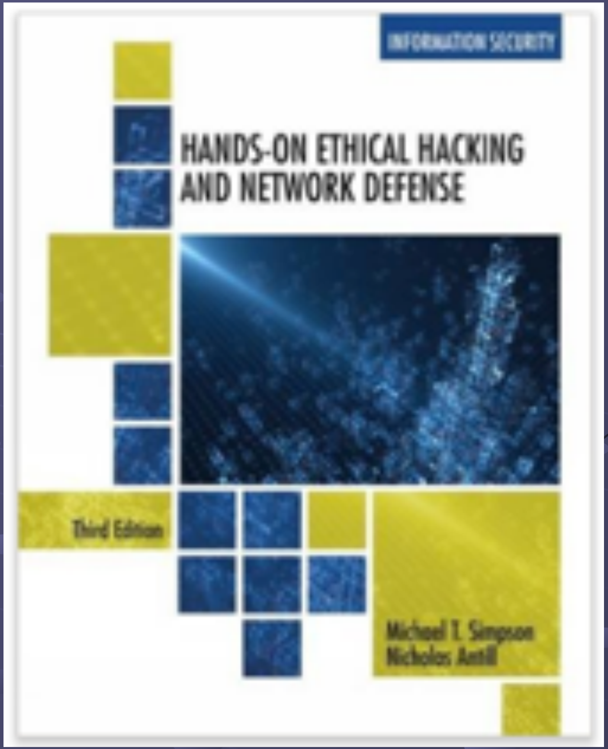
Hands-On Ethical Hacking and Network Defense 3rd Edition

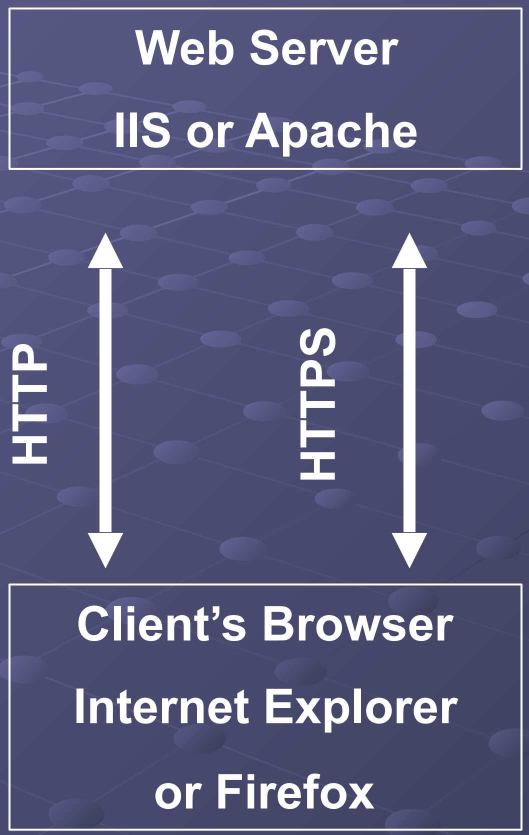


Chapter 10
Hacking Web Servers

Revised 1-11-17

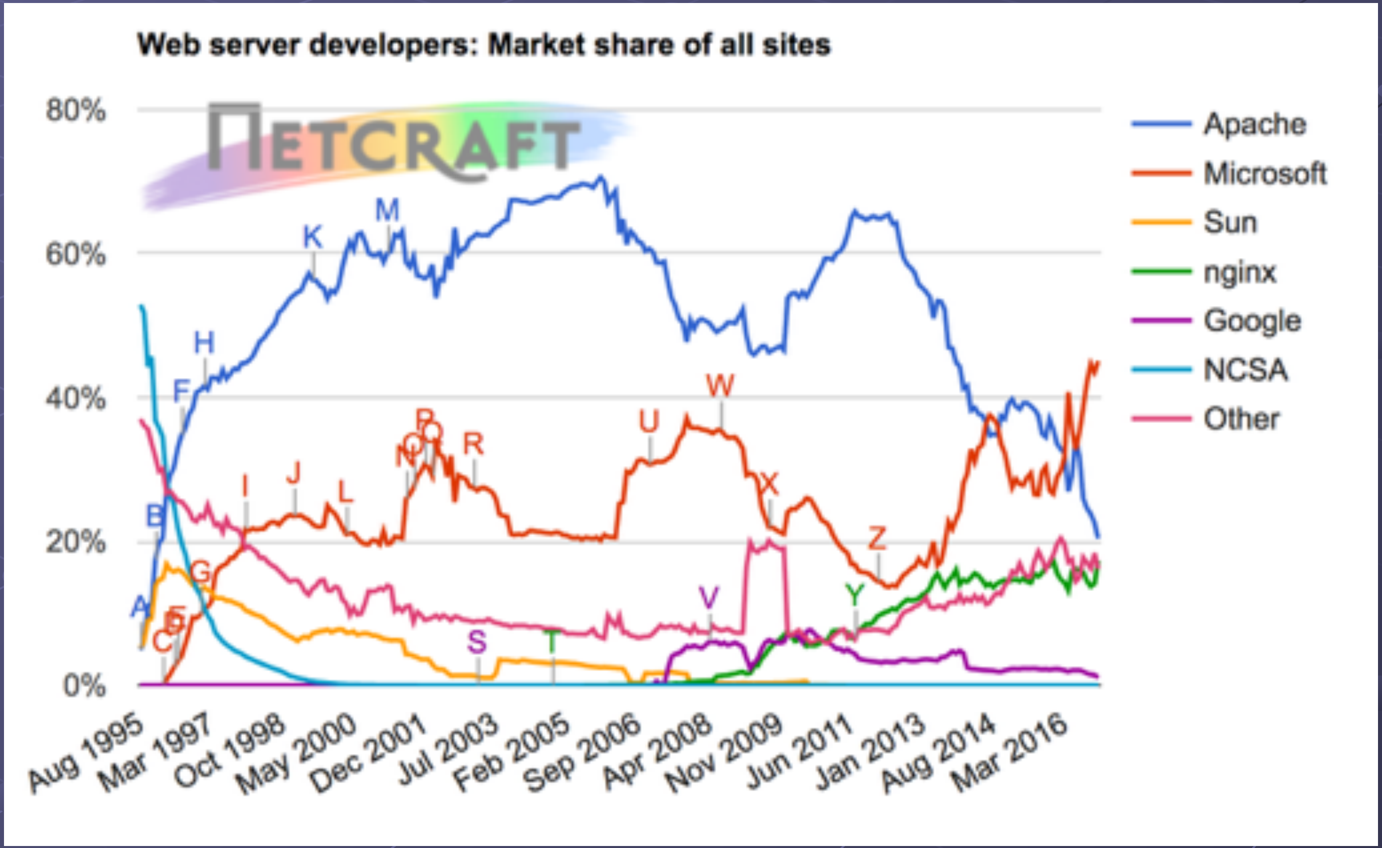
Objectives

- Describe Web applications
- Explain Web application vulnerabilities
- Describe the tools used to attack Web servers


Web Server
IIS or Apache
HTTP
HTTPS
Client’s Browser
Internet Explorer
or Firefox

Web Servers

- The two main Web servers are Apache (Open source) and IIS (Microsoft)
  - Link Ch 10c



Understanding Web Applications

- It is nearly impossible to write a program without bugs
  - Some bugs create security vulnerabilities
- Web applications also have bugs
  - Web applications have a larger user base than standalone applications
  - Bugs are a bigger problem for Web applications

Web Application Components

- Static Web pages
  - Created using HTML
- Dynamic Web pages
  - Need special components
    - <form> tags
    - Common Gateway Interface (CGI) scripts
    - Active Server Pages (ASP)
    - PHP
    - ColdFusion
    - Scripting languages like JavaScript
    - ODBC (Open Database connector)

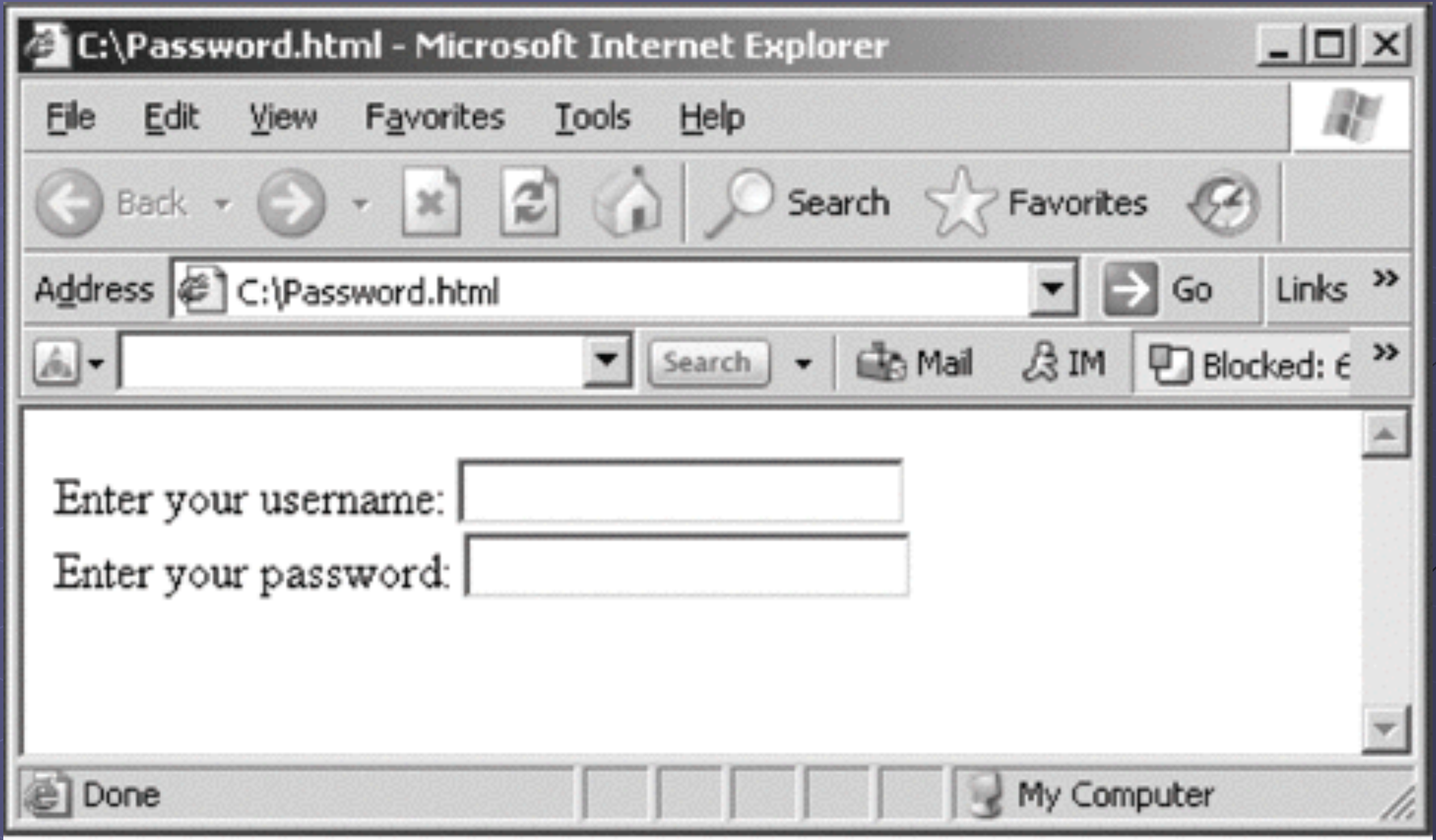
Web Forms

- Use the <form> element or tag in an HTML document
  - Allows customer to submit information to the Web server
- Web servers process information from a Web form by using a Web application
- Easy way for attackers to intercept data that users submit to a Web server

Web Forms (continued)

- Web form example

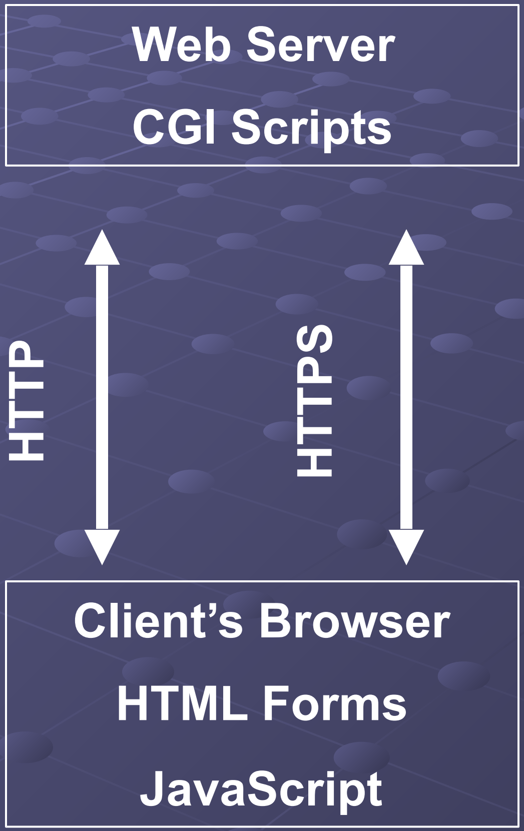
```
<html><body>
<form>
Enter your username:
<input type="text" name="username">
<br>
Enter your password:
<input type="text" name="password">
</form></body></html>
```


C:\Password.html - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Password.html Go Links
Search Mail IM Blocked: 6
Done
My Computer

Enter your username:

Enter your password:

Figure 10-1 An HTML Web page with a form


Web Server
CGI Scripts
HTTP
HTTPS
Client's Browser
HTML Forms
JavaScript

Common Gateway Interface (CGI)

- Handles moving data from a Web server to a Web browser
- The majority of dynamic Web pages are created with CGI and scripting languages
- Describes how a Web server passes data to a Web browser
  - Relies on Perl or another scripting language to create dynamic Web pages

CGI Languages

- CGI programs can be written in different programming and scripting languages
  - C or C++
  - Perl
  - Unix shell scripting
  - Visual Basic
  - FORTRAN

Common Gateway Interface (CGI) (continued)

- CGI example
  - Written in Perl
  - Hello.pl
  - Should be placed in the *cgi-bin* directory on the Web server

```
#!/usr/bin/perl
print "Content-type: text/html\n\n";
print "Hello Security Testers!";
```

Another CGI Example

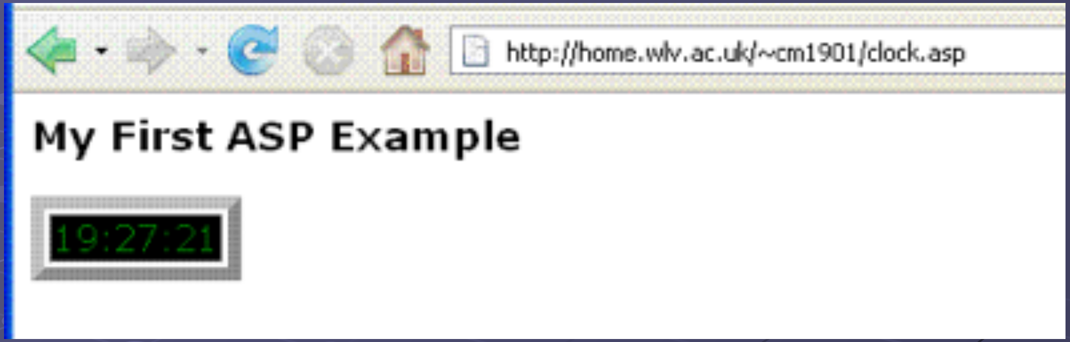
- Link Ch 10a: Sam’s Feedback Form
- Link Ch 10b alternate (at bottom of page): CGI Script in Perl that processes the data from the form

Active Server Pages (ASP)

- Microsoft’s server-side script engine
  - HTML pages are static—always the same
  - ASP creates HTML pages as needed. They are not static
- ASP uses scripting languages such as JScript or VBScript
- Not all Web servers support ASP
  - IIS supports ASP
  - Apache doesn’t support ASP as well

