COMP307 Assignment 2

Instructions

Work in teams of maximum two students. Research online and give the answers.

Marks

This assignment is marked out of 10.

Submission

Dropbox your submissions.

Name of the student with student number

1. ……
2. ……

Consequences of compromised security for Web apps Evaluating web server Vulnerability

Every time you connect to the Internet and the World Wide Web (WWW), you are advertising to the world where you are and which data you may hold. It is like opening a Pandora's Box, the risks, threats, and vulnerabilities from attackers Web sites, Web applications, and e-commerce sites are prime targets for attackers seeking mailing lists, credit card information, and other confidential data that can be sold or used for monetary attacks. Before you connect your network and Web applications to the Internet, you must have a proper security strategy for inbound and outbound traffic entering the LAN-to-WAN Domain.

Without properly secured Web servers, businesses face a number of risks, including:

- Unauthorized access to privacy data which can lead to potential lawsuits
- Compromise of customer privacy data which is a compliance law violation
- Compromise of credit card data and address-verification data leading to PCI DSS non-compliance and potential lawsuits
- Lawsuits from customer or business partners resulting from loss of confidential information which, in turn, can cause a loss of revenue and business credibility

It is critical to perform periodic vulnerability assessments and penetration tests for all Web Applications. Whenever you update your Web application, install software, or load an upgraded version of software onto the server, you should first test this on a development server and a test environment. A full vulnerability-assessment scan and penetration test should be performed. Whenever you upgrade a production Web server operating system or Web server application, you should perform a vulnerability assessment scan and maintain an intrusive penetration test compliance and ensure confidentiality, integrity, and availability (CIA) for the Web server and the Web application.

In this lab, you will learn the capabilities of the vulnerability assessment tools for Web application servers: the Live HTTP Headers add-on for the Firefox browser. You will research the threats, connecting your servers to the Internet and World Wide Web (WWW), and access the impact to the several real-world business situations.

Use Live HTTP Headers to Access a Web

1. **Press** the **Alt key** to display the Firefox browser's menu.

2. From the Firefox browser's menu, **click Tools** and **select Live HTTP headers** to turn on this option. Add screen shot.
3. **Minimize** the **Live HTTP headers dialog box.**
4. **Click** the **Reload current page icon** at the right of the address box in the Firefox toolbar to refresh the page.
5. **Maximize** the **Live HTTP headers dialog box.**
6. The dialog box will display the HTML code for the header of the active Web page. Add the screen shot.

Question 1. What does the Live HTTP Headers plug-in application do, and why is this a good tool for Web-server and Web-application security testing?

In this part of the lab, you will act as a Web Applications asked security specialist. Your supervisor has asked you to document your assessment of the vulnerabilities of several Web applications and the possibility of threats that go well beyond an attacker defacing the Web site. You know that an attack can also include extracting customer's privacy data or confidential information which is a major threat not only to the organization, but to the customer as well. In fact, seventy percent of all unauthorized access and loss of data comes from Internet-based attacks on Web sites and applications where users are on the Wide Web (WWW).

You will review several business scenarios and describe the legal and technical risks as a deliverable for this lab.

Question 2 In your Lab Report file, **describe** the business threat posed by each of the following situations and **explain** what its effect may be if a Web application is compromised.

- A publicly traded retailer with retail outlets and online shopping and shipping options
- A small, private law firm having a small website with forms for potential clients to complete; including name, address, contact number, and reason for scheduling an appointment
- A real estate Appraisal Company that provides online appraisals for a publicly traded financial institution's residential-loan applicants which sends all applicant information to the appraisal company electronically
- A Web hosting company that provides leased servers for Web sites of client's ranging from small firms to large online retailers
- A city government that allows people with parking tickets to pay the fines online using a credit card or online check
- A local residential-cleaning site that acts as a company business with a Web site brochure; no forms of any type are located on the Web site
- A software Development Company that develops and licenses online shopping Software to large corporations
- A locally owned private bank with a Web site that accepts loan applications online
- A local doctor's office that keeps all patient information at the office, doesn't share with electronically with any entities, and doesn't have a Web site or use any custom- developed software
- An online-only retailer that sells athletic equipment using shopping-cart software that has been developed in-house and uses PayPal whenever a customer makes a purchase