Running Head: SITE SECURITY

Week 4: E-Commerce Site Security

Jered McClure

Walden University

Week 4: E-Commerce Site Security

The site I chose to analyze was Amazon.com (Amazon.com, Inc., 2012). This site is one of the few e-commerce sites I frequent on a regular occasion. As such, it seemed like the perfect choice for penetration testing.

Amazon has implemented several layers of security (which I am thankful for) which include, but are not exclusive to: HTTPS, security certificates, data encryption, and TSL data transmission.

The security certificates are all certified by VeriSign: Class 3 secure server CA – G2. The encryption is at the 128 bit level, with a RSA public key of 1024 bits long. Finally, the TLS connection is secured from TLS renegotiation, which is when a client connects to a server “then splices in a new TLS connection” (Internet Engineering Task Force (IETF), 2010).

I tested SQL injection on the site by trying to pass a simple select statement in the URL. I did not believe this would work as it is the most basic of security guidelines to guard against, but felt it should be tried nonetheless. Needless to say, it did not work. Using a live script editor, I could edit the actual code of the rendered page on my client. This could lead to back attacks on the server if the JavaScript on the page actually sends data back to the system. However, I could not see any apparent code that did this.

Overall, there only seemed to be one improvement I would recommend. There are a lot of hidden div lines that contained no relevant code. It is possible these were left behind for development reasons. However, they could also contain hidden modules, which when opened using a live script editor, could unlock areas of the site unsecured from backwards code injections. I would remove these div lines, or simply place a block of html there such as “…” just as a filler to show that it is indeed design related.

Reference

Amazon.com, Inc. (2012). *Home.* Retrieved August 7, 2012, from Amazon: http://www.amazon.com/

Internet Engineering Task Force (IETF). (2010, February). *Transport Layer Security (TLS) Renegotiation Indication Extension.* Retrieved August 7, 2012, from Request for Comments: 5746: http://tools.ietf.org/html/rfc5746