CENTRE FOR DEVELOPMENT OF ADVANCED COMPUTING (C-DAC), THIRUVANANTHAPURAM, KERALA

A PROJECT REPORT ON

"VAPT on Home of Acunetix Art Web Application"

SUBMITTED TOWARDS THE

PG-DCSF September 2023

BY

Group Number – 04

Amit Kotwal	**PRN: 230960940004**
Pranay Anil Karanjakar	**PRN: 230960940022**
Satnam Singh	**PRN: 230960940023**
Lalit Yeshwant Maske	**PRN: 230960940026**
Shubham Manohar Patil	**PRN: 230960940037**

Under The Guidance Of

Mr. Jayaram Peggam   **Dr. Hiron Bose**

(Centre Co- Ordinator)   **(Project Guide)**

Table of Contents

Abstract

The "Vulnerability Assessment and Penetration Testing (VAPT) on "HOME OF ACUNETIX ART WEB APPLICATION" project aims to perform a comprehensive security assessment of the deliberately vulnerable web application, HOME OF ACUNETIX ART WEB APPLICATION. The primary objective is to identify, analyze, and document various security vulnerabilities within the application, thereby enhancing participants' understanding of web application security and providing insights into effective remediation strategies.

The project involves the systematic exploration of HOME OF ACUNETIX ART WEB APPLICATION's codebase, functionalities, and interactions to simulate real-world attack scenarios. By employing established VAPT methodologies and a range of security testing tools, the project team will uncover vulnerabilities such as SQL injection, cross-site scripting (XSS), Cross-Site Request Forgery (CSRF), and more. The vulnerabilities' potential impact on the application's security and user data integrity will be evaluated, highlighting the importance of proactive security measures.

Throughout the assessment, a structured approach will be maintained, encompassing vulnerability identification, proof of concept exploitation, risk assessment, and recommendation formulation. The outcomes of the project will include a detailed report summarizing the discovered vulnerabilities, their potential implications, and recommendations for mitigation. Additionally, the project will provide valuable insights into commonly used testing methodologies and tools, empowering participants to effectively tackle web application security challenges.

This project's significance lies in its educational nature. By analyzing and addressing vulnerabilities within HOME OF ACUNETIX ART WEB APPLICATION, participants will enhance their practical knowledge of security threats and countermeasures. The project's outcomes will facilitate improved security practices, contribute to the growth of security expertise, and foster a heightened awareness of web application vulnerabilities among developers, testers, and security enthusiasts.

Objective

The objective of the assessment was to assess the state of security and uncover vulnerabilities in **Home of Acunetix Art Web Application** and provide with a final security assessment report comprising vulnerabilities, remediation strategy and recommendation guidelines to help mitigate the identified vulnerabilities and risks during the activity.

CERTIFICATE

THIS IS CERTIFY THAT,

Amit Kotwal	PRN: 230960940004
Pranay Anil Karanjakar	PRN: 230960940022
Satnam Singh	PRN: 230960940023
Lalit Yeshwant Maske	PRN: 230960940026
Shubham Manohar Patil	PRN: 230960940037

Have Satisfactory completed the project work Entitled, "Enhancing Security Posture: Vulnerability Assessment and Penetration Testing "HOME OF ACUNETIX ART WEB APPLICATION" to Centre for Advanced Computing in the partial fulfilment of the requirement of Post-Graduate Diploma (PG-Diploma), is a record of project work carried out by them under my guidance and supervision. The matter presented in this project report has not been submitted either in part of full to any University or Institute for award of any degree.

Mr. Jayram Peggam   **Dr. Hiron Bose**

(Centre Co-Ordinator)   (Project Guide)

1. Introduction

1.1. Introduction to Home of Acunetix Art Web Application pen testing report

This pen testing report provides an in-depth analysis of the security assessment conducted on the HOME OF ACUNETIX ART WEB APPLICATION platform. As a purposely vulnerable web application designed for educational and training purposes, HOME OF ACUNETIX ART WEB APPLICATION presents a unique opportunity to explore and understand the intricacies of web application security vulnerabilities. The objective of this assessment was to systematically identify potential security weaknesses within HOME OF ACUNETIX ART WEB APPLICATION, evaluate their impact, and propose effective mitigation strategies.

1.2. Background and context

In the digital landscape, where web applications have become integral to daily activities, security remains a paramount concern. Cyber threats targeting web applications have evolved, leading to an increased emphasis on identifying, understanding, and mitigating vulnerabilities before they are exploited by malicious actors. To address this, HOME OF ACUNETIX ART WEB APPLICATION offers an environment that simulates real-world vulnerabilities, enabling security professionals, developers, and enthusiasts to learn, practice, and develop effective Défense strategies.

1.3. VAPT

VAPT stands for "Vulnerability Assessment and Penetration Testing." It is a process used to evaluate the security of computer systems, networks, or applications by identifying vulnerabilities and attempting to exploit them in a controlled manner.

Vulnerability Assessment (VA): This involves using various tools and techniques to identify potential vulnerabilities in a system, network, or application. It is essentially a systematic process of scanning and analyzing for security weaknesses. These vulnerabilities could include outdated software, misconfigurations, weak passwords, and more.

Penetration Testing (PT): Also known as ethical hacking, penetration testing involves simulating real-world attacks on a system, network, or application to determine how vulnerable it is to different types of threats. This is typically done by security professionals who mimic the actions of malicious hackers but do so in a controlled environment.

The main goal of VAPT is to find and address security weaknesses before malicious attackers can exploit them. By conducting regular VAPT assessments, organizations can identify vulnerabilities, prioritize their mitigation efforts, and ultimately enhance their overall security posture.
It is important to note that VAPT requires specialized knowledge and skills, and it should be performed by experienced professionals to avoid any unintentional disruptions or damage to the systems being tested.

Advantages of VAPT

1. Identify Weaknesses: VAPT helps identify vulnerabilities and weaknesses in systems, networks, and applications that could potentially be exploited by malicious actors. This allows organizations to take proactive steps to address these issues before they are exploited.
2. Prioritize Remediation: VAPT provides insight into the severity of vulnerabilities, helping organizations prioritize which vulnerabilities to address first based on their potential impact and risk.
3. Real-world Simulation: Penetration testing simulates real-world attack scenarios, giving organizations a practical understanding of how their systems might be targeted and breached by actual attackers.
4. Risk Reduction: By addressing vulnerabilities proactively, VAPT helps reduce the risk of security breaches, data leaks, and other cyber incidents that could lead to financial and reputational damage.
5. Compliance: Many industries and regulatory frameworks require organizations to conduct regular security assessments, including VAPT, to ensure compliance with security standards.
6. Enhanced Security Awareness: VAPT increases the overall security awareness within an organization. It educates employees and stakeholders about potential threats and the importance of security best practices.
7. Continuous Improvement: Regular VAPT assessments promote a culture of continuous improvement in an organization's security practices. As new vulnerabilities emerge, organizations can adapt and update their defenses accordingly.
8. Validation of Security Measures: VAPT validates the effectiveness of existing security measures and controls. It confirms whether the implemented security mechanisms are providing the intended protection.
9. Third-party Validation: Organizations can demonstrate their commitment to security to customers, partners, and stakeholders by undergoing VAPT assessments. This can enhance trust and confidence in their services.
10. Reduced Attack Surface: Through the identification and remediation of vulnerabilities, VAPT helps shrink the potential attack surface, making it more difficult for attackers to find entry points.
11. Cost Savings: Detecting and addressing vulnerabilities early in the development lifecycle can save organizations significant costs that would otherwise be incurred to recover from a security breach.
12. Customization: VAPT can be customized to the specific needs and requirements of an organization. It can target critical systems, specific applications, or network segments.
13. Threat Awareness: VAPT not only focuses on technical vulnerabilities but also helps organizations understand the potential threat landscape they operate in, allowing them to make informed decisions about security investments.
14. Overall, VAPT is a crucial practice for organizations looking to fortify their cybersecurity defenses, minimize risks, and protect sensitive data from evolving cyber threats.

1.4. Methodology and Approach

The assessment was conducted through a meticulous blend of manual testing, automated vulnerability scanning, and targeted exploitation. This multifaceted approach allowed for a comprehensive examination of HOME OF ACUNETIX ART WEB APPLICATION vulnerabilities, ranging from easily detectable flaws to more intricate security challenges. The methodology included the following key steps:

1.1.1 **Pre-Assessment Preparation:**
Gaining a deep understanding of the Home of Acunetix Art Web Application, its architecture, functionalities, and potential attack vectors.

1.1.2 **Vulnerability Scanning:**
Employing automated tools to conduct initial scans for common vulnerabilities, providing a baseline for further exploration.

1.1.3 **Manual Testing and Exploitation:**
Utilizing ethical hacking techniques to manually validate and exploit vulnerabilities identified through scanning, delving into the intricacies of each weakness.

1.1.4 **Impact Analysis:**
Assessing the potential consequences of successful exploitation, considering factors such as data exposure, unauthorized access, and potential for privilege escalation.

1.1.5 **Reporting:**
Documenting findings, including vulnerability descriptions, impact assessments, and detailed recommendations for mitigation.

