Security on Government Websites

Luis M. Oliveras Reyes
Master in Computer Science
Dr. Jeffrey Duffany
Electrical & Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

Abstract *— Given the advances in technology and the cyber-attacks; new viruses that affect networks, computers, servers and other principal elements within any infrastructure on government agencies, the following question should be asked: Are government users web site data are secure? The government of Puerto Rico has been criticized for not having a good infrastructure within its web pages. This year appeared a news in which it was said about an attack that was realized to one of the pages of government. Rut N. Tellado Doménech [1] and Obed Borrero [2]. It tells us that a government website and other sites of Puerto Rico had been attacked and taxpayer information was in danger of being compromised. That is why it is important to do an investigation of how secure are the web pages of the government of Puerto Rico and how to detect all vulnerabilities on the sites.*

Key Terms *— Cyber-Attacks, Government, Vulnerabilities, Websites.*

VULNERABILITIES ON WEBPAGES

A security vulnerability [3] is a weakness in a product that could allow an attacker to compromise the integrity, availability, or confidentiality of that product. Security vulnerabilities involve inadvertent weaknesses; by-design weaknesses may sometimes occur in a product, but these aren't security vulnerabilities. Security vulnerabilities are a result of a problem in a product. Problems that result from adhering to imperfect but widely accepted standards are not security vulnerabilities. For this reason, the vulnerabilities compromise: Availability, Confidentiality and Integrity. In computer security, a weakness in the physical layout, organization, procedures, personnel, management, administration, hardware or software that may be exploited to cause harm to the ADP system or activity. In conclusion, we need to identify the vulnerabilities to make sure all the systems are secure.

Advantages for users:

- Protect their information
- Give relief with top security
- Stay away from phishing sites

Advantages for Owners:

- Increase ROI
- Google ranking benefits
- Increase website legitimacy
- Secure communication between Browsers and Server

INVESTIGATION

In this investigation, I will make an analysis in the security inside the website of the Treasury of Puerto Rico (Hacienda). First, I make an initiative to verify several things: analysis of the common ports, analysis of the HTML code to check if this implies in the security of the website. On this webpage, the mission is to identify different security elements to make sure that this webpage was secured to the users. In conclusion, this research verifies a series of principal elements to verify the security of the website.

Figure 1
SSL Secure Connection

WEB APPLICATION SECURITY

Web application security [4] is the process of securing confidential data stored online from

unauthorized access and modification. This is accomplished by enforcing stringent policy measures. Security threats can compromise the data stored by an organization is hackers with malicious intentions try to gain access to sensitive information.

The aim of Web application security is to identify the following:

- Critical assets of the organization.
- Genuine users who may access the data.
- Level of access provided to each user.
- Various vulnerabilities that may exist in the application.
- Data criticality and risk analysis on data exposure.

INVESTIGATION PROCESS

In this investigation, I will make an analysis in the security inside the website of the Treasury of Puerto Rico (Hacienda). On this part I make an initiative to verify if the common ports and the HTML code to check if were open and what this implies to the security of the website. On this webpage, I identify a different security element to make sure that this webpage was secured to the users.

First, I'll checked one of the most common security issue on webpage: "https" protocol. HTTP VS HTTPS. Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted. HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms. Web browsers such as Internet Explorer, Firefox and Chrome also display a padlock icon in the address bar to visually indicate that a HTTPS connection is in effect. In this case I'll used Google Chrome to check the security method.

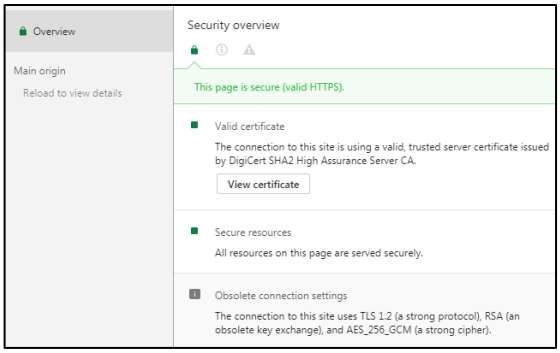

Figure 2
Webpage Certificate

Results: This page contains an HTTPS connection, which provides important security to it.

Certificates

SSL Certificates are small data files that digitally bind a cryptographic key to an organization's details. When installed on a web server, it activates the padlock and the https protocol and allows secure connections from a web server to a browser. Typically, SSL is used to secure credit card transactions, data transfer and logins, and more recently is becoming the norm when securing browsing of social media sites.

