Instructor Manual (Sample Lab Reports)

SEED: A Suite of Instructional Laboratories for Computer Security Education

Wenliang (Kevin) Du
Department of Electrical Engineering and Computer Science
4-206 CST Building, Syracuse University, Syracuse, New York 13244
Email: wedu@syr.edu   Tel: 315-443-9180
URL: http://www.cis.syr.edu/~wedu/seed/

Table of Contents

1. Buffer Overflow Vulnerability Lab 1
2. Retrun-to-libc Attack Lab 13
3. Format String Vulnerability Lab 23
4. Race Condition Vulnerability Lab 43
5. Chroot Sandbox Vulnerability Lab 49
6. Set-UID Program Vulnerability Lab 71
7. Web Same-Origin-Policy Exploration Lab 81
8. Cross-Site Request Forgery Attack Lab 93
9. Cross-Site Scripting Attack Lab 105
10. SQL Injection Attack Lab 111
11. Clickjacking Attack Lab 117
12. TCP/IP Attack Lab 125
13. DNS Pharming Attack Lab 153
14. Packet Sniffing & Spoofing Lab 173
15. Linux Firewall Lab 181
16. Crypto Lab – Secret-Key Encryption 189
17. Crypto Lab – One-Way Hash Function 201
18. Linux Capability Exploration Lab 211

Please keep the reports to yourself.
Please never give them to students.

Sponsored by NSF CCLI Program (Phase-II)
For each lab, we picked the best student reports over the last few years, and put them together to produce this instructor manual. We would like to thank those students who have contributed to this manual.

This manual is meant to help instructors to prepare their labs. If falling to students’ hands, it will affect the intended education objectives of the labs that we have developed over the last eight years. I really appreciate that you keep this instructor manual to yourself. Please never post this manual online; please do not give to other people, especially students. If other people ask you for a copy, please ask them to send a request email to me (wedu@syr.edu).

Thanks.

Wenliang (Kevin) Du
September 15th, 2010