1.5. System Requirements

The hardware and software requirements for conducting Vulnerability Assessment and Penetration Testing (VAPT) can vary based on the scope of the assessment, the target systems, and the specific tools and methodologies being employed. Here is a general overview of the typical requirements:

Hardware Requirements:

Computer Systems: Depending on the complexity of the assessments, you will need one or more powerful computers to run the necessary tools and perform testing activities.

Virtualization: Virtualization software like VMware or VirtualBox is often used to create isolated environments for testing. This allows you to simulate different network setups and test configurations without affecting your production environment.

Powerful Resources: For certain types of testing, such as brute force attacks or password cracking, more computational power may be needed to expedite the testing process.

Software Requirements:

Operating Systems: A variety of operating systems might be needed to support different testing scenarios. This could include Windows, Linux distributions, and specialized penetration testing

platforms like Kali Linux.

Penetration Testing Frameworks: Tools like Metasploit, Burp Suite, OWASP Top 10, Nmap, and Wireshark are commonly used for different stages of VAPT.

Vulnerability Scanners: Vulnerability assessment tools like Nessus, OpenVAS, and Qualys can be used to scan systems for known vulnerabilities.

Network Analysis Tools: Network analyzers like Wireshark are used to capture and analyze network traffic.

Virtualization Software: Software like VMware or VirtualBox is essential for creating virtual environments for testing and isolating your activities.

Exploitation Tools: These tools are used to exploit vulnerabilities in a controlled environment to determine their impact. Examples include tools from the Metasploit framework.

Password Cracking Tools: For password security assessment, tools like John the Ripper or Hash cat can be used.

Documentation and Reporting Tools: Tools for documenting findings and generating detailed reports about the vulnerabilities and their potential impact.

Collaboration Tools: Communication and collaboration tools can be essential for team members to coordinate and share information during the testing process.

Custom Scripts: Depending on your specific testing requirements, you might need custom scripts or tools to carry out specific tests.

VPN and Anonymity Tools: In some cases, VPNs and anonymity tools might be used to ensure ethical testing practices and to protect the tester's identity.

It's important to note that VAPT requires careful planning and adherence to ethical guidelines. Always ensure you have proper authorization and consent before performing any testing, especially on systems and networks that you do not own. Additionally, keep your tools and software up to date to ensure accurate results and optimal security during testing Project outcomes.

1.6. Ethical Consideration

It is imperative to acknowledge that the vulnerabilities uncovered within this report are exclusive to the HOME OF ACUNETIX ART WEB APPLICATION platform, purposefully designed for educational purposes. Therefore, the vulnerabilities identified here do not reflect vulnerabilities that could occur in real-world applications. The intention behind this assessment is to enhance the understanding of security professionals, developers, and learners regarding common web application vulnerabilities and the importance of implementing effective security measures.

1.7. Report Structure

This comprehensive pen testing report is organized into distinct sections, each dedicated to a specific category of vulnerabilities found within HOME OF ACUNETIX ART WEB APPLICATION. Each section follows a consistent structure:

Introduction to the vulnerability category and its implications. Detailed description of identified vulnerabilities, their potential impact, and their reproducible steps. Severity assessment of each vulnerability based on its potential consequences. Recommendations for mitigating the vulnerabilities, including technical solutions and best practices.

2. Summary

2.1 Scope and Objectives

The scope of this pen testing assessment encompassed a comprehensive evaluation of HOME OF ACUNETIX ART WEB APPLICATION vulnerabilities across various categories. These included but were not limited to injection attacks,cross-site scripting (XSS), session management issues, insecure configurations, and other common and advanced security flaws. The assessment's objectives were multifaceted:

- To systematically identify vulnerabilities that could potentially compromise the confidentiality, integrity, or availability of the application.
- To assess the robustness of security controls and countermeasures implemented within HOME OF ACUNETIX ART WEB APPLICATION.
- To provide actionable recommendations that enhance the application's overall security posture.

2.2 Project outcomes

" HOME OF ACUNETIX ART WEB APPLICATION" it is a deliberately vulnerable web application used for practicing and learning about web application security. Conducting a Vulnerability Assessment and Penetration Testing (VAPT) on HOME OF ACUNETIX ART WEB APPLICATION can have several project outcomes, depending on the goals and scope of the assessment. Here are some possible outcomes:

Identification of Vulnerabilities: The primary outcome of a VAPT on HOME OF ACUNETIX ART WEB APPLICATION would be the identification of various vulnerabilities present in the application. These vulnerabilities could include SQL injection, cross-site scripting (XSS), CSRF (Cross-Site Request Forgery), insecure authentication mechanisms, and more.

Documentation of Findings: The vulnerabilities and weaknesses discovered during the assessment would be documented in detail. This documentation would include descriptions of the vulnerabilities, their potential impact, and recommendations for remediation.

Exploitation and Proof of Concept: For educational purposes, the testing team might exploit the identified vulnerabilities to demonstrate how an attacker could potentially compromise the application. This can help stakeholders understand the real-world impact of these vulnerabilities.

Risk Assessment and Prioritization: The vulnerabilities found can be categorized based on their severity and potential impact on the application's security. This allows the project team to prioritize which vulnerabilities should be addressed first.

Remediation Recommendations: The testing team would provide recommendations for fixing the vulnerabilities. This could include suggesting code changes, configuration adjustments, or other measures to mitigate the risks.

Detailed Reporting: A comprehensive report would be generated to summarize the assessment's findings. The report might include an executive summary, details about vulnerabilities, risk assessments, recommendations, and any other relevant information.

Proof of Competence: For individuals or teams involved in conducting the VAPT, successfully identifying and demonstrating vulnerabilities on HOME OF ACUNETIX ART WEB APPLICATION could serve as a form of validation for their skills and competence in the field of web application security. Remember that HOME OF ACUNETIX ART WEB APPLICATION is intentionally vulnerable, so any findings and outcomes from a VAPT conducted on it are primarily educational. The goal is to learn how to identify and address vulnerabilities in a safe environment, rather than applying the findings to a production application.

Table 1: Risk Rating

Info	Low	Medium	High	Critical
No direct threat to host/ individual user account. Sensitive information can be revealed to the adversary.	Vulnerabilities may not have public exploit (code) available or cannot be exploited in the wild. Vulnerability observed may not have high rate of occurrence. Patch workaround released by vendor.	Vulnerabilities may not have public exploit (code) available or cannot be exploited in the wild. Patch/ workaround not yet released by vendor.	Vulnerabilities which can be exploited publicly, workaround or fix/ patch available by vendor.	Vulnerabilities which can be exploited publicly, workaround or fix/ patch may not be availableby vendor.

Table 2 categorizing vulnerabilities

Category	Description
No. of live host	1
No. vulnerabilities	8
No. of critical vulnerabilities	0
No. of high vulnerabilities	3
No. of medium vulnerabilities	5
No. of low vulnerabilities	0

Table 3 List of Exploited vulnerabilities

Sr No	Category	Severity
1	Broken Access Control	Medium
2	Cryptographic Failure	Medium
3	SQL injection	High
4	Server-Side Request Forgery	Medium
5	Reflected XSS	Medium
6	Stored XSS	High
7	Clickjacking	High
8	Directory Index disclosure	Medium

3. Technical Report

3.1 Broken Access Control

Reference No:	Risk Rating:
WEB_VUL_01	Medium

Tools Used:
Browser

Vulnerability Description:
It was observed that in the signup page we can bypass the user authentication by adding SQL queries and can enter the accounts. Also, a weak password management policy is implemented during the user registration process.

Vulnerability Identified by / How It Was Discovered
Manual analysis

Vulnerable URLs / IP Address
http://testphp.vulnweb.com/login.php

Impacts / Consequences of not Fixing the Issu
An adversary having knowledge of SQL could easily bypass the user authentication and can gain access to the any users account even the admin too. He /She can make changes to the account, and if the account has administrative privileges, then the whole web application can get compromised.

Suggested Mitigation
1. Implement multi-factor authentication to prevent automated, credential stuffing, brute force, and stolen credential re-use attacks. 2. Do not ship or deploy with any default credentials, particularly for admin users. 3. Implement weak-password checks, such as testing new or changed passwords against a list of the top 10000 worst passwords. 4. Align password length, complexity, and rotation policies with NIST 800-63 B's guidelines in section 5.1.1 for Memorized Secrets or other modern, evidence-based password policies.