This kind of cryptography harnesses the power of two keys which are long strings of randomly generated numbers. One is called a private key and one is called a public key. A public key is known to your server and available in the public domain. It can be used to encrypt any message. This webpage uses an SHA-2 SSL Certificate, they used this type of certificate due to concerns that the algorithm is no longer secure. SHA-2 will likely remain in use for at least five years. However, some unexpected attack against the algorithm could be discovered which would prompt an earlier transition. Primarily, people focus on the bit-length as the important distinction. SHA-1 is a 160-bit hash. SHA-2 is actually a "family" of hashes and comes in a variety of lengths, the most popular being 256-bit.

Results: Hacienda Webpage contains an SHA256RSA certificate, a good certificate on actual time.

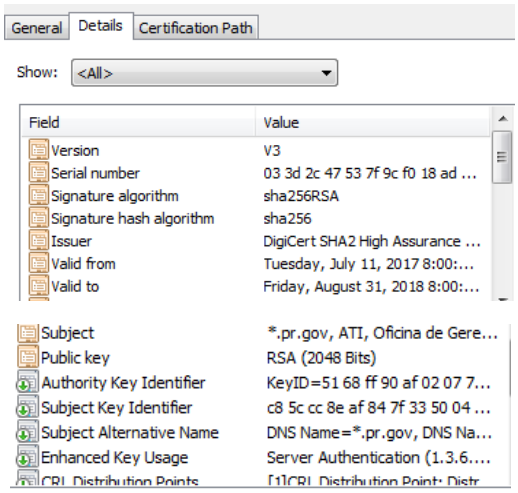

Figure 3
DigiCert Details

Webpages Vulnerabilities

A vulnerability [3] is a weakness that allows an attacker to reduce the system's information assurance. Within the vulnerability on the systems the attacker is available to produce a systems susceptibility or flaw, access to the flaw or exploit a vulnerability. Within the pages of government, I consider the need to check how vulnerable could be doing simplex things such as checking ports, the verification code on the website. Due to the need to verify if the government pages were secure, a small investigation was carried out to verify the vulnerabilities of the system. Many vulnerabilities can be considered when investigating of this type. There is a list of the common vulnerabilities on webpages:

1. **SQL Injections** - is a type of web application security vulnerability in which an attacker attempts to use application code to access or corrupt database content.
2. **Cross Site Scripting (XSS)** - targets an application's users by injecting code, usually a client-side script such as JavaScript, into a web application's output.
3. **Broken Authentication & Session Management** - encompass several security issues, all of them having to do with maintaining the identity of a user.
4. **Insecure Direct Object References** - Insecure direct object reference is when a web application exposes a reference to an internal implementation object. Internal implementation objects include files, database records, directories, and database keys.
5. **Security Misconfiguration** - Security misconfiguration encompasses several types of vulnerabilities all centered on a lack of maintenance or a lack of attention to the web application configuration.

To verify these elements within the government's website, a series of tests were used through web pages that are dedicated to investigating the elements of vulnerability. Below you can see a series of tests that were carried out using online tools to check vulnerabilities on the website.

Investigation: Using SUCURI [5] one of the most popular free website malware and security scanner. You can do a quick test for Malware, Website blacklisting, Injected SPAM and Defacements. SUCURI clean and protect your website from online threats and works on any website platforms including WordPress, Joomla, Magento, Drupal, phpBB, etc, and Scanurl's online scanner. The tool itself will provide you with few details on your site's security, including:

a. Whether anyone has marked your site as "unsafe"
b. Whether it passed the Google Safe Browsing test
c. Whether Phish Tank has a file on your site
d. Whether Web of Trust has any negative ratings on your site It shows the followings results:

Figure 4
Sucuri Results

Results: This program found that the firewall should be reviewed within the website. A firewall is a software program or piece of hardware that helps screen out hackers, viruses, and worms that try to reach your computer over the Internet.

Recommendation: Try to update or modify firewall configuration.

