HCTL Open International Journal of Technology Innovations and Research (IJTIR)
http://ijtir.hctl.org
Volume 14, April 2015
e-ISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3

Securing Web Services and Applications using Captcha Security

Sandeep Mahato[1], Varun Prakash Saxena[2], Raj Gaurav Mishra[3]

sandeep.mahato94@gmail.com

Abstract

There are many services in the internet including Email, search engine, social networking are provided with free of cost. To access these web services users have to register regarding the websites. During registration, some intruders or attackers write malicious programs that waste the website resources by making automatic false enrolments which are called as bots. Security researchers developed many techniques to prevent from accessing web resources by these bots. This paper describes about web security and importance. It also describes different methods and ways to implement web security.

Keywords
Web Security, CAPTCHA Security, BOT.

Introduction

Internet is usually a worldwide system of interconnected networks which uses TCP/IP network protocol to reach billion of users. The Internet changed our life enormously. The influence in the Internet on society is sort of impossible in summary properly as it would be so that all-encompassing. Though a lot of the globe, unfortunately, still does not have Access to the internet. To see it within the most general of terms, the net has definitely made many areas of today's modern life much easier. From paying your bills and buying clothes to researching and learning interesting things, from keeping talking to website visitors to meeting new people, all of these products have become far easier on account of the Internet.

[1]Central University Jharkhand Mtech (CSMC) (Sandeep Mahato).
[2]Govt.Women Engg College Ajmer. (V.P saxena), Email: varunsaxena82@gmail.com
[3]The ICFAI University, Dehradun (Raj Gaurav Mishra), Email: raj.g.mishra@gmail.com

"Web security" is relative and contains two components, one internal and something public. Your relative security is high in case you have few network resources of financial value, your company and site aren't controversial the slightest bit, your network is placed with tight permissions, your web server is patched up to date with all settings done properly, your applications online server are all patched and updated, as well as your website code is finished to high standards. Your web security is actually comparatively lower but if your company has financial assets like updated or identity information, in case your web page content is controversial, your servers, applications and site code are complex or old and so are maintained by an underfunded or outsourced IT department. All IT departments are budget challenged and tight staffing often creates deferred maintenance conditions that play to the hands of any who wish to challenge your web security.

Web Server Security

The earth's most secure web server would be the one that's put off. Simple, bare-bones web servers who have few open ports and few services on those ports include the next most convenient thing. Powerful and flexible applications are needed to run complex sites that are naturally more susceptible to web security issues.

Any system with multiple open ports, multiple services and multiple scripting languages is vulnerable due to the fact they have countless points of admission to watch. If the system have been correctly configured as well as your IT staff have been very punctual about applying security patches and updates your risks are mitigated. Then there is an few the applications you're running. These too require frequent updates. And last there is the website code itself.

Web Site Code and Web Security:

Your website undoubtedly provides some ways of communication using its visitors. In each and every place that interaction is quite possible you have a potential web security vulnerability. Websites often invite people to:

1. Load a brand new page containing dynamic content
2. Visit a product or location
3. Submit a contact form
4. Search the website content
5. Start using a shopping cart software package
6. Create an account
7. Logon a great account

Every time noted above your site visitor is effectively sending a command to or through your web server - most likely to a database. In each possibility to communicate, like a form field, search field or blog, correctly written code lets only a very narrow selection of commands or information types to pass through - in or out. This can be perfect for web security. However, these limits will not be automatic. It will require well trained programmers a large amount of time to write code that permits all expected data to pass through and disallows all unexpected or possibly damaging data. Code with your site

comes from the various programmers, most of whom be employed by alternative vendors. Most of that code now has wrinkles, perhaps very old. Your web site could possibly be running software from seven sources, and your web site designer whilst your webmaster has each produced more code that belongs to them, or made revisions to another's code that may have altered or eliminated previously established web security limitations.

Complement which the software that could are purchased in the past and which is not in current use. Many servers have accumulated applications which have been no more available is actually which nobody on your current staff is familiar. This code is frequently quite difficult to uncover, is around as valuable just as one appendix and possesses not been used, patched or updated for many years - however it could be precisely what a hacker is looking for! [3]

Why Web based security is needed?

