COMP307 – Assignment 2:

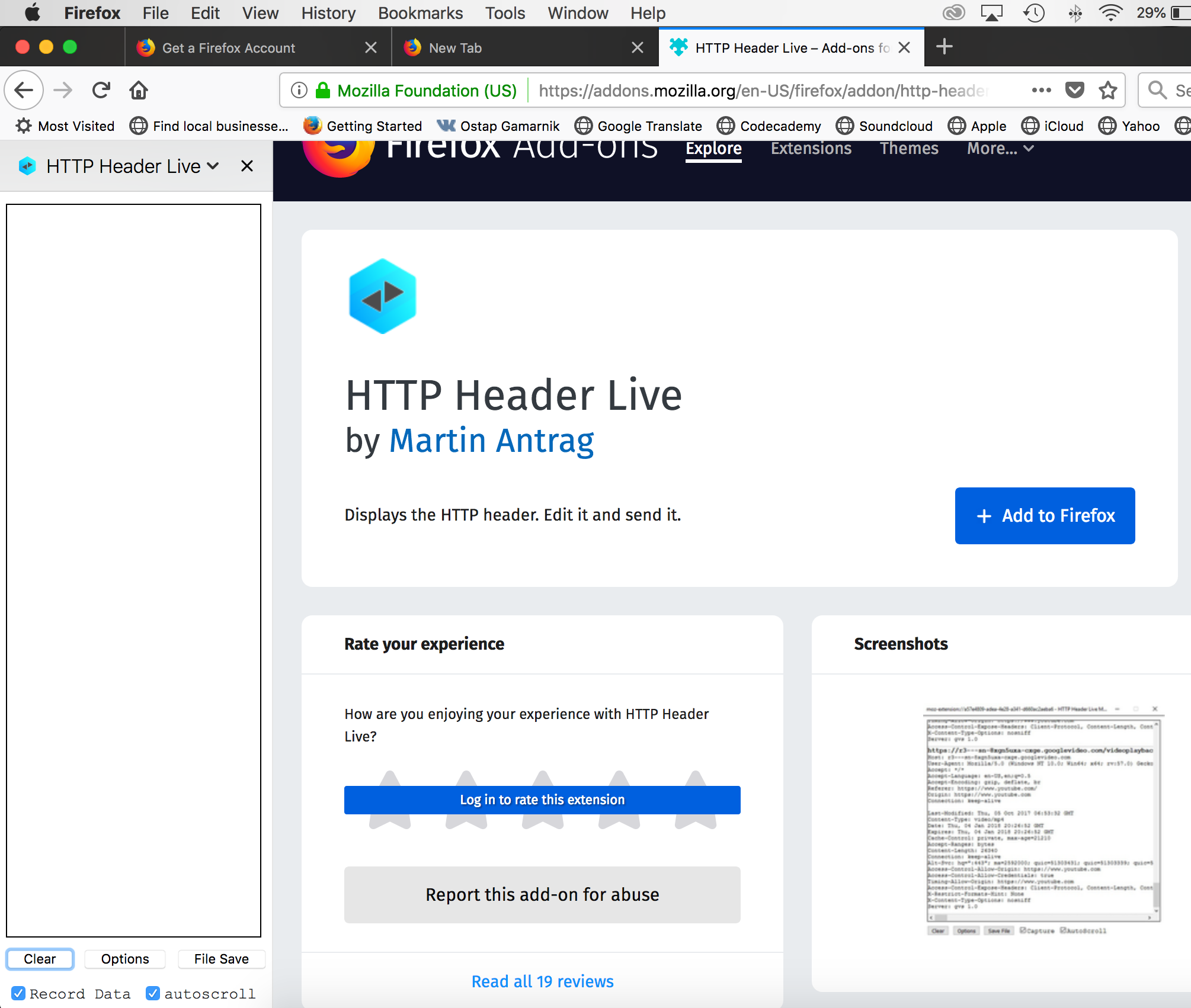
Consequences of compromised security for Web apps: Evaluating web server Vulnerability

September 12, 2018 Ostap Hamarnyk (#300836326)

