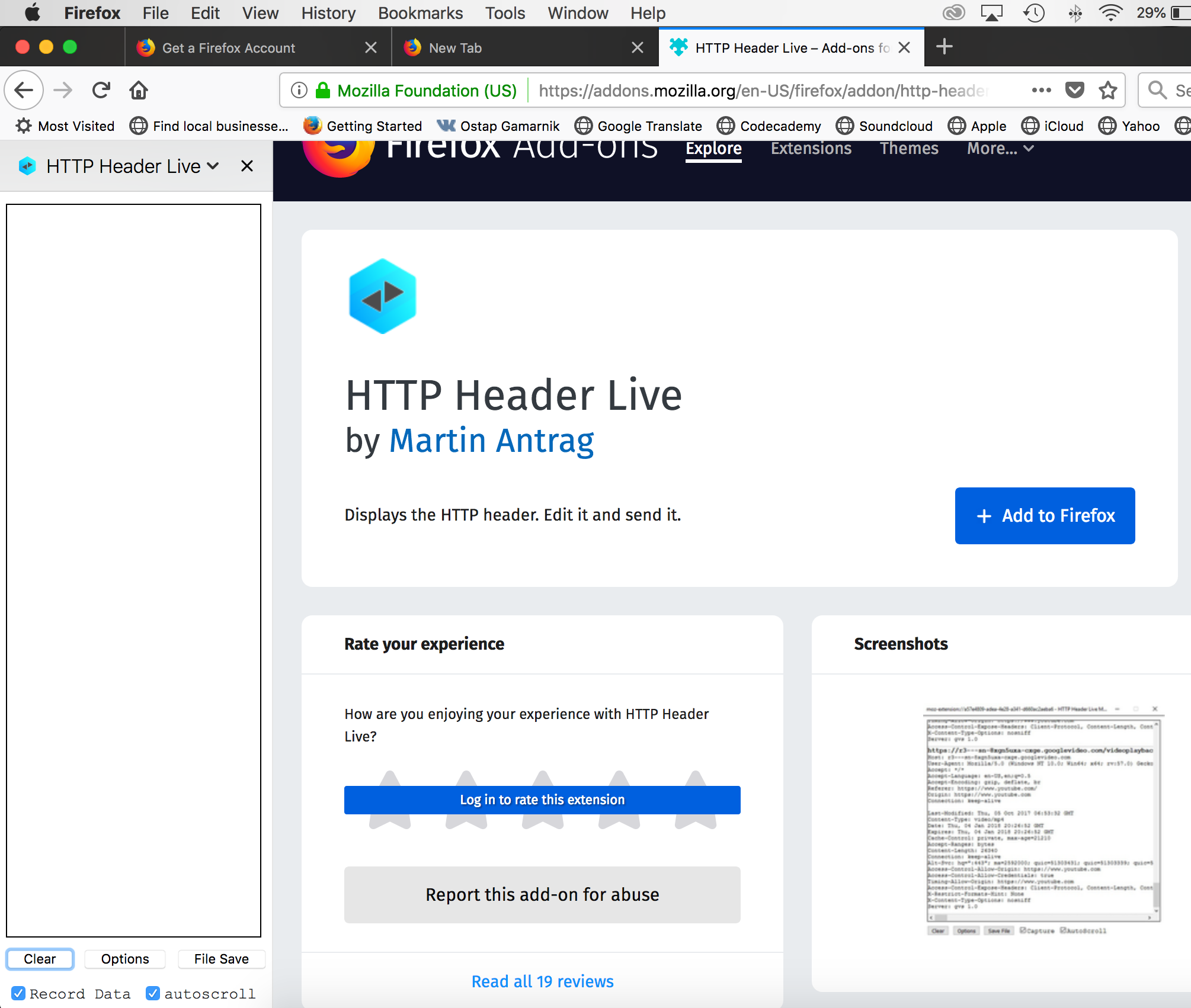
COMP307 – Assignment 2:

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

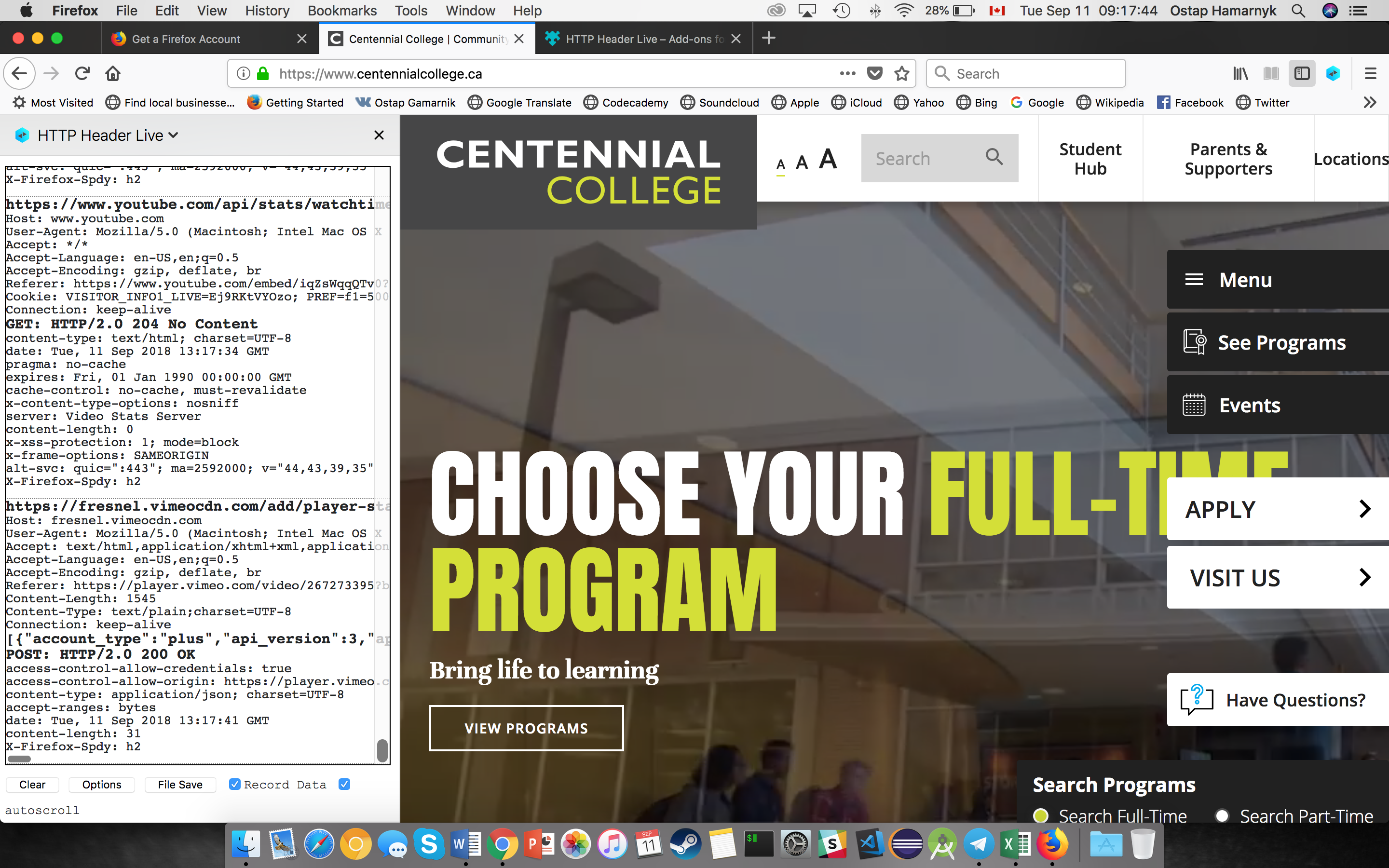
September 12, 2018 Ostap Hamarnyk (#300836326)

Kevin Ma (#300867968)

# Use Live HTTP Headers to Access a Web



# Reload the page and check HTML code in the header:



# 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 shows the HTTP header response in a separate window. Therefore, the developer can use it to set security parameters related to HTTP response headers that balance usability and security. 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.

Provides Vulnerability scan

Can show u if unintended information is being sent over the web

This data can be intercepted by man in the middle

Esp if not encrypted

Also sensitive data should not be sent via http header/request

# Question 2

make table

business effects

what can be compromised

* If the authentication is poorly done, the trade retailer might lose his outlets.
* If the form does not have a proper validation the site might be attacked by SQL injections or similar injection attacks, which can bring the website down or result in data loss