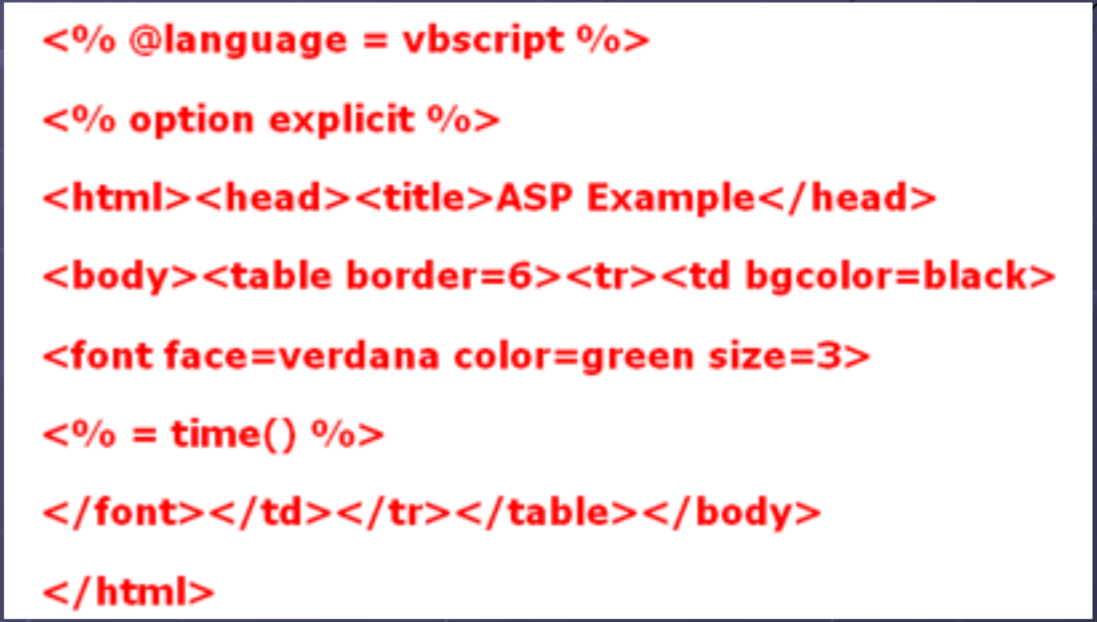
Active Server Pages (ASP)

- You can't see the source of an ASP page from a browser
- This makes it harder to hack into, although not impossible
- ASP examples at links
  Ch 10d, e, f


http://home.wlv.ac.uk/~cm1901/clock.asp

My First ASP Example

19:27:21


```
<% @language = vbscript %>
<% option explicit %>
<html><head><title>ASP Example</head>
<body><table border=6><tr><td bgcolor=black>
<font face=verdana color=green size=3>
<% = time() %>
</font></td></tr></table></body>
</html>
```

Apache Web Server

- Apache is the most popular Web Server program
- Advantages
  - Stable and reliable
  - Works on just about any *NIX and Windows platform
  - It is free and open source
    - See links Ch 10g, 10h

Using Scripting Languages

- Dynamic Web pages can be developed using scripting languages
  - VBScript
  - JavaScript
  - PHP

PHP: Hypertext Processor (PHP)

- Enables Web developers to create dynamic Web pages
  - Similar to ASP
- Open-source server-side scripting language
  - Can be embedded in an HTML Web page using PHP tags <?php and ?>
- Users cannot see PHP code in their Web browser
- Used primarily on UNIX systems
  - Also supported on Macintosh and Microsoft platforms

PHP Example

```
<html><head><title>Example</title></head>
<body>
<?php
echo 'Hello, World!';
?>
</body></html>
```

  - See links Ch 10k, 10l
- PHP has known vulnerabilities
  - See links Ch 10m, 10n
- PHP is often used with MySQL Databases

ColdFusion

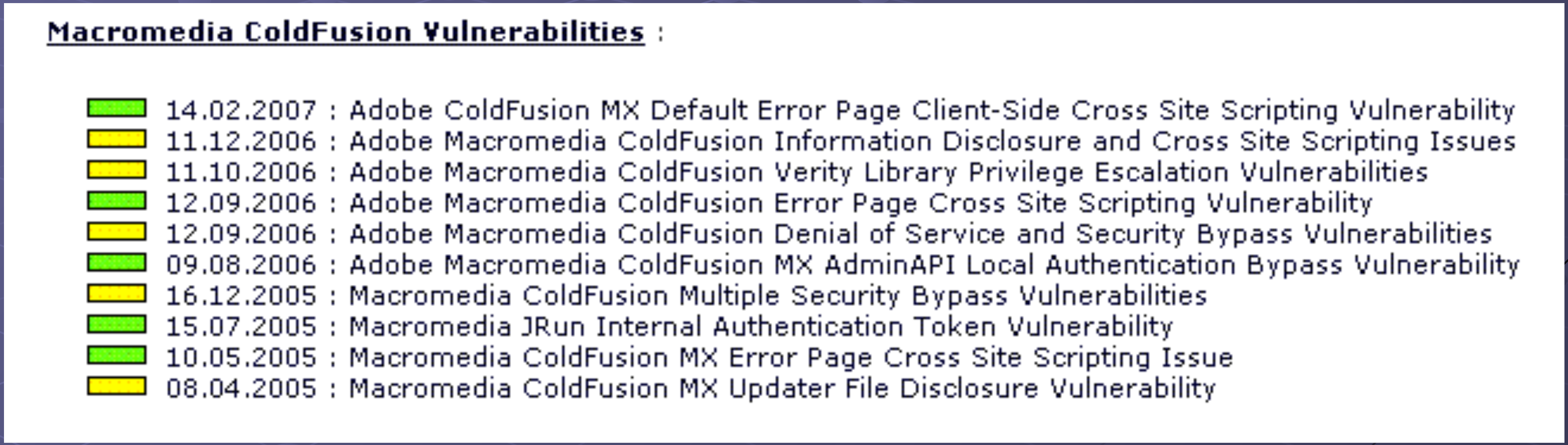
- Server-side scripting language used to develop dynamic Web pages
- Created by the Allaire Corporation
  - Purchased by Macromedia, now owned by Adobe -- Expensive
- Uses its own proprietary tags written in ColdFusion Markup Language (CFML)
- CFML Web applications can contain other technologies, such as HTML or JavaScript

ColdFusion Example

```
<html><head><title>Ex</title></head>
<body>
<CFLOCATION URL="www.isecom.org/cf/
  index.htm" ADDTOKEN="NO">
</body>
</html>
```

- See links Ch 10o

ColdFusion Vulnerabilities



Macromedia ColdFusion Vulnerabilities :

- 🟩 14.02.2007 : Adobe ColdFusion MX Default Error Page Client-Side Cross Site Scripting Vulnerability
- 🟨 11.12.2006 : Adobe Macromedia ColdFusion Information Disclosure and Cross Site Scripting Issues
- 🟨 11.10.2006 : Adobe Macromedia ColdFusion Verity Library Privilege Escalation Vulnerabilities
- 🟩 12.09.2006 : Adobe Macromedia ColdFusion Error Page Cross Site Scripting Vulnerability
- 🟨 12.09.2006 : Adobe Macromedia ColdFusion Denial of Service and Security Bypass Vulnerabilities
- 🟩 09.08.2006 : Adobe Macromedia ColdFusion MX AdminAPI Local Authentication Bypass Vulnerability
- 🟨 16.12.2005 : Macromedia ColdFusion Multiple Security Bypass Vulnerabilities
- 🟩 15.07.2005 : Macromedia JRun Internal Authentication Token Vulnerability
- 🟩 10.05.2005 : Macromedia ColdFusion MX Error Page Cross Site Scripting Issue
- 🟨 08.04.2005 : Macromedia ColdFusion MX Updater File Disclosure Vulnerability

- See links Ch 10p, 10q

VBScript

- Visual Basic Script is a scripting language developed by Microsoft
- You can insert VBScript commands into a static HTML page to make it dynamic
  - Provides the power of a full programming language
  - Executed by the client’s browser

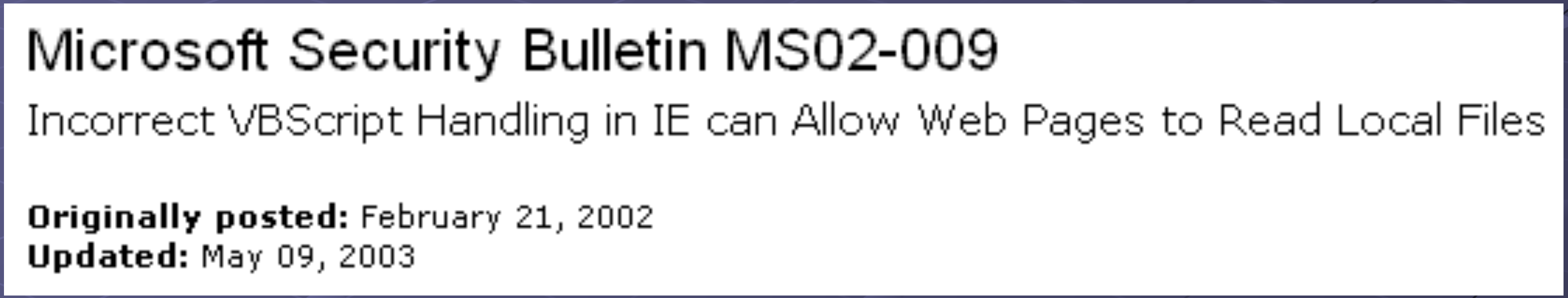
VBScript Example

```
<html><body>
<script type="text/vbscript">
document.write("<h1>Hello!</h1>")
document.write("Date Activated:  " &
  date())
</script>
</body></html>
```

- See link Ch 10r – works in IE, but not in Firefox
- Firefox does not support VBScript (link Ch 10s)

VBScript vulnerabilities

- See links Ch 10t, 10u



Microsoft Security Bulletin MS02-009

Incorrect VBScript Handling in IE can Allow Web Pages to Read Local Files

Originally posted: February 21, 2002
Updated: May 09, 2003

JavaScript

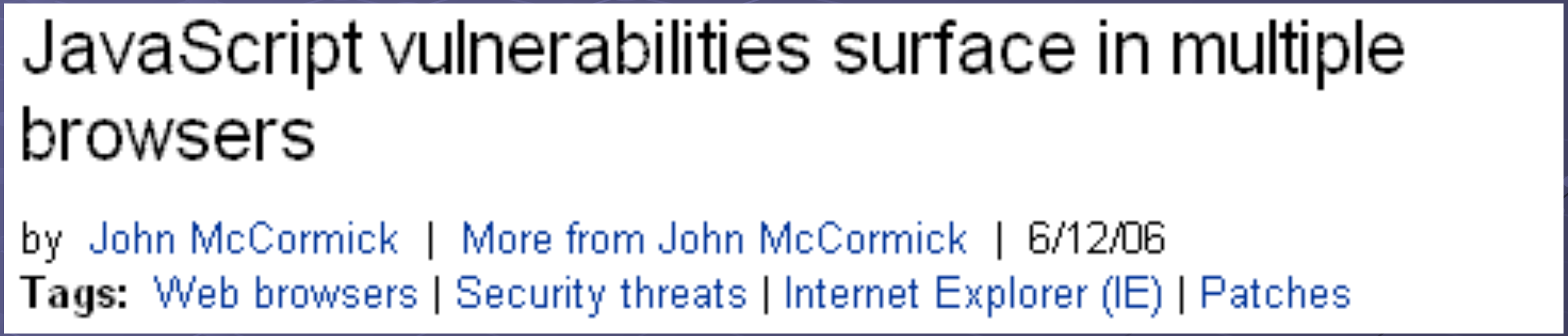
- Popular scripting language
- JavaScript also has the power of a programming language
  - Branching
  - Looping
  - Testing

JavaScript Example

```
<html><head>
<script type="text/javascript">
function chastise_user(){
alert("So, you like breaking rules?")
document.getElementById("cmdButton").focus(
  )}
</script></head>
<body><h3>Don't click the button!</h3>
<form>
<input type="button" value="Don't Click!"
  name="cmdButton"
  onClick="chastise_user()" />
</form></body></html>
```

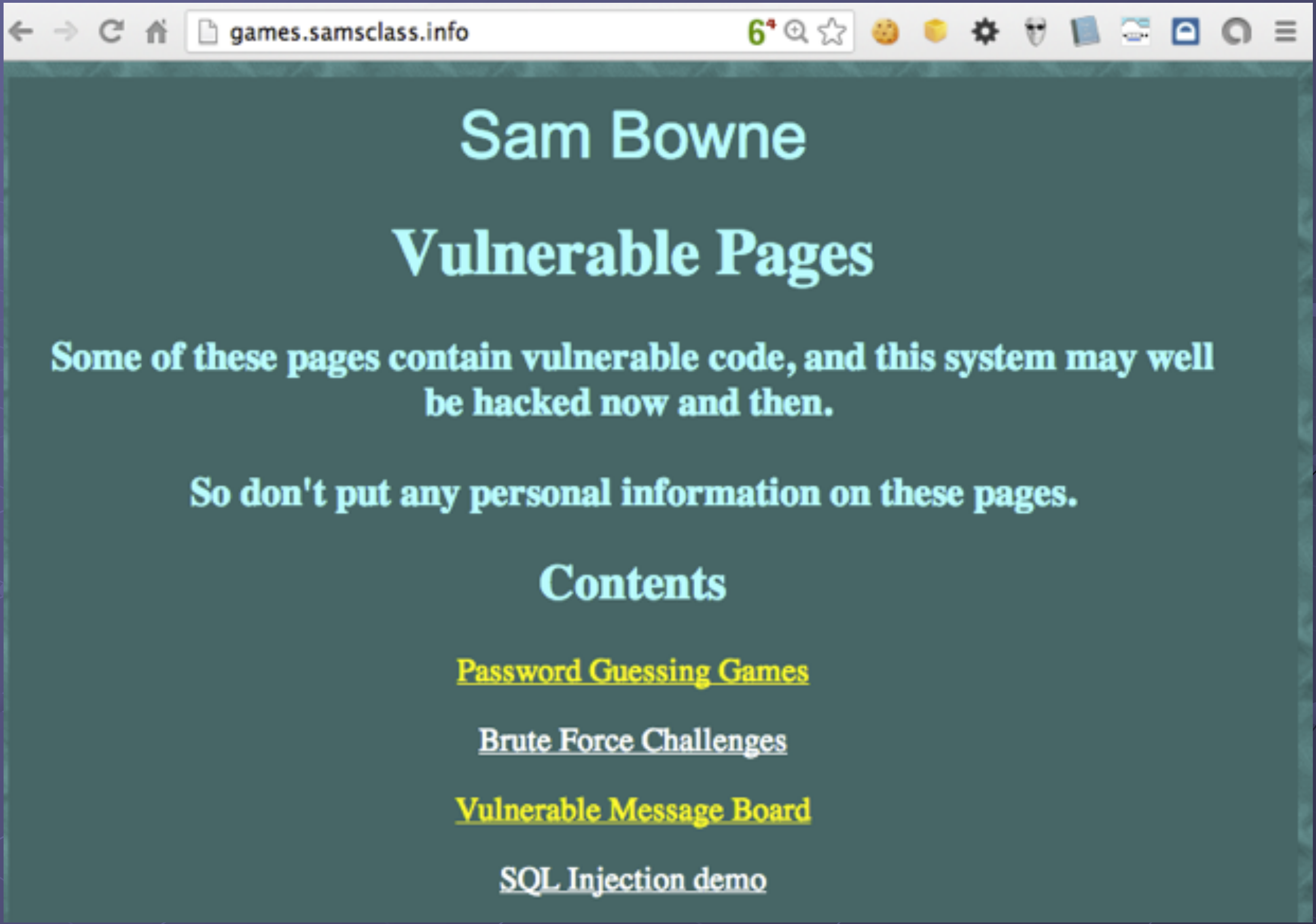
- See link Ch 10v – works in IE and Firefox

JavaScript Vulnerabilities


JavaScript vulnerabilities surface in multiple browsers

by John McCormick | More from John McCormick | 6/12/06
Tags: Web browsers | Security threats | Internet Explorer (IE) | Patches

- See link Ch 10w


games.samsclass.info

Sam Bowne

Vulnerable Pages

Some of these pages contain vulnerable code, and this system may well be hacked now and then.

So don't put any personal information on these pages.

