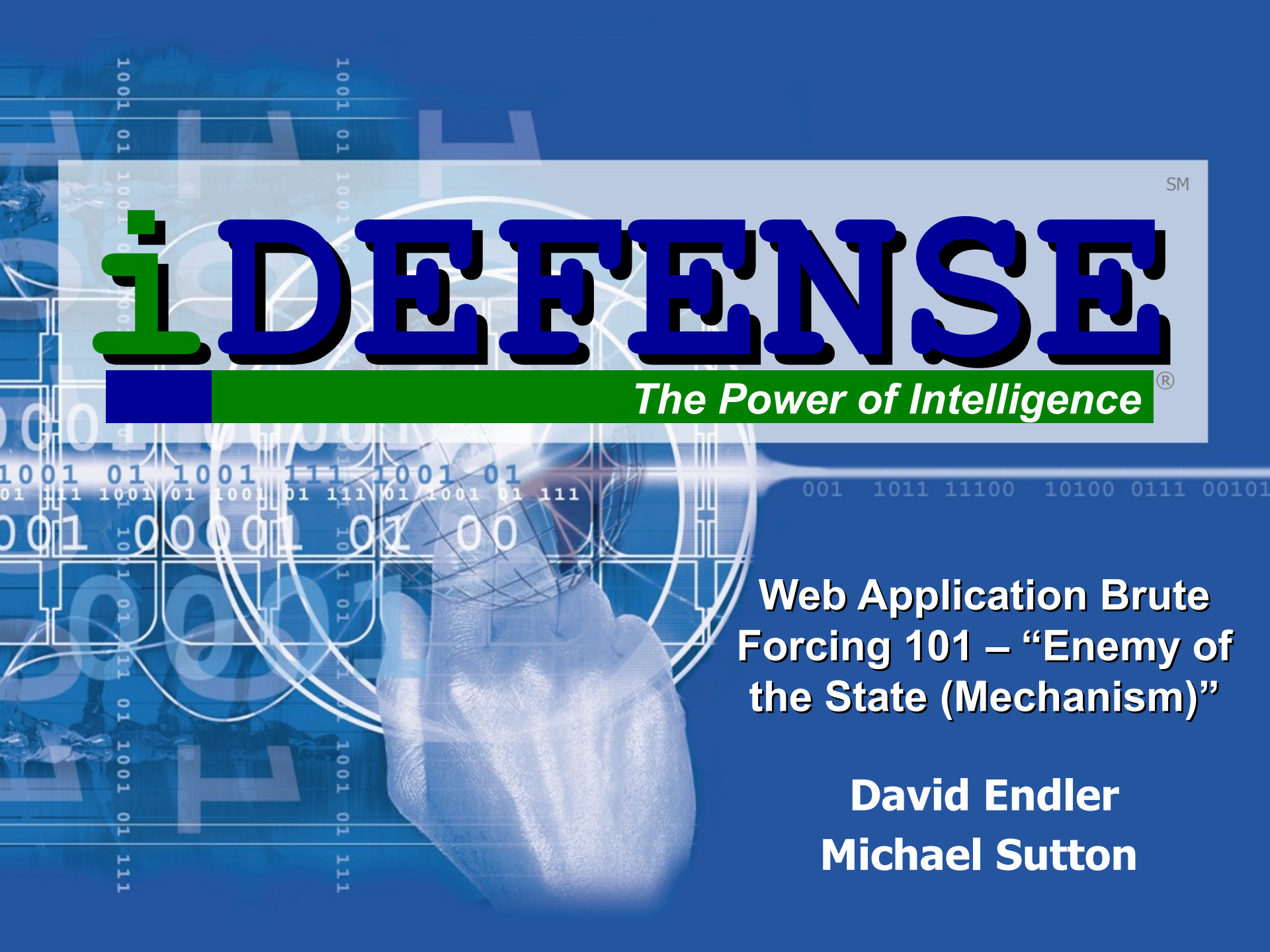

SM
iDEFENSE
The Power of Intelligence
Web Application Brute Forcing 101 – "Enemy of the State (Mechanism)"
David Endler
Michael Sutton

Outline

- What are Session IDs?
- Security Problems with Session IDs
- An Emerging Threat - Brute Forcing Web Session ID's
- Notable News Items
- Fun Exploitation Examples
- 6 Common Problems
- General Protection Measures
  - Developers
  - Users
- Resources

• Copyright © 2002 iDEFENSE Inc.

Session ID Overview

- HTTP is stateless protocol
- Rather than make a user authenticate upon each click in a web application, a sense of "state" is created
- In order to maintain state, a shared string, token, or secret between HTTP client and server is usually used by developers
- Essentially, authentication data (username/password) exchanged for "Session ID"

• Copyright © 2002 iDEFENSE Inc.

Session ID Overview

- While it is generally clear that username/password pairs are indeed authentication data and therefore sensitive, it is not generally understood that session IDs are also just as sensitive because of their frequent use for authentication. See RFC 2964 (Use of HTTP State Management).

• Copyright © 2002 iDEFENSE Inc.

Session ID Overview

- Session IDs are commonly stored in cookies and/or URLs, and hidden fields of web pages
- Session ID generated by WEB SERVER (IIS, etc.) when the user first hits the site or by WEB APPLICATION (ATG dynamo, Apache Tomcat, BEA Websphere, .jsp, .asp, perl, etc.) when the user logs in

• Copyright © 2002 iDEFENSE Inc.

Cookie Refresher

- Sometimes the cookies are set to expire (i.e., be deleted) upon closing the browser; these are typically called "session cookies" or "non-persistent" cookies
- Persistent cookies last beyond a user's session (i.e. "Remember Me" option)
- Persistent cookies are usually stored on the user's hard drive in a location according to the particular operating system and browser (e.g. , C:\Program files\netscape \users*username*\cookies.txt for Netscape and C:\Documents and Settings *username*\Cookies for IE on Win2K).

• Copyright © 2002 iDEFENSE Inc.

Cookie Refresher

- Cookie Refresher (RFC 2965)

1	2	3	4	5	6	7
www.redhat.com	FALSE	/	FALSE	1154029490	Apache	64.3.40.151.1601899634924 7480

1.) domain: The website domain that created and that can read the variable.

