Identity Theft, Phishing and Pharming: Accountability & Responsibilities

Danny Allan
Research Analyst, Watchfire
dannya@watchfire.com
781-547-7833

OWASP AppSec DC

October 2005

The OWASP Foundation
http://www.owasp.org/

NOTE !!

- Some demonstrated phishing techniques are shown in this presentation
- All brands used in the screenshots are fictitious and do not reflect true organizations

Discussion Topics

- Definitions and Statistics
- Malicious Techniques
  - Phishing
  - Pharming
  - Advanced
- Current Security Models
- Best Practices
  - Technical
  - Operational

The Demolished Man

Snim trudged downtown to Maiden Lane and cased the banks in that pleasant esplanade … Snim entered the bank, crossed the crowded main flood to the row of desks opposite the tellers' cages, and stole a handful of deposit slips and a pen.

Snim lurked outside the bank, watching the tellers' cages closely. A solid citizen was making a withdrawal at Cage Z. The teller was passing over big chunks of paper cash. This was the *fish*. Snim hastily removed his jacket, rolled up his sleeves, and tucked the pen in his ear.

As the *fish* came out of the bank, counting his money, Snim slipped behind him, darted up and tapped the man's shoulder.

"Excuse me, sir," he said briskly. "I'm from Cage Z. I'm afraid our teller made a mistake and short-counted you. Will you come back for the adjustment please?" Snim waved his sheaf of slips, gracefully swept the money from the *fish's* fins and turned to enter the bank. "Right this way, sir," he called pleasantly. "You have another hundred coming to you."

As the surprised solid citizen followed him, Snim darted busily across the floor, slipped into the crowd and headed for the side exit. He would be out and away before the *fish* realized he'd been gutted.

Alfred Bester, 1951

Definitions

- Identity Theft
  - The act of impersonating another, by means of using the person's information
- Phishing
  - A form of social engineering, characterized by attempts to fraudulently acquire sensitive information
- Pharming
  - The exploitation of a vulnerability in the DNS server software that allows a hacker to acquire the Domain Name for a site, and to redirect that website's traffic to another web site

APWG Statistics – July 2005

Phishing Reports Received	14,135
Hijacked Brands	71
Number of brands in top 80%	6
Phish targeted at Financial Services	86%
Country hosting most phishing sites	United States
Contain some form of target name	46%
No target name – just IP address	41%
Average time online for site	5.9 days
Longest time online for site	30 days

More Statistics

Estimated number of people who think they got phishing emails in the past year	57 million
Recipients who opened a phishing e-mail	19%
Recipients who divulge personal or financial information to phishers	3 – 5%
People who are duped into acting on a phishing e-mail that was identified as probably fraudulent	1 in 10
At EarthLink, which averages eight unique phishing attacks each month, the cost per attack	> $40,000
Number of calls in one hour to a top 20 US Bank after a phishing attack	> 90,000

Causes for Growth

- Average web user can be fooled
  - Websites & branding look official
  - Social engineering plays on fear
  - Advanced techniques difficult to detect
- Organizations are only beginning to address the issue
  - Web and email protections lacking
  - Communication is inconsistent
- Enforcement and Prosecution is difficult

Common Phishing Attack Methodology

From: admin@hackme.com
Subject: Security Alert

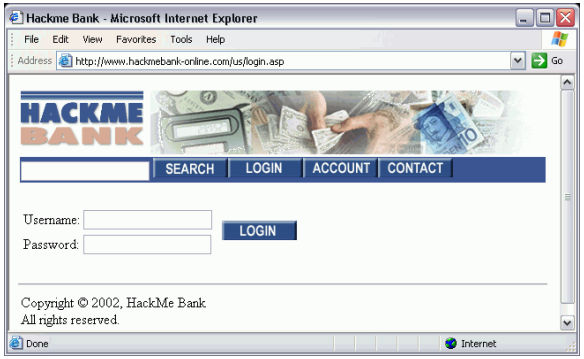
Dear HackMe Bank Client,

We are performing system maintenance, wich may interfere with access to your Online Services. Due to these technical updates your online account has been deactivated.

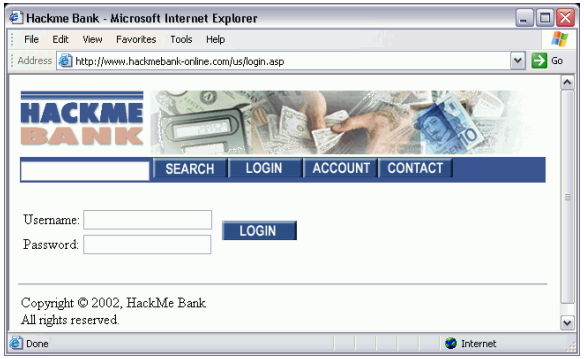
Click here to reactivate:

