IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 12, Issue 10, October 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.625

© 2024 IJIRCCE | Volume 12, Issue 10, October 2024| DOI: 10.15680/IJIRCCE.2024.1210013

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Shields and Swords: Navigating Vulnerability Assessment and Penetration Testing

Dhruv Mitesh Mori[1], Kiran R Dodiya[2], Akash khunt[3], Divya Patel[4]

M. Sc Cyber Security, NSIT-IFSCS (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India [1]

Assistant Professor & Program Co-ordinator of DFIS (Cyber Security & Digital Forensics) NSIT-IFSCS (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India [2]

Assistant Professor & Program Co-ordinator of Cyber Security (Cyber Security & Digital Forensics) NSIT-IFSCS (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India [3]

Assistant Professor & Course Co-ordinator of DFIS (Cyber Security & Digital Forensics) NSIT-IFSCS (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India [4]

ABSTRACT: Vulnerability Assessment and Penetration Testing (VAPT) are essential methodologies used in identifying, testing and remedying weaknesses in security systems and networks. In the present study, we attempt to investigate the effectiveness and methodology of VAPT, offering an all-around view of its role in modern cybersecurity trends. Vulnerability Assessment is the evaluation that focuses on the identification and catalog of possible security weaknesses in a system, whereas Penetration Testing is to simulate real-world attacks in exploiting those vulnerabilities to define the real effect and feasibility of such exploitation. This dual method ensures in-depth understanding of potential security risks as well as the effectiveness of existing safeguards. This research explains the critical methodologies involved in VAPT which include some of the automated scanning tools to identify vulnerabilities and some of the manual testing techniques carried out to provide an extensive level of detail. Automation scanning tools provide a general overview of all possible vulnerabilities, but the manual techniques involve the use of social engineering and custom exploit development.

KEYWORDS: Vulnerability Assessment, Penetration Testing, Identification, Detection, VAPT Tools.

I. INTRODUCTION

Vulnerability Assessment and Penetration Testing is a process of detecting vulnerabilities from the Web application, Authentication Vulnerabilities, Configuration Weakness Vulnerabilities and Mobile Application Vulnerabilites. Vulnerability Assessment involves systematically scanning and identifying systems for vulnerabilities misconfigurations and providing a detailed report on real-world attacks to exploit vulnerabilities found from the system or application. It will be helpful for the organization to protect their system from the attackers and defend to resolve the actual breaches. Penetration testing is the step after vulnerability assessment. Penetration Testing is a pivotal cybersecurity practice aimed at relating and focusing vulnerabilities within an association's systems and networks. If you're curious about how companies keep their digital information secure from hackers. Penetration testing frequently called "pen testing" or "ethical hacking" is a system used to find vulnerability in a computer system, network, or web operation. By misleading real- world cyberattacks, pen testing helps associations uncover security before attackers can exploit them. This visionary approach not only enhances the overall security posture but also ensures compliance with regulations, laws and norms. Securing sensitive data and maintaining robust security defences. The thing is to discover these vulnerabilities before the bad guys do, so they can be fixed to help any unauthorized access or data breaches. This process is essential for guarding sensitive data and secure their organizations from the attackers[1], [2], [3], [4].

1.1 Types of Vulnerability Assessment and Penetration Testing:

1. Network Penetration testing: -The process of conducting attacks on a network to discover any implicit vulnerabilities which can be exploited by hackers to harm your systems and database. Adopting a phased approach, penetration testing

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

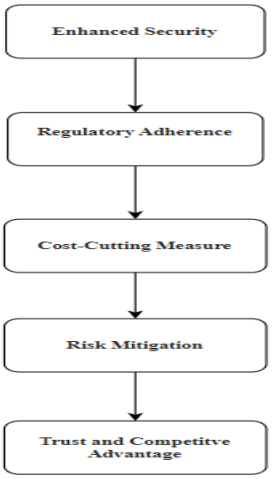
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

experts map the network architecture, identify systems and services, and then leverage various automated tools and manual techniques to gain unauthorized access, mimicking real-world attacker behaviour
[5], [6].

2. Web Application Testing: - Web application testing simulates attacks against your web application to help you identify security breaches and vulnerabilities so they can be exploited by the association. Attackers attempt to inject malicious code (e.g., SQL injection, XSS), manipulate sessions, and exploit logic flaws so web application testing helps you to identify, prioritize, and mitigate risks before attackers exploit them[7], [8].