2.) flag: A TRUE/FALSE value indicating whether all machines within a given domain can access the variable.

3.) path: Pathname of the URL(s) capable of accessing the cookie from the domain.

4.) secure: A TRUE/FALSE value indicating if an SSL connection with the domain is needed to access the variable.

5.) expiration: The Unix time that the variable will expire on. Unix time is defined as the number of seconds since 00:00:00 GMT on Jan 1, 1970. Omitting the expiration date signals to the browser to store the cookie only in memory; it will be erased when the browser is closed. (expires July 27, 2006)

6.) name: The name of the Session ID variable (in this case Apache).

7.) value: The value of the Session ID variable (in this case 64.3.40.151.1601899634924748O) .

• Copyright © 2002 iDEFENSE Inc.

Cookie Stored Session ID Examples

.starwars.com	TRUE	/	FALSE	1341753778	Wookie-Cookie	13fe8fff4799f27dcf19c959dafa8437
.www.ibm.com	TRUE	/rc	FALSE	1293768100	sauidp	p0010000000006DCC10255298230000591992.003F75FEF2
.ebay.com	TRUE	/	FALSE	1183296824	lucky8	694036
.amazon.com	FALSE	/	FALSE	1026115299	session-id	103-1456769-7895034
.yahoo.com	TRUE	/	FALSE	1271361612	B	3qpaarsu48dai&b=2
.yahoo.com	TRUE	/	FALSE	1154029490	I	ir=9p&in=4aweec66&i1=AFABCl
.yahoo.com	TRUE	/	FALSE	1154029490	PU	t=1

• Copyright © 2002 iDEFENSE Inc.

URL Stored Session ID

- http://www.123greetings.com/view/7AD30725122120803
- http://evite.citysearch.com/r?iid=KVIJBUFDLPVMIVLXYUKB
- http://view.greetings.yahoo.com/greet/view?FXA96K95JAEJS
- http://www.atg.com/en/index.jhtml;jsessionid=HYMJK3PJUSJ4CCQCQBJCGWQKAKAFUIV0?_requestid=21122
- http://www.amazon.com/exec/obidos/subst/home/home.html/102-4524380-3923344

• Copyright © 2002 iDEFENSE Inc.

Session IDs in HTML Hidden Fields

```
<FORM METHOD=POST ACTION="/cgi-bin/bankonline.cgi">

<input type="hidden" name="sessionID" value="abcde1234">
<input type="hidden" name="useraccount" value="673-12745">

<input type="submit" name="Access My Bank Information"></form>
```

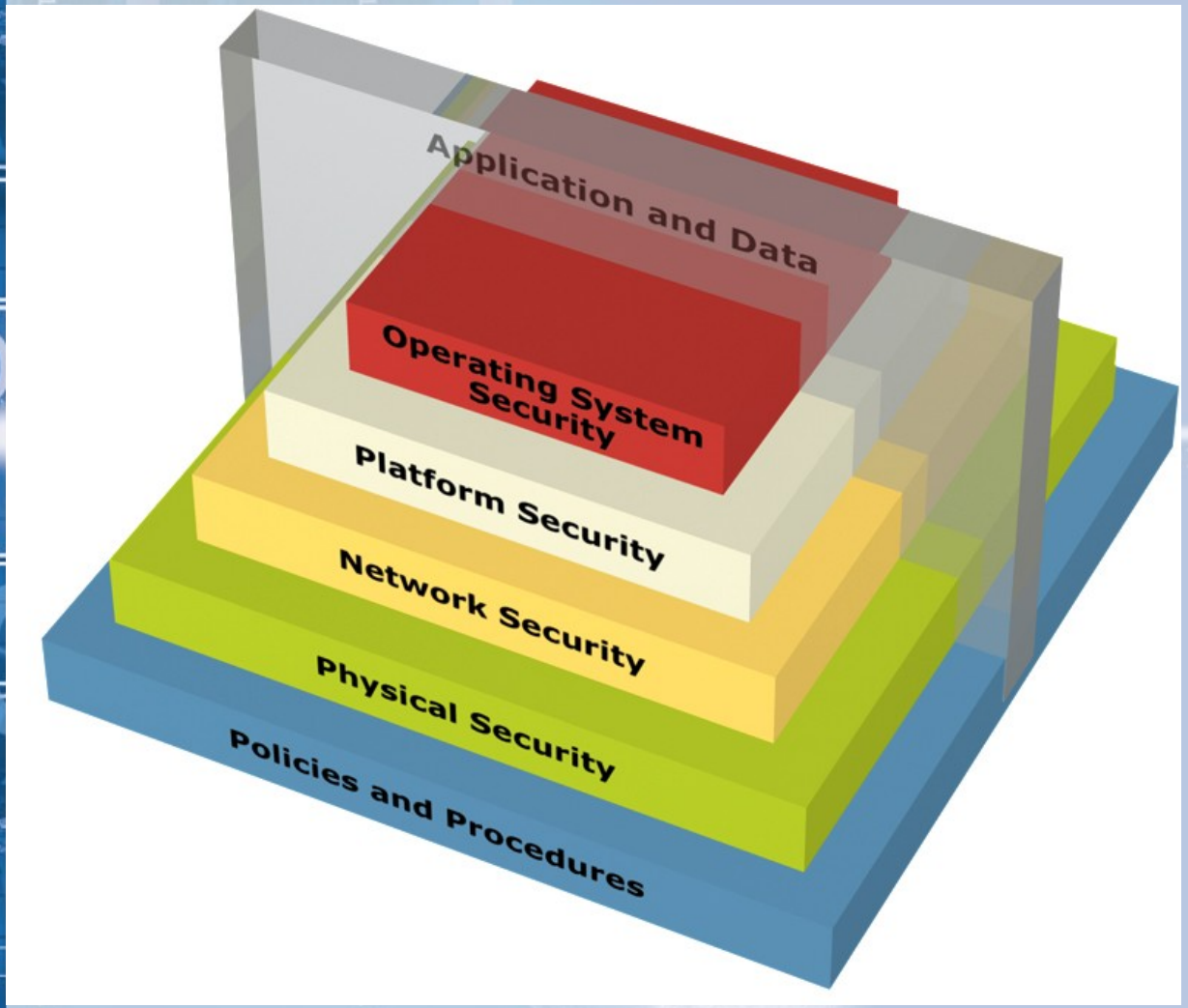
• Copyright © 2002 iDEFENSE Inc.

