

Secure
Enterprise 2.0
Forum



WEB 2.0 HACKING INCIDENTS & TRENDS

2009 Q1

VULNERABILITIES, TARGETS AND ATTACK METHODS

MAY 2009

SUMMARY

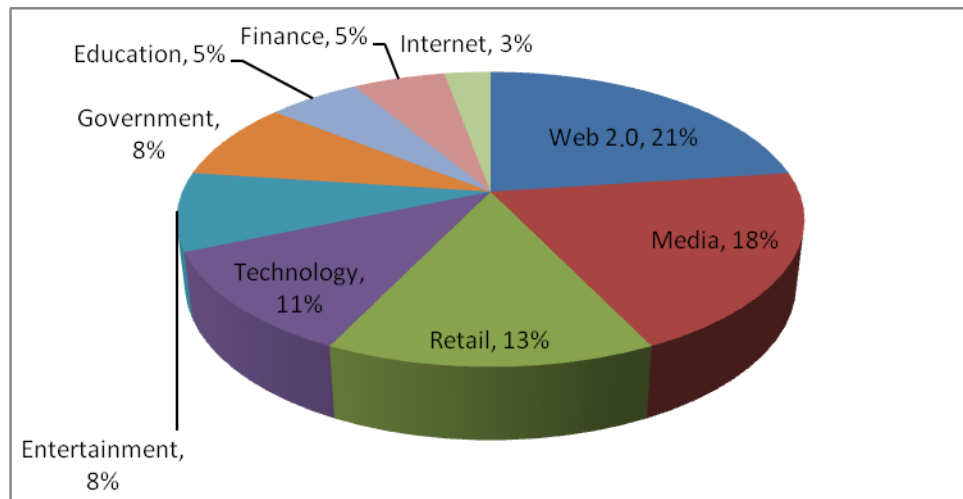
An analysis of recent web hacking incidents performed by the [Secure Enterprise 2.0 Forum](#) shows that Web 2.0 sites are becoming a premier target for hackers. Based on analysis of recent 'web hacking incidents of importance,' the Secure Enterprise 2.0 Forum found that:

- Q1 2009 showed a steep rise in attacks against Web 2.0 sites. This is the most prevalent attack with 21% of the incidents.
- Attack vectors exploiting Web 2.0 features such as user-contributed content were commonly employed in Q1: Authentication abuse was the 2nd most active attack vector, accounting for 18% of the attacks, and Cross Site Request Forgery (CSRF) rose to number 6 with 8% of the reported attacks.
- Leakage of sensitive information remains the most common outcome of web hacks (29%), while disinformation came in 2nd with 26%, mostly due to the hacking of celebrity online identities.

The study is based on incidents recorded in the 'Web Hacking Incidents Database' for Q1 2009. More information about the database can be found at www.xiom.com/whid.

WHICH ORGANIZATIONS ARE HACKED?

Analysis of Q1 incidents reveals a significant rise in the number of Web 2.0 sites hacked. Web 2.0 organizations such as social networks, wikis and community blogging sites (which were not classified as a separate site class until now) suffered most of the hacking incidents this quarter.

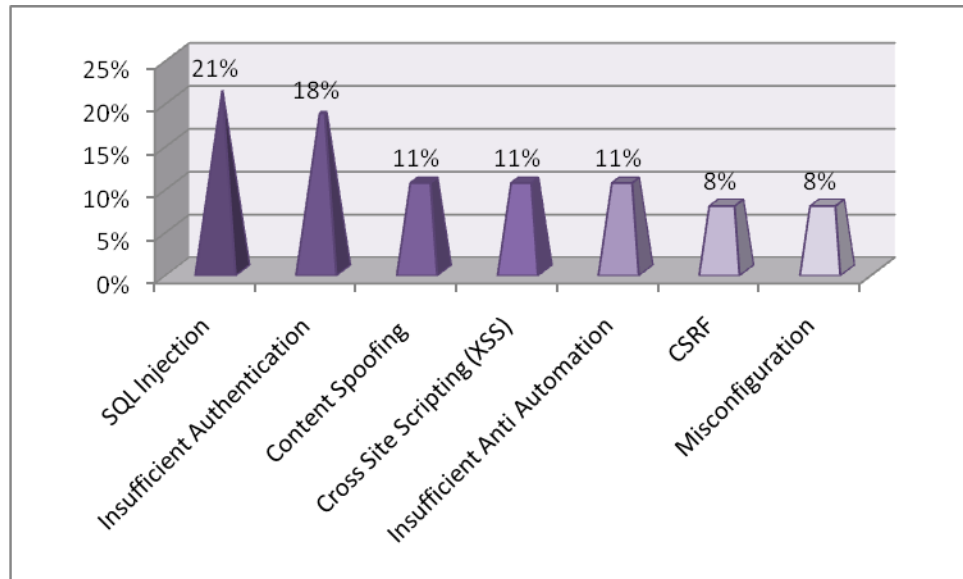


Naturally, such a steep rise raises questions, so the attacks were analyzed to find the underlying cause for the rise. When examining the data, it was found that a major reason for the steep rise was a series of high-profile attacks on Twitter, which is

rapidly becoming a popular social network/micropublishing site. Additionally, since Web 2.0 hacks spread virally, it is easier to detect these hacks.

