Web security in the Finance Sector

Analysing the security of financial web applications – a case study

Tiago Vieira, Carlos Serrão
ISCTE – Instituto Universitário de Lisboa
Ed. ISCTE, Av. das Forças Armadas, 1649-026, Lisboa, Portugal
Lisbon, Portugal
tiago.vieira@iscte.pt, carlos.serrao@iscte.pt

Abstract—**Nowadays, information security is an increasing concern in institutions and organizations. This concern is even greater in the finance sector, not only because the financial amount involved but also clients and organization's private and sensitive information. As a way to test security in infrastructures, networks, deployed web applications and many other assets, organizations have been performing penetration testing (*pentest*) which simulates an attacker's behavior in a controlled environment in order to identify its vulnerabilities. This article focusses on the analysis of the results of security audits conducted on several financial web applications from one institution with aid of automatic tools in order to assess their web applications security level. To help in security matters, many organizations build security frameworks for vulnerability assessment, security assessment, threat modeling, penetration testing, risk management and many more. As for penetration testing, organizations such as OWASP provide vulnerability and security information, a testing methodology, risk analysis and penetration testing tools.**

Keywords-component; web security; finance sector; pentesting; penetration testing; vulnerability; risk analysis; CVSS.

I. INTRODUCTION

Information security is an increasingly concern subject for institutions and organizations who depend on information technology [2]. The finance sector is one with the most valuable assets in information technology. Banking account information, client's sensitive data and transactions are a few examples. They communicate with clients though web platforms and need to insure security and confidentiality. Financial entities are investing in pen(etration) testing, a line of defense in information technology to assert security in applications, systems and networks [1].

A pen test simulates an attacker's behavior (commonly known as hacker) but in a controlled environment to identify and mitigate possible vulnerabilities [3]. A great number of organizations provide frameworks and services to assess security such as pen testing, risk assessment, threat modeling and even teach ethical hacking [4][5][6]. An ethical hacker is a security professional who uses hacking tools and techniques in a legitimate way and with consent from an organization to test and find vulnerabilities in a system [7]. Pen test is used mainly in the end of the software development process. Whether other security software development processes are adopted or not in this life cycle, pen testing will ultimately check software security [8].

This article presents the web testing results, its conclusions and evaluates the tested institution in terms of security maturity. Based on this security audit, a superficial understanding of other financial institutions can be made and what vulnerabilities emerge in the finance sector web applications that are based on the same development technologies. On top of that, link the vulnerabilities found with OWASP Top 10.

II. PENETRATION TESTING (*PENTESTING*)

During the penetration testing (*pentesting*), information security specialists access tools and techniques capable of compromising systems, networks or applications in their confidentiality, integrity and availability [3]. The first step before starting a pen test is make sure the rules of engagement are set and the organization formally authorizes the pen test and its conditions [1]. Pen tests can adopt a black box, grey box or white box approach. In a black box approach, commonly the hacker's environment, is where the ethical hacker has no knowledge of the system he is testing. In the white box approach the systems are well known and there might even be access to the source code [9]. Pen testing is more than just finding vulnerabilities, is also the process of verifying if they can be exploited and suggest possible mitigations [10].

A *pentest* is a complex and time consuming endeavor, not only that, the time windows to perform the tests is short. Before the test begin, they have to be coordinated and accepted with organizations management, the it administrators have to be on alert for any situation and continuing applications development can't be halted. Typically, web applications are also extensive and for that matter, the tests should be organized and methodical so that the best approach is reached.

There are many vulnerabilities in web applications. OWASP [13] keeps track of the top 10 most critical ones (OWASP Top 10) ordered by risk and probability [11]. This list is updated based on data from several security specialized organizations and individuals. Alongside OWASP, Web Application Security Consortium (WASC) is another institution devoted to the development of security standards [12] that also ranks web application security risks.

There are at a security professional disposal a set of *pentesting* methodologies and their use is most important but it's the security team responsible for choosing the one who better suits their needs. A pen testing methodology organizes a testing program and helps organizations prepare an auditing, if applicable [4][5][6].