Session ID Security

- While it is generally clear that username/password pairs are indeed authentication data and therefore sensitive, it is not generally understood by users AND developers that session IDs are also just as sensitive because of their use for authentication. See RFC 2964 (Use of HTTP State Management).

• Copyright © 2002 iDEFENSE Inc.

Session ID Security Overview

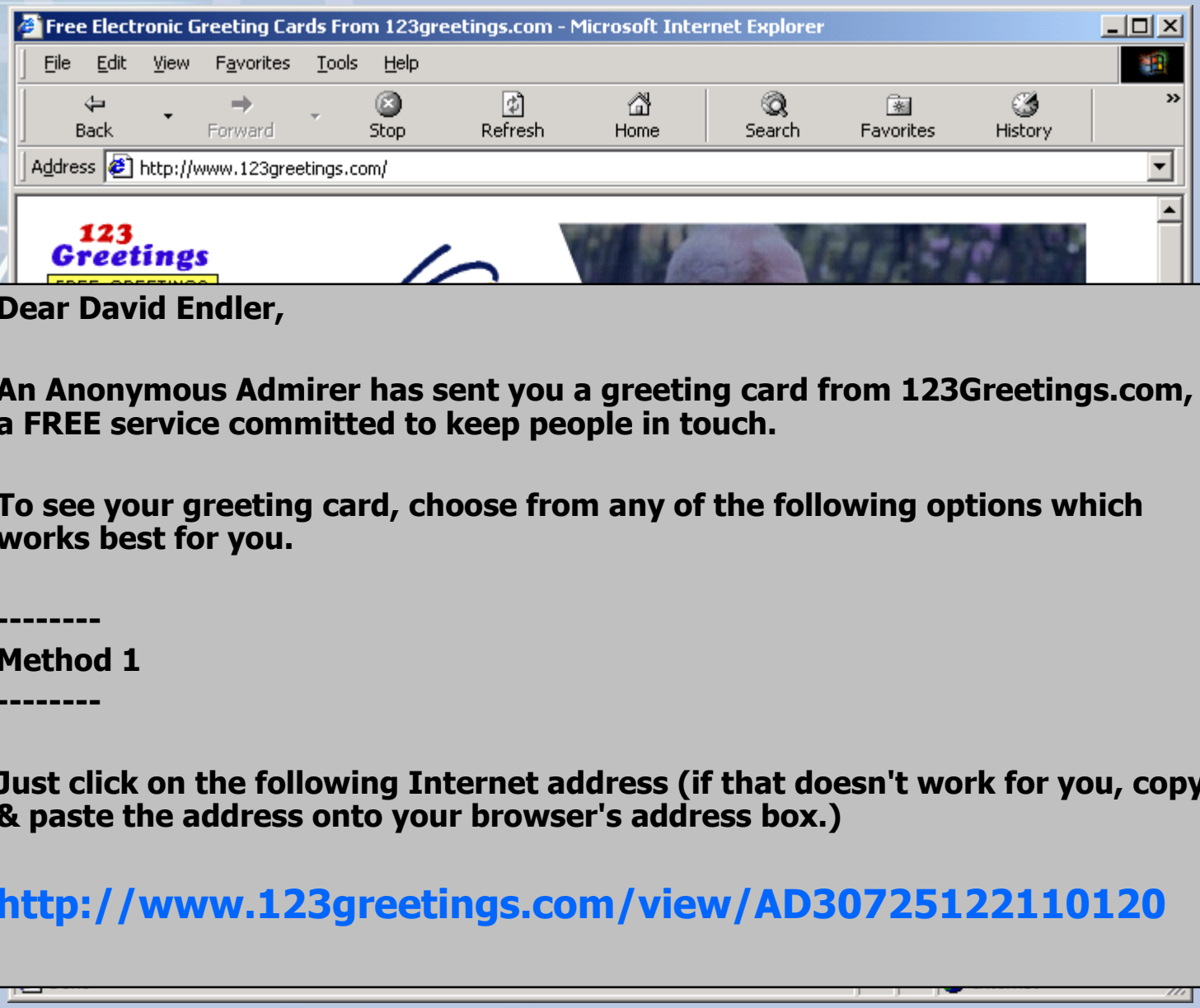


Session ID security is a microcosm of Web Application Security.

Web Application Security cuts through many different aspects of an organization's information security infrastructure

• Copyright © 2002 iDEFENSE Inc.

An Example: Brute Forcing Session ID's in URLS



• Copyright © 2002 iDEFENSE Inc.