Internet based security is needed for avoiding various web threats. Some threats are

1. Phishing: Among the less advanced, nevertheless effective threats is phishing. The term identifies attacks the spot that the victim is made to believe that she / he is with a legitimate website, substantially fact it is just a copy of the real one. This attack depends on the belief that anyone can make their very own website and any web site looks as with other. An actual world example is a fake ATM that's put in the middle of an busy mall. There would be hardly any signs showing victims that it must be not really a real ATM – until nothing happens. Similarly, within a phishing attack victims could imagine that they're on their own bank's website, and as a consequence do not think about using pin numbers as requested. This attack seriously isn't on a banking systems. Phishing attacks are actually seen to target company email websites (webmail), public email websites (like Gmail) and popular sites like Amazon or eBay.

   Users can identify a phishing website in many ways. The first is to check out the URL. Another effective prevention strategy is to not ever follow links by email but to type them in or use bookmarks. However , not foolproof, they allow it to become tougher for attackers to journey scam.

2. Internet browser exploits: Cybercriminals in addition have fix websites that exploit security holes inside internet browser. It lets them gain access with no victim's knowledge. Web browsers are complex software. They have to handle various file formats, like images, sound and HTML, Java script and also a multitude of other technologies. All of these features increase the attack surface of the internet browser, thus making the technology relatively weak from your security standpoint. Yet this same functionality is why it so useful. For example, both Ie and Firefox experienced their great number of security vulnerabilities. Some security flaws might be exploited to permit people to remotely compromise that user account. This typically implies that a prosperous attacker who exploits the net browser gets usage of private emails, sensitive documents and anything that that this user running the internet browser has having access to.

3. Vacation add-ons: A lot of websites require the usage of vacation add-ons for instance Adobe Flash player and Acrobat Reader. Those two trusted products are getting to be a favourite target for cybercriminals. Weight loss administrators and home users update their machines using the latest security updates and patches for his or her browsers, as well as the chance to automate the process, it might be harder to work with browsers as a possible attack vector.

   However, vehicles might be updating their browser software, it is additionally factual that lots of people forget to update third party add-ons just like the Flash player. Just last year a number of malware “within the wild” (around on the Internet) have exploited the PDF file format, Adobe Acrobat, Flash, a number of ActiveX components and Java. These alternative party add-ons are utilized to push users along with other websites that were compromised.

4. Hybrid attack: While the web offers much greater scope for attackers, email still remains a powerful tool. Combined with the web, the threats not only multiply though the risk that the user becomes a willing prey is quite high. One common trick is with current news events to spread malware spam. Emails purporting to provide exclusive news, videos or files are popular online traps to spread out dangerous attachments or perhaps be redirected to infected or fake websites. [2]

What is a Bot attack?

A botnet is really a bunch of Internet-connected programs communicating along with other similar programs as a way to perform tasks. This is often as mundane as keeping power over a broadband Relay Chat (IRC) channel, or it could be helpful to send spam email or be involved in distributed denial-of-service attacks.

What is a Bot (or Zombie)?

A 'bot' is a type of malware that enables an attacker to get complete control within the affected computer. Computers that are contaminated with a 'bot' usually are known as 'zombies'. You can find literally hundreds of thousands of computers on the web which might be contaminated with some type of 'bot' and don't even realize it. Attackers will be able to access lists of 'zombie' PC's and activate these to help execute DoS (denial-of-service) attacks against Sites, host phishing attack Internet sites or distribute a large number of spam email messages. Should anyone trace the attack time for its source, they will find an unwitting victim as opposed to the true attacker.

Identifying a 'Zombie' Computer

'Bots' are great at hiring inside shadows of this computer to make sure they will not be noticed. In the event you could easily detect that something was running on your pc, you'd probably quickly remove or disable it. They often times have file and process names which have been similar, or even identical, to normal system file names and processes so that users won't think even though they do see them. You may notice anything odd, as if

your computer appears to relax or crash for no apparent reason, you could suspect that there is some malware running in the shadows causing a problem. There's some other reasons for symptoms like those likewise though. Scan your personal computer with current versions of antivirus and anti-spyware software to detect any known malware. [4]

What are the possible ways of implementing Web-based Security?