Contents

Password Guessing Games

Brute Force Challenges

Vulnerable Message Board

SQL Injection demo

Web Server

Apache or IIS

HTML Forms

CGI Scripts

ODBC or

OLE DB

Or ADO

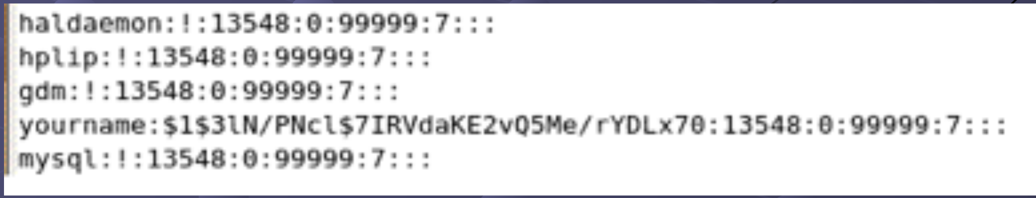
Database

SQL Server or

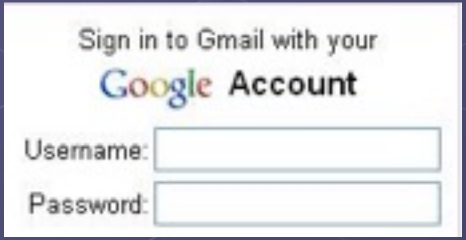
Oracle or

MySQL

HTTP or HTTPS



```
haldaemon:!:13548:0:99999:7:::
hplip:!:13548:0:99999:7:::
gdm:!:13548:0:99999:7:::
yourname:$1$3lN/PNcl$7IRVdaKE2vQ5Me/rYDLx70:13548:0:99999:7:::
mysql:!:13548:0:99999:7:::
```



Sign in to Gmail with your

Google Account

Username:

Password:

Client's Browser

Connecting to Databases

- Web pages can display information stored on databases
- There are several technologies used to connect databases with Web applications
  - Technology depends on the OS used
    - ODBC
    - OLE DB
    - ADO
  - Theory is the same

Open Database Connectivity (ODBC)

- Standard database access method developed by the SQL Access Group
- ODBC interface allows an application to access
  - Data stored in a database management system (DBMS)
  - Can use Oracle, SQL, or any DBMS that understands and can issue ODBC commands
- Interoperability among back-end DBMS is a key feature of the ODBC interface

Open Database Connectivity (ODBC) (continued)

- ODBC defines
  - Standardized representation of data types
  - A library of ODBC functions
  - Standard methods of connecting to and logging on to a DBMS

OLE DB and ADO

- Object Linking and Embedding Database (OLE DB) and
- ActiveX Data Objects (ADO)
  - These two more modern, complex technologies replace ODBC and make up"Microsoft’s Universal Data Access“
  - See link Ch 10x

Understanding Web Application Vulnerabilities

- Many platforms and programming languages can be used to design a Web site
- Application security is as important as network security

Attackers controlling a Web server can

- Deface the Web site
- Destroy or steal company's data
- Gain control of user accounts
- Perform secondary attacks from the Web site
- Gain root access to other applications or servers

Open Web Application Security Project (OWASP)

- Open, not-for-profit organization dedicated to finding and fighting vulnerabilities in Web applications
- Publishes the Ten Most Critical Web Application Security Vulnerabilities

Top-10 Web application vulnerabilities

- Cross-site scripting (XSS) flaws
  - Attackers inject code into a web page, such as a forum or guestbook
  - When others user view the page, confidential information is stolen
  - See link Ch 10za
- Command injection flaws
  - An attacker can embed malicious code and run a program on the database server
  - Example: SQL Injection

Top-10 Web application vulnerabilities

- Malicious file execution
  - Users allowed to upload or run malicious files
- Unsecured Direct Object Reference
  - Information in the URL allows a user to reference files, directories, or records
- Cross-site Request Forgery (CSRF)
  - Stealing an authenticated session, by replaying a cookie or other token

Top-10 Web application vulnerabilities

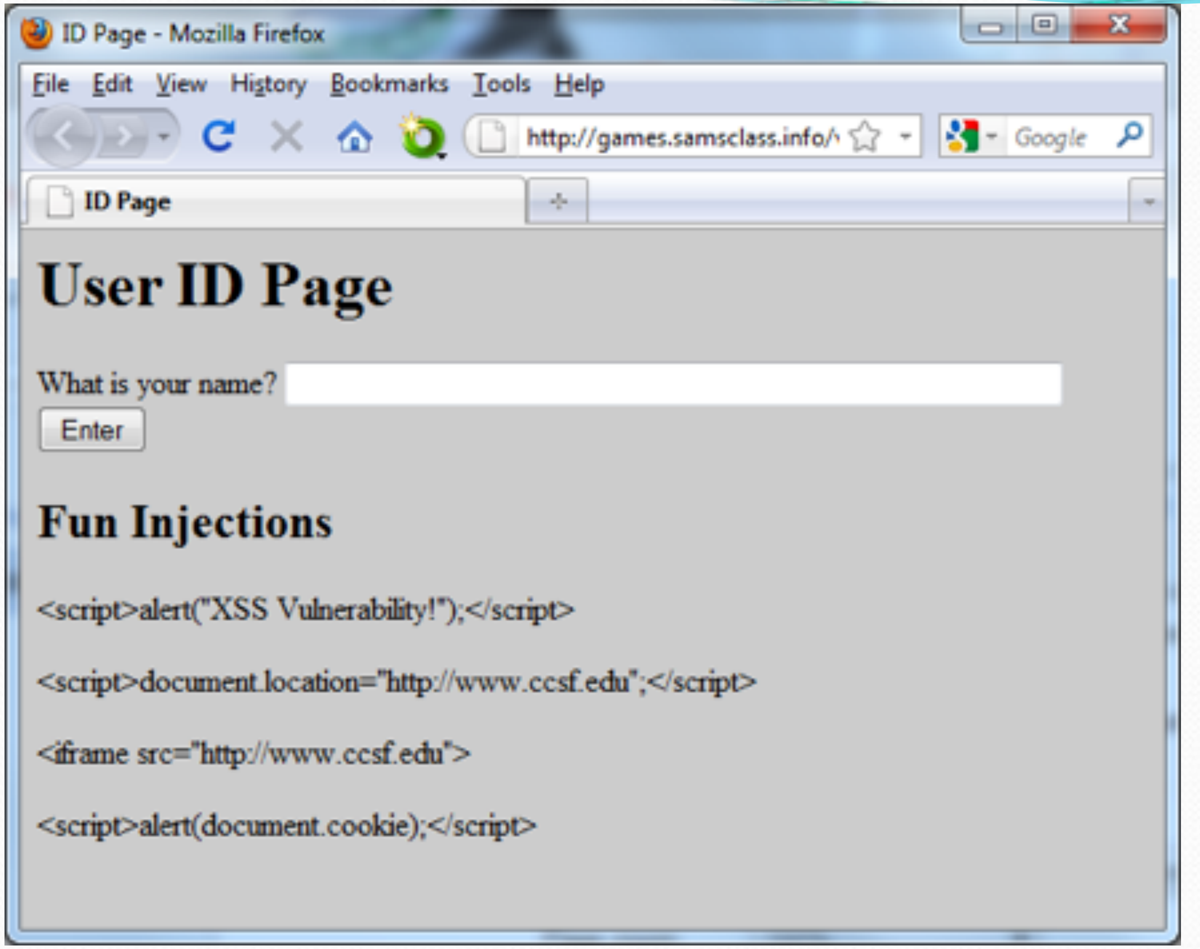
- Information Leakage and Incorrect Error Handling
  - Error messages that give away too much information
- Broken Authentication and Session Management
  - Allow attackers to steal cookies or passwords

Top-10 Web application vulnerabilities

- Unsecured cryptographic Storage
  - Storing keys, certificates, and passwords on a Web server can be dangerous
- Unsecured Communication
  - Using HTTP instead of HTTPS
- Failure to Restrict URL Access
  - Security through obscurity
  - Hoping users don't find the "secret" URLs

Cross-Site Scripting (XSS)

- One client posts active content, with <script> tags or other programming content
- When another client reads the messages, the scripts are executed in his or her browser
- One user attacks another user, using the vulnerable Web application as a weapon


ID Page - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://games.samsclass.info/
Google
ID Page

User ID Page

What is your name?

Enter

Fun Injections

<script>alert("XSS Vulnerability!");</script>

<script>document.location="http://www.ccsf.edu";</script>

<iframe src="http://www.ccsf.edu">

<script>alert(document.cookie);</script>

- <script>alert("XSS vulnerability!")</script>
- <script>alert(document.cookie)</script>
- <script>window.location="http://www.ccsf.edu"</script>

XSS Scripting Effects

- Steal another user's authentication cookie
  - Hijack session
- Harvest stored passwords from the target's browser
- Take over machine through browser vulnerability
- Redirect Webpage
- Many, many other evil things…

Application Vulnerabilities Countermeasures (continued)

- WebGoat project
  - Helps security testers learn how to perform vulnerabilities testing on Web applications
  - Developed by OWASP
- It’s excellent, and now has video tutorials

Assessing Web Applications

- Issues to consider
  - Dynamic Web pages
  - Connection to a backend database server
  - User authentication
  - What platform was used?

Does the Web Application Use Dynamic Web Pages?

- Static Web pages do not create a secure environment
- IIS attack example: Directory Traversal
  - Adding ..\ to a URL refers to a directory above the Web page directory
  - Early versions of IIS filtered out \, but not %c1%9c, which is a Unicode version of the same character
  - See link Ch 10 zh

Connection to a Backend Database Server

- Security testers should check for the possibility of SQL injection being used to attack the system
- SQL injection involves the attacker supplying SQL commands on a Web application field

SQL Injection Example

- HTML form collects *name* and *pw*
- SQL then uses those fields:

```
SELECT * FROM customer
WHERE username = 'name' AND password = 'pw'
```

- If a hacker enters a name of

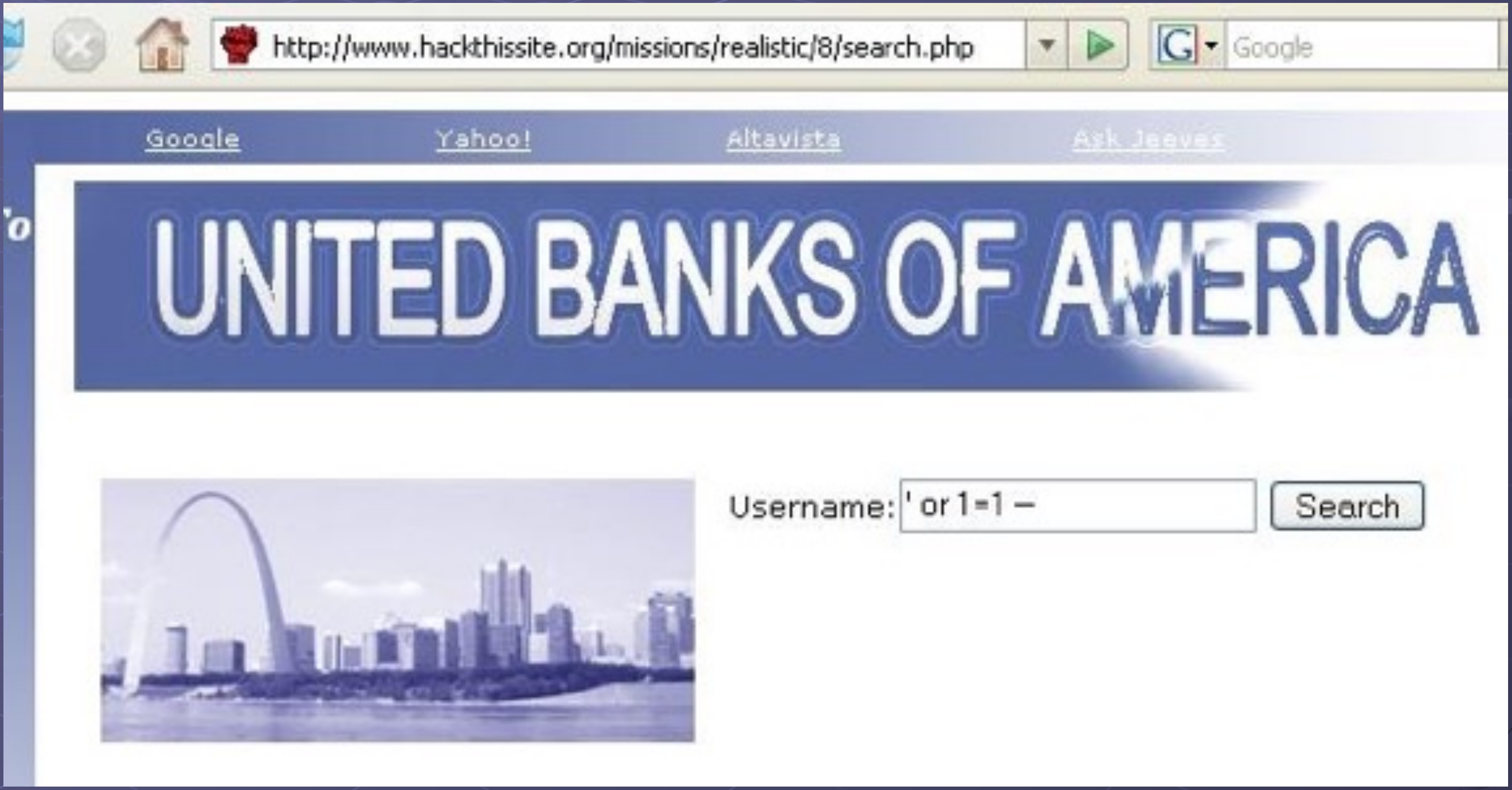
' OR 1=1 --

- The SQL becomes:

```
SELECT * FROM customer
WHERE username ='' OR 1=1 --' AND password =
  'pw'
```

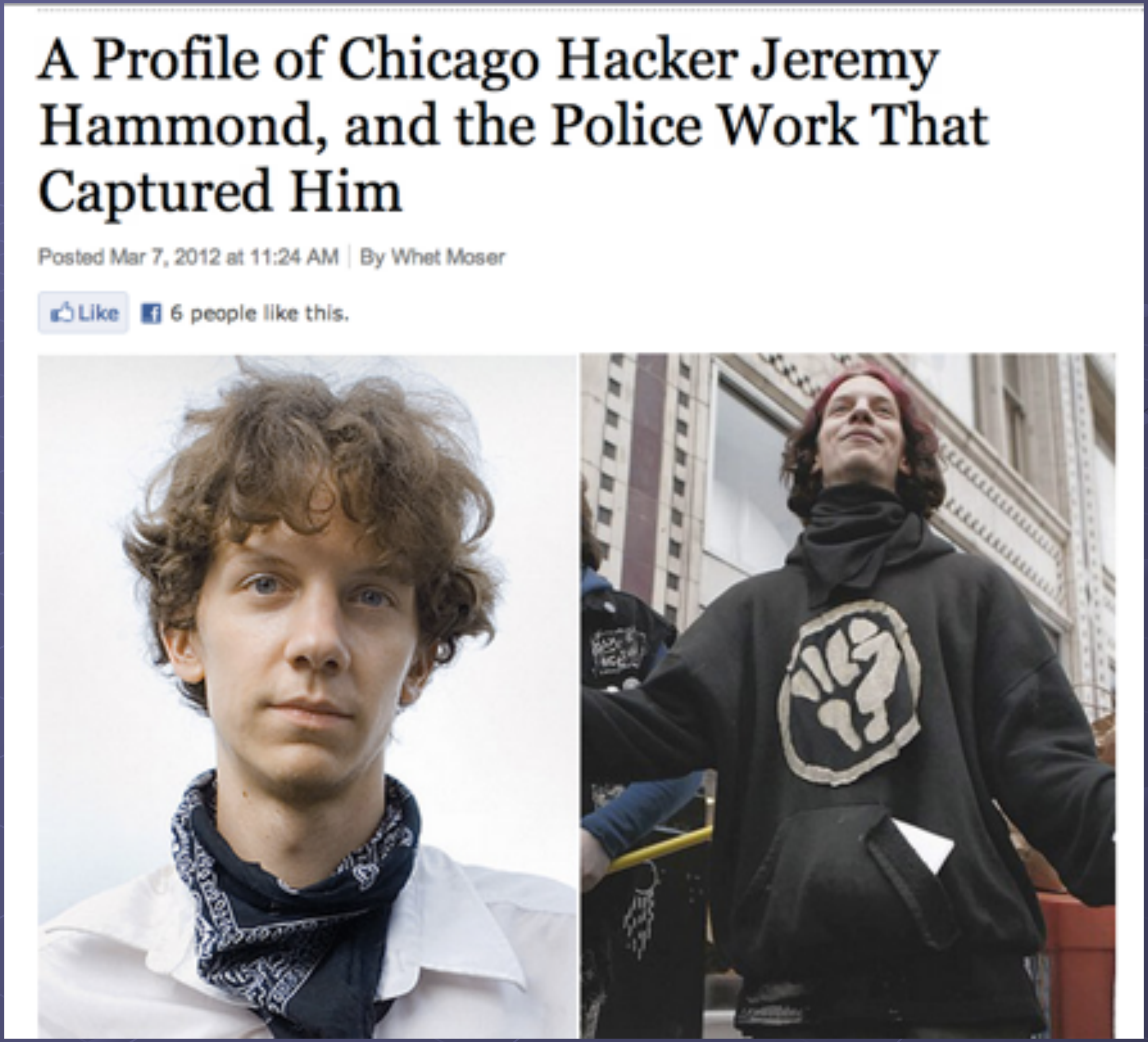
- Which is always true, and returns all the records

