

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

9940 572 462

🕥 6381 907 438

🛛 🖂 ijircce@gmail.com

🛛 🙋 www.ijircce.com

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<sup>1</sup>, Kiran R Dodiya<sup>2</sup>, Akash khunt<sup>3</sup>, Divya Patel<sup>4</sup>

M. Sc Cyber Security, NSIT-IFSCS (Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India<sup>1</sup>

Assistant Professor & Program Co-ordinator of DFIS (Cyber Security & Digital Forensics) NSIT-IFSCS (Affiliated to

National Forensic Sciences University), Gandhinagar, Gujarat, India<sup>2</sup>

Assistant Professor & Program Co-ordinator of Cyber Security (Cyber Security & Digital Forensics) NSIT-IFSCS

(Affiliated to National Forensic Sciences University), Gandhinagar, Gujarat, India<sup>3</sup>

Assistant Professor & Course Co-ordinator of DFIS (Cyber Security & Digital Forensics) NSIT-IFSCS (Affiliated to

National Forensic Sciences University), Gandhinagar, Gujarat, India<sup>4</sup>

**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 Vulnerabilities. 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



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.





#### **IV. METHODOLOGY**



#### 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



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 .

N = 1 2 3 4 1	🖬 🖬 💭 💭 🌲 🔿 13:28 🗎 🖨 G
C root@kali: /home/kali	$\odot \odot \odot$
LL, NULL, NULL	
(13-24-30) [linty] the back-tend upps 1s system web application technology: PHP 56.40, Apache, PHP	
back-end DBMS: MySQL ≥ 5.0.12	
[13:24:36] [INPO] FETCHING COLUMNS TOT TABLE 'news' in Gatabase "aforgoki_afor [13:24:36] [INPO] fetching entries for table 'news' in Gatabase 'aforgoki afdb'	
[13:24:55] [INFO] retrieved: 'upd_img_13_Pic 3.JPG', 'img_13_Pic 3.JPG', 'Ms Anis Haroon, Member, Board of Governors, Aurat Foundation, presided over the	ceremony. ',' <p <="" style="text-align: justify;" th=""></p>
[13:24:57] [INFO] retrieved: 'upd_img_11_nigar 6.jpg', 'img_11_nigar 6.jpg', The ceremony was organized at the auditorium of Department of Earth Science	s, Quaid-e-Azam University.',' <div style="te&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:005] [IMFO] FET1EVEG: upt_mmg_15220501m_1mg_1550000500 Pit 1.70 , Img_15220501m_1mg_1550000500 Pit 1.70 , Aufat Foundation, in Collaboration, in C&lt;/td&gt;&lt;th&gt;native Report on CEDAW-2012 on December 20&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:02] [INFO] retrieved: 'upd_img_18_Pic 1.JPG','img_18_Pic 1.JPG','Aurat Foundation Quetta office organized the launching ceremony of the 'Pakistar&lt;/td&gt;&lt;th&gt;NGO Alternative Report on CEDAW-2012', on D&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:03] [INFO] retrieved: 'upd_img_19_1.PFG','img_19_1.PFG','Aurat Foundation launched 'Pakistan NGO Alternative Report on CEDAW-2012' on December 18&lt;br&gt;[13:25:03] [INFO] retrieved: 'upd_img_19_1.PFG','img_19_1.PFG','Aurat Foundation launched 'Pakistan NGO Alternative Report on CEDAW-2012' on December 18&lt;/td&gt;&lt;th&gt;, 2012, at Pearl Continental Hotel, Karachi&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:06] [INFO] retrieved: upd_mmg_zb_rk risk of the consultation intro, img_zb_rk view of the consultation intro, and roundationet's Ammaz&lt;/td&gt;&lt;th&gt;men legislation by the Punjab Assembly, ','&lt;&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:07] [INFO] retrieved: 'upd_img_1363072519_Pic 1 - TN.jpg','Img_1363072519_Pic 1 - TN.jpg','ISLAMABD: Today we, as women of Pakistan, declare our&lt;/td&gt;&lt;th&gt;solidarity with the women of the world on th&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:08] [INFO] retrieved: 'upd_img_1362649559 Pic - TN.jpg', 'img_1362649559 Pic - TN.jpg', 'Aurat Foundation, in collaboration with Parliamentarians Of&lt;br&gt;[13:25:03] [INFO] retrieved: 'upd_img_1362649559 Pic - TN.jpg', 'img_1362649559 Pic - TN.jpg', 'Aurat Foundation, in collaboration backdow by blogs Pic - TN.jpg', 'img 1362605197 [Intilded in the second backdow by blogs Pic - TN.jpg', 'img 1362605197 [Intilded in the second backdow by