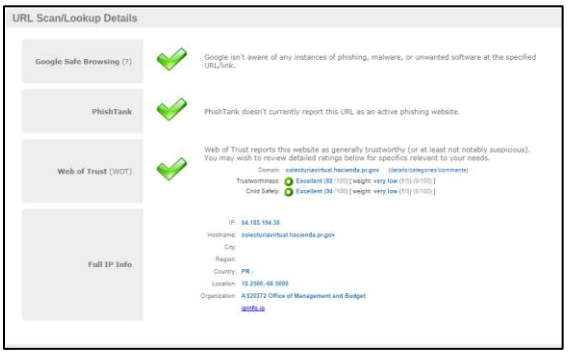

Figure 5
Scanurl's Results

Results: The results show that the page's security and vulnerabilities are not enough to show an imminent security risk. These results help me establish how secure the website is and what recommendations can be made to improve security on the government's website or another important one. In conclusion, it was shown that the hacienda internet page does not have an active virus which can be exploited, however it was shown that it has a problem with the firewall

Recommendation: Verify the firewall configuration on the website.

Ports Security

Port Security [6] is the first line of security on the systems. As a security good practice, ports should be open only on a need-to-be basis. You are exposing the services that are listening on those ports you left open to exploits. Why? Because a service means something is processing data and thus you are also exposing the vulnerabilities of the applications using those ports.

For example, if you let your FTP port open to everyone without any restriction rules (firewall) then a hacker could load lot of porn videos to consume lot of space of your server which thing will lead for example to very slow connection to your FTP service. Also, lot of ports open expose you more to Trojan Ports.

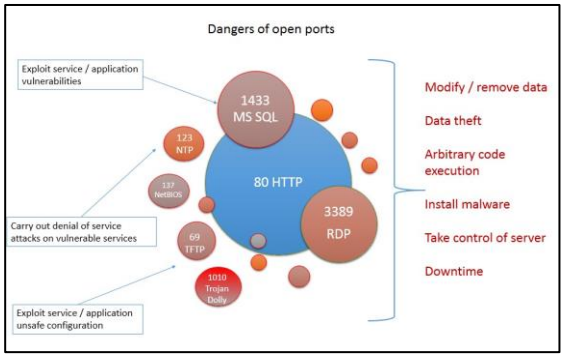

Figure 6
Dangers of Open Ports

Investigation: In this part of the investigation, a test was conducted to verify if the ports of the website were safe. This type of research helps us that web pages are not victims of hacker attacks. A study was made of 10 common ports within the website

1. Port 80- in Internet — TCP port 80, most often used by Hypertext Transfer Protocol

Vulnerabilities Exploit on this Port

- SQL Injection. SQL injection attacks attempt to use application code to access or corrupt database content.
- Cross-Site Scripting (XSS).
- Session Fixation.
- Information Leakage.

Figure 7
Port 80 Results

2. Port 21 - File Transfer Protocol (FTP) is one of the oldest Internet protocols. FTP servers open their machine's port 21 and listen for incoming client connections. FTP clients connect to port 21 of remote FTP servers to initiate file transfer operations. Since there's much more to FTP

protocol than this, see the discussion below for the details.

Vulnerabilities Exploit on this Port

- FTP proxy server for Novell BorderManager 3.6 SP 1a allows remote attackers to cause a denial of service (network connectivity loss) via a connection to port 21 with a large amount of random data.

Figure 8
Port 21 Results

3. Port 22 - Secure Shell - most common use is command line access, secure replacement of Telnet. Could also be used as an encrypted tunnel for secure communication of virtually any service [RFC 4251], [RFC 4960]

Vulnerabilities Exploit on this Port

- freeSSHd 1.2 and earlier allows remote attackers to cause a denial of service (crash) via a SSH2_MSG_NEWKEYS packet to TCP port 22, which triggers a NULL pointer dereference. References: [CVE-2008-0852] [BID-27845] [SECUNIA-29002]

Figure 9
Port 22 Results

4. Port 1433 MSSQL - Microsoft's SQL Server, including the desktop editions that are often silently installed with other Microsoft applications, opens and services queries delivered over incoming TCP connections through this port. The port used by the Database Engine is listed in the SQL Server error log. Instances of SQL Server Express, SQL Server Compact, and named instances of the Database Engine use dynamic ports.

Vulnerabilities Exploit on this Port

- Buffer overflow in the authentication function for Microsoft SQL Server 2000 and Microsoft Desktop Engine (MSDE) 2000 allows remote attackers to execute arbitrary code via a long request to TCP port 1433, a.k.a. the "Hello" overflow [7].
- **References:** [CVE-2002-1123], [BID-5411]

Figure 10
Port 1433 Results

5. Port 53 DNS - DNS (Domain Name Service) is used for domain name resolution.

Vulnerabilities Exploit on this Port

- There are some attacks that target vulnerabilities within DNS servers. Some trojans also use this port: ADM worm, li0n, MscanWorm, MuSka52, Trojan.Esteem.C (05.12.2005), W32.Spybot.ABDO (12.12.2005).
- W32.Dasher.B (12.16.2005) - a worm that exploits the MS Distributed Transaction Coordinator Remote exploit (MS Security Bulletin [MS05-051]).