There are different possible ways of implementing Web-based Security, some of them are discussed below:

1. Web Security Defence Strategy: There are two techniques for finding excellent security. On one we would assign all of the resources required to maintain constant attentive to new security issues. we might ensure that all patches and updates are carried out at one time, have got all of the existing applications reviewed for correct security, be sure that only security knowledgeable programmers will deliver with your site and have absolutely their work checked carefully by security professionals. You would also maintain a good firewall, antivirus protection and run IPS/IDS.
   Our other option is to use an online scanning means to fix try out your existing equipment, applications and website code to discover in case a KNOWN vulnerability actually exists. While firewalls, antivirus and IPS/IDS are all worthwhile, it can be simple logic to also lock leading door. It's much more effective to correct half-dozen actual risks compared to to leave them constantly in place and try to build higher and better walls around them. Network and site vulnerability scanning is regarded as the efficient security investment coming from all.
2. Web Security Using a Website Security Audit: Healthy defence against a attack on our website is always to regularly scan a competently setup domain that is certainly running current applications and whose website code was done well. Internet site testing, often known as web scanning or auditing, is really a hosted service furnished by Beyond Security called WSSA - Web page Security Audit. This particular repair requires no installing software or hardware and it is done without any interruption of web services.

   WSSA can explain to you its entire database that could reach over $ 10 , 000 vulnerabilities which enable it to report on which are present and better yet, look into the thousands which aren't. To be able data on hand we are able to address your actual web security vulnerabilities and, when handled, realize that our site is very clear of known issues regardless of what updates and patches are already done and what condition our code is or what unused code may reside, hidden, on our site or web server.
   Then, WSSA is usually run using regularly which means that your site are going to be tested against new vulnerabilities as they become known and offer you with solid data whether or not action is vital, needed or low priority. We will even be alerted if new code have been put into your website which is insecure, a different port continues to be opened that's unexpected, or maybe a new service may be loaded and started that may present a chance to burglary.
   In complex, large systems it may be that daily web scanning would be the Best way to make sure that none of the many changes designed to site code or by

using an application could possibly have opened an opening with your carefully established security perimeter. [5]

3. Network-based Security: Network-Based Security offers multiple, complementary services to help you protect our enterprise internally. These layers work in conjunction with endpoint computer anti-malware software and internal company firewalls to intercept diverse threats.