References
https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication

Proof of concept

Fig 1: Go to the target URL

Fig 2: Type ' or true # in both the fields and click on Login button
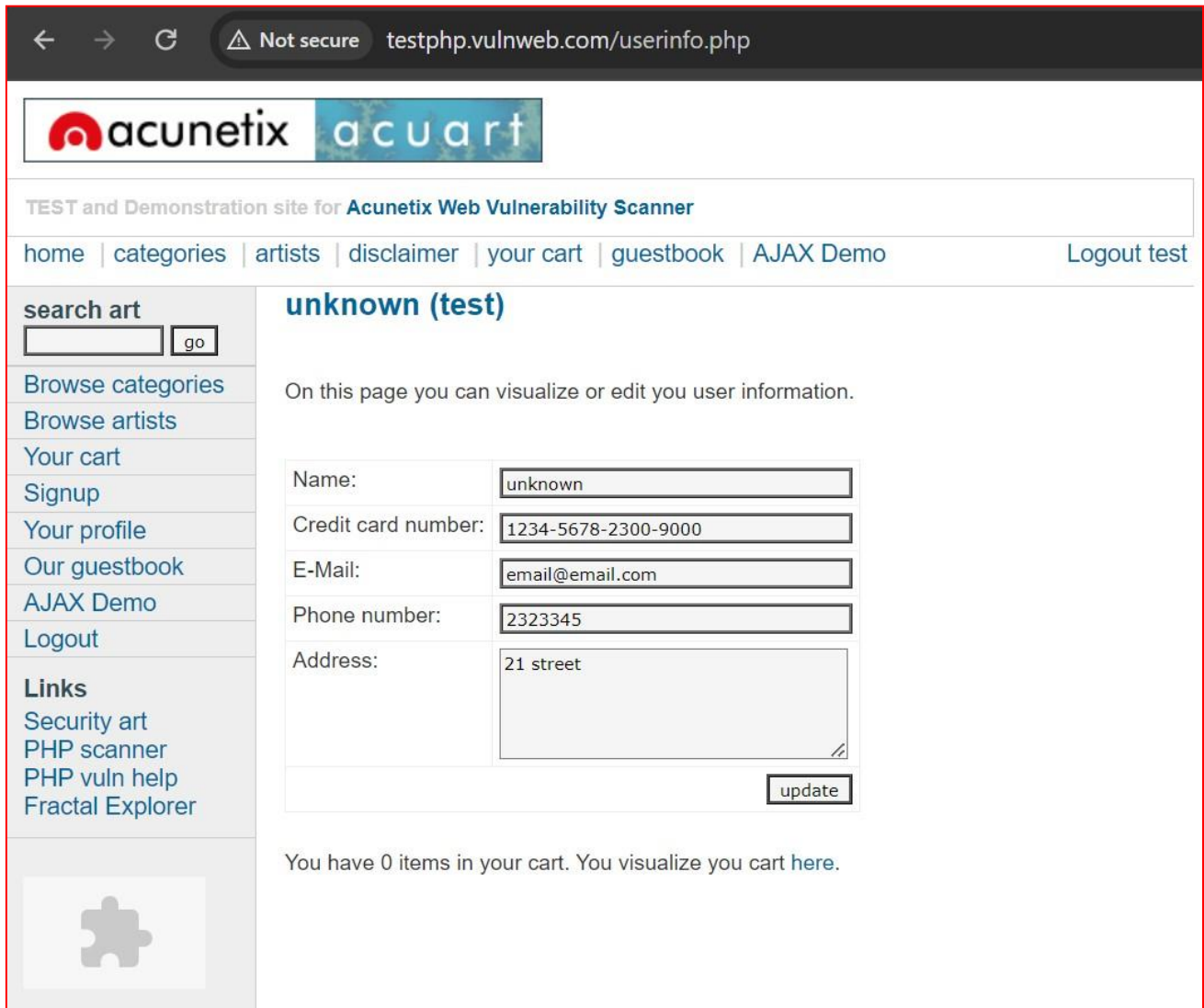
Fig 3: We have been successfully logged into somebody's account

3.2 Cryptographic Failure

Reference No:	Risk Rating:
WEB_VUL_02	Medium
Tools Used:	
Burp suite	
Vulnerability Description:	
We have found that whatever password we entered in the password field can be available when we catch the request using Burp suite application. Value of the passwordis not stored in any hash value or in the cryptic format and because of this when we got hacked hacker able to knew the password easily.	
Vulnerability Identified by / How It Was Discovered	
Manual analysis	
Vulnerable URLs / IP Address	
http://testphp.vulnweb.com/login.php	
Impacts / Consequences of not Fixing the Issu	
Attackers who intercept the credentials can use them to impersonate users and gain unauthorized access to their accounts. User privacy is compromised as their sensitivedata is exposed during transmission. Sensitive information, including usernames, passwords, and tokens, is exposed, and can be easily intercepted by attackers.	
Suggested Mitigation	

1. User entered password need to be saved in hashed format.

2. "Use HTTPS" to encrypt the communication channel between the client and the server. HTTPS uses SSL/TLS protocols to provide confidentiality, integrity, and authentication for the data. HTTPS also prevents downgrade attacks that can force the connection to use HTTP instead of HTTPS.

3. "Use secure flags" to prevent the transmission of sensitive data over clear text HTTP. For example, if HTTP cookies are used for transmitting session tokens, then the secure flag should be set to prevent transmission over clear text HTTP.

4. "Use hashing or encryption" to protect the sensitive data before transmitting it over HTTP. Hashing generates a fixed-length value from the data that can be verified by the receiver without revealing the original data. Encryption makes thedata unreadable and unmodifiable by anyone who does not have the secret key.

5. "Use proper logging and monitoring" of the access and usage of sensitive data. Detect and respond to any suspicious or anomalous activities or breaches.

References

https://crashtest-security.com/owasp-cryptographic-failures/

Proof of concept

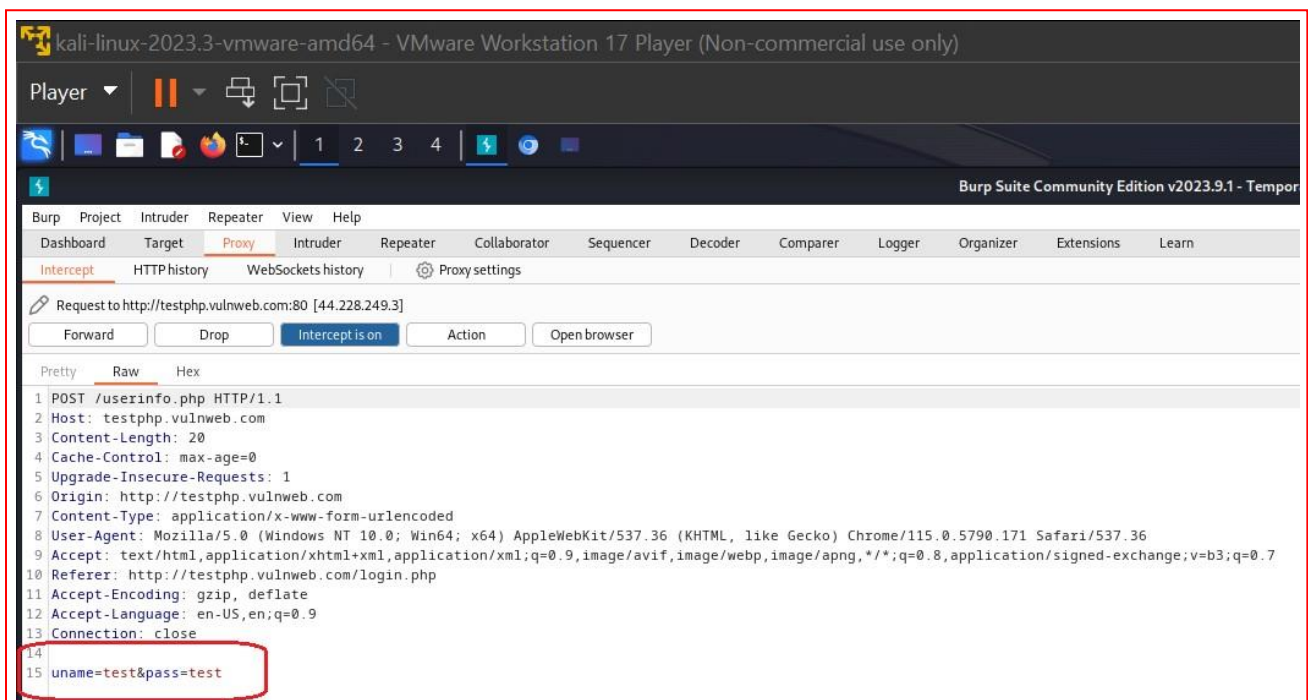Fig 4: open the web application with Burp Suite and enter the login credentials.

Fig 5: Whenever we capture the request in the burp suite you can able to view user entered credentials.