An Example: Brute Forcing Session ID's in URLS

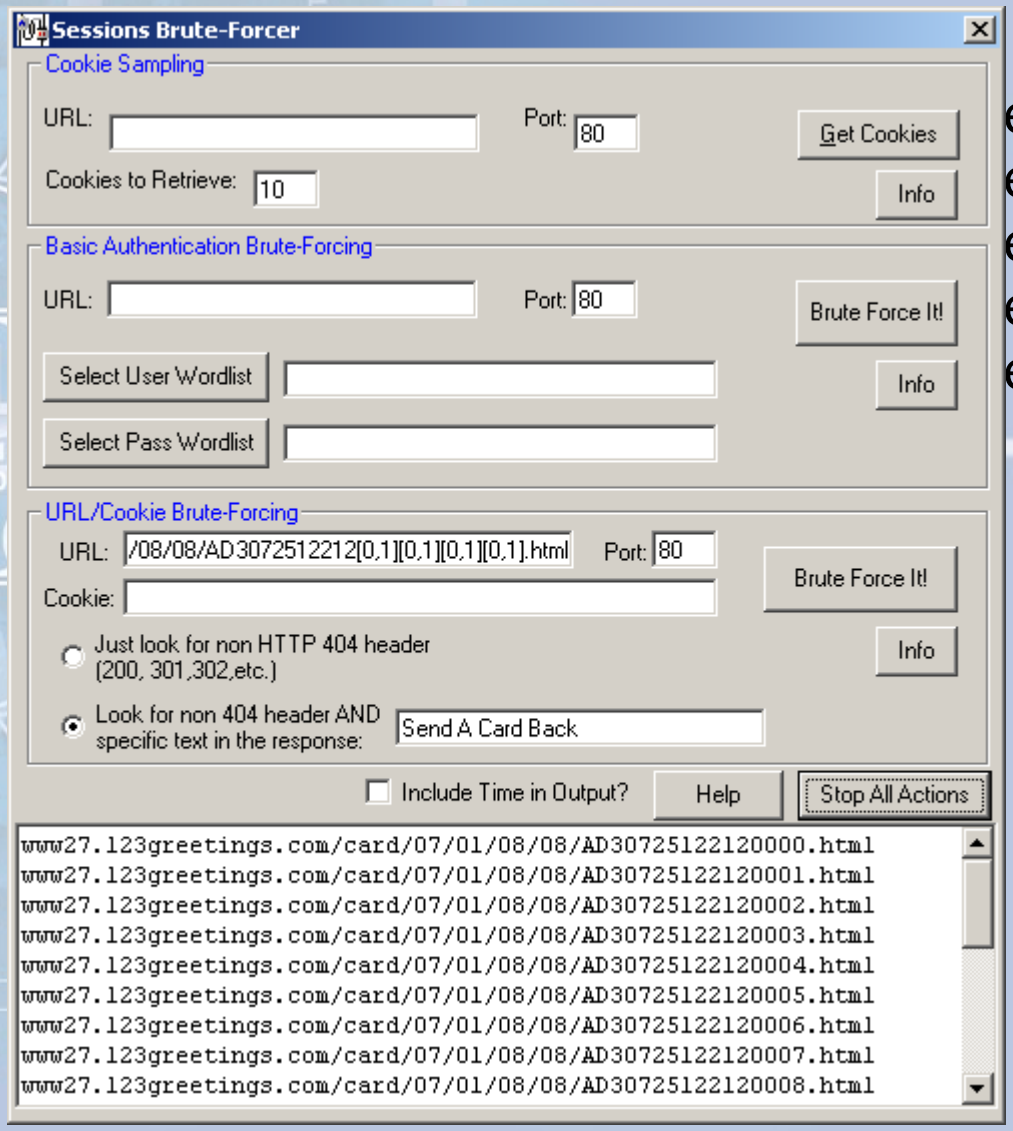
http://www.123greetings.com/view/AD30725122116211
http://www.123greetings.com/view/AD30725122118909
http://www.123greetings.com/view/AD30725122120803
http://www.123greetings.com/view/AD30725122122507
http://www.123greetings.com/view/AD30725122124100

As we start to associate that the date we sent these electronic cards on was July 25 at 12:21 PST, we can start to eliminate some more entropy out of this session ID (07251221). Notice then that we're left with five incrementing "random" digits at the end of the URL.

http://www.123greetings.com/view/AD3072512211 6211
http://www.123greetings.com/view/AD3072512211 8909
http://www.123greetings.com/view/AD3072512212 0803
http://www.123greetings.com/view/AD3072512212 2507
http://www.123greetings.com/view/AD3072512212 4100

• Copyright © 2002 iDEFENSE Inc.

An Example: Brute Forcing Session ID's in URLS AUTOMATED DEMO!



ew/AD307251221**16211**
ew/AD307251221**18909**
ew/AD307251221**20803**
ew/AD307251221**22507**
ew/AD307251221**24100**

• Copyright © 2002 iDEFENSE Inc.

Why Brute Forcing Web Session ID's is Bad

- Can result in an online user's web application account being hijacked or loss of privacy
- Easy to exploit
- Unlike typical login scenario, no failed login lockout
- Prevalent disclosure among security mailing lists
- Typical security solutions (firewalls, IDS, etc.) do nothing to detect attacks
- Log data is usually not that detailed
- IDS is not well developed for Web Application attacks
- SSL does nothing to protect against these attacks

• Copyright © 2002 iDEFENSE Inc.

In the News

- "Privacy hole found in Verizon Wireless Web site " Computerworld, Sept 6, 2001.

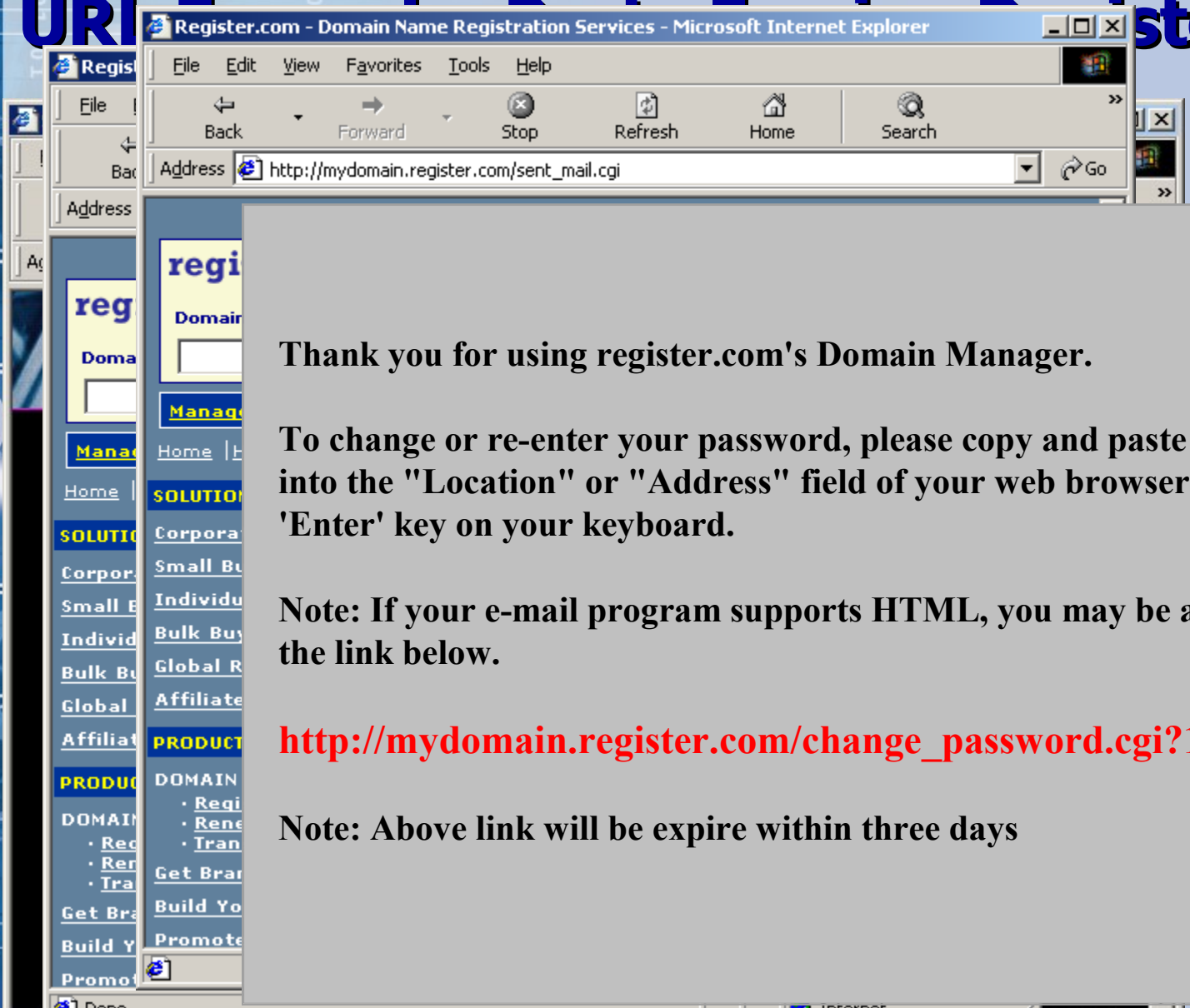
  http://www.computerworld.com/securitytopics/security/privacy/story/0,10801,63587,00.html

