IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 20, Issue 6, Ver. II (Nov - Dec 2018), PP 41-51
www.iosrjournals.org

Testing By Application Software On-Brute Force Attack On Open Functionality Secured

Sony Jacob[1], Mr.B Senthil Kumar Msc.,Mphil.,(Ph.D)[2]
[1]*M.Phil Scholar Department Of Computer Science Sree Narayana Guru College Kg Chavady, Coimbatore 641105 Tamil Nadu*
[2]*Asst. Professor Department Of Computer Science Sree Narayana Guru College Kg Chavady, Coimbatore 641105 Tamil Nadu*
Corresponding Author: Sony Jacob

Date of Submission: 18-11-2018 Date of acceptance: 04-12-2018

I. Introduction

The project entitled as **Brute Force Attack On Open Functionality Secured** is to design and develop the application package for well secured dynamic application. A common threat web developer's face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

In the world of Cyber crimes, brute force attack is an activity which involves repetitive successive attempts of trying various password combinations to break into any website. This attempt is carried out vigorously by the hackers who also make use of bots they have installed maliciously in other computers to boost the computing power required to run such type of attacks. Usually, every common ID (for e.g. "admin") has a password. All you need to do is try to guess the password. Let's say if it's a 2-digit-pin, you have 10 numeric digits from 0 to 9. This means there are 100 possibilities. You can figure this out with pen and paper like Mr. Bean who tried to find correct last two digits of the phone number of the lost kid's father in the movie, *Mr. Bean's Holiday*.

But, the truth is that no password in the world consists of only 2 characters. Even, the pin numbers (a sort of password) used on mobile phones or in a bank consist of minimum 4 characters.And, on the internet, 8 is generally the standard number for shortest length of a password. Furthermore, complexity is added as alphabets are added within a password to make it more secure. By the way, alphabets can be used in both UPPER and lower cases, thus making a password case sensitive.

Behind brute force attack, hacker's motive is to gain illegal access to a targeted website and utilize it in either executing another kind of attack or stealing valuable data or simply shut it down. It is also possible that the attacker infect the targeted site with malicious scripts for long term objectives without even touching a single thing and leaving no trace behind.

In my survey provides solutions by using some components mainly Administration Management and User Management. Access can be restricted to only those manipulates and perspectives that Administrator.

The main objective of this is to secure enforce by using IP Address tracking ,webcam capturing, password authentication, using bio metric sensors, Mobile phone SMS,ID and password security, Fingerprint based security system.

If any one try to make any trouble the data will be locked and a message will send to administrators and particular computer's users e-mail address and cell phone too. The software is connected with the employs track record and to service history.

II. Related Works

- **Performance testing**
- **Latest fingerprint security system with eye detection**
- **IP address tracker**
- **Administration progress**
- **User progress**
- **Locking accounts**
- **Hacker list**
- **Results and discussion**

III. Performance Testing

Fingerprint recognition is a popular security feature in the newer generation of smartphones and is a well-known biometric technology. Since Microsoft introducing iris recognition feature in its smartphones, there were comparisons between these two biometric traits. We will be discussing both these biometric technologies, their capabilities and security features.

Iris and fingerprint recognition both have higher accuracy, reliability and simplicity as compared to other biometric traits. These attributes make iris and fingerprint recognition perform better and a particularly promising security solution in today's society. The process starts by capturing the images of iris and fingerprint which are then pre-processed to remove any noise effects. The distinguishing features are then extracted and matched to find similarity between both the feature sets. The matching scores that are generated from the individual recognizers are given to the decision module which decides if a person is genuine or an impostor.

Why do Performance Testing?

Performance Testing is done to provide stakeholders with information about their application regarding speed, stability and scalability. More importantly, Performance Testing uncovers what needs to be improved before the product goes to market. Without Performance Testing, software is likely to suffer from issues such as: running slow while several users use it simultaneously, inconsistencies across different operating systems and poor usability. Performance testing will determine whether or not their software meets speed, scalability and stability requirements under expected workloads. Applications sent to market with poor performance metrics due to non existent or poor performance testing are likely to gain a bad reputation and fail to meet expected sales goals. Also, mission critical applications like space launch programs or life saving medical equipments should be performance tested to ensure that they run for a long period of time without deviations.

Types of Performance Testing

- **Load testing -** checks the application's ability to perform under anticipated user loads. The objective is to identify performance bottlenecks before the software application goes live.
- **Stress testing -** involves testing an application under extreme workloads to see how it handles high traffic or data processing. The objective is to identify breaking point of an application.
- **Endurance testing -** is done to make sure the software can handle the expected load over a long period of time.
- **Spike testing -** tests the software's reaction to sudden large spikes in the load generated by users.
- **Volume testing** - Under Volume Testing large no. of. Data is populated in database and the overall software system's behavior is monitored. The objective is to check software application's performance under varying database volumes.
- **Scalability testing** - The objective of scalability testing is to determine the software application's effectiveness in "scaling up" to support an increase in user load. It helps plan capacity addition to your software system.