http://www.hackmebank.com/us/login.asp

Real Site



Fake Site



Attacker Data Collection

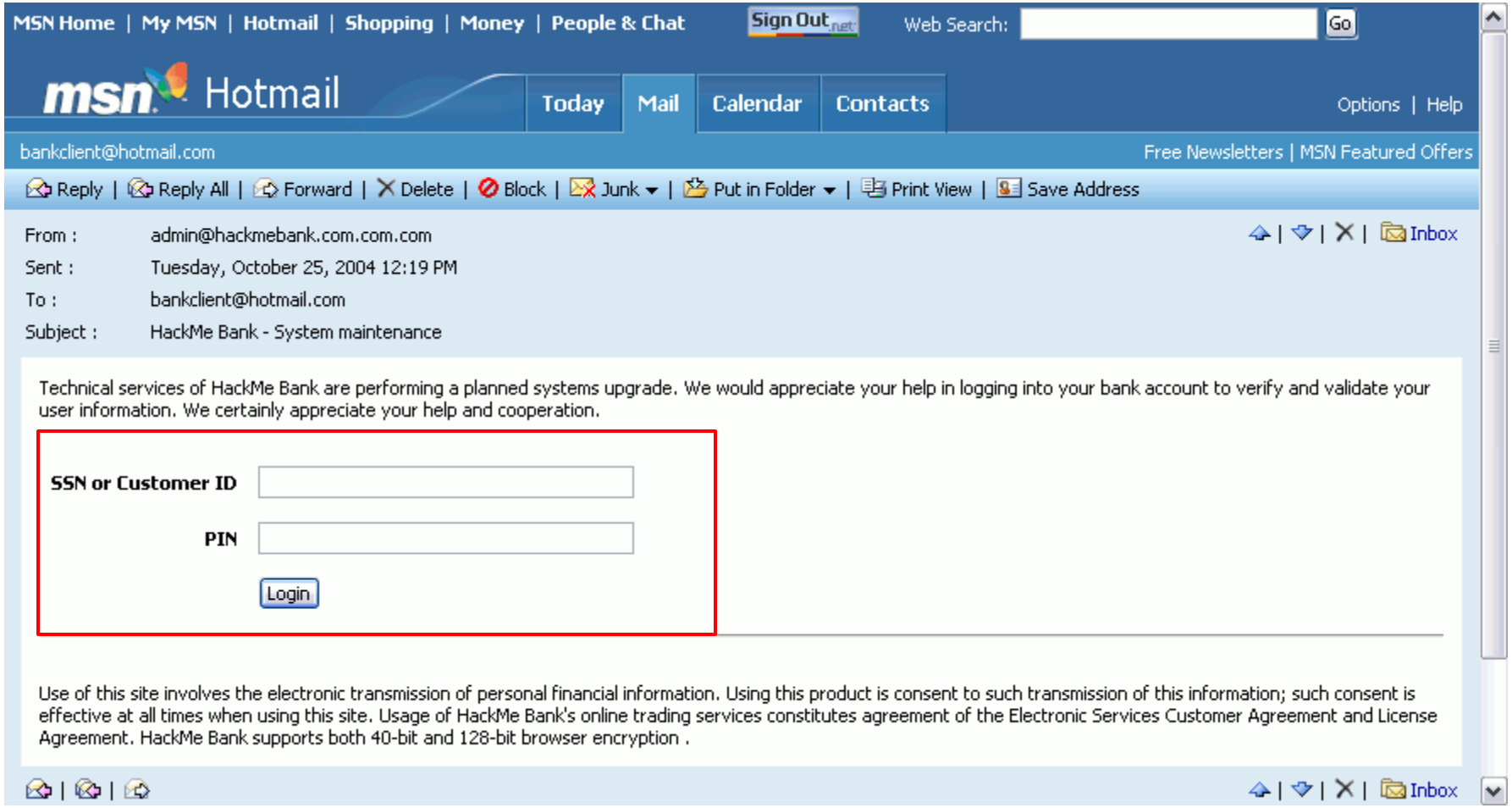
Name: John Doe
Address: 15 Broadway Ave
SSN: 123 45 6789
CC: 4388 1234 1234 1234
Username: jdoe
Password: password

Name: Jane Doe
Address: 15 7th Ave
SSN: 123 45 6798
CC: 4388 1234 1234 4321
Username: jane.doe
Password: password

Common Email Attack Techniques

- Look & Feel Replication
- Direct Data Collection
- Link Obfuscation
  - JavaScript Redirection
  - URL Encoding
  - Direct IP Address
- Hot linked image

Direct Data Collection



JavaScript Redirection

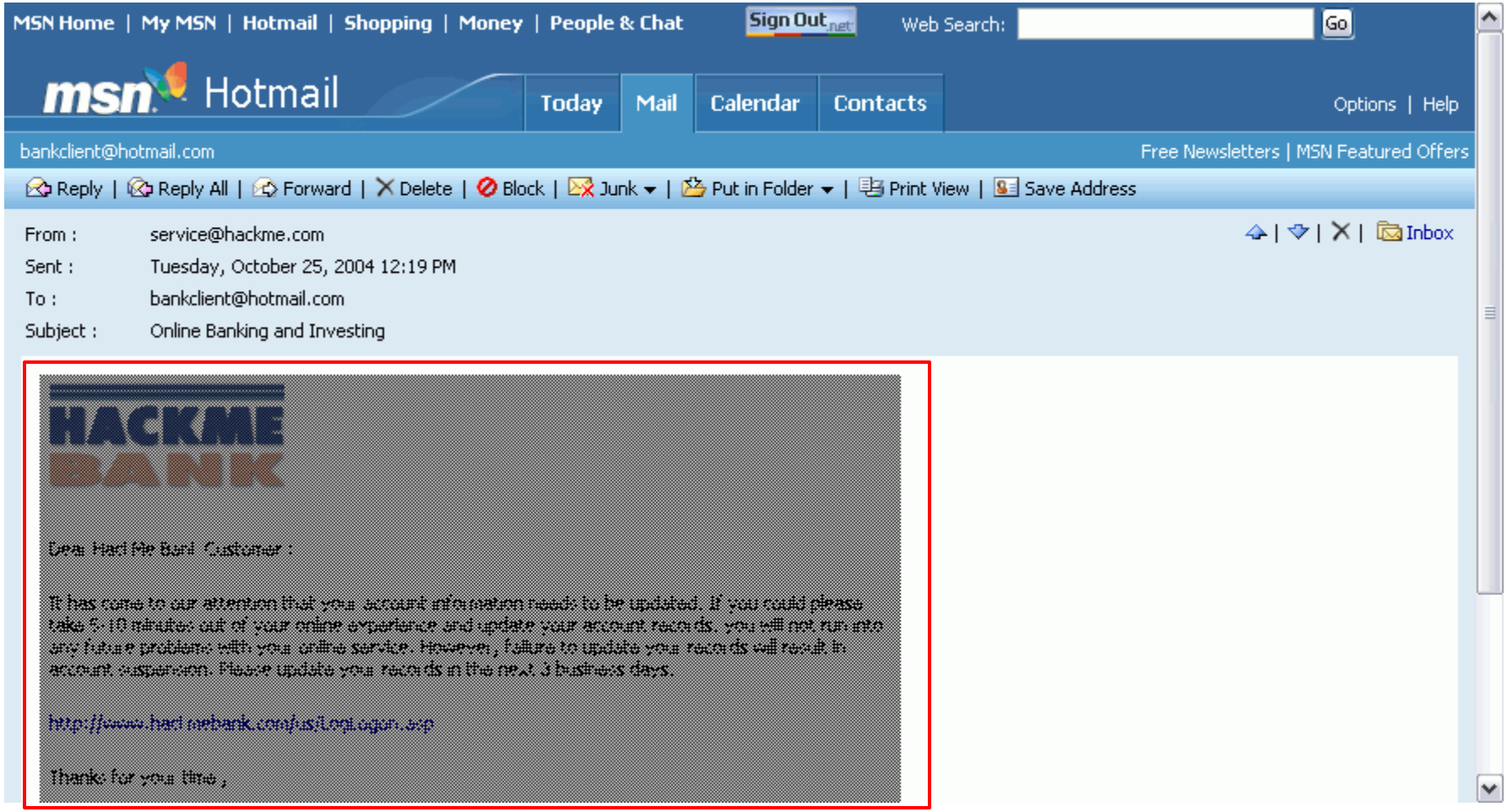
- <a href=http://www.legitsite.com
  onClick=validate>http://www.legitsite.com