3. Mobile Application Testing: - Mobile Application Penetration Testing is process of reviewing the safety of a mobile app by exploiting real-world attacks. It identifies vulnerabilities and implicit entry points that attackers could exploit and harm the mobile device. Often attackers focus on areas such as insecure data storage (cleartext passwords), intercept sensitive data in transit, exploit business logic vulnerabilities, and flaws in inter-app communication or API integrations and to identify CVEs of card holders[9], [10].4.API Penetration Testing: - API Penetration Testing used for real-world attacks by precisely crafting requests to uncover vulnerabilities such as broken authentication, Injection flaws and authorization weakness. Pen testers may also use automated tools like postman to automate attacks, manipulate data packets and identifying exploitable business logic vulnerabilities[11], [12], [13].

II. BENEFITS OF PERFORMING VAPT



Flowchart 1Benefits of performing VAPT

III. WHERE VAPT IS USED

1. Cybersecurity: Organizations utilize VAPT to identify and address vulnerabilities in their IT infrastructure, including networks, applications, and systems.
2. Compliance: Many industries require regular VAPT as part of regulatory compliance (e.g., PCI-DSS, HIPAA, GDPR).
3. Risk Management: Companies assess their security posture to understand risks and prioritize remediation efforts.
4. Product Development: Developers use VAPT to ensure security is integrated into software products before deployment.
5. Security Training: VAPT results can inform training programs for security teams, highlighting real-world threats and vulnerabilities.
6. Incident Response: Post-incident, VAPT helps organizations learn from breaches and strengthen defences.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. METHODOLOGY

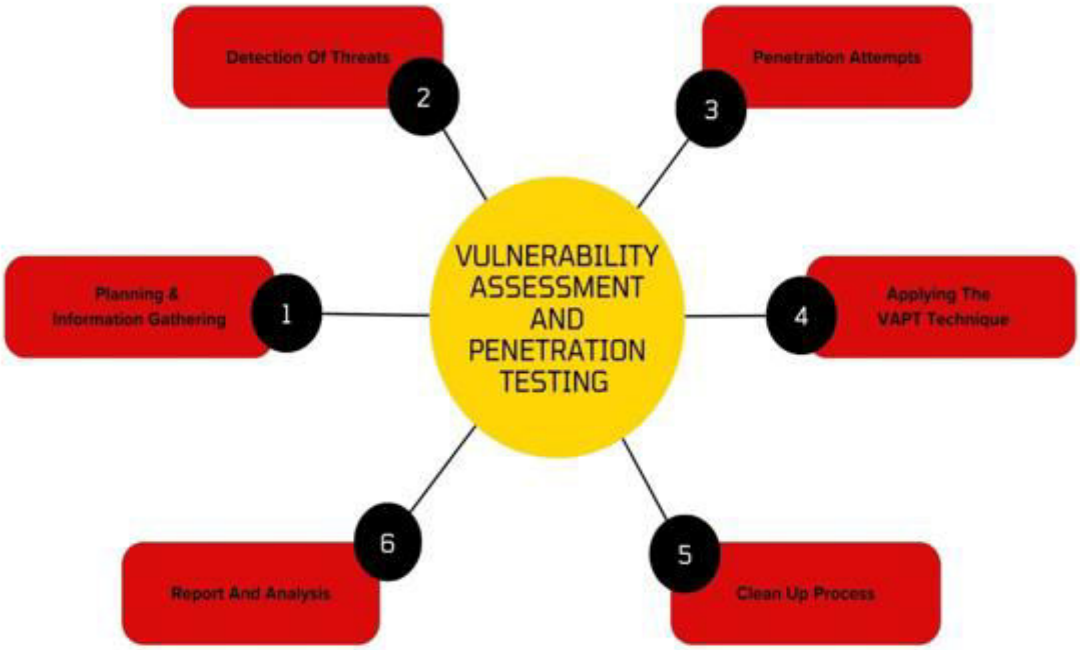


Figure 1Methodology of VAPT

V. RESULT &DISCUSSION:

Sr. No. Title: -01(SQL Injection)	
Description	
SQL injection is an attack vector that uses malicious SQL code or script for database exploitation to access information that was not proposed to be displayed. That data are sensitive it should not be exploited[14].	
Severity	**CRITICAL**
Impact	
Hackers can bypass security measures of applications and use SQL queries to modify, add, update, or delete records from database.	
Tools Used	SQL MAP
Proof of Vulnerability	

