Web Vulnerability Study of Online Pharmacy Sites

JOANNE KUZMA

University of Worcester, Henwick Grove, Worcester, UK
j.kuzma@worc.ac.uk

Abstract

Background. Consumers are increasingly using online pharmacies, but these sites may not provide an adequate level of security with the consumers' personal data. There is a gap in this research addressing the problems of security vulnerabilities in this industry.

Objectives. The objective is to identify the level of web application security vulnerabilities in online pharmacies and the common types of flaws, thus expanding on prior studies. Technical, managerial and legal recommendations on how to mitigate security issues are presented.

Method. The proposed four-step method first consists of choosing an online testing tool. The next steps involve choosing a list of 60 online pharmacy sites to test, and then running the software analysis to compile a list of flaws. Finally, an in-depth analysis is performed on the types of web application vulnerabilities.

Results. The majority of sites had serious vulnerabilities, with the majority of flaws being cross-site scripting or old versions of software that have not been updated.

Conclusions. A method is proposed for the securing of web pharmacy sites, using a multi-phased approach of technical and managerial techniques together with a thorough understanding of national legal requirements for securing systems.

Keywords: *Security, web applications, online pharmacies, N-Stalker*

1. Introduction

A number of factors have contributed to the increase in online healthcare systems, including web-based pharmacies. The cost savings and ease of use of these sites have created a way for consumers to gain knowledge about their health concerns as well as efficiently purchase less-costly products compared to some traditional pharmacies. Even though an increasing number of consumers are using these sites, these consumers may be under the assumption that the private data they provide to these firms is secure, and that these online firms take care with providing them with a secure purchasing environment. They may also assume that any national data or security protection law extends to all international sites. Although some countries have enacted laws to protect consumer data and mandate secure sites, consumers should realize that legal protection of their data is not comprehensive among all sites due to the myriad of laws (or lack of) across countries and local entities [1].

Internet web applications are highly susceptible to various types of attacks, and more attacks occur every year with unprotected sites [2]. Some of the most common vulnerabilities reported by industry groups include cross-site scripting, injection and buffer overflow flaws [2,3,4]. Several studies of web vulnerabilities have previously been done, and will be discussed in section 2.3 of this paper. However, these studies concentrated only on some aspects of web vulnerabilities, such as Secure Sockets Layer (SSL) encryption, e-mail security and scripting. This research study expands the literature by reviewing a more robust list of vulnerabilities including cross-site scripting, infrastructure vulnerabilities, backup issues and web signature attacks. This study analyzes 60 online pharmacies to determine which types of vulnerabilities were the most common and the level of security protection that consumers can expect from this industry.

2. Framework for Web Security

2.1 Consumer Viewpoint

The growth of online pharmaceutical sales has been growing at an outstanding pace for the past 10 years. According to Claburn [5], a study by MarkMonitor estimates that sales have risen from $4 billion in 2007 to $12 billion in 2008 and the average number of daily visitors at pharmacy sites has risen from 32,000 in 2007 to 99,000 in 2008. The number of potential consumers searching online pharmacy sites for lower-cost medicines has increased, with a 34% increase in the web traffic for the number of people searching for online prescription drugs from first quarter of 2008 to the first quarter of 2009 [6].

The growth of this market is due to a variety of factors. First, the cost of the products is one overriding concern with consumers, especially those with no health insurance. According to the latest study by the U.S. Census Bureau [7], almost 46 million Americans (15.3% of the population) were not covered by health insurance in 2007. Due to the weak global economy, consumers are turning to cheaper alternatives, such as in the case of Americans turning to cheaper foreign pharmacies and spending over $1 billion annually with these firms [8].

The quality of pharmaceutical purchases is another reason for the growth of this market. Cook [9] indicates that with greater exposure to online purchasing, consumers have supplanted the novelty of online purchasing with a desire for a better quality purchasing experience and products that are comparable to offline healthcare options. A reason for the growth of these sites is that costs of pharmaceuticals are lower compared to costs in traditional pharmacies. A study by Quon, Firszt & Eisenberg [10] found that “Americans can save a mean of approximately 24% per unit of drug if they purchase their medications from

Canadian Internet pharmacies instead of from major online U.S. drug chain pharmacies." A more recent analysis by an industry research firm, PharmacyChecker.com [6], finds that brand name medications can often be purchased at a 70% savings in overseas online pharmacies compared to traditional American pharmacies.

The U.S. General Accounting Office [11] and Food and Drug Administration (FDA) official Hubbard [12] emphasize that they recognize the potential benefits of online prescription drug purchasing for American consumers. Hubbard cites several factors that consumers find positive, especially those individuals who are disabled or ill. These benefits include ease of use, convenience, privacy for consumers who have problems they do not wish to discuss in person, and vastly expanded information access.

2.2 Legal Aspects

There is no comprehensive legal protection of online consumers with respect to security of their private information, and most protection would fall under the realm of computer security breaches or privacy laws. Security safeguards are dependent upon a range of various international, national and local laws, and it is difficult for consumers to know the level of protection for a specific pharmacy, as well as the actual security measures the pharmacy site has implemented to secure the purchasing event. For example, a consumer living in California may submit an order from a well-designed web site that appears to originate from the U.S., but may be based in another country. Thus, if a security problem occurred, and their records were compromised, the consumer would not be afforded the same level of legal protection that they might have under U.S. or California law.