- <script>
  function validate() {
  top.location.href =
  http://www.badsite.com;
  return false;
  }
  </script>

URL Encoding

- **Viewed in Source**
  - http://%31%39%35%2E%32%33%39%2E%37%39%2E%31%37%30:%38%37/%73%74/%69%6E%64%65%78%2E%68%74%6D
- **Resolved by Browser**
  - http://192.239.79.170:87/st/index.htm
- **Useful sites**
  - http://www.netdemon.net/decode.html

Hot Linked Image



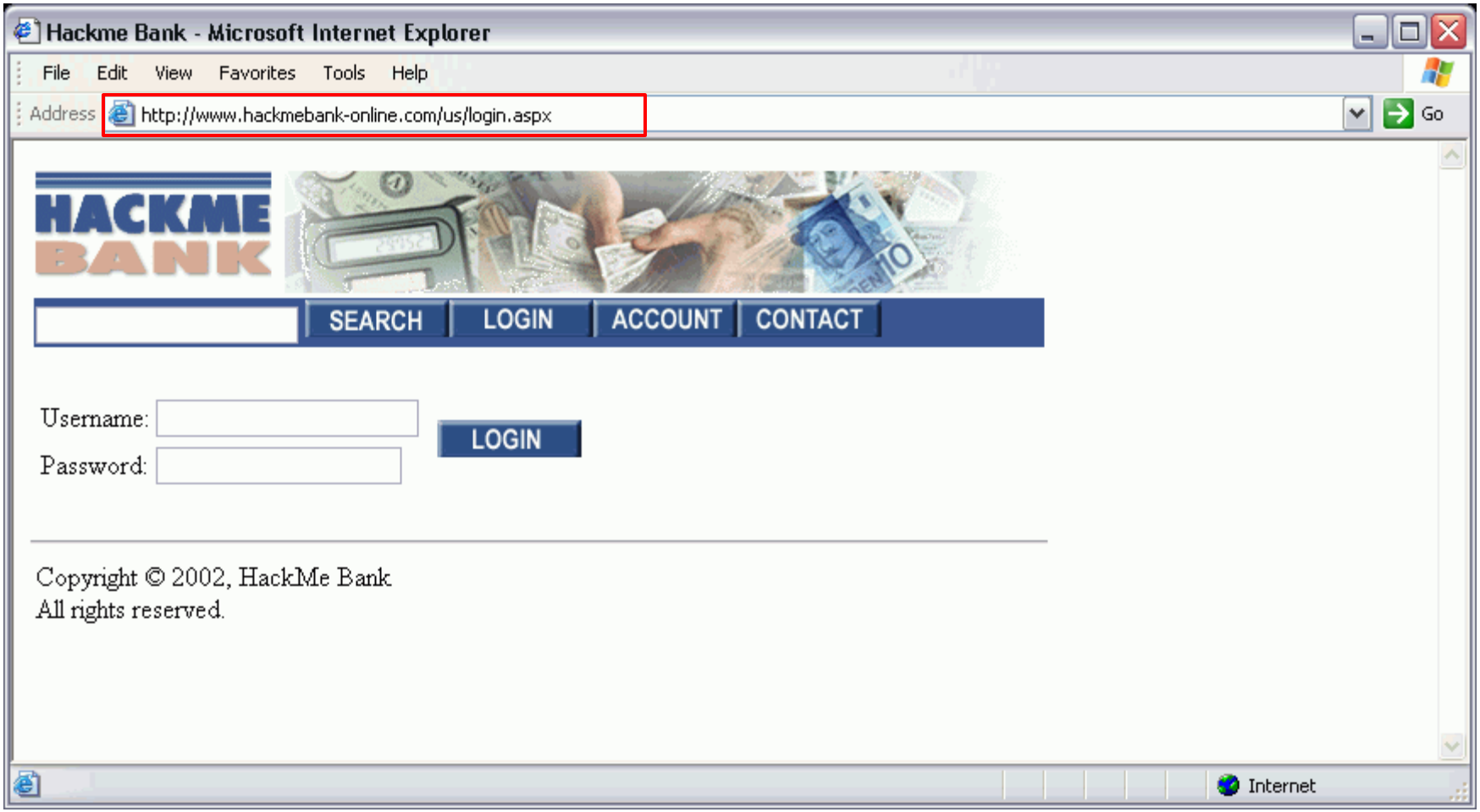
Other Communication Attack Techniques

- Instant messages
- Message boards
- Guestbooks
- Blog Comments
- Wireless
- Virus, Trojans
- Etc.

