

# Identification of Internet Hackers' Attacks through Keywords by Analyzing the Server Log File

Hamed Jelodar

Department of Computer, Science and Research, Islamic Azad University, Bushehr, Iran

[hjelogvdar@gmail.com](mailto:hjelodardar@gmail.com)

## ABSTRACT

Attacks and damages caused by hackers to the servers have raised some worries for the manager of the servers. DDoS, XSS and Sql Injection are some of the attacks. All the interactions between the server and client save in server log file. We can identify Internet hackers' attacks by analyzing Server Log File. This article deals with identification of internet hackers' attack by key words and analyzing server log file, and by doing some experiments; they identify different damages of hackers to a website of downloading software.

**Keywords:** *Identifying Internet hackers, Server Log file, Attack Detection*

## 1. INTRODUCTION

Many website are giving services in an online way in World Wide Web. Lack of security against hackers' attacks causes losing data and lack of servicing websites. DDoS, XSS and Sql Injection are some of the most famous vulnerable attacks to websites. To identify hackers' attacks, some systems named diagnosis system have been designed, that the most popular of them is "Snort". All the interaction between server and agent registers in server Log file and much information is save in this file. By analyzing this file we can discover useful information. In this article we deal with identifying Internet hackers' attack by key words with analyzing server log files. The classification of different parts of this article is as follows: In second part, we discuss previous works. In third part we examine some of the hackers'. In fourth part, we discuss server log file. In fifth part, we discuss the introduced way to identify the attacks, and in sixth part we deal with doing experiments and in the seventh part we have the conclusion.

## 2. RELATED WORK

Safety of the websites from hackers' attacks is an important part of security of website. Server Log file includes many information such as users' application, Error, entrance time of user, user' IP and so on. Analyzing Server log file helps to deduce knowledge. Identifying the hackers', that is an important issue to avoid website from begin vulnerable, in order to solve this problem, diagnosis system have been designed, the most popular of them is Snort. Researchers are searching for ways which identify the attacks more carefully and with fewer mistakes. S.E Salama and et al investigated how to analyze server log file with XML format in order to identify and discover the attacks [1]. B Deoker and et al in their article examine advantages and disadvantages of identifying intrusion system and had propounded a suggestion in order to reduce the mistakes of intrusion identification [2]. In this article we study Internet hackers' attacks by key words with analyzing server log file.

## 3. IDENTIFICATION OF THE ATTACKS

In this part, we study some of the attacks to servers such as DDoS, Sql Injecton and XSS.

### 3.1 Sql Injection Attacks

SQL Injection is one of the illegal acquiring methods to the server data that hackers could pervade to the website by putting the excessive letters beside the query. In this method, the SQL commands are like Select, Insert and Update [3]. Poor Programming of website causes Sql Injection attacks easily and hackers access to the content of database. For example they entered a digit hacker instead of number one of website. If the website IS designed poorly and the programmer didn't explain numerical limit, the error log happen that finally shows the name of tables and columns and the hacker perform vulnerability.

### 3.2 DDoS Attacks

In this attack, some http applications were sent repeatedly to the server by a person or a group of people. By making a coordinate attacks on server, DDoS would made traffic in server, that it is one of its feature [4]. The aim of this work is to "Down" the server and to reduce giving services. To identify this attack we can see server log file and could perform examination of the IPs that have most applications to the server. In this article we identify the attacks by analyzing a server log file. In figure (1) hackers are performing DDoS attack to the server that finally the full gate way becomes 100% and causes the lack of gateway width.



**Figure 1:** View of DDoS attacks and the full bandwidth of the server

### 3.3 XSS attacks

If for HTML's tag and Specific Characters like ", ', < or > encoding has not been done, a hacker could damage a website by destructive JavaScript code [5]. In these attacks, hacker

<http://www.scientific-journals.org>

injects script codes to the site and can access to the content of Cookies. Evaluation of credit of the user and output codification avoid vulnerability of this method to the website.

#### 4. SERVER LOG FILE

The requests that are sent to the server by users are stored in the Server File Log. In another words all the interactions between user and server save in server log file. [7]. There is much information in this file that we can discover useful information from.

##### 4.1 Classification of the content of server log file

The information of the server log file is divided into four groups including Agent, Error, Transfer, Referrer. Figure (2) shows this classification.

