INTERNATIONAL RESEARCH JOURNAL OF MULTIDISCIPLINARY STUDIES
SPECIAL ISSUE ON ADVANCEMENT IN FIELD OF COMPUTER SCIENCE AND INFORMATION TECHNOLOGY

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

A Review on Maintaining Web Applications and Brute Force Attack

[1]Prof. Marne Gauri,[2]Prof. Ingole R.Y.
[1,2,]Assistant Professor, Mamasaheb Mohol College,Paud Road, Pune 38,

Abstract :-
Now a days ,almost all generations are using technology. Every and other person is active on social media like Facebook, twitter, as well mail accounts. Each and every organizations,institutes,companies are having their own web portals. Every site is handling lots of data. This data is in terms of product ,employee information, financial data etc.. Most of the time the data attributes are confidential. Through the use of emerging data technologies like cloud computing,Big data etc. these data gets properly stored and accessed. People are using Internet are exchanging information and communicating with each other for business and Personal purpose.Everyone needs safe and secure way of communication.This paper is discussing different aspects of network security-threats,attacks and Vulnerabilities. Theweaknesses in web application security are also discussed. The network security aspects such as authentication, Confidentiality, Integrity are also discussed.Different attack methodology like Hidden Field Manipulation attack,Parameter Tampering attack,Buffer Overflow attack (Denial of Service), SQL Injection etc. are also discussed. The paper is focusing on Brute force attack,reverse Brute force attack.The different tools like Aircrack-ng,John the Ripper, Rainbow crack,Cain and Abel, Hashcat,Ncrack are explained. Hacker's/attacker's purpose and malware activities are identified. Precautionary measures are mentioned against Brute force attack in this paper.Like the Wordpress brute force attack has occurred and the team monitored the attack and traced its consequences are also discussed in this paper. Also Microsoft office365 brute force attack is given in this paper.
Keywords : Attack,Security,ThreatVulnerabilities,Authentication

Introduction

Web application is a software that runs on web browser which allows user interaction for various purpose. Network security is designed to protect the usability and integrity of the network and data. It includes both hardware and software technologies. It targets a variety of threats and stops them from entering or spreading on your network. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Security Elements

Security relies on the following elements:

1. Authentication process uniquely identifies clients of the applications and services. The clients might be end users,other services,process or computers.Authenticated clients are referred as principles.
2. Authorizationprocess governs the resources and operations that the authenticated client is permitted to access. Resources include files, databases, tables, rows, and so on, together with system-level resources such as registry keys and configuration data. Operations may include financial operations such as purchasing a product, transferring money from one account to another.
3. Effective auditing and logging is the key to non-repudiation.

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

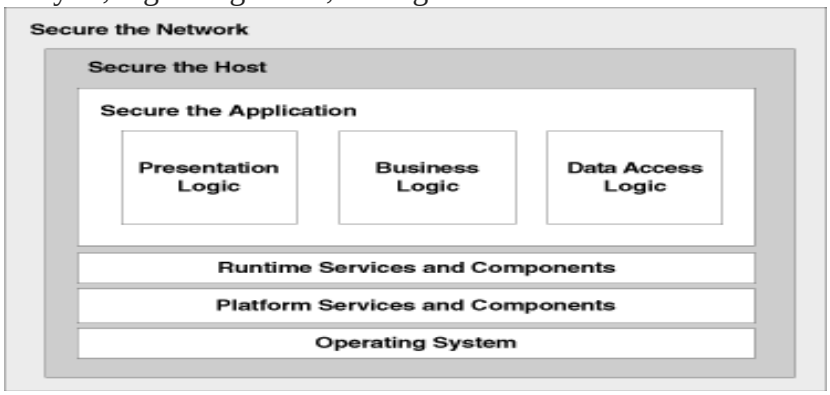
4. Confidentiality, is the process of making sure that data remains private and confidential, and that it cannot be viewed by unauthorized users or eavesdroppers who monitor the flow of traffic across a network. Encryption is used to enforce confidentiality.
5. Integrity is the guarantee that data is protected from accidental or malicious modification. Integrity for data in transit isachieved by using hashing techniques and message authentication codes.
6. Availabilitymeans that systems remain available for legitimate users. The goal for many attackers with denial of service attacks is to crash an application or to make sure that it is sufficiently overwhelmed so that other users cannot access the application.