In this case, the chosen approach was the OWASP Testing Guide. This is the forth release of this open source web testing framework created and maintained by OWASP. OWASP is a nonprofit organization that promotes web security with a vast number of resources produced all connected proving to be one of the best choices in vulnerability testing and risk management. Some examples are the OWASP Code Review Project, the Developers Guide and web scanner OWASP Zed Proxy [4]. The OWASP Testing Guide is a framework exclusive to web security.

III. Web scanners

A web scanner is a tool built to simplify the pen tester task. They are able to perform automatic attacks to web applications with little or none human intervention [14]. One of the main functions of a web scanner is crawling, the ability to discover which pages exist in the web application so that a full test can be made [15]. Web scanners allow fast testing and fuzzing, multiple attack modes and ease the pen tester task. In a black or grey box pen testing where the pen tester has no access to the application source code or when he does not have knowledge of the programming language web scanners are ideal [4]. Despite that, the number of requests a web scanner can perform automatically is substantially bigger than manual testing. The test time reduction and coverage are two of the most important advantages a web scanner can provide [6].

Web scanner functions are based on the most common vulnerabilities through techniques such as fuzzing and input testing therefor, even one tool may not be enough. A web scanner can be most effective in certain circumstances and poor in others. Using more than one tool, can provide better confidence in the test results [6].

The most negative aspect of the automated web scanners is the heavy generation of false positives. These are situations incorrectly classified as vulnerabilities by the web scanner which require the pen tester to spend much time confirming them [16]. Another crucial point of the web scanner are its configuration options - for instance, if a web scanner can't perform authentication, the web scanner will not be able to pass the login page and therefore complete the web application test [16].

The web scanners used in these tests were OWASP Zed Attack Proxy (ZAP) [17] and Burp Professional [18]. ZAP is a free and no limitation web scanner, Burp is a commercial application and the tests were made in a free trial version with full functionality. Both act as proxy, can perform crawling, create a site tree view, identify and classify vulnerabilities as found with explanation and mitigation suggestions. Both tools can build simple reports with all vulnerabilities and issues found in several formats. An attempt to use also W3AF was made, however W3AF is unable to perform automatic POST fuzzing requests and therefore limited its results.

IV. Test Environment

This case study includes results from 4 applications with several modules each based on .Net technologies. The applications were developed by different teams and have different frameworks. Although the applications are accessible outside the tested institution, they are accessible though dedicated secure connections. The tests performed, were accomplished internally.

V. Testing Methodology

Following a methodology helps a pen tester to prepare its audit, prevents from targets being missed and helps organize the process [5]. In this security audit, the OWASP Testing Guide (version 4) methodology steps were followed but with the help of web scanners.

For the financial web applications security audit, and considering the methodology selected, the major ten tasks to consider were the following:

1) ***Setting up web scanner configuration***: The scanner will register all the pen tester actions on the application acting as a proxy and storing HTTP requests. Setting the web scanner proxy configuration, the technologies used such as programming language, specify which pages are to be considered on the web application, is of key importance to track all the desired targets and avoid unnecessary tests.

2) ***Navigate through the web application***: This is important for the pen tester to get acquainted with the application, its purpose, how it is build, and which technologies it supports (such as JavaScript) while the web scanner logs the requests conducted for further analysis.

3) ***Perform the crawling***: Use the scanner web crawler functionality to explore every link it can find in the targeting application. Web scanners are capable of automatically building the entire web application tree structure for analysis and possible attack exploration and vulnerabilities identification.

4) ***Explore the web application crawled pages***: While crawling through the different web application pages, every time it finds new pages, tries to explore them as well.

5) ***Follow the chosen pen testing methodology steps****:* Test every aspect of web security as possible keeping notes, test results and report every critical issue found. In this phase the web scanner can be extremely helpful as it identifies certain security issues just by navigating through the web pages. The web crawler acts as a test accelerator.

6) ***Perform automatic attacks***: Most web scanners have built-in attack capabilities. Using this functionality, it is possible for the web scanner to test the web application against a series of vulnerabilities.

7) ***Perform fuzzing on the web application pages****:* The attack functionality is great for quick results and a better look and feel of the application but, a manual fuzzing can produce more precise attacks. For instance, focusing SQL injection in the login page. Manual fuzzing allows the pen tester to combine the application inputs with the knowledge from the

application behavior's analysis, allowing for targeted or variations on automated attacks, in order to obtain better results from the tests.