HackThisSite



http://www.hackthissite.org/missions/realistic/8/search.php

Username: ' or 1=1 --



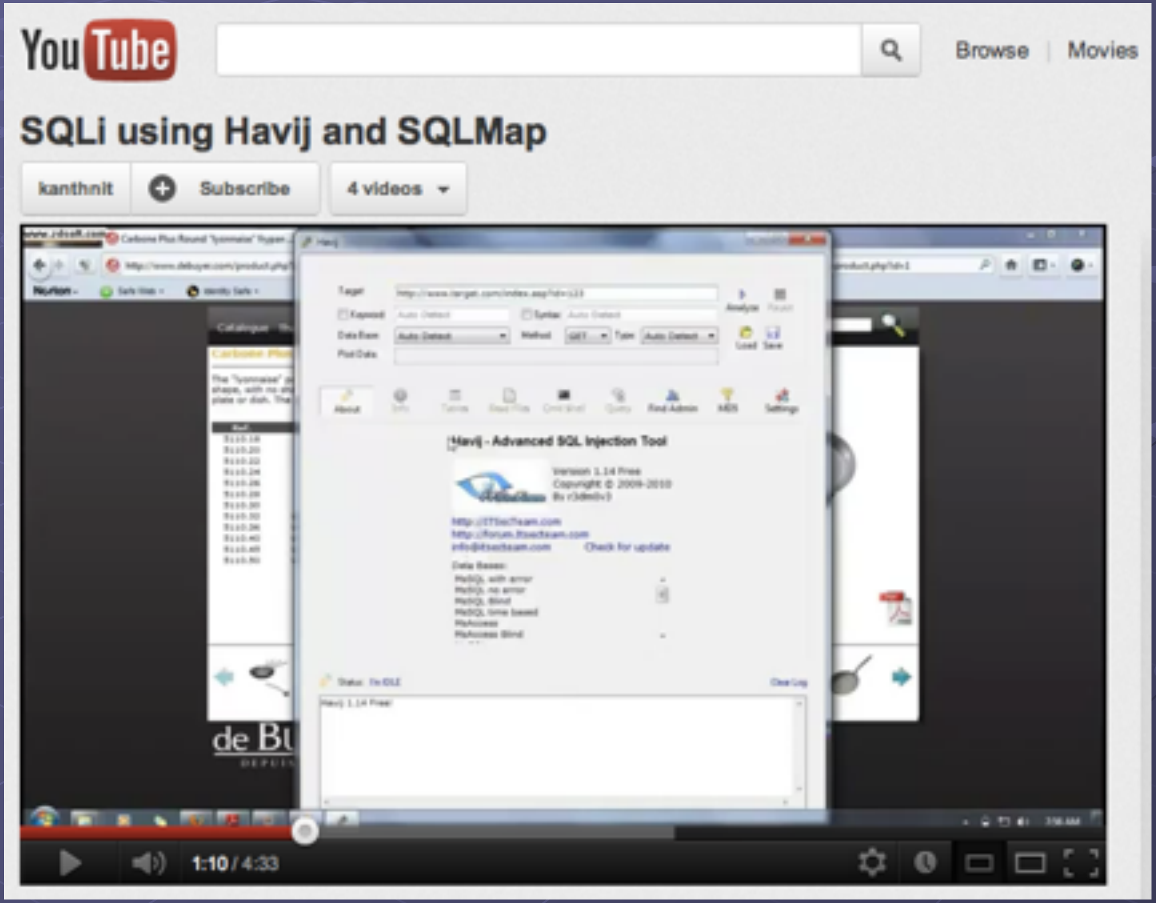
A Profile of Chicago Hacker Jeremy Hammond, and the Police Work That Captured Him

Posted Mar 7, 2012 at 11:24 AM | By Whet Moser

Like 6 people like this.

- Link Ch 10zr

Havij & SQLmap


YouTube
Browse
Movies
SQLi using Havij and SQLMap
kanthnit
Subscribe
4 videos
Havij - Advanced SQL Injection Tool
1:10 / 4:33

- Link Ch 10zq

Connection to a Backend Database Server

- Basic testing should look for
  - Whether you can enter text with punctuation marks
  - Whether you can enter a single quotation mark followed by any SQL keywords
  - Whether you can get any sort of database error when attempting to inject SQL

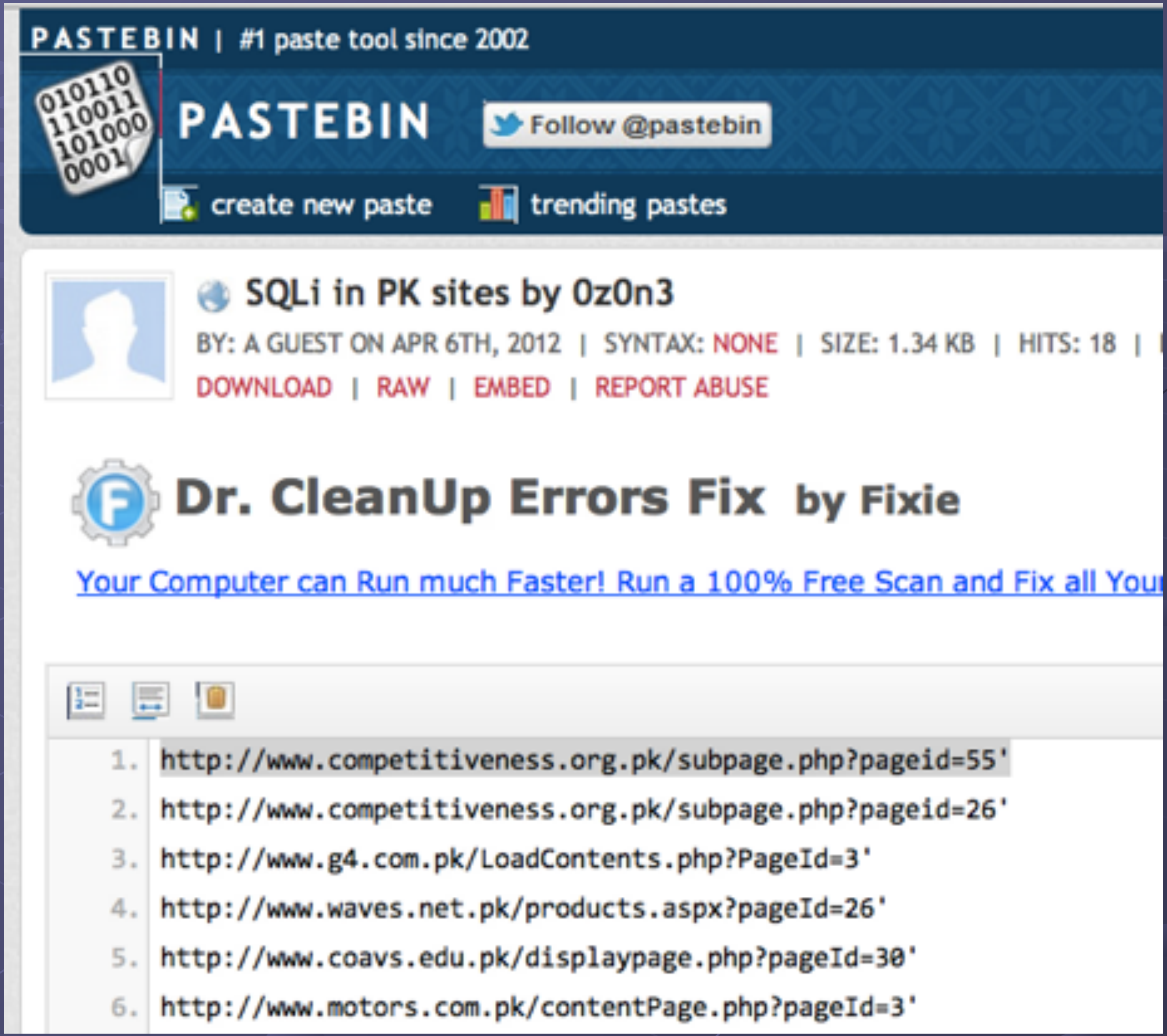
User Authentication

- Many Web applications require another server to authenticate users
- Examine how information is passed between the two servers
  - Encrypted channels
- Verify that logon and password information is stored on secure places
- Authentication servers introduce a second target

What Platform Was Used?

- Popular platforms include:
  - IIS with ASP and SQL Server (Microsoft)
  - Linux, Apache, MySQL, and PHP (LAMP)
- Footprinting is used to find out the platform
  - The more you know about a system the easier it is to gather information about its vulnerabilities

SQLI on Pastebin



SQLi in PK sites by 0z0n3

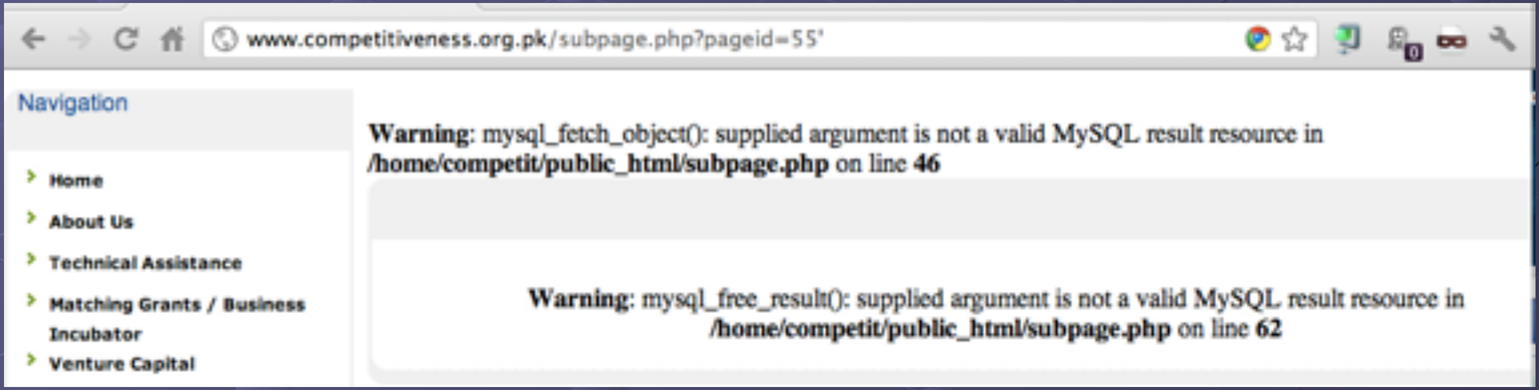
BY: A GUEST ON APR 6TH, 2012 | SYNTAX: NONE | SIZE: 1.34 KB | HITS: 18 |

DOWNLOAD | RAW | EMBED | REPORT ABUSE

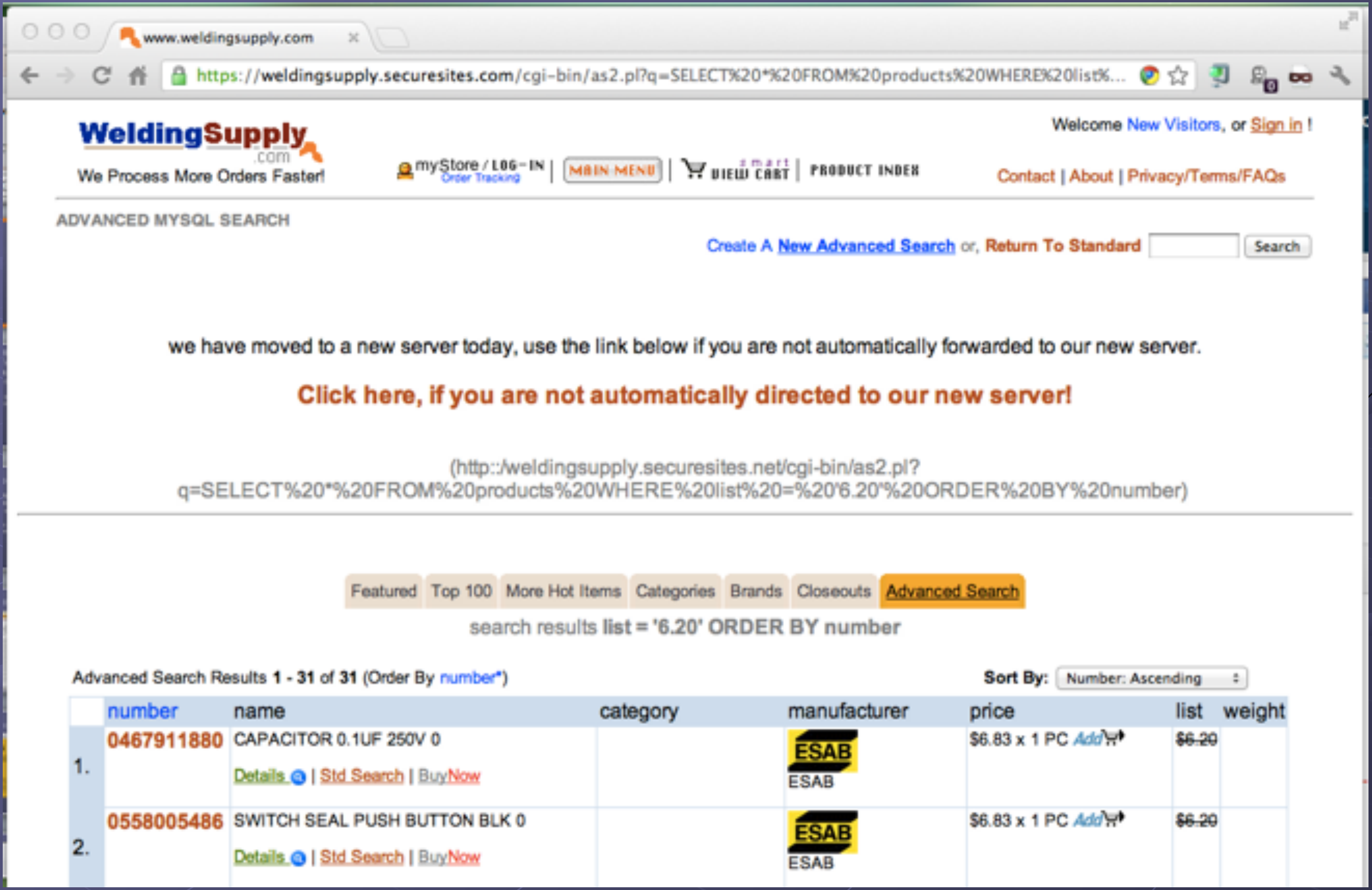
Dr. CleanUp Errors Fix by Fixie

Your Computer can Run much Faster! Run a 100% Free Scan and Fix all You

```
http://www.competitiveness.org.pk/subpage.php?pageid=55'
http://www.competitiveness.org.pk/subpage.php?pageid=26'
http://www.g4.com.pk/LoadContents.php?PageId=3'
http://www.waves.net.pk/products.aspx?pageId=26'
http://www.coavs.edu.pk/displaypage.php?pageId=30'
http://www.motors.com.pk/contentPage.php?pageId=3'
```


www.competitiveness.org.pk/subpage.php?pageid=55'

```
Warning: mysql_fetch_object(): supplied argument is not a valid MySQL result resource in
/home/competit/public_html/subpage.php on line 46

Warning: mysql_free_result(): supplied argument is not a valid MySQL result resource in
/home/competit/public_html/subpage.php on line 62
```


www.weldingsupply.com
https://weldingsupply.securesites.com/cgi-bin/as2.pl?q=SELECT%20*%20FROM%20products%20WHERE%20list%...
WeldingSupply.com
We Process More Orders Faster!
myStore / LOG-IN
Order Tracking
MAIN MENU
smart VIEW CART
PRODUCT INDEX
Welcome New Visitors, or Sign in !
Contact | About | Privacy/Terms/FAQs
Create A New Advanced Search or, Return To Standard
Search
Featured
Top 100
More Hot Items
Categories
Brands
Closeouts
Advanced Search
Sort By:
Number: Ascending

ADVANCED MYSQL SEARCH

we have moved to a new server today, use the link below if you are not automatically forwarded to our new server.

