SAFEGUARD YOURSELF FROM BEING HACKED THROUGH VAPT

[1]Pranav Pandey, [2]Dr.Puneet Mathur

[1]Undergraduate, [2]Associate Professor
[1]Computer Engineering Department,
[1]Poornima Institute Of Engineering & Technology, Jaipur, India

Abstract : The usage of internet has been increased worldwide from the last few decades and most of the organizations have started keeping their data online either on their own servers or on clouds. But the security issues are been ignored by quite a many organizations and they do not invest much in securing their confidential data. Black Hat Hackers are some sharp minds who can bypass the present security mechanisms and could cause harm to organizations by stealing and selling their confidential data.
Security should be the major concern for any user while sharing their data to some third parties. And to provide such security aspects the good organizations uses different mechanisms like Vulnerability Assessment & Penetration Testing (VAPT).
This paper explains different web vulnerabilities and some methodologies to prevent web applications from being compromised.

***IndexTerms* – Ethical Hacking, Injection, Vulnerability Assessment & Penetration Testing(VAPT),Broken Authentication, data breach**

1. INTRODUCTION

The world is changing too fast and we are getting digital now a days but the main problem is that we do not focus much on security aspects. We rely on companies who claim their product is secured but the Question is that “are they actually secured?” Uber was also a victim of data breach. In 2016 Uber was attacked by hackers and they stole information of 57 million riders and drivers. For this Uber paid $148 million to settle the 2016 Data Breach (Conger, 2018).
No matter whether the platform is safe of not we give our confidential information to them. It is their duty to have well secured platforms which could preserve the privacy, integrity and availability of the data.
In the last few decades, many organizations have made different tools and frameworks that could be used to find the vulnerabilities present in the platforms like websites or servers. And these tools are in use by the security researchers for finding and patching the vulnerabilities before allowing anyone to exploit these vulnerabilities and harm the organizations.
Confidential Data could be stolen from the servers through various vulnerabilities like injections or misconfigured servers. The concept of data leak allows hackers to have access over the data and allows them to manipulate it too. Data leak surely comes into high risk category as the organizational data is no more confidential at all. Sometimes the attacker also manipulates the data on servers of organizations and this false information could be used to make profits like the bank balance of customer gets updated from 20,000Rs to 20,00,000Rs[1].
The main cause apart from software and hardware vulnerabilities is social engineering. Social engineering is the act of extracting confidential information from the person without their intentions to reveal it. Many of the big organizations have best security mechanisms even though they get hacked because of such acts. Social Engineering is the last step used by hackers and it is considered one of the toughest too as it requires lots of patience and sometimes this act takes more than 3-4 years to build such trusts on the victim.

2 Vulnerability Assessment & Penetration Testing

Many organizations are not able to cope up with the security issues. In such situations Vulnerability Assessment & Penetration Testing (VAPT) could be the best solution to cope up with the security loop holes.
The hackers need to find the vulnerable input points to enter and launch their attacks. But these vulnerable input points could be made secured by penetration testing using some tools and frameworks. The VAPT helps the organizations to patch the security loopholes before allowing anyone to harm the organization.
VAPT is not an easy job and requires multiple methodologies like updated platforms, correct server configurations, giving minimal permissions to employees regarding manipulation of confidential data over the servers etc.
The aim of VAPT is to maintain the privacy, integrity and availability of confidential data.
These vulnerabilities have different severity levels. For example version disclosure is having low severity on the other hand SQLi is considered as high severity. There is a non profitable charitable organisation OWASP (Open Web Application Security Project) which provides practical and cost effective information regarding application security [3]. The real problem we are facing is that most of the developers have knowledge about one domain like MEAN Stack or JavaScript or php etc and very few are having knowledge of security also. This lack of knowledge causes the security loop holes and sometimes causes big losses to medium scale and small scale organizations.

To make the tasks easier there are some paid tools which could find the vulnerabilities in web platforms like Nessus, Burp Suite etc. And those organizations which cannot afford such expensive tools can go for open source. Before discussing about the solutions I would like to put forward the problems which need to be understood first.

3 Classifications of Vulnerabilities

Vulnerabilities are nothing but the loop holes in the platform and it shows the overlooked mistakes by the developers. These vulnerabilities show the carelessness of the developers and the lack of testing of platform during the project development life cycle. It is a best practice to involve white box, gray box & black box testing in the application development life cycle.

Vulnerability	Rank
Injection	1
Broken Authentication	2
Sensitive Data Exposure	3
XML External Entities (XXE)	4
Broken Access Control	5
Security Misconfiguration	6
Cross-Site Scripting	7
Insecure Deserialization	8
Using Components With Known Vulnerabilities	9
Insufficient Logging And Monitoring	10

[3]
OWASP TOP 10 2017

3.1 Injection

Injection vulnerability is quite common and it is found in SQL, LDAP, OS Commands, SMTP Headers etc and they could be discovered easily when the source code is analyzed. Injection could cause in loss of sensitive data, modification of data or denial of access to the data. The application is vulnerable to injection flaw when it does not filter or validate the input given to it. The easiest way to prevent from such flaws is to keep commands and queries separate from data[5].

There are various tools in the market which could be used to find the injection flaws. One of them is sqlmap. Sqlmap is a powerful pen testing tool which is having a very big database of different payloads and these payloads are sent as the raw data to the input points. If the input point executes those payloads then that point makes the whole application vulnerable to such flaw.