Threats, Vulnerabilities, and Attacks

A threat is any potential occurrence, malicious or otherwise, that could harm an asset.
A vulnerability is a weakness that makes a threat possible. This may be because of poor design, configuration mistakes, or inappropriate and insecure coding techniques. Weak input validation is an example of an application layer vulnerability, which can result in input attacks.
An attack is an action that exploits a vulnerability or enacts a threat. Examples of attacks include sending malicious input to an application or flooding a network in an attempt to deny service.

Monitoring Web application for security

To design and build a secure Web application you must know the threats.Developers, must develop secure, robust, and hack-resilient solutions by applying security checkpoints and techniques at early stages of development as well as throughout the software development lifecycle for the web application. Security mechanisms that should be used include, threat modeling, risk analysis, static analysis, digital signature, among others.



The Weaknesses in web application security

Invalidated Input : When the program accepts input from an uncontrolled source, there is a chance for a attacker to pass data. If you don't validate the input, it might cause program crashes by allowing an attacker to execute his own code. This can happen like:Buffer overflows,Format string vulnerabilities,URL commands,Code insertion,Social engineering.

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

Broken Access Control –While developing web application different roles are provided to different persons which can access different contents and functions of the site.For secure session proper authorization and secure authentication has to be done with controlled access.

Broken Authentication and Session Management

In case of **Cross Site Scripting** (XSS) attacker injects his own code into legitimate website sometimes to break access control, authentication etc.

Through **Injection attacks** attackers inject some code in the program that accompanies unstructured data to get confidential information.

Improper Error Handling,Insecure Storage,Insecure Configuration Management are also some weaknesses in web application.

Attack methodology

Hidden Field Manipulation attack- Sometimes websites may use hidden form fields, which do not get displayed on the page, to post some confidential data in back end database.Hackers can easily hack and manipulate these field values and exploit it. .

Parameter Tampering attack- Information passed with request is not validated before it is used in the application. The request parameters in URL string can be manipulated to get certain information

Buffer Overflow attack (Denial of Service)- An attacker can overwrite the buffer values in the call stack to execute malicious code for the specific purpose and can take advantage of buffer overflow.

Cross-Site Scripting (Hacking / Identity Theft)- In this case attacker can insert and execute malicious code into client side script to deliver malicious script to visitors browser.

Backdoor and Debug Options (Technology Trespassing)- Applications which accesses remote computers are targeted to breakdown the victims network.

Directory Browsing (Hacking into servers and accessing data)- An attacker can access other parts of the file system by stepping out of the root directory. The attacker can view restricted files to gain information to breakdown the system.The attacker executesmalicious commands as if the userof the website.

HTTP Response Splitting-It is the ability to write one HTTP request so that the target generates two responses one to be completely under control of attacker. The attacker can inject malicious script for intended purpose.

Stealth Commanding- Through a set of techniques attackers exploit parsing problems in server-side scripts tries to change the code executed by the server. It is basically used in execution of operating system commands, for complete takeover of the server.

3rd Party Misconfiguration-This is most commonly used attack for web application by introducing third party plugins or services to perform malicious task by the website.

Known Vulnerabilities & SQL Injection- Here, the attacker forms a query and inputs it as part of the authentication and the database .Web server marks this as a valid query executed and opens gates into the web based system as the attempted user.

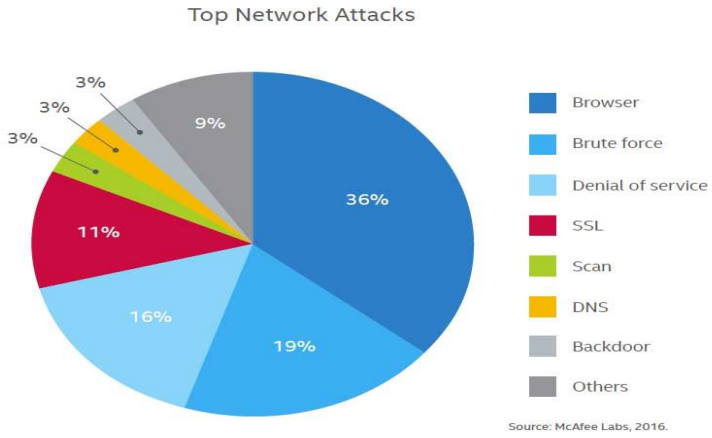
The Brute force attack

Brute force is a trial and error method used by application programs to decode encrypted data such as passwords or Data Encryption Standard keys, through exhaustive effort (using brute force) rather than employing intellectual strategies. Hackers writes scripts to carry out those numerous attempts instead

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

of carrying out it manually,but the success of attack depends on various factors like length and combination of characters,numbers and special characters in forming password. Sites usually suggest for strong passwordwith long length and diversity of characters in password.This make brute force attack difficult but not impossible.It will take longer time to reach password by brute forcing. So sites generally use brute force password cracking to check weak password for security. One more way to prevent this attack ,user can be restricted for number of unsuccessful login attempts.This is why web-based services start showing captchas if you hit the wrong passwords three times or they will block your IP address.

