Advanced Science and Technology Letters
Vol.98 (CES-CUBE 2015), pp.128-131
http://dx.doi.org/10.14257/astl.205.98.32

Safe Automatic Attendance Check System Applying Secure Coding Rule

Bae-Mi Young, Young-Wook Cha, Dae-Jea Cho[1], Han-Kyu Lim

Dept. Of Multimedia Engineering, Andong National University,
1375 Kyungdong-ro, Andong 760-749, South KOREA
djcho@anu.ac.kr

Abstract. With the recent increase of supply of smart phones and internet, personal information leakage is increasing, and open platform Android due to providing various interfaces is seeing increases of cyber-attacks such as hacking and damage such as malicious codes. For this to study applied and implemented secure coding rule on the automatic attendance check system using Android-based smart phones. To implement a safe system, security weaknesses were removed using a method of the system developer testing codes line by line in the security weaknesses in web application development security items to implement a safe automatic attendance check system.

Keywords: Automatic attendance check system, secure code, QR code,

1 Introduction

With the recent increase of supply of smart phones and internet, personal information leakage is increasing, and open platform Android due to providing various interfaces is seeing increases of cyber-attacks such as hacking and damage such as malicious codes. For this to study applied and implemented secure coding rule on the automatic attendance check system using Android-based smart phones. To implement a safe system, security weaknesses were removed using a method of the system developer testing codes line by line in the security weaknesses in web application development security items to implement a safe automatic attendance check system.

When Safe Net analyzed the global first quarter data breach incidents, within this period through 254 incidents about 200 million items of personal information or other sensitive company information was found to be leaked. This is an increase by 233% compared to last year and it was found that every hour 90,000 cases of important information was leaked by insiders or hackers[1]. Especially Android which is most widely used in the world is an Open Platform opens external interface to provide API(application programming interface) during application development and supports easy use of network services. This has many benefits but due to provision of various interfaces it becomes the cause of cyber attacks such as hacking and malicious code

[1] Corresponding author.

ISSN: 2287-1233 ASTL

damage[2].' names of the authors, should be checked before the paper is sent to the Volume Editors.

In a period where software security related incidents are largely rising every year, the Korean government put effort into removing security weaknesses which is the cause of vulnerabilities in the software development process for software security strengthening. From 2012 application of software development security was institutionalized on the mystic public institution web services[3]. For security enhancement of websites OWASP(The Open Web Application Security Project) published 'Web Application Development Security Guide' by classifying considerations and website development security[3, 4]. Secure coding is a coding method that reflects upon the problems of security considering the security vulnerabilities that exist on software before completion of development. When developing software without considering secure coding, in some cases security weakness detection expense can be up to 30 times higher[5]. The first method of removing security vulnerabilities is for a developer well-versed in secure coding to test codes line by line and the second method is to use a static analysis tool.

In this paper, to remove security weaknesses and to implement safe systems, removed the security weaknesses in the web application development security topic within 'Web Application Development Security Guide' to implement a smart phone-based automatic student attendance management system. For method of removing security vulnerabilities the study used the method of the system developer testing the codes line by line. In the automatic attendance management system with the security weaknesses removed, is in the form of where newly created QR codes every lesson are recognized and automatically attendance is acknowledged, and if required the student can always check their information and timesheets about their attendance status through web or app and they can manage[6]. This is a development of software where security and safety is strengthened to develop credible software, and it will be the cornerstone to customer credibility improvement in sales increase.

2 Automatic attendance check system applying secure coding rule

Table 1 is the 12 inspection items that need to be considered in web application development and the other items that the study used for inspection. And it shows whether the developed system was observing security coding rule.

Table 1. Inspection items and observance of secure coding rule.

Inspection items	KISA	OWASP	Observance of security rule
Script insertion(XSS)	O	O	-
Malicious file execution	O	O	-
SQL injection	O	O	X
URL/Parameter manipulation	O	O	-
File Upload	O	O	-
File Download	O	O	-

URL Forced Access	O	O	X
Exposure Information	O	O	O
ID/PW Management			O
Security Considerations	O	O	O

2.1 Injection of SQL Syntax

SQL syntax injection is a problem that occurs because the URL’s parameter value does not verify the validity on the web server about the transmitted strings, and that is where the SQL syntax is directly transmitted to the DB server and executed. Here the attacker uses the SQL syntax injection to attempt login authentication bypass, website modulation, and internal data leakage.

```
$strSQL = "select * from tbs_co_haksa_date where hddbcreate = 'Y' ";
$strSQL.= " and (hdsidt <= '" .$curDateStr. "' and '" .$curDateStr. "' <= hdjodt ) ";
$strSQL.= "order by hdsidt desc ";
```

```
$query = sprintf("SELECT hdsidt, hdjodt FROM tbs_co_haksa_date WHERE id = '%s';",
addslashes($id));
$result = @OCIParse($conn, $query);
if(!@OCIExecute($result)) error("SQL Syntax Error“);
exit;
@OCIFetchInto($result, &$rows);
```

Fig. 1. Example of not secure code(top) and secure code(down).

2.2 URL Forced Access / Authentication Bypass

It is the method of directly inputting the page URL that is accessible on the website in the address bar where the user rights management is not operated normally, or manipulating the cookie. Through these methods the attacker accesses the administrator menu page without login process and acquires sensitive data such as member information and in writing boards that need authentication such as announcements they can post malicious posts.

This system used SSL technology to encrypt the entire log in transaction, and in user certification, cookies were not used.

2.3 Service Method Setting

Method is a tool for communicating with the client in the web application and there are various methods such as GET, POST, PUT, MOVE, DELETE and it performs various functions. The attacker can use the methods allowed in the Web server to manipulate the web server without authentication such as file uploading and web server file deletion. In this system, the httpd.conf file of Apache was modified so that users that did not have login authorization on the Apache web server could not use method.

2.4 ID/PW Management

The vulnerability of vulnerable ID/PW is generally using ID/PW that can be easily guessed when creating user accounts or administrator accounts. The system does not use the method of using ID/PW and uses the cellular phone number of the student to login through a user authentication and it was used encrypted for user authentication.

3 Conclusion

In automated attendant system sensitive data that can affect the grades of the student exist and because it is a system that can be used linked to education management in needs to be robust about external malicious attacks.

In this paper, based on the application development Security guide provided by the Korean government, analyzed if there were security vulnerabilities in the smart phone-based automated attendant system and removed them. The study applied secure coding rule on the Android-based smart phone automated attendance system to implement. For future research the study tries to use various types of open static analysis tools to process analysis of the suggested system and to comparatively analyze the results.

Acknowledgements. This work (C0185025) was supported by Business for Cooperative R&D between Industry, Academy, and Research Institute funded Korea Small and Medium Business Administration in 2015.

References

1. http://www.datanet.co.kr/news/articleView.html?idxno=72320
2. S. H. Seo, G. S. Jun: Smartphone Security Threats and Countermeasures. In: TTA Standardization Strategy Map, no. 132(2010)
3. Ministry of Security and Public Administration: Secure Coding Inspection Guide for e-gov SW, (2014)
4. Ministry of Security and Public Administration: Secure Coding Guide for Web Application Program. (2010)
5. G. Tassey: The Economic Impacts of Inadequate infrastructure for Software Testing. NIST.(2012)
6. M. Y. Bae, D. J. Cho, H. K. Lim: Automatic Attendance Check System using QR Code based on Smartphone. Proceedings of KIIT Summer Conference , pp. 256--258(2014)