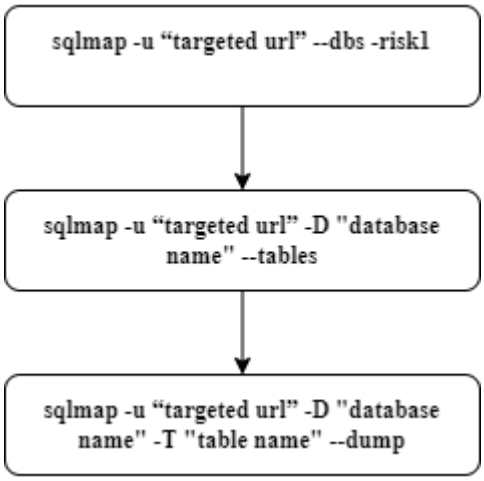
Table 1 SQL Injection

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

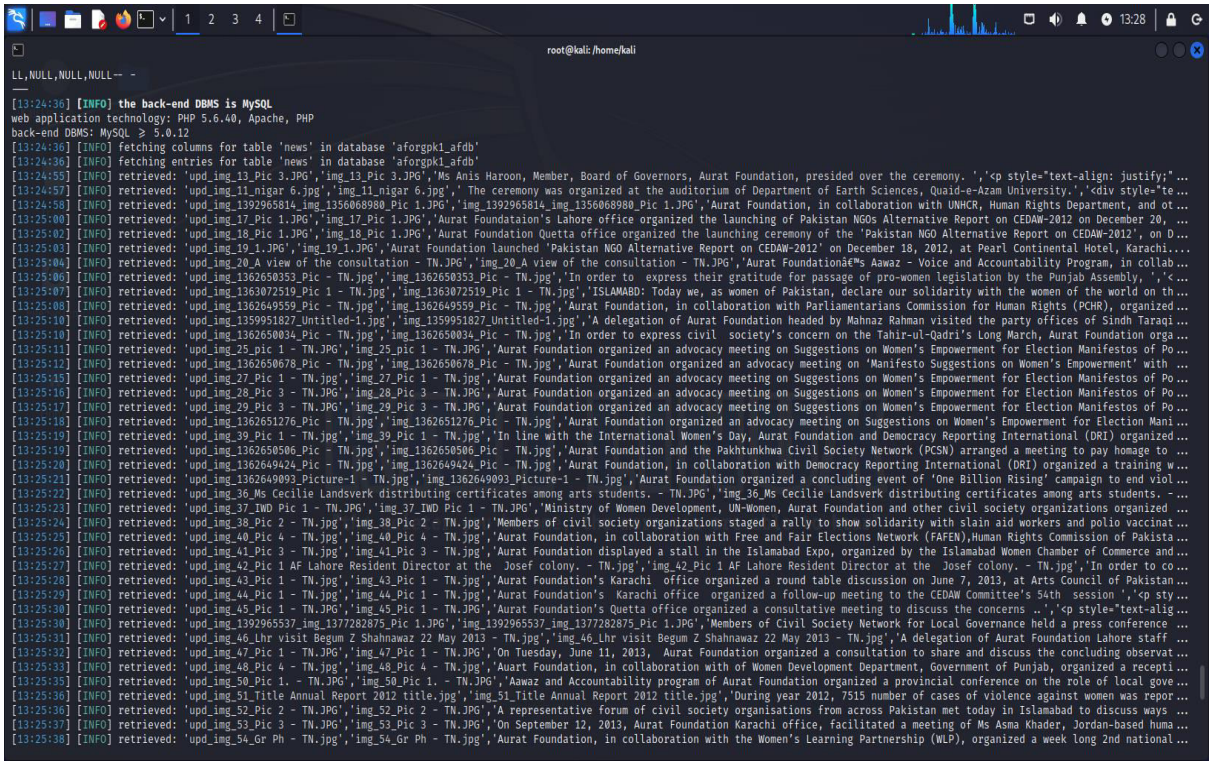
(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

In this we have used sqlmap tool this tool helps to expolit the database where you can get the data from the database. As shown below first we have found the database name and then we are finding table name from that database so we can access that column and then dump the file whole data will be visible.Step by step process of sqlmap is shown in below given flowchart.



Flowchart 2 SQL Injection

This is the proof of database files where we can see the data .



Picture 1 SQL Injection

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

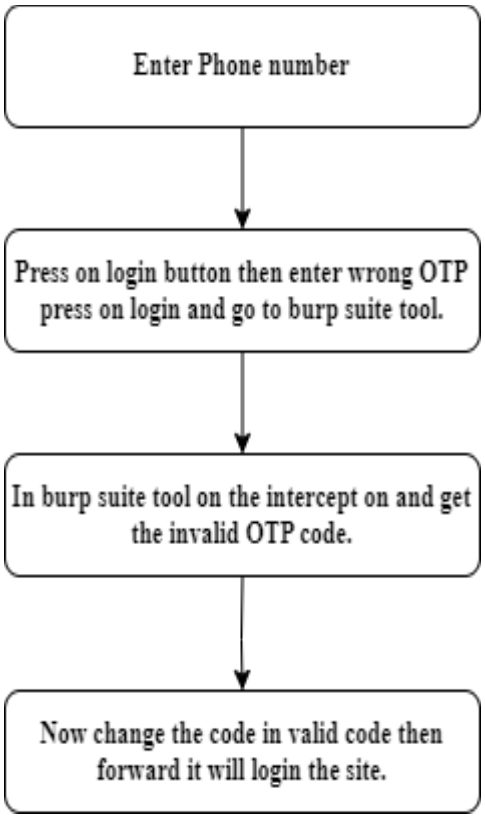
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Sr. No. Title: -02 (OTP BYPASS)	
Description	
An OTP bypass occurs when an attacker finds a way to compromise the authentication processwithout having the legitimate OTP[15].	
Severity	**High**
Impact	
By getting unauthorized identity to access their accounts, such as bank accounts or credit cards. The hacker can make misuse of your information and blackmail to the user.	
Tools Used	Burp suite
Proof of Vulnerability	

