VOL. 11, NO. 15, AUGUST 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

CLICK JACKING PREVENTION IN WEBSITES USING IFRAME DETECTION AND IP SCAN TECHNIQUES

P. Asha, Roshni Sridhar and Rinnu Rose P. Jose
Computer Science and Engineering, Sathyabama University, Chennai, Tamil Nadu, India
E-Mail: ashapandian225@gmail.com

ABSTRACT

Distributed Denial of Service (DDOS) is said to be an attack that is faced by many prominent web sites currently. Tight security policies and active measures like using firewalls, Vendor paths can be used to face the former security threats. Though protections are available, for click jacking attack vulnerability can be used to exploit the browser's weaknesses. In addition, it becomes easier for an attacker to detect and frame a page. In this paper we have proposed a solution for preventing the DDOS attack along with Click Jacking attack method. The impact of this click jacking vulnerability is difficult to access or demonstrate.

Keywords: click IDS, click jacking, DDOS, HTML, IFRAME, IP address.

1. INTRODUCTION

The development of web applications have originated from the gathering of straightforward HTML records to undeniable applications that contain many progressively created pages. Rich interface with a decent look and feel impact is accomplished by the consolidated utilization of customer and server-side scripting. Mix of different substance and functionalities from various sources have been utilized to develop web-applications. The expanding measure of data's gotten to through the web, has acquired a relating increment in number and experience of online assaults. The primary thought is to give a strict partition between various sources by executing an arrangement of component in the program. This cooperation between the pages can be averted hence accomplishing the division. It is said that the birthplace of the page is for the most part the blend of the area name, TCP port number and the application layer convention. Assailants, continually determined by the prospering economy always search for the defects, special cases, program bugs to dodge the birthplace checks with an intension of stealing or adjust the client delicate data.

These undesirable bugs can be uprooted with the assistance of a strategy known as snap jacking. The target of this snap jacking assault is: An angry page is built in a manner that it traps the client to tap on something else from what the client really recognizes. This snap thusly prompts the un-purposeful activities in the substance of a true blue site. This snap jacking assault by and large happens in a mouse snap which traps the client to tap on a component, for example, the flag promotions, discussion messages, notices that thusly has been usable by the aggressors to exchange cash. This mouse click happens to be sheltered from the client's perspective yet it really stratagems the client unconsciously. In this paper a computerized methodology is introduced to handle this snap jacking assault. A genuine web program has been planned and built up that examines the website pages for the attack (Click jacking) and an observational study has been directed over a million novel site pages. This concentrate likewise demonstrates that the framework functions admirably by and by. This arrangement can be utilized by the security specialists to test immense number a sites consequently for snap jacking. Additionally, the module formed can be coordinated into the standard program design such that it keeps the typical clients from snap jacking amid their ordinary web use. This paper gives an instinct into the present all inclusive statement of snap jacking endeavors on the web. The significant presents of this paper are:

- An mechanized way to deal with distinguish click jacking has been introduced.
- A huge scale endeavor to assess the commonness of snap jacking assaults on the web has additionally been introduced.
- After having inspected a great many well known sites a tick jacking protection system has been received.
- Developed Click IDS program module has been portrayed, and more than a million web website pages have been sent to break down.

In Denial-of-service (DoS) [9] assault, an assailant endeavors to keep the honest to goodness clients from getting to data or administrations. The most widely recognized and clear kind of DoS assault happens when an assailant "surges" a system with data. At the point when the client sort a URL for a specific site into your program, it's sending a solicitation to that site's PC server to see the page. The server can just process a specific number of solicitations on the double, so if an assailant over-burdens the server with solicitations, it can't be process your solicitation. This is a "Refusal of Service" since you can't get to that site.

2. PROPOSED SYSTEM

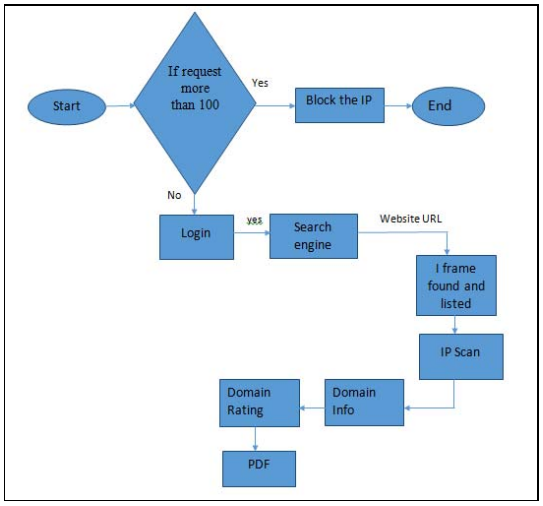
The point of this proposed framework is to add some new assault discovery strategy notwithstanding the current framework. It is performed so firmly such that it gives an insurance to the clients sparing profitable system assets. The bundles that contain honest to goodness source IP location are being recognized from those that contain the caricature addresses. Initial a website page is being made that acknowledges a solitary parameter meaning a URL