8) ***Explore the application logic parameters***: Some parameters have some logic meaning in the application context, and may expect values that the web scanner does not know how to automatically interpret, by opposition to the human *pentester*. Therefore, it is necessary to combine the scanner fuzzing possibilities with the *pentester* knowledge of the web application being tested.

9) ***Exploitation***: In this stage of the methodology it is important to verify if the vulnerability that was identified actually exits and if consists in any danger to the web application security.

10) ***Mitigations and Reporting***: Web scanners can provide useful information to mitigate a vulnerability which should be given to the organization along with the *pentester* complementary information. This information is an output from many web scanners such as ZAP and Burp.

As a recommended procedure, during the tests, it is important to report immediately any critical or strange situation found to the security responsible. In order to have better and more complete results from the *pentest* audit, it is recommended to repeat the entire process using one or more web scanners as a failsafe.

The following section on this article presents and discusses the results of the tests that were conducted on the different financial web applications, while using the automated web scanners and methodology previously identified.

VI. Results and Discussion

This section handles the results obtained during tests. All tests were made in controlled environment that replicate the finals user's platform so that the real system is not affected in performance or availability.

The approach described earlier was followed in order to achieve this results. The amount of logging generated during automatic and manual testing was more that 2Gb of information in requests and responses captured by ZAP and Burp. This amount of data expresses well the advantage of a web scanner usage in terms of performing attacks, identifying and annualizing a great amount of results.

In Figure 1 it is possible to observe the different vulnerabilities that were discovered and confirmed in all the tested applications. For security and confidentiality reasons, no details about the system or provable exploits to the identified application vulnerabilities will be given.

Vulnerabilities listed in Figure 1 are grouped by severity (high, medium, low and information) given by the web scanner during test. The first vulnerabilities listed are the critical ones at the beginning of the chart followed by medium, low and information. The high severity vulnerabilities are also a part of OWASP Top 10 and are confirmed vulnerabilities which may compromise one of the security vectors: integrity, confidentiality or availability.

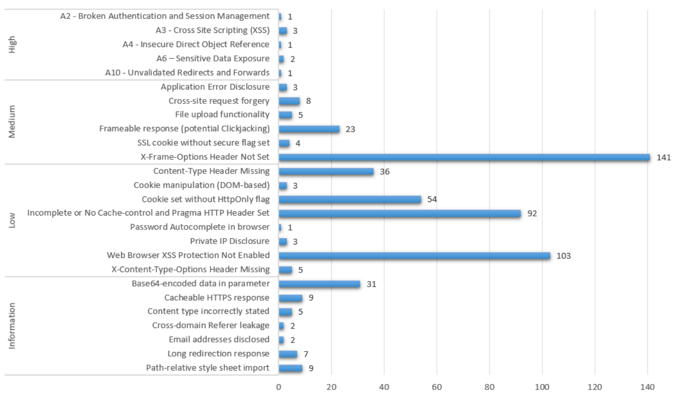

Figure 1 - Vulnerabilities Found

As a result, during the *pentest* auditing were identified and confirmed 26 different vulnerabilities, across 4 applications with several modules each, totaling 554 occurrences.

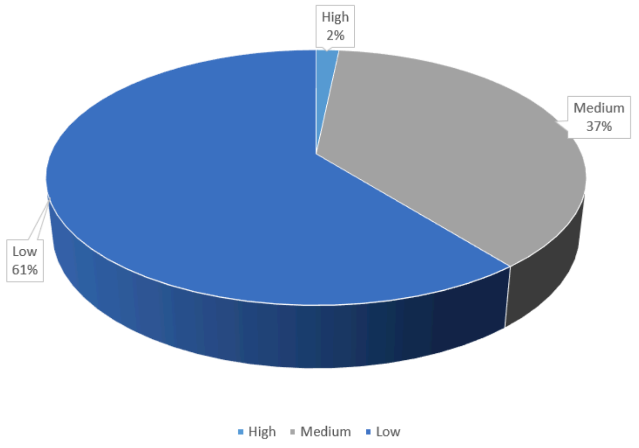

Figure 2 – Vulnerabilities severity distribution

The severity distribution of these vulnerabilities is showed in Figure 2. The number of high severity vulnerabilitites found was 8, 184 with medium severity and 297 with low severity. This classification so far was calculated by the web scanners by may change if a risk analysis is performed. The information severity vulnerabilities were not taken accountable in this distribuition and from here on.