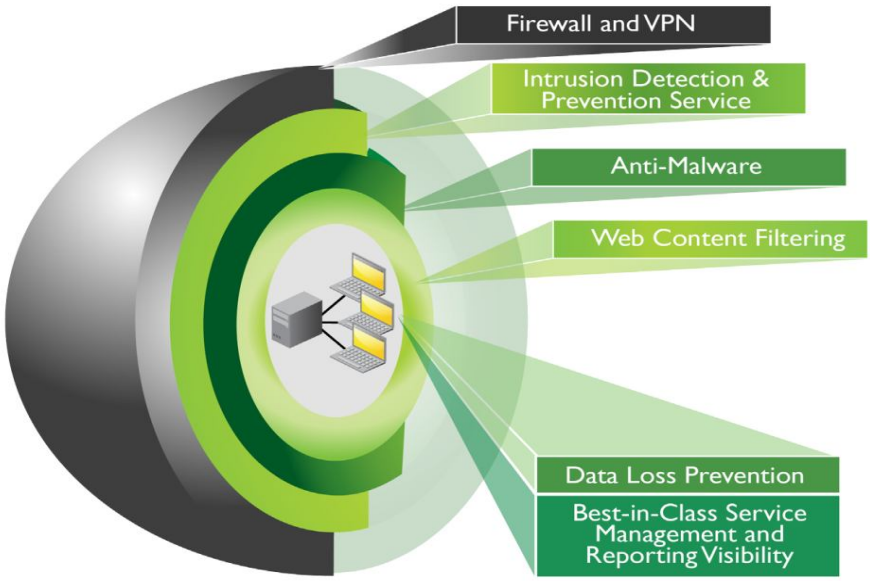

Figure 1 Network security layers

4. Captcha Based Web and Application Security: A CAPTCHA (Completely Automated Public Turing test to share with Computers and Humans Apart) is a challenge-response test accustomed to decide if an individual is human you aren't. Computers cannot decode the distorted words within a CAPTCHA easily, while humans can simply decipher the writing. Inside most frequent form of CAPTCHA user obtains letters of a distorted image. Next the user is asked to solve the CAPTCHA simply by entering the right characters. By definition CAPTCHAs are fully automated, it requires little human maintenance. An excellent CAPTCHA will have two characteristics like usability and security. Security means the strength for preventing the variant attacks, while usability means the user friendliness of the CAPTCHA. It's alias human Interactive Proof (HIP) and based upon AI. Captcha can be a program that protects websites from web-bots by generating tests that computer cannot pass but human can pass. CAPTCHA is essentially used as a defence against these malicious programs like Bot. Now daily's for web security we are using different style of captcha.

(CAPTCHAs) at the moment are almost standard security mechanisms for defending against Undesirable and malicious bot programs online. CAPTCHAs generate and grade tests that a lot of humans can pass but current computer programs can't. It is additionally often known as Human Interaction Proofs (HIPs).It a hardship on someone to write a computer program that could pass test generated by CAPTCHA even if they understand precisely how Captcha works. Captcha are occasionally called "reverse Turing tests":

since they are meant to allow some type of computer to view if a remote client is human you aren't. CAPTCHAs are exactly like Turing test.

1. Turing Test: In original Turing test, an individual judge was permitted to ask a number of inquiries to two players, one of these was computer and other a human being. Both players pretended to become a persons and the judge has to separate them.

2. Reverse Turing Test: In reverse Turing test Judge is often a CAPTCHA program & participant is user or computer if user passes CAPTCHA, he or she is human if user fails, it's a machine. If people desire to join a free email service, before the guy can submit web form; he first has got to pass an exam. Test is simple. For human, the exam ought to be easy and easy. Captcha are sometimes called “reverse Turing tests”: since they're intended to allow a computer to determine if a remote client is human or not. An excellent CAPTCHA should not only be human friendly but also robust enough to resist computer programs that attackers email automatically pass CAPTCHA tests.

A Captcha can be a cryptographic protocol whose underlying hardness assumption will depend on an AI problem. The AI problems handle the benefit of humans in sensory processing. Logic problems are also suggested like a basis for captchas these present similar difficulties, as generation looks like it's difficult. Recent progress in AI has yielded programs which solve these complaints with very high success probability, exceeding that surrounding humans. Cryptography, can be very ideal for the progress of algorithmic development.

Why do we need a Captcha?

The captcha is often a visual or audio challenge towards user in order to avoid bots and automated scripts from accessing the services protected because of it. It really is valuable for: forums looking to prevent spambots/adbots from joining and protecting downloads from automated access by bots (that is not really a security risk in itself, but a bandwidth drain).

A CAPTCHA will not provide some other form of security, it only provides defense against bots and the rate limiting that include it. A CAPTCHA is really a program that protects websites against bots by generating and grading tests that humans can pass but current computer programs cannot. One example is, humans can read distorted text as the one shown below, but current computer programs can't.

CAPTCHAs have several applications for practical security, including (but is not limited by): Preventing Comment Spam in Blogs, Protecting Website Registration .Protecting Email Addresses From Scrapers. Online Polls, Preventing Dictionary Attacks, Internet search engine Bots, Worms and Spam.

Types of Captcha

1. **Text based Captcha**: These are generally an easy task to implement. The most convenient yet novel approach would be to present anyone with a few questions which a human user can solve. Gimpy: Created by Yahoo and CMU Accumulates 10 random words from dictionary and distorts, fills with noise User has to recognize at least 3 words If user is correct, he's admitted EZ-Gimpy: A modified version of Gimpy Yahoo used this version in Messenger Has only 1 random string of characters Not just a dictionary word, so not at risk of dictionary attack A bad implementation, already broken by OCRs.