Figure 11
Port 53 Results

6. Port 443 SSL - This port is used for secure web browser communication. Data transferred across such connections are highly resistant to eavesdropping and interception. Moreover, the

identity of the remotely connected server can be verified with significant confidence.

Vulnerabilities Exploit on this Port

- Trojans that use this port: W32.Kelvir.M (04.05.2005) - worm that spreads through MSN Messanger and drops a variant of the W32.Spybot.Worm. Connects to IRC servers on the s.defonic2.net and s.majesticwin.com domains, and listens for commands on port 443/tcp.
- Directory traversal vulnerability in Cisco Network Admission Control (NAC) Manager 4.8.x allows remote attackers to read arbitrary files via crafted traffic to TCP port 443, aka Bug ID CSCtq10755.
- **References:** [CVE-2011-3305] [BID-49954]

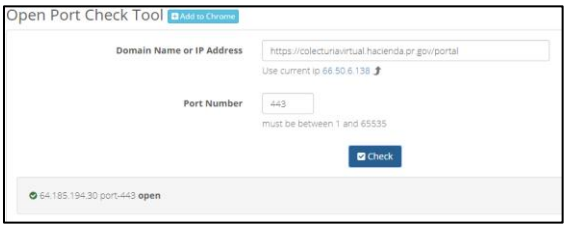

Figure 12
Port 443 Results

7. Port 23 Telnet - Telnet is one of the oldest Internet protocols and the most popular program for remote access to Unix machines. It has numerous security vulnerabilities [RFC 854].

Vulnerabilities Exploit on this Port

- Trojans that also use this port: ADM worm, Aphex's Remote Packet Sniffer , AutoSpY, ButtMan, Fire HacKer, My Very Own trojan, Pest, RTB 666, Tiny Telnet Server - TTS, Truva Atl, Backdoor.Delf variants, Backdoor.Dagonit (109.26.2005)
- Stack-based buffer overflow in RabidHamster R2/Extreme 1.65 and earlier allows remote authenticated users to execute arbitrary code via a long string to TCP port 23.
- **References:** [CVE-2012-1222] [BID-52061]

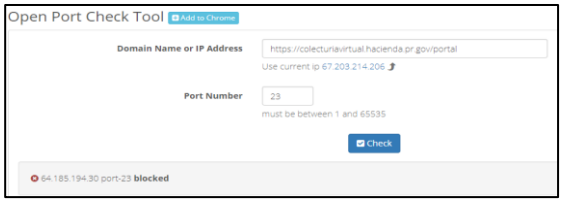

Figure 13
Port 23 Results

8. Port 139 NetBIOS - NetBIOS is a protocol used for File and Print Sharing under all current versions of Windows. While this in itself is not a problem, the way that the protocol is implemented can be. There are a number of vulnerabilities associated with leaving this port open.

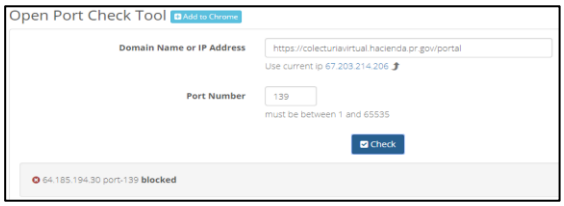

Figure 14
Port 139 Results

9. Port 110 POP3 - is used by eMail clients for the retrieval of their eMail from designated eMail "post office" servers. Email Clients such as Microsoft Outlook, Netscape, Eudora, and many others, connect to port 110 of a remote eMail server, then use the pop3 protocol to retrieve their eMail.

Vulnerabilities Exploit on this Port

- Security Concerns: Re-usable cleartext password, no auditing of connections & attempts thus subject to grinding. Some POP3 server versions have had buffer overflow problems. CERT Advisories: CA-97.09
- ADM, ProMail trojans also use port 110 (TCP).

Figure 15
Port 110 Results

10. Port 5900 VNC - This port (and port 5800) are opened by the VNC system allowing remote multi-platform console access.