Common Performance Problems

Most performance problems revolve around speed, response time, load time and poor scalability. Speed is often one of the most important attributes of an application. A slow running application will lose potential users. Performance testing is done to make sure an app runs fast enough to keep a user's attention and interest. Take a look at the following list of common performance problems and notice how speed is a common factor in many of them:

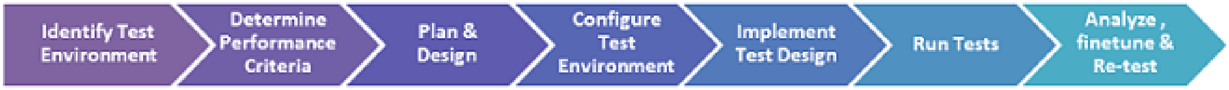
- **Long Load time -** Load time is normally the initial time it takes an application to start. This should generally be kept to a minimum. While some applications are impossible to make load in under a minute, Load time should be kept under a few seconds if possible.
- **Poor response time -** Response time is the time it takes from when a user inputs data into the application until the application outputs a response to that input. Generally this should be very quick. Again if a user has to wait too long, they lose interest.
- **Poor scalability -** A software product suffers from poor scalability when it cannot handle the expected number of users or when it does not accommodate a wide enough range of users. 'Load Testing 'should be done to be certain the application can handle the anticipated number of users.
- **Bottlenecking -** Bottlenecks are obstructions in system which degrade overall system performance. Bottlenecking is when either coding errors or hardware issues cause a decrease of throughput under certain loads. Bottlenecking is often caused by one faulty section of code. The key to fixing a bottlenecking issue is to find the section of code that is causing the slow down and try to fix it there. Bottle necking is generally fixed by either fixing poor running processes or adding additional Hardware. Some **common performance bottlenecks** are

- CPU utilization
- Memory utilization
- Network utilization
- Operating System limitations
- Disk usage

Performance Testing Process

The methodology adopted for performance testing can vary widely but the objective for performance tests remain the same. It can help demonstrate that your software system meets certain pre-defined performance criteria. Or it can help compare performance of two software systems. It can also help identify parts of your software system which degrade its performance.

Below is a generic performance testing process :-


Identify Test Environment
Determine Performance Criteria
Plan & Design
Configure Test Environment
Implement Test Design
Run Tests
Analyze , finetune & Re-test

1. **Identify your testing environment -** Know your physical test environment, production environment and what testing tools are available. Understand details of the hardware, software and network configurations used during testing before you begin the testing process. It will help testers create more efficient tests. It will also help identify possible challenges that testers may encounter during the performance testing procedures.
2. **Identify the performance acceptance criteria -** This includes goals and constraints for throughput, response times and resource allocation. It is also necessary to identify project success criteria outside of these goals and constraints. Testers should be empowered to set performance criteria and goals because often the project specifications will not include a wide enough variety of performance benchmarks. Sometimes there may be none at all. When possible finding a similar application to compare to is a good way to set performance goals.
3. **Plan & design performance tests -** Determine how usage is likely to vary amongst end users and identify key scenarios to test for all possible use cases. It is necessary to simulate a variety of end users, plan performance test data and outline what metrics will be gathered.
4. **Configuring the test environment -** Prepare the testing environment before execution. Also, arrange tools and other resources.
5. **Implement test design -** Create the performance tests according to test design.
6. **Run the tests -** Execute and monitor the tests.
7. **Analyze, tune and retest** - Consolidate, analyze and share test results. Then fine tune and test again to see if there is an improvement or decrease in performance. Since improvements generally grow smaller with each retest, stop when bottlenecking is caused by the CPU. Then you may have the consider option of increasing CPU power.

IV. Latest Fingerprint Security System With Eye Detection

Fingerprint recognition is a popular security feature in the newer generation of smartphones and is a well-known biometric technology. Since Microsoft introducing iris recognition feature in its smartphones, there were comparisons between these two biometric traits. We will be discussing both these biometric technologies, their capabilities and security features.

Iris and fingerprint recognition both have higher accuracy, reliability and simplicity as compared to other biometric traits. These attributes make iris and fingerprint recognition perform better and a particularly promising security solution in today’s society. The process starts by capturing the images of iris and fingerprint which are then pre-processed to remove any noise effects. The distinguishing features are then extracted and matched to find similarity between both the feature sets. The matching scores that are generated from the individual recognizers are given to the decision module which decides if a person is genuine or an impostor.

EYE DETECTION

The accurate extraction and measurement of eye features is crucial to a variety of domains, including human-computer interaction, biometry, and medical research. This paper presents a fast and accurate method for extracting multiple features around the eyes: the center of the pupil, the iris radius, and the external shape of the eye. These features are extracted using a multistage algorithm. On the first stage the pupil center is localized using a fast circular symmetry detector and the iris radius is computed using radial gradient projections, and on the second stage the external shape of the eye (of the eyelids) is determined through a Monte Carlo sampling framework based on both color and shape information. Extensive experiments performed on a different dataset demonstrate the effectiveness of our approach. In addition, this work provides eye annotation data for a publicly-available database.

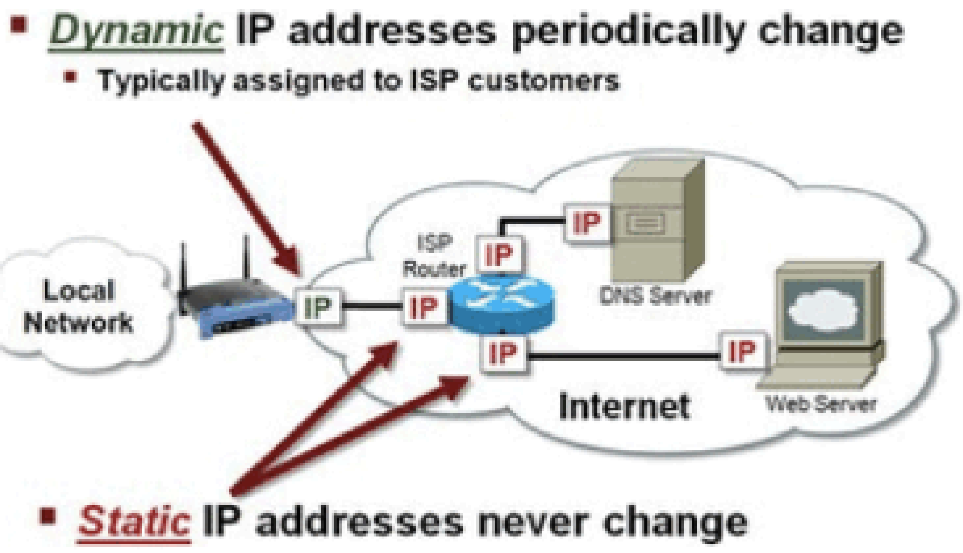
FINGERPRINT DETECTION

Fingerprints are the most common and often most reliable crime scene evidence. Since no two fingerprints are alike, crime scene investigators can rely on fingerprint impressions to pinpoint suspects of the crime. Since the emergence of fingerprint identification in the 19th century, police age over the world use fingerprint evidence to catch culprits.

