Modern Environmental Science and Engineering (ISSN 2333-2581)
September 2018, Volume 4, No. 9, pp. 827-830
Doi: 10.15341/mese(2333-2581)/09.04.2018/006
Academic Star Publishing Company, 2018
www.academicstar.us

Analysis of Information Security in a Framework for the Development of Volunteered Geographic Information

Sivoney Pinto Dias[1], Fábio de Oliveira Sales[2], and Helder Guimarães Aragão[3]

1. Uniasselvi University, Brazil

2. Ruy Barbosa University, Brazil

3. Centro Universitario Estacio da Bahia University, Brazil

Abstract: Volunteered Geographic Information includes collaborative features that involve spatial or geographic data to Web systems. This type of voluntary contribution has grown significantly in recent years. Due to the growing demand for Web systems with VGI, some frameworks were developed with the aim of facilitating the implementation of this type of system. A key feature that these frameworks should have in their implementation is information security. In this context, the present paper aims to evaluate the information security level of one of these frameworks available for the implementation of Web systems with VGI. The framework evaluated was the ClickOnMap. We did this evaluation in stages and with specific information security tools. At the end of this paper, the results of this evaluation are presented.

Key words: ClickOnMap, OWASP, VGI

1. Introduction

Nowadays, business productivity depends on the use of the Internet. As a result, companies' dependence on technology resources in the Web environment has grown significantly. To maintain business continuity, the corporate world needs to protect its information. Information is a valuable asset that arouses the interest of various threatening agents in obtaining it unlawfully. A significant number of applications used on the Web contain security holes. These failures may be in the computational resources or even in the implementation of systems [1]. These vulnerability problems represent damages and losses to companies. The damage that the attackers do is not always financial. Any organization that relies on volunteers, engaged in the contribution of specific website content can have its reputation devastated if minimal security measures are not taken [2]. Recently, the advent of Web 2.0 made the end user a content producer. The concern about information security plays a key role. In this context, the present paper addresses information security of Volunteered Geographic Information (VGI). We evaluated the security aspects in a framework called ClickOnMap, a platform specifically for the implementation of collaborative sites with geographic information. The objective of this work, therefore, is to analyse the security risks in Web applications for collaborative mapping, as well as to present some tools that developers can use to evaluate the safety of VGI framework development.

2. Material and Methods

M. F. Goodchild [3] describes that a large number of people use the web to create, collect and disseminate Volunteered Geographic Information. Wikimapia and OpenStreetMap are examples of sites that allow the creation of collaborative maps by users. These sites create a structure that allows users to locate places and

Corresponding author: Sivoney Pinto Dias, Systems Analyst, research areas/interests: VGI. E-mail: sivoneypdias@gmail.com.

edit the map by marking points. The Web 2.0 introduced this form of contribution, making the final user the consumer as well as the producer of information. This new form of generating of geographic content made by the user is now available to Geographic Information Systems (GIS), which are systems capable of manipulating geographic data. M. F. Goodchild [3] calls of the Volunteered Geographic Information (VGI) this form of the user-generated content. For the development of a VGI site, it is necessary to use technological resources to highlight geotags. The geotags allow the user to insert information on a particular point of the map [3].

In order to support the development of VGI sites with geotag resources several frameworks have been developed. One of these frameworks is the ClickOnMap, which was created to support the development of VGI features in a geobrowser based on the GoogleMaps API and the Dynamic Metadata for VGI (DM4VGI) [4].

ClickOnMap can collect information related to the user contribution according to categories and types of subjects informed by the collaborator. The issues are diverse, ranging from urban (infrastructure, security and entertainment) to environmental (disasters, forest fires and floods). The system allows anonymous or identified collaboration, depending on the site's use policy. For example, in a system that collects alerts about crimes, the voluntary user can make a complaint anonymously. On the other hand, in a system of evaluation of the quality of customer service in an establishment, the user can have their collaboration identified [4].

