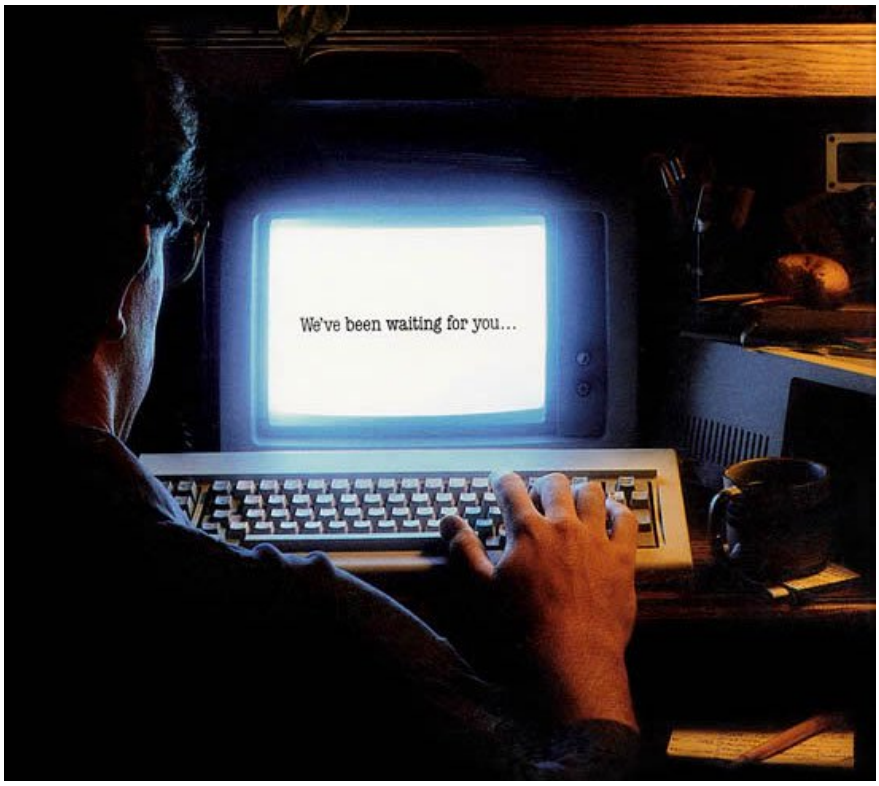
Top 10 attack techniques on the web

Security experts have listed the top 10 attacks on the web and forecast online banking transactions at the highest risk of hackers. The discovery of Duong Ngoc Thai, a Vietnamese security expert, ranks first.

Security experts have listed the top 10 attacks on the web and forecast online banking transactions at the highest risk of hackers. The discovery of Duong Ngoc Thai, a Vietnamese security expert, ranks first.



The Council of Security Experts ranked web attack techniques in 2010 and the experts also listed a list of the top 10 web attack techniques after the evaluation and acknowledgment process.

The ratings are sponsored by *Black Hat , OWASP , White Hat Security* and the content that simulates the attack methods will be presented at the 2011 IT-Defense conference next month in Germany.

Here are 10 ways to attack the web by security experts:

1. The 'padding oracle crypto' attack, an attacker (hacker) will exploit ASP.Net framework, hackers can take control of any website using ASP.NET and even More serious releases can take complete control of Windows servers containing these sites. (The discoverer: Duong Ngoc Thai and Juliano Rizzo).

2. Evercookie: can use Javascript to create cookies and hide cookies in 8 different places in the browser, making it difficult to clean them. Through Evercookie, hackers can break into computers even if cookies have been deleted. (Creator: Samy Kamkar).

3. Attack Autocomplete: this feature will automatically fill in the form (form) available on the website (autocomplet feature will automatically turn on), then the malicious website may "force" the browser to fill in the information. Personal information that data is taken from different sources is located on the victim computer. (Creator: Jeremiah Grossman).

4. Attack HTTPS with cache injection: 'inject' malicious code into Javascript library in browser cache, so hackers can 'break' the site even if it is protected by SSL, and cause the cache to be wiped clean. Nearly half of the top 1 million websites use Javascript extension libraries. (Creator: Elie Bursztein, Baptiste Gourdin and Dan Boneh).

5. Ignore CSRF protection with ClickJacking and HTTP Parameter Pollution: this attack will trick users into getting access to e-mail passwords. Attackers can recreate the victim's new password and directly access the victim's account. (Creator: Lavakumar Kuppan).

6. Universal XSS in IE8: The vulnerability in IE8 will help hackers 'release' malicious code into web pages and take control of the machine. (Creator: David Lindsay and Eduardo Vela).

7. HTTP POST DoS: this is a DDoS attack technique based on an POST method architecture vulnerability in HTTP that extends connection time to deplete server resources. Once too much data is sent to the destination machine, the server becomes overloaded. (Creator: Wong Onn Chee and Tom Brennan).

8. JavaSnoop: When the data is transferred to the destination machine, it is accompanied by the JavaSnoop tool to check whether the applications on the destination computer are secure. Hackers can 'hide' under this tool (Creator: Arshan Dabirsiagh).

9. Attack via CSS History in Firefox does not need JavaScript for PortScanning in the local network: this attack can deprive the browser's history data. The information in the history can help hackers attack in the form of a phishing site. (Creator: Robert "RSnake" Hansen).

10. Java Applet DNS Rebinding: Hackers can control Java applets, making the browser 'ignore' DNS cache, then users can 'trap'. Java applets are usually small programs that run inside Web browsers (Creator: Stefano Di Paola).