Nevertheless, considering that the most media sites on the Internet are morphing into true Web 2.0 sites, the nearly 40% of Web 2.0 hacks are impressive. Furthermore, it was noted that some attacks against non-Web 2.0 sites, still exploited Web 2.0 technologies. For example, a recent hack against Amazon.com, exploited its community rating engine to delist books.

WHICH VULNERABILITIES WERE EXPLOITED?

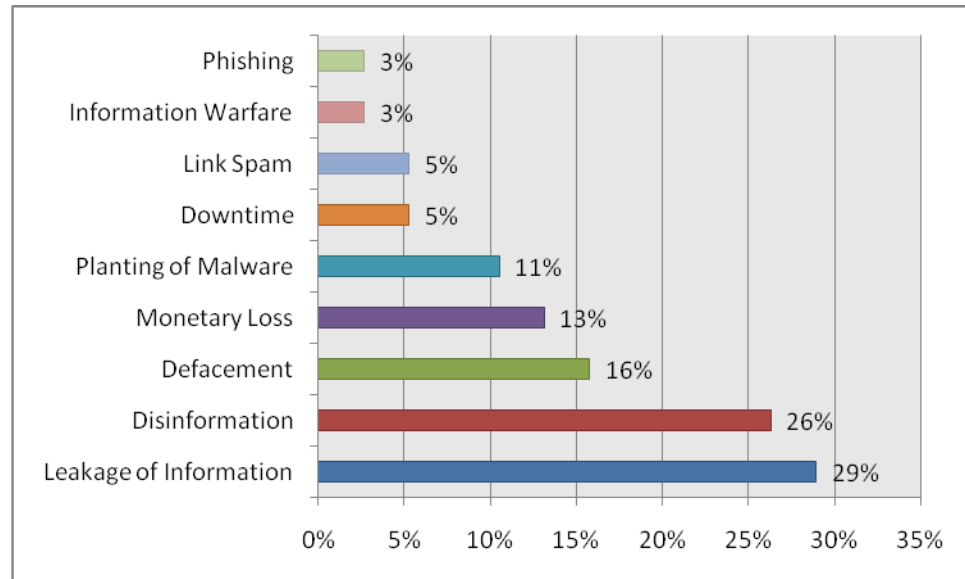


SQL Injection remains the top vulnerability exploited by hackers, only slightly losing ground since previous quarters. The other attack vectors that topped the list are as follows:

- Insufficient authentication – while not a new attack vector, insufficient authentication attacks have become increasingly severe due to the proliferation of user-contributed and managed web sites. As such, it is not surprising to see more incidents this quarter.
- Automation is fast becoming a major security threat to web applications. Abuse examples range from brute force password attacks, to bypassing the wait queue in reservation systems, to opinion poll skewing.
- Cross-Site Request Forgery (CSRF) was recognized several years ago as a potentially potent attack vector. While it took longer than expected to appear, this year it has become a mainstream hacking tool. A rise in the exploit of CSRF vulnerabilities is in line with authentication abuse, since it essentially provides an alternative mechanism for performing actions on behalf of a victim.

WHAT IS THE OUTCOME?

Most major categories for attack outcomes maintained their standing in Q1 2009. However, after two years of virtually a tie for 1st place, it seems that information leakage has surpassed defacements for the top spot. Furthermore, a new entrant, “disinformation,” has jumped from the bottom of the list to the second spot.



NOTABLE INCIDENTS IN Q1 2009

The online identities of several high-profile celebrities were hacked, including the Twitter accounts of Barak Obama, Britney Spears and the rapper, Kanya West. Two incidents caused particular harm to the violated celebrity. In one, a hacker broke into Twitter, stole a celebrity’s password and used the same password to log on to the celebrity’s Gmail account. The hacker then found and published embarrassing pictures of teen star Miley Cyrus. In the other incident, a hacker broke into female rapper Lil Kim’s MySpace account and used the access to besmirch a colleague.

In at least two incidents, false rumors were spread about Apple CEO, Steve Jobs’ health, causing Apple’s stock to plummet. In one of the incidents, an abused user contributed images to Wired.com, while in the other, someone broke into a live Mac Rumors feed to announce Job’s death (see box below).

9:28 am	Places can show a map with all photos t
9:27 am	Steve did not die.
9:27 am	Retraction on Steve Jobs comment...we feed.
9:26 am	Showing a "pumpkin patch" event with r iPhoto assists using its database of loca
9:25 am	Hovering over a pin at Aspen. Click an a photos, even across multiple events.
9:24 am	STEVE JOBS JUST DIED :

Lastly, multiple vulnerabilities have hit Twitter, causing false tweets to be sent by hundreds of famous people, and user contact information to leak, thus potentially exposing Twitter users to malware. These incidents have made Twitter acutely aware of its responsibility to address the security needs of its customer base.

ABOUT THE SECURE ENTERPRISE 2.0 FORUM

The Secure Enterprise 2.0 Forum is comprised of top executives at Global Fortune 500 companies that are ready to address the security challenges posed by Web 2.0 technologies, such as wikis, blogs, RSS, widgets and gadgets, personalized homepages, social networks and social bookmarking, which are becoming increasingly popular in the enterprise. The Forum promotes awareness, industry standards, best practices, and interoperability issues related to the introduction of consumer technology into the workplace.

Spearheaded by WorkLight, a Web 2.0 for Business Company, the Forum seeks to promote the secure use of Web 2.0 to do business. For more information, visit www.secure-enterprise20.org.