blogs Pic - TN.jpg', 'img 1362605197 [Intilded in the second backdow by blogs Pic - TN.jpg', 'img 1362605197 [Intilded in the second backdow by blogs Pic - TN.jpg', 'img 1362605197 [Intilded in the second backdow by blogs Pic - TN.jpg', 'img 1362605197 [Intilded in the second backdow by blogs Pic - TN.jpg', 'img 1362605197 [Intilded in the second backdow back&lt;/td&gt;&lt;th&gt;ommission for Human Rights (PCHR), organized&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:10] [INFO] Ferieved: upd_mg_136560034 Pit - TN.jpg', img_1362650034 Pit - TN.jpg', in order to express civil society's concern on the Tahir-&lt;/td&gt;&lt;th&gt;ul-Qadri's Long March, Aurat Foundation orga&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:11] [INFO] retrieved: 'upd_img_25_pic 1 - TN.JPG','img_25_pic 1 - TN.JPG','Aurat Foundation organized an advocacy meeting on Suggestions on Womer&lt;/td&gt;&lt;th&gt;'s Empowerment for Election Manifestos of Po&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:12] [INFO] retrieved: 'upd_img_1362650678_Pic - TN.jpg', 'img_1362650678_Pic - TN.jpg', 'Aural Foundation organized an advocacy meeting on 'Manike'&lt;br&gt;[12:25:15] [INFO] retrieved: 'upd_img_1362650678_Pic - TN.jpg', 'aural Foundation organized an advocacy meeting on Setting on Momentary&lt;br&gt;(Interview) [Interviewed: 'upd_img_1362650678_Pic - TN.jpg', 'aural Foundation organized an advocacy meeting on Setting on Momentary&lt;br&gt;[Interview] [Interviewed: 'upd_img_1362650678_Pic - TN.jpg', 'aural Foundation organized an advocacy meeting on Setting on Momentary&lt;br&gt;[Interview] [Interviewed: 'upd_img_1362650678_Pic - TN.jpg', 'aural Foundation organized an advocacy meeting on Setting on Momentary&lt;br&gt;[Interviewed: 'Interviewed: 'upd_img_1362650678_Pic - TN.jpg', 'aural Foundation organized an advocacy meeting on Setting on Momentary&lt;br&gt;[Interviewed: 'Interviewed: 'upd_img_1362650678_Pic - TN.jpg', 'aural Foundation organized an advocacy meeting on Setting on Momentary&lt;br&gt;[Interviewed: 'Interviewed: 'Interviewed: 'Interviewed: 'Aural Foundation organized an advocacy meeting on Setting of the S&lt;/td&gt;&lt;th&gt;to Suggestions on Women's Empowerment' with&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:16] [INFO] retrieved: upd_img_ze_ret i n.ppg, img_z_ret i n.ppg, variet roundation organized an advocacy meeting on suggestions on womer&lt;/td&gt;&lt;th&gt;'s Empowerment for Election Manifestos of Po&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:17] [INFO] retrieved: 'upd_img_29_Pic 3 - TN.JPG', 'img_29_Pic 3 - TN.JPG', 'Aurat Foundation organized an advocacy meeting on Suggestions on Womer&lt;/td&gt;&lt;th&gt;'s Empowerment for Election Manifestos of Po&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:18] [INFO] retrieved: 'upd_img_1362651276_Pic - TN.jpg', 'img_1362651276_Pic - TN.jpg', 'Aurat Foundation organized an advocacy meeting on Suggest)&lt;br&gt;[13:25:10] [INFO] retrieved: 'upd_img_1362651276_Pic - TN.jpg', 'Aurat Foundation organized an advocacy meeting on Suggest)&lt;/td&gt;&lt;th&gt;ons on Women's Empowerment for Election Mani&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:19] [INFO] retrieved: upd_img_13:26:25:05:06_Pic_TN.jpg', img_13:26:25:05:06_Pic_TN.jpg', Aurat Foundation and the Pakturkhwa (ivil Society Network&lt;/td&gt;&lt;th&gt;(PCSN) arranged a meeting to pay homage to&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:20] [INFO] retrieved: 'upd_img_1362649424_Pic - TN.jpg', 'img_1362649424_Pic - TN.jpg', 'Aurat Foundation, in collaboration with Democracy Reporting&lt;/td&gt;&lt;th&gt;g International (DRI) organized a training w&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:21] [INFO] retrieved: 'upd_img_1362649093_Picture-1 - TN.jpg', 'mg_1362649093_Picture-1 - TN.jpg', 'Aurat Foundation organized a concluding event&lt;br&gt;[13:25:22] [INFO] retrieved: 'upd_img_16k Corbite Landwork distribution certificates among arts students - TN DGC 'imm 26 Mc Corbite Landwork dist&lt;/td&gt;&lt;th&gt;of 'One Billion Rising' campaign to end