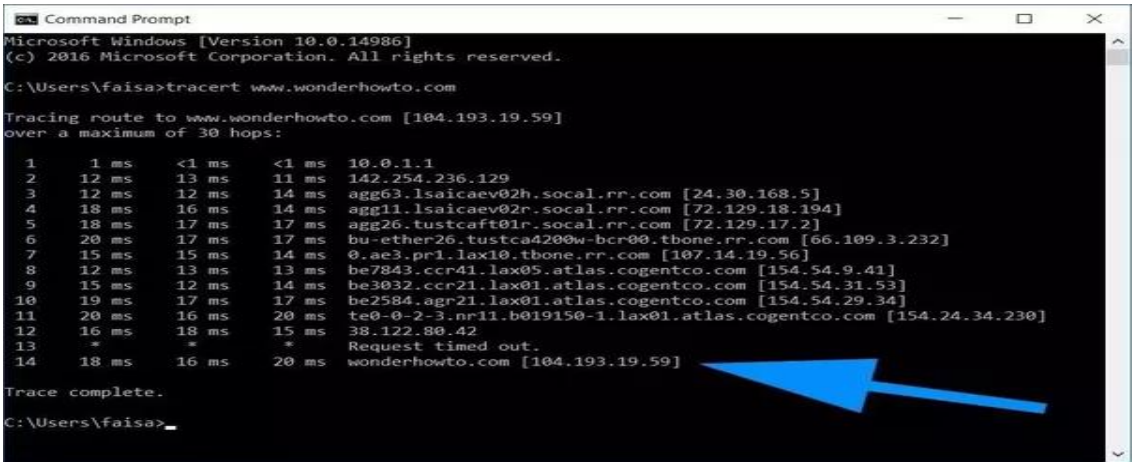
A latent fingerprint examiner handles identification processes, inclusive of taking photos of fingerprints or utilizing different methods of latent fingerprint identification in the crime scene and identifying the fingerprints by running them against FBI's Automated Fingerprint Identification System. Part of a latent print examiner's job description is to prepare reports on fingerprint evidence and methods used for identification and analysis. A latent print examiner may be asked to testify in court trials in relation to crime scene evidence procedures.

V. IP Address Tracker

We have to admit one thing, though—it is a little unnerving to realize that someone who has your IP address (or captured it at one time) has a pretty good idea of the region or city you live in. It can feel somewhat intrusive.But keep in mind that it's not as if our names and addresses are listed in some public Internet phone book that's handed out.



- Dynamic IP addresses periodically change
  - Typically assigned to ISP customers
- Static IP addresses never change



```
Microsoft Windows [Version 10.0.14986]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\faisa>tracert www.wonderhowto.com

Tracing route to www.wonderhowto.com [104.193.19.59]
over a maximum of 30 hops:

  1     1 ms    <1 ms    <1 ms  10.0.1.1
  2    12 ms    13 ms    11 ms  142.254.236.129
  3    12 ms    12 ms    14 ms  agg63.lsaicaev02h.socal.rr.com [24.30.168.5]
  4    18 ms    16 ms    14 ms  agg11.lsaicaev02r.socal.rr.com [72.129.18.194]
  5    18 ms    17 ms    17 ms  agg26.tustcaft01r.socal.rr.com [72.129.17.2]
  6    20 ms    17 ms    17 ms  bu-ether26.tustca4200w-bcr00.tbone.rr.com [66.109.3.232]
  7    15 ms    15 ms    14 ms  0.ae3.pr1.lax10.tbone.rr.com [107.14.19.56]
  8    12 ms    13 ms    13 ms  be7843.ccr41.lax05.atlas.cogentco.com [154.54.9.41]
  9    15 ms    12 ms    14 ms  be3032.ccr21.lax01.atlas.cogentco.com [154.54.31.53]
 10    19 ms    17 ms    17 ms  be2584.agr21.lax01.atlas.cogentco.com [154.54.29.34]
 11    20 ms    16 ms    20 ms  te0-0-2-3.nr11.b019150-1.lax01.atlas.cogentco.com [154.24.34.230]
 12    16 ms    18 ms    15 ms  38.122.80.42
 13     *        *        *     Request timed out.
 14    18 ms    16 ms    20 ms  wonderhowto.com [104.193.19.59]

Trace complete.

C:\Users\faisa>_
```

In fact, the Internet is very anonymous in many ways. Most of the time, you give away your identity by establishing relationships, business and personal, online.So, if you don't want someone zeroing in on your IP address, make it a habit not to be so quick to give up your name and address online, especially to people or companies you don't know very well.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see ‘Bug Search Tool’ and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.
Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

RESTRICTIONS FOR IP SOURCE TRACKER

Packets Can Be Dropped for Routers

IP source tracking is designed to track attacks against hosts. Packets can be dropped if the line card or port adapter CPU is overwhelmed. Therefore, when used to track an attack against a router, IP source tracking can drop control packets, such as Border Gateway Protocol (BGP) updates.

Engine 0 and 1 Performances Affected on Cisco 12000 Series

There is no performance impact for packets destined to nontracked IP addresses on Engine 2 and Engine 4 line cards because the IP source tracker affects only tracked destinations. Engine 0 and Engine 1 performances are affected because on these engines all packets are switched by the CPU.

VI. Administration Progress

A website coordinator administers a company's website by keeping content and design current. Coordinators who have experience with design software, as well as in marketing, design and communications, are often sought out by employers. Although not a requirement, a degree in web design, communications, or journalism might be useful when seeking employment.