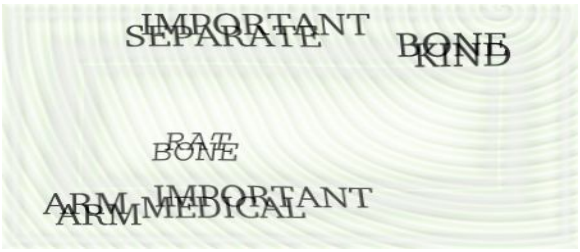

Figure 2 Gimpy and EZ Gimpy

Advantages of Text-based images:

1) Text-based captcha is straightforward to implement so that it's mostly found in websites.
2) Battle Text-based captcha can be used to defeat dictionary attacks.
3) Re-captcha Text-based captcha uses new dictionary words that can't read using optical character recognition

Disadvantages of Text-based images:

1) Therein type of CAPTCHAs, users have faced some problems to get in the best text or characters or letter. Following include the some reasons that confuse a persons to identify the precise text.
i. By using various lines.
ii. Utilization of various shapes.
iii. Using Multiple fonts.
iv. Font size variation.
v. By using Blurred Letters
2) Text-based CAPTCHAs can be simply broken by OCR techniques (example: Content based image retrieval).
3) The peoples which have low visibility power cannot easily pass the test.

2. **Graphic based Captcha:**
Graphic CAPTCHAs are challenges that entail pictures or objects who have getting some sort of similarity how the users ought to guess. They are visual puzzles, a lot like Mensa tests. Computer generates the puzzles and gradesthe answers, but is itself can not solve it.

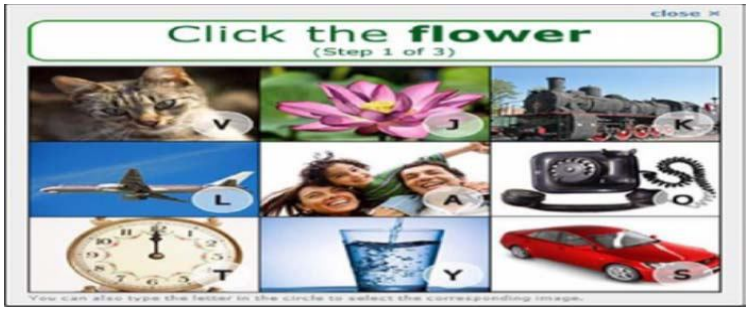

Figure 3 Graphic CAPTCHA

PIX is really a program which has a large database of labelled images. Most of these images are pictures of concrete objects (a horse, a table, a property, a flower). This program picks an object haphazardly, finds six images of these object by reviewing the database, presents these to the consumer and then asks the question "exactly what these pictures of?" Hence, writing a course that may answer the question "exactly what these pictures of?" is simple: search the database to the images presented and locate their label. Fortunately, this can be fixed. One way for PIX to become a CAPTCHA is usually to randomly distort the photographs before presenting these phones anyone, so that computer programs cannot easily search the database for that undistorted image.

Advantages of Image-based Captcha:

1) Within the text-based captcha zinc increases the safety.
2) Simple click based system so no necessity of typing.
3) Using Image-based CAPTCHA pattern recognition of image is tough AI program.

Disadvantages of Image-based CAPTCHA

1) Therein kind of CAPTCHAs, users have faced some problems to go in the precise text or characters or letter. Following are classified as the some reasons that confuse the users to recognize the correct text.
i. Using various lines.
ii. By using various shapes.
iii. Usage of Multiple fonts.
iv. Font size variation.
v. Usage of Blurred Letters
2) Text-based CAPTCHAs can be easily broken by OCR techniques (example: Content based image retrieval).
3) The peoples that contain low visibility power cannot easily pass quality.

3. Audio based CAPTCHA

The program picks a thing or even a sequence of numbers indiscriminately, renders the phrase or numbers in a sound clip and distorts the sound clip; it then is definitely the distorted sound clip towards the user and asks users to go into its contents. This CAPTCHA is founded on the real difference in ability between humans and computers in recognizing spoken communication. It is a crude

strategy to filter humans in fact it is not so popular considering that the user must understand the language and also the accent the location where the sound clip is recorded.