3.2 Broken Authentication

A user can authenticate themselves through usernames and passwords. But sometimes these login credentials are easy to guess through brute force or dictionary attacks. And attackers only need to gain access to only few accounts and this could lead to access to whole application if the permissions allotted is of admin and this could lead to money laundering, identity theft etc[6]. The application is vulnerable to broken authentication when it allows you to keep weak passwords like “123456” or allows you to apply brute force or dictionary attacks or reveals the session id. One of the easiest way is to use reCAPTCHA to prevent brute force attacks.
It is always better to use multi security layers instead of using one solid layer. Do not use easy passwords and change your passwords on regular basis[6]. This is how you can prevent yourself from being hacked.

3.3 Sensitive Data Exposure

Http protocol sends the data in plain text and it is possible to have successful man in the middle attack where the attacker can steal the credit card details or login credentials. Even sometimes the servers also store the data in plain text and this leads the data in danger. Hence encryption should be used wherever possible. Like instead of using http it is more preferable to use https or use SHA256 to encrypt data before storing on server. So in case of data breach the attacker won’t be able to use the encrypted data.
It should also be kept in mind not to use the older encryption algorithms like MD5. It is because the key which is used to encrypt the data can be found through brute force attacks and the data could be decrypted through the found key.

3.4 Broken Access Control

Misconfiguration is assigning improper permissions to the non-admin users which could result in big trouble sometimes. If the user gets admin privileges it could result in unauthorized information acess, modification or destruction of data etc [7]. An application is said to be vulnerable to broken access control if the url or application state could be modified [7].

3.5 Security Misconfiguration

Configuration of servers, web applications is a very tedious task and the misconfigurations could occur at any level either at web server or application server or database or custom code or any frameworks[8] . These misconfigurations could lead to unauthorized access to few functionalities and many a times whole system gets compromised[8]. A server is vulnerable to such attack if unnecessary services or ports (like ftp or telnet) are enabled.

4 Methodology of Hacking

There is no robust way for hacking but generally we use the following five steps-

4.1 Information Gathering

It involves gathering information about the target before launching the attacks and one of the first phases is dumpster diving[9]. In this phase the hacker finds important information like old passwords, information regarding important employees or finding how the organisation works etc[9]. After gathering such information the hacker performs foot printing regarding open ports, ip address of alive hosts, operating system of machines, services running on server etc.

4.2 Scanning

In this phase the hacker tries to find the possible vulnerabilities using the information he has gained. This phase has further 3 methods- pre-attack, port-scanning & information extraction [9]. The main idea of scanning is to find an input point which is vulnerable to some attack. This vulnerable point might be used in future to gain access to system or network. There could be many tools or scripts used but generally port scanners, vulnerability scanners, sweepers etc are used.

4.3 Gain Access

In this phase the hacker firstly arranges the information gained in phase 1 & phase 2 and then creates a blueprint of network. This is the step where actual skills of hacker are used. So the loop holes discovered are exploited to gain unauthorized access. So depending upon the kind of vulnerability found he could use either Buffer Overflow or Denial of Service (DOS) or Session Hijacking etc.

4.4 Maintaining Access

Maintaining access is often considered an important part as you need to implant some backdoors or Trojans in the system that no one could found easily. Of course you will not give a name like shell.php or backdoor.php etc as they could be found and removed easily. So the location of such malicious codes must be found very carefully and the name of code should match with the surrounding code scripts name. This steps helps to access the unauthorized information or used to launch other attacks over the victim.

4.5 Cover Tracks

This phase is the most important one where the hacker removes their traces by modifying the log files or undoing the changes he made during gaining access.Covering tracks makes it difficult for security personnel to backtrack the hacker and prevents him from any legal actions. Sometimes the new script kiddies used the backdoors and give some clue in it like their mail address where the messages will be forwarded automatically or some other clued without even encoding the shells. This small mistake could send them behind the bars.

5 Conclusions

There are good chances that the organization is vulnerable to some attacks. So it's better to invest some money over VAPT which will provide you a report of the possible attacks and what could be the consequences of these attacks to the organization. So the VAPT helps in finding the glitches in the code or the misconfigurations of their network. And the most important thing is that it prevents the loss of reputation of the organization. An attack could cause a massive share market loss as it is dependent upon the reputation of organization.

References

[1] R. Barona, E. A. Mary Anita (2017), "A Survey on Data Breach Challenges in Cloud Computing Security: Issues and Threats", 2017 International Conference on Circuit , Power and Computing Technologies (ICCPCT), 2017.

[2]Conger, Cate (2018, September 26). Uber Settles Data Breach Investigation for $148 Million. The New York Times. Retrieved from https://www.nytimes.com/2018/09/26/technology/uber-data-breach.html

[3]Owasp.org,"OWASP",2019.[Online].Available: https://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project. [Accessed: 17-March - 2019].

[4] owasp.org, "OWASP", 2019. [Online]. Available: https://www.owasp.org/index.php/Top_10-2017_Top_10. [Accessed: 17-March - 2019].

[5] owasp.org, "OWASP", 2019. [Online]. Available:https://www.owasp.org/index.php/Top_10-2017_A1-Injection. [Accessed: 17-March - 2019].

[6]owasp.org,"OWASP", 2019. [Online]. Available:https://www.owasp.org/index.php/Top_10-2017_A2-Broken_Authentication. [Accessed: 17-March - 2019].

[7]owasp.org,"OWASP",2019. [Online]. Available:https://www.owasp.org/index.php/Top_10-2017_A5-Broken_Access_Control. [Accessed: 17-March - 2019].

[8]owasp.org,"OWASP",2019.[Online].Available:https://www.owasp.org/index.php/Top_10-2017_A6-Security_Misconfiguration. [Accessed: 17-March - 2019].

[9]Arora, Shivam (2019, February 7). Webinar Wrap-up: The Five Phases of Ethical Hacking. Retrieved from https://www.simplilearn.com/phases-of-ethical-hacking-article