For the implementation of a VGI, it is fundamental to use information security. This is because undue collaborations, or identification of collaborations with errors, can cause problems in the use of the VGI site. According to [5], unsafe software, developed without security criteria increases the risk of a variety attacks. In order to alert developers, managers and companies about the consequences of the most important Web application security vulnerabilities, the Foundation Open Web Application Security Project (OWASP) created the Top Ten Project. OWASP is an open community dedicated to empowering organizations to develop, acquire, and maintain trusted applications. It provides free standards and security testing tools [2, 5].

The impact that attackers can generate on Web systems and, in particular, on VGI sites is very large [2]. One can imagine the troubles caused by illicit manipulation of data in an application like Waze, which contains traffic information. An attacker can generate false alerts regarding bottlenecks or include unreliable routes, exposing the user to various security risks. In the year of 2015, Miami police included false information about radars and blitzes in Waze in the United States [5, 6].

Some applications have been developed to help in application security testing. Among the tools, there is the SQLMap, which is an open source penetration testing tool that automates the process of detecting and exploiting SQL injection. An SQL injection consists of inserting an SQL statement on the Web system through an address bar in the browser. By executing this type of exploit, the attacker is able to obtain confidential data from the database, modify the data and perform operations with administrator profile in databases [7].

In this paper, we present the results of the ClickOnMap information security analysis made four steps. In the first stage, we structured the test environment as per the tutorial available on the "Site VGI" project [8]. In the second stage, we mapped the vulnerabilities using the Zed Attack Proxy (ZAP) tool, which was developed by the OWASP Foundation and is one of the world's most popular free security tools. Hundreds of international volunteers maintain the ZAP tool. The ZAP tool performs a search for security holes in a Web application, following the categorization of risks according to OWASP TOP 10 [2].

In the third step, the data contained in the report generated by the ZAP Proxy tool was used, specifically of the "A1-Code Injection" category, which

corresponds to the insertion of code to execute some unwanted instruction by the application. This report has addresses and parameters that are vulnerable to attack. With this information, it was possible to run SQLMap for the address of the test environment [2].

Finally, in the last step, after using the SQLMap options to find out the type and name of the database, as well as table names, we execute the query showed in Fig. 1 in order to obtain all data from the user table of the ClickOnMap database.

3. Results and Discussion

According to the definition described in the ten security risks in OWASP TOP 10 – 2013 applications, "SQL injection failures occur when untrusted data is sent to an interpreter as part of a command or query".

One of the ways to discover SQL Injection failures is by examining the source code of application. The aim is to check if instructions with untrusted data can be sent to the interpreter via the browser [2]. Fig. 1 shows a code snippet of the ClickOnMap, in which an attacker can insert a value for the "login" parameter not provided by the application via HTTP (Hypertext Transfer Protocol) request.

An alternative to correct security errors shown in Fig. 1 is the use of dynamic queries with the implementation of the Prepared Statement. In this way, it is not possible to send data to the interpreter using the address bar of the browser, avoiding the SQL injection [9].

Fig. 2 is an example of a code snippet minimizing the risks of the vulnerability pointed to in the code in Fig. 1.

Another way to find code injection failures is to use tools like ZAP Proxy and Skipfish [10]. Fig. 3 shows a highlight of the result of executing a statement to retrieve all data from the user table of the VGI Site. We can see in the Fig. 3 some important information: the names and the respective emails of the volunteers of the collaborative system. In this way, the attacker would get a list of email contacts, which could be easily used for spreading false emails or spam.

```
// trecho de código retirado do arquivo autentica_outros.php
$query = "SELECT * FROM usuario WHERE endEmail = '$login' ";
$result = mysql_query($query, $connection);
```

Fig. 1 ClickOnMap code snippet that allows reception of untrusted data in SQL query construction.

```
// $pdo é uma instância da classe PDO de acesso ao banco de dados
$query = "SELECT * FROM usuario WHERE endEmail = :login";
$stmt = $pdo->prepare($query);
$stmt->bindParam(':login', $login);
$ result = $stmt->execute();
```

Fig. 2 Example of using Prepared Statements to avoid SQL injection.