In the U.S., the Administrative Simplification portion of the Health Information Portability and Accountability Act of 1996 (HIPAA) was designed to provide the

development of a uniform, computer-based health information system and to address privacy and security of personal health-related data [13]. Although it may be assumed that all types of health care types of web sites, including online pharmacies, would be included in this legislation, this is not necessarily the case. According to Choy [13], HIPAA only applies to three types of entities: health care providers, health plans and health care clearing houses. Because it is often ambiguous which activities are covered under the guise of online pharmacies, it is difficult to ascertain whether a specific U.S.-based online pharmacy would fall under HIPAA legislation. Different rules may apply to different sites offering the same services, and thus consumers may or may not legally have privacy and security protection for a specific US-based online pharmacy.

Due to deficiencies with HIPAA in covering all entities and the lack of consumer notification when computer security breaches occur, the Federal Trade Commission (FTC) proposed a Data Breach Notification Rule in April 2009 [14]. Traditionally, the FTC has concentrated on protecting consumer privacy for traditional commerce, but the growth of new technologies and online health-related entities, such as online pharmacies, has led them to propose this new rule to strengthen privacy and also address security matters, such as data breaches. The Recovery Act expands the types of web-based entities that are not covered under HIPAA, and requires security and breach notification requirements when computer breaches have occurred [14]. However, this is merely a proposed rule, and is not yet in effect.

Other countries may or may not have similar legislation that protects online consumers from security breaches and unsecure data. Under the U.K.'s Data Protection Act of 1998, entities have the legal obligation to protect consumer's personal data and the Act governs responsibilities for those entities storing data. However, there are shortcomings with the law, and additional legislation was introduced in 2008 to include notification requirements for breaches and giving the Information Commissioner the power to conduct computer audits [1].

In Ireland, only businesses on a prescribed list are required to notify consumers of breaches, and in Sweden and Germany, they are not required to notify except under specific circumstances [1]. Some countries in the Asia Pacific region have weak protection. For example, in Japan there is a weak Personal Information Protection Act, while China has no data protection legislation [1].. Thus, with a myriad of different security and protection laws throughout the world, it is difficult for online consumers to establish what level of protection they have when purchasing from these sites.

2.3 Security Problems and Breaches

According to Mello [15], a study of 3,200 online pharmacies monitored by the researchers at MarkMonitor found serious problems with security in online pharmacies. The study found the following problems:

- More than 50% of sites did not secure customer information
- A majority of sites did not use SSL encryption
- In more than 20% of post-purchase e-mails, unencrypted links to customer information were found

Another assessment of over 1,000 Internet pharmacies found that 25% did not secure patient's information [16]. Similar security breaches have occurred in other online health-related sites, such as a major breach of over 800 Kaiser Permanente (KP) members through KP Online, a web-enabled health care portal. Two programmers had written poorly designed scripts which resulted in emails breaching the confidentiality and integrity of the members' personal health information A case study was completed on this breach, and the authors concluded that in order to protect sensitive patient information, safeguards should be built

into online systems in addition to complying with good information security practice and regulations suggested in HIPAA [17].

In 2004, the Office of the Privacy Commissioner of Canada received complaints about a specific online pharmacy alleging that consumers' personal information had been compromised and that the pharmacy had failed to implement computer security safeguards to protect personal sensitive information. After an investigation, the company admitted to a security breach and did institute appropriate safeguards to mitigate future security problems [18].

2.4 Web Application Security

With the growth of electronic commerce, web application security has become a significant concern of consumers whose data may be at risk from unsecured systems. A report by web security firm, Cenzic [2], indicates that for the second half of 2008, almost 80% of all web-related flaws are caused by web applications vulnerabilities, while plugins/ActiveX vulnerabilities are 12%, web browsers are 7% and web servers are 2%. The study further analyzed the major types of vulnerabilities by their particular class, and reported the most common flaws and the percentage of such vulnerabilities:

- SQL Injection – 24%
- Denial of Service – 18%
- Cross-Site Scripting – 14%
- Miscellaneous – 14%
- Buffer Overflow – 11%
- Directory Traversal – 7%

Diverse security firms have reported slightly different results in their top vulnerabilities, although the most common flaws are included within all studies. For example, the Open Web Application Security Project (OWASP), a worldwide free and open community focused on improving application security, publishes a list of common application vulnerabilities, as well as tools and documentation on how to protect systems. For 2007, they list the top five vulnerabilities as

- Cross-Site Scripting
- Injection Flaws
- Malicious File Execution
- Insecure Direct Object Reference
- Cross Site Request Forgery [3]

Another worldwide security organization, the SANS (SysAdmin, Audit, Network, Security) Institute, also lists cross-site scripting, structured query language (SQL) injection and cross site forgery as major web vulnerabilities for 2007 [4]. Thus although various organizations may list certain vulnerabilities in different ranking order, all agree that certain web application vulnerabilities are common across the industry, including scripting and injection flaws.

3. Methodology

The research was accomplished through completing an analysis of 60 online pharmacy sites to determine the most prevalent security problems for these sites. The project consisted of four phases:

1. Choosing an online testing tool
2. Choosing a list of online pharmacy sites to test

3. Running a software analysis
4. Performing an in-depth analysis of the results

3.1 Choosing a Testing Tool

The first phase of the study was to choose a tool which could scan for web application security vulnerabilities for the chosen pharmacy sites. For this project, the researchers were looking for either a free demo version or an affordable version that would test a variety of problems, including scripting issues. In addition, the software had to be installed on a stand-alone PC that would require minimal installation configuration or programming knowledge. A number of tools were evaluated including: International Business Machines (IBM) Rational AppScan, Nessus, Retina and Sara. However, there were a variety of reasons that these products were eliminated including: costs, difficulty in using the product and needing to install the product on a network instead of a personal computer (PC). It should be noted that the functionality and product availability for various platforms was reviewed during the research phase of this project. Between this time and subsequent publication, software versions and functions may have emerged, thus enabling different testing for future research.