ESSENTIAL INFORMATION :-

A website coordinator, sometimes called a website administrator or a webmaster, works to maintain a cohesive design for a company's website and increase its online marketing presence. Successful coordinators need a thorough knowledge of website design practices and should keep up with trends in marketing, including social networking strategies. Employers often look for someone with experience in marketing, design or communications, and the candidates must be proficient in using design software. While not always required, an undergraduate degree in journalism, Web design or communication can be useful.

JOB DESCRIPTION :-

A website coordinator works as an administrator to a company's websites, managing content, maintaining Web design and answering consultation questions. Most work 40-hour work weeks during regular business hours, though some hold contract positions and make their own hours. Good attention to detail, creativity and knowledge of information technology are all highly sought-after qualities in a website coordinator.

JOB DUTIES :-

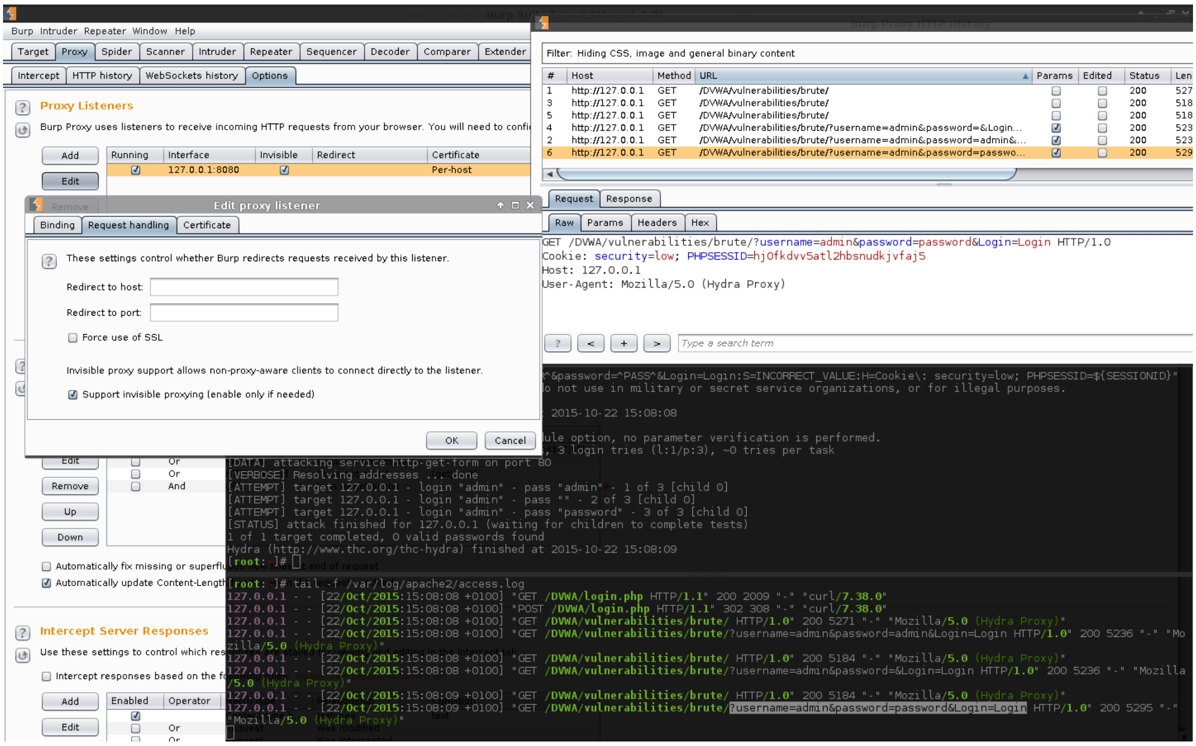
A website coordinator is in charge of publishing content, maintaining continuity of themes, designing layout, streamlining navigation and increasing online presence to potential customers. They must have knowledge of search engine analytics to maximize traffic to websites. Website coordinators should be familiar with publishing and design software in order to maintain client websites. They must also have strong communication skills and an up-to-date awareness of marketing techniques.

JOB REQUIREMENTS:-

To qualify for most positions, those interested in becoming website coordinators need to gain experience in marketing, communications and design. Though not required, an associate's or bachelor's degree in a related field, such as journalism, Web design or communications, can help increase employability and provide a solid background in technical skills. Courses could include communication studies, psychology, computer programming and sociology.

Salary information and advancement opportunities:- Most website coordinators can advance with experience to a more managerial position, depending on their employer. For example, a website coordinator can advance to an editorial position in which they manage other Web coordinators. According to *PayScale.com*, the national median salary of a website coordinator as of 2016 was $52,791. Those interested in the technical side of websites might pursue additional education in software design and database management in order to become Web developers.

Website coordinators update and publish content on a company's website, making sure to always adhere to that site's style and theme. Increasing traffic is another important responsibility in this position, so website coordinators need to have a solid grasp of search engine analytics. Postsecondary education in a similar field may be required by some employers.



Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender
Intercept HTTP history WebSockets history Options
Add
Edit
Remove
Up
Down
Request Response
Raw Params Headers Hex
OK
Cancel

Proxy Listeners

Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to confi

Running	Interface	Invisible	Redirect	Certificate
☑	127.0.0.1:8080	☑		Per-host

Edit proxy listener

Binding | Request handling | Certificate

These settings control whether Burp redirects requests received by this listener.

Redirect to host:

Redirect to port:

□ Force use of SSL

Invisible proxy support allows non-proxy-aware clients to connect directly to the listener.

