PAPER DETAILS

TITLE: SOFTARE SECURTY OF WEB APPLICATION AND WEB ATTACKS

AUTHORS: Hanim Eken

PAGES: 70-78

ORIGINAL PDF URL: https://dergipark.org.tr/tr/download/article-file/257042

INTERNATIONAL JOURNAL OF eBUSINESS AND eGOVERNMENT STUDIES
Vol 5, No 2, 2013 ISSN: 2146-0744 (Online)

SOFTARE SECURTY OF WEB APPLICATION AND WEB ATTACKS

Hanım Eken
Gazi University
hanim.eken@os.gazi.edu.tr

─Abstract ─

Today, thousands of applications world-wide web, and mobile media applications are used by people. People are using these applications in a multi-process, using the Internet or mobile devices can easily. These applications facilitate the lives of people. People have been entering a significant amount of information into these applications by information screens every day. Therefore, applications and databases of these applications contain a large amount of information. Each user can only have access to their own knowledge. Each user is the only authority competent in operations. Also, this information should be avoided by malicious people to reach. Only by malicious people to seize the information may not be objective. They can make the system or application may be inaccessible. Therefore, this requires software security and reliability. Therefore, this study aims web software applications, whereas the threats and vulnerabilities, how to be mentioned steps might be taken.

Key Words: *Information security, Information Security Management System (ISMS), Web Application Security.*
JEL Classification: H80

1. INTRODUCTION

The Internet is an outcome of visionary thinking in the early 1960s, aiming to realize great potential value in allowing computers to share information on research and development in scientific and military fields. J.C.R. Licklider of MIT first proposed a global network of computers in 1962, and moved over to the Defense Advanced Research Projects Agency (DARPA) in late 1962 to head the work to develop it. Leonard Kleinrock of MIT and later UCLA developed the theory of packet switching, which was to form the basis of Internet connections (Walt Howe, 2012).

Using internet has some problems. People start to develop malicious code for getting information about other people from Internet. Hacker started to discover any information from Internet through malicious code. The term "computer virus" was introduced in the world. Viruses start to be important problems for systems, applications etc.

"Computer virus" means a harmful computer program. It is developed by people in order to damage to system or computer. It is described a worm or malware. Today, many harmful computer programs threaten system or computer on Internet. People continuously try to develop the most harmful viruses. However, The Morris worm was the first computer worms on Internet.

The Morris worm or Internet worm of November 2, 1988 was one of the first computer worms distributed via the Internet. It is considered the first worm and was certainly the first to gain significant mainstream media attention. It also resulted in the first conviction in the US under the 1986 Computer Fraud and Abuse Act (Dressler, J. ,2007).

The Morris worm prompted DARPA to fund the establishment of the CERT/CC at Carnegie Mellon University to give experts a central point for coordinating responses to network emergencies (CERT, 1997).

Threats

A threat is anything (manmade or act of nature) that has the potential to cause harm. A vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset) (ISACA, 2006).

Threats consist of two sources. These are humans and nature. Nobody can stop nature threats. Examples are earthquakes, hurricanes, floods, lightning, and fire. They can cause severe damage to computer systems and hardware. Data can be lost. Human threats can be divided into two categories: malicious and non-malicious. The non-malicious threats come from users or employers. Malicious attacks usually come from non-employees or complainant employees. They have a specific goal or objective to achieve in order to damage web application or seize information.

A threat will use a vulnerability to cause harm creates a risk. Thus, web application vulnerability must be found and removed.

Nowadays, thousands of applications world-wide web are used by people. People have been entering a significant amount of information into these applications by information screens every day. Therefore, applications and databases of these applications contain a large amount of information. As a result, security of web application is important. Owners of web applications must protect the web applications very carefully. In this study, first identifies a description of few threats then identifies a description of web application and software security of web application.

1. SOFTWARE SECURITY OF WEB APPLICATION

2.1 What is a web application?

A Web application is an application that is run on Internet or Intranet that the user can use the internet or mobile devices at home or office. In addition, everybody can access the web application easily. A web application consists

of n-tiered architecture. They are client, a web server, an application server, and database. Accordingly, it is difficult to ensure the security of the web application. Security should be provided for all the layers of the web application.

