Figure 4 Hacked UNICEF Web page




anything he or she can think of to attempt to gain access to or disrupt the target system. While this is the most realistic and useful, some clients balk at this level of testing. Clients have several reasons for this, the most common of which is that the target systems are "in production" and interference with their operation could be damaging to the organization's interests. However, it should be pointed out to such clients that these very reasons are precisely why a "no-holds-barred" approach should be employed. An intruder will not be playing by the client's rules. If the systems are that important to the organization's well-being, they should be tested as thoroughly as possible. In either case, the client should be made fully aware of the risks inherent to ethical hacker evaluations. These risks include alarmed staff and unintentional system crashes, degraded network or system performance, denial of service, and log-file size explosions.

Regular auditing, vigilant intrusion detection, good system administration practice, and computer security awareness are all essential parts of an organization's security efforts. A single failure in any of these areas could very well expose an organization to cyber-vandalism, embarrassment, loss of revenue or mind share, or worse. Any new technology has its benefits and its risks. While ethical hackers can help clients better understand their security needs, it is up to the clients to keep their guards in place.


## Acknowledgments

The author would like to thank several people: the members of the Global Security Analysis Lab at IBM Research for sharing their amazing expertise and their ability to make just about anyone understand more about security; Chip Coy and Nick Simicich for their trailblazing work in defining IBM's Security Consulting Practice at the very beginning; and Paul Karger for his encyclopedic knowledge of computer security research and for his amazing ability to produce copies of every notable paper on the subject that was ever published.






## Cited references and notes


1. E. S. Raymond, *The New Hacker's Dictionary*, MIT Press, Cambridge, MA (1991).
2. S. Garfinkel, *Database Nation*, O'Reilly & Associates, Cambridge, MA (2000).
3. The first use of the term "ethical hackers" appears to have been in an interview with John Patrick of IBM by Gary Anthens that appeared in a June 1995 issue of *ComputerWorld*.
4. P. A. Karger and R. R. Schell, *Multics Security Evaluation: Vulnerability Analysis*, ESD-TR-74-193, Vol. II, Headquarters Electronic Systems Division, Hanscom Air Force Base, MA (June 1974).
5. S. M. Goheen and R. S. Fiske, *OS/360 Computer Security Penetration Exercise*, WP-4467, The MITRE Corporation, Bedford, MA (October 16, 1972).
6. R. P. Abbott, J. S. Chen, J. E. Donnelly, W. L. Konigsford, and S. T. Tokubo, *Security Analysis and Enhancements of Computer Operating Systems*, NBSIR 76-1041, National Bureau of Standards, Washington, DC (April 1976).
7. W. M. Inglis, *Security Problems in the WWMCCS GCOS System*, Joint Technical Support Activity Operating System Technical Bulletin 730S-12, Defense Communications Agency (August 2, 1973).
8. D. Farmer and W. Z. Venema, "Improving the Security of Your Site by Breaking into It," originally posted to Usenet (December 1993); it has since been updated and is now available at ftp://ftp.porcupine.org/pub/security/index.html#documents.
9. See http://www.faqs.org/usenet/.
10. Who can really determine who said something first on the Internet?
11. See http://www.cs.ruu.nl/cert-uu/satan.html.
12. This strategy is based on the ideal of raising the security of the whole Internet by giving security software away. Thus, no one will have any excuse not to take action to improve security.
13. S. Garfinkel and E. Spafford, *Practical Unix Security*, First Edition, O'Reilly & Associates, Cambridge, MA (1996).
14. For a collection of previously hacked Web sites, see http://www.2600.com/hacked_pages/ or http://defaced.alldes.de. Be forewarned, however, that some of the hacked pages may contain pornographic images.
15. In 1965, Intel cofounder Gordon Moore was preparing a speech and made a memorable observation. When he started to graph data about the growth in memory chip performance, he realized there was a striking trend. Each new chip contained roughly twice as much capacity as its predecessor, and each chip was released within 18–24 months of the previous chip. In subsequent years, the pace slowed down a bit, but data density has doubled approximately every 18 months, and this is the current definition of Moore's Law.
16. J. O. Kephart, G. B. Sorkin, D. M. Chess, and S. R. White, "Fighting Computer Viruses," *Scientific American* **277,** No. 5, 88–93 (November 1997).
17. See http://www.research.ibm.com/antivirus/SciPapers.htm for additional antivirus research papers.
18. A. Boulanger, "Catapults and Grappling Hooks: The Tools and Techniques of Information Warfare," *IBM Systems Journal* **37,** No. 1, 106–114 (1998).
19. R. R. Schell, P. J. Downey, and G. J. Popek, *Preliminary Notes on the Design of Secure Military Computer Systems*, MCI-73-1, ESD/AFSC, Hanscom Air Force Base, Bedford, MA (January 1973).



*Accepted for publication April 13, 2001.*



**Charles C. Palmer** *IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598 (electronic mail: ccpalmer@us.ibm.com).* Dr. Palmer manages the Network Security and Cryptography department at the IBM Thomas J. Watson Research Center. His teams work in the areas of cryptography research, Internet security technologies, Java™ security, privacy, and the Global Security Analysis Lab (GSAL), which he cofounded in 1995. As part of the GSAL, Dr. Palmer worked with IBM Global Services to start IBM's ethical hacking practice. He frequently speaks on the topics of computer and network security at conferences around the world. He was also an adjunct professor of computer science at Polytechnic University, Hawthorne, New York, from 1993 to 1997. He holds four patents and has several publications from his work at IBM and Polytechnic.