3.3 SQL Injection by injecting queries in the URL GET parameter

Reference No:	Risk Rating:
WEB_VUL_03	High
Tools Used:	
Browser	
Vulnerability Description:	
It was observed that the application had the list of artists contributed and just by implementing SQL queries into the GET Requests in the URL, severe information of the users could be fetched.	
Vulnerability Identified by / How It Was Discovered	
Manual analysis	
Vulnerable URLs / IP Address	
http://testphp.vulnweb.com/listproducts.php?cat=1	
Impacts / Consequences of not Fixing the Issu	
An adversary having knowledge about SQL could easily get into the database and can fetch juicy details of all the users present inside the database by injecting SQL queries in the URL GET parameter. The details include cc, email, name, phone, address etc.	
Suggested Mitigation	
It is recommended to implement below control for mitigating the SQLi: • Use Stored Procedure, Not Dynamic SQL • Use Object Relational Mapping (ORM) Framework • Least Privilege • Input Validation • Character Escaping • Use WAF (Web Application Firewall)	
References	
https://owasp.org/www-community/attacks/SQL_Injection https://logz.io/blog/defend-against-sql-injections/	

Proof of concept:
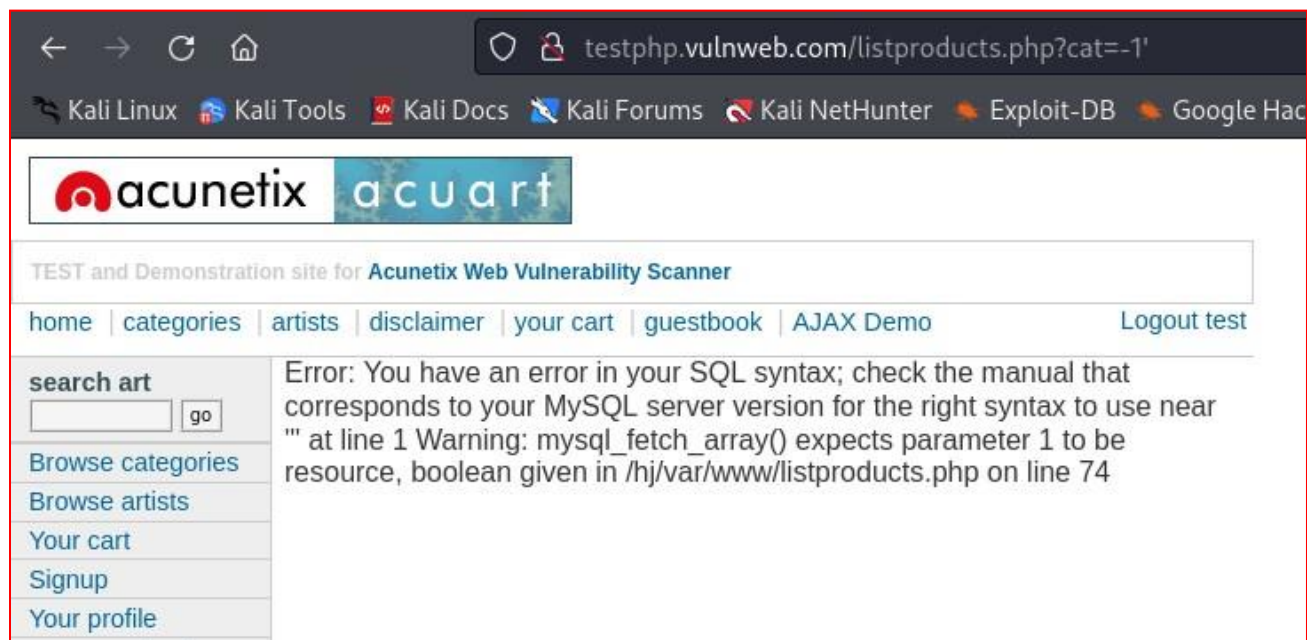
Fig 6: Error based SQL
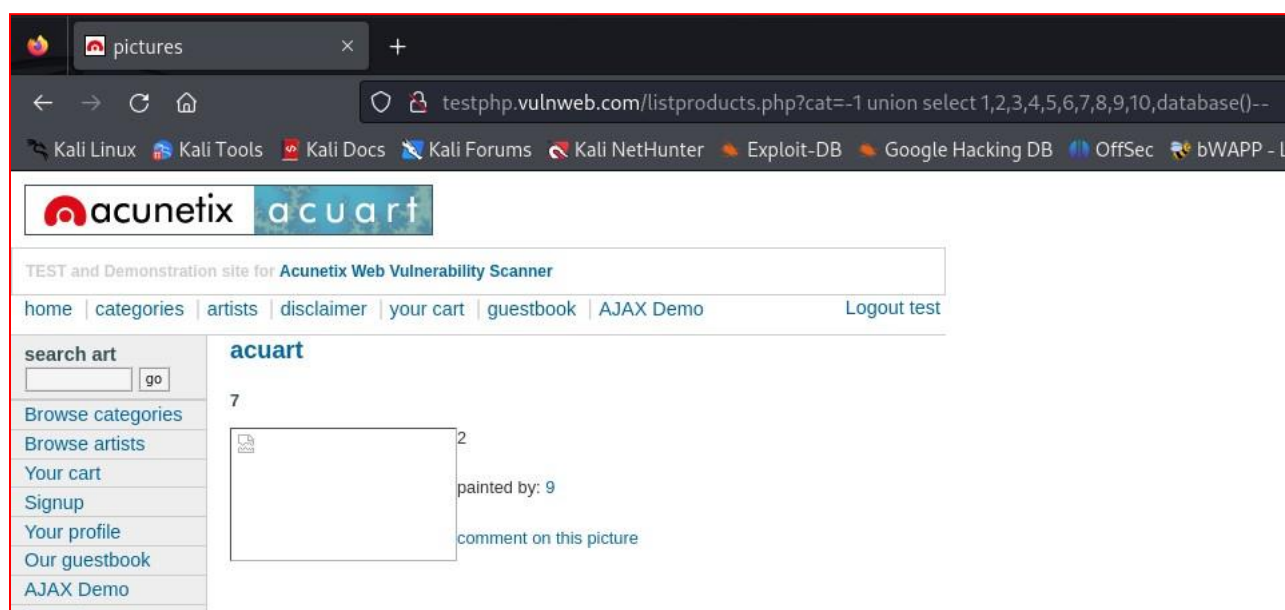
Fig 7: Union Based SQL Injection Showing Database
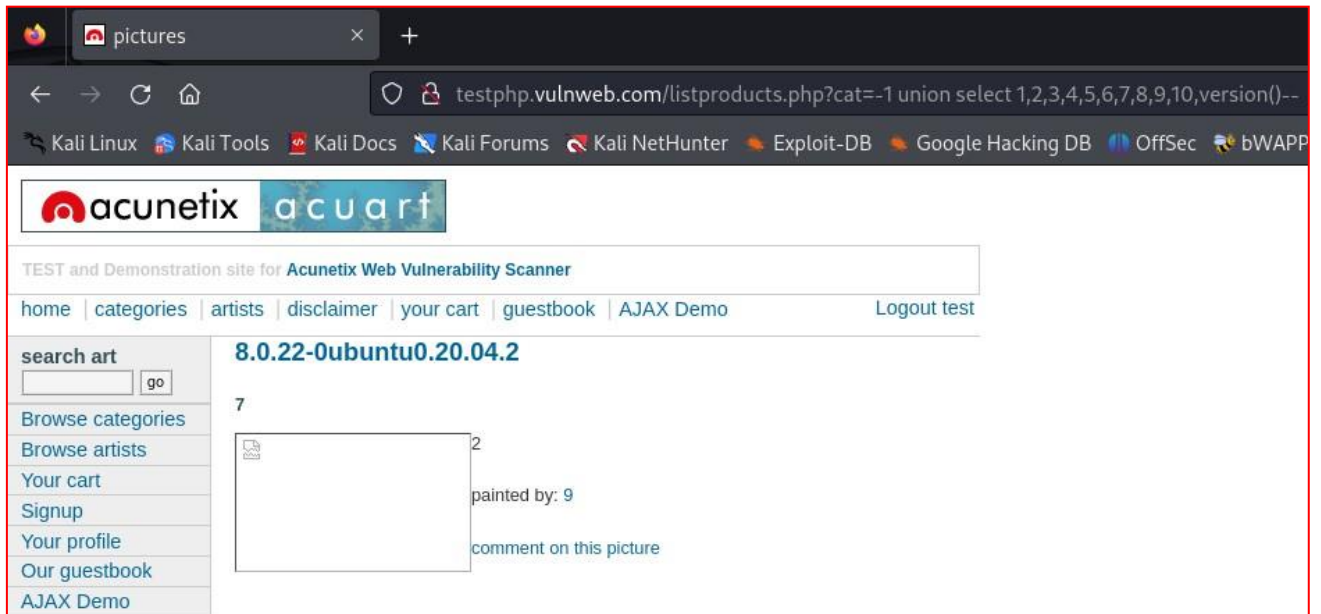
Fig 8: Union Based SQL Injection Showing Version

3.4 Server-Side Request Forgery

Reference No:	Risk Rating:
WEB_VUL_04	Medium

Tools Used:
Burp suite

Vulnerability Description:
Server-side request forgery is a web security vulnerability that allows an attacker tocause the server-side application to make requests to an unintended location. In a typical SSRF attack, the attacker might cause the server to make a connection to internal-only services within the organization's infrastructure. In other cases, they may beable to force the server to connect to arbitrary external systems. This could leak sensitive data, such as authorization credentials.