The first product that was reviewed was IBM's Rational AppScan (Version 7.9), which appeared very robust and could scan a wide variety of web application vulnerabilities including buffer overflows, cross-site scripting and SQL injection [19]. Although a free download version of the software was offered, this version was limited in only being able to test one pre-defined web site [20]. The second product reviewed was Nessus Vulnerability Scanner (version 4.2.2), from Tenable Network Security. This product had a variety of functions, including vulnerability scanning, auditing, data discovery and configuration auditing, most of which were not a fit for this research project [21].

Retina software from eEye Digital Security (version 5.11.1) was also analyzed. From the documentation, this product was geared more towards network scanning for an enterprise, as opposed to third party vulnerability testing. The installation also required one gigabyte (GB) Ram, Microsoft .NET framework and Microsoft Windows 2000 Server [22], which negated installing on a stand-alone PC. The last piece of software reviewed and rejected was Security Auditor's Research Assistant (Sara) (version 7.9.1), from Advanced Research Corporation. This product could be installed on a standalone PC and checks for a variety of vulnerabilities like cross-site scripting and SQL injection tests, and was free to use [23]. However, after downloading the zipped installation file, it was difficult to progress further with the installation. The downloaded zipped file contained several hundred of installation files and there were no clear-cut directions for installation or use. Due to lack of time to research this product, its use was rejected.

N-Stalker Web Application Security Scanner 2009 Free Edition (version 7.0) was reviewed and chosen. This is a free version of N-Stalker's Enterprise Scanner and is aimed towards individuals and small organizations who wish to perform a more limited vulnerability test than the full functionality contained in their Enterprise-wide scanning tool [24]. However, the level of functional testing for the Free Edition was robust enough for the purpose of this study, which is to test overall vulnerability of online pharmacy sites from a general perspective as opposed to an in-depth penetration testing that would be completed by a security consulting firm. The free version will check up to 100 pages within a target site, and contains the following tests:

1. Cross-Site Script Injection
2. Web Server Infrastructure including Web Server, Platform, secured sockets layer (SSL) encryption, HTTP Method discovery, Directory Brute-Force, hypertext transfer protocol (HTTP) protocol and other vulnerabilities

3. Web Signature Attacks including Internet Information Services (IIS), FrontPage, common gateway interface (CGI) Security, hypertext preprocessor (PHP) Security, active server pages (ASP) Security, SANS Top 20 and other tests
4. Backup security check [25]

After a successful download and installation of this product on a PC, a usability review was done on using the software. It was relatively easy to choose and configure options for testing, and an easy-to-read report of vulnerabilities was produced. Figure 1 shows the resulting screen print of the initial test after installation. The column 'Scanner Events" shows the specific vulnerabilities for this site in an easy-to-understand format. Therefore, because the level of functional testing, ease of installation, free cost and comprehensive testing report, N-Stalker was chosen for this study.

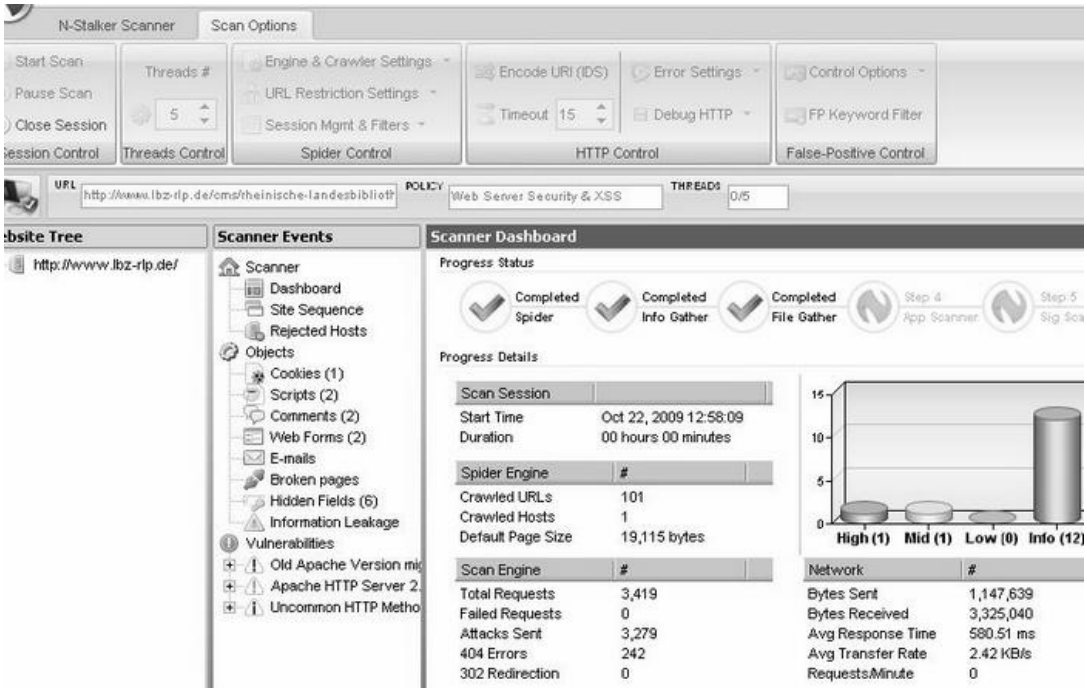

Figure 1: Screen print of N-Stalker testing report

3.2 Choosing Testing Sites

The second phase of this project was to choose a list of online pharmacies to test. An advanced Google search was used to find the top 60 results of online pharmacies using the following criteria:

- Search within site domain = .com
- Keywords = online pharmacy

Although thousands of Google results were displayed, only the top commercial sites were chosen. When reviewing the results, each site was reviewed and only sites that sold products and had shopping carts were added to the list. Some of the sites in the top were purely informational sites, such as www.pharmacychecker.com, so these sites were discarded. Thus, 60 functional e-commerce sites were compiled, and the complete list is shown in Appendix A.