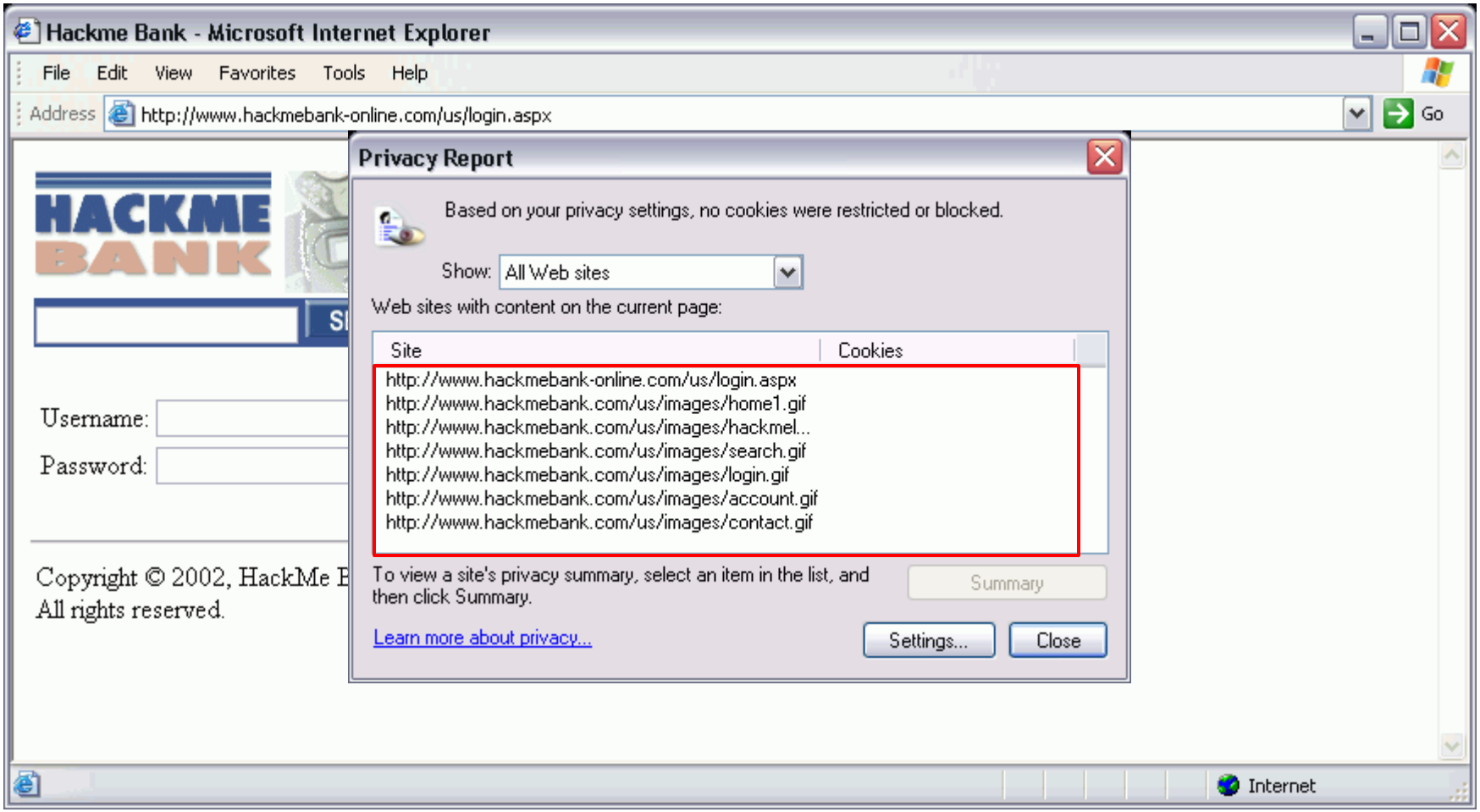
Website Attack Techniques

- Fully spoofed site
- Stolen images
- Browser GUI manipulation
- Framed Keyloggers
- Pop-up / Pop-under
- XSS defacement
- Pharming