  http://online.securityfocus.com/archive/1/211520

- https://www.app.airtouch.com/jstage/plsql/ec_navigation_wrapper.nav_frame_display?p_session_id=3346178&p_host=ACTION

• Copyright © 2002 iDEFENSE Inc.

URI ... ster.com



Thank you for using register.com's Domain Manager.

To change or re-enter your password, please copy and paste the URL below into the "Location" or "Address" field of your web browser and hit the 'Enter' key on your keyboard.

Note: If your e-mail program supports HTML, you may be able to click on the link below.

http://mydomain.register.com/change_password.cgi?155218782787

Note: Above link will be expire within three days

Example 2: Brute Forcing Web Session ID's

http://mydomain.register.com/change_password.cgi?486218782865

http://mydomain.register.com/change_password.cgi?440218782891

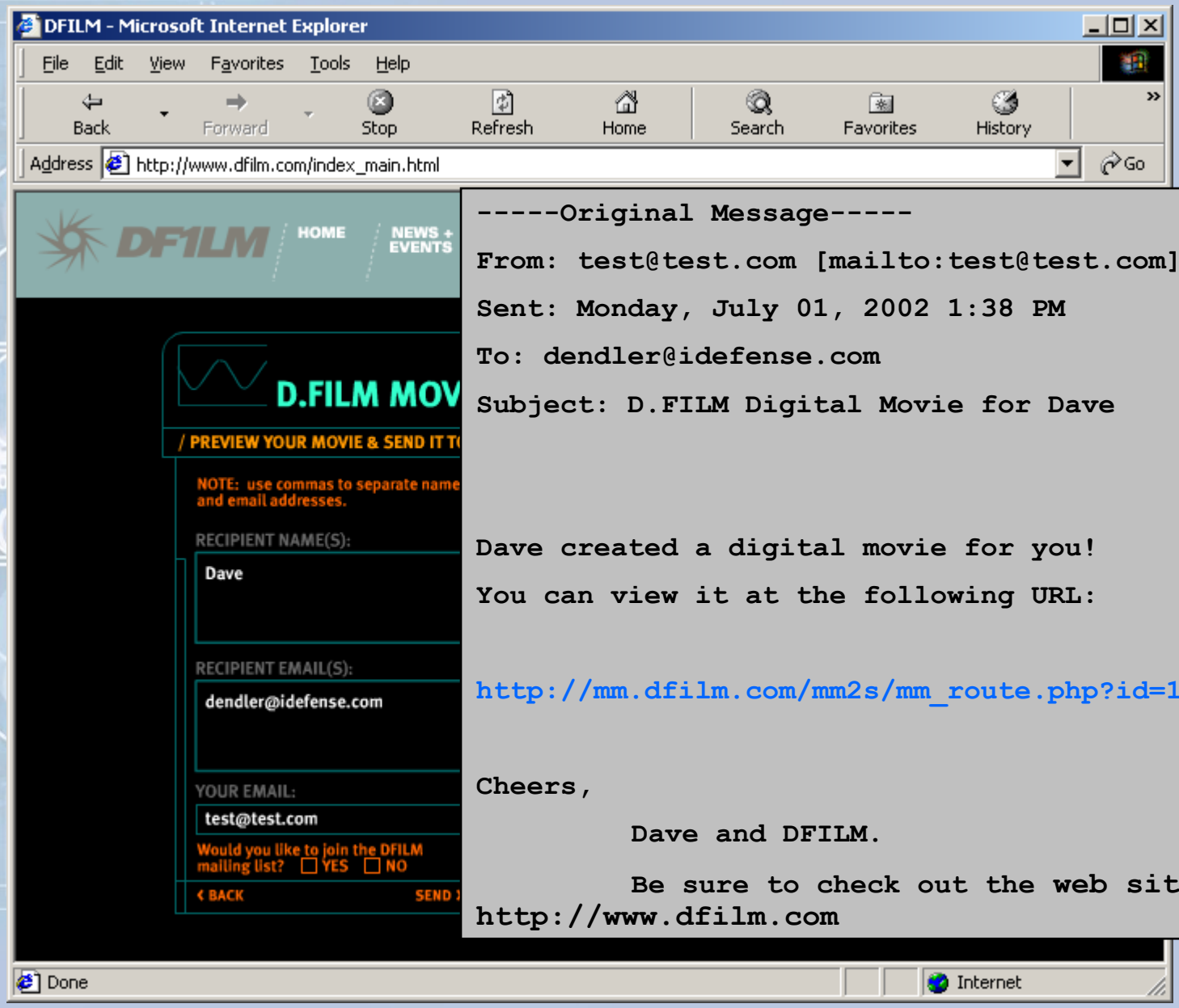
http://mydomain.register.com/change_password.cgi?685218782917

http://mydomain.register.com/change_password.cgi?505218782956

http://mydomain.register.com/change_password.cgi?486218782865
http://mydomain.register.com/change_password.cgi?440218782891
http://mydomain.register.com/change_password.cgi?685218782917
http://mydomain.register.com/change_password.cgi?505218782956
http://mydomain.register.com/change_password.cgi?435218782969

• Copyright © 2002 iDEFENSE Inc.