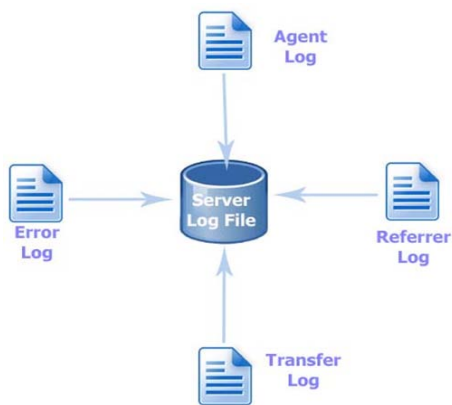


Figure 2: All documents stored in log file server

#### 5. The Way of Identifying the Attacks

In this part, we identify the attacks including DDoS, Sql Injection, and XSS. Here we identify XSS and Sql Injection attacks by using keyword from the order which the hacker uses. And also to identify DDoS attacks, we started to identify suspected IPs. This article discusses the way of identifying the attacks.

##### 5.1 How to identify Sql Injection attacks?

Hackers send their injections with URL. By examination of keywords that are with URL parameter, we can discover Sql Injection attacks. You can see the keywords in table I and also in figure (3) is function used to identify keywords of Sql Injection attack.

Table1: Keywords Commands Sql Injection

Keywords		
Select	Insert	Update
Drop	Delete	Count
'	--;	Where

```

public static string checkForSQLInjection(string userInput)
{
    bool isSQLInjection = false;
    string[] sqlCheckList = { "select", "update", "drop", "insert", "count",
        "delete", "or", "create", "where", "''", "''"; };

    string CheckString = userInput.Replace("'", "");
    for (int i = 0; i <= sqlCheckList.Length - 1; i++)
    {
        if ((CheckString.IndexOf(sqlCheckList[i], StringComparison.OrdinalIgnoreCase) >= 0))
        {
            isSQLInjection = true;
        }
    }
    return Convert.ToString(isSQLInjection);
}
  
```

Figure 3: The function used to detect keywords Sql Injection[6]

##### 5.2 How to identify XSS attacks?

XSS attacks happen with JavaScript codes. By examination of keywords that are with address' parameter, we can discover XSS attacks. The keywords are shown in table II and also in figure (4) is the function.

Table 2: Keywords commands XSS

Keywords		
<script	<script>	Script >
document.write	alert(	Alert
javascript	location	document.location
document.cookie	function	windows.open

```

public static string checkFor_XSS(string userInput)
{
    bool isXss = false;
    string[] XssCheckList = { "<script>", "<script", "/script>",
        "document.write", "alert(", "alert",
        "javascript", "location", "document.location", "document.cookie", "function",
        "windows.open", "function",
        ".location" };

    string CheckString = userInput.Replace("'", "");
    for (int i = 0; i <= XssCheckList.Length - 1; i++)
    {
        if ((CheckString.IndexOf(XssCheckList[i], StringComparison.OrdinalIgnoreCase) >= 0))
        {
            isXss = true;
        }
    }
    return Convert.ToString(isXss);
}
  
```

Figure 4: The function used to detect keywords XSS

##### 5.3 How to identify DDoS attacks?

Hackers, by various application of http reduce and reply to servers that is DDoS attacks. Some of the IPs requests a page suspiciously and constantly and we can guess that the server is under the attack of DDoS.

## 6. EXPERIMENT AND RESULT

We want to analyze the log file server of a software downloading website in order to identify the hacker's attacks. This file has 2271 URL register parameter. In this experiment, 475 records of individual user will be analyzed. The aim of this experiment is to identify XSS, Sql Injection and DDoS attacks. The experiment has two parts. The first part use to identify XSS and Sql Injection attacks and the second part is to identify DDoS attacks. In order to have a correct concept and result, we should be sure that web site which we want to analyze server log file has some damages. Because of that, at first as a hacker we attack to the website by XSS, Sql Injection and DDoS attacks.

### 6.1 Doing experiment to identify SqlInjection and XSS

At first server log file is given to a software that have been designed to do this experiment in order to identify the attack that have been designed by C# language, by using the function that have introduced in fifth part, to examine URL parameters and to identify XSS and SqlInjection. The obtained results out of this software including 22 SqlInjection and 1 XSS identify attacks. In Figure 5 shows the detected attacks.