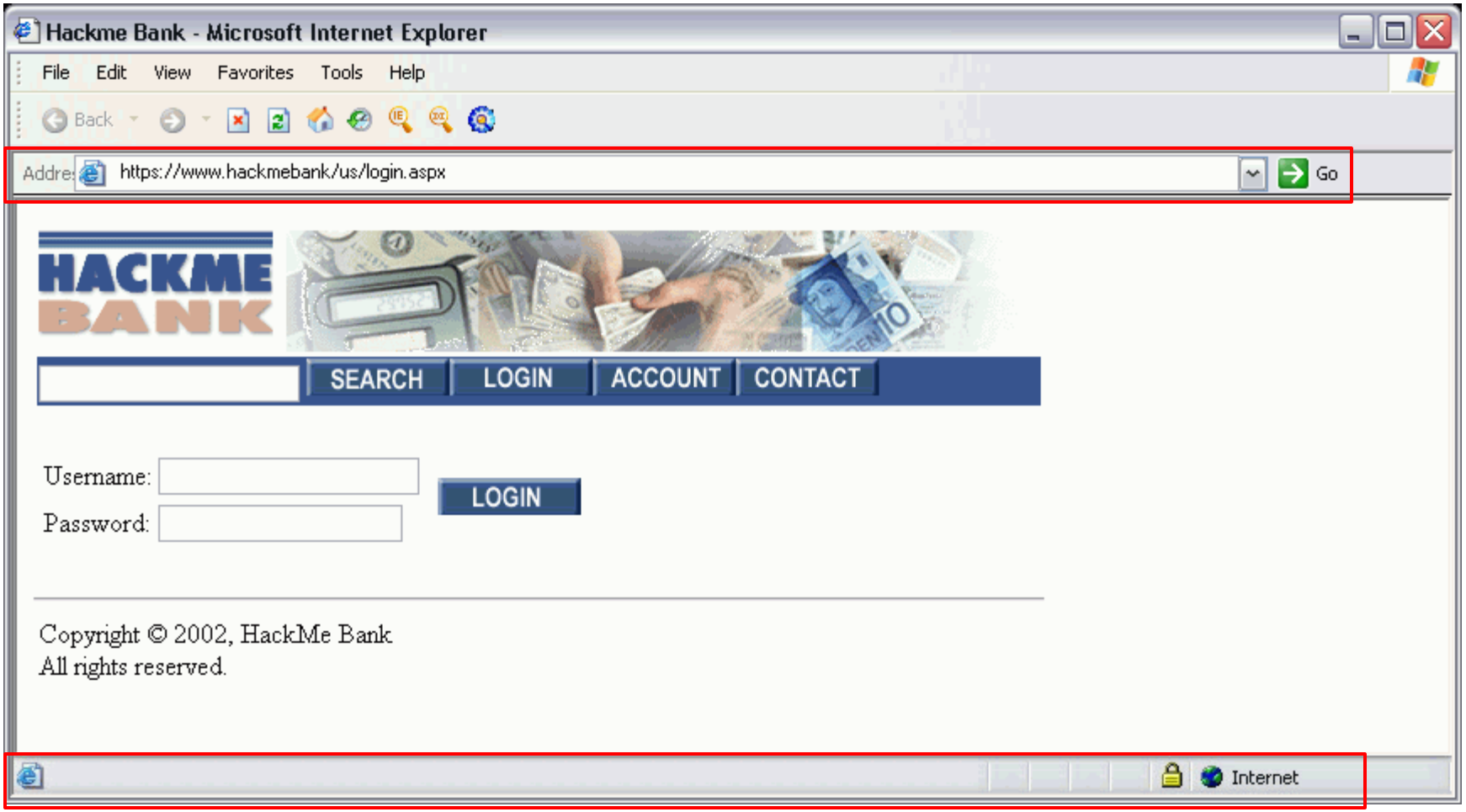
Fully Spoofed Site



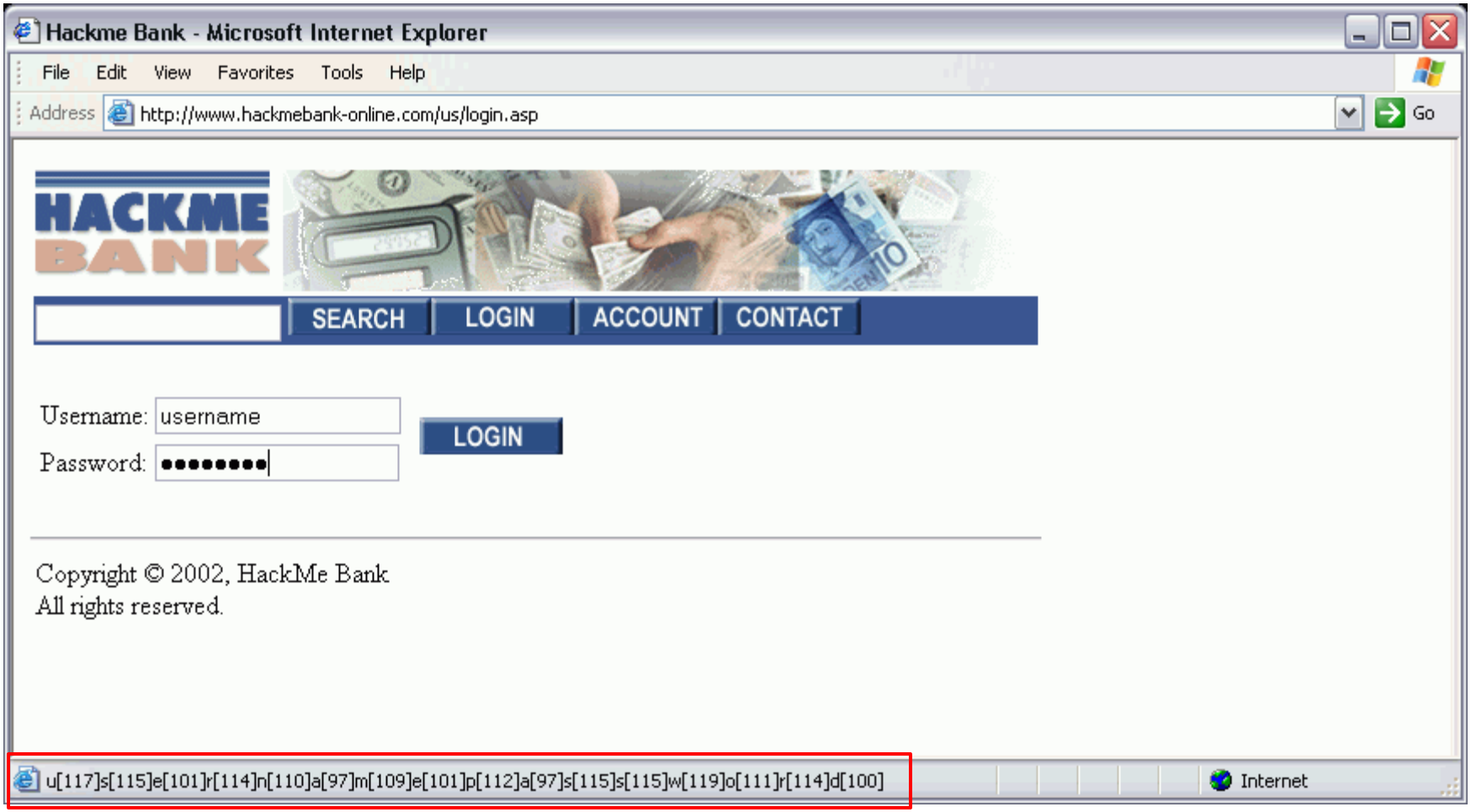
Stolen Images



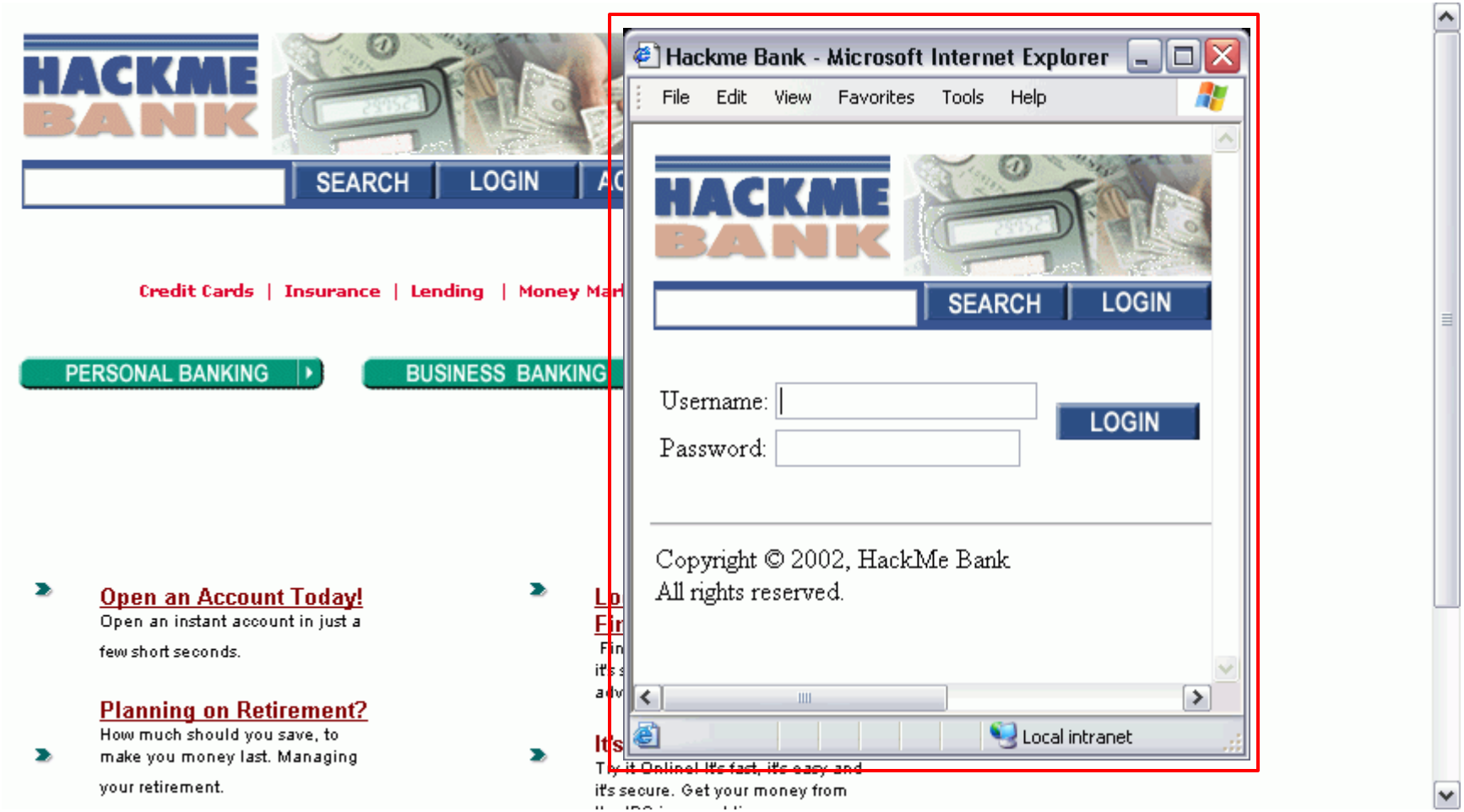
Browser GUI Manipulation



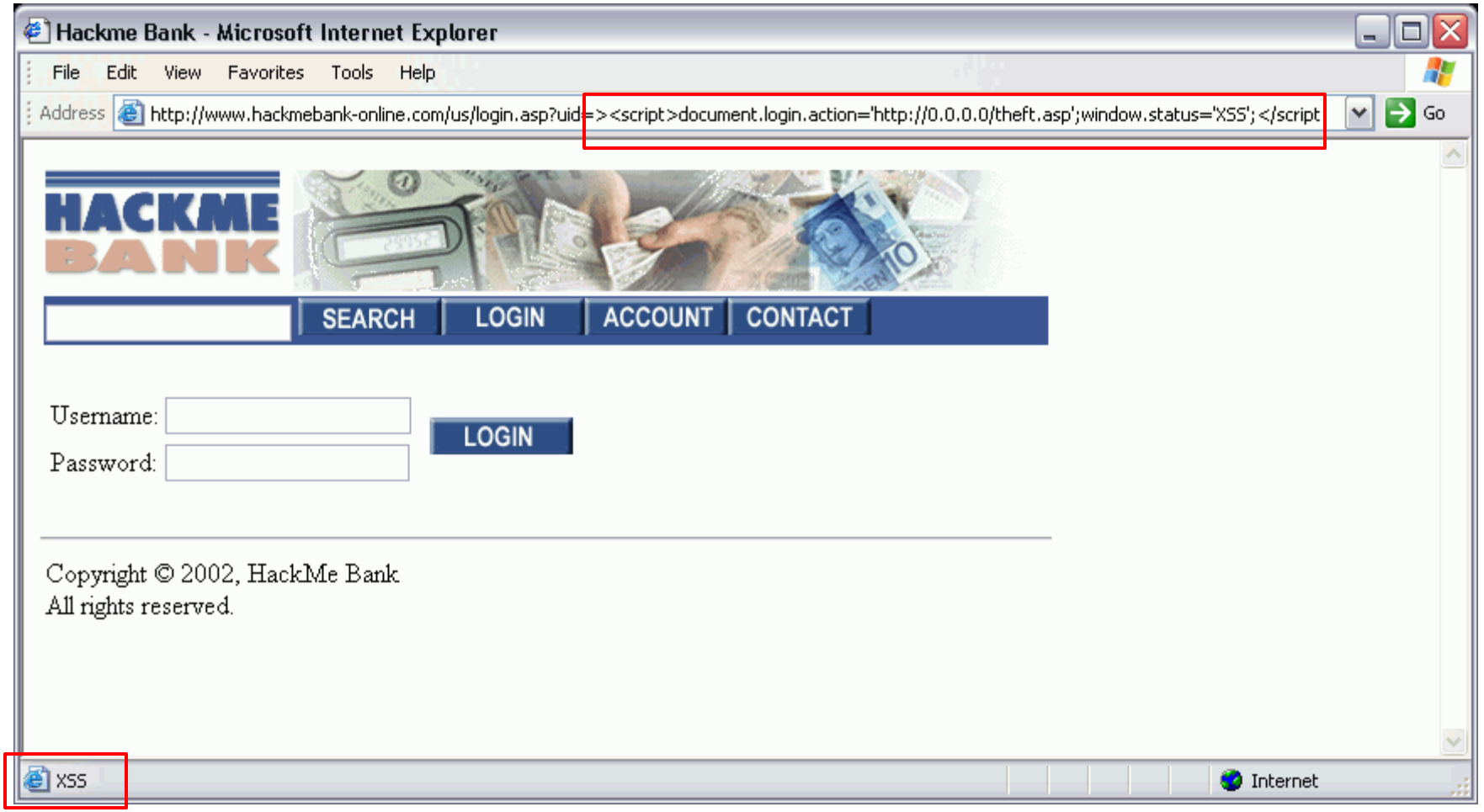
Framed Keylogger



Pop-up / Pop-under



XSS Defacement



Pharming

- HOSTS file modification
- DNS Attacks
- Web Cache Poisoning

