



Authentication Security

Hui Zhu



Agenda

- Authentication Components
- Authentication Hacking
- Consideration for Authentication Security
- Principle for Authentication Security
- Case Study



Authentication components

- Login
- Logout
- Registration or Enrolment
- “Forget Password” Function
- “Reset Password” Function
- De-registration



Authentication Hacking

- Server-side Hacking
 - Authentication Bypass
 - Authentication Replay
 - Session Attack
 - Information Disclosure
 - Brute Force and Dictionary Attack
 - Denial of Service Attack
 - Business Logic Vulnerability
 - Miscellaneous Vulnerability



Authentication Hacking


- Client-side Hacking
 - Man-in-the-Middle Attack
 - Sniffing
 - Phishing Attack
 - Keystroke and Screen Logger
 - Password Disclosure
 - Denial-of-Service Attack

Authentication Bypass (server-side)

Gain unauthorized access to the application without knowing password and/or username.

- Impact: **High**
- Levels of skills required: Medium
- Likelihood of Occurrence: **High**

Authentication Bypass (server-side)



```
strUsername = request.getParameter("username");
StrUserPassword = request.getParameter("password");
strSQL = "select * from login where username=" + strUsername
        + "and password=" + strUserPassword;
db.setNTType(0);
db.setStrQuery(strSQL);
db.run();
sqlRst = db.getSqIRst();
sqlRst.last();
intRowCount = sqlRst.getRow();
If (intRowCount <= 0) login=false;
else login=true;
```

- <http://www.vulnerable.com/login.jsp?username=hack&password=1%20or%201=1>

Authentication Bypass (server-side)

.NET forms authentication vulnerability

A standard forms authentication setup requires the presence of "web.config" to set the authentication method and login procedure. The presence of this file prevents access to certain files (.aspx files for example) unless authenticated.

Normal Request:

<http://localhost/secure/somefile.aspx>

Attacks:

<http://localhost/secure\somefile.aspx> (Mozilla)

<http://localhost/secure%5Csomefile.aspx> (IE)

Authentication Replay (Server-side)

Replay the victim's authentication request by exploiting the caching feature provided by the browser.

- Impact: **High**
- Levels of skills required: Low
- Likelihood of Occurrence: **High**

Authentication Replay (Server-side)



Log In - ????-???? http://www.Devchina.com/netsafe/

File Edit View Favorites Tools Help

Back Forward Stop Search Favorites Media Print

Address http://www.net/wwwboard/index.php?s=0&act=Login&CODE=00 Go Links

Google Search Web 751 blocked AutoFill Options

Please enter your details below to log in

Please enter your name	<input type="text" value="dragon001"/>
Please enter your password	<input type="password" value="*****"/>

Options

Remember me? If enabled, you will be automatically logged in again when you visit. This is not recommended for shared computers.	<input checked="" type="radio"/> Yes <input type="radio"/> No
Privacy , do you want to appear on the active users list?	<input type="checkbox"/> Don't add me to the active users list

[Script Execution time: 0.3963] [4 queries used] [GZIP Enabled]

Powered by [Invision Board](#) v1.0.1 © 2002 [Invision PS](#)

Done Internet

Authentication Replay (Server-side)



Discussion Board (Powered by Invision Board) - ?????-???? http://www.Devchina.com/netsafe/

File Edit View Favorites Tools Help

Address http://www. .net/wwwboard/index.php?s=d49986e7f8121556f5d1a3570e3d5ee0&

by Invision Board © 2002 Search Web 751 blocked AutoFill Options Pot

Invision DISCUSSION BOARD

Logged in as: **dragon001** ([Your Control Panel](#) | [Log Out](#) | [0 new messages](#)) Search | Member List | Help