3.3 Running the Software Analysis

For this study, the N-Stalker free edition software was downloaded from the vendor's web site, and then installed on a PC. For each online pharmacy, the Uniform Resource Locator (URL) for the pharmacy's home page was inserted into the Scan Wizard box and scans were run on the pharmacy site. The cross-site scripting, web signature attacks and web server infrastructure functions were chosen to test. Each specific test took between 0.5 and 3 hours to run, depending upon the size of the pharmacy site, number of pages and number of vulnerabilities found in the test results. The software then scanned the URL for a number of web application vulnerabilities.

After the test was completed, a report was produced showing a list of web vulnerabilities. Each vulnerability was categorized into one of three levels:

- High level – severe problems that had serious repercussions on web application security and could lead to a high risk of damage or potential of attacks. These issues should take precedence when setting a schedule for correction.
- Medium – moderately ranked problems that could pose some level of risk to users of the web application. These should be corrected, but after high-level issues are fixed.
- Informational – messages that probably posed little or no issue of risk to users, but still should be reviewed and addressed by web developers.

This phase of the study was completed in June 2009, with the use of N-Stalker to determine the main types and quantities of vulnerabilities for each site. One issue was found when attempting to run the scan for the site http://www.online-pharmacy.cc/. N-Stalker produced an 'Access Violation' problem and the scan was aborted. Therefore, another pharmacy was substituted. The raw data from the results was then compiled into tabular format and analyzed.

4. Analysis of Results

Table 1 shows a compiled report of vulnerability testing results of the 60 online pharmacies. The first column shows various statistical results, while the second, third and fourth columns various severity level results: the quantity of high, medium and informational priority levels for specific vulnerabilities. The first and second rows show the total numbers of vulnerabilities (351 high level, 7576 medium and 405 informational) for all 60 sites and the mean value of flaws per each site (5.85 high, 126.3 medium and 6.75 informational).

There was a wide range of the number of total vulnerabilities for each site. High priority issues ranged from 0 to 73, medium level ranged from 0 to 2091 and informational messages

ranged from 0 to 23 per site. Regarding the specific types of flaws, the high category ranged from 0 to 12, while medium priority ranged from 0 to 252, and informational ranged from 0 to 3. An example for the prior two rows would mean that one type, such as 'old mod ssl versions', could be found for that URL, thus counting as one occurrence in the 'range of vulnerability types per site.' However, each pharmacy site could contain one or many occurrences of that specific vulnerability. So a site like http://www.speedyhealth.com/ might contain the high priority issue 'old mod ssl versions', but could have 12 occurrences located on various pages throughout the site.

In addition, the fifth row in Table 1 shows the number of sites that had no specific vulnerabilities for each of the three priority levels. Thirty sites did not contain any high priority flaws, while 12 sites did not have any medium priority vulnerabilities and only four sites contained no informational messages. The final row contains the totals for how many different types of vulnerabilities were found for all combined sites. In this study, there were 31 high-priority and 481 medium priority errors types, and 3 different informational vulnerabilities.

Table 1. Vulnerability Testing Results

Vulnerability Issues	**High**	**Medium**	**Informational**
Number of vulnerabilities for all 60 sites	351	7576	405
Mean number of flaws per site	5.85	126.3	6.75
Range of total number of vulnerabilities per site	0 to 73	0 to 2091	0 to 23
Range of types of flaws per site*	0 to 12	0 to 252	0 to 3
Number of sites with no vulnerabilities	30	12	4
Total number of different types of vulnerabilities for all 60 sites	31	481	3

*****Refer to Table 2 for details on types

Results in Table 2 show the most common vulnerability types for each of the three severity levels: high, medium and informational. Although a large number of flaws (31 high and 481 medium) were compiled for each level, this table only shows the top 10 vulnerabilities. For the informational issues, only three different types were exhibited in the scanning results. Column 2 of Table 2 differentiates the specific web vulnerability messages that were produced in the N-Stalker report. The last two columns show the total number of occurrences for that vulnerability, along with the number of sites that contained that vulnerability.

Table 2. Most Common Problem Types

	Total Number of Errors	**Number of Sites per Error**
High Level		
SAP Internet Transaction Server COMMAND Cross-Site Scripting	86	4
SAP Internet Transaction Server URLMME Cross-Site Scripting	86	4
E-business Designer 3.1.4 Multiple Input Validation	47	1
Mini-SQL w3-msql 2.0.11 Buffer Overflow	22	2
Old OpenSSL Version Might Be Susceptible	18	14
Old apache Version May Be Susceptible	17	17
Old Mod_ssl versions Might Be Susceptible	11	11
CGI-Club im TRBBS 1.0.2 Remote Command Execution	9	1
Microsoft Windows 2000 Resource Kit W3Who.DLL	9	11
MyServer 0.6.2 Multiple Remote Math_sum.mscgi Example Script Vulnerability	9	1
Medium Level		
Apache 2.0 Encoded Backslash Directory Traversal	277	1
Possible Cross-Site Scripting and/or HTML Injection	262	11
WebMod 0.48 AUTH W Cross-Site Scripting	136	4
Aestiva HTML/OS 2.4 Cross-Site Scriptng	134	5
NetWin Dnews 57e1 Dnewsweb EXE Cross-Site	101	4