Table 1 OTP Bypass

Enter the phone number and then click on get OTP then you have to enter wrong OTP click on login button then go to burp suite tool and, on the intercept, then will get invalid code you have to change it in valid code then forward that code it will be automatically login to the site.



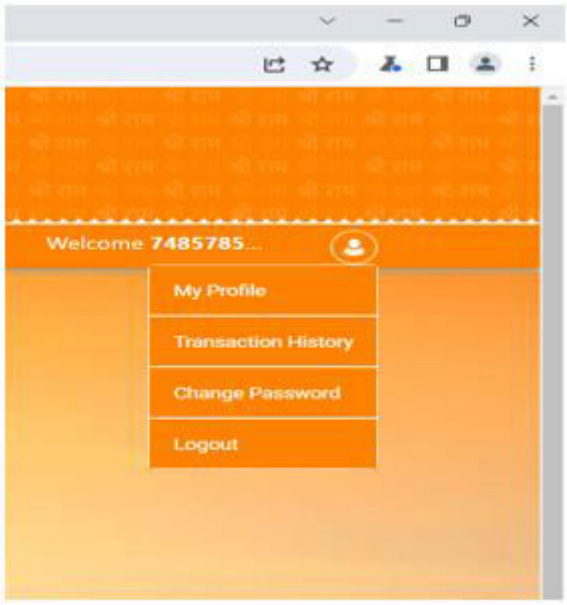
Flowchart 2 OTP Bypass

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

This is the proof of login has been bypassed and it is authenticated to the web page.



Picture 2 OTP BYPASS Login

Enter the email address and then click on get OTP then you have to enter wrong OTP click on login button then go to burp suite tool and, on the intercept, then will get invalid code you have to change it in valid code then forward that code it will be automatically login to the site.

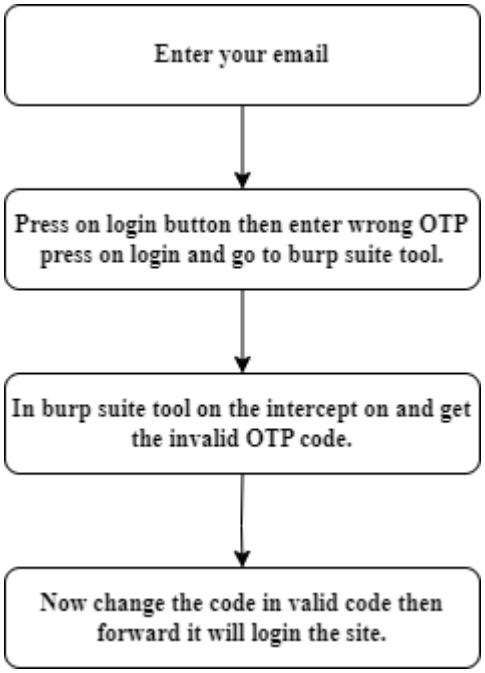
Sr. No. Title: -03 (Email Bypass)	
Description	
In Email bypass there can be vulnerability found that OTP can be bypass and there can be unauthorized login and gathering information to harm the user's private data.[16]	
Severity	**High**
Impact	
Hackers use to get unauthorized login and collect the important information attacker use to get success in gathering access and information uses privileges of the account.	
Tools Used	Burp Suite
Proof of Vulnerability	