Top network attacks for 2016



Reverse Brute force attack

It is reverse approach for cracking password. Suppose attacker know the password and have no idea about the username. The attacker will try the same password against all possible guesses for username for the purpose. This technique can be used against any site that do not get blocked after defined number of unsuccessful attempts.

Tools used for brute force

Aircrack-ng –As the name suggest this is wireless password cracking tool to attack on WIFI802.11. It performs dictionary attacks against wireless network. The productive password dictionary is more likely to become victim .This tool is available for Windows, Linux, IOS and Android platform.

John the Ripper- This tool can perform brute force attack against encrypted password as it automatically identify hashing used in password.It perform attack by guessing all possible combinations of text and numbers for password.It can also perform dictionary attack.Basically it was designed for cracking Unix password but now it supports fifteen different platforms.

Rainbow Crack- This tool generates rainbow table or uses pre-computed rainbow tables published by various organizations to crack the password. The table reduces the time in performing attack.This tool is available for latest versions of Windows and Linux.

Cain and Abel –This tool performs brute force attack and cryptanalysis attack,can decode scrambled password,recover wireless network keys,analyze routing protocol,crack encrypted passwords using dictionary,reveal password boxes ,Man in the Middle attack .But some virus scanner like Avast and Microsoft Security Essentials find it malware and block it in system.

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

L0phtCrack- This tool is basically used to crack windows password of less than 14 character lengths containing only alphabets and numbers and is accompanied by rainbow tables.It cracks the password by usingLM hashing through rainbow tables.

Crack- This oldest password cracking tool is used for the UNIX system to check weak passwords by performing dictionary attacks.

Hashcat- The various attacks like Brute-Force attack, Dictionary attack, Fingerprint attack, Hybrid attack, Mask attack, Table-Lookup attack and Toggle-Case attack etc are supported by this tool. It uses hashing algorithm like LM Hashes, MD4, MD5, SHA-family, Unix Crypt formats for CPU based password cracking. It supports Windows,Linux and MAC OS platform.

SAMInside- It can perform Mask attack, Dictionary attack, Hybrid attack and Attack with Rainbow tables using over 400 hashing algorithms.It is used for cracking Windows OS password.

DaveGrohl- It performs brute force attack for Mac OS X and supports both dictionary attacks and incremental attacks. It enables to perform attacks from multiple computers to attack on the same password hash.

Ncrack-It performs different attacks including bruteforce attacks by supporting various protocols such as RDP, SSH, http(s), SMB, pop3(s), VNC, FTP, and telnet. It can be used with various platforms including Linux, BSD, Windows and Mac OS X.

THC Hydra-It can crack passwords of network authentications by performing brute-force attacks and performs dictionary attacks against various protocols including telnet, ftp, http, https, smb etc. It is available for various platforms including Linux, Windows/Cygwin, Solaris 11, FreeBSD 8.1, OpenBSD, OSX and QNX/Blackberry

Treasure for Hackers–

Aattackerscanuse files and the web host server to cause a wide variety of damage through malicious behavior once they gain access.

Deform: In this case site can display unwanted and malicious content, by deletingthe original content and the website can be broken down.;

Malware distribution: The site visitors get infectedthrough distribution of malware, ransomware and viruses.

Spamvertising*:* It deals with introducing spam content or links to spam websites

Redirecting to malicious site*:* Through accessing the legitimate site may cause visitors to be redirected to malicious websites, or to pages that contain affiliate links and make money for the hackers.

Stealing system resources: Attackers may carry out tasks such as email campaigns and content delivery by using the web server's resources.

Fun: some attackers may perform brute force attacks which are simple and easy just for entertainment and fun.

