

Secure Lab 12

VULNERABILITY

REPORT

FRIDAY, JUNE 11, 2021

MODIFICATIONS HISTORY

Version	Date	Author	Description
1.0	06/11/2021	A.Karthik	Initial Version

TABLE OF CONTENTS

1.	General Information	4
1.1	Scope	4
1.2	Organisation	4
2.	Executive Summary	5
3.	Technical Details	6
3.1	title	9
4.	Vulnerabilities summary	6

GENERAL INFORMATION

SCOPE

VIT-AP has mandated us to perform security tests on the following scope:

ORGANISATION

The testing activities were performed between 06/11/2021 and 06/12/2021.

EXECUTIVE SUMMARY

VULNERABILITIES SUMMARY

Following vulnerabilities have been discovered:

Risk	ID	Vulnerability	Affected Scope
High	IDX-003	DOMXSS	
High	IDX-001	Buffer Overflow	
High	IDX-002	Clickjacking	

TECHNICAL DETAILS

DOMXSS

CVSS SEVERITY	High	CVSSv3 SCORE	7.9
CVSSv3 CRITERIAS	Attack Vector : Network Attack Complexity : High Required Privileges : Low User Interaction : Required	Scope : Changed Confidentiality : High Integrity : High Availability : Low	
AFFECTED SCOPE			
DESCRIPTION	DOM-based XSS vulnerabilities usually arise when JavaScript takes data from an attacker-controllable source, such as the URL, and passes it to a sink that supports dynamic code execution, such as <code>eval()</code> or <code>innerHTML</code> . This enables attackers to execute malicious JavaScript, which typically allows them to hijack other users' accounts. To deliver a DOM-based XSS attack, you need to place data into a source so that it is propagated to a sink and causes execution of arbitrary JavaScript.		
OBSERVATION			
TEST DETAILS			
REMEDIATION			
REFERENCES			

BUFFER OVERFLOW

CVSS SEVERITY	High	CVSSv3 SCORE	7.5
CVSSv3 CRITERIAS	Attack Vector : Local Attack Complexity : High Required Privileges : Low User Interaction : Required	Scope : Changed Confidentiality : High Integrity : High Availability : High	
AFFECTED SCOPE			
DESCRIPTION	A buffer overflow occurs when the data that is written into the buffer exceeds the allocated space and results in the overwriting of adjacent memory locations. Security attacks using buffer overflow are fairly common and most of them seek to modify data in the memory, gain access to confidential data and many more similar exploits.		
OBSERVATION			
TEST DETAILS			
REMEDIATION			
REFERENCES			

CLICKJACKING

CVSS SEVERITY	High	CVSSv3 SCORE	7.5
CVSSv3 CRITERIAS	Attack Vector : Network Attack Complexity : Low Required Privileges : High User Interaction : Required	Scope : Changed Confidentiality : High Integrity : Low Availability : Low	
AFFECTED SCOPE			
DESCRIPTION	<p>Clickjacking is an attack that tricks a user into clicking a webpage element which is invisible or disguised as another element. This can cause users to unwittingly download malware, visit malicious web pages, provide credentials or sensitive information, transfer money, or purchase products online.</p> <p>Typically, clickjacking is performed by displaying an invisible page or HTML element, inside an iframe, on top of the page the user sees. The user believes they are clicking the visible page but in fact they are clicking an invisible element in the additional page transposed on top of it.</p>		
OBSERVATION			
TEST DETAILS			
REMEDIATION			
REFERENCES			

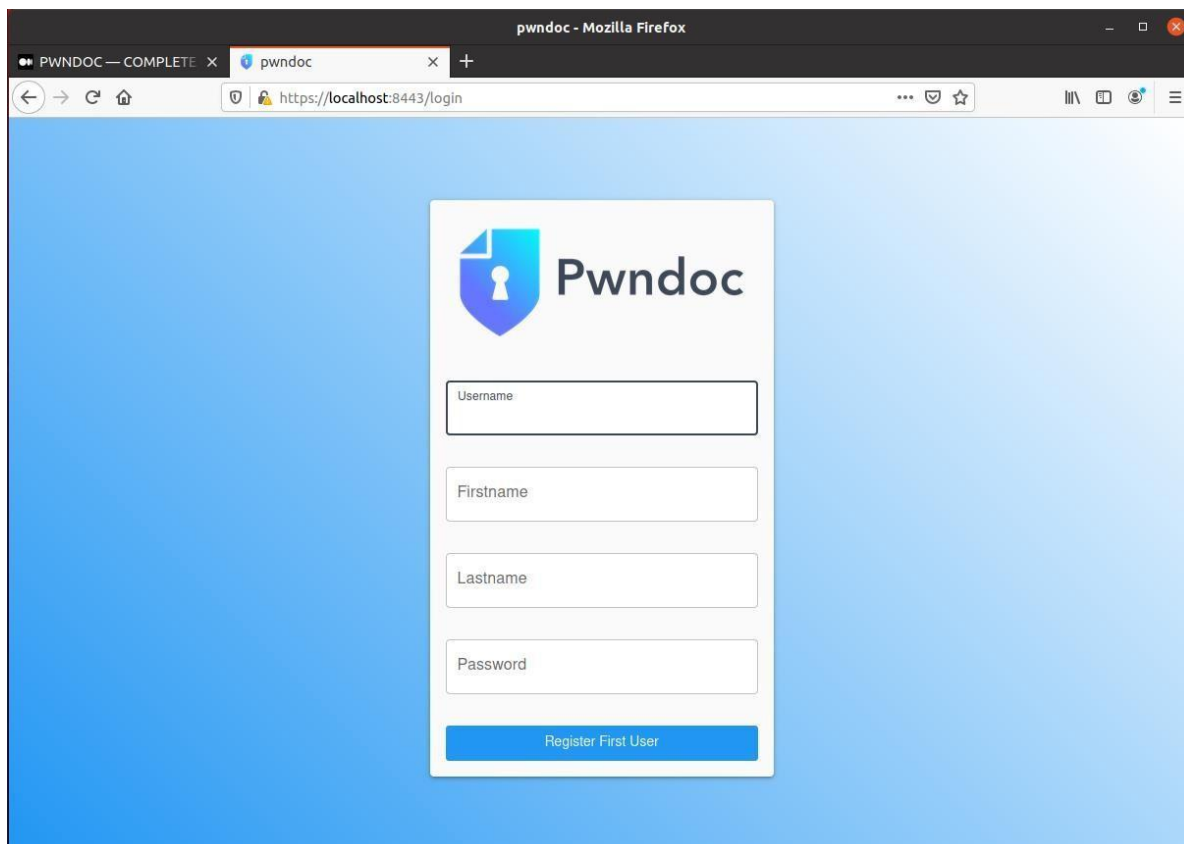
Name : A.Karthik

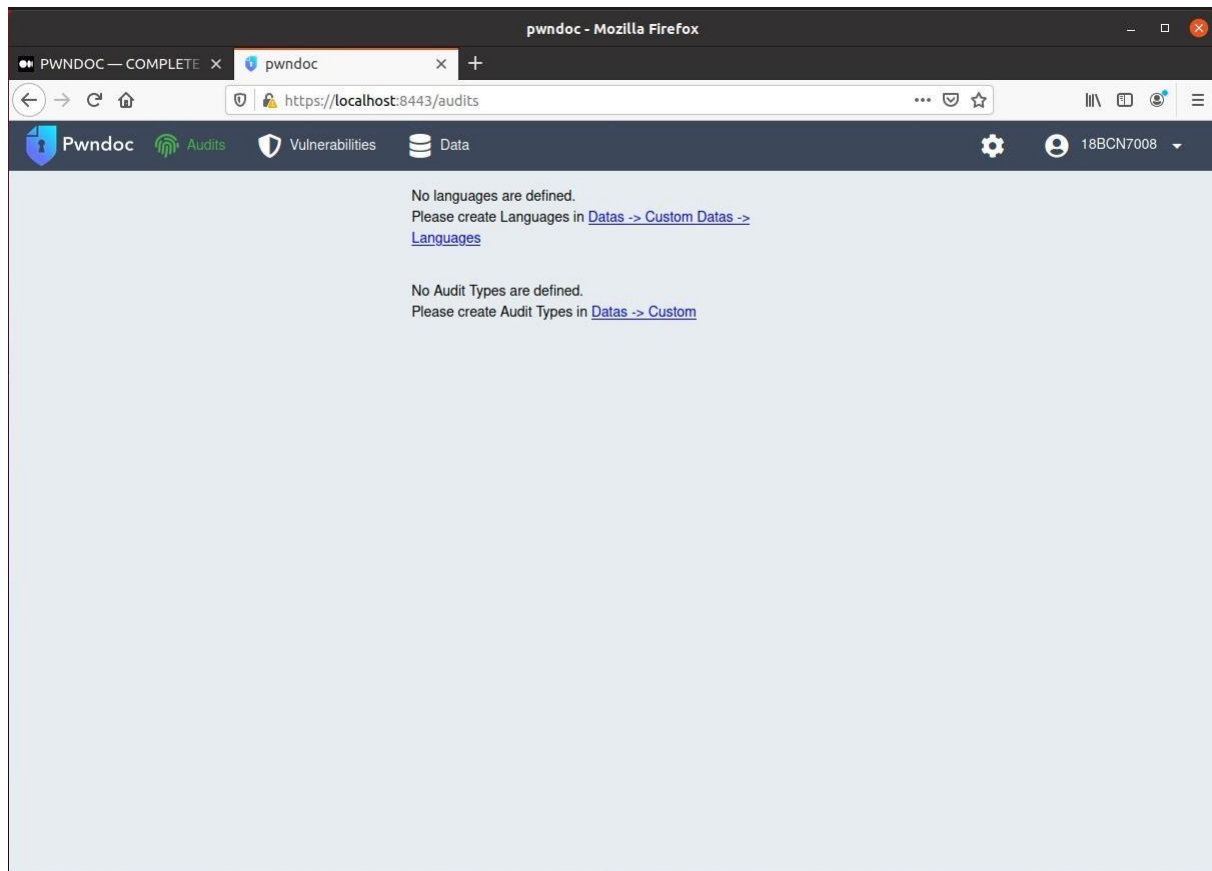
Reg. No: 18BCN7037

Installing the Pwndoc

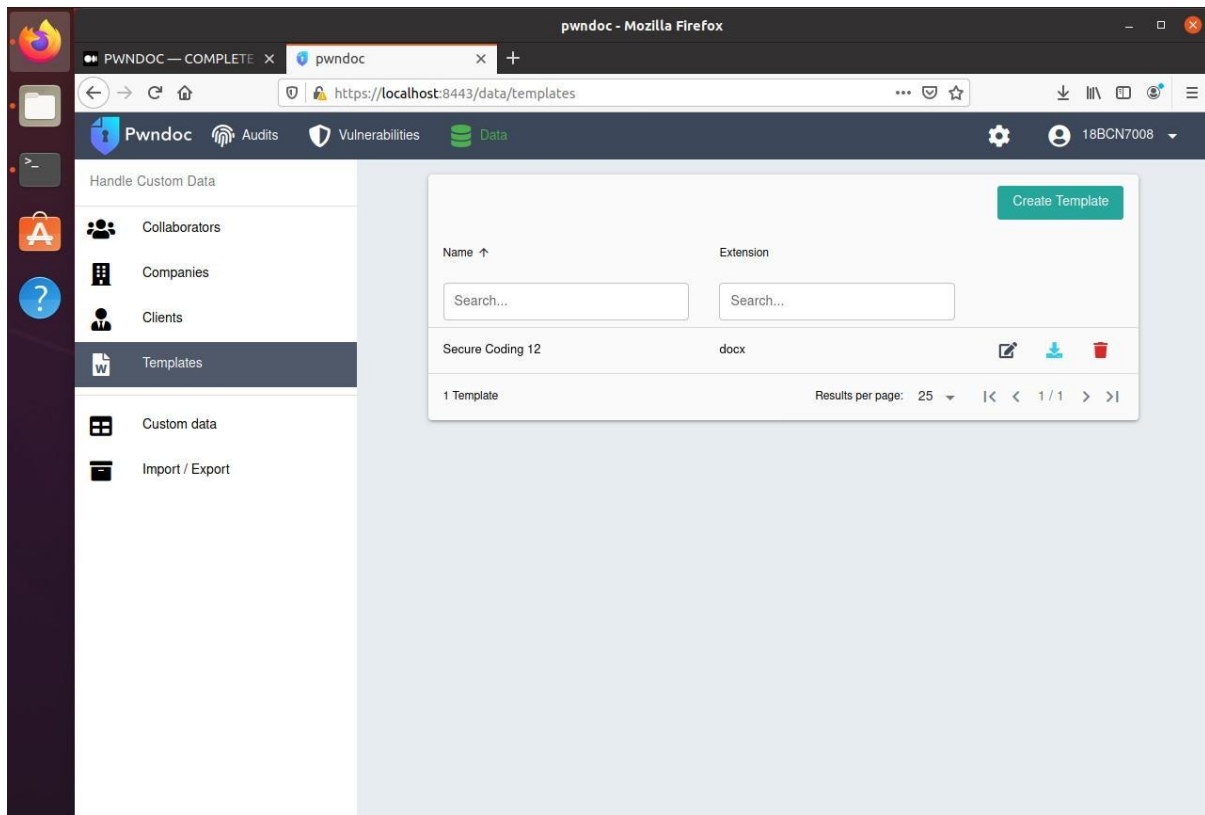
```
root@avatar-VirtualBox: /home/avatar/pwndoc
stable-alpine: Pulling from library/nginx
540db60ca938: Pull complete
b824a2584ece: Pull complete
82d0e0426b2d: Pull complete
ed76aa154407: Pull complete
ef4cf5a20f8a: Pull complete
9d3441de5d5e: Pull complete
Digest: sha256:4c945e23f40334b2f0e8d6e5040a0ea06fc5c2e0cb355d1af0ae8ba0cdf80ea8
Status: Downloaded newer image for nginx:stable-alpine
--> e1cce1fb908
Step 8/13 : COPY .docker/nginx.conf /etc/nginx/conf.d/default.conf
--> 90a2d723b201
Step 9/13 : RUN mkdir -p /etc/nginx/ssl
--> Running in 83e0bdecfe7e
Removing intermediate container 83e0bdecfe7e
--> c448a9e7a258
Step 10/13 : COPY ssl/server* /etc/nginx/ssl/
--> 6ae4aed2092d
Step 11/13 : COPY --from=build /app/dist/spa /usr/share/nginx/html
--> d8a9570785b5
Step 12/13 : EXPOSE 80
--> Running in df2b85252fce
Removing intermediate container df2b85252fce
--> 08488c70da8e
Step 13/13 : CMD ["nginx", "-g", "daemon off;"]
--> Running in c2dbc23aa406
Removing intermediate container c2dbc23aa406
--> 8f739e6ae4f5
Successfully built 8f739e6ae4f5
Successfully tagged yeln4ts/pwndoc:frontend
Creating mongo-pwndoc ... done
Creating pwndoc-frontend ... done
Creating pwndoc-backend ... done
root@avatar-VirtualBox:/home/avatar/pwndoc# docker-compose start
Starting mongodb ... done
Starting pwndoc-backend ... done
Starting pwndoc-frontend ... done
root@avatar-VirtualBox:/home/avatar/pwndoc#
```

After Installing Pwndoc





After uploading Template and Language



Creating Vulnerabilities

Activities Firefox Web Browser Jun 11 19:06

pwndoc - Mozilla Firefox

PWND0C — COMPLETE x pwndoc x cl1p.net - The internet cl x +

https://localhost:8443/vulnerabilities

Add Vulnerability (No Category)

Title * Buffer Overflow Type Language English

Description

A buffer overflow occurs when the data that is written into the buffer exceeds the allocated space and results in the overwriting of adjacent memory locations.

Security attacks using buffer overflow are fairly common and most of them seek to modify data in the memory, gain access to confidential data and many more similar exploits.

Observation

pwndoc - Mozilla Firefox

PWND0C — COMPLETE x pwndoc x cl1p.net - The internet cl x +

https://localhost:8443/vulnerabilities

CVSSv3 Base Score 7.5 (High)

Attack Vector Network Adjacent Network Local Physical

Scope Unchanged Changed

Attack Complexity Low High

Confidentiality Impact None Low High

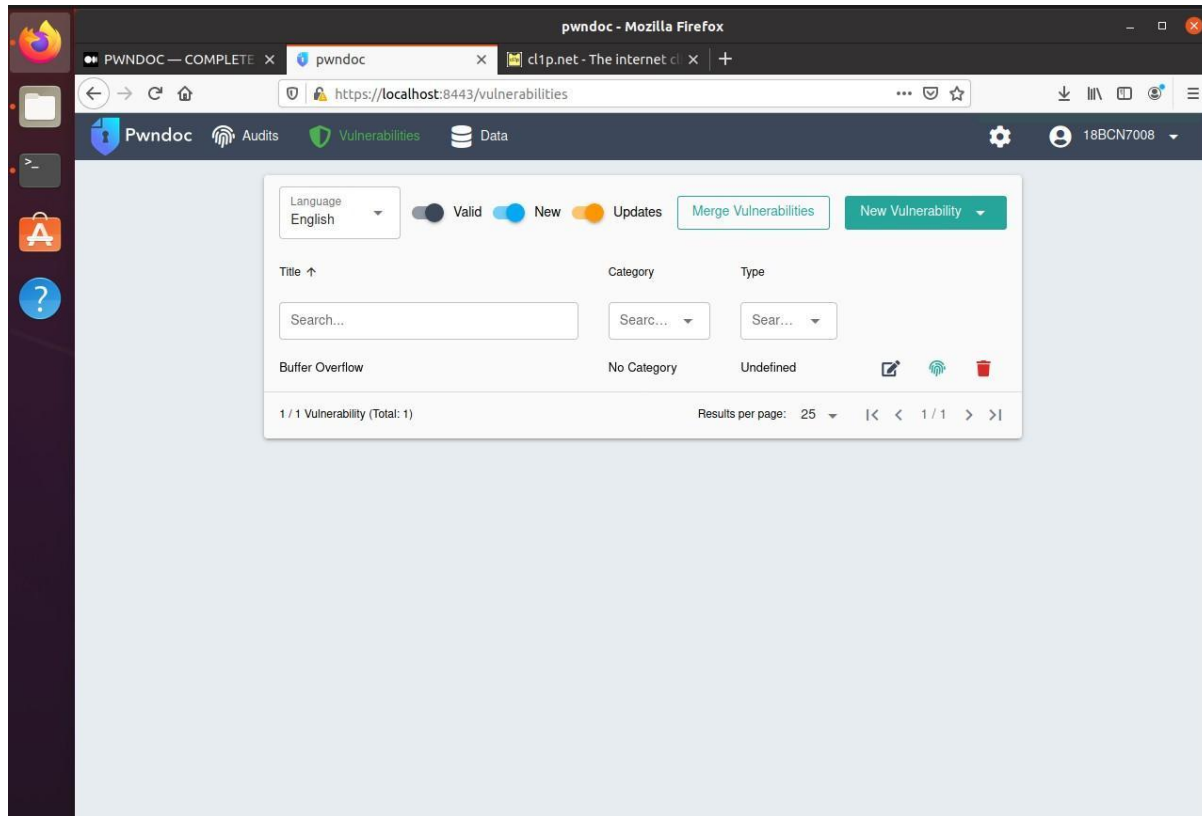
Privileges Required None Low High

Integrity Impact None Low High

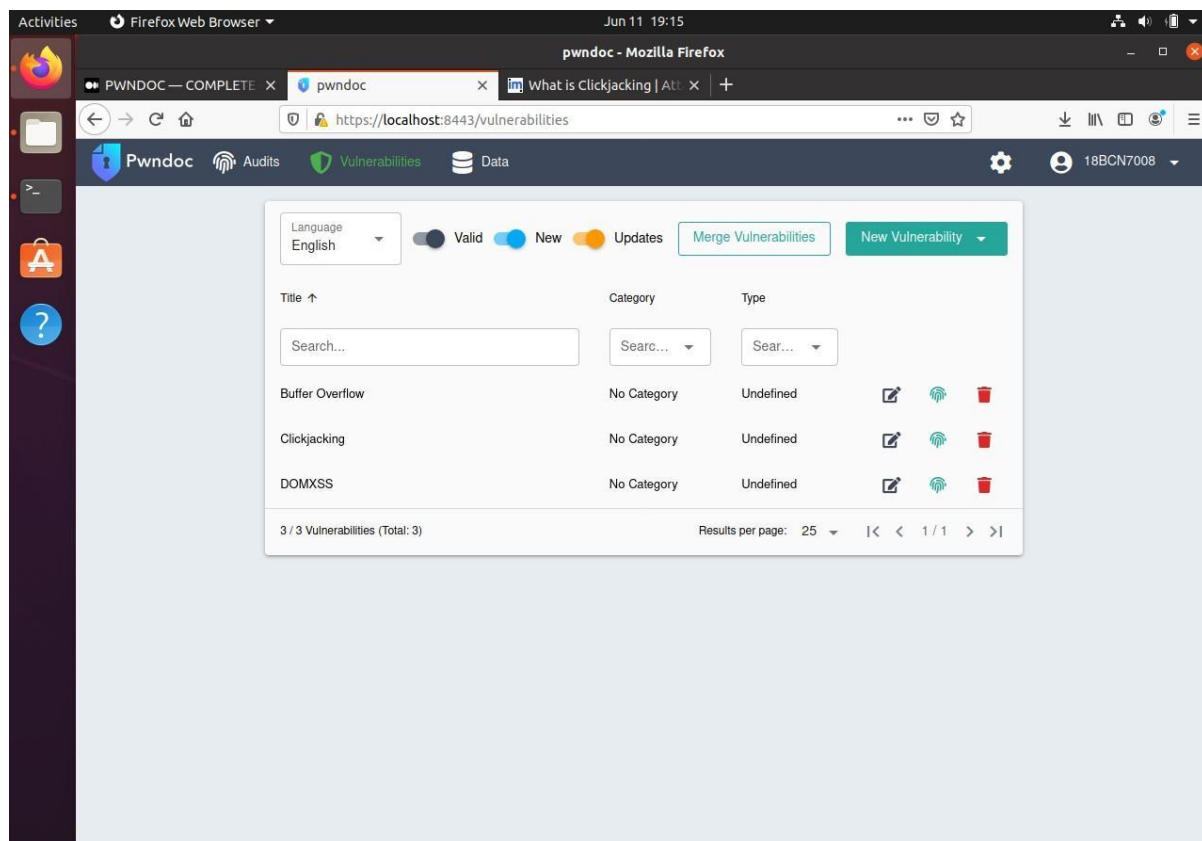
User Interaction None Required

Availability Impact None Low High

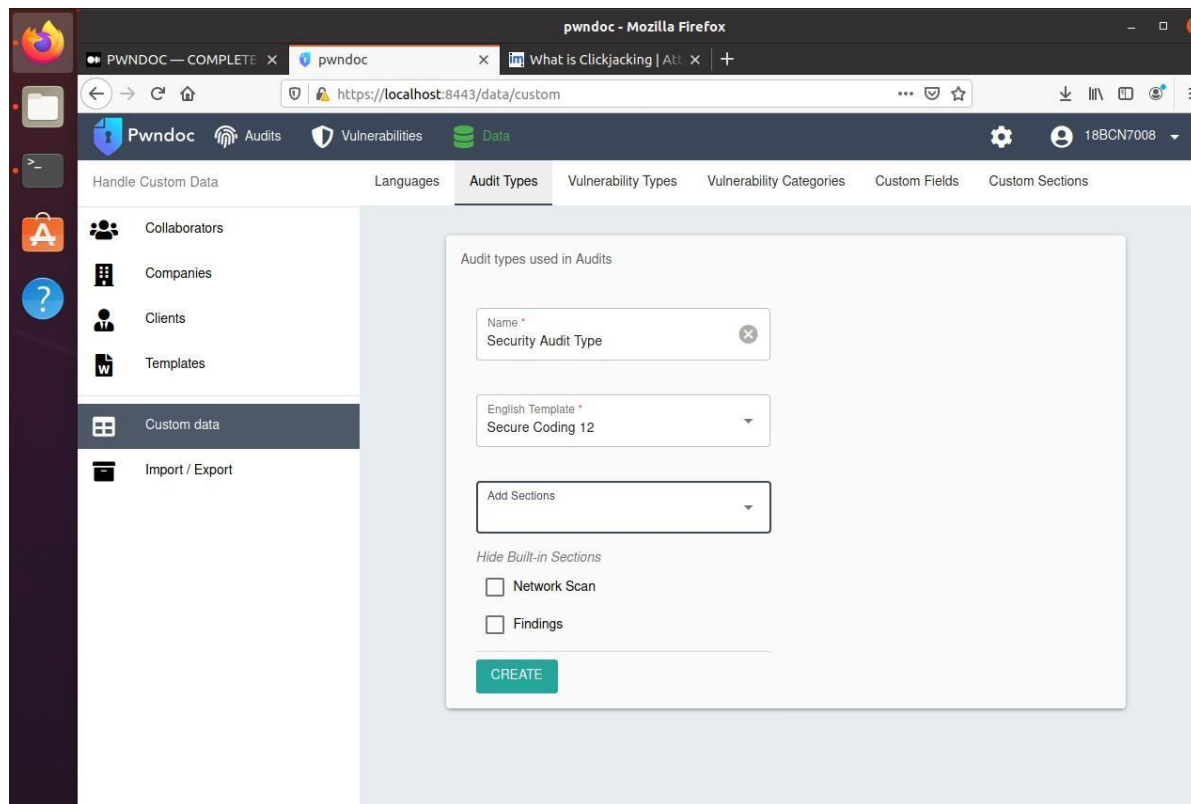
Remediation



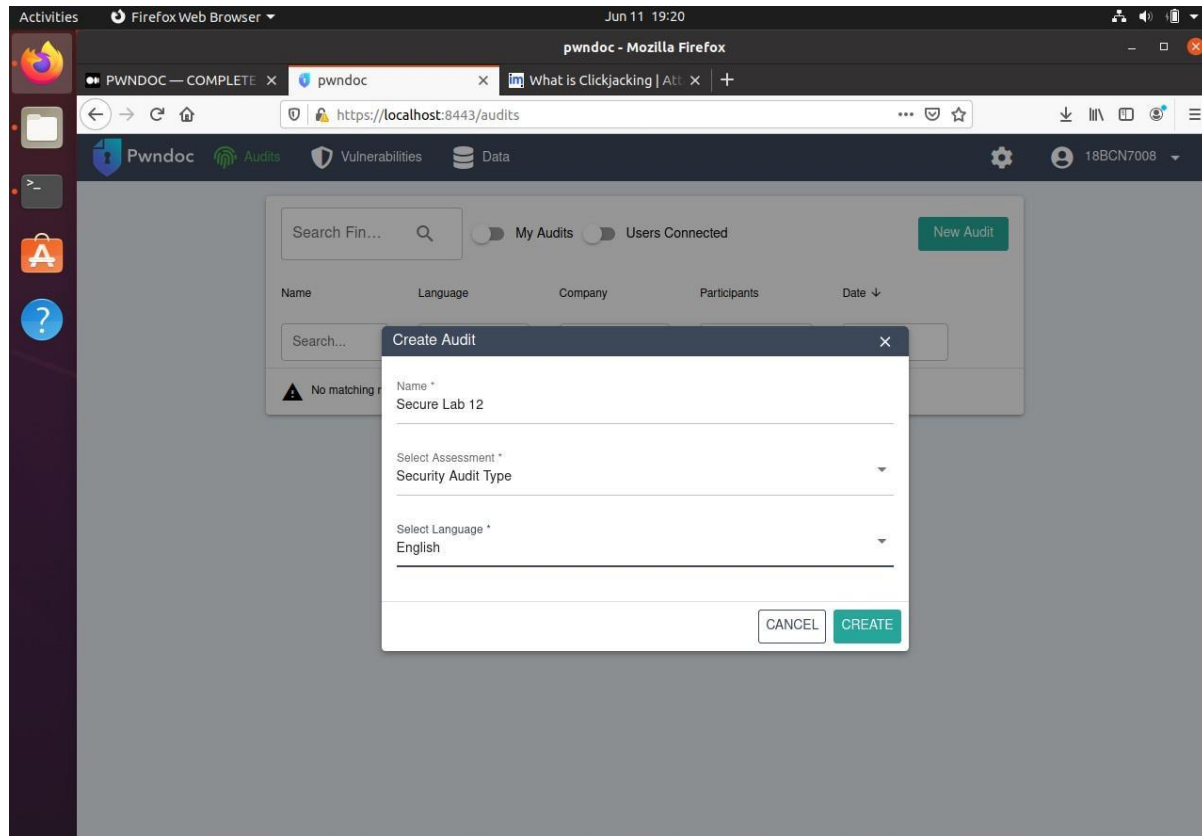
After adding some other vulnerabilities

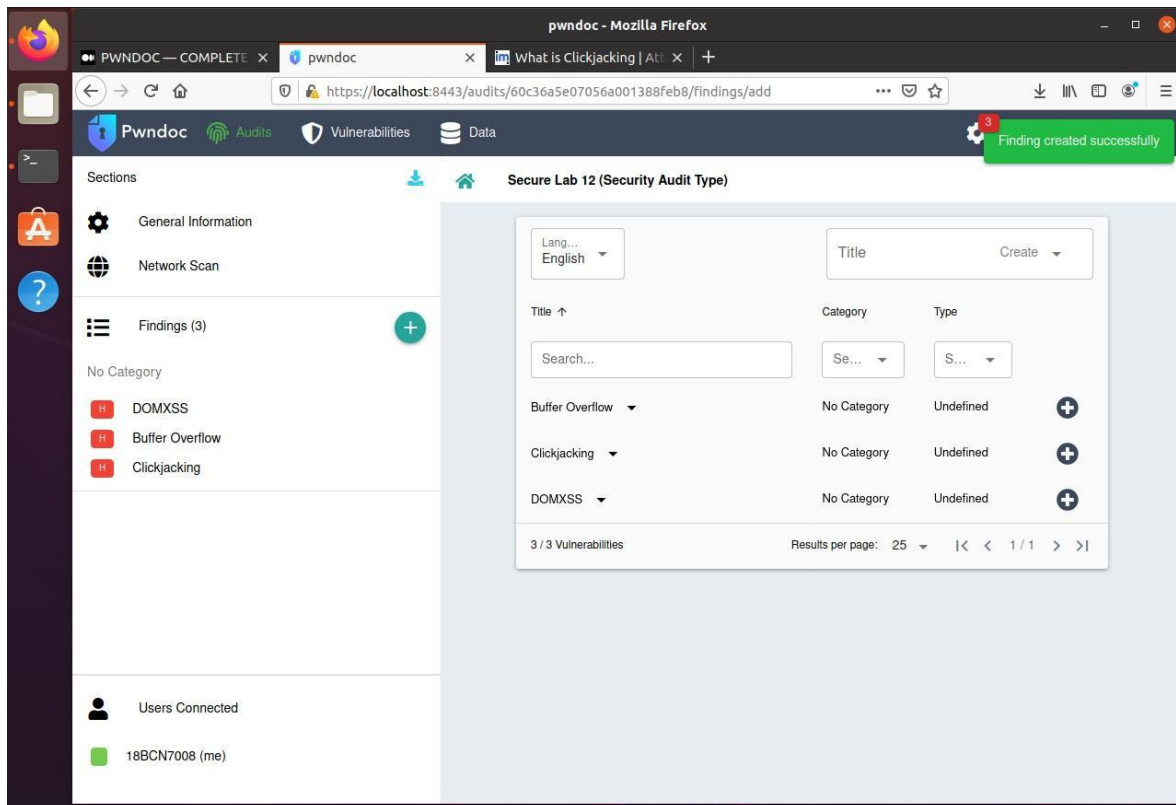
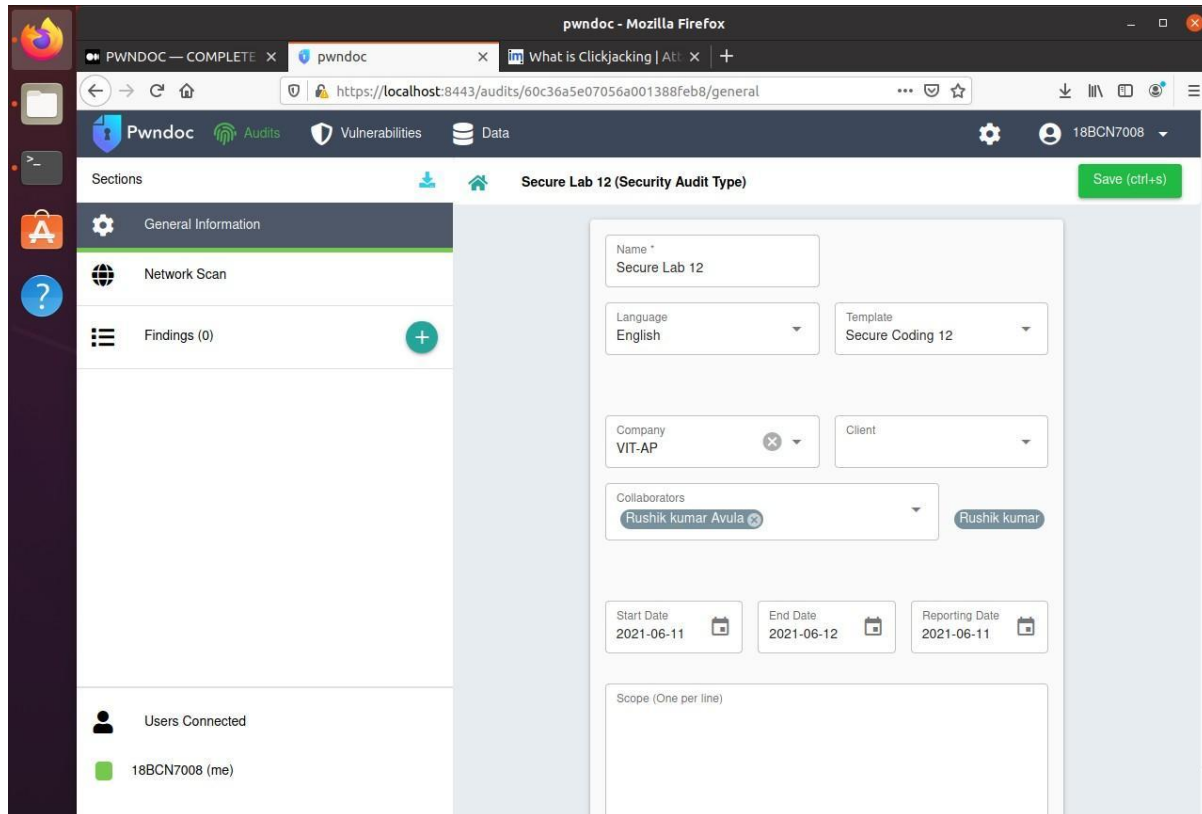


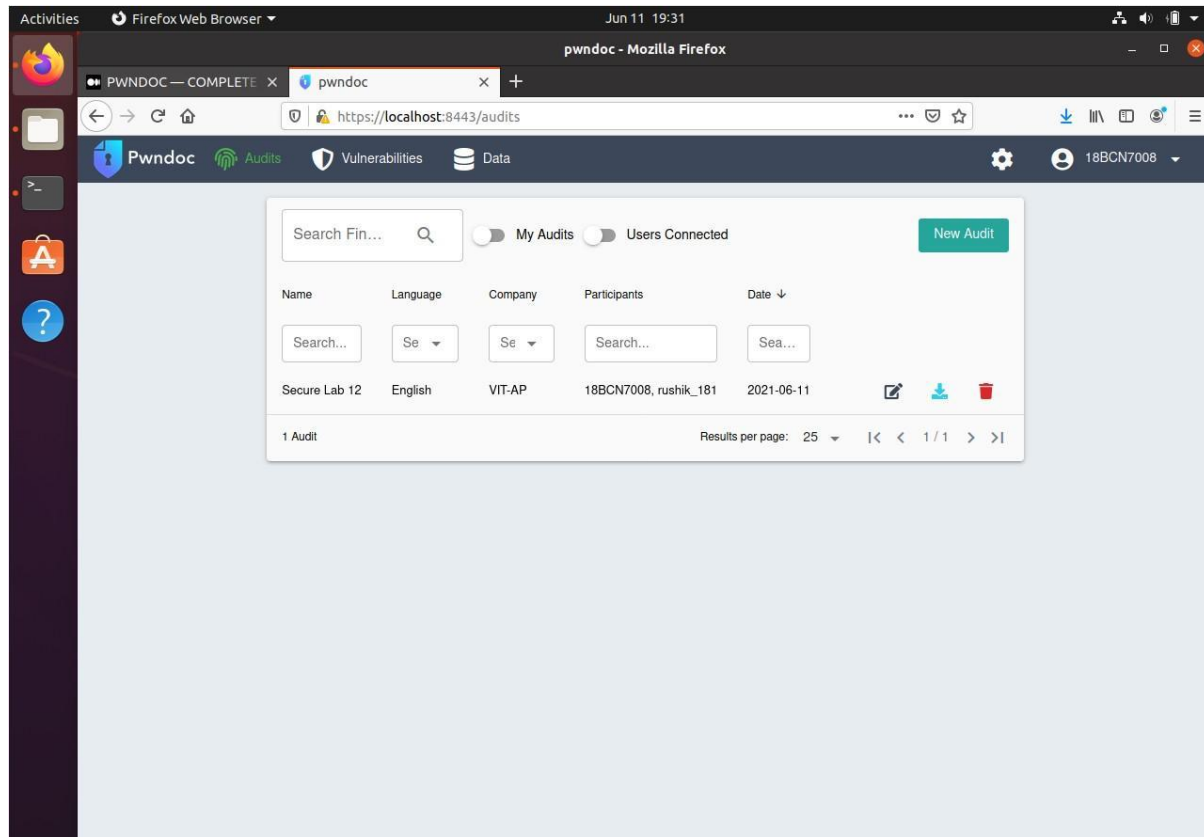
Create audit types



Then create new Audit type







Downloaded report can be found here.