	Scripting		
	OmniHTTPD 2.4 Sample Scripting Cross-Site Scripting	98	6
	Lilikoi Software Celldh 2.70 Cross-Site Scripting	94	4
	Lighthouse CMS 1.1 Search Cross-Site Scripting	93	5
	Box UK Amaxus 3.0 Cross-Site Scripting	92	5
	Sambar Server 6.1 beta2 Administrative Interface Multiple Cross-Site Scripting	90	4
Informational			
	Uncommon HTTP Methods Supported	385	53
	Downloadable Object Found	16	4
	Directory Allows for File Listing	12	3

Among the high priority vulnerabilities, there were a sizable number in various categories within the top 10 results. The top 2 error types belonged to cross-site scripting issues, with 86 total occurrences found in four different sites for each of these scripting flaws. Input validation (47 errors in one site) and buffer overflows (22 errors in two sites) were also numerous. Three other common types dealt with old versions of software, such as OpenSSL, Apache, and mod_ssl.

Cross-site scripting vulnerabilities also showed up quite frequently in the medium priority category. Although the most common medium level flaw was an Apache Directory Traversal vulnerability (277 occurrences for one site), the other 9 most common errors were all related to cross-site scripting issues.

The most common informational message was ‘Uncommon HTTP Methods supported,’ which occurred 385 times in 53 sites. Other common messages were ‘Downloadable Object Found’ (16 occurrences in four sites) and ‘Directory Allows for File Listing’ (12 occurrences in three sites).

5. Technical Implications

Evaluation results showed that the majority of sites (80%) had either critical or medium-level vulnerabilities, which could pose grave problems to online consumers who use the sites. Old software version is a flaw common in the high priority vulnerability level. Although only three types of 'old' software issues were listed in Table 2, there were three other vulnerabilities of this type that were actually included in the raw data: a) old .NET framework version (two occurrences), b) old version of mod_python (one occurrence) and c) old versions of Microsoft-IIS (19 occurrences). Thus, combining these numbers and the results of the three types found in Table 2, there were 68 occurrences of version-type problems, of which a site could possibly have several occurrences depending upon which type of software they have installed. In order to fix this vulnerability, N-Stalker [25] recommended that the software be upgraded to the latest version.

One other problem that relates to older versions of software and not installing upgraded versions deals with the medium level vulnerability 'Apache 2.0 Encoded Backslash Directory Traversal.' A vulnerability exists in the default installation of Apache, as well as versions earlier than 2.0.39. The exploitation could result in disclosure of sensitive information, and it is recommended that the site operator install an updated version of Apache [25]

Although security experts recommend prompt upgrades of software upgrades and patches, this study clearly shows that this recommendation is not being implemented by many site operators. Cox [26] lists several reasons why developers may not perform timely upgrades including.

1. Developers "install and forget." They install a default piece of software and forget that it needs to be kept up-to-date to maintain security.
2. The users may not consider security flaws worth worrying about. With so many vulnerability released each day by attackers, developers may have difficulty trying to determine which upgrades and important and which are trivial.

3. Developers may not perform the upgrade correctly. For example, they may properly upgrade a new version of OpenSSL, but then may forget that the Apache server also needs to be restarted in order to pick up shared libraries.

One of the most common informational messages was ‘Uncommon HTTP Methods supported,’ where N-Stalker determined that an insecure HTTP method was detected in the web server, which could lead to possible exploitation. Web developers can use several HTTP methods in their applications including: a) GET, b) HEAD, c) POST, d) PUT, e) DELETE, f) TRACE and g) CONNECT [27]. According to W3C [28] “the GET and HEAD methods should not have the significance of taking an action other than retrieval. These methods ought to be considered "safe". This allows user agents to represent other methods, such as POST, PUT and DELETE, in a special way, so that the user is made aware of the fact that a possibly unsafe action is being requested.” Thus, if a web developer improperly uses a TRACE verb, N-Stalker [25] indicates that information leakage problems could occur, or this method could reveal internal private HTTP Headers. N-Stalker also cautions that a method such as DELETE may allow for arbitrary file uploading and should not be available under normal conditions. Thus, web developers should take care in using HTTP methods and use those considered ‘safe.’

Other common web application flaws that were also found in 2007 and 2008 industry reports included cross-site scripting, buffer overflow, injection and traversal flaws [1, 2, 3]. These types of problems, especially cross-site scripting vulnerabilities, were found prominently in this study. The SANS Institute [29] indicates that to protect against these flaws, developers should engage in strong coding practices and use input validation methods to validate data before storing or displaying it. Injection flaws can occur when attackers trick an interpreter into executing unintended commands. This vulnerability can be minimized by either avoiding interpreters in coding, or if requiring their use, then practicing safe coding

practices such input validation and showing care when using stored procedures [30]. Buffer overflows are best minimized by keeping up with security patches to web application servers and proper input coding validation [31].

6. Design and Business Implications

Besides reviewing their web applications for specific web vulnerabilities such as cross site scripting problems, designers and site owners also need to take a broader approach to their overall security and realize that they should take a multi-phase approach to their security agenda. First, they must realize that effective web application security is a business factor in running a successful firm, not just a technical issue. Ko and Dorantes [32] performed a study to gauge the market reaction and change to financial performance after the announcement of security breaches. Their results show that breaches can have a negative impact on the short-term financials of the firm, although they do not contribute to long-term economic impact. They suggest that immediately after the breach, companies enact stronger security measures to prevent future breaches, thus having a positive impact on the future of the firm. However, companies should understand that in the short term, they can suffer from negative publicity, financial problems and loss of time as employees struggle to contain the impacts of the breach. The financial setbacks to a firm can be sizable. A study by the Ponemon privacy and information management research institute reported that of 43 data breaches at large firms, it found that the average per-incident cost range to $6.65 million in 2008, with the cost per compromised customer estimated at $202. Most of the costs were attributed to business loss of angry customers abandoning the firm due to the loss or compromising of their personal data [33]. Thus, with the potential for actual financial loss and bad publicity among customers, firms should put security into the light of protecting their business assets.