viol&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[312522] [INFO] retrieved: upo_img_3_mode settie Lanusverk distributing GetTifted and and a source of a source of a source of the source of th&lt;/td&gt;&lt;th&gt;other civil society organizations organized&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:24] [INFO] retrieved: 'upd_img_38_Pic 2 - TN.jpg','img_38_Pic 2 - TN.jpg','Members of civil society organizations staged a rally to show solidari&lt;/td&gt;&lt;th&gt;ty with slain aid workers and polio vaccinat&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:25] [INFO] retrieved: 'upd_img_40_Pic 4 - TN.pg', 'img_40_Pic 4 - TN.pg', 'Aurat Foundation, in collaboration with Free and Fair Elections Network&lt;br&gt;[12:25:25] [INFO] retrieved: 'upd_img_41_Pic 4 - TN.pg', 'img_41_Pic 4 - TN.pg', 'Aurat Foundation disclosed a trail in the Telemethed Even correlation of the telemethed and the telemethed and the telemethed and the telemethed and telemethed&lt;/td&gt;&lt;th&gt;k (FAFEN),Human Rights Commission of Pakista&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:27] [INFO] retrieved: upo_img_2-1_rid 3 mi.pg , ang1_rid 5 mi.pg , and roundation displayed a start in the istamada capo, significa or&lt;br&gt;[13:25:27] [INFO] retrieved: upo_img_2-2_rid 1 AF Lahore Resident Director at the Josef colony TK.pg, 'img_2-2 pit 1 AF Lahore Resident Director at&lt;/td&gt;&lt;th&gt;the Josef colony TN.jpg','In order to co&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:28] [INFO] retrieved: 'upd_img_43_Pic 1 - TN.jpg','img_43_Pic 1 - TN.jpg','Aurat Foundation's Karachi office organized a round table discussion&lt;/td&gt;&lt;th&gt;on June 7, 2013, at Arts Council of Pakistan&lt;/th&gt;&lt;/tr&gt;&lt;tr&gt;&lt;td&gt;[13:25:29] [INFO] retrieved: 'upd_img_44_pic 1 - TN.jpg', img_44_pic 1 - TN.jpg', Aurat Foundation's Karachi office organized a follow-up meeting to i&lt;br&gt;[12:25:29] [INFO] retrieved: 'upd_img_44_pic 1 - TN.jpg', img_44_pic 1 - TN.jpg', Aurat Foundation's Karachi office organized a follow-up meeting to i&lt;/td&gt;&lt;th&gt;he CEDAW Committee's 54th session ', discuss the concerns ' 'constyle=" text-aligned"<="" th=""></div>
[13:25:39] [INFO] FETTEVEd: hpp_img0_ft in.g. 137/28287_Pit 1.JPG', Yamg 139296537_img_137/28287_Pit 1.JPG', Yamphers of Civil Society Network f	or Local Governance held a press conference
[13:25:31] [INFO] retrieved: 'upd_img_46_Lhr visit Begum Z Shahnawaz 22 May 2013 - TN.jpg', 'img_46_Lhr visit Begum Z Shahnawaz 22 May 2013 - TN.jpg', 'A	delegation of Aurat Foundation Lahore staff
[13:25:32] [INFO] retrieved: 'upd_img_4/_Pic1 - IN.JPG', 'img_4/_Pic1 - IN.jPG', 'On Tuesday, June 11, 2013, Aurat Foundation organized a consultation [13:25:32] [INFO] retrieved: 'und img 48 Pic 4 - IN ing', 'img 48 Pic 4 - IN ing', 'larat Foundation, in collaboration with of Mean Development Department	to share and discuss the concluding observat
[13:25:35] [INFO] retrieved: updimg_50_ic1 TN.JPG', img_50_ic1 TN.JPG', Aawaz and Accountability program of Aurat Foundation organized a pro-	vincial conference on the role of local gove
[13:25:36] [INFO] retrieved: 'upd_img_51_Title Annual Report 2012 title.jpg','img_51_Title Annual Report 2012 title.jpg','During year 2012, 7515 number	of cases of violence against women was repor
[13:25:30] [INFO] retrieved: 'upd_img_52_Pic 2 - TN.JPG', img_52_Pic 2 - TN.JPG', A representative forum of civil society organisations from across Paki [13:25:32] [INFO] netriaved: 'upd_img_53_Pic 3 - TN JPG' 'img_53_Pic 3 - TN JPG' 'On Sentember 12_2013 Aurat Enumdation Karaphi Affice from the civilitated as a sentember 12_2013 [INFO] netriaved: 'upd_img_53_Pic 3 - TN JPG' 'img_53_Pic 3 - TN JPG' 'Info Sentember 12_2013 Aurat foundation Karaphi Affice for a sentember 1	stan met today in Islamabad to discuss ways meeting of Ms Asma Khader Jordan-based huma
[33:25:36] [INO] retrieved: upd_img.54 cf $h^{-1}$ [30] ( $h^{-1}$ [31:25:36] [INO] retrieved: upd img.54 cf $h^{-1}$ [31:25:36] [INO] retrieved: upd img.54 cf $h^{-1}$ [31:25:36]	ip (WLP), organized a week long 2nd national