Pharming: HOSTS File Modification

- Trumps DNS settings
- Virus, trojans, spyware
  - April, 2005 – 77
  - May, 2005 – 79
  - June, 2005 – 154
  - July, 2005 – 174
- Disable AV update sites
- Advanced techniques
  - Multi-part

Pharming: DNS Attacks

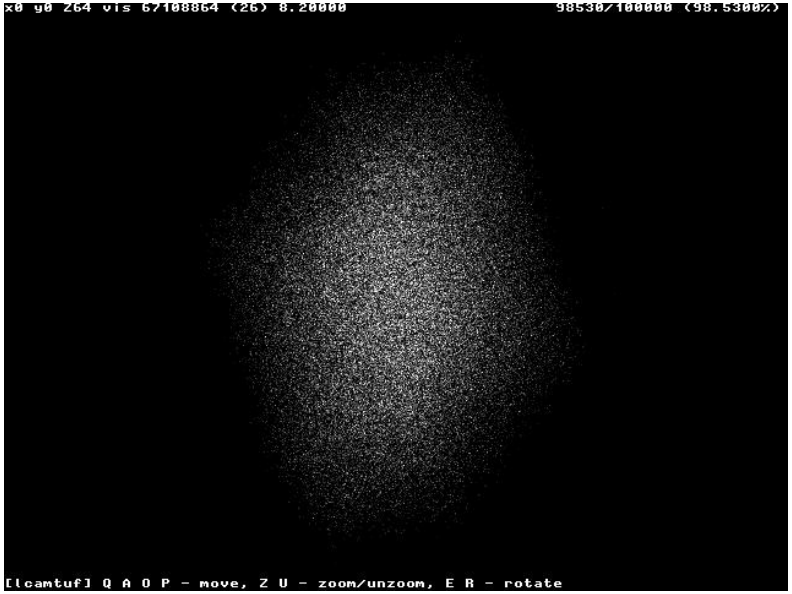
- Known vulnerabilities
- DNS protocol solely dependant on port and ID