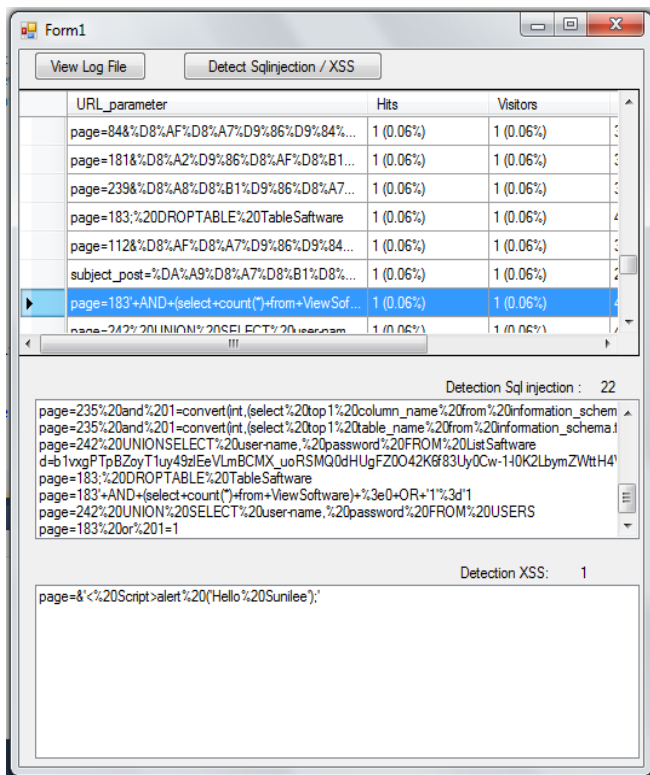
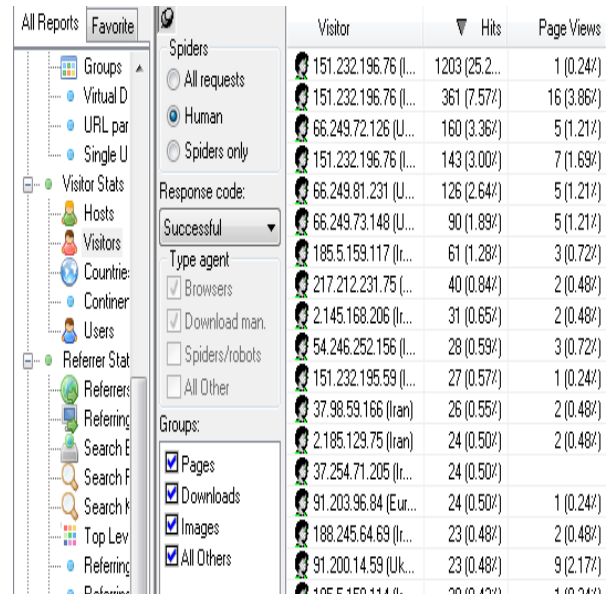


Figure 5: Run the software and attacks identified

### 6.2 Doing experiment to identify DDoS

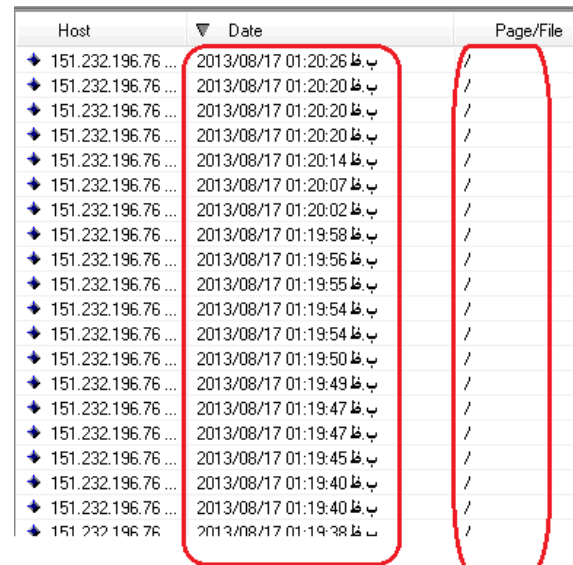
As we mentioned in sixth part, in order to identify DDoS attacks, we should identify suspected IPs. To do this experiment, at first we analyze server log file with "Web Log Explorer" software. Figure (6) shows some of the users that visit website. In this experiment we examine 151.232.196.76 IP and 66.249.72.126 IP that have several applications. If we look at "Date" column in figure (7) the application of 151.232.196.76 IP is at frequent intervals and also this IP visit no pages that is specified in "Page/file" column. And now if

we take a look at "Date" column in figure (8) the applications of 66.249.72.126 IP is at different intervals. According to a comparison between these two IPs, we can say that 151.232.196.76 IP is as Suspected IP that put the server under the DDoS attack.



