynamic queries or non-parameterized calls without context-aware escaping are used directly in the interpreter.
- Hostile data is used within object-relational mapping (ORM) search parameters to extract additional, sensitive records.
- Hostile data is directly used or concatenated. The SQL or command contains the structure and malicious data in dynamic queries, commands, or stored procedures.

Reference: https://owasp.org/Top10/A03_2021-Injection/

3.1 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

Description:

The product 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.

Location:

http://microweber.local/login?username={payload}&password={payload} http://microweber.local/module http://microweber.local/api/save_option

Impact:

In some circumstances it may be possible to run arbitrary code on a victim's computer when cross-site scripting is combined with other flaws.

Reference: https://cwe.mitre.org/data/definitions/79.html

Vulnerability Detail [4]

There is XSS vulnerability in the login. The vulnerability arises from the ability of inserting credentials in GET request, which then allows attacker to bypass the security measures implemented and execute javascript code.

Proof of Vulnerability [4]

I simply used request to add username and password and then checked where it gets reflected in the source code, Image [11]. Then instead of escaping the input tag, I executed the javascript code inside it Image [12], Image [13]. Same can be done for password parameter, Image [14].

Public

This report is made as effort to increase security in open source projects.



• • • III 172.16.241.132:8080/admin/us × III Unauthorized	× Microweber	× 🔃 Login	× +		~
← → C ▲ Not Secure 172.16.241.132:9090/login?userna	me=admin&password=admin⟨=en_US&where_to=	admin_content		∆ ☆ 🔏 🗆	1 🛎 🗄
	Microweber				
	Username: admin Password: Language: English [en_US]				
	Login				
	Back to My WebSite Forgot my password?				
	Create a website with Microweber Version: 2.0.4				

Image [11]



Image [12]

Public



••• To 172.16.241.132:8 x To Unauthorized x To Microweber x To Login x To Login x To Login x To Login x	~
← → X 🔺 Not Secure 172.16.241.132:9090/login?username="onfocus=alert(1)%20autofocus> 🖞 🖈 👗 🔲 😩	:
1 I I I I I I I I I I I I I I I I I I I	

Image [13]

• • • 172.16.241.132:8 × 🔃 Unauthorized × 🔃 Mict	roweber X 🗊 Login X 🗊 Login X 🔯 Login X C Login X + V
\leftrightarrow \rightarrow X (1) 172.16.241.132:9090/login?password="onfocus=aler	t(%27xss_pass%27)%20autofocus> 🖞 🖈 🖪 😩 🗄
1 x	72.16.241.132:9090 says ss_pass OK
	Username: Username of Emili Password: Password * required> Language: English [en_US]
	Login
	Back to My WebSite Forgot my password?
	Create a website with Microweber Version: 2.0.4

Image [14]

Public This report is made as effort to increase security in open source projects.



Vulnerability Detail [5]

There is a CSS Injection while sending request to /module/. Module adds parameters inside div which can be misused.

Proof of Vulnerability [5]

In Image [15] I added background URL and it sent a request to my server, Image [16]. In this case the style attribute was injected with external url. More information about CSS injection: https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/11-Client_Side_Testing/05-Testing_for_CSS_Injection



Image [15]







Vulnerability Detail [6]

There is HTML Injection in the /api/save_option. The vulnerability appears while editing email.

Proof of Vulnerability [6]

In Image [17] I edit email sender name and use a payload. In Image [18] we can see that our payload worked and it is in all the fields which can be seen in the picture.

Public This report is made as effort to increase security in open source projects.