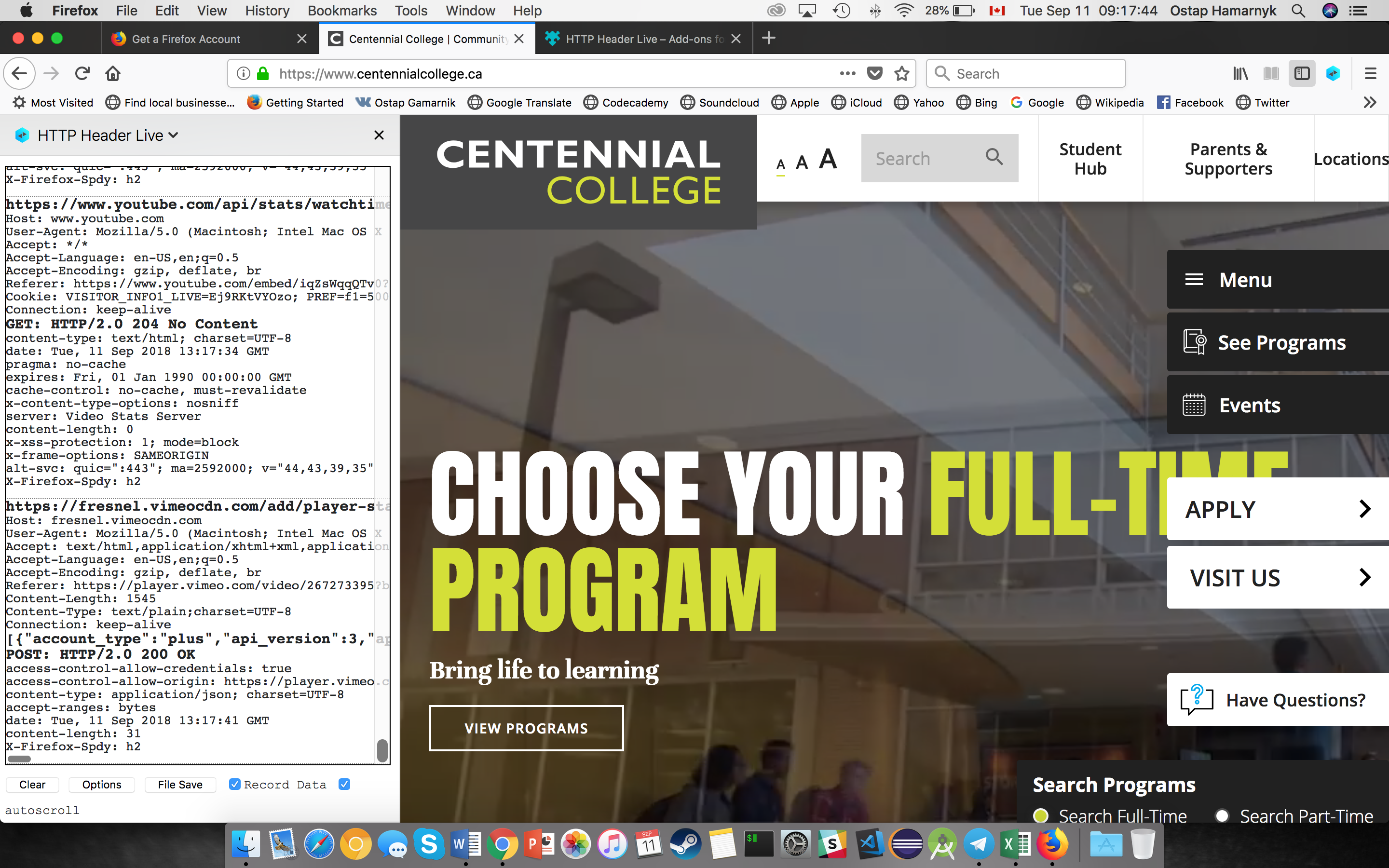
Kevin Ma (#300867968)

# Use “Live HTTP Headers” Firefox Add-On to Access the Web

1. Download and Add the “HTTP Header Live” Add-On to Firefox



1. Reload the page and check HTTP headers using the Live HTTP Headers dialog box



# 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?*

The Live HTTP Headers plug-in application provides vulnerability scanning capabilities. It shows the user the HTTP header response and can help identify any unintended information that is being sent over the web. This can help the developer to use it to integrate security parameters related to HTTP response headers that balance usability and security. It is critical to an application’s security that unintended information is not sent over the internet. This is because the data can be intercepted by “main in the middle” attacks, especially if the data is not encrypted. By verifying the info in the header parameters, you can avoid dangerous connections that use HTTP or lower version of TLS (not HTTPS), protect applications from clickjacking attacks by setting *X-Frame-Options* parameter to *Deny,* prevent XSS attacks, and create a defense in depth from injection attacks.

