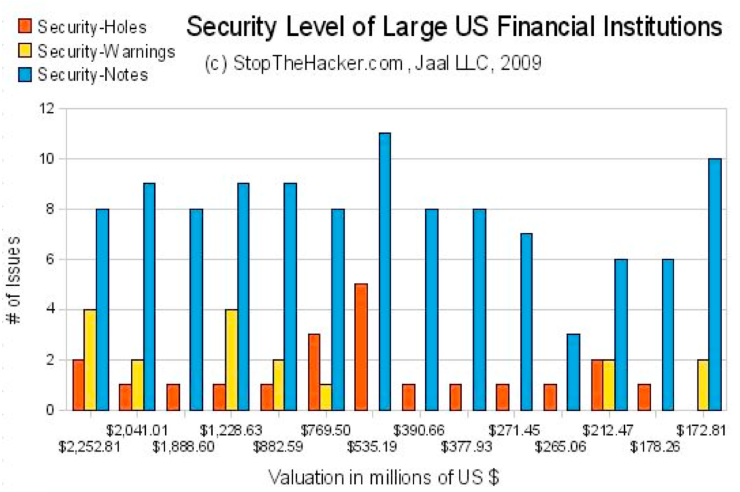
StopTheHacker

Website vulnerability study
13 out of 14 banks have at least one critical vulnerability

The StopTheHacker team conducted a study to understand how secure are the websites of large financial institutions in terms of vulnerabilities: how do these websites look to a potential hacker. The study was conducted in November 2009.



We evaluated 14 institutions among the top 50 financial institutions in the US according to [1]. These organizations handle trillions of transactions every few days. They are arguably the financial backbone of the country. By virtue of their role, one would expect that the security standards at these organizations would be exemplary. As a reference, the valuation of these financial institutions in total assets ranges from hundreds of millions to a few billion dollars in total assets.

The results are astonishing: 13 out of 14 websites had at least one critical vulnerability. In more detail, we highlight some key results below:

(1) There are 1.5 critical security holes in each financial institution on average.
(2) There are 1.2 security warnings in each financial institution on average.
(3) There are 7.9 security notes in each financial institution on average.
(4) The company valuation in total assets does not correlated to the highest security.
(5) The institution with the least valuation was the one with no critical security holes

[1] Top 50 financial institutions http://www.ffiec.gov/nicpubweb/nicweb/Top50form.aspx

The identified vulnerabilities are very serious: security holes are widely seen as critical security concerns by security experts, and security standards.

The most prevalent vulnerability among all of the ones discovered allows a hacker to spawn what is known as a shell, more commonly known as the command-prompt, and thereby remotely executing harmful commands on the web server. Other vulnerabilities range from major Cross Site Scripting (XSS) vulnerabilities, which can enable hacker to steal credentials of website visitors, to a plethora of concerns with various software installations used on these systems.