									arp ouro					,	,							
ashbo	bard	Target	Proxy	Intru	der	Repeater	Collab	orator	Sequen	cer [Decoder	Comparer	Logger	Organ	izer Lea	im Ex	tensions	InQL			© s	Settin
×	css inj	ection unau	th ×	3 ×	4 ×	5 ×	6 ×	7 ×	8 ×	9 ×	htm	l injection ×	11 ×	+								Q
Send	0	Cancel	<	V														Target: ht	tp://172.16.24	1.132:8080 0	Р нттр	/1
Burp Suite Community Edition v2023.7.3 - Temporary Project Dation or langet Prove find or langet Decoder Compare Logget Organize Lean Logget Organize Logget Organize Logget Organize Logget Organize Logget Decoder Compare Logget Organize Logget Decoder Compare Logget Decoder Decoder				0																		
etty POST	Raw /api/s	Hex ave opti	on HTT	P/1.1				6	\n ≣	Pretty 1 HTT	Raw	Hex BØ OK	Render				🗐 VI	=	Request attrib	utes	2	
lost	: 172.1 ent-Len	6.241.13 gth: 126	2:8080)						2 Dat 3 Ser	e: Sat, ver: Ap	18 Nov 202 ache/2.4.57	3 14:03:5 (Debian)	4 GMT					Request query	parameters	0	
K-XS eyJp	RF-TOKE dil6Ikl	N: 6dFI5R12	RaG9EK	2NNM3Q21	MGxwR1E	9PSIsIn2	hbHVlIjc.	iNGFkd	y85azl	5 Cac 6 Set	he-Cont -Cookie	rol: no-cac laravel_s	he, priva	te					Request body	parameters	4	
ðZUh FqVk DFaT	ZOTRTdz 8vQllTK 3FWaDJt	E0VTc1Vr 0t5SWhN2 YmR1VnNG	hyQXNN WxwR2x YkRlcX	SFRCaXg: KL2hEWU OiLCJtY	zR0FWNU VkeFBGd WMi0iIw	ISqUmk0Qm IkhMN0NMS M2IwZGNi	Q4S2xJVE WVwSmIvU MTU40GFm	ppM3cva Øt3anU ZDI4MD/	aWRKS1 rdXhVW A4ZmU1	8u5 16: 7 Con	CEuPv7f 03:54 G	qlI7Myolwrq 1T; Max-Age : close	m7UQFaVfh =7200; pa	/IU6fxfC th=/; ht	G; expire ponly; sa	s=Sat, 1 mesite=l	8 Nov 20 ax	23	Request cooki	es	6	
NGFm iIn@	Nzg3M2E =	5N2Q4Mjd	ImM2VjM	IDI3MmVm	ZjI20GE	yZTU2NmJ	hYTFhYjN	liIiwid	GFn I jo	8 Con 9 Con	tent-Ty	pe: applica ngth: 17	tion/json						Request head	ers	13	
ser	-Agent: eWebKit	Mozilla /537.36	/5.0 ((KHTML	Windows , like	NT 10. Gecko)	0; Win64 Chrome/1	; x64) 15.0.579	0.171		11 { "	is_save	d":true							Response hea	ders	8	
afa	<pre>ri/537. ent-Typ in: htt</pre>	36 e: appli	cation	122.90	form-ur	lencoded	l; charse	t=UTF-8	в													
efe	rer: ://172.	16.241.1	32:808	0/admin,	/contac	t-form?f	ilter[or	derFie	ld]=id													
fil	ter[ord pt-Enco	erType]= ding: gz	desc&i	flate	Page=10																	
ook	ie: isE diI6Ikl	ditMode= 6dFI5R12	true; RaG9EK	lang=en (2NNM302)	_US; XS MGxwR1E	RF-TOKEN	hbHVlIic	iNGFkd	v85azl													
ZUh qVk	ZOTRTdz 8vQllTK	EØVTc1Vn Øt5SWhN2	hyQXNN WxwR2x	ISFRCaXg KL2hEWU	zRØFWNU VkeFBGd	ISqUmk0Qm IkhMN0NMS	Q4S2xJVE WVwSmIvU	ppM3cva Øt3anU	aWRKS1 rdXhVW													
IGFm ToP	3FWaDJt Nzg3M2E %3D: la	YmR1VnNO 5N2Q4Mjd	iYkRlcX ImM2VjM	QiLCJtY DI3MmVm Bu5CFuP	WMiOiIw ZjI20GE v7folI7	M2IwZGNi yZTU2NmJ Myolwron	MTU40GFn hYTFhYjN 7U0FaVfh	ZDI4MD/ IiIiwid(A4ZmU1 GFnIjo fCvG:													
eme %70	mber_we yLhdywS	b_59ba36 fk3qy0X0	addc2b XalDvk	2f94015 bGzgbB0	80f014c cJe9yn0	7f58ea4e mXafAy6b	30989d= cxj0La00	azfpL3	fs7%7C													
bac	y%2410% k_to_ad %34//17	2400KLJ8 min= 2.16.241	. 132%3	.ZFREXUO	m5UK2TT	ntact-fo	/s/Uop.U1	ter%5B	1509.;													
eld	%5D%3Di ection:	d%26filt close	er%5Bo	rderTyp	e%5D%3D	desc%26i	temsPerF	age%3D	10													
pti odu ont	on_key= le-cont act_for	email_fr act-form m%2Fsett	om_nam -setti ings	e&optio	n_group ion_val	= .ue=" <h1></h1>	<h1>test</h1>	module	e=													
63	€ →	Search.						0	matches	00	€ >	Search					0 ma	tches				

Image [17]



Image [18]

Public