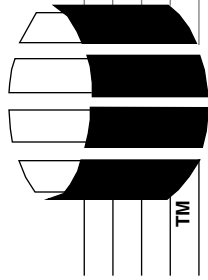


**STONEHENGE CONSULTING SERVICES** 4470 SW Hall Suite 107 Beaverton, OR 97005 (503) 777-0095

# Secure CGI Scripting

brian d foy, Randal L. Schwartz, and Tom Phoenix  
Version 1.2.3 (12/05/98) []



## Table of Contents

### **Introduction 2**

What this course is about 3

### **We're Not in Kansas Anymore 4**

Where's the threat? (it's them) 5

Where's the threat? (it's us!) 6

Large and complex systems 7

Who's on first? think about: 8

Oz wasn't built in a day 9

### **Lions 10**

A few points about cgi programs 11

Buggy software have known exploits 12

Lions don't hunt alone 13

Session IDs 14

Database access 15

Hide your hard-coded passwords 16

Common problems with "free scripts" 17

Poor configuration allows for exploitation 18

How stack smashing ruins your day 19

Robots wreaking havoc 20

Sniffing 21

Parsed pages can execute code 22

Multiple users on one computer 23

Accessing the filesystem 24

Restricting the filesystem 25

### **Tigers 26**

An introduction to setuid 27

More about setuid 28

Incorrectly set file permissions 29

Data files in the wrong place 30

Using old or buggy libraries 31

Changes to modules 32

File locking with flock 33

flock: an example 34

File locking with lock files 35

File locking with lock files (cont'd) 36

Overly verbose error output 37

Giving out sensitive information 38

Send mail to yourself 39

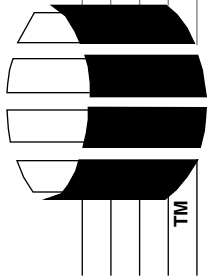
Sample error email 40

Responding to a bad request 41

Lack of data paranoia 42

Lack of data paranoia (cont'd) 43

Overly flexible environment 44



Using the shell 45  
Passing data to shell 46  
Programs can use the shell 47  
Avoiding the shell 48  
Use built-in functions where possible 49

**Bears 50**  
Security can be annoying 51  
Revision Control System (RCS) 52  
Taint checking 53  
Removing the taint from data 54  
Removing the taint from data (continued) 55  
Watch for odd characters in SQL data 56  
Things to think worry about 57  
Special users and groups 58  
Maintaining current version levels 59  
Monitoring changes 60  
Tracking errors from CGI programs 61  
Dealing with robots 62  
Password protecting scripts 63  
Encrypt data for transmission 64  
Mail is not a secure protocol 65  
Don't use /bin/mail or /bin/mailx to send mail 66  
Use a valid return address when sending mail 67  
Sending mail with Net::SMTP 68

**Oh My! 69**

Avoiding the Lions, Tigers, and Bears 70

**Ding Dong the Witch is...? 71**

References 72  
More references 73