Vulnerability Identified by / How It Was Discovered
By changing the GET request in Burp Suite

Vulnerable URLs / IP Address
http://testphp.vulnweb.com/showimage.php?file=./pictures/6.jpg

Impacts / Consequences of not Fixing the Issue
A successful SSRF attack allows a hacker to manipulate the target web server into executing malicious actions or exposing sensitive information. This technique can causeserious damage to an organization. Targets of SSRF are- Sensitive Data Exposure Cross-Site Port Attack (XSPA) Denial of Service (DoS) Remote Code Execution (RCE)

Suggested Mitigation
From Application layer: Sanitize and validate all client-supplied input data Enforce the URL schema, port, and destination with a positive allow list Do not send raw responses to clients Disable HTTP redirections Be aware of the URL consistency to avoid attacks such as DNS rebinding and "time of check, time of use" (TOCTOU) race conditions. **From Network layer:** Segment remote resource access functionality in separate networks to reduce the impactof SSRF Enforce "deny by default" firewall policies or network access control rules to block all but essential intranet traffic.

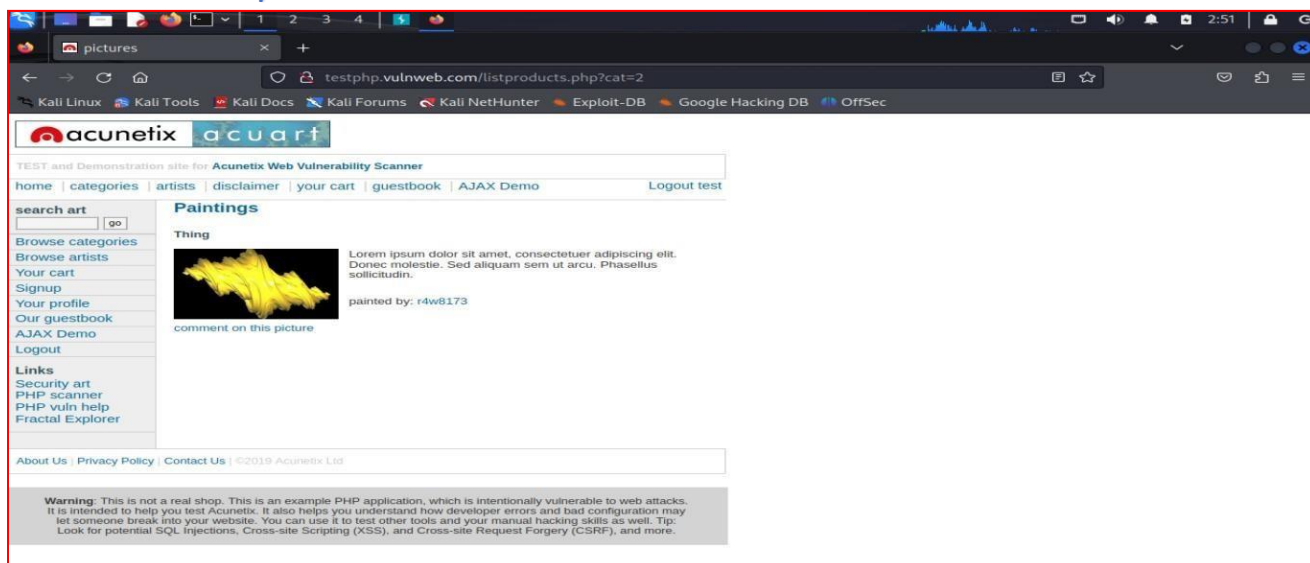| References |
|---|
| 1. Online version of the SSRF bible.
2. https://aws.amazon.com/blogs/security/defense-in-depth-open-firewalls-reverse-proxies-ssrf-vulnerabilities-ec2-instance-metadata-service/ |

Proof of concept

Fig 9: This is the original page which contains only one image under paintings section in categories tab.
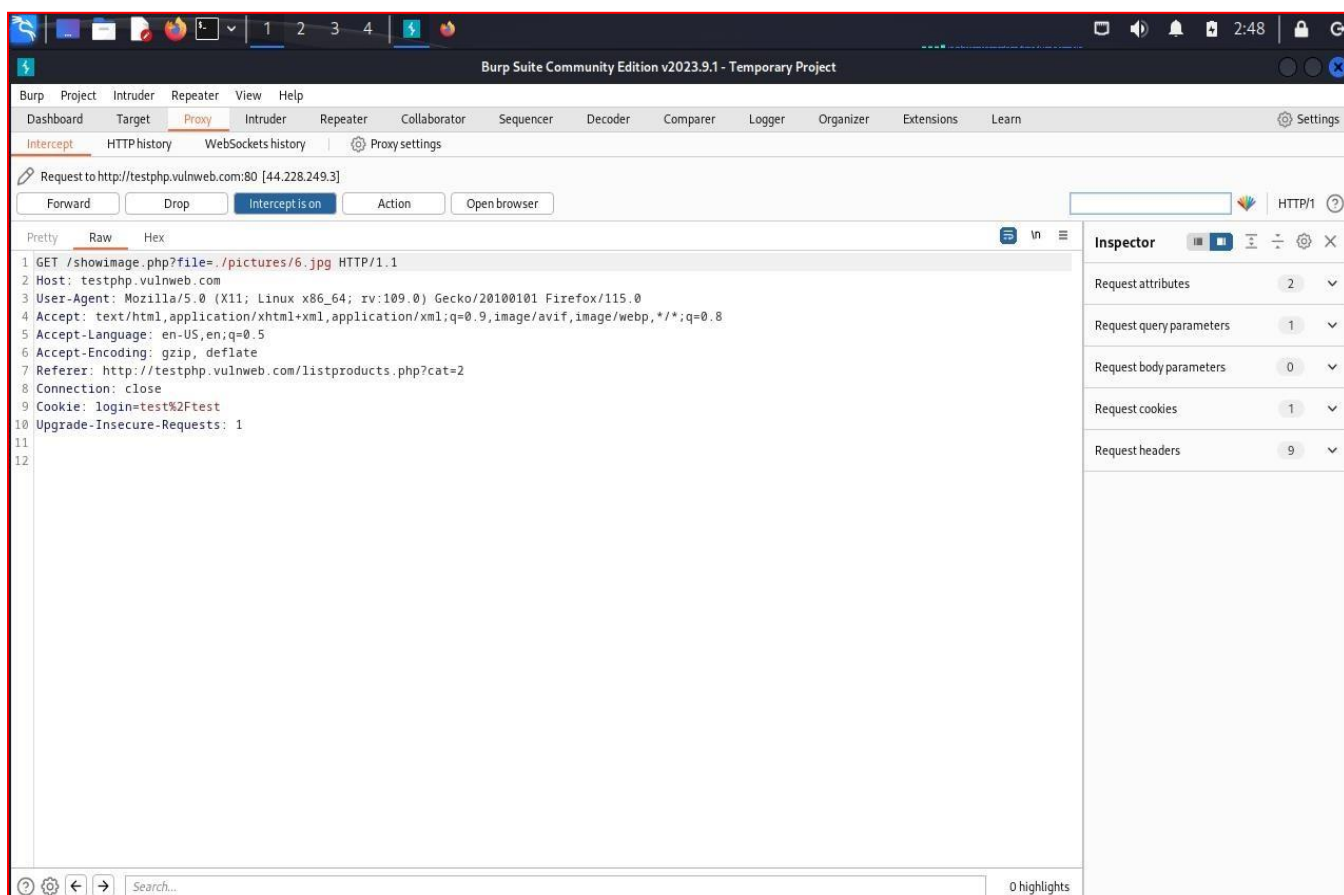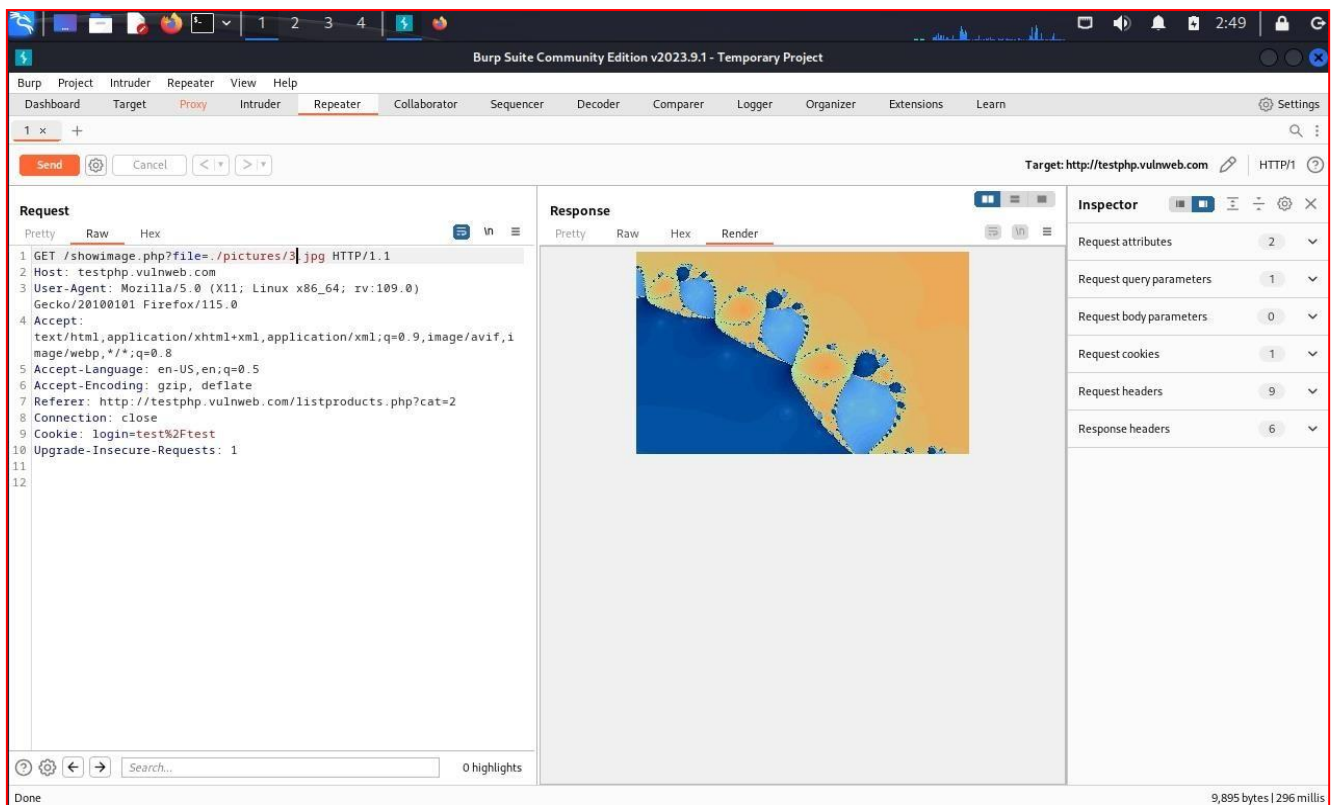