URL Example – Brute Forcing Dfilm.com




```
-----Original Message-----
From: test@test.com [mailto:test@test.com]
Sent: Monday, July 01, 2002 1:38 PM
To: dendler@idefense.com
Subject: D.FILM Digital Movie for Dave


Dave created a digital movie for you!
You can view it at the following URL:

http://mm.dfilm.com/mm2s/mm_route.php?id=110532

Cheers,
        Dave and DFILM.
        Be sure to check out the web site at
http://www.dfilm.com
```

• Copyright © 2002 iDEFENSE Inc.

URL Example – Brute Forcing Dfilm.com

No privacy of other user's creations:

```
http://mm.dfilm.com/mm2s/mm_route.php?id=110532
http://mm.dfilm.com/mm2s/mm_route.php?id=110531
http://mm.dfilm.com/mm2s/mm_route.php?id=110530
http://mm.dfilm.com/mm2s/mm_route.php?id=110529
http://mm.dfilm.com/mm2s/mm_route.php?id=110528
http://mm.dfilm.com/mm2s/mm_route.php?id=110527
http://mm.dfilm.com/mm2s/mm_route.php?id=110526
http://mm.dfilm.com/mm2s/mm_route.php?id=...
```

• Copyright © 2002 iDEFENSE Inc.

URL Example – Sendomatic.com

http://www.sendomatic.com/servlets/servlets/mysendo?uId=76330

• Copyright © 2002 iDEFENSE Inc.

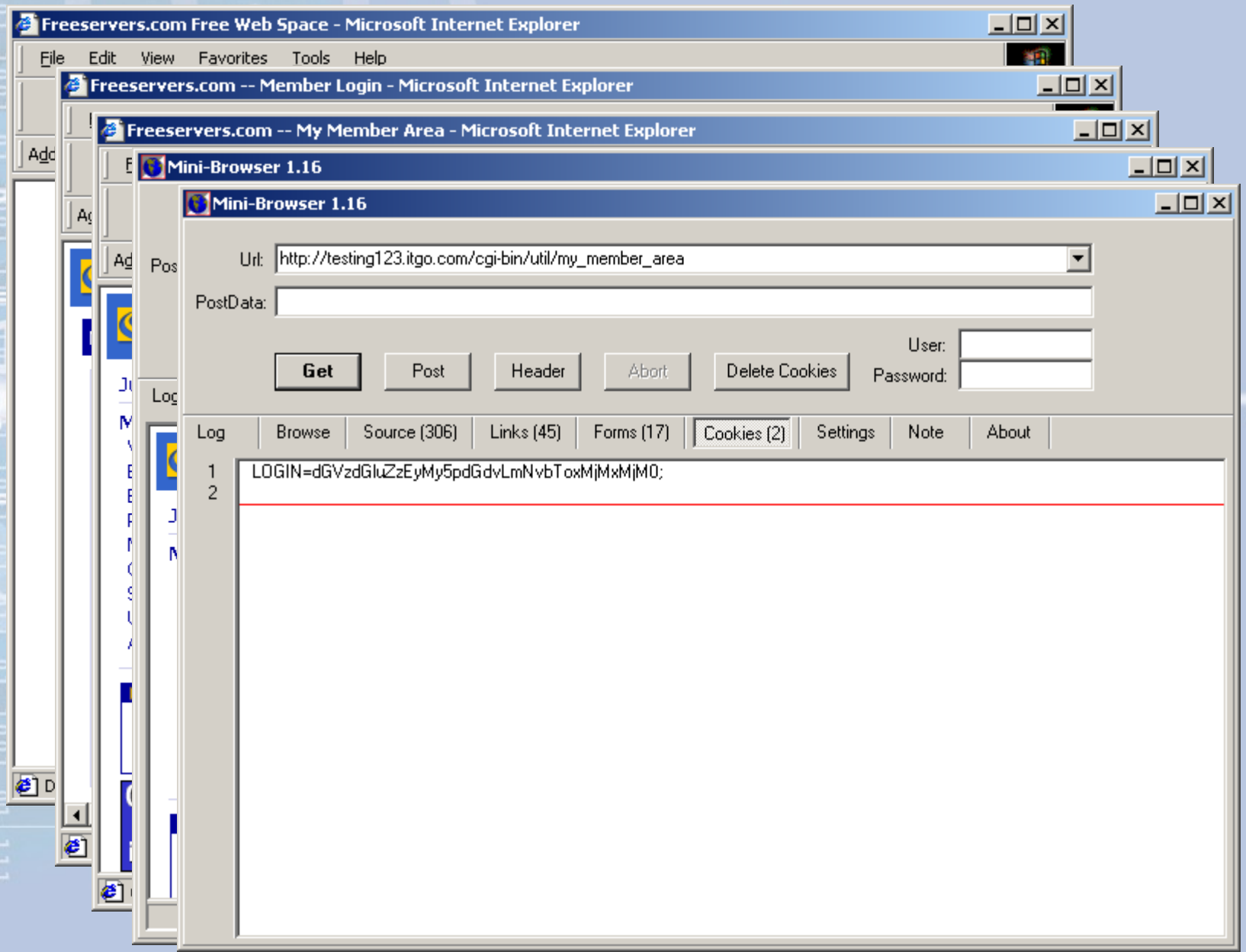
URL Example – Sendomatic.com

View other people's events. Crash a party, edit an event, cancel and event, etc.

http://www.sendomatic.com/servlets/servlets/mysendo?uId=76330
http://www.sendomatic.com/servlets/servlets/mysendo?uId=76331
http://www.sendomatic.com/servlets/servlets/mysendo?uId=76332
http://www.sendomatic.com/servlets/servlets/mysendo?uId=76333
http://www.sendomatic.com/servlets/servlets/mysendo?uId=76334
http://www.sendomatic.com/servlets/servlets/mysendo?uId=76335
http://www.sendomatic.com/servlets/servlets/mysendo?uId=76336
http://www.sendomatic.com/servlets/servlets/mysendo?uId=...