Click here, if you are not automatically directed to our new server!

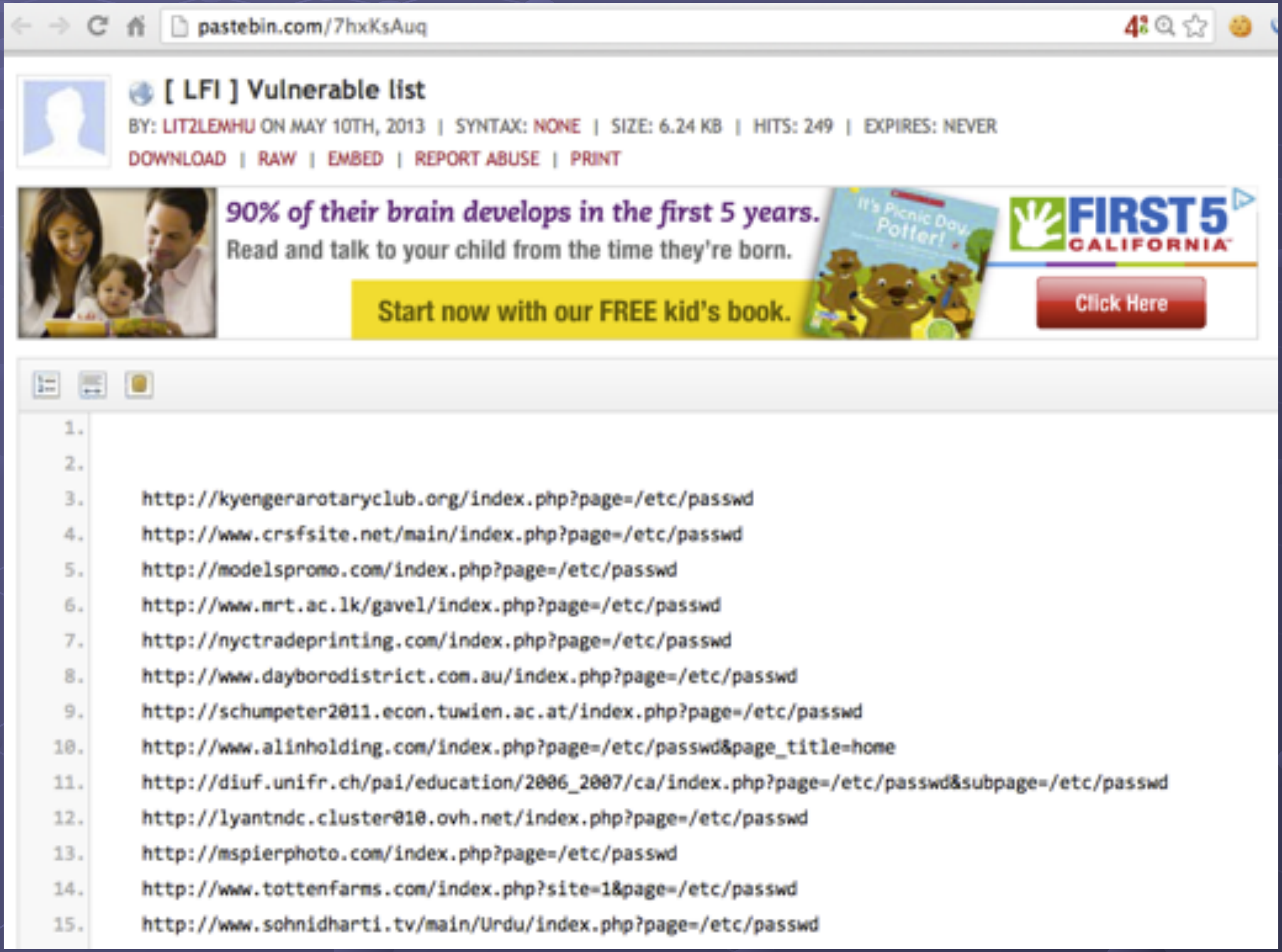
(http::/weldingsupply.securesites.net/cgi-bin/as2.pl?q=SELECT%20*%20FROM%20products%20WHERE%20list%20=%20'6.20'%20ORDER%20BY%20number)

search results **list = '6.20' ORDER BY number**

Advanced Search Results **1 - 31** of **31** (Order By number*)

	number	name	category	manufacturer	price	list	weight
1.	0467911880	CAPACITOR 0.1UF 250V 0 Details | Std Search | BuyNow		ESAB	$6.83 x 1 PC Add	~~$6.20~~	
2.	0558005486	SWITCH SEAL PUSH BUTTON BLK 0 Details | Std Search | BuyNow		ESAB	$6.83 x 1 PC Add	~~$6.20~~	

Local File Inclusion


pastebin.com/7hxKsAuq

[LFI] Vulnerable list

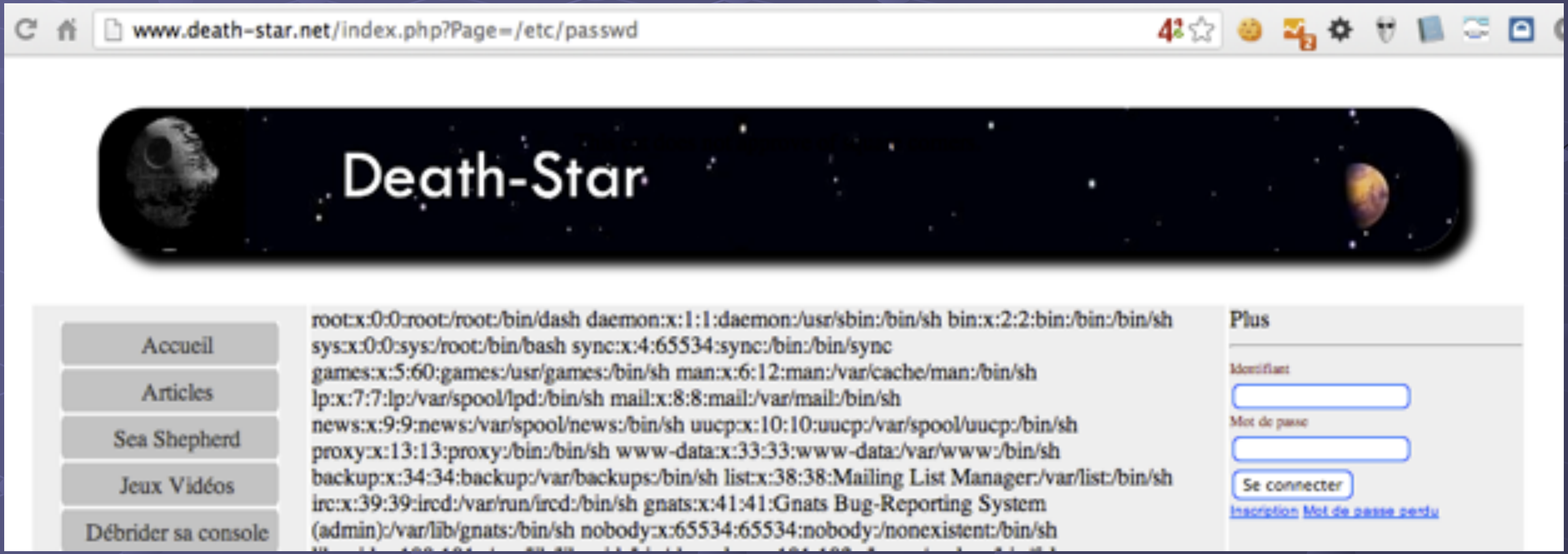
BY: LIT2LEMHU ON MAY 10TH, 2013 | SYNTAX: NONE | SIZE: 6.24 KB | HITS: 249 | EXPIRES: NEVER

DOWNLOAD | RAW | EMBED | REPORT ABUSE | PRINT

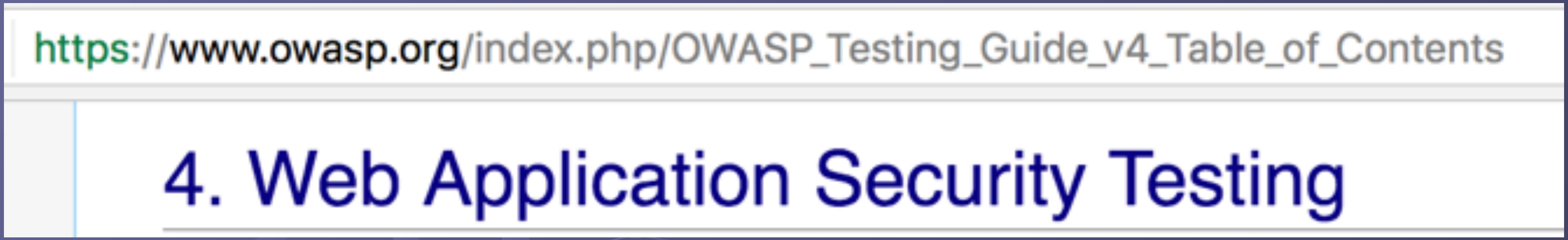
90% of their brain develops in the first 5 years.
Read and talk to your child from the time they're born.
Start now with our FREE kid's book.
FIRST 5 CALIFORNIA
Click Here

```
http://kyengerarotaryclub.org/index.php?page=/etc/passwd
http://www.crsfsite.net/main/index.php?page=/etc/passwd
http://modelspromo.com/index.php?page=/etc/passwd
http://www.mrt.ac.lk/gavel/index.php?page=/etc/passwd
http://nyctradeprinting.com/index.php?page=/etc/passwd
http://www.dayborodistrict.com.au/index.php?page=/etc/passwd
http://schumpeter2011.econ.tuwien.ac.at/index.php?page=/etc/passwd
http://www.alinholding.com/index.php?page=/etc/passwd&page_title=home
http://diuf.unifr.ch/pai/education/2006_2007/ca/index.php?page=/etc/passwd&subpage=/etc/passwd
http://lyantndc.cluster010.ovh.net/index.php?page=/etc/passwd
http://mspierphoto.com/index.php?page=/etc/passwd
http://www.tottenfarms.com/index.php?site=1&page=/etc/passwd
http://www.sohnidharti.tv/main/Urdu/index.php?page=/etc/passwd
```