Figure 4 Audio CAPTCHA

Advantages of Audio-based CAPTCHA:

Audio-based CAPTCHA:
1) It is employed for moat people that have vision defect.
2) Friendly to peoples.

Disadvantages of Audio-based CAPTCHA

1) System available in the English so person needs to have a thorough English Vocabulary.
2) Similar sound characters.
3) Not working for dumb people or some people that have low listening power.

4. **Video based CAPTCHA**

Video CAPTCHA is a newer and fewer commonly seen CAPTCHA system. In video-based CAPTCHAs, three words (tags) are offered towards user which describes a movie. Anyone's tag must match into a set of automatically generated ground truth tags then exactly the test has been said to become passed. The phrase video CAPTCHA is used to any CAPTCHA which utilizes a relevant video since it's method for present information to your user Although video CAPTCHA is bound, both commercial and academic application do exist.

Advantages of Video-based CAPTCHA:

1) It cannot break using Optical Character Recognition (OCR).
2) It cannot effect by laundry attacks.
3) In some cases it provides greater security than Text-based CAPTCHA and Image based CAPTCHA.

Disadvantages of Video-based CAPTCHA:

1) How big is files is large, so problem face by users to download video and pass the CAPTCHA test.
2) Speed of video.

5. **Puzzle based CAPTCHA**

Usually in puzzle based CAPTCHA confirmed picture is divided to chunks. A user should combine these chunks so that you can make up the complete picture comparable to the first one. [11]

Advantages of Puzzle-based CAPTCHA:

1) It looks like an exciting.
2) It helps the user to observe their brain.
3) It's just like a game so user can more communicate with this CAPTCHA system.

Disadvantages of Puzzle-based CAPTCHA

1) Time consuming.
2) User cannot identify the puzzle easily.

Conclusion

Security is one of the most important factors of web based applications these days. This paper gives an introduction and overview of the CAPTCHA based security system as a potential method of securing web based applications.

References

[1] A Brief Guide to the History of the Internet: http://www.investintech.com/content/historyinternet/

[2] Web-based security threats: how attacks have shifted and what to do about it, GFI White Paper http://www.gfi.com/whitepapers/GFI-Web_Based_Threats_v2_Whitepaper.pdf

[3] Web Security Basics: Web Security and Web Scanning, Web Security, Your Site and Your Network. http://www.beyondsecurity.com/web-security-and-web-scanning.html

[4] Tony Bardley, What is a Bot or Zombie? http://netsecurity.about.com/od/frequentlyaskedquestions/qt/pr_bot.htm

[5] http://www.wiley.com/legacy/compbooks/press/0471348201_09.pdf

[6] Arshey M., C. Balakrishnan, Prevention Strategies and Network Intrusion Prevention Techniques for Dos Attacks, International Journal of Advanced Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2013.

[7] Ashwini Mujumdar, Gayatri Masiwal, Dr. B. B. Meshram, Analysis of Signature-Based and Behavior-Based Anti-Malware Approaches, IJARCET Volume 2, Issue 6, June 2013.

[8] http://www.abox.com/PDFM/webcontefilt.pdf

[9] https://securosis.com/assets/library/reports/DLP-Whitepaper.pdf

[10] Ved Prakash Singh, Preet Pal, Survey of Different Types of CAPTCHA, IJCSIT Vol. 5 (2), 2014, 2242-2245.

[11] Kiranjot Kaur, Sunny Behal, Captcha and Its Techniques: A Review, International Journal of Computer Science and Information Technologies, Vol. 5 (5), 2014, 6341-6344.

[12] Sandeep Mahato; Varun Prakash Saxena; Devendra Bhavsar, A Survey of Captcha based Web and Application Security Methods and Techniques, HCTL Open International Journal of Technology Innovations and Research (IJTIR), Volume 14, April 2015, eISSN: 2321-1814, ISBN (Print): 978-1-62951-946-3.