• Copyright © 2002 iDEFENSE Inc.

Cookie Example – Freeservers.com



Cookie Example – Freeservers.com

- LOGIN=dGVzdGluZzEyMy5pdGdvLmNvbToxMjMxMjM0;
- Base 64 decode the string: http://www.securitystats.com/tools/base64.asp

  testing123.itgo.com:1231234

  username:password
- Next, automate it with a perl exploit by feeding encoded strings in to he cookie

• Copyright © 2002 iDEFENSE Inc.

Cookie Example – Freeservers.com

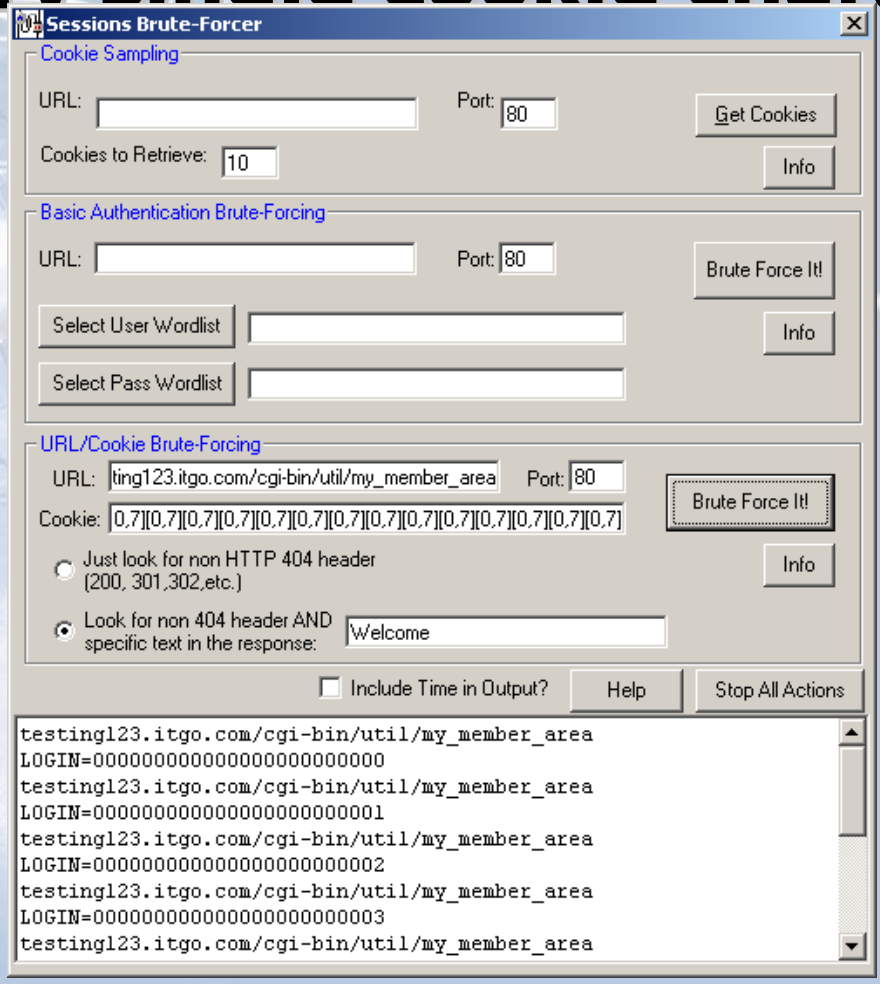
```
%perl freeservershack.pl
trying test
trying test123
trying 123123
trying 1231234

Cracked it! The password to testing123.itgo.com is
  1231234

GET http://testing123.itgo.com/cgi-
  bin/util/my_member_area
User-Agent: Mozilla/4.75 [en] (Windows NT 5.0; U)
Cookie: LOGIN=dGVzdGluZzEyMy5pdGdvLmNvbToxMjMxMjM%3D
Cookie2: $Version=1
%
```

Cookie Example – Freeservers.com

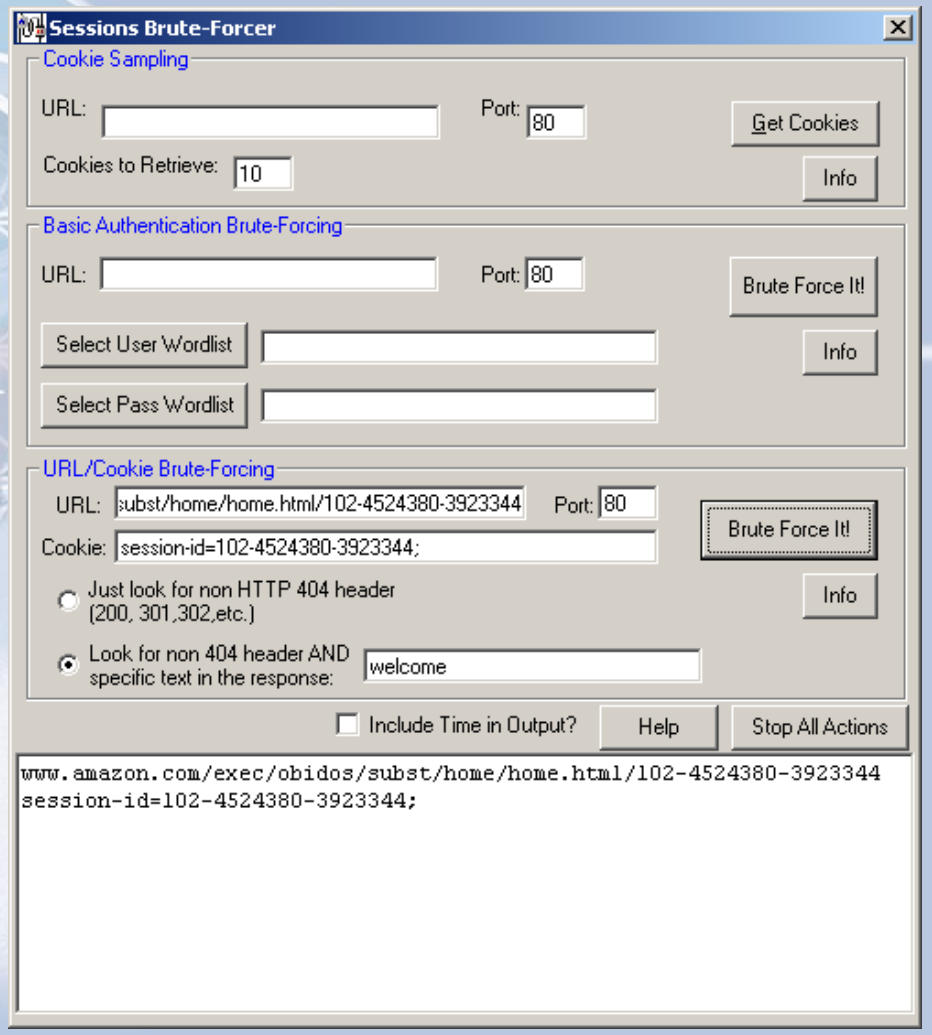
- Or a much longer way: use the brute forcer on every single cookie character combination