Visitor	Hits	Page Views
151.232.196.76 (I...	1203 (25.2%)	1 (0.24%)
151.232.196.76 (I...	361 (7.57%)	16 (3.86%)
66.249.72.126 (U...	160 (3.36%)	5 (1.21%)
151.232.196.76 (I...	143 (3.00%)	7 (1.69%)
66.249.81.231 (U...	126 (2.64%)	5 (1.21%)
66.249.73.148 (U...	90 (1.89%)	5 (1.21%)
185.5.159.117 (I...	61 (1.28%)	3 (0.72%)
217.212.231.75 (I...	40 (0.84%)	2 (0.48%)
2.145.168.206 (I...	31 (0.65%)	2 (0.48%)
54.246.252.156 (I...	28 (0.59%)	3 (0.72%)
151.232.195.59 (I...	27 (0.57%)	1 (0.24%)
37.98.59.166 (Iran)	26 (0.55%)	2 (0.48%)
2.185.129.75 (Iran)	24 (0.50%)	2 (0.48%)
37.254.71.205 (I...	24 (0.50%)	1 (0.24%)
91.203.96.84 (Eur...	24 (0.50%)	1 (0.24%)
188.245.64.69 (I...	23 (0.48%)	2 (0.48%)
91.200.14.59 (Uk...	23 (0.48%)	9 (2.17%)

Some users's visiting



Host	Date	Page/File
151.232.196.76 ...	2013/08/17 01:20:26	/
151.232.196.76 ...	2013/08/17 01:20:20	/
151.232.196.76 ...	2013/08/17 01:20:20	/
151.232.196.76 ...	2013/08/17 01:20:14	/
151.232.196.76 ...	2013/08/17 01:20:07	/
151.232.196.76 ...	2013/08/17 01:20:02	/
151.232.196.76 ...	2013/08/17 01:19:58	/
151.232.196.76 ...	2013/08/17 01:19:56	/
151.232.196.76 ...	2013/08/17 01:19:55	/
151.232.196.76 ...	2013/08/17 01:19:54	/
151.232.196.76 ...	2013/08/17 01:19:54	/
151.232.196.76 ...	2013/08/17 01:19:50	/
151.232.196.76 ...	2013/08/17 01:19:49	/
151.232.196.76 ...	2013/08/17 01:19:47	/
151.232.196.76 ...	2013/08/17 01:19:47	/
151.232.196.76 ...	2013/08/17 01:19:45	/
151.232.196.76 ...	2013/08/17 01:19:40	/
151.232.196.76 ...	2013/08/17 01:19:40	/
151.232.196.76 ...	2013/08/17 01:19:38	/

Figure 6 :Suspected numerous requests with short time interval

<http://www.scientific-journals.org>

Host	Date	Page/File
66.249.72.126 [...]	2013/08/18 10:02:15 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 09:42:26 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 09:15:15 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 08:50:25 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 08:00:55 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 07:11:21 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 06:34:14 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 06:31:44 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 05:57:04 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 05:10:00 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 04:45:19 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 03:58:15 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 03:45:45 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 03:38:26 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 03:28:33 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 02:56:21 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 02:26:40 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 02:11:47 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 12:45:09 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 12:19:31 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/18 12:09:33 ق.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/17 11:42:31 ب.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/17 10:46:15 ب.ظ	/ViewSoftwa...
66.249.72.126 [...]	2013/08/17 09:52:05 ب.ظ	/ViewSoftwa...

**Figure 7** :Suspected numerous requests with different distances and long time

international workshop on Software engineering and middleware, pp. 106-113. ACM, 2005.

- [4] Kottenko, Igor, Alexey Alexeev, and Evgeny Man'kov. "Formal framework for modeling and simulation of DDoS attacks based on teamwork of hackers-agents." , IAT. IEEE/WIC International Conference on, pp. 507-510. IEEE, 2003.
- [5] Johns, Martin. "SessionSafe: Implementing XSS immune session handling." In Computer Security–ESORICS, pp. 444-460. Springer Berlin Heidelberg, 2006.
- [6] <http://www.dascode.net/post/2009/11/01/An-example-of-how-to-check-for-SQL-Injections.aspx>
- [7] Jelodar, H. " Exploitation of Server Log Files of User Behavior in Order to Inform Administrator.", International Journal of Computer Applications, pp. 26-30, 2013

## 7. CONCLUSION

This study is about identification of Internet hackers' attacks. In this article it was suggested that by using keywords and server log file, hackers' attacks can be identified. The selected keywords to identify the attacks were among the most popular words that the hackers used in their orders, that is mentioned in this article. Also in this article we identify DDoS attacks. The way to identify DDoS attack is more probable. Websites' developers can increase the security of websites by different ways like correct programming.

## REFERENCES

- [1] S.E Salama, M.I Marie, L.M El-Fangary, Y.K Helmy, "Web Server Logs Preprocessing for Web Intrusion Detection," Computer and Information Science, vol. 4, No. 4, pp. 123-133, 2011
- [2] B. Deokar, A. Hazarnis, " Intrusion Detection System using Log Files and Reinforcement Learning ", International Journal of Computer Applications, Vol. 45, No. 19, pp. 28-35, 2012.
- [3] Buehrer, Gregory, Bruce W. Weide, and Paolo AG Sivilotti. "Using parse tree validation to prevent SQL injection attacks." In Proceedings of the 5th