that should be inserted in the IFRAME. Once the stacking of the page and its substance are totally (i.e., the IFRAME) rendered, the vicinity for the IFRAME is checked. Pages performing outline blasting would substitute the entire substance in the program window, in this way totally uprooting the IFRAME. To computerize this examination, a Firefox augmentation is actualized such that it takes the rundown of URLs to be gone to. After the page is been stacked, the expansion sits tight for a few moments to confirm the vicinity of IFRAME. On the off chance that the IFRAME is not observed to be a part of the reports DOM-tree then we can close it by saying that the inserted page has performed outline blasting. This may prompt a message DENY. We have additionally started in looking over the edge blasting practice for the main 500 sites. In the wake of having utilized both known and novel assault strategies, we found that all the snap jacking safeguards experienced can be avoided in a few or the other way.

- The proposed framework has a couple added advantage when contrasted with the current method in distinguishing the DDOS assault.
- This framework checks for all the IFRAMES present in the site.
- It likewise checks for both the area and IP address.
- Finally a PDF report is made as the outcome.

3. PROJECT FLOW DIAGRAM

The flow diagram represents the prevention technique proposed in this system.



According to our method, if there are more than 100 continuous requests from the same IP then that particular IP gets blocked. If there is no IP block, then the search engine gets the website URL and checks for the IFrame and later performs the IP scan and the listing technique after which the domain information and the rating are determined.

After the entire procedure is performed, it then produces the result in the form of a PDF report thus, concluding if the attack is taking place or not.

4. TECHNIQUES

Different procedures have been proposed with a specific end goal to keep the assault. Included to it we have acquired a couple of unused strategies to keep this snap jacking assaults and the DDOS assault. They are:

4.1 Check for the URL

4.2 Source page seeing and discovering IFRAME

4.3 A check for the IP address

4.4 Anti-infection rating check

4.5 Analyze the IP solicitation to server

4.6 Reverse IP

4.7 Blocking IP address

4.1 Check for the URL

URL is extended as a uniform asset locator. It goes about as a kind of perspective to the source which indicates the asset situated on a PC system and a procedure to recover it. Here, we check if the URL given by the client is legitimate or not.

4.2 Source page seeing and discovering i-FRAME

- The source code of the given URL is seen and the vicinity of the IFRAME tag is checked.
- Iframe: An inline frame (IFRAME) is only a HTML archive installed inside another HTML report in a site. This IFrame html component is utilized to embed substance from a source into another source. E.g., an include into a site page.
- We get the URL from I-outline tag furthermore the space name is distinguished.

4.3 A check for the IP address

An IP address (Internet Protocol) is said to be a novel numerical name given to each gadget (Eg: Computer, printer and so forth..) that partakes in the PC system utilizing the web convention for correspondence. Here all the IP locations are checked on the grounds that each space comprising of the IP location would be enlisted before dispatching the site. The IP locations are checked to discover in the event that they are in white rundown or square rundown.

4.4 Anti-infection rating check

The age of the site, authentic areas and changes are the variables that choose its scores. The signs of suspicious exercises are found through the investigation of malware conduct. Here we demonstrated headway in applying web notoriety to keep pace with the new sorts of assaults that can happen or even stay covered up. On the off chance that the counter infection rating is got then a 100% safe space can be accomplished.

4.5 Analyze the IP solicitation to server

In PC organizes a server that acts as a mediator for requests from the customers looking for assets from other server is known as intermediary server. A solicitation is made by the customer to the intermediary server for different data's, for example, the records, associations or different assets that are accessible from various servers and this intermediary server assesses the solicitation with a specific end goal to diminish the multifaceted nature and make it simplified. These intermediary servers were found to add structures and epitome to disseminated frameworks.