• Copyright © 2002 iDEFENSE Inc.

Cookie/URL Example – Amazon.com

- Some sites use the URL AND Cookie for authentication:



• Copyright © 2002 iDEFENSE Inc.

6 Common Problems

- **Weak Algorithm** – Many of the most popular web sites today are currently using linear algorithms based on easily predictable variables such as time or IP address.
- **No Form of Account Lockout** – With regard to Session ID brute force attacks, an attacker can probably try hundreds or thousands of Session IDs embedded in a legitimate URL without a single complaint from the web server.
- **Short Key Space** – Even the most cryptographically strong algorithm still allows an active Session ID to be easily determined if the size of the string's key space is not sufficiently large.

• Copyright © 2002 iDEFENSE Inc.

6 Common Problems – Continued

- **Indefinite Expiration on Server–** Session IDs that do not expire on the web server can allow an attacker unlimited time to guess a valid Session ID.
- **Transmitted in the Clear –** Assuming SSL is not being used while the Session ID cookie is transmitted to and from the browser, the Session ID could be sniffed across a flat network taking the guess-work away for a miscreant. This is still a problem with proxy servers.
- **Insecure Retrieval** – By tricking the user's browser into visiting another site, an attacker can retrieve stored Session ID information and quickly exploit this information before the user's sessions expire. This can be done a number of ways: DNS poisoning, Cross-site Scripting, etc.

• Copyright © 2002 iDEFENSE Inc.

Tools

- **Sessions Auditor**
  www.idefense.com/idtools/Session_Auditor.zip
- **Visual Testing – WebSleuth**
  www.geocities.com/dzzie/sleuth
- **WebProxy -**
  www.atstake.com/research/tools/index.html
- **HTTPush -** httpush.sourceforge.net
- **Achilles -** www.digizen-security.com/downloads.html
- **MiniBrowser -** aignes.com/download.htm

• Copyright © 2002 iDEFENSE Inc.

What Can I Do As a User?

- Logout of all sessions when done
- Do not select the "Remember me" Option
- Protect your cookies! Desktop Security
- Ensure you use SSL – when given choice of standard / secure login
- Patch your browser to be safe from some nasty Cross-site Scripting attacks
- Treat emails with Session ID info in URL's just as securely as username/passwords

• Copyright © 2002 iDEFENSE Inc.

What can I do as a Developer?

- Build and require SSL (or other encryption) into the web application so that the authentication token can not be easily sniffed in transit between browser and server;
- Ensure that all cookies enable the "secure" field
- Provide a logout function that expires all cookies and other authentication tokens
- Re-authenticate the user before critical actions are performed (i.e. a purchase, money transfer, etc.)

• Copyright © 2002 iDEFENSE Inc.

What can I do as a Developer? - Con't

- Regenerate the Session ID after certain intervals (30, 15 min. ,etc.)
- Create "booby-trapped" Session IDs to detect brute forcing attempts
- When practical, limit successful sessions to specific IP addresses. Nly works in intranet setting where ranges are predictable and finite.
- Auto-expire sessions after 15 minutes of inactivity

• Copyright © 2002 iDEFENSE Inc.

What can I do as a Developer? – Con't

- AND MOST IMPORTANT!!
  - Vendors and website developers should ensure through a good algorithm (MD5, SHA-1, etc.) that a cryptographically strong enough session ID with a large key space is transmitted to the user over an SSL/TLS connection.
  - DO NOT derive the algorithm inputs from guessable personal or login information (name, birthday, user id, etc.)

• Copyright © 2002 iDEFENSE Inc.

Resources

- **Open Web Application Security Project** (OWASP) http://www.owasp.org
- **OWASP is an open source community project staffed entirely by volunteers from across the world. The project is developing software tools and knowledge based documentation that helps people secure web applications and web services.**
- **The OWASP Guide to Building Secure Web Applications and Web Services**

  http://www.owasp.org/guide/OWASPBuildingSecureWebApplicationsAndWebServic-V1.0.pdf
- **The OWASP Security Testing Framework**

  http://www.owasp.org/testing

• Copyright © 2002 iDEFENSE Inc.

Resources

- iDEFENSE paper on Brute Forcing Session ID's, http://www.idefense.com -> whitepapers
- CGI SECURITY, http://www.cgisecurity.net
- WhiteHat Security, http://community.whitehatsec.com
- Web Application Security Mailing List, http://online.securityfocus.com/archive/107
- MIT Cookie EATERS

  http://pdos.lcs.mit.edu/cookies/pubs.html

  "Dos and Don'ts of Client Authentication on the Web"

• Copyright © 2002 iDEFENSE Inc.

Questions

?

dendler@idefense.com
msutton@idefense.com

http://www.idefense.com

• Copyright © 2002 iDEFENSE Inc.