Discussion Board

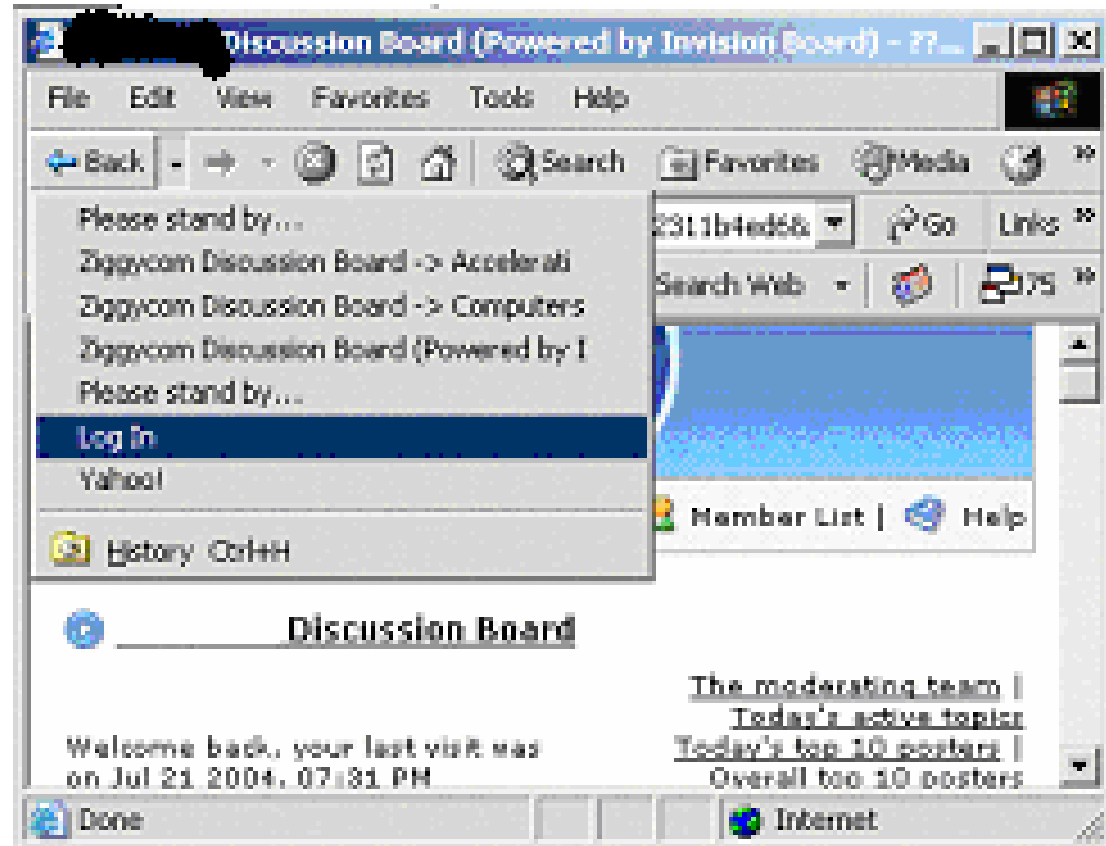
Welcome back, your last visit was on Jul 21 2004, 07:31 PM [The moderating team](#) | [Today's active topics](#)
[Today's top 10 posters](#) | [Overall top 10 posters](#)

▸ General Forum

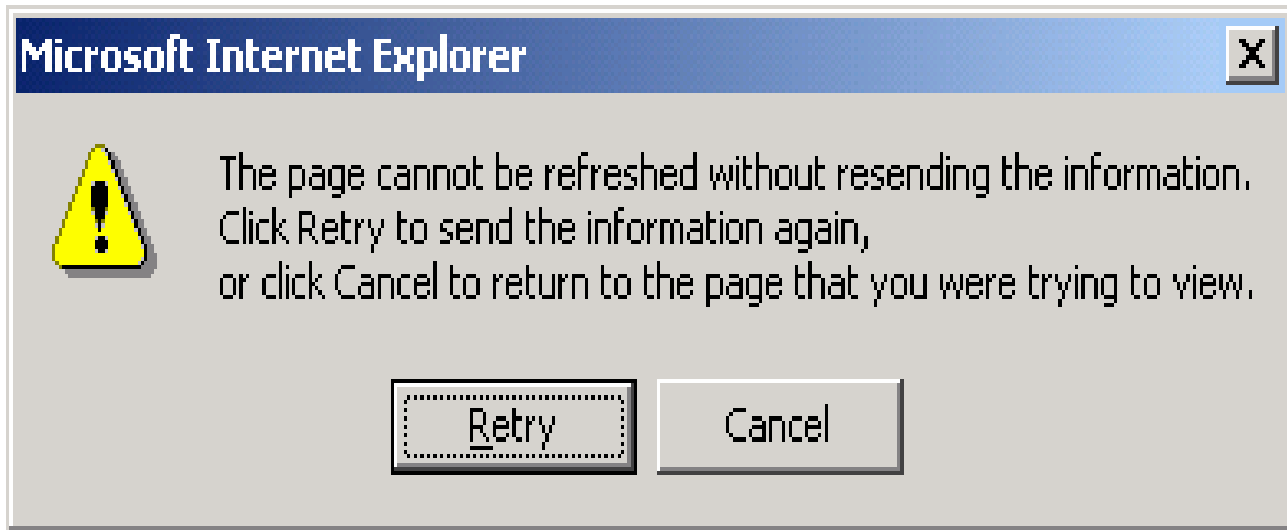
Forum	Topics	Replies	Last Post Info
Computers / Internet / Technology	4	0	Jul 13 2004, 12:21 PM In: Acceleration Software By: Ziqqycom-Chuck
Education	0	0	-- In: By:
Finances	1	0	Jan 16 2003, 02:15 PM In: A Budget By: hazel in kentucky
Healthcare / Insurance	0	0	-- In: By:

Internet

Authentication Replay (Server-side)



Authentication Replay (Server-side)





Session Attack (server-side)

Take advantage of the weak session management to break into or hijack authenticated session

- Impact: **High**
- Levels of skills required: **High**
- Likelihood of Occurrence: Medium



Session Attack (server-side)

- Cookie:
timestamp=9894849323&UserID=dragon001&sessionