**Dev-leadgen.apexure.org**

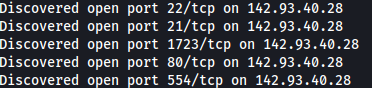
Started off with a port scan to find out which ports are running on the dev server.

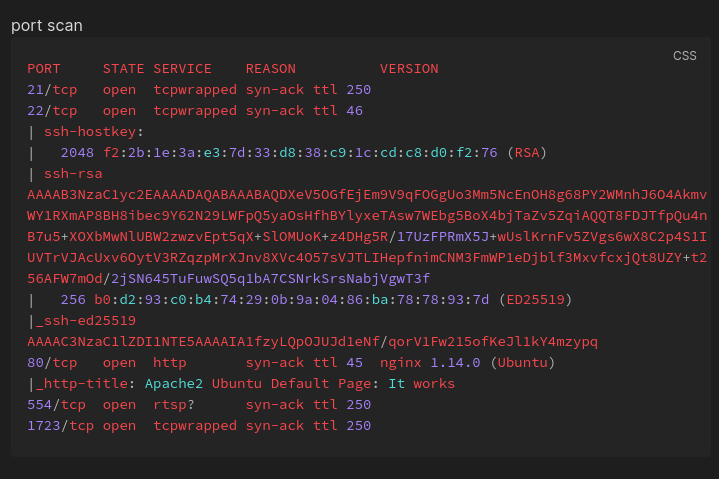


$ip = 142.93.40.28

Mail server = mail.dev-leadgen.apexure.org

5 open ports found





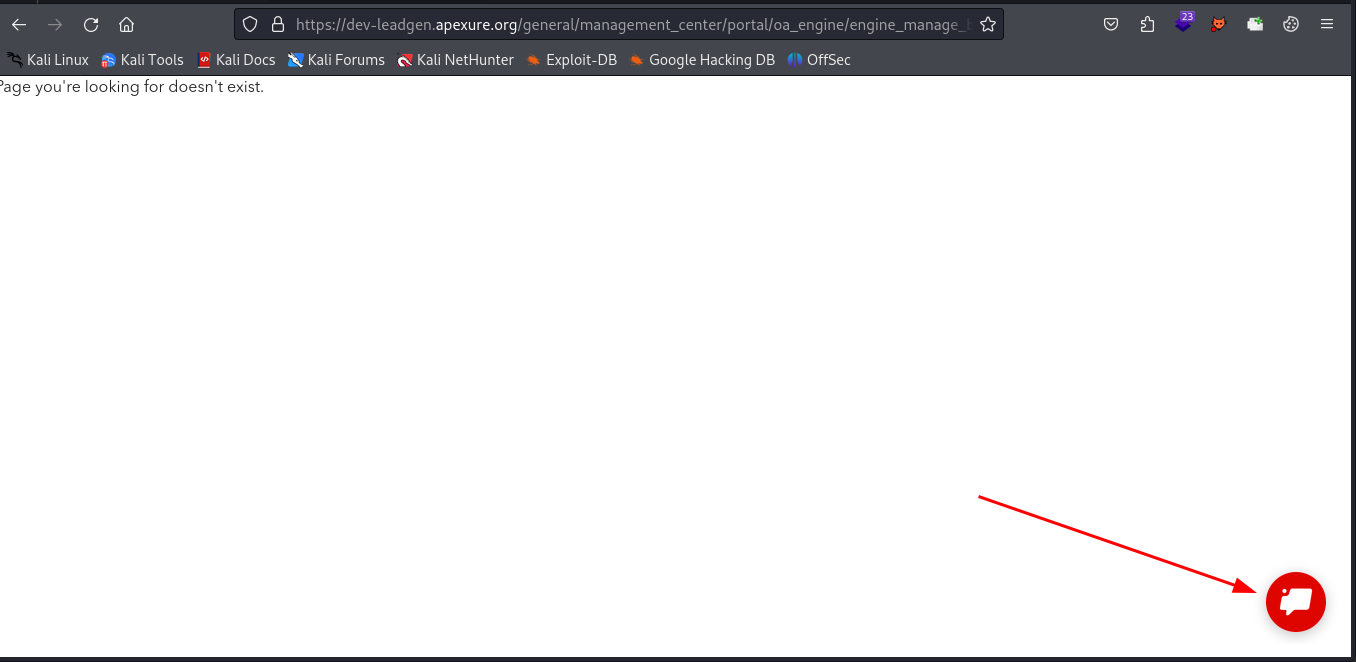
Findings:

* Programing language used :- PHP
* Operating system :- Ubuntu
* 22/tcp open ssh syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
* 80/tcp open http syn-ack nginx 1.14.0 (Ubuntu)
* Js framework vue.js
* Subject Alternative Name: DNS: api.dev-leadgen.apexure.org

Port 22 ssh is running on openssh 7.6p1 its most commonly vuln to username enum (means the hacker can determine what users accounts are on the machine to launch a brute force attack)

After scanning for open ports I was going to go for some dir busting (means to look for any sensitive information that should not be on a web app). (i am testing it without creating a user account first).

While looking at the endpoints of the application I noticed that the web application is letting me use the chatbot without authentication.

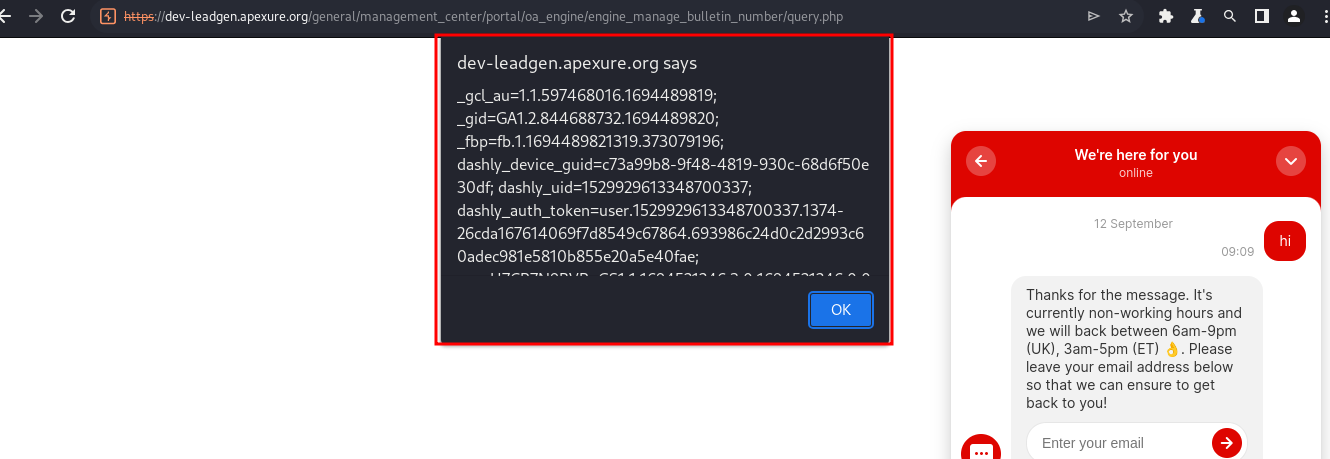


Then I started testing the chatbot using my proxy server to intercept the request and check out how the chat bot is working with the application.

I injected the payload into the request



And this how the server responded



This vuln is know as Cross Site scripting (XSS)

Cross-site scripting (XSS) is **an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website**.

So now with this vuln an attacker is not just able to steal the cookies it can also manipulate them or in worst case scenario an attacker can also compromise the whole system this is why it is considered as a high level security issue and its on the owasp top 10 vuln.