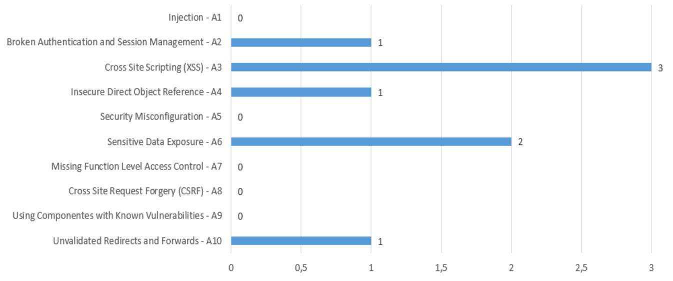

Figure 3 – Owasp top 10 findings

The most critical vulnerabilities found within the OWASP Top 10 are identified in Figure 3. These vulnerabilities were classified has having high severity and therefore should be addressed by the web applications security teams as soon as found, due to the exploitability level of the vulnerabilities discovered.

A2 - Broken authentication and session management: this vulnerability deals with the aspects of handling and maintaining sessions in web applications. A vulnerability of this type may allow an attacker to take the user session and access to his data and his profile in the application.

A3 - Cross site scripting (XSS): XSS allows an attacker to send malicious code through the web application, usually as client side code. A successful script execution is a XSS vulnerability. The malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site.

A4 - Insecure direct object reference: is a reference to an object, file, directory or database without access control. Data manipulation can be achieved by exploiting this vulnerability.

A6 – Sensitive data exposure: this is a confidentiality vulnerability where an attacker gains access to private information like credit card number or other information that can be used to other malicious purpose.

A10 – Invalidated redirects and forwards: consists in allowing page redirect without validation that can lead to phishing or malware sites allowing social engineering.

Cross-site scripting (XSS) was the most recurrent of the OWASP Top 10 vulnerabilities that was found. This kind of vulnerability is ratter dangerous not only because of what mentioned above but also because it can allow to explore social engineering against a user, a conscious user in security matters can avoid many exploits. An updated and modern browser is also an important security measure. In many situations, one institution cannot control what browser the client uses nor keep the web application compliant with new browser versions. More recent browsers already prevent some exploits such as XSS.

In the finance sector, these vulnerabilities may compromise not only systems but also, at a higher scale, compromise businesses. The access to confidential data may leverage competitors in decisions making or attackers to perform fraud and identity theft. The damage in the finance sector ban be monetary or reputational and are hard to calculate [22].

Many kinds of attacks can emerge based on one vulnerability like social engineering can start from an invalidated redirect and forward.

TABLE 1 – VULNERABILITIES FOUND AND FALSE POSITIVES

Vulnerabilities	Total	Severity	FP
A2 - Broken Authentication and Session Management	1	High	
A3 - Cross Site Scripting (XSS)	3		
A4 - Insecure Direct Object Reference	1		
A6 – Sensitive Data Exposure	2		
A10 - Unvalidated Redirects and Forwards	1		
Application Error Disclosure	3	Medium	
Cross-site request forgery	8		
File upload functionality	5		1%
Frameable response (potential Clickjacking)	23		
SSL cookie without secure flag set	4		
X-Frame-Options Header Not Set	141		
Content-Type Header Missing	36	Low	
Cookie manipulation (DOM-based)	3		
Cookie set without HttpOnly flag	54		
Incomplete/ No Cache-control & Pragma HTTP Header Set	92		
Password Autocomplete in browser	1		
Private IP Disclosure	3		1%
Web Browser XSS Protection Not Enabled	103		
X-Content-Type-Options Header Missing	5		
	489		

In Table 1 all vulnerabilities are listed as their false positive occurrence. No precision rate can be calculated because we do not know if there are any other exploitable vulnerabilities but the false positives found are only 2% of the results.

VII. Risk Analysis

The final contribution for this study is a classification of the findings. The chosen framework for risk analysis was Common Vulnerability Scoring System (CVSS) v3. This is the latest version of this industry standard released in the end of 2014. Although it is recent, some studies have concluded that this version provides better risk analysis that it's previous version.