Setting aside enough funding for web application security should be of critical concern to firms. However, with the economic budget crisis, many firms are holding back on setting appropriate security budgets. Even though web application vulnerabilities comprise 80% of web attacks, firms are not increasing funds for web applications, even though they are still spending money on network security [2]. This is a shortsighted view and displays a lack of priority-setting for a significant portion of a firm's business.

Within a multi-phased approach to securing web applications, pharmacy site owners and developers need to emphasize secure application development as a priority. Waters [34] indicates that it is ultimately the developers who are responsible for application security. However, instead of the firm emphasizing rapid development and finishing projects as soon as possible while spending the least amount of money, site owners and managers need to put just as high a priority on securing the systems. However, this often does not happen in many web application projects. Sergey Gordeychik, a contribution to the Web Application Security Consortium (WASC), indicates that most web applications are vulnerable and security requirements are often not considered in the system design, making them vulnerable to breaches [35].

Site owners should understand how the legal issues can affect their business. Online pharmacies should review applicable federal, state and local ordinances with regards to security and personal data safeguards. Many laws have already been passed, and others are pending, so it would be wise for pharmacies to coordinate with their legal advisors to properly assess and analyze applicable and upcoming legislation [36]. In addition, mandatory workshops or training for staff and developers should be held in order to update them on their legal obligations to providing secure systems and safeguarding consumer data. Staff should understand how to properly handle data, and application developers should be taught how

improper security development could have an adverse affect on the school from a legal standpoint.

Perceived lack of trust or ineffective security can have an adverse effect on consumer perception of online health portals and some site owners have implemented measures to increase this level of trust and provide consumers the opportunity to review security robustness of the site [37]. Luo & Najdawi [37] analyzed consumer health sites and suggested that site owners have self-regulating policies such as publishing their privacy and security policies directly on their site. Consumers could then check the sites security practices and procedures, and determine whether they wish to purchase from a pharmacy based on stated practices. Although this allows for consumers to gage some measure of a firm's security measures, self-regulating policies are not standardized and consumers may find a large difference in detail among sites [37].

Another method consumers can use to review security levels is to check if the site has a third-party seal or code of conduct. Third-party seals are licensing programs where sites can be accredited in a specific area by a third-party organization. There are five main categories of seals: a) reliability web site seals, b) security seals, c) vulnerability web site seals, d) privacy seals and e) consumer ratings seals [38]. To check for overall online security, consumers could check if a site has a seal from firms such as Verisign, Comodo, and GeoTrust validating that a site has SSL protection (or a 'lock' image at the bottom of the browser window) [38]. Vulnerability Web site seals, such as HackerSafe and SquareTrade, signify that a third-party firm scans the site periodically for common security vulnerabilities [38]. One caveat for consumers is that is that it may be confusing on how the third-party seals are differentiated and which functions each provides. For example, the HONcode seal is often included on health-related sites and evaluates the reliability of health information on the sites, but does not review security vulnerabilities [39]. Also, consumers should understand that

although a vulnerability seal may provide some level of security mitigation, new vulnerabilities do appear quickly and may not necessarily be caught in a monthly third-party scan.

7. Conclusion

This research shows that a preponderance of worldwide online pharmacy sites do not provide adequate protection to their consumers. Almost all sites showed a range of vulnerability flaws, especially cross-site scripting and old versions of software that have not had security patches applied. The main types of issues displayed in these pharmacy sites correspond to the top vulnerabilities found by security industry groups. Although it is impossible to make an application 100% secure, site owners and developers can still utilize a multi-phased approach to minimizing vulnerabilities to their site. Besides implementing published technical updates and safe coding practices, developers and site owners should also become more educated on the business reasons and legal mandates that make a secure site advantageous from a business perspective. This multi-phased approach to security will provide a better level of consumer protect and ultimately lead to higher levels of consumer trust and profitability.

Appendix A: List of Pharmacy Sites Tested

Company	URL
Official Medicines	http://officialpharmacy.com/
Discount Online Pharmacy	http://westmeds.com/
Abconlinepharmacy.com	http://www.abconlinepharmacy.com/ns/customer/home.php
AffordableRx.com	http://www.affordablerx.com/
Alismed	http://www.alismed.com/
Allcures.com	http://www.allcures.com/
Allpharmacy.com	http://www.allpharmacy.com/
VitoPharma	http://www.andrespharmacy.com/
Buy-pharmacy-online.com	http://www.buy-pharmacy-online.com/
Canadadrugspharmacy.com	http://www.canadadrugpharmacy.com/