- Techniques
  - Blind spoofing
  - PRNG problems
  - Birthday paradox
  - DOS attacks
    - October, 2002

Blind Spoofing

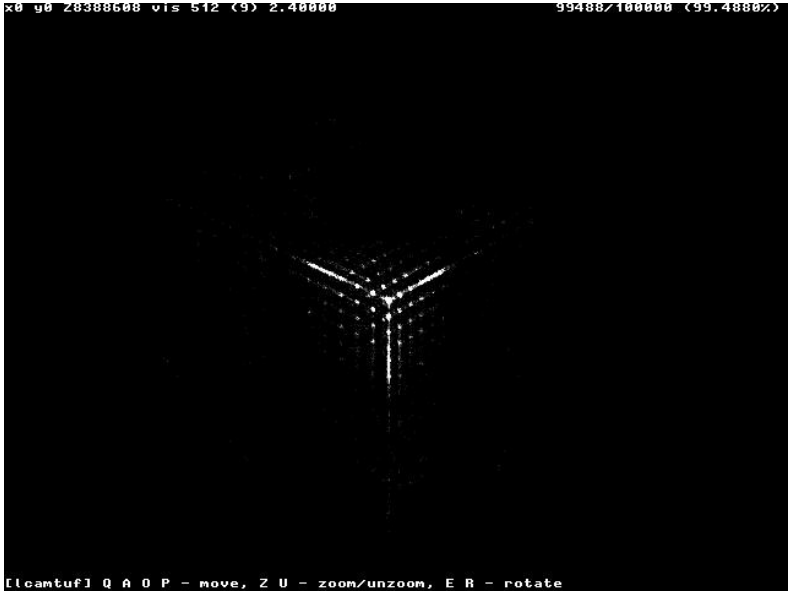
- Attacker can not see the query
  - Must guess the transaction ID and port
- Poor DNS implementations make this easy
  - Static port configuration
  - Sequential transaction IDs