The following table indicates Times required for Brute force attack on various key lengths using Deep Crack technology

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

Bits	Number of Keys	Brute Force Attack Time
56	7.2×10^{16}	20 hours
80	1.2×10^{24}	54,800 years
128	3.4×10^{38}	1.5×10^{19} years
256	1.15×10^{77}	5.2×10^{57} years

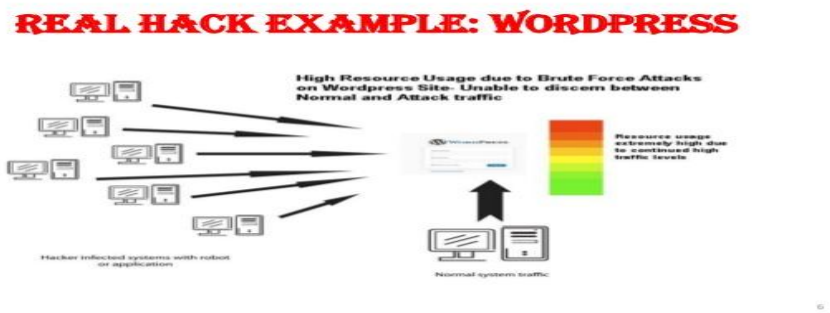
Deep Crack technology was developed in 1998 by the EFF (Electronic Frontier Foundation). They built a machine called the Deep Crack capable of trying a million DES keys per microsecond against a readable ASCII string hours to try all possible keys.

Protecting against Brute force attack-

1. To block Brute force attacks,accounts can be locked after unsuccessful attempt of login. Accounts can be locked for specific period of time or till manuallyunlocked by administrator.But sometimes some websites are unable toenforce this policy due to constant unlocking of accounts.
2. One can block Brute force attack just by injecting random pauses while checking password authentication. Adding a few seconds pause can slow down a Brute force attack without affecting the legitimate users as they login.
3. Advanced users can be allowed to login from certain IP address only to protect their accounts.
4. Unique login URLs can be assigned, so that not all users can access site from the same URL.
5. CAPTCHA can be used to prevent automated attacks.
6. Accounts can be placed in lockdown mode with limited capabilities.

Example

Real life example of Brute Force attack is, large network of compromised servers are trying to break wordpress website through wp-login.php brute force attack since April 2013.Wordpress is a open source software tool foe Content Management System using PHP and SQL. It can be used for creating websites or blogs. The attack is broad in that it uses a large number of attacking IPs, and is also deep in that each IP is generating a huge number of attacks. This is the most aggressive campaign we have seen to date, peaking at over 14 million attacks per hour.

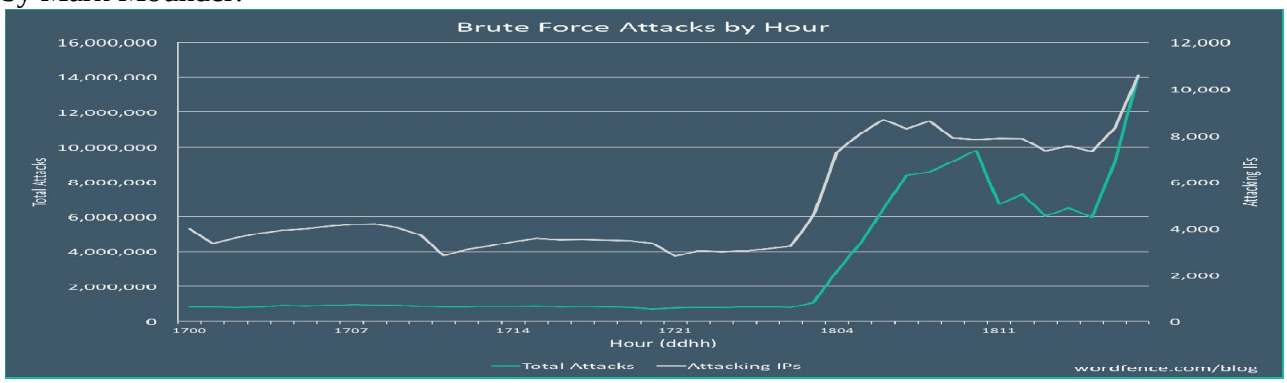


Wordpress can be protected against Brute forcing. The suggestions are as follows

Use strong password with at least 8 character long with proper combination of upper-lower case characters, punctuations numbers or non alphanumeric characters.

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

Changing default username for admin.
Locking admin access with hatches.
Disabling CPU intensive login limit plugins.
Scanning website for hacks.
Backup wordpress.
Disable wordpress autosave.
CloudFlare DNS level protection.
Observation by WordPress team for the attack posted in Wordpress Security on December 18 2017 by Mark Mounder.



The attack has so far peaked at 14.1 million attacks per hour.
The total number of IPs involved at this time is over 10,000.
up to 190,000 WordPress sites targeted per hour.
This is the most aggressive campaign seen by hourly attack volume.