Fig 10: We can see the request in Burp Suite.

Fig 11: After modifying picture no. We can able to view images which are available internally but not on the client side. (Pictures/6 -> Pictures/3)

3.5 Reflected XSS in the application

Reference No:	Risk Rating:
WEB_VUL_05	Medium
Tools Used:	
Browser	
Vulnerability Description:	
It was observed that in the search bar instead of search query if we inject JavaScript codethen the JS code executes hence results into XSS.	
Vulnerability Identified by / How It Was Discovered	
Manual analysis	
Vulnerable URLs / IP Address	
http://testphp.vulnweb.com/	
Impacts / Consequences of not Fixing the Issu	
An adversary having knowledge of JavaScript will be able to steal the user's credentials,hijack user's account, exfiltrate sensitive data and can access the client's computer.	
Suggested Mitigation	
It is recommended to: • Filter input on arrival • Encode data on output • Use appropriate response headers • Use Content Security Policy (CSP) to reduce the severity of any existing XSS	
References	
[What is cross-site scripting (XSS) and how to prevent it? | Web Security Academy (portswigger.net)](#)	

Proof of concept:
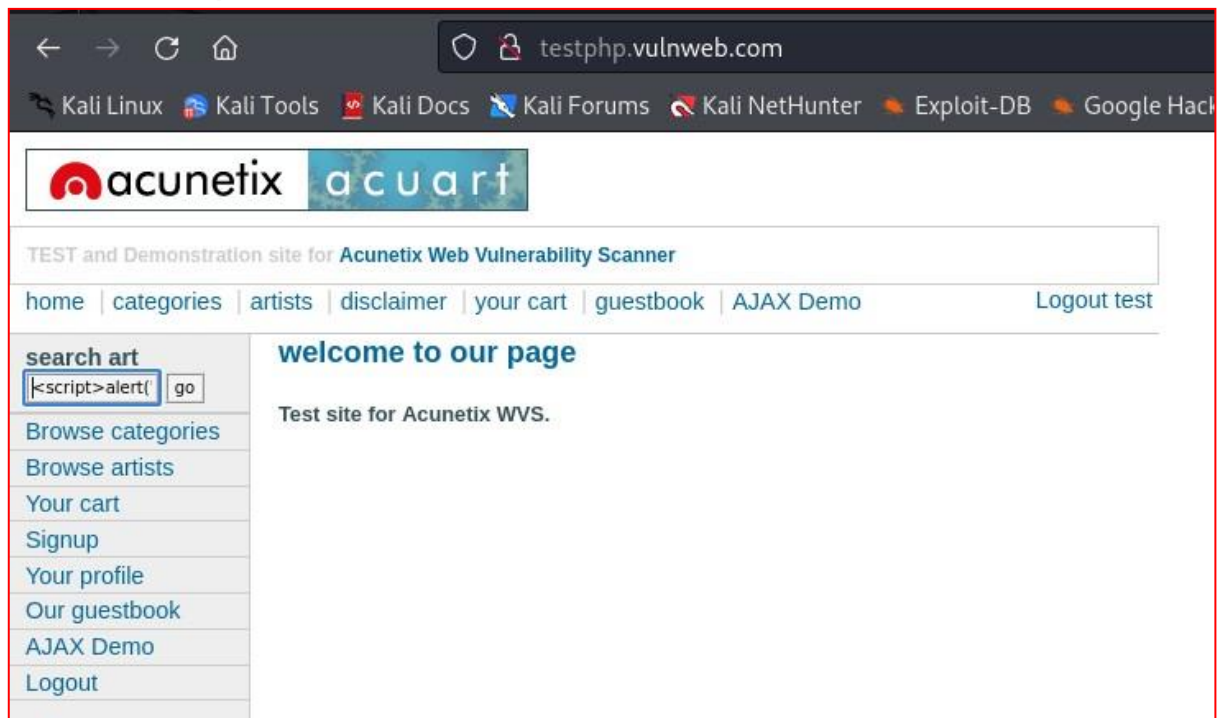
Fig 12: We have entered malicious script in the search box
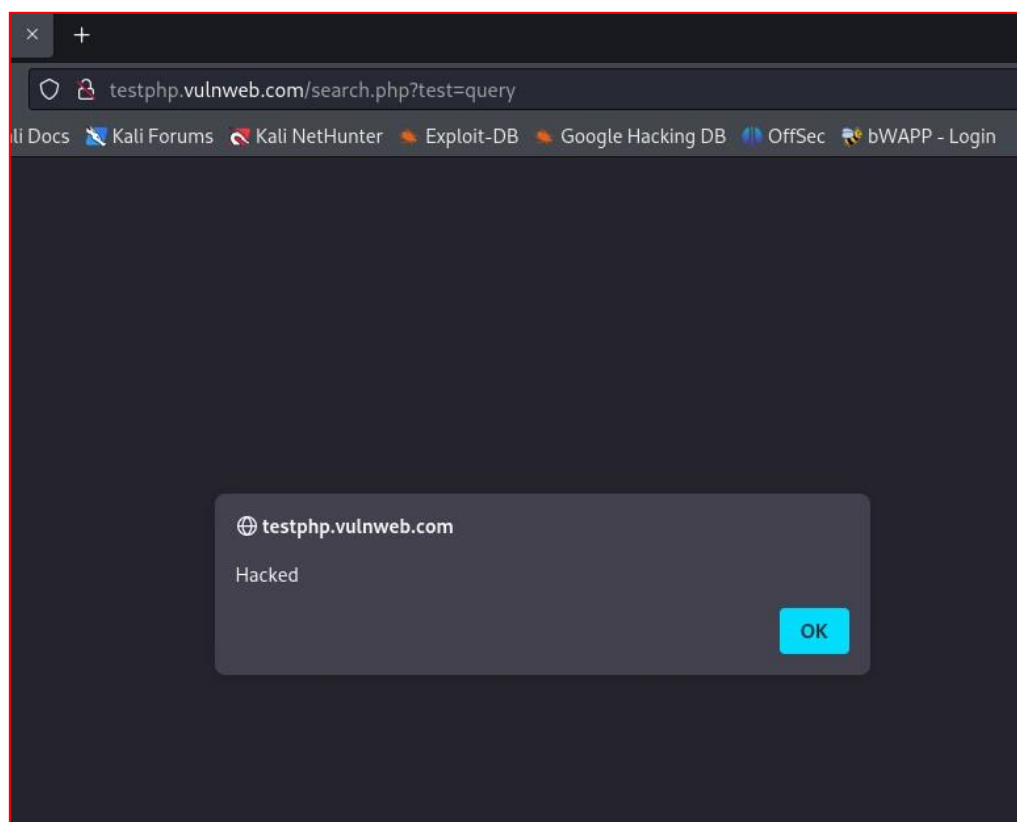
Fig 13: Whatever script we have entered it is reflected back

3.6 Stored XSS in the application

Reference No:	Risk Rating:
WEB_VUL_06	High

Tools Used:
Browser

Vulnerability Description:
It was observed that in your profile area instead of normal input if we execute JS code, thenit gets stored in the server and hence it results into Stored XSS.

Vulnerability Identified by / How It Was Discovered
Manual analysis

Vulnerable URLs / IP Address
http://testphp.vulnweb.com/userinfo.php

Impacts / Consequences of not Fixing the Issu
An adversary having knowledge of JavaScript will be able to steal the user's credentials, hijack user's account, exfiltrate sensitive data, can access the client's computer and even can redirect into other pages created by the adversary. And the impact will be faced by all users visiting the compromised page.