CVSS evaluation consists in capturing the vulnerability main characteristics and compile a score which reflects the risk severity. The calculated score can be translated to a quantitative scale (low, medium and high) [19]. CVSS is set by three groups, the base group, and two optional, temporal and environmental. The base group represents vulnerabilities that don't change in time, the temporal group categorizes vulnerabilities that change over time and the environmental group considers variables specific to the user's environment.

CVSS is a multi-vector vulnerability analysis that can define a vulnerability in such way an institution can understand and prioritize its resolution. Is provides both a qualitative and quantitative risk analysis [20]. CVSS v3 brings a new metric, score. It allows to define what component is compromised by exploiting the vulnerability. Another new important metric is the definition of user interaction needed to explore a vulnerability. Attacks like social engineering are linked to this metric.

With limited resources such as time, in order to choose between two risk for resolution, a score is not enough to understand the consequences for management. That is why the ability to describe and articulate the risk exposure is of great importance. It allows risk exploit understanding and what kind of action and time requires [21].

VIII. Conclusion

Security is critical in the finance sector, each vulnerability can be exploit in many ways and compromise monetary or financially the parties involved. *Pentesting* and important and effective security defense mechanism but the results of a security audit are useless unless mitigations of vulnerability are performed.

Analyzing the results in the web context, even with security considerations in their development, critical vulnerabilities were found. With time and motivation, perhaps even more critical vulnerabilities or with critical consequences could be found.

A superficial comparison can be made in the finance sector where web applications services based on .Net technologies are developed. Although the .Net Framework has defense mechanisms like injection defense, other vulnerabilities may exist their exploit can be dire to the parties involved.

References

[1] M. Walker, CEH Certified Ethical Hacking All-in-one Exam Guide, 2nd ed., McGraw Hill.

[2] A. Razzaq, A. Hur, N. Haider, and F. Ahmad, Multi-Layered Defense against Web Application Attacks, 2009.

[3] M. Buchler, J. Oudinet, A. Pretschner, Semi-automatic security testing of web applications from a secure model.

[4] OWASP Testing Guide v4, https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents.

[5] The CIS Critical Security Controlls for Effective Cyber Defense v6.0.

[6] A. Austin, L. Williams, One Technique is not Enough: A comparison of Vulnerability Discovery Techniques. pp

[7] EC Council, http://eccouncil.org/.

[8] N. Teodoro, C. Serrão, Web application security, 2011.

[9] Y. H. Tung, S. S. Tseng, J. F. Shid, H. L. Shan, W-VST: A testbed for evaluating web vulnerability scanner, 2014.

[10] Choose the best penetration testing method for your company, http://www.techrepublic.com/article/choose-the-best-penetration-testing-method-for-your-company/5755555/.

[11] Owasp Top 10, http://www.owasp.org/index.php/Category:Owasp_Top_TenProject.

[12] Web Application Security Consortium, http//www.webappsec.org/.

[13] OWASP Foundation, https://owasp.org/index.php/About_OWASP#The_OWASP_Foundation

[14] A. Doupé, X. Cova, F. Akowuah, A case study on web application security testing with tools and manual testing, 2014.

[15] WASC Thread classification, http://projects.webappsec.org/f/WASC-TC-v2_0.pdf, 2010.

[16] How to choose a web vulnerability scanner, https://www.acunetix.com/blog/articles/hot-to-choose-web-vulnerability-scanner/, 2010.

[17] OWASP zed atttack proxy web scanner, https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project.

[18] Burp web scanner, https://portswigger.net/burp/.

[19] K. Scarfone, P. Mell, An analysis of cvss version 2 vulnerability scoring, 2019.

[20] A. Younis, Y. Malaiya, Comparing and Evaluating CVSS Base Metrics and Microsoft Rating System, 2015.

[21] E. Wheeler, Security risk management, building an information security risk management program from the gound up, Sungress, pp. 87-103, 2011.

[22] The Damage of a Security Breach: Financial Institutions Face Monetary, Reputational Losses, https://securityintelligence.com/the-damage-of-a-security-breach-financial-institutions-face-monetary-reputational-losses/, 2015.