4.6 Reverse IP

An opposite intermediary is an intermediary server that gives off an impression of being a normal server to the customers. The converse intermediary server can likewise be called as a surrogate server. The solicitations can be sent to one or more servers (intermediary) that can deal with the solicitation. The reaction that is gotten from the intermediary server has all the remarks of being similar to it has originated from the first server. These opposite intermediaries are introduced in many web servers. All the activity that originates from the web with one or more neighborhood's web server as its destination experiences the intermediary server. It is from the "forward proxy" that the utilization of "reverse" has got its source since this converse intermediary rests closer to the web server and servers for just a confined arrangement of sites.

4.7 Blocking IP address

Aversion of association between a server and site and even among certain IP addresses or scope of locations is known as IP location blocking. This hindering of IP addresses successfully bans the undesirable associations from host utilizing self important locations to a mail server, sites or other web servers. The hindering of the IP location is for the most part used to secure against the animal power assaults. Here, the purposeful hindering of the IP is done if there is more than 7 nonstop demands from the customer side to the server keeping in mind the end goal to maintain a strategic distance from the entrance of unique page of the server. Thus we stop the [9] DDOS assault that happens.

5. EXPERIMENTAL RESULT

This is said to be a site page that contains the snap jacking assault. The stamped zone is the place the assault happens that is the point at which a tick is made anyplace inside the checked circle region the assault happens

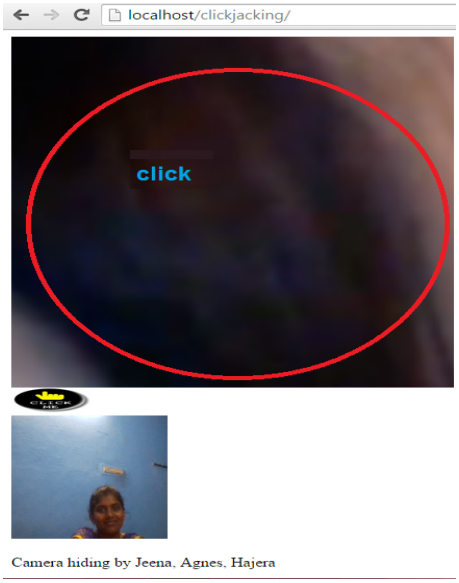


Figure-1. Webpage with click jacking attack.

At the point when the client clicks anyplace inside the circle (the focused on zone) the camera gets misused and the snap jacking assault happens. This abusing of camera is done without the information of the user. After the camera screen opens, the picture gets caught as appeared in the above figure consequently facilitate demonstrating this snap jacking assault. This assault fundamentally is done just by a solitary snap on the focused on range.

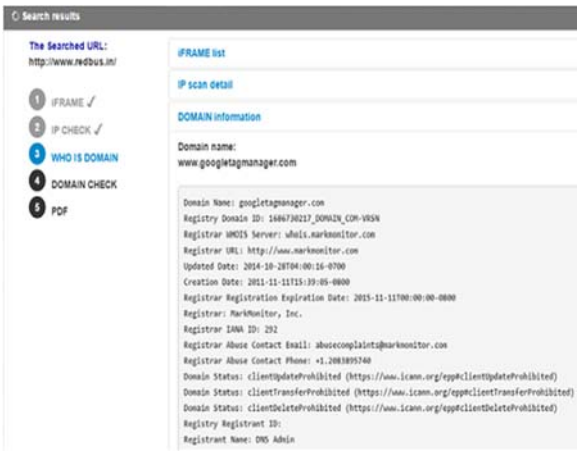


Figure-2. Domain details.

To keep this assault a register page is composed. This page asks for the client to fill in the fundamental points of interest to sign in. "Make account" catch is likewise accessible for the clients who enter surprisingly. This can be signed in either with a current enlisted account points of interest or with the recently made one. After the log in is done, it prompts the page where the client can discover a dashboard. This dashboard is utilized for showing all the data's gotten after the pursuit operation.

When tapping on the dashboard it will request the URL of the site page to be sought. Once the URL is entered, the pursuit operation is performed. This seek additionally confirms and displays whether the site is secured or not.

The following check is on the IFRAME. The IFRAME punch line number, its URL and the aggregate number of Frame's available are recorded for the same URL that was indicated initially. After the IFRAME check, the prompt next check will be on the IP address. The IP location is checked and confirmed whether the IP location is in white recorded or square recorded.

Figure-3. Click jacking report.

Last step will be the generation of report. Final report of this attack (click jacking) is fetched in steps and displayed together at the end. This report is generated in a PDF format.