☑ Support invisible proxying (enable only if needed)

□ Automatically fix missing or superflu

☑ Automatically update Content-Length

Intercept Server Responses

Use these settings to control which res

□ Intercept responses based on the f

Enabled	Operator
☑	
□	Or

Filter: Hiding CSS, image and general binary content

#	Host	Method	URL	Params	Edited	Status	Len
1	http://127.0.0.1	GET	/DVWA/vulnerabilities/brute/	□	□	200	527
3	http://127.0.0.1	GET	/DVWA/vulnerabilities/brute/	□	□	200	518
5	http://127.0.0.1	GET	/DVWA/vulnerabilities/brute/	□	□	200	518
4	http://127.0.0.1	GET	/DVWA/vulnerabilities/brute/?username=admin&password=&Login...	☑	□	200	523
2	http://127.0.0.1	GET	/DVWA/vulnerabilities/brute/?username=admin&password=admin&...	☑	□	200	523
6	http://127.0.0.1	GET	/DVWA/vulnerabilities/brute/?username=admin&password=passwo...	☑	□	200	529

```
GET /DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.0
Cookie: security=low; PHPSESSID=hj0fkdvv5atl2hbsnudkjvfaj5
Host: 127.0.0.1
User-Agent: Mozilla/5.0 (Hydra Proxy)
```

```
^&password=^PASS^&Login=Login:S=INCORRECT_VALUE:H=Cookie\: security=low; PHPSESSID=${SESSIONID}"
o not use in military or secret service organizations, or for illegal purposes.

 2015-10-22 15:08:08

ule option, no parameter verification is performed.
, 3 login tries (l:1/p:3), ~0 tries per task
[DATA] attacking service http-get-form on port 80
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "admin" - 1 of 3 [child 0]
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "" - 2 of 3 [child 0]
[ATTEMPT] target 127.0.0.1 - login "admin" - pass "password" - 3 of 3 [child 0]
[STATUS] attack finished for 127.0.0.1 (waiting for children to complete tests)
1 of 1 target completed, 0 valid passwords found
Hydra (http://www.thc.org/thc-hydra) finished at 2015-10-22 15:08:09
[root:~]# 
```

```
[root:~]# tail -f /var/log/apache2/access.log
127.0.0.1 - - [22/Oct/2015:15:08:08 +0100] "GET /DVWA/login.php HTTP/1.1" 200 2009 "-" "curl/7.38.0"
127.0.0.1 - - [22/Oct/2015:15:08:08 +0100] "POST /DVWA/login.php HTTP/1.1" 302 308 "-" "curl/7.38.0"
127.0.0.1 - - [22/Oct/2015:15:08:08 +0100] "GET /DVWA/vulnerabilities/brute/ HTTP/1.0" 200 5271 "-" "Mozilla/5.0 (Hydra Proxy)"
127.0.0.1 - - [22/Oct/2015:15:08:08 +0100] "GET /DVWA/vulnerabilities/brute/?username=admin&password=admin&Login=Login HTTP/1.0" 200 5236 "-" "Mo
zilla/5.0 (Hydra Proxy)"
127.0.0.1 - - [22/Oct/2015:15:08:08 +0100] "GET /DVWA/vulnerabilities/brute/ HTTP/1.0" 200 5184 "-" "Mozilla/5.0 (Hydra Proxy)"
127.0.0.1 - - [22/Oct/2015:15:08:08 +0100] "GET /DVWA/vulnerabilities/brute/?username=admin&password=&Login=Login HTTP/1.0" 200 5236 "-" "Mozilla
/5.0 (Hydra Proxy)"
127.0.0.1 - - [22/Oct/2015:15:08:09 +0100] "GET /DVWA/vulnerabilities/brute/ HTTP/1.0" 200 5184 "-" "Mozilla/5.0 (Hydra Proxy)"
127.0.0.1 - - [22/Oct/2015:15:08:09 +0100] "GET /DVWA/vulnerabilities/brute/?username=admin&password=password&Login=Login HTTP/1.0" 200 5295 "-"
"Mozilla/5.0 (Hydra Proxy)"
```

VII. User Progress

CYBER SECURITY IS CHANGING THE WEB DESIGN INDUSTRY:-

The industry of web design, I think of the many talented people responsible for populating the internet with information over the past couple of decades. But our job is never done! From continual refinement of responsive design, to developing content worthy of Google's latest search strategy; our jobs as designers and web managers is an ever-evolving landscape. In today's market it is essential to stay current with technology and the threats targeting those we serve and those who search online. Without constant awareness and action by our peers in technology, cybercriminals will continue to challenge our time, patience, and livelihood.

WEBSITES HAVE BECOME KEY POINT OF ATTACK FOR CYBERCRIMINALS:-

While many believe that email phishing is a key entry point for most cyber criminals, it has become apparent that they are often using an unsuspecting website to hide their activity of malware designed collect valid emails and launch other criminal schemes. While some argue that nothing is hack-proof; content management systems built on open-source code have enabled the unsecure environment we now reside. It goes without saying that sharing code saves time; but is it worth the longer-term cost?

Let's explore the leading CMS platform, WordPress. It is an easy-to-use interface making it popular among novice developers and DIY professionals, but it is often a prime target of hackers who specifically build robotic scripts designed to quickly search through the openly published source files looking for vulnerabilities. Technical web designers (those who know how to customize the code and apply advanced security settings) understand that keeping current on updates and effectively managing a recovery plan for the sites you have created has become a time-consuming task and one that is raising the overall cost of website management. However, the millions without some technical skillset, have likely already become an unsuspecting victim to one of the many ongoing threats facing the WordPress community.

A prime example of how open-source code created a breeding ground for a cyberattack happened in early 2017 when one of 20 hacking groups launched a digital turf war on WordPress by discovering a flaw found in their REST API script. A wide-spread attack impacted roughly 1.5 million pages of WordPress sites1 across 39,000 unique domains in a matter of days as reported by security plugin developers WordFence and Sucuri. Keep in mind that only 1.5 million of the 24 billion pages running WordPress2 are protected by these firewall applications.