Picture 1 SQL Injection





#### 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



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			





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

m | 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.		
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 proceed 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



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.





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			

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

Table 6 Directory Traversal





#### 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.





Flowchart 7 HTML Injection

Please Login	×
Hello what's the weather of Ahemdabad	
Username: Password: → Submit	

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.





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

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

#### REFERENCES

"What is VAPT? Audit, Types and Process." Accessed: Oct. 02, 2024. [Online]. Available: [1] https://www.getastra.com/blog/security-audit/what-is-vapt/ "What is VAPT Testing? Importance, Types and Methodology." Accessed: Oct. 09, 2024. [Online]. Available: [2] https://qualysec.com/what-is-vapt-testing-its-methodology-importance-for-business/ "What is VAPT? Audit, Types and Process." Accessed: Oct. 09, 2024. [Online]. Available: [3] 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-tonetwork-penetration-testing-and-network-penetration-methodology-43f5c9fdb91d "What is Network Penetration Testing? | IBM." Accessed: Oct. 09, 2024. [Online]. Available: [6] https://www.ibm.com/topics/network-penetration-testing "What is Web Application Penetration Testing & How to Conduct it?" Accessed: Oct. 09, 2024. [Online]. [7] Available: https://qualysec.com/web-application-penetration-testing-a-comprehensive-guide/ "What is Web App Penetration Testing? [How to Conduct It]." Accessed: Oct. 09, 2024. [Online]. Available: [8] https://www.getastra.com/blog/security-audit/web-application-penetration-testing/ "Mobile Application VAPT - CyberSapiens." Accessed: Oct. 09, 2024. [Online]. Available: [9] https://cybersapiens.com.au/mobile-application-vapt/ "Mobile Application Penetration Testing." Accessed: Oct. 09, 2024. [Online]. Available: [10] 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/ 'What is API Penetration Testing? A Complete Guide." Accessed: Oct. 09, 2024. [Online]. Available: [12] https://www.getastra.com/blog/security-audit/api-penetration-testing/ "What is API Penetration Testing? - BreachLock." Accessed: Oct. 09, 2024. [Online]. Available: [13] https://www.breachlock.com/resources/blog/what-is-api-penetration-testing/ "What is SQL Injection? Tutorial & Examples | Web Security Academy." Accessed: Sep. 26, 2024. [Online]. [14] Available: https://portswigger.net/web-security/sql-injection "Bypassing One-Time Password (OTP) Verification with Burp Suite by Hemanth V, Naveen PK, Dinesh [15] Kumar T, Deebalakshmi R :: SSRN." Accessed: Sep. 26, 2024. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract\_id=4948939 "Bypassing OTP verification. We know that security is the main... | by Amolo Hunters | System Weakness." [16] Accessed: Sep. 26, 2024. [Online]. Available: https://systemweakness.com/bypassing-otp-verification-797851057e79 "What is Clickjacking? Tutorial & Examples | Web Security Academy." Accessed: Sep. 26, 2024. [Online]. [17] Available: https://portswigger.net/web-security/clickjacking "Cleartext submission of password - PortSwigger." Accessed: Sep. 26, 2024. [Online]. Available: [18] https://portswigger.net/kb/issues/00300100 cleartext-submission-of-password "Directory Traversal (Path Traversal)." Accessed: Sep. 26, 2024. [Online]. Available: [19] https://www.invicti.com/learn/directory-traversal-path-traversal/ "HTML Injection - Vulnerabilities - Acunetix." Accessed: Sep. 26, 2024. [Online]. Available: [20]

https://www.acunetix.com/vulnerabilities/web/html-injection/



INTERNATIONAL STANDARD SERIAL NUMBER INDIA







## **INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH**

IN COMPUTER & COMMUNICATION ENGINEERING

🚺 9940 572 462 应 6381 907 438 🖂 ijircce@gmail.com



www.ijircce.com