PRNG Problems

- Random numbers are not always random
- Some transaction IDs more likely to be used



Linux 2.2
Attack feasibility: < 0.05%



Windows 98 SE
Attack feasibility: 100%

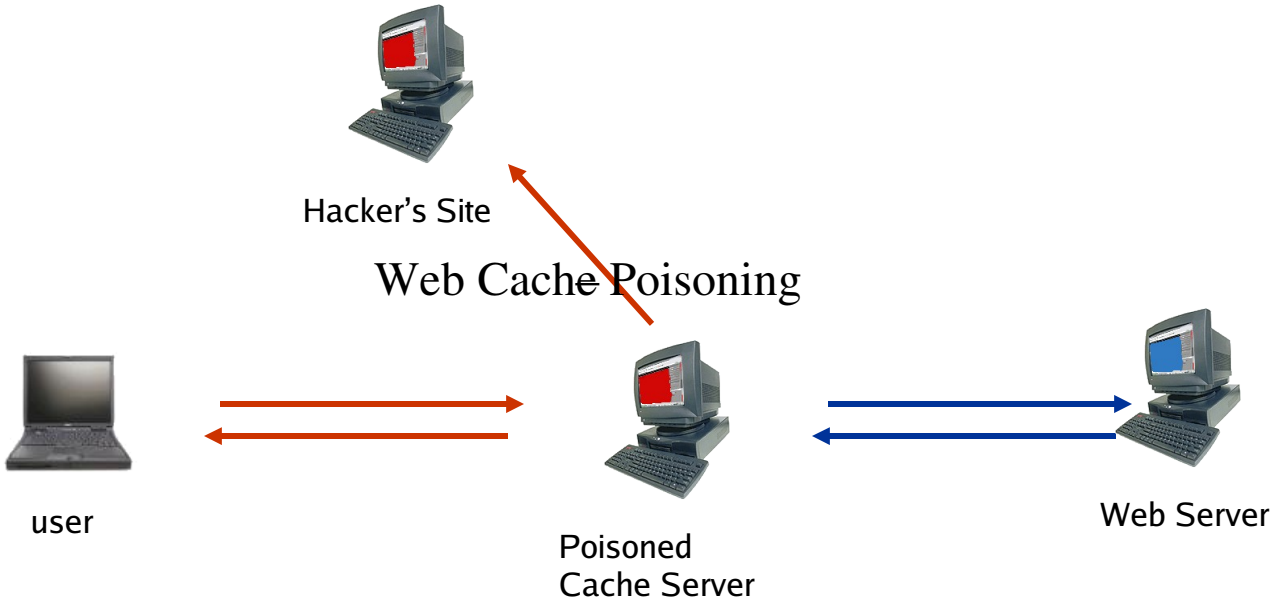
Birthday Paradox

- "If there are 23 people in a room then there is a chance of more than 50% that at least two of them will have the same birthday"

- Conventional logic suggests a transaction ID collision probability of 1 in 65,535
  - Birthday paradox reduces this probability to only 1 in 700

Web Cache Poisoning

- Coming soon to a phishing pond near you



Hacker taints only pages that interest them. Personal Information is collected and sent to hacker's site using ***your*** cache server!

Current Security Models

- Secure Sockets Layer (SSL)
  - Encrypts the data between the server and client
- Web Browser Security
  - Same origin policy
  - Cookie flag (httpOnly)
  - Cookie flag (secure)
- Two Factor Authentication
  - Something you know / have / are / do
- Consumer Education

Best Practice Responsibilities

- Prevention
- Detection
- Resolution
- Operational Controls

Best Practices: Prevention

- Technology
  - Web application security
    - Restrict Track / Trace HTTP methods
    - Output Encoding
    - Use “httpOnly” & “secure” cookie flags
    - Break out of frames
      - if (self != top) top.location = self.location;
  - Web application firewalls
    - XSS detection
    - Content referrer restrictions
  - Email integrity solutions
    - Digital signatures
    - Email sender verification

Best Practices: Operational Prevention

- Operational
  - Customer Education
    - Describe how you will interact with them
    - Possible ID theft techniques & safeguards
  - Email Communication
    - Be consistent with all customer communication
    - Do not ask for personal information
  - Web
    - Blanket SSL
    - Two factor authentication
    - Domain name consistency

Best Practices: Detection

- Technology
  - Phishing email monitoring
  - Domain name management
  - Traffic analytics monitoring
  - Internet monitoring
- Operational
  - Email bounce back analysis
  - Call centers
  - Website feedback

Best Practices: Resolution

- Counter Measures - Site Take Down
  - ISP communication
  - Contact Email Provider
  - Notify law officials
  - Data Poisoning
- Fraudulent Site Forensics
  - Owner identification: Email & Website
  - Risk assessment
  - Website characteristics
    - Code, Technologies, ISP, etc.

Best Practices: Operational Controls

- Policy and Procedures
  - Incident Response Plan
  - Internal and External Communications Plan
- Prioritization
- Customer Impact Assessment
  - Customers affected
  - Financial impact
- Feedback
  - Learn from each event and improve process and countermeasures

Thank - you

- Questions ?
- Comments ?