Suggested Mitigation
It is recommended to: • Filter input on arrival • Encode data on output • Use appropriate response headers • Use Content Security Policy (CSP) to reduce the severity of any existing XSS vulnerabilities • Using an Auto-Escaping Template System • Using HTML Encoding

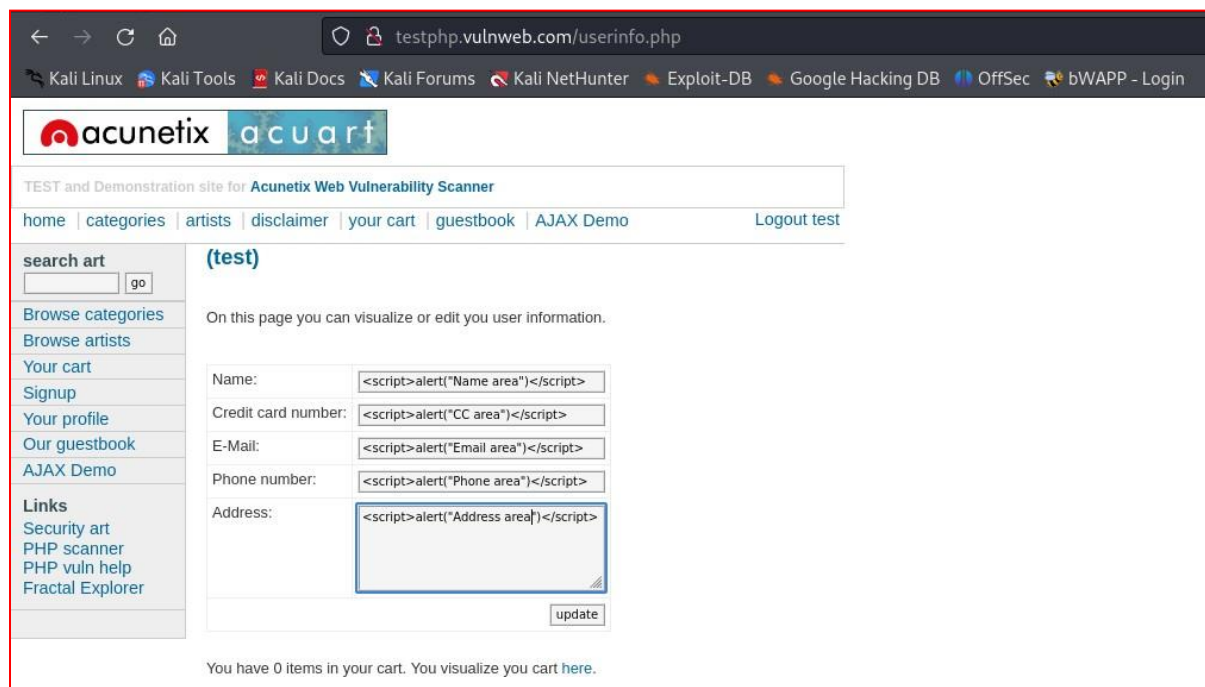| References |
|---|
| What is cross-site scripting (XSS) and how to prevent it? \| Web Security Academy (portswigger.net)
Application Security Management \| Datadog (datadoghq.com) |

Proof of concept:

Fig14: Type the JavaScript code to all the field as any of them could be vulnerable to stored XSS and then click on the Update button
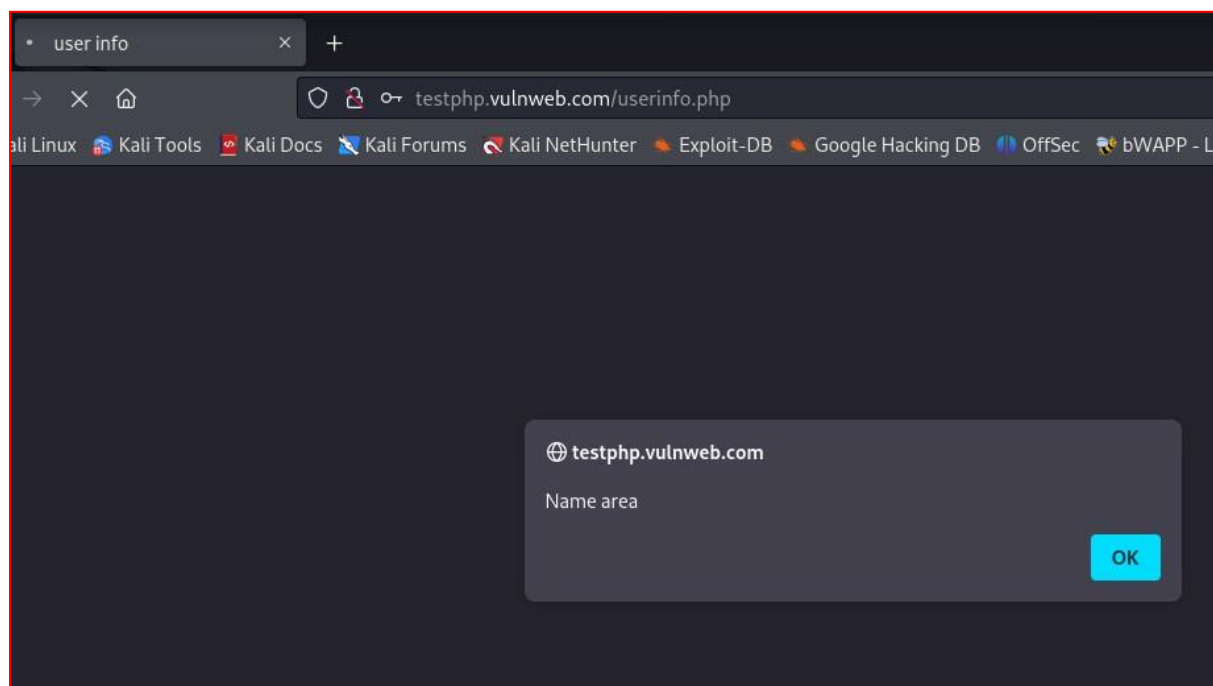

Fig 15: Hence the code gets executed and it's permanently stored in the server. Also it is found that the name field is vulnerable to stored XSS.

3.7 Clickjacking in Our Guestbook Page.

Reference No:	Risk Rating:
WEB_VUL_07	High
Tools Used:	
Browser	
Vulnerability Description:	

If a page fails to set an appropriate X-Frame-Options or Content-Security-Policy HTTPheader, it might be possible for a page controlled by an attacker to load it within an iframe. This may enable a clickjacking attack, in which the attacker's page overlays thetarget application's interface with a different interface provided by the attacker. By inducing victim users to perform actions such as mouse clicks and keystrokes, the attackercan cause them to unwittingly carry out actions within the application that is being targeted. This technique allows the attacker to circumvent defenses against cross-site request forgery, and may result in unauthorized actions.

Vulnerability Identified by / How It Was Discovered

By inspecting headers of a page

Vulnerable URLs / IP Address

http://testphp.vulnweb.com

Impacts / Consequences of not Fixing the Issue

Main impacts of clickjacking:

1. Unauthorized actions

Clickjacking allows attackers to trick users into unknowingly performing actions they didn't intend to. This could include making unauthorized purchases, sharing sensitive information, granting permissions to malicious applications, or interacting with hidden elements that compromise security.

2. Data theft

Clickjacking attacks can lead to the theft of sensitive user data.

For example, attackers can deceive users into clicking on hidden elements that trigger the download of malware or prompt the user to enter confidential information.

3. Financial losses

If clickjacking leads to unauthorized actions, users may suffer financial losses due to fraudulent purchases or transactions made without their knowledge or consent.

Suggested Mitigation

Client-side methods – the most common is called Frame Busting. Client-side methods canbe effective in some cases, but are considered not to be a best practice, because they can be easily bypassed.

Server-side methods – the most common is X-Frame-Options. Server-side methods are recommended by security experts as an effective way to defend against clickjacking.

The X-Frame-Options response header is passed as part of the HTTP response of a web page, indicating whether a browser should be allowed to render a page inside a <FRAME>or <IFRAME> tag.