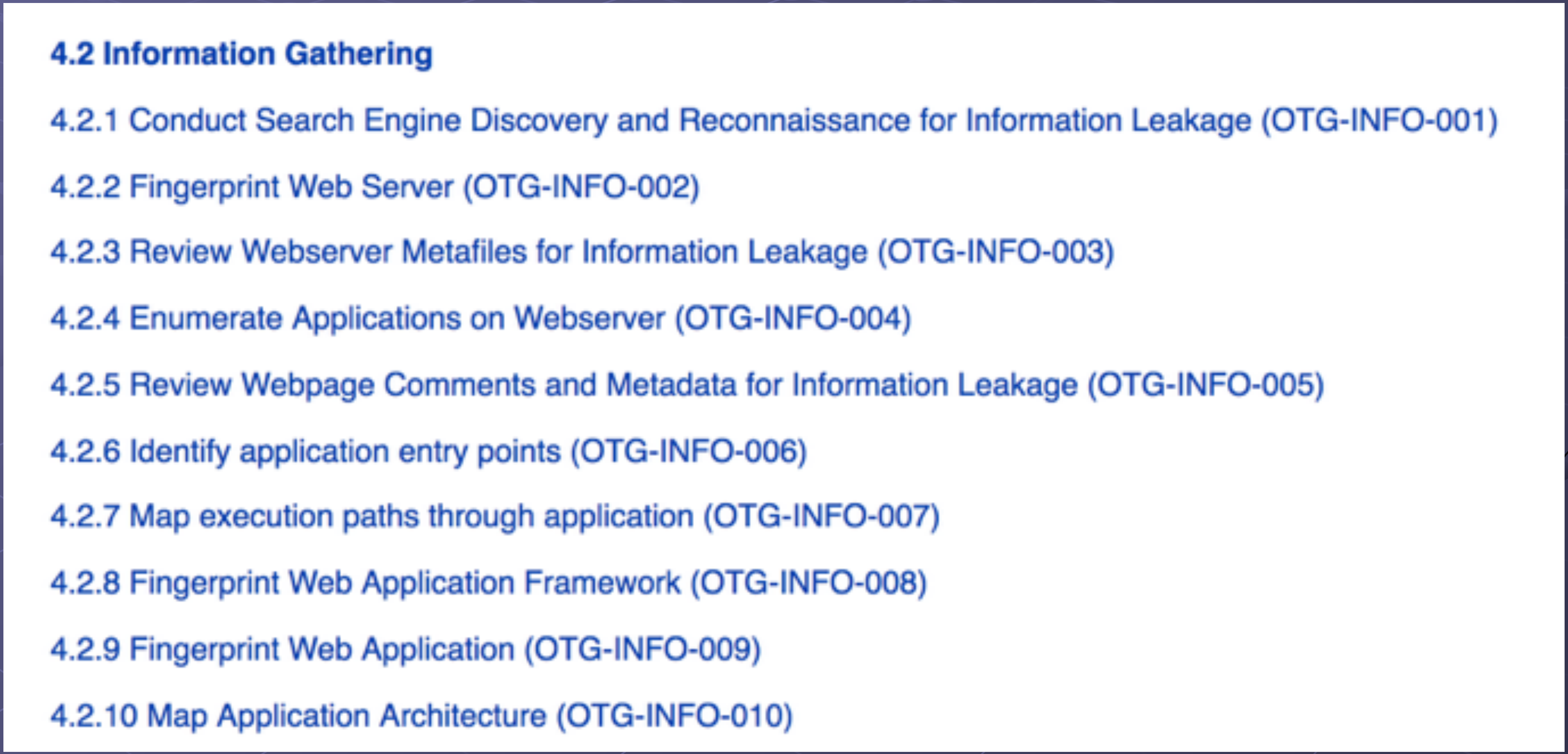
LFI Example

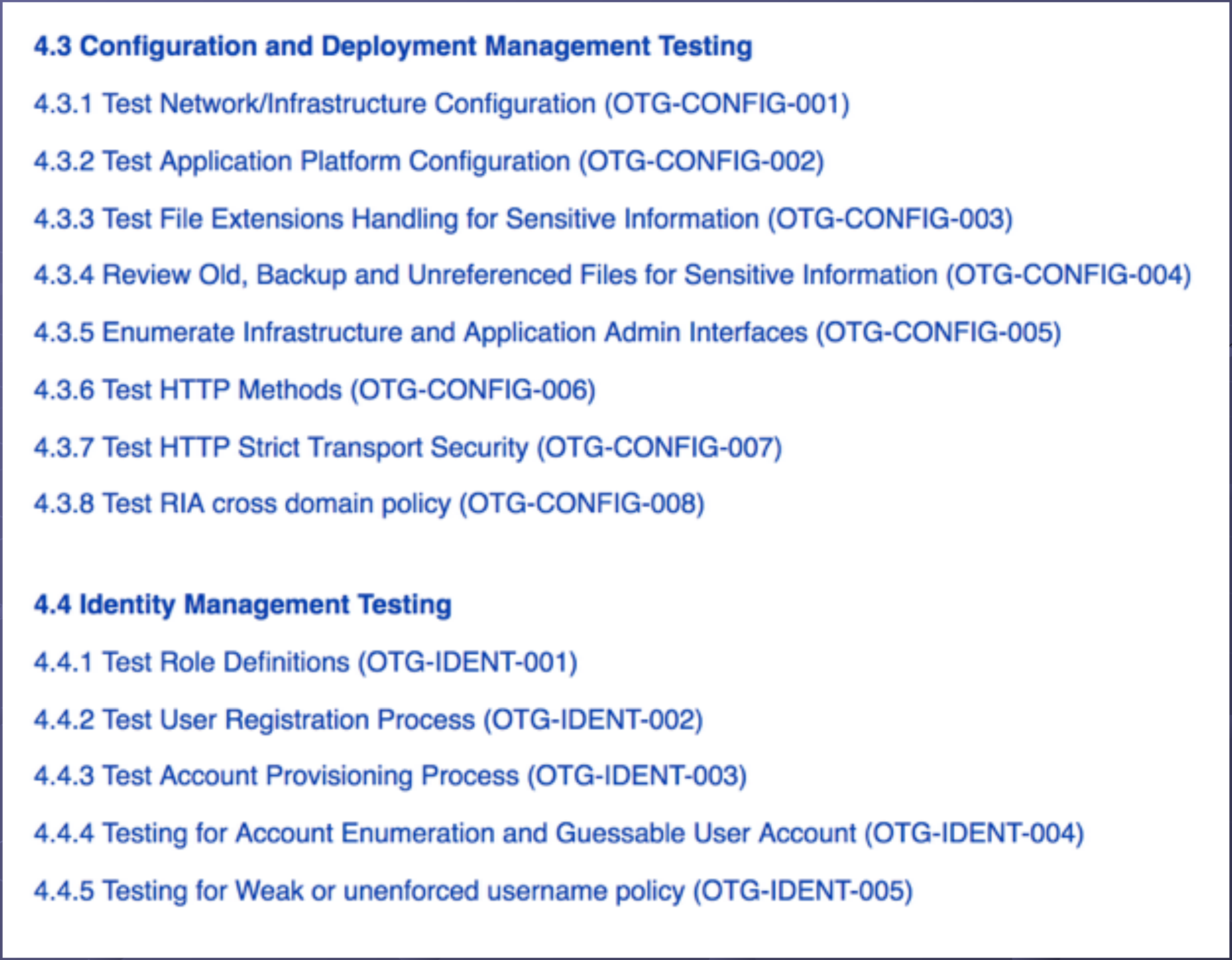


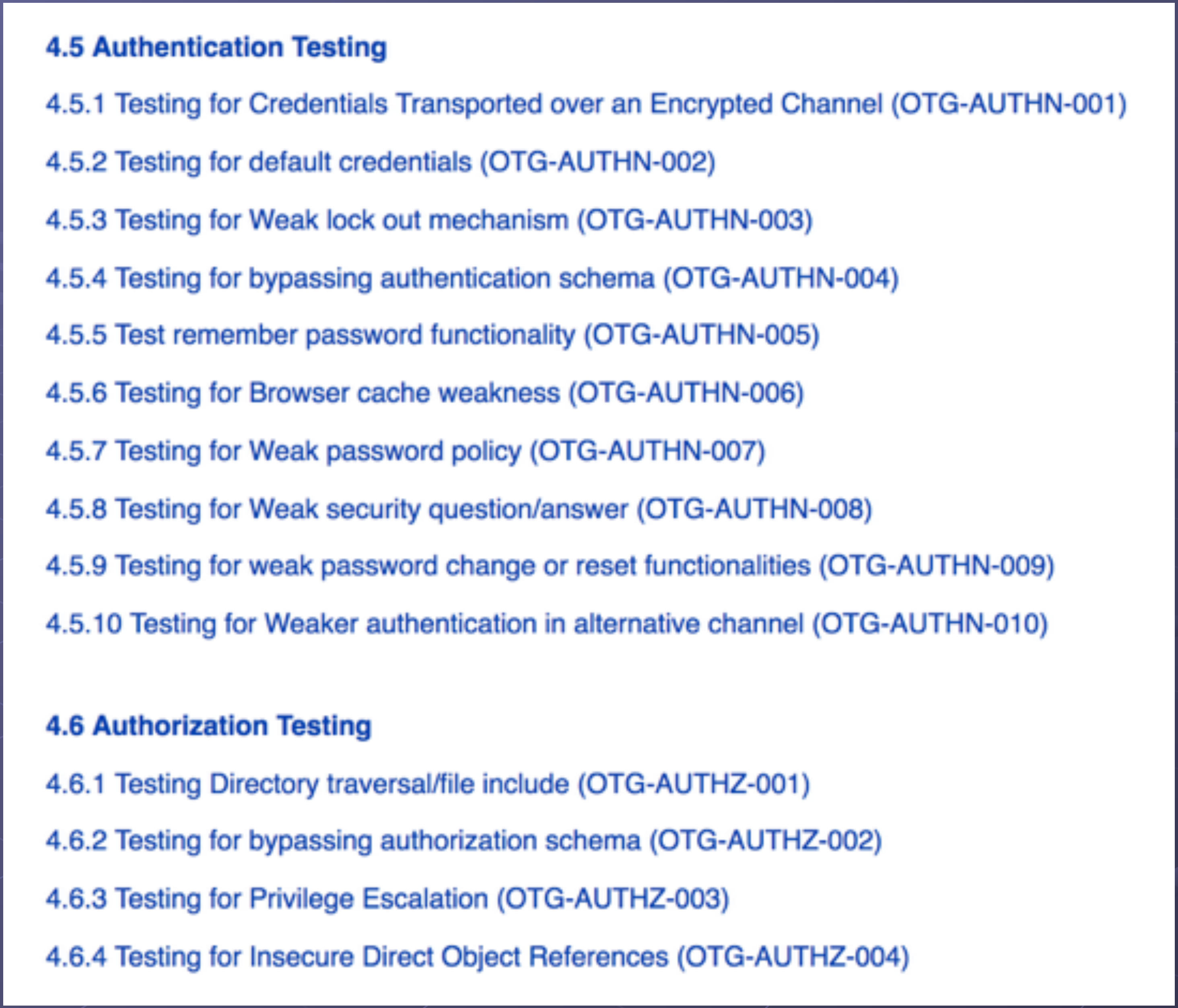
```
root:x:0:0:root:/root:/bin/dash daemon:x:1:1:daemon:/usr/sbin:/bin/sh bin:x:2:2:bin:/bin:/bin/sh
sys:x:0:0:sys:/root:/bin/bash sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/bin/sh nobody:x:65534:65534:nobody:/nonexistent:/bin/sh
```

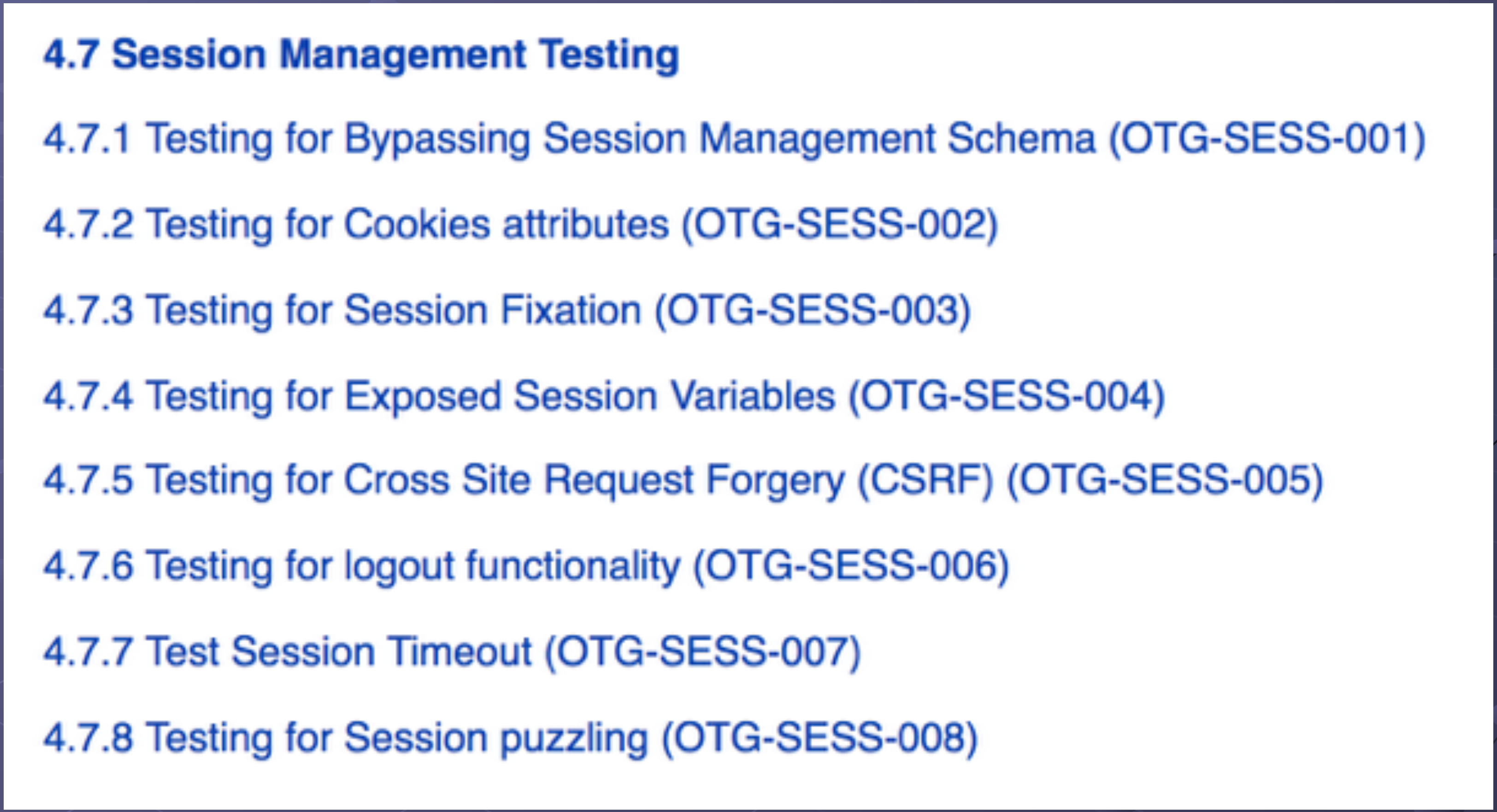

https://www.owasp.org/index.php/OWASP_Testing_Guide_v4_Table_of_Contents

4. Web Application Security Testing









4.7 Session Management Testing

4.7.1 Testing for Bypassing Session Management Schema (OTG-SESS-001)

4.7.2 Testing for Cookies attributes (OTG-SESS-002)

4.7.3 Testing for Session Fixation (OTG-SESS-003)

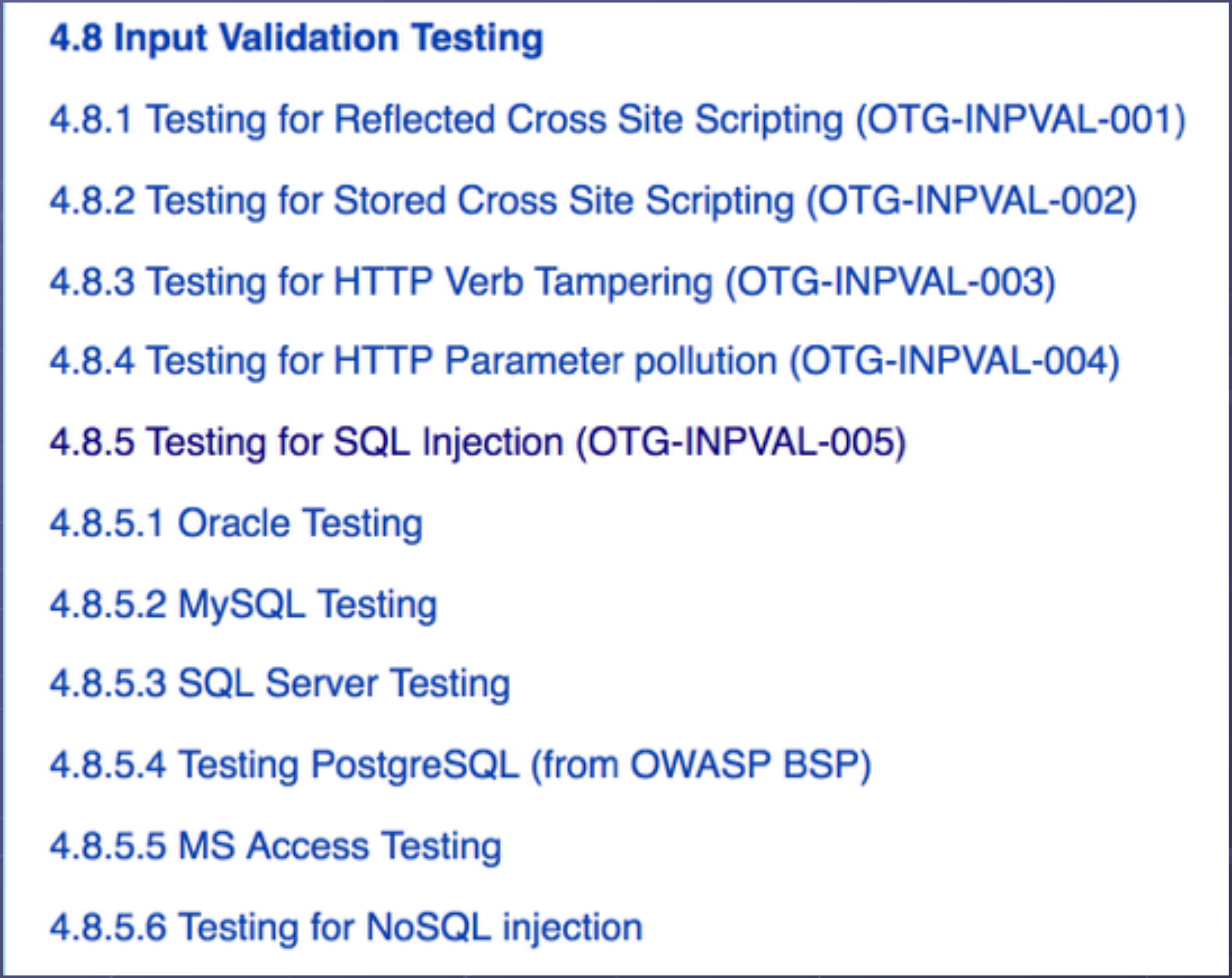
4.7.4 Testing for Exposed Session Variables (OTG-SESS-004)

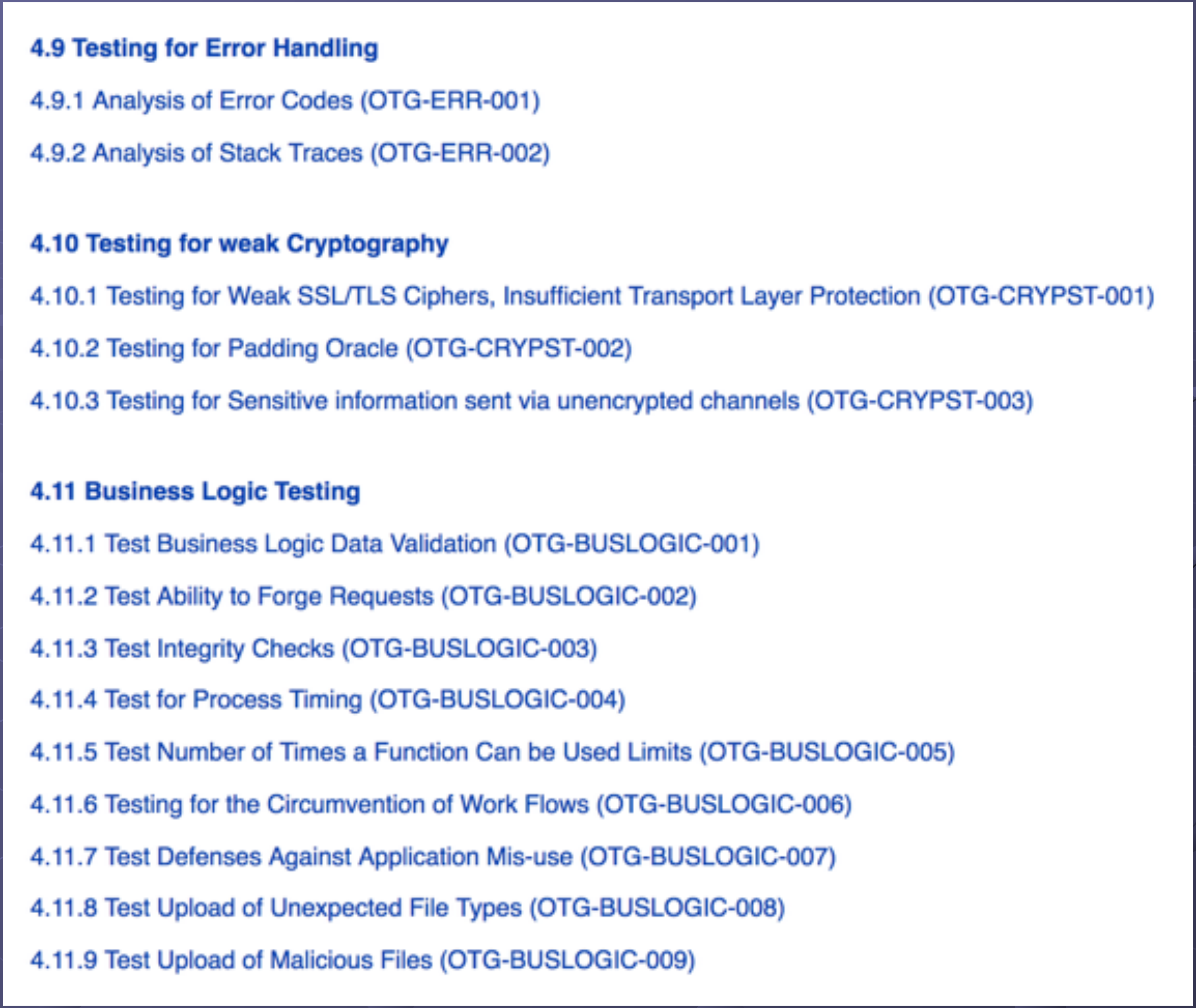
4.7.5 Testing for Cross Site Request Forgery (CSRF) (OTG-SESS-005)