The first reported instance of a Web application attack was perpetrated in 2000 by a 17 year-old Norwegian boy. While making online transactions with a large bank, he noticed that the URLs of the pages he was opening displayed his account number as one of the parameters. He then substituted his account number with the account numbers of random bank customers to gain access to the customers' accounts and personal details (Acunetix, 2005).

2.2 Software Security of Web Application

Today, information security is important. Hence, all points of system must be protected. Networks are protected by many methods. These are firewall, IPS, IDS security scanner etc. If hackers cannot find vulnerability from network layer, they try to find from other layers.

The Gartner Group estimates that over 70% of attacks against a company's web site or web application come at the application layer, not the network or system layer (Susan Kennedy, 2005).

Web application can be used by hackers in order to find a gaping hole in the corporate security infrastructure. Always, web applications are publicly available on the Internet. Everybody can access the web application easily. Hackers try to attack web application every time. Every hour of the day they use application and try new web attacks on web application. Web application security is difficult because of these reasons. Web applications have some specific vulnerability. Therefore, they must be protected many points within a system. Figure 1 shows many points within a system.

Figure-1: Web application security concerns

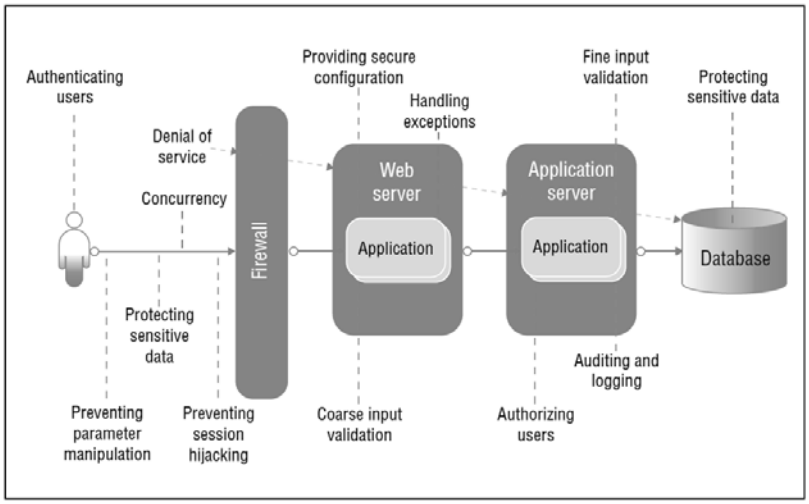


Figure 1: Web application security concerns

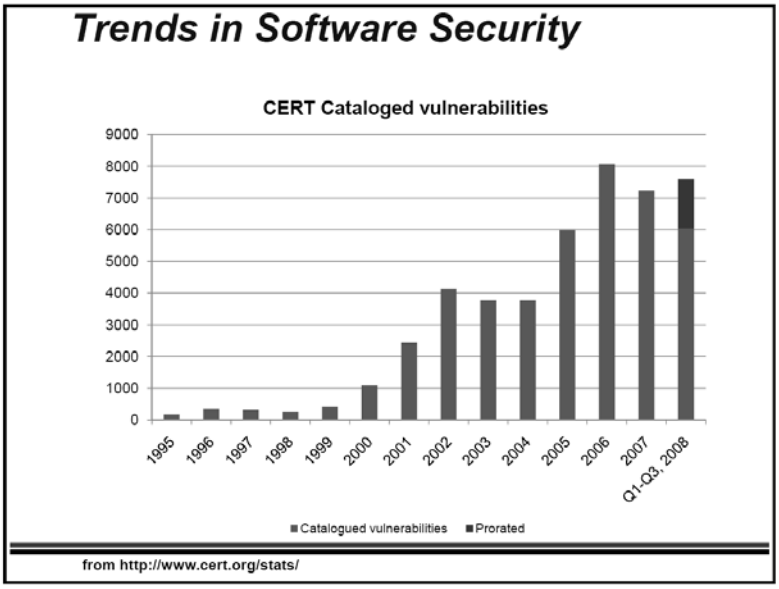
Source: IBM :2008

Every year vulnerabilities are changed. OWASP periodically update the OWASP Top 10. However, a final version will be released in May 2013. The OWASP Top 10 for 2013 is available following (OWASP, 2013):

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Known Vulnerable Components
- A10 Invalidated Redirects and Forwards

Vulnerabilities in software security are changed every year. Figure 2 shows trend in software security.