Brute Force Attack on Microsoft Office365 cloud

Cloud services are on path to become the standard for enterprise IT solutions, and Office 365, which offers cloud access to Microsoft Word, Excel and other productivity apps, has taken a dominant role with 58.4% of all sensitive corporate data in the cloud is stored in Office 365.The Microsoft office 365 attack was cloud to cloud attack . The hackers used public hosting services infrastructure to attack on Saas service.This attack was directed against a few targets across multiple companies instead of many users as possible. There were 100,000 failed-login attempts originating from 67 IPs and 12 networks over a period of nearly 7 months.It used slow and low strategy to avoid the detection by the provider.First the hackers acquired corporate usernames and passwords from multiple companies that may be tied to multiple cloud services and then tried different email variations derived from the employee name to try to gain access to sensitive information.It can be inferred that they used the same password for each user for every username variation because each email was only used once to attempt the unauthorized login.Another assumption was that the accounts lacked basic security provisions, such as multi-factor authentication (MFA). Organizations using Office 365 have been forced to rely on traditional and inadequate username-password authentication to try to protect themselves from sophisticated attackers. Current versions of Office 365 mail clients support basic two-factor authentication while older Microsoft clients and third-party email applications do not. Because of this antiquated approach to authentication, attackers know that Office 365 is ripe to be exploited, and we

Vol. 4, Special Issue 8, February, 2018 ISSN (Online): 2454-8499
Impact Factor: 1.3599(GIF), 0.679(IIFS)

anticipate attacks against Office 365 to proliferate for the foreseeable future."It can be difficult for organizations to fully protect themselves from sophisticated attacks targeting the cloud without having a robust cloud security infrastructure.Organizations need to gain awareness of their cloud usage in order to mitigate the risk of a security incident in a meaningful way.

Conclusion

Security of web application is getting more attention. The security treats and internet should be analyzed to determine security technology. Confidentiality, Authentication,Integrity, Authorization, Non-repudiation must be considered while developing secure application.Web Application must be protected against Threats, Vulnerabilities and attacks.Secure host secure application and secure network are the key for secure web application. Hackers or attackers identifies weaknesses in web application and applies various attacking methodology.Brute force attack is popular amongst attackers to crack password or user authentication to a web application to perform malfunction for specific purpose.Almost all hash cracking algorithms use the brute-force to hit and try. This attack is best when you have offline access to data. In that case, it makes it easy to crack, and takes less time.Brute-force password cracking is also very important in computer security as it can be used to check the weak passwords used in the system, network or application.There is a long list of password cracking tools which use brute-force or dictionary attack. Here are listedsome of them, the best and most popular tools.Protecting against Brute force attacks can be achieved upto some extent.Wordpress brute force attack example can be a new topic research.

References

1. *https://en.wikipedia.org/wiki/Web_application_security*
2. *http://paper.ijcsns.org/07_book/201212/20121211.pdf*
3. *https://msdn.microsoft.com/en-us/library/ff648636.aspx*
4. *http://searchsoftwarequality.techtarget.com/tutorial/Top-10-Web-application-security-vulnerabilities*
5. *https://www.securityconsulting.net.au/types-of-website-security-attacks/*
6. *http://searchsecurity.techtarget.com/definition/brute-force-cracking*
7. *https://www.wordfence.com/learn/brute-force-attacks/*
8. *http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref*
9. *http://www.cs.virginia.edu/~csadmin/gen_support/brute_force.php*
10. *https://www.cisco.com/c/en/us/products/security/what-is-network-security.html*
11. *https://en.wikipedia.org/wiki/Network_security#Security_management*
12. *https://developer.apple.com/library/content/documentation/Security/Conceptual/SecureCodingGuide/Articles/ValidatingInput.html*
13. *https://www.coursehero.com/file/p6d7ohl/NETWORK-SECURITY-4-Summary-and-Conclusion-Network-security-is-an-important/*
14. *http://resources.infosecinstitute.com/popular-tools-for-brute-force-attacks/#gref*
15. *https://www.inmotionhosting.com/support/edu/wordpress/wp-login-brute-force-attack*
16. *https://www.slideshare.net/karawash/brute-force-attack-63754038*
17. *https://www.calyptix.com/top-threats/top-7-network-attack-types-2016/*
18. *https://www.tripwire.com/state-of-security/featured/new-type-brute-force-attack-office-365-accounts/*
19. *https://www.experts-exchange.com/articles/12460/Cryptanalysis-and-Attacks.html*
20. *https://www.infosecurity-magazine.com/news/widespread-bruteforce-office-365/*
21. *https://www.wordfence.com/blog/2017/12/aggressive-brute-force-wordpress-attack/*