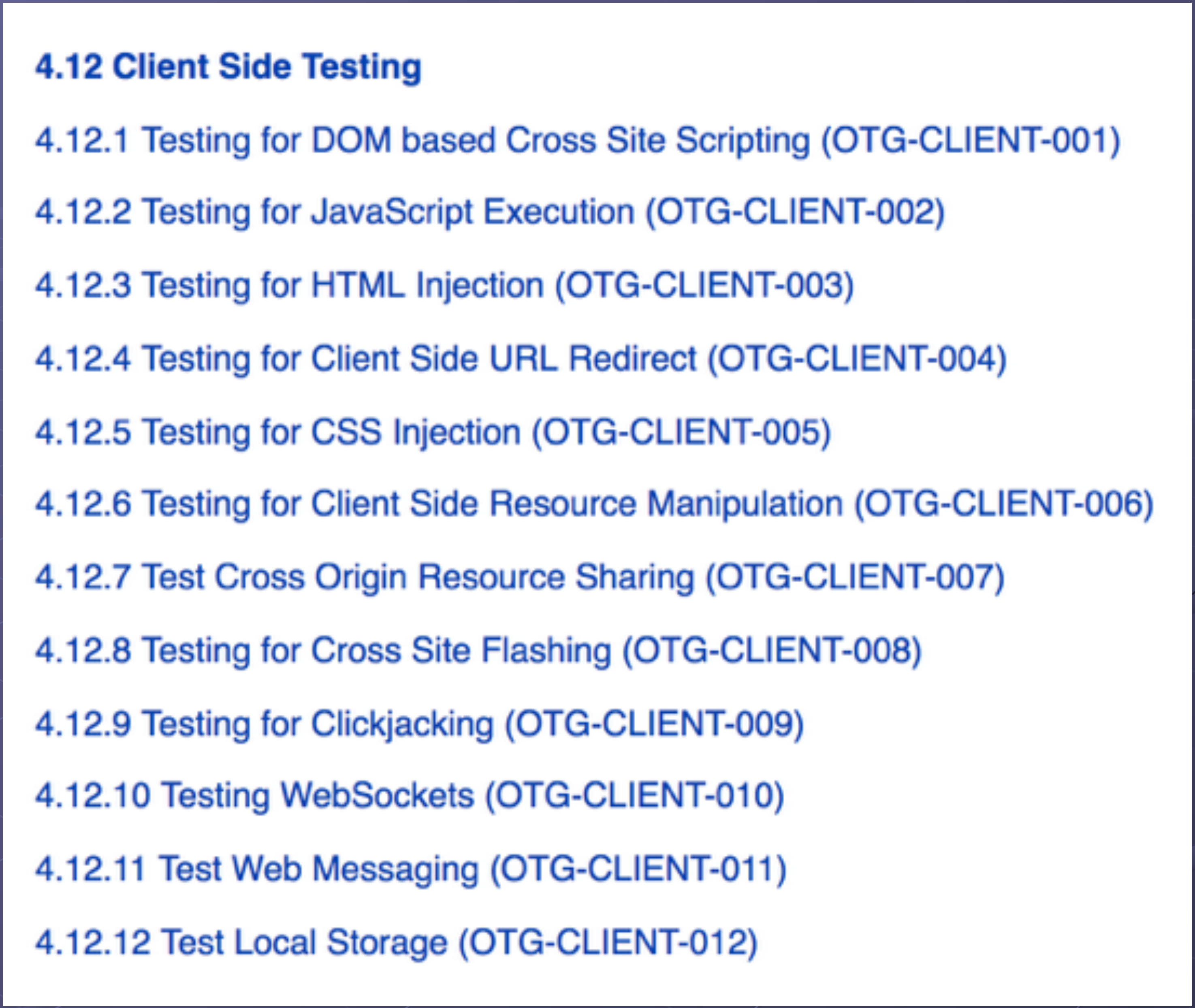
4.7.6 Testing for logout functionality (OTG-SESS-006)

4.7.7 Test Session Timeout (OTG-SESS-007)

4.7.8 Testing for Session puzzling (OTG-SESS-008)







4.12 Client Side Testing

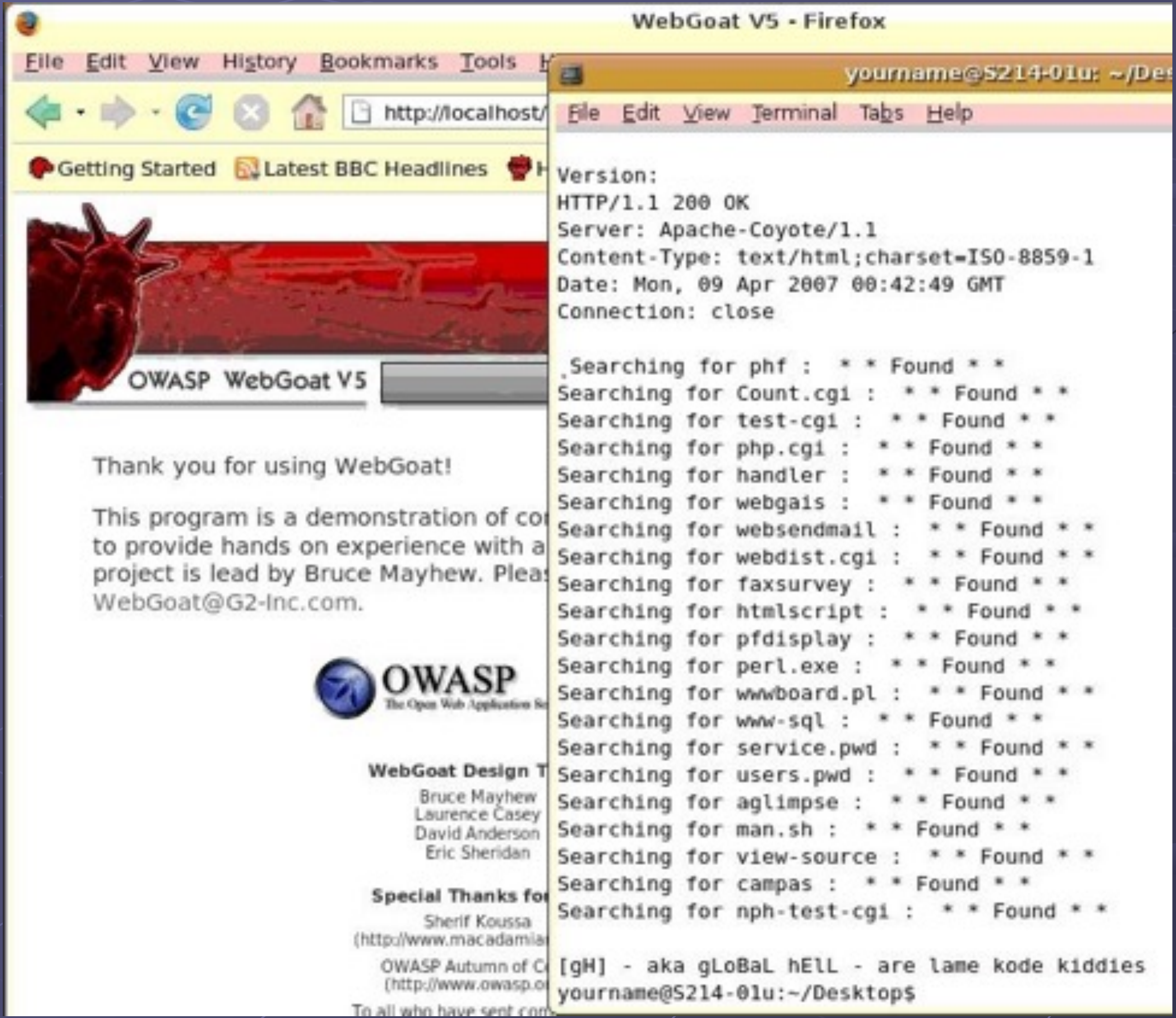
Tools of Web Attackers and Security Testers

- Choose the right tools for the job
- Attackers look for tools that enable them to attack the system
  - They choose their tools based on the vulnerabilities found on a target system or application

Web Tools

- Firefox and Chrome Developer Tools
  - View parameters and cookies
  - Modify and resend requests
- BurpSuite
  - Powerful proxy used for Web App hacking
- Zed Attack Proxy
  - Can do simple vulnerability scans

cgiscan and WebGoat



Thank you for using WebGoat!

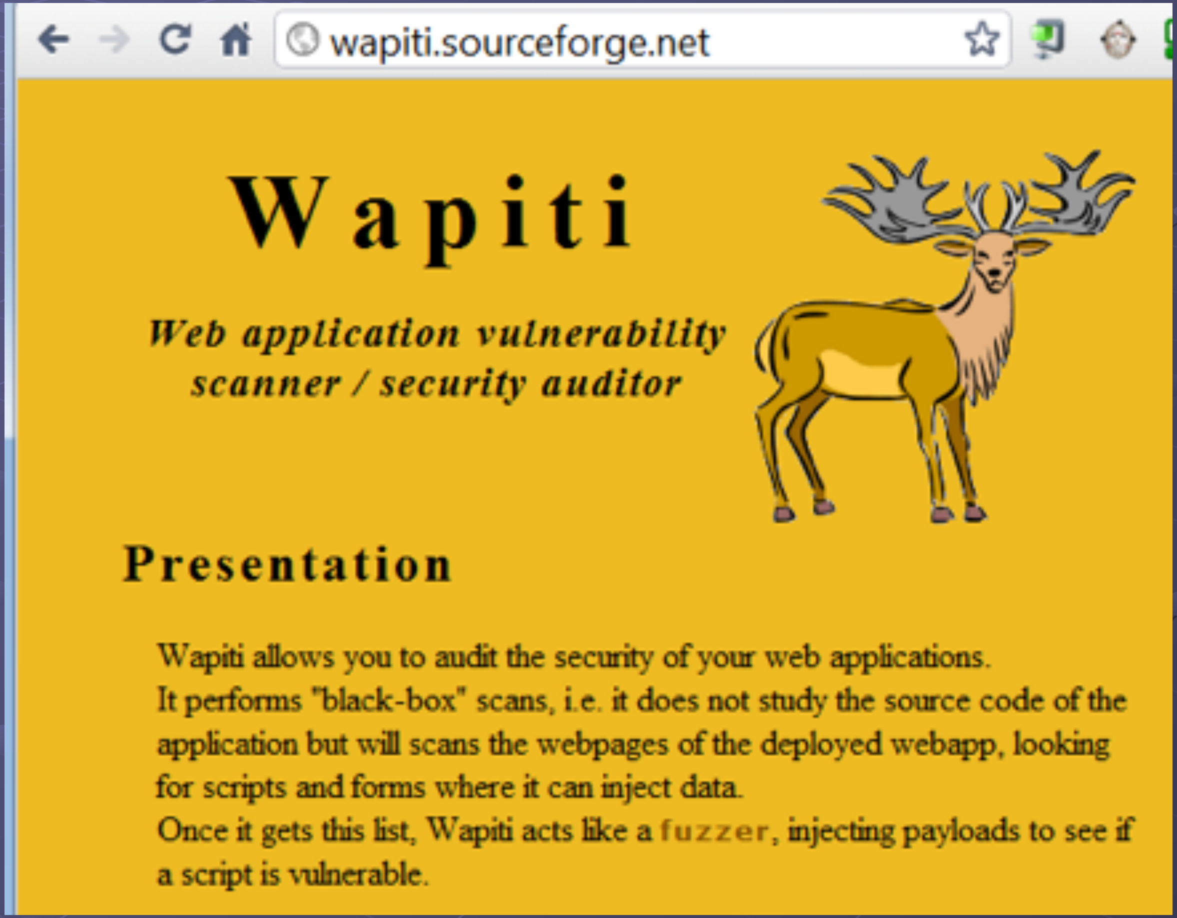
This program is a demonstration of co
to provide hands on experience with a
project is lead by Bruce Mayhew. Plea
WebGoat@G2-Inc.com.

WebGoat Design T
Bruce Mayhew
Laurence Casey
David Anderson
Eric Sheridan

Special Thanks fo
Sherif Koussa
(http://www.macadamia
OWASP Autumn of C
(http://www.owasp.o

```
Version:
HTTP/1.1 200 OK
Server: Apache-Coyote/1.1
Content-Type: text/html;charset=ISO-8859-1
Date: Mon, 09 Apr 2007 00:42:49 GMT
Connection: close

 Searching for phf :  * * Found * *
Searching for Count.cgi :  * * Found * *
Searching for test-cgi :  * * Found * *
Searching for php.cgi :  * * Found * *
Searching for handler :  * * Found * *
Searching for webgais :  * * Found * *
Searching for websendmail :  * * Found * *
Searching for webdist.cgi :  * * Found * *
Searching for faxsurvey :  * * Found * *
Searching for htmlscript :  * * Found * *
Searching for pfdisplay :  * * Found * *
Searching for perl.exe :  * * Found * *
Searching for wwwboard.pl :  * * Found * *
Searching for www-sql :  * * Found * *
Searching for service.pwd :  * * Found * *
Searching for users.pwd :  * * Found * *
Searching for aglimpse :  * * Found * *
Searching for man.sh :  * * Found * *
Searching for view-source :  * * Found * *
Searching for campas :  * * Found * *
Searching for nph-test-cgi :  * * Found * *

[gH] - aka gLoBaL hElL - are lame kode kiddies
yourname@S214-01u:~/Desktop$
```

Web Tools (continued)



wapiti.sourceforge.net

Wapiti

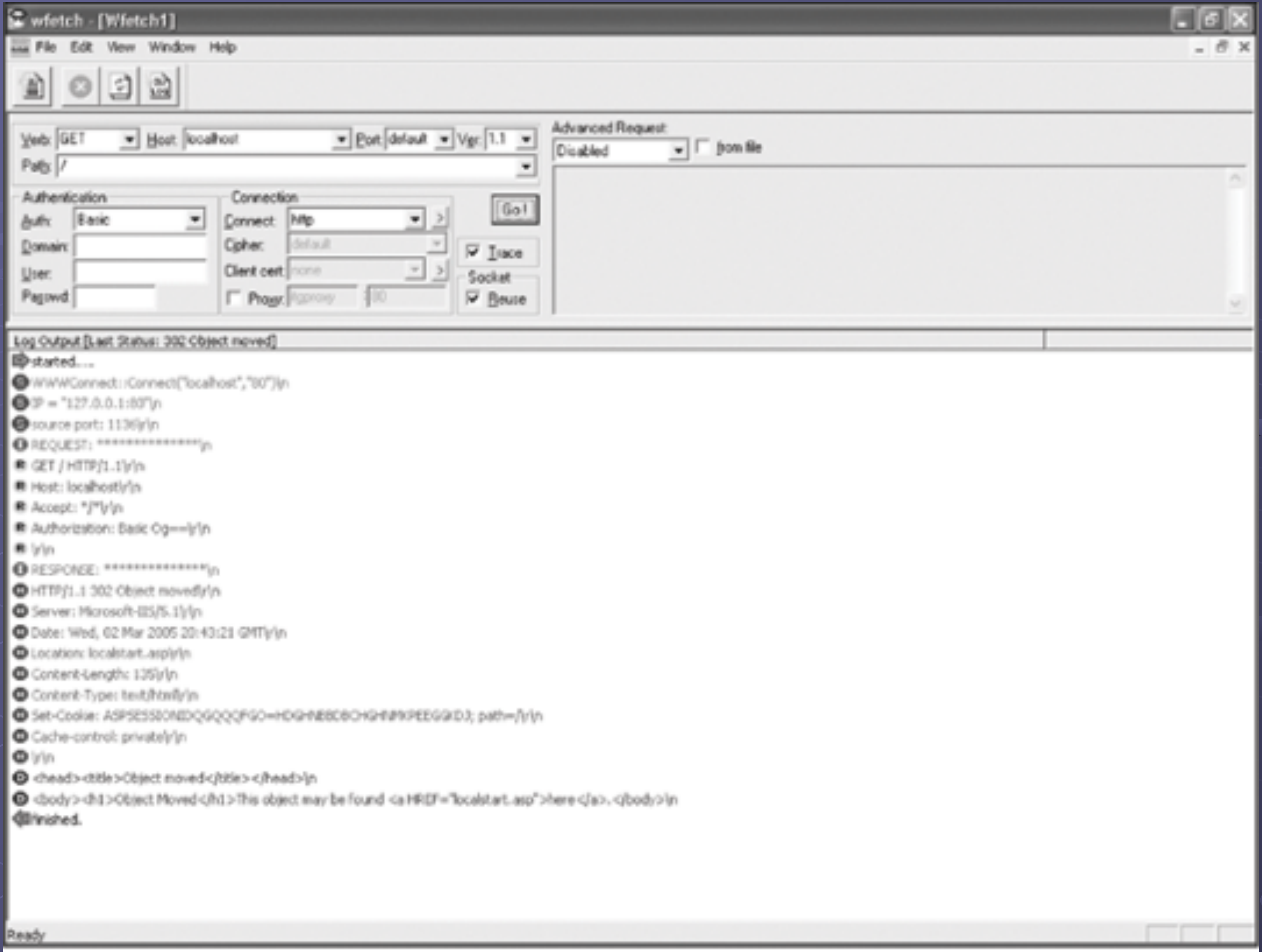
Web application vulnerability scanner / security auditor

Presentation

Wapiti allows you to audit the security of your web applications.
It performs "black-box" scans, i.e. it does not study the source code of the application but will scans the webpages of the deployed webapp, looking for scripts and forms where it can inject data.
Once it gets this list, Wapiti acts like a fuzzer, injecting payloads to see if a script is vulnerable.