Vulnerabilities Exploit on this Port

- VNC (Virtual Network Computing) - remote control program, http://www.realvnc.com/. It also uses ports 5800+ and 5900+ for additional machines.
- Backdoor.Evivinc also uses this port.
- Some Apple applications use this port as well: Apple Remote Desktop 2.0 or later (Observe/Control feature), Screen Sharing (Mac OS X 10.5 or later)
- RealVNC 4.0 and earlier allows remote attackers to cause a denial of service (crash) via a large number of connections to port 5900.
- **References:** [CVE-2004-1750], [BID-11048]

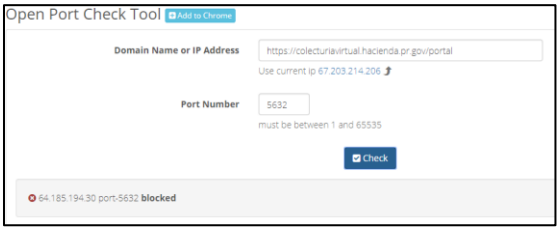

Figure 16
Port 5632 Results

RESULTS

Within the results of this investigation it was possible to verify that at least this government website is 80% safe. Within the investigation, an analysis of vulnerabilities, ports and important security elements was carried out to ensure the availability of the webpage. It is important to mention that due to the short time it was not possible to carry out other important tests with other government websites.

Vulnerabilities Exploit on this Port

- The following trojans/backdoors also use these ports: Chode, God Message worm, Msinit, Netlog, Network, Qaz W32.HLLW.Moega
- W32.Reidana.A (03.27.2005) - worm that spreads using the MS DCOM RPC vulnerability (MS Security Bulletin [MS03-026]) on port 139. The worm attempts to download and execute a remote file via FTP. Opens TCP port 4444.
- W32.Klez worm - a class of worms that collects email addresses from an infected computer's Windows address book and propagates using its own SMTP server.

Table 1
Results of Open/ Closed Ports

Port	Use	Results
80	TCP	Open
21	FTP	Blocked
22	Secure Shell	Blocked
1433	Microsoft's SQL Server	Blocked
53	DNS	Blocked
443	SSL	Open
23	Telnet	Blocked
239	NetBIOS	Blocked
110	POP3	Blocked
5900	VNC	Blocked

FUTURE WORK

It is important to mention that all government pages must be secured to avoid attacks. For this reason, an investigation of all the pages of the government should be done to be sure of its security capacity. It is important to mention that many of these pages do not have recent updates so they are more vulnerable. Therefore, after this research it is recommended to choose around 10 pages of the government and carry out a complete analysis to verify if they have any vulnerability that causes some damage in them.

- Develop the investigation process.
- Allow users to give ratings and leave comments about the viruses that they found when visit these webpages.
- Put more security on it.

CONCLUSION

In this project, I could learn to perform a vulnerability test on a web page. Within the same can put into practice the knowledge I acquired in security classes in the IT area. There are many elements that I can learning within this research, such as port analysis, code analysis and other security elements. Also in this project, I could learn the crucial elements within the security of the web pages. Within it you can see the definition of vulnerability and why it is important to keep the systems safe from them. Finally, I could see the importance of security elements in web pages and how you can avoid having any vulnerability within the systems

REFERENCES

[1] R. N. Tellado Doménech. (2017). *El "hackeo" a Hacienda retrasa la radicación de planillas* [Online]. Available: https://www.elnuevodia.com/negocios/economia/nota/hackeoahaciendaretrasaradicaciondeplanillas-2301476.

[2] O. Borrero (2015, May 14). *Proliferan los ataques cibernéticos en Puerto Rico* [Online]. Available: https://www.elnuevodia.com/tecnologia/tecnologia/nota/proliferanlosataquesciberneticosenpuertorico-2047274.

[3] Developer Network. (2017). *Definition of a Security Vulnerability* [Online]. Available: https://msdn.microsoft.com/en-us/library/cc751383.aspx.

[4] Techopedia. (2017). *Web Application Security* [Online]. Available: https://www.techopedia.com/definition/24377/web-application-security.

[5] C. Kumar. (2017). *12 Online Free Tools to Scan Website Security Vulnerabilities & Malware* [Online]. Available: https://geekflare.com/online-scan-website-security-vulnerabilities/#3-Qualys-SSL-Labs-Qualys-FreeScan.

[6] Study-ccna.com. (2016). *Port security* [Online]. Available: http://study-ccna.com/port-security/.

[7] Speed Guide. (2017). *Ports Details* [Online]. Available: https://www.speedguide.net/port.php?.