Table 3 Email Bypass

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

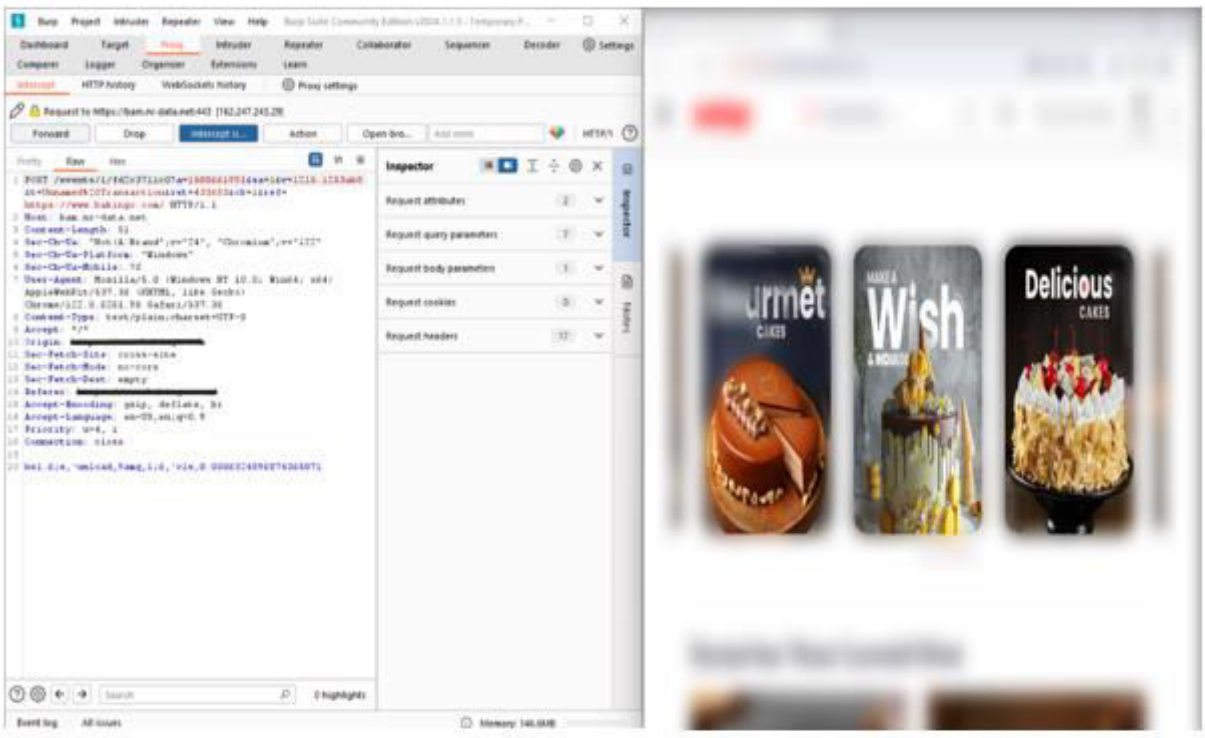
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Flowchart 3 Email Bypass

Below there is the proof of login of the user in the website.



Picture 3 Email Bypass Login

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

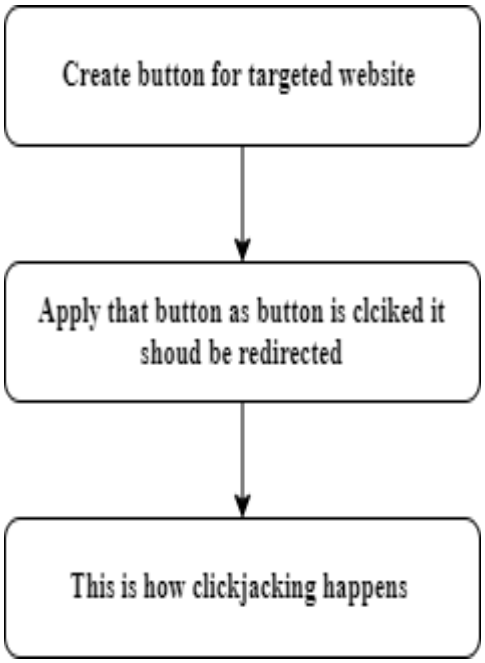
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Sr. No. Title: -04 (Click Jacking)	
Description	
It can be lied to that the user would share or like links on Facebook, click on Google AdSense advertisements for pay-per-click revenue generation, make users follow someone on Twitter or Facebook, download and run malware allowing a remote attacker to take control of other computers, get likes on the Facebook fan page or +1 on Google Plus[17].	
Severity	**High**
Impact	
Clickjacking is a vulnerability through which users are tricked to click some buttons or UI elements of the parent page, but they are clicking something in the vulnerable web application, because that is being hidden behind the UI of the parent page.	
Proof of Vulnerability	

Table 4 Click Jacking

In this clickjacking we took website of (A) through that we will procced on website (B). We are using <iframe> tag and we will put targeted website there and we will keep a button on website (A) which will be redirecting to website (B). There is code in button which is given below.