CanadaDrugs.com	http://www.canadadrugs.com/
CanadaDrugsOnline	http://www.canadadrugsonline.com/
Canada Pharmacy	http://www.canadapharmacy.com/
Canadianpharmacychoice.com	http://www.canadianpharmacychoice.com/
Canadianpharmacymeds.com	http://www.canadianpharmacymeds.com/
Canada Online Healthlink	http://www.candrugstore.com/
Clockwork Pharmacy	http://www.clockworkpharmacy.com/
Costapharmacy.com	http://www.costapharmacy.com/
DirectChemist.com	http://www.directchemist.com/
DoctorSolve Healthcare	http://www.doctorsolve.com/
DrugsBoat Online Pharmacy	http://www.drugsboat.com/
Drugs-Med.com	http://www.drugs-med.com/
Drugstore.com	http://www.drugstore.com/
Drugstore Telemedicine	http://www.drugstoretm.com/
Epharma2u.com	http://www.epharma2u.com/
Euromedspharmacy.com	http://www.euromedspharmacy.com/
Centralux ltd	http://www.exactfindrx.com/
Freedom Pharmacy RX	http://www.freedompharmacyrx.com/
European Pharmacie	http://www.globalpharmacie.com/
RF Drugstore	http://www.gonorthpharmacy.com/
Health Check Pharmacy	http://www.healthcheckpharmacy.com/
Internationaldrugmart.com	http://www.internationaldrugmart.com/
Labodiscount	http://www.labodiscount.com/
Medicones2u.com	http://www.medicines2u.com/
Medrx-One	http://www.medrx-one.com/
Meds4u	http://www.meds4u.com/
mexmeds4you.com	http://www.mexmeds4you.com/home.asp
Mrs Pharmacy	http://www.mrspharmacy.com/
Multipharmacy.com	http://www.multipharmacy.com/
My Dispensary	http://www.mydispensary.com/
Norton Clinic	http://www.nortonclinic.com/
Onlinepharmaciescanada.com	http://www.onlinepharmaciescanada.com/
Online-pharmacy.cc	http://www.online-pharmacy.cc
Online Pharmacy Meds	http://www.onlinepharmacymeds.com/
Orderpharma.com	http://www.orderpharma.com/
PharmacyRxWorld.com	http://www.pharmacyrxworld.com/
Pillsforall	http://www.pillsforall.com/
Planetdrugsdirect.com	http://www.planetdrugsdirect.com/
Reach Pharmacy	http://www.reachpharmacy.com/
Rxeruope.com	http://www.rxeurope.com/
Rxfastfind.com	http://www.rxfastfind.com/
Rxmedscanada.com	http://www.rxmedscanada.com/
Speedyhealth.com	http://www.speedyhealth.com/
Squaremeds.com	http://www.squaremeds.com/
TabMD.com	http://www.tabmd.com/
Tl-pharmacy	http://www.tl-pharmacy.com/
Travelpharm.com	http://www.travelpharm.com/
Ukmedix	http://www.ukmedix.com/
Universal Drugstore	http://www.universaldrugstore.com/
WorldRxStore.com	http://www.worldrxstore.com/

Appendix B: List of Abbreviations

ASP	Active Server Pages
CGI	Common Gateway Interface
FDA	Food and Drug Administration
FTC	Federal Trade Commission
GB	Giga byte
HIPPA	Health Insurance Portability and Accountability Act
HTTP	Hypertext Transfer Protocol
IBM	International Business Machines
IIS	Internet Information Services
KP	Kaiser Permanente
OWASP	Open Web Application Security Project
PC	Personal Computer
PHP	Hypertext preprocessor
SANS	SysAdmin, Audit, Network, Security
Sara	Security Auditor's Research Assistant
SQL	Structure Query Language
SSL	Secured Sockets Layer
WASC	Web Application Security Consortium

Declaration of interest: The author reports no conflicts of interest. The author alone is responsible for the content and writing of the paper.

References

[1] Castro-Edwards, J. "Data Protection: Where Are We Now?", Journal of Database Marketing and Customer Strategy Management, 2008, December. Vol. 15, No. 4, pp. 285-292.

[2] Cenzic [Internet]. "Web Application Security Trends Report Q3-Q4, 2008",2009, Available from: http://www.cenzic.com/downloads/Cenzic_AppSecTrends_Q3-Q4-2008.pdf

[3] Open Web Application Security Project (OWASP) [Internet]. "Top 10 2007", 2008. Available from: http://www.owasp.org/index.php/Top_10_2007#Introduction.

[4] SANS Institute [Internet]. "SANS Top-20 2007 Security Risks (2007 Annual Update)", 2009. Available from: http://www.sans.org/top20/#s1.

[5] Claburn, T. [Internet]. "Online Pharmacy Risks Rising", *Information Week*. 2008, August 26. Available from: http://www.informationweek.com/news/internet/security/showArticle.jhtml?articleID=210200864

[6] PharmacyChecker.com [Internet]. "Online Prescription Drug Searches Surge 34% Over Past Twelve Months", 2009, April 6. Available from: http://www.pharmacychecker.com/news/online_drug_searches_surge_040609.asp

[7] U.S. Census Bureau News [Internet]. "Income, Poverty, and Health Insurance Coverage in the United States: 2007", U.S. Census Bureau, 2008, August, Available from: http://www.census.gov/prod/2008pubs/p60-235.pdf