Figure-2: Trends in Software Security



Source: CERT : 2008

Some protection methods can be used to secure information. There are many methods of protection.

Web application's software life-cycle must include security policy. When the software is designed for the project, it is added to the design of security measures. The incorrect or missing input validation must be controlled. Penetration tests should be performed in order to discover web application's vulnerability. Software code of web application is scanned and found software coding errors**,** vulnerability in software code. Accordingly, only one method will be discussed in this study. This is a web application scanner.

2.3 Web application scanner

A *web application scanner* is an automated program that examines web applications for security vulnerabilities. In addition to searching for web

application specific vulnerabilities, the tools also look for software coding errors, such as illegal input strings and buffer overflows (Hawaii, 2007).

Web application scanners find vulnerabilities in source code of web applications. They give recommendation about protecting to web applications.

Many vulnerability scanning tools are currently available in the market. Some of them are commercial. Some of them are free. For example AppScan tool is developed by IBM and it is commercial tool. OpenVAS tool is developed by OpenVAS and it is free tool.

When application is developed, software life cycle is important. If we want to develop secure web application, we must include information security into software life cycle. Web application scanner helps people to find vulnerabilities in source code. Thus, web application scanner must be used.

2. CONCLUSION

Today information security is important because of information on Internet. People use Internet all aspects of their life. They share on Internet most information on the life of. Therefore information security is important for applications. Testing web application vulnerabilities has become very important. Every layer of web application must be protected. This paper identifies only web application vulnerabilities and web application scanner.

ACKNOWLEDGMENT

Thank Tunc Medeni (YBU, METU, Turkey) for his support for the publication of this paper.

BIBLIOGRAPHY

Acunetix, November 2005, The Importance of Web Application Scanning, http://www.acunetix.com/websitesecurity/the-importance-of-web-application-scanning/, [Accessed 02.03.2013]

CERT (1997), Security of the Internet, http://www.cert.org/encyc_article/tocencyc.html, [Accessed 04.04.2013]

CERT (2008), CERT Statistics (Historical), http://www.cert.org/stats, [Accessed 04.04.2013]

Daniel Petri, (2005), The Importance of Web Application Scanning, http://www.petri.co.il/importance_of_web_application_scanning.htm, [Accessed 24.03.2013]

Dressler, J. (2007). "United States v. Morris". *Cases and Materials on Criminal Law*. St. Paul, MN: Thomson/West. ISBN 978-0-314-17719-3

ISACA (2006), *CISA Review Manual 2006*. Information Systems Audit and Control Association, p.85, ISBN 1-933284-15-3

OWASP (2007), Category: Threat, https://www.owasp.org/index.php/Category:Threat, [Accessed 04.04.2013]

OWASP (2013), Category:OWASP Top Ten Project, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project, [Accessed 04.04.2013]

Proceedings of the 40th Hawaii International Conference on System Sciences, Elizabeth Fong and Vadim Okun (2007), “Web Application Scanners: Definitions and Functions”

SANS , Tanya Baccam, Ralf Durkee, Barbara L. Filkins, Kevin Fuller, Leo McCavana, Mark Williams, Lenny Zeltser, ”Secure Coding. Practical steps to defend your web apps.”, *SANS Software Security FAQ*

Susan Kennedy (2005), Common Web Application Vulnerabilities, http://www.computerworld.com/s/article/print/99981/Common_Web_Application_Vulnerabilities [Accessed 02.03.2013]

Walt Howe (2012), An anecdotal history of the people and communities that brought about the Internet and the Web, http://walthowe.com/navnet/history.html, [Accessed 02.03.2013]

White paper, Rational Software, IBM (2008), Understanding Web application security challenges, Web application security management