INSURANCE COMPANIES ARE LOOKING AT WHO TO BLAME FOR THE INCREASE IN COMMERCIAL CLAIMS

From the outside looking in, the internet landscape is under attack, but who is to blame? This is a question many insurance companies are beginning to ask3 as their costs to cover cyber-attacks on commercial policies continue to rise.

Looking at a big picture, here are some general facts to consider…

- According to the Small Business Administration, there are approximately 28 million small businesses in America which account for approximately 54% of all sales in the country. [4]
- In a 2017 report by Kaspersky Lab, the average cost for a data breach against a small and medium-sized business in North America was $117,000.[5]
- An article published in 2017 by INC Magazine, referenced a presentation made at the NASDAQ by Michael Kaiser, the Executive Director of the National Cyber Security Alliance, who stressed concerns about the attack on Small Business and that such attacks are expected to continually rise because of their (the small business professional's) lack of awareness of the pending risks.[6]
- A 2016 study performed by Ponemon Institute LLC and Keeper Security revealed that the number one type of cyber attack targeting small and medium sized businesses was through a web-based attack with the web server being the most vulnerable entry point.[7]
- That same study by Ponemon Instutute cited "negligent employees or contractors" as the root cause of the data breach. [7]

When the Insurance companies follow the facts, who do you think they will turn to recover their loss?

- Will it be the random person who pointed out their vulnerability by successfully holding their web presence ransom? – likely not. That person is too difficult for them to track.
- Will they blame the contractor who their customer hired to create their website? – Yes!

VIII. Locking Accounts

- **Should user account be locked after 'three' times of failed logins.**
- **Account lockout policy**
- **Sidebar: Using CAPTCHAS**
- **Strong passwords**

The most obvious way to block brute-force attacks is to simply lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator. However, account lockout is not always the best solution, because someone could easily abuse the security measure and lock out hundreds of user accounts. In fact, some Web sites experience so many attacks that they are unable to enforce a lockout policy because they would constantly be unlocking customer accounts.

The problems with account lockouts are:

An attacker can cause a denial of service (DoS) by locking out large numbers of accounts.Because you cannot lock out an account that does not exist, only valid account names will lock. An attacker could use this fact to harvest usernames from the site, depending on the error responses.An attacker can cause a diversion by locking out many accounts and flooding the help desk with support calls.

An attacker can continuously lock out the same account, even seconds after an administrator unlocks it, effectively disabling the account.Account lockout is ineffective against slow attacks that try only a few passwords every hour.Account lockout is ineffective against attacks that try one password against a large list of usernames.Account lockout is ineffective if the attacker is using a username/password combo list and guesses correctly on the first couple of attempts.

Powerful accounts such as administrator accounts often bypass lockout policy, but these are the most desirable accounts to attack. Some systems lock out administrator accounts only on network-based logins.

Even once you lock out an account, the attack may continue, consuming valuable human and computer resources.Account lockout is sometimes effective, but only in controlled environments or in cases where the risk is so great that even continuous DoS attacks are preferable to account compromise. In most cases, however, account lockout is insufficient for stopping brute-force attacks. Consider, for example, an auction site on which several bidders are fighting over the same item. If the auction Web site enforced account lockouts, one bidder could simply lock the others' accounts in the last minute of the auction, preventing them from submitting any winning bids. An attacker could use the same technique to block critical financial transactions or e-mail communications.

Password Authentication Delay: C#

```
private void AuthenticateRequest(object obj, EventArgs ea)
 {
   HttpApplication objApp = (HttpApplication) obj;
   HttpContext objContext = (HttpContext) objApp.Context;
   // If user identity is not blank, pause for a random amount of time
   if ( objApp.User.Identity.Name != "")
     {
       Random rand = new Random();
       Thread.Sleep(rand.Next(minSeconds, maxSeconds) * 1000);
     }
 }
```

Password Authentication Delay: VB.NET

```
Public Sub AuthenticateRequest(ByVal obj As Object, ByVal ea As System.EventArgs)
 Dim objApp As HttpApplication
 Dim objContext As HttpContext
 Dim ran As Random
 objApp = obj
 objContext = objApp.Context

 ' If user identity is not blank, pause for a random amount of time
 If objApp.User.Identity.Name <> "" Then
   ran = New Random
   Thread.Sleep(ran.Next(ran.Next(minSeconds, maxSeconds) * 1000))
 End If
End Sub
```

IX. Hacker List

- **List will send with time and date**
- **To administrators mail**
- **To individual system users**

If anecdote of exploiter is being hacked with the purpose of possibilities searching the password by the plodder, when the exploiter login the hacker list displays the detail about the plodder with IP address. The hacker list sends to the exploiter mail. The hacker list visible the IP address with hacking time.

The software will send automatically the hackers list with IP address,date and time to administrators e-mail and also to his/her mobile number.