Web Tools (continued)

- Wfetch: GUI tool from Microsoft
  - Displays information that is not normally shown in a browser, such as HTTP headers
  - It also attempts authentication using
    - Multiple HTTP methods
    - Configuration of host name and TCP port
    - HTTP 1.0 and HTTP 1.1 support
    - Anonymous, Basic, NTLM, Kerberos, Digest, and Negotiation authentication types
    - Multiple connection types
    - Proxy support
    - Client-certificate support
      - See link Ch 10zl



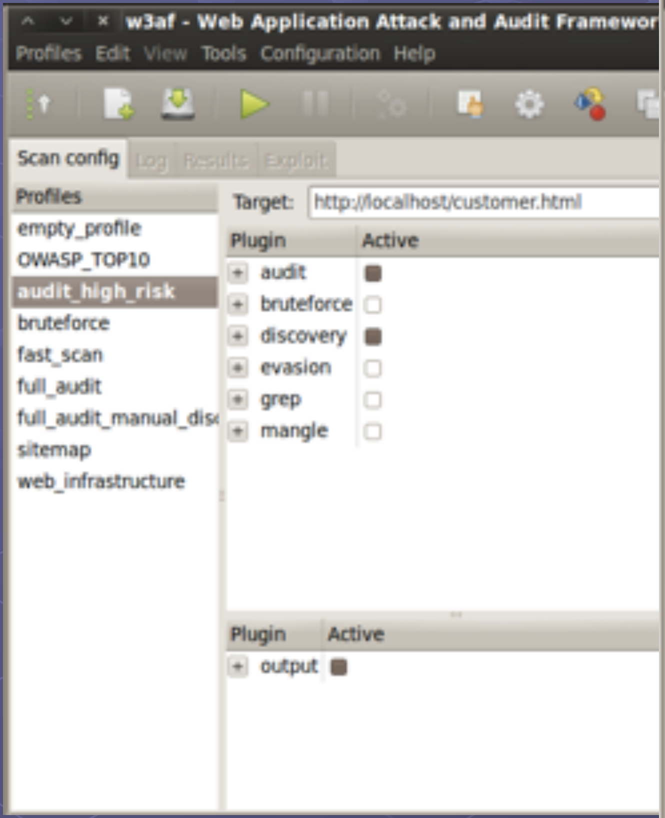
Verb: GET
Host: localhost
Port: default
Ver: 1.1
Path: /
Advanced Request: Disabled
☐ from file
Authentication
Auth: Basic
Domain:
User:
Passwd:
Connection
Connect: http
Cipher: default
Client cert: none
☐ Proxy: itgproxy 80
Go !
☑ Trace
Socket
☑ Reuse

```
Log Output [Last Status: 302 Object moved]
started....
WWWConnect::Connect("localhost","80")\n
IP = "127.0.0.1:80"\n
source port: 1136\r\n
REQUEST: **************\n
GET / HTTP/1.1\r\n
Host: localhost\r\n
Accept: */*\r\n
Authorization: Basic Og==\r\n
\r\n
RESPONSE: **************\n
HTTP/1.1 302 Object moved\r\n
Server: Microsoft-IIS/5.1\r\n
Date: Wed, 02 Mar 2005 20:43:21 GMT\r\n
Location: localstart.asp\r\n
Content-Length: 135\r\n
Content-Type: text/html\r\n
Set-Cookie: ASPSESSIONIDQGQQQFGO=HDGHNBBDBCHGHNMKPEEGGKDJ; path=/\r\n
Cache-control: private\r\n
\r\n
<head><title>Object moved</title></head>\n
<body><h1>Object Moved</h1>This object may be found <a HREF="localstart.asp">here</a>.</body>\n
finished.
```

Ready

Figure 10-32 Using the Wfetch program

W3af (in BackTrack)


w3af - Web Application Attack and Audit Framewor
Profiles Edit View Tools Configuration Help
Scan config Log Results Exploit

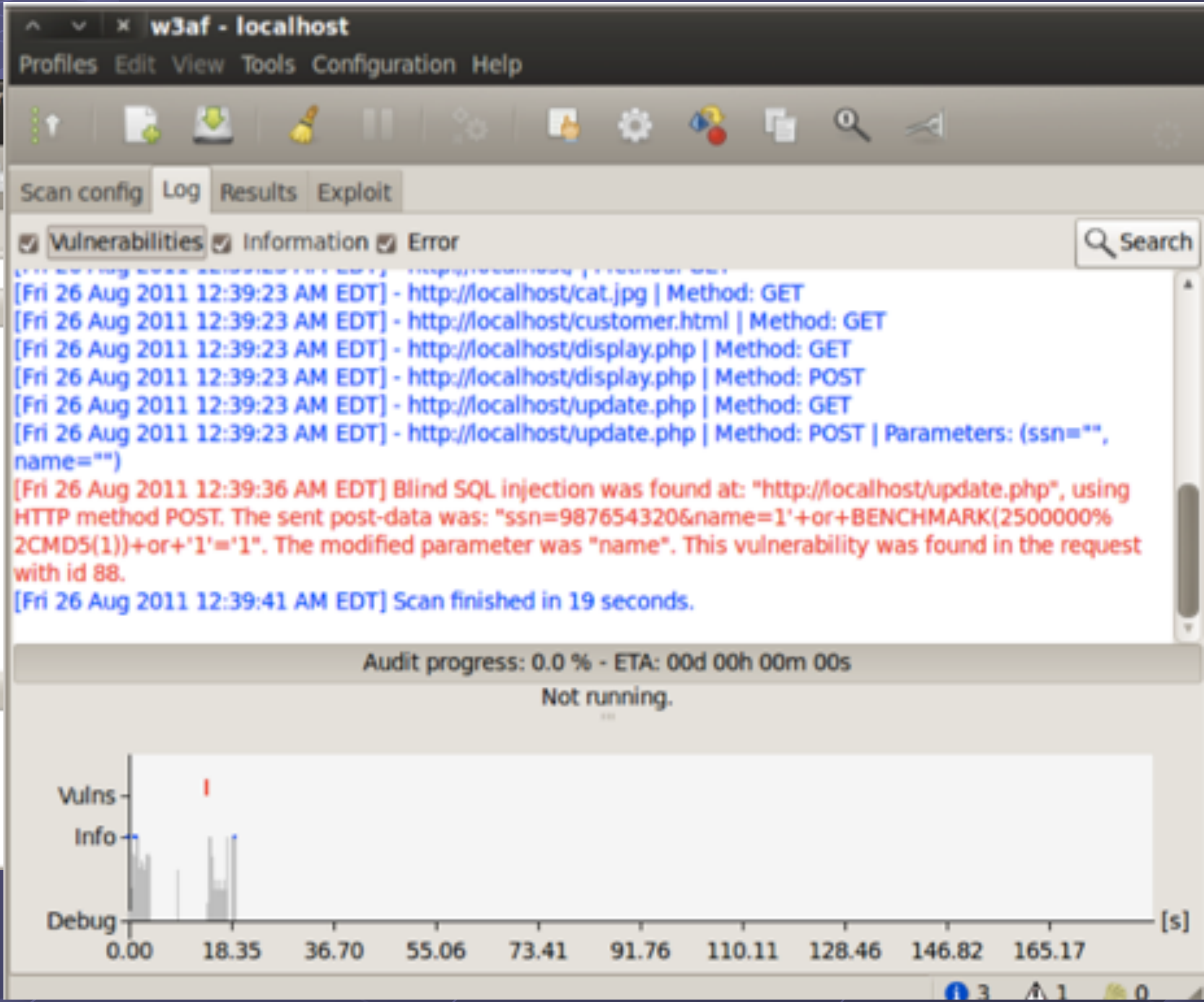
Profiles

- empty_profile
- OWASP_TOP10
- audit_high_risk
- bruteforce
- fast_scan
- full_audit
- full_audit_manual_dis
- sitemap
- web_infrastructure

Target: http://localhost/customer.html

Plugin	Active
audit	■
bruteforce	☐
discovery	■
evasion	☐
grep	☐
mangle	☐

Plugin	Active
output	■

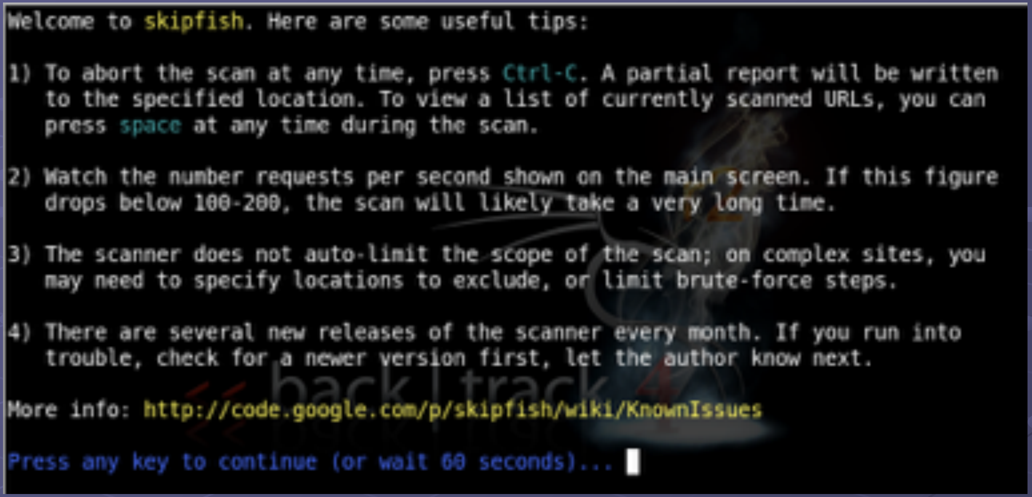

w3af - localhost
Profiles Edit View Tools Configuration Help
Scan config Log Results Exploit
Vulnerabilities Information Error
Search
Vulns
Info
Debug
0.00
18.35
36.70
55.06
73.41
91.76
110.11
128.46
146.82
165.17
[s]
3
1
0

```
[Fri 26 Aug 2011 12:39:23 AM EDT] - http://localhost/cat.jpg | Method: GET
[Fri 26 Aug 2011 12:39:23 AM EDT] - http://localhost/customer.html | Method: GET
[Fri 26 Aug 2011 12:39:23 AM EDT] - http://localhost/display.php | Method: GET
[Fri 26 Aug 2011 12:39:23 AM EDT] - http://localhost/display.php | Method: POST
[Fri 26 Aug 2011 12:39:23 AM EDT] - http://localhost/update.php | Method: GET
[Fri 26 Aug 2011 12:39:23 AM EDT] - http://localhost/update.php | Method: POST | Parameters: (ssn="",
name="")
[Fri 26 Aug 2011 12:39:36 AM EDT] Blind SQL injection was found at: "http://localhost/update.php", using
HTTP method POST. The sent post-data was: "ssn=987654320&name=1'+or+BENCHMARK(2500000%
2CMD5(1))+or+'1'='1". The modified parameter was "name". This vulnerability was found in the request
with id 88.
[Fri 26 Aug 2011 12:39:41 AM EDT] Scan finished in 19 seconds.
```

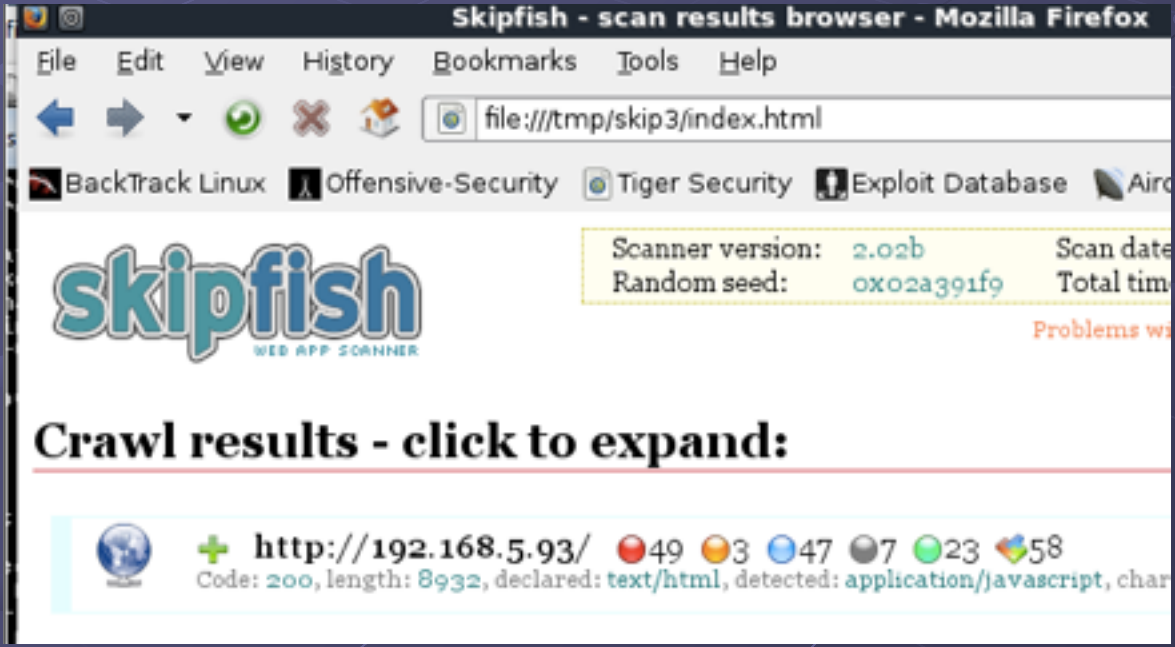
Audit progress: 0.0 % - ETA: 00d 00h 00m 00s

Not running.

Skipfish from Google



```
Welcome to skipfish. Here are some useful tips:

1) To abort the scan at any time, press Ctrl-C. A partial report will be written
   to the specified location. To view a list of currently scanned URLs, you can
   press space at any time during the scan.

2) Watch the number requests per second shown on the main screen. If this figure
   drops below 100-200, the scan will likely take a very long time.

3) The scanner does not auto-limit the scope of the scan; on complex sites, you
   may need to specify locations to exclude, or limit brute-force steps.

4) There are several new releases of the scanner every month. If you run into
   trouble, check for a newer version first, let the author know next.

More info: http://code.google.com/p/skipfish/wiki/KnownIssues

Press any key to continue (or wait 60 seconds)...
```



Skipfish - scan results browser - Mozilla Firefox

Scanner version: 2.02b
Random seed: 0x02a391f9
Scan date
Total tim
Problems wi

Crawl results - click to expand:

http://192.168.5.93/ 49 3 47 7 23 58
Code: 200, length: 8932, declared: text/html, detected: application/javascript, char