[8] CBC News [Internet]. “Prescription drugs: more business for Canadia online pharmacies?” 2009, February 27, Available from http://www.cbc.ca/health/story/2009/02/27/f-onlinedrugs.html
[9] Cook, D., Joseph, J., & Morton, R. “Quality drivers for e-pharmaceuticals system management: a theoretical framework”, *International Journal of Electronic Business*. 2004. Vol. 2, No. 2. pp 174-192.
[10] Quon, B., Firszt, R., & Eisenberg, M. “A Comparison of Brand-Name Drug Prices between Canadian-Based Internet Pharmacies and Major U.S. Drug Chain Pharmacies”, *Annals of Internal Medicine*. 2005. Vol. 143, No. 6, pp. 397-403.
[11] U.S. General Accounting Office. [Internet]. Internet pharmacies—adding disclosure requirements would aid state and federal oversight. 2000, October 19. Available from: www.gao.gov/cgi-bin/getrpt?GAO-01-69
[12] Hubbard, W. K. “Internet pharmacy consumer safeguards”, *FDCH Congressional Testimony*. March 27, 2003.
[13] Choy, A., Hudson, Z., Pritts, J. [Internet]. “Exposed Online: Why the new federal health privacy regulation doesn't offer much protection to Internet users*”, Report of the Pew Internet & American Life Project, Health Privacy Project*. 2001, November, Available from: http://www.pewinternet.org/~/media//Files/Reports/2001/PIP_HPP_HealthPriv_report.pdf.pdf
[14] U.S. Federal Trade Commission (FTC), [Internet]. “Health Breach Notification Rule”, 2009. Available from: http://www.ftc.gov/os/2009/04/R911002healthbreach.pdf
[15] Mello, J. [Internet]. “Online Pharmacy Brandjacking: Buyer Beware”, *E-Commerce Times*, 2007, August 25. Available from: http://www.ecommercetimes.com/rsstory/58999.html?wlc=1243690944
[16] National Association of Boards of Pharmacy (NABP) [Internet]. “NABP Findings Underscore Dangers of Purchasing Prescription Medicine Online and from Foreign Sources”, 2008, October 23. Available from: http://www.nabp.net/news/nabp-findings-underscore-dangers-of-purchasing-prescription-medicine-online-and-from-foreign-sources/
[17] Collmann, J., Cooper, T. “Breaching the Security of the Kaiser Permanente Internet Patient Portal: the Organizational Foundations of Information Security”, *Journal of the American Medical Informatics Association*. 2007, March-April. Vol 14, No. 2, pp. 239-243.
[18] Office of the Privacy Commissioner of Canada [Internet]. “PIPEDA Case Summary #2005-310, Commissioner initiated complaints against Internet pharmacies”, 2005. Available from: http://www.priv.gc.ca/cf-dc/2005/310_20050525_e.cfm.
[19] IBM [Internet]. “Rational AppScan ”, 2009. Available from: http://www-01.ibm.com/software/awdtools/appscan/standard/features/?S_CMP=rnav&S_CMP=rnav
[20] IBM [Internet]. “Trial: Rational AppScan”, 2009. Available from: http://www.ibm.com/developerworks/downloads/r/appscan/learn.html?S_TACT=105AGX28&S_CMP=TRIALS.
[21] Tenable Network Security [Internet]. “Nessus Vulnerability Scanner Features”, 2009. Available from: http://www.tenablesecurity.com/nessus/features/
[22] eEye Digital Security [Internet] “Retina Network Security Scanner”, 2009. Available from: http://www.eeye.com/html/products/retina/specs/index.html.
[23] Advanced Research Corporation [Internet]. “Security Auditor’s Research Assistant”, 2009. Available from: http://www-arc.com/sara/.

[24] N-Stalker [Internet]. "N-Stalker Free Edition", 2009. Available from: http://nstalker.com/products/free
[25] N-Stalker [Internet]. "N-Stalker Security Checks", 2009. Available from: http://nstalker.com/products/security-checks
[26] Cox, M. [Internet]. "Apache Security Secrets: Revealed", *Proceedings of ApacheCon 2002*, Los Angeles, Ca. 2002. Available from: http://www.awe.com/mark/talks/tu04-handout.pdf.
[27] W3C [Internet]. "Hypertext Transfer Protocol – HTTP/1.1 RFC 2616 Method Definitions", 2004. Available from: http://www.w3.org/Protocols/rfc2616/rfc2616-sec9.html.
[28] W3C [Internet]. "RFC 2616: Hypertext Transfer Protocol – HTTP/1.1", 2004. Available from: http://www.w3.org/Protocols/rfc2616/rfc2616.html
[29] SANS Institute [Internet]. "SANS Top-20 2007- Cross Site Scripting", 2009. Available from: http://www.owasp.org/index.php/Top_10_2007-A1.
[30] SANS Institute [Internet]. "SANS Top-20 2007 – Injection Flaws", 2009. Available from: http://www.owasp.org/index.php/Top_10_2007-A2.
[31] SANS Institute [Internet]. "Buffer Overflow", 2009. Available from: http://www.owasp.org/index.php/Buffer_Overflow.
[32] Ko, M., & Dorantes, C., "The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation", *Journal of Information Technology Management*. 2006. Vol. 17, No 2, pp 13-22.
[33] White, K. [Internet]. "Breach costs on the up", *Computer Business Review*. 2009, February 2. Available from: http://www.cbronline.com/news/datalossmeanslostcustom_020209.
[34] Waters, J. "IT Security: Target: The Web", *T.H.E. Journal*, 2009, February. Vol. 36, No. 2.
[35] Moscaritolo, A. [Internet] "Web apps account for 80 percent of internet vulnerabilities", *SC Magazine*. 2009, March 18. Available from: http://www.scmagazineus.com/Web-apps-account-for-80-percent-of-internet-vulnerabilities/article/129027/.
[36] Salomon, K., Cassat, P., & Thibeau, B. [Internet] "IT Security for Higher Education: A Legal Perspective", *EDUCAUSE*, 2003, March 20. Available from: http://net.educause.edu/ir/library/pdf/CSD2746.pdf
[37] Luo, W. & Najdawi, "Trust-building Measures: A Review of Consumer Health Portals", *Communications of the ACM*, 2004. Vol. 47, No. 1, pp. 109-113.
[38] TRUSTe, [Internet]. "Making Sense of Web Site Privacy and Security Seals", 2010. Available from http://www.truste.com/privacy_seals_and_services/consumer_privacy/Seal_Comparisons.html
[39] Yap, K., Raaj, S. & Chan, A. "OncoRx-IQ: a tool for quality assessment of online anticancer drug interactions", International Journal for Quality in HealthCare, 2010. Vol. 22, No. 2, pp. 93-106.