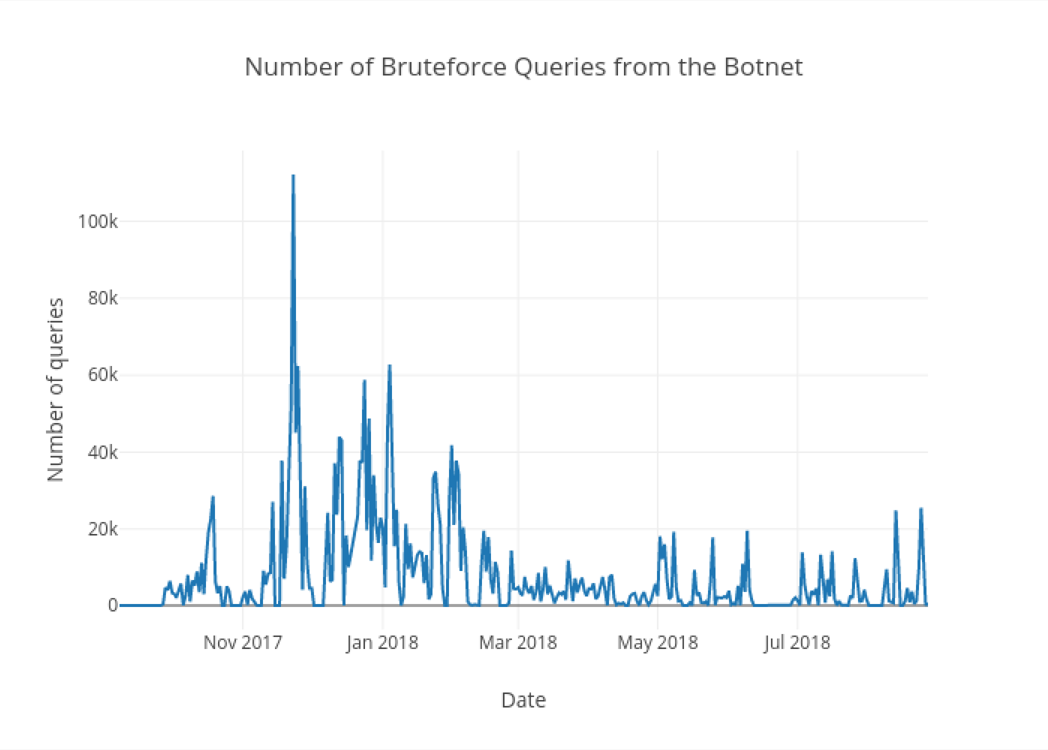
Also the software will send automatically the hackers list with IP address,date and time to individual user’s e-mail and also to his/her mobile number.

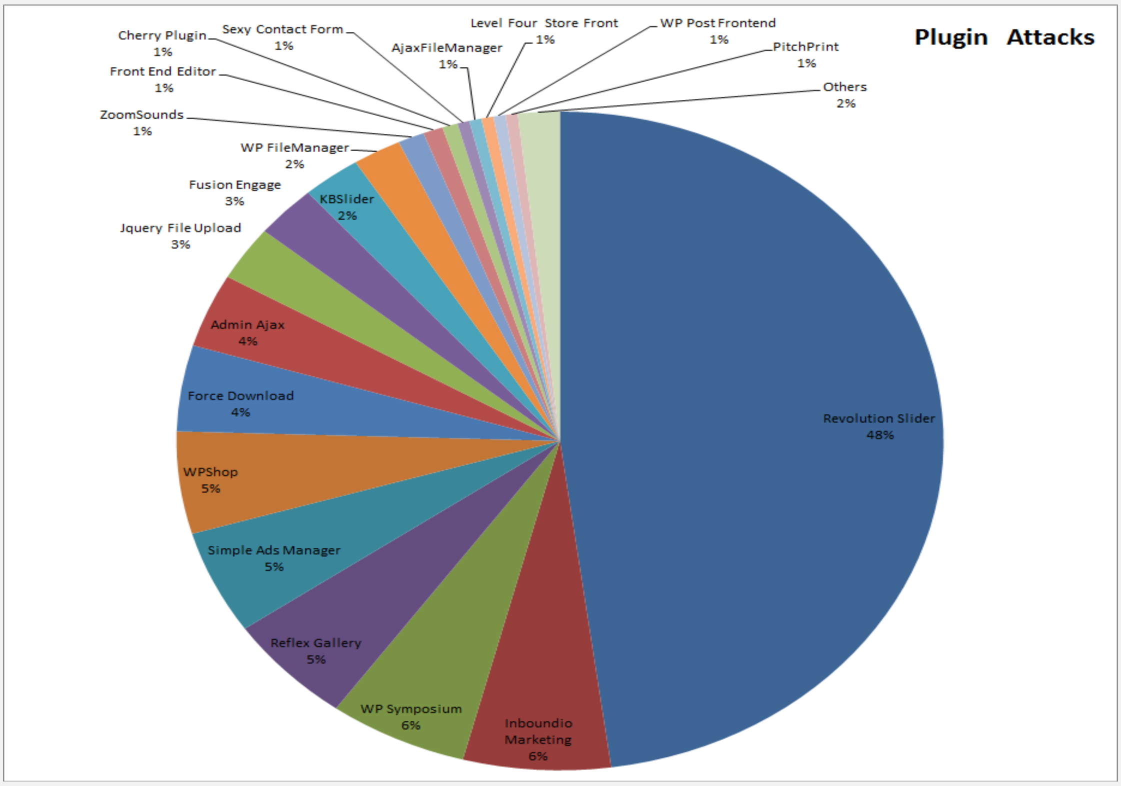
Administrator owns the overall determination of controls, setting of major objectives, and the identification of general purposes, guidance, leadership & control of the efforts of the groups towards some common goals. Admin also have the rights to restricts the users and give the access justices to the user to register their details.In this module, include the user registration details. The username and mail id is already available or not checking this process. The user only accesses the mail within the organization. The hackers hacking company details that time will send the mail to your id and password is hacking.