Flowchart 4 Click Jacking

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

```
<!DOCTYPE html>
<html>
<head>
    <style type="text/css">
        #prep {
            position: absolute;
            width: 100%;
            height: 300px;
            z-index: 2;
            text-align: center;
        }
        .btn {
            width: 20%;
            height: 40px;
            opacity: 1;
        }
    </style>
</head>
<body>
    <center>
        <div id="prep">
            <br><br><br>

            <button class="btn"><a href=                                    ></a></button>
        </div>
        <iframe id="target" src=                              width="500" height="500"></iframe>
    </center>
</body>
</html>
```

Picture 2 Click Jacking Script

Sr. No. Title: -05 (Clear Text PasswordSubmission)	
Description	
These types of attacks are commonly referred to as "Host header injection" attacks. The header value is also expected to be involved in many communication exchanges between different systems of the infrastructure.[18]	
Severity	**High**
Impact	
There are some web pages transmit passwords over unencrypted connections, making them vulnerable.	
Tools Used	Burp Suite
Proof of Vulnerability	

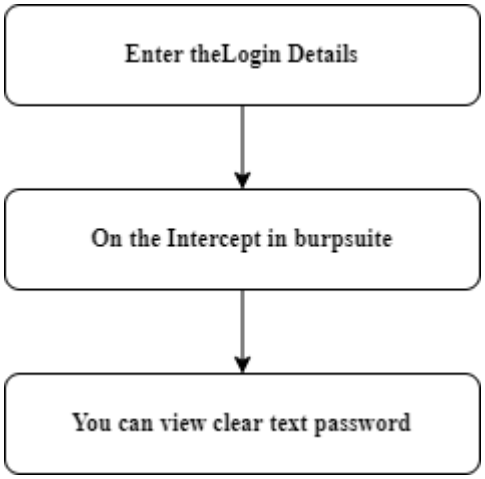
Table 5 Clear Text Password

Enter the details on the site and use burp suite tool. As we on intercept then we will get the code in that we can the ID and password this should not be happened . Any person can see your details and missuse your account privacy.

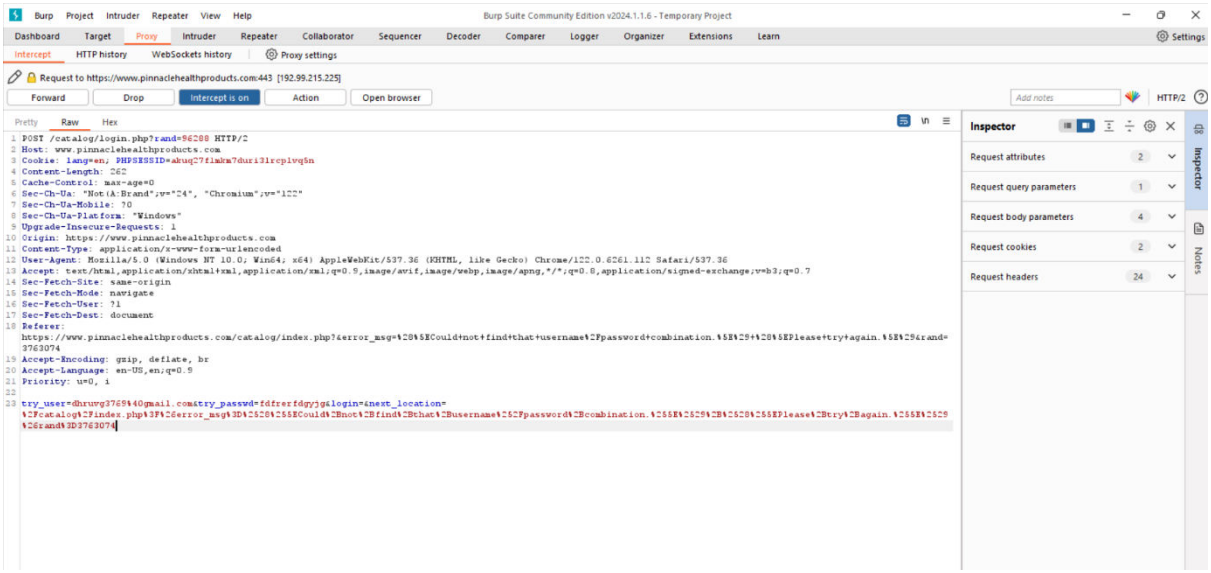
www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Flowchart 5 Clear Text Password