6. CONCLUSIONS

It is critical identifying the DDOS flooding assaults at their initial dispatching stage before broad harms are done to the licit applications on the casualties framework. The web worms that already took days or weeks to spread now take minutes or even seconds. Administration suppliers and the sellers are rapidly adjusting to the new scene. Resistance must be honed inside and out by the administration suppliers as zero day adventures are discharged. In this paper we exhibit a way to deal with experience the snap jacking assault. To conquer the confinements posted already the client's input is utilized to make dynamic highly contrasting records as an answer. IP location of the client can be obstructed by our strategies, yet in the event that the client changes the IP address still the assault must not happen. To make this conceivable we make utilization of the treats or the session ID alongside the IP to obstruct a hub.

- To finish up saying that executing the DDOS(Distributed Denial of Service) procedure to keep the assault alongside the snap jacking anticipation method in the site we additionally give a PDF report to the client.
- Click jacking is an electronic assault which has as of late picked up the consideration of the media scope. There are numerous news things, exchanges and blog posted on this issue. In any case, this issue still remains a nightmare to the clients concerning how the assault is being finished by the aggressors. In this paper we introduced our drawing nearer framework that naturally recognizes the snap jacking endeavors on the website pages. The made apparatus has been accepted in the wake of leading tests that identify the vicinity of such assaults on the web. It is additionally said to be a programmed testing instrument that checks for the pernicious substance in the page and it has been tried on more than a large number of site pages went by the clients. By dispersing this examination on various virtual machines we will have the capacity to look over to 15000 site pages in a day. Further we have additionally built up another location procedure known as the clickIDS that supplement the unmistakable snap guard gave by the No script module. later every one of the parts are being robotized into a web application testing framework. Indeed, even for the situation where the pages containing the snap jacking assaults have been posted, i.e., security-related sites, can be discovered naturally. Few fascinating cases like the marginal assaults have additionally been identified. Such assaults are hard to precisely group since they are either genuine assaults or false positive.
- Since the response time has gone from days to minutes, the robotized DOS/DDOS checking and reporting will get to be standard for the administration suppliers. Planning is the key for the administration suppliers to discharge the lock from the assaults that happen. The organizations have turned out to be more reliant on the web and its uses. Clients have begun expecting the same unwavering quality from the web like other basic bases which incorporates the force, PSTN and water. The administration suppliers and the sellers today meet a test with the abnormal state participation and advancement.

REFERENCES

[1] Chen J.F., Q. Li., C. Y. Mao., D. Towey, Y. Z. Zhan. and H. H. Wang. 2014. A web services vulnerability testing approach based on combinatorial mutation and SOAP message mutation. Service Oriented Computing and Applications. Vol. 8, No. 1.

[2] Heiderich. M., F. Tilman and H. Thorsten. 2011. Iceshield: Detection and mitigation of malicious websites with a frozen dom, In Recent Advances in Intrusion Detection, pp. 281-300. Springer Berlin Heidelberg.

[3] Du. P and S. Abe. 2008. IP packet size entropy-based scheme for detection of DoS/DDoS attacks, IEICE Trans. Inf. Syst. E91-D(5): 1274-1281.

[4] Ledesma S and D. Liu. 2000. Synthesis of fractional Gaussian noise using linear approximation for generating self-similar network traffic, Comput. Commun. Rev. 30(2): 4-17.

[5] Perrin. E *et al*. 2001. n^{th}-order fractional Brownian motion and fractional Gaussian noises. IEEE Trans. Signal Process. 49(5): 1049-1059.

[6] Jawwad A. Shamsi., Sufian Hameed, Waleed Rahman, Farooq Zuberi, Kaiser Altaf and AmmarAmjad. 2014. Clicksafe: providing security against click jacking attacks. IEEE 15th International Symposium on High-Assurance Systems Engineering.

[7] Bao Y and H., Krim. 2003. Renyi entropy based divergence measures for ICA in Proc. IEEE Workshop on Statistical Signal Processing. pp. 565-568.

[8] Gu. Y., A. McCallum and D. Towsley. 2005. Detecting anomalies in network traffic using maximum entropy estimation, in Proc. ACM SIGCOMM Conf. Internet Measurement (IMC 2005). pp. 32-32.

[9] Jin. X *et al*. 2006. ZSBT: A novel algorithm for tracing DoS attackers in MANETs, EURASIP J. Wireless Commun. Netw. (2): 1-9.

[10] Carl. G *et al*. 2006. Denial-of-service attack-detection techniques. IEEE Internet Comput. 10(1): 82-89.