There are three values allowed for the X-Frame-Options header:

DENY – does not allow any domain to display this page within a frame

SAMEORIGIN – allows the current page to be displayed in a frame on another page, butonly within the current domain

ALLOW-FROM URI – allows the current page to be displayed in a frame, but only in aspecific URI – for example *www.example.com/frame-page.*

References
CWE-1021: Improper Restriction of Rendered UI Layers or Frames
CWE-693: Protection Mechanism Failure

Proof of concept:

In http://testphp.vulnweb.com in response headers X-frame is not used. Therefore, its vulnerable to clickjacking
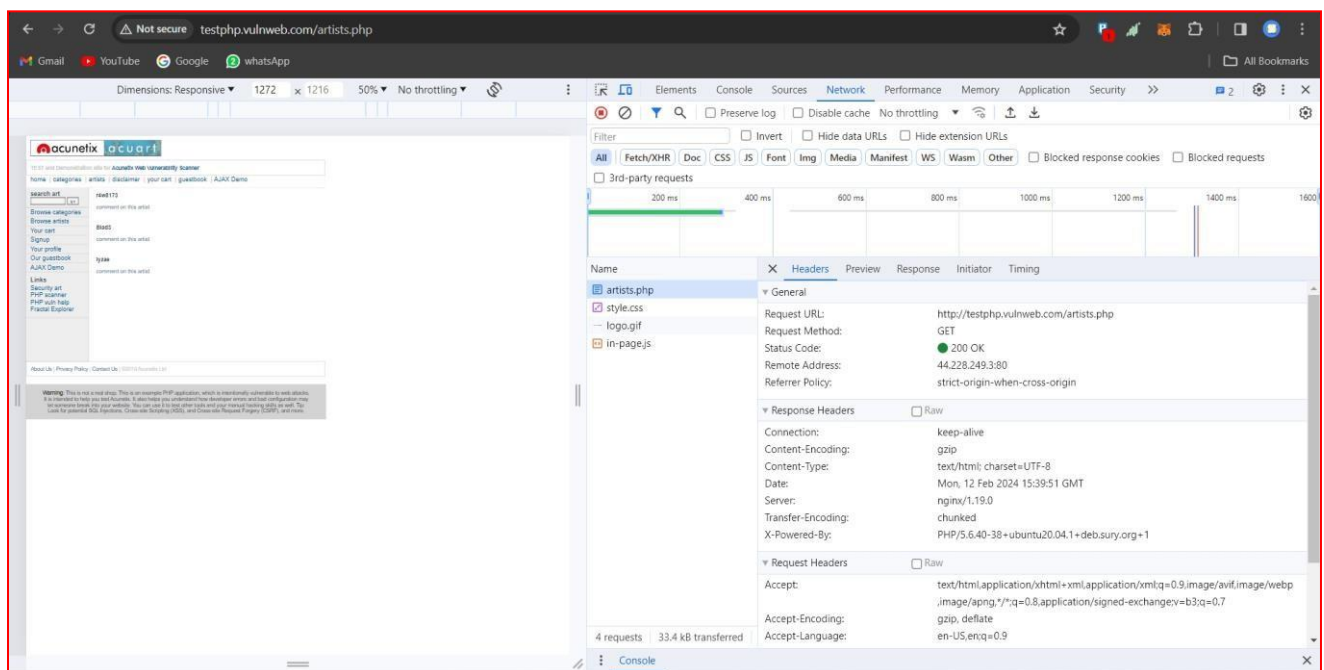
Fig no 16 : Is the example of secure website: http://google.com where we can clearly see use of X-Frame as allow from specific uri only.
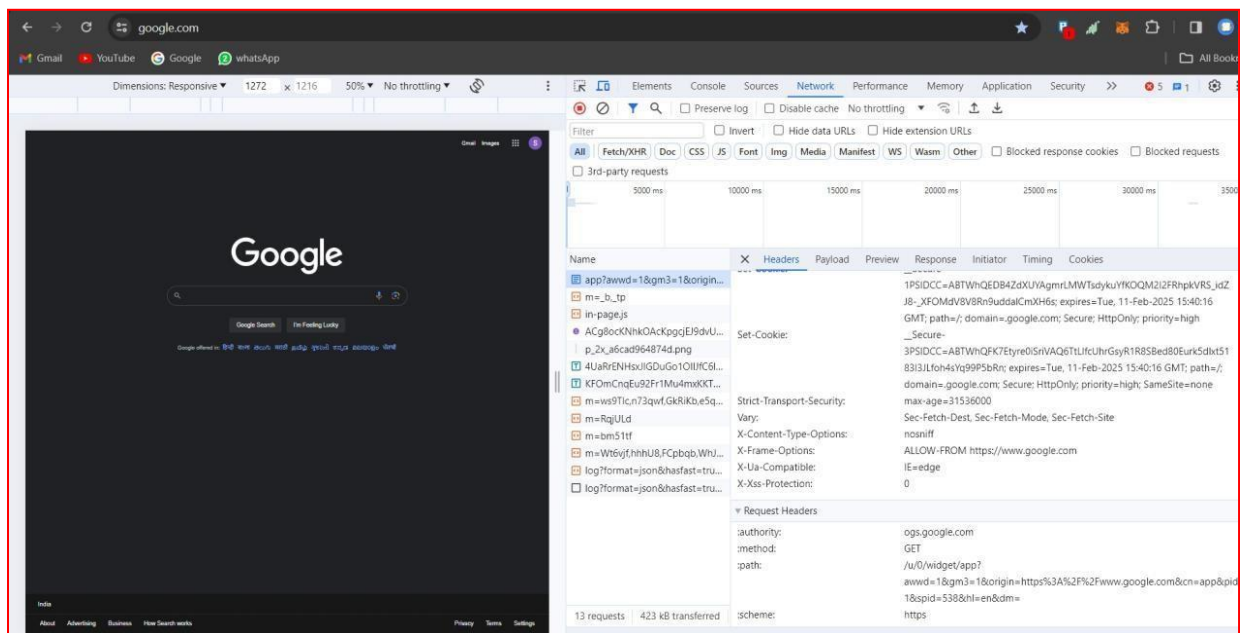
Fig no 17

3.8 Directory Index disclosure.

Reference No:	Risk Rating:
WEB_VUL_08	Medium

Tools Used:
Browser

Vulnerability Description:
It has been identified that the system is susceptible to Directory Index disclosure, whichcould enable an unauthorized user to access sensitive information such as system configuration files, source code, and other critical data stored in the web server's directories.

Vulnerability Identified by / How It Was Discovered
Manual analysis

Vulnerable URLs / IP Address
http://testphp.vulnweb.com/admin/http://testphp.vulnweb.com/CVS/ http://testphp.vulnweb.com/pictures/

Impacts / Consequences of not Fixing the Issu
A directory listing is inappropriately exposed, yielding potentially sensitive information to attackers. A directory listing provides an attacker with the complete index of all the resources located inside of the directory. The specific risks and consequences varydepending on which files are listed and accessible.

Suggested Mitigation
1- Disable directory indexing: Disable directory indexing on the server to prevent sensitive information from being exposed. This can be done by modifying the server configurationfiles or using web server modules or plugins. 2- Implement access controls: Ensure that sensitive directories and files are only accessible to authorized personnel who require access to perform their job duties. Userole-based access controls to limit access to sensitive files and data.

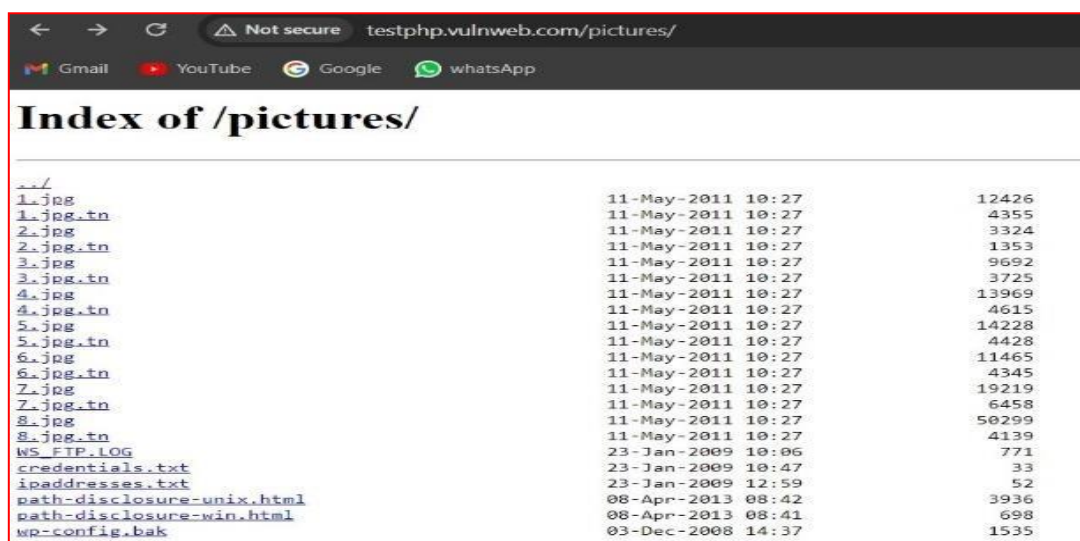| References |
|---|
| https://github.com/v0re/dirb/blob/master/wordlists/common.txt |

Proof of concept:

Fig 18: Index of Admin

Fig 19: Index of CVS

Fig 20: Index of Picture

4. Conclusion

This pen testing report serves as a comprehensive repository of insights garnered from the security assessment conducted on the HOME OF ACUNETIX ART WEB APPLICATION platform. The intention is to facilitate a holistic understanding of web application vulnerabilities, encourage hands-on learning, and equip professionals with the knowledge to safeguard applications against potential threats. Through this report, we endeavor to contribute to the collective effort in fortifying web applications' security, ensuring a safer digital environment for users and organizations alike.