# Question 2

*Describe the business threat (what may be compromised) posed by each of the following situations and explain what its effect may be if a Web application is compromised.*

|  |  |  |  |
| --- | --- | --- | --- |
| # | Situation | What can be Compromised | Effects |
| 1 | A publicly traded retailer with retail outlets and online shopping and shipping options | * Name * Home address * Credit card information * Email address * Phone Number | If this data were to be compromised, customers would lose trust in the reliability of the company and they would need to compensate the customers (unless otherwise stated in their agreements). This would decrease the customer base of the business and result in a negative image that would be hard to build back up. In the worst-case scenario, the business would collapse and must close. The customer’s information can be abused and misused online for malicious purposes. |
| 2 | 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 | * Name * Address * Contact number * Personal issues which clients would not want to be disclosed to the world | If this data were to be compromised, customers would lose trust in the reliability of the company. Depending on the severity and privacy of the reason for scheduling the legal appointment, the clients may sue the law firm. This could potentially cause the law firm to lose credibility and deter clients from returning/visiting. The customer’s information can be abused and misused online for malicious purposes. |
| 3 | 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 | * Name * Address * Contact number * Email * Credit history * Income * Banking information | If this data were to be compromised, both the financial institution and appraisal company would lose credibility. This would cause customers to not return and deter future customers from coming as well. The customer’s information can be abused, sold and misused online for malicious purposes. |
| 4 | A Web hosting company that provides leased servers for Web sites of client’s ranging from small firms to large online retailers | * Name * Server configuration information * Data stored in the server | If this data were to be compromised, hackers can steal all the sensitive information from the organization leasing servers from the Web Hosting company. This information can be used for malicious purposes and cause the collapse of the organization. Additionally, the web hosting company would lose credibility and customers. |
| 5 | A city government that allows people with parking tickets to pay the fines online using a credit card or online check | * Name * Parking data * Location * Travel habits * Credit card information * Bank information | If this information were to be compromised, hackers can use this for malicious purposes such as selling the information online and abusing financial information. The city government would also be blamed by the public and lose credibility and reputation. Depending on the severity of the incidents, the government may need to compensate the clients as well. |
| 6 | 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 | * End user internet activity * Location | This situation is safer than the others as it presents a static website to the end user where the end user does not input any information via forms. However, there is still the risk of a “man in the middle” attack where a user with malicious intents can spoof the website and redirect traffic to his/her own website where there may be further threats which expose the vulnerabilities of the end user’s system. |
| 7 | A software Development Company that develops and licenses online shopping Software to large corporations | * Name * Address * Credit card information (of customer) * Financial information (of corporation) * Phone numbers * Emails | Manage application and coding security. Developers in the development company need to plan for security concerns at the time the applications are created. They should not wait until incidents occur before implementing security features.  However, if security was not properly implemented during development, users with malicious intent can exploit these vulnerabilities in the licensed software and steal sensitive information from the corporation and its shopping customers. As a result, the corporations would lose invaluable customers and their credibility/reputation. Additionally, there can be potentially legal repercussions between the corporations and the software development company as well. |
| 8 | A locally owned private bank with a Web site that accepts loan applications online | * Name * Phone number * Email * Credit history * Income information * Banking information | As with the other situations, any time a business exposes its operations online, the risk of information being compensated increases. Hackers would be given opportunities through various channels to seek out and exploit vulnerabilities in the Web site in order to steal sensitive information about the customers. As a result of this, the financial institution would lose credibility, lose its customers and potentially have to compensate its customers as well. |
| 9 | A local doctor’s office that keeps all patient information at the office, doesn’t share electronically with any entities, and doesn’t have a Web site or use any custom-developed software | * Patient information * Name * Age * Date of birth * Height * Weight * Bio metrics * Disease history * Medication history * Health card * Credit card information | Although the information is not directly shared electronically, there is still a risk for it to be stolen as long as it exists on the computer in the office. This is because as long as the computer is connected to the local network, any virus that successfully penetrates the security and enters the network can find its way to the computer storing the data. The virus would then be able to extract the data and export it back to the hacker’s hands. This can result in the information being sold online to various advertising companies or can even be as severe as identity theft. |
| 10 | 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 | * Name * Credit card information * Home address * Phone number * Email | Developing the software in-house eliminates one risk of having an external company exploiting known vulnerabilities to steal sensitive data. Using a well-known software such as PayPal to take care of financial transactions eliminates more risk of financial information being stolen. However, it is impossible to eliminate all risk, we can simply mitigate risk. There is still the chance that PayPal gets hacked and the retailer’s client’s financial information gets leaked, or retailer’s system being infected with a virus from external sources. This would result in sensitive information being stolen and customers taking legal action against the retailer and/or the retailer compensating its customers. |