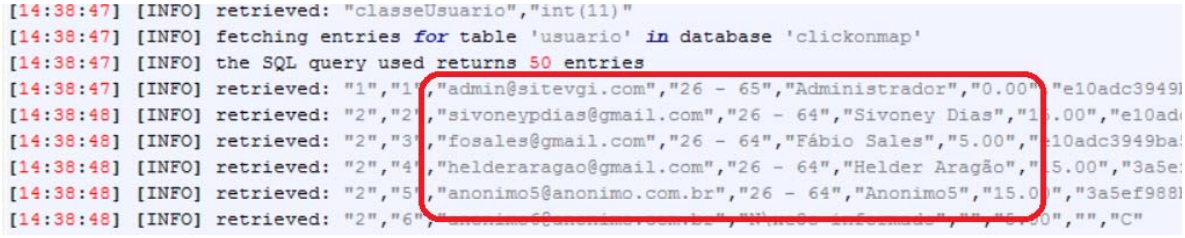

Fig. 3 Scan result done with SQLMap.

The attacker with the mailing list can also spread fraudulent activity on the Internet. Email is one of the main ways to try to induce a person to access websites with messages containing links to malicious code that redirect to fraudulent e-commerce or Internet Banking. In addition, an e-mail list can be used to spread

unwanted fake news [11].

4. Conclusion

Web systems that implement VGI information associated with a geographical position created new forms of collaboration on the Internet. As a result, some frameworks have been developed to facilitate the construction of VGI sites. However, we can see in this paper that the ClickOnMap framework does not contain aspects of information security in its implementation. It is worth mentioning that failures in information security can cause irreparable damage to collaborative systems.

Finally, we can see in the results of this work, that basic information security features existing in traditional Information Systems are not implemented in the ClickOnMap framework. We hope that this work will act as a stimulant to developers of frameworks and technologies for VGI implementation to include security features.

Future studies could include: i) evaluation of other information security issues of the ClickOnMap, such as user session management failures and ii) evaluation aspects of information security in other VGI frameworks.

References

[1] N. Ghoddosi, Gestao da seguranca da informacao, Indaial: Uniasselvi, 2012.

[2] OWASP Top 10-2013 Brazilian Portuguese, accessed on 17 October, 2016, available online at: https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/owasptop10/OWASP_Top_10_-_2013_Brazilian_Portuguese.pdf.

[3] M. F. Goodchild, Citizens as Sensors: the world of volunteered geography, *Geo Journal* 69 (2007) 211-221.

[4] W. D. Souza, J. Lisboa-Filho, J. H. S. C?mara, J. N. Vidal Filho and A. P. Oliveira, *ClickOnMap: A Framework to Develop Volunteered Geographic Information Systems with DynamicMetadata*, 2014, pp. 532-546.

[5] A. A. Fernandes and V. F. Abreu, Implantando a governanca de TI: da estratégia à gestao dos processos e servicos, Rio de Janeiro, 2008.

[6] Exame, accessed on 23 May, 2017, available online at: http://exame.abril.com.br/tecnologia/policiais-enchem-waze-de-informacoes-falsas-para-tentar-despistar-motoristas.

[7] SQLMap: Automatic SLQ injection and database takeover tool, accessed on 23 October, 2016, available online at: http://sqlmap.org/.

[8] CLICKONMAP, accessed on 17 October, 2016, available online at: http://www.dpi.ufv.br/projetos/clickonmap.

[9] W3SCHOOLS-PHP Prepared Statements, accessed on 20 May, 2017, available online at: https://www.w3schools.com/php/php_mysql_prepared_statements.asp.

[10] SKIPFISH-Google Code Archive, accessed on 22 May, 2017, available online at: https://code.google.com/archive/p/skipfish/.

[11] CERT.BR: cartilha de seguranca para internet, accessed on 31 October, 2016, available online at: http://cartilha.cert.br/seguranca.