

28 October 2008

By: Lucian Constantin, Web News Editor



Yahoo! HotJobs XSS vulnerability used in phishing attack  
Yahoo! Inc.

## [Phishing Attack Uses Yahoo HotJobs XSS Vulnerability](#)

*Attackers stole authentication cookies by injecting malicious code into the Yahoo! HotJobs website*

Netcraft, a British company that offers Internet and security services, [announced](#) that a phishing attack was compromising Yahoo accounts. According to the company, the attack was using obfuscated JavaScript code injected in the hotjobs.yahoo.com website in order to gather authentication cookies from users accessing the page. Yahoo was notified and fixed the problem.

The attackers used a cross-site scripting vulnerability in the Yahoo! HotJobs website in order to inject malicious obfuscated JavaScript code into the page. The JavaScript code was used to pass the authentication cookies sent by the browsers to another external website set up by the attackers in the US. Using the stolen cookies, the attackers hijacked the user sessions and gained access to all Yahoo services that required authentication.

An authentication cookie is a text file served by the web server to the user's browser after a successful login. The file allows the web server to keep the session opened for a period of time or until the user logs out. When trying to access a resource that requires authentication, the web server asks the browser for this cookie file. If the file exists and the browser is able to return it, the web server allows access to the resource.

According to Netcraft, enforcing HTTP-only cookies, which are supported by all modern browsers, would have mitigated this attack, since cookies tagged with this attribute cannot be accessed by server-side scripts. The company also points out that a highly similar attack using Yahoo compromised pages was detected earlier this year.

"In both cases, Netcraft found that the Yahoo cookies stolen by the attacker would have allowed him to hijack his victims' browser sessions, letting him gain access to all of their Yahoo Mail emails and any other account which uses cookies for the yahoo.com domain," is noted in their report.

The number of users affected by this phishing attack has not been disclosed, but a Yahoo spokeswoman announced that the issue was fixed within hours since it came to their attention on Sunday. As a precaution, she also advised all users who visited the compromised page to reset their account password.

Mike Perry, a security researcher and developer at Riverbed Technology, presented earlier this year at DEFCON a Gmail Account automatic hacking tool that uses the same principle of stealing authentication cookies. Later, he released a tool named [CookieMonster](#) which is able to automate man-in-the-middle attacks and steal such cookies for [many popular websites](#) like Bank of America, Register, NetFlix, NewEgg, eBay and others.