Picture 3 Clear Text Password

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

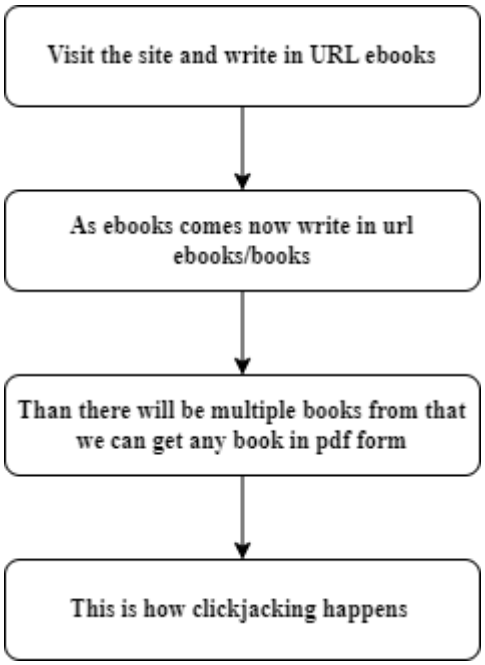
International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Title : -06 (Directory Traversal)	
Description	
Directory traversal is a type of HTTP exploit in which hacker exploit web pages on a server to exploit data of directory other than root directory and that can be viewed by the user.[19]	
Severity	**Medium**
Impact	
Access to sensitive information.	
Tools Used	-
CWE	**OWASP Top 10**
-	01
Proof of Vulnerability	

Table 6 Directory Traversal

Here is the website in that we have found eBooks from directory. Now write in URL ebooks then it will show you index of ebooks. After going to the books Directory and open parent directory. After going to the open Directory and there are many ebooks are shown there and we have selected the Crude oil exploration in the world.pdf.

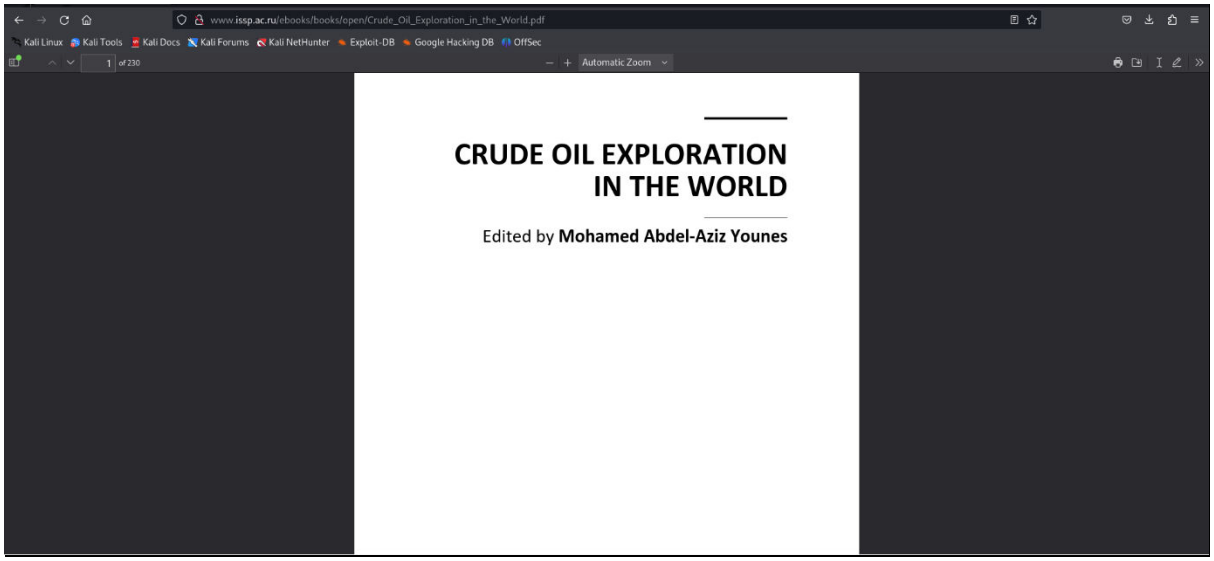


Flowchart 6 Directory Traversal

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Picture 4 Directory Traversal

Sr.No. Title: -07 (HTML INJECTION)	
Description	
There is a security vulnerability that allows hacker to inject HTML script and exploit web pages or application that are viewed by other users[20].	
Severity	**Low**
Impact	
There can be exploit in web pages by injecting HTML code in web pages and allow an attacker to modify the page.	
Proof of Vulnerability	

Table 7 HTML Injection

Enter the login details on the site and enter but as you have not registered you will get the error message in that go to URL and change error message and write in <h1> tag and press enter the message will be displayed in the dialog box.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Flowchart 7 HTML Injection

Picture 5 HTML Injection

VI. CONCLUSION

In this paper, we elaborated on the applications of Vulnerability Assessment and Penetration Testing. We articulated the necessity of VAPT being made mandatory for all forms of cyberspace. We detailed every stage of the VAPT process. This paper covers the definition of Vulnerability Assessment and Penetration Testing, and its practical application as a technology. This paper should consider the growing importance of VAPT. This paper will be useful for the future researchers in VAPT process, tools, and techniques. It will aid in the creation of novel instruments and methodologies for VAPT. Postponable VAPT testing can curb the incidence of cyber-warfare and reinforce the security of the system.