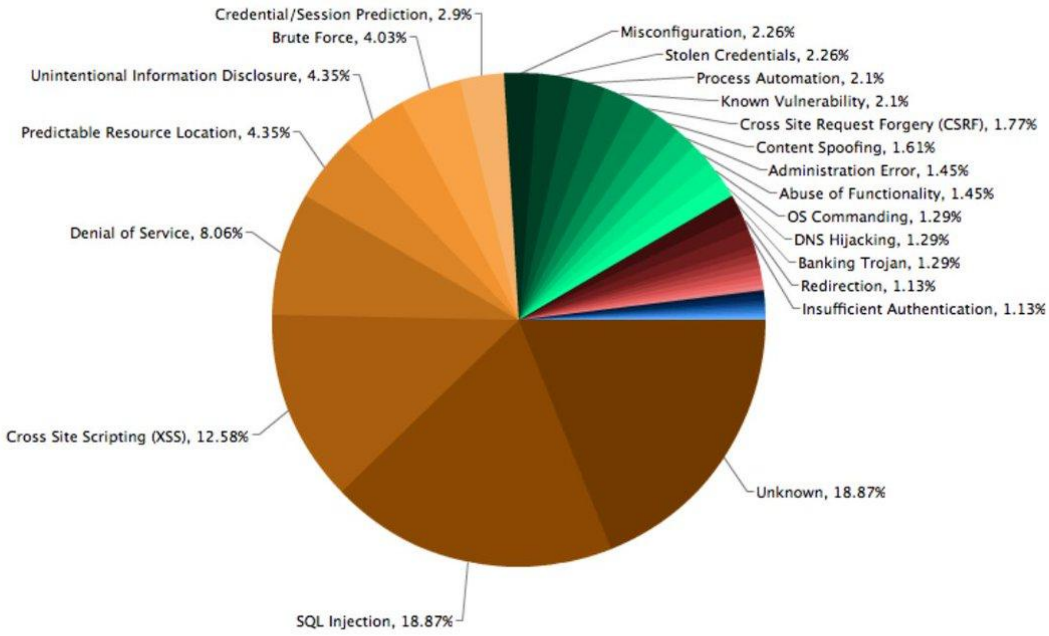
X. Results And Discussion

A brute force attack is a trial-and-error method used to decode sensitive data. The most common applications for brute force attacks are cracking passwords and cracking encryption keys (keep reading to learn more about encryption keys). Other common targets for brute force attacks are API keys and SSH logins.What differentiates brute force attacks from other cracking methods is that brute force attacks don’t employ an intellectual strategy, they simply try using different combinations of characters until the correct combination is found. This is kind of like a thief trying to break into a combo safe by attempting every possible combination of numbers until the safe opens.The biggest advantages of brute force attacks is that they are relatively simple to perform and, given enough time, they always work. Every password-based system and encryption key out there can be cracked using a brute force attack. In fact the amount of time it takes to brute force into a system is a useful metric for gauging that system’s level of security.

On the other hand, brute force attacks are very slow, as they may have to run through every possible combination of characters before achieving their goal. This sluggishness is compounded as the number of characters in the target string increases (a string is just a combination of characters). For example, a four-character password takes significantly longer to brute force than a three-character password, and a five-character password takes significantly longer than a four-character password. Once character count is beyond a certain point, brute forcing a properly randomized password becomes unrealistic.







XI. Conclusion

My software is very reliable and useful to all web developers and web developing companies.It is easy to install. Administrator can control all over the computers in one hand. Hackers list with IP address, time and date will be send to admins e-mail. If any one try to hack any user computer thrise, individual computer will be locked. Then it will unlocked by only using admin system.

References

[1]. Adleman, Leonard M.; Rothemund, Paul W.K.; Roweis, Sam; Winfree, Erik (June 10–12, 1996). On Applying Molecular Computation To The Data Encryption Standard. Proceedings of the Second Annual Meeting on DNA Based Computers. Princeton University.

[2]. Cracking DES – Secrets of Encryption Research, Wiretap Politics & Chip Design. Electronic Frontier Foundation. ISBN 1-56592-520-3.

[3]. Burnett, Mark; Foster, James C. (2004). Hacking the Code: ASP.NET Web Application Security. Syngress. ISBN 1-932266-65-8.

[4]. Diffie, W.; Hellman, M.E. (1977). "Exhaustive Cryptanalysis of the NBS Data Encryption Standard". Computer. **10**: 74–84. doi:10.1109/c-m.1977.217750.

[5]. Graham, Robert David (22 June 2011). "Password cracking, mining, and GPUs". erratasec.com. Retrieved 17 August 2011.

[6]. Ellis, Claire. "Exploring the Enigma". Plus Magazine.

[7]. Kamerling, Erik (2007-11-12). "Elcomsoft Debuts Graphics Processing Unit (GPU) Password Recovery Advancement". Symantec.

[8]. Kingsley-Hughes, Adrian (2008-10-12). "ElcomSoft uses NVIDIA GPUs to Speed up WPA/WPA2 Brute-force Attack". ZDNet.

[9]. Landauer, L (1961). "Irreversibility and Heat Generation in the Computing Process". IBM Journal of Research and Development. **5**. doi:10.1147/rd.53.0183.

[10]. Paar, Christof; Pelzl, Jan; Preneel, Bart (2010). Understanding Cryptography: A Textbook for Students and Practitioners. Springer. ISBN 3-642-04100-0.

[11]. Reynard, Robert (1997). Secret Code Breaker II: A Cryptanalyst's Handbook. Jacksonville, FL: Smith & Daniel Marketing. ISBN 1-889668-06-0. Retrieved 2008-09-21.

[12]. Ristic, Ivan (2010). Modsecurity Handbook. Feisty Duck. ISBN 1-907117-02-4.

[13]. Viega, John; Messier, Matt; Chandra, Pravir (2002). Network Security with OpenSSL. O'Reilly. ISBN 0-596-00270-X. Retrieved 2008-11-25.

[14]. Wiener, Michael J. (1996). "Efficient DES Key Search". Practical Cryptography for Data Internetworks. W. Stallings, editor, IEEE Computer Society Press.

[15]. "Technical Cyber Security Alert TA08-137A: Debian/Ubuntu OpenSSL Random Number Generator Vulnerability". United States Computer Emergency Readiness Team (CERT). 2008-05-16. Retrieved 2008-08-10.

[16]. "NSA's How Mathematicians Helped Win WWII". National Security Agency. 15 Jan 2009.

Sony Jacob. " Testing By Application Software On-Brute Force Attack On Open Functionality Secured." IOSR Journal of Computer Engineering (IOSR-JCE) 20.6 (2018): 41-51.