VII. FUTURE SCOPE

Increased popularity of smart phone has increased the use of mobile application or increased popularity of applications have increased the use of smart phone!! Whateverreason is, but one thing is very clear that Mobile applications are as popular as mobiles. Due to this hard-hitting competition among mobile application developers lead them todevelop an application which serves a different purpose of the users and make their daily task easy. But developers overlook a complete software development life cycle and skip or allot less time for testing an application as they want to fill their pockets with bucks by launching new applications rapidly in the market.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.625| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

REFERENCES

[1] "What is VAPT? Audit, Types and Process." Accessed: Oct. 02, 2024. [Online]. Available: https://www.getastra.com/blog/security-audit/what-is-vapt/
[2] "What is VAPT Testing? Importance, Types and Methodology." Accessed: Oct. 09, 2024. [Online]. Available: https://qualysec.com/what-is-vapt-testing-its-methodology-importance-for-business/
[3] "What is VAPT? Audit, Types and Process." Accessed: Oct. 09, 2024. [Online]. Available: https://www.getastra.com/blog/security-audit/what-is-vapt/
[4] "Understanding VAPT: What it is and Why You Need It." Accessed: Oct. 02, 2024. [Online]. Available: https://www.testingxperts.com/blog/vapt
[5] "Full Guide To Network Penetration Testing and Network Penetration Methodology | by Muhanad Israiwi | Medium." Accessed: Oct. 09, 2024. [Online]. Available: https://medium.com/@mohanad.hussam23/full-guide-to-network-penetration-testing-and-network-penetration-methodology-43f5c9fdb91d
[6] "What is Network Penetration Testing? | IBM." Accessed: Oct. 09, 2024. [Online]. Available: https://www.ibm.com/topics/network-penetration-testing
[7] "What is Web Application Penetration Testing & How to Conduct it?" Accessed: Oct. 09, 2024. [Online]. Available: https://qualysec.com/web-application-penetration-testing-a-comprehensive-guide/
[8] "What is Web App Penetration Testing? [How to Conduct It]." Accessed: Oct. 09, 2024. [Online]. Available: https://www.getastra.com/blog/security-audit/web-application-penetration-testing/
[9] "Mobile Application VAPT - CyberSapiens." Accessed: Oct. 09, 2024. [Online]. Available: https://cybersapiens.com.au/mobile-application-vapt/
[10] "Mobile Application Penetration Testing." Accessed: Oct. 09, 2024. [Online]. Available: https://qualysec.com/a-deep-dive-into-mobile-application-penetration-testing/
[11] "Vulnerability Assessment and Penetration Testing : The Complete Guide | Blog." Accessed: Oct. 02, 2024. [Online]. Available: https://blog.entersoftsecurity.com/what-is-vapt/
[12] "What is API Penetration Testing? A Complete Guide." Accessed: Oct. 09, 2024. [Online]. Available: https://www.getastra.com/blog/security-audit/api-penetration-testing/
[13] "What is API Penetration Testing? - BreachLock." Accessed: Oct. 09, 2024. [Online]. Available: https://www.breachlock.com/resources/blog/what-is-api-penetration-testing/
[14] "What is SQL Injection? Tutorial & Examples | Web Security Academy." Accessed: Sep. 26, 2024. [Online]. Available: https://portswigger.net/web-security/sql-injection
[15] "Bypassing One-Time Password (OTP) Verification with Burp Suite by Hemanth V, Naveen P K, Dinesh Kumar T, Deebalakshmi R :: SSRN." Accessed: Sep. 26, 2024. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4948939
[16] "Bypassing OTP verification. We know that security is the main… | by Amolo Hunters | System Weakness." Accessed: Sep. 26, 2024. [Online]. Available: https://systemweakness.com/bypassing-otp-verification-797851057e79
[17] "What is Clickjacking? Tutorial & Examples | Web Security Academy." Accessed: Sep. 26, 2024. [Online]. Available: https://portswigger.net/web-security/clickjacking
[18] "Cleartext submission of password - PortSwigger." Accessed: Sep. 26, 2024. [Online]. Available: https://portswigger.net/kb/issues/00300100_cleartext-submission-of-password
[19] "Directory Traversal (Path Traversal)." Accessed: Sep. 26, 2024. [Online]. Available: https://www.invicti.com/learn/directory-traversal-path-traversal/
[20] "HTML Injection - Vulnerabilities - Acunetix." Accessed: Sep. 26, 2024. [Online]. Available: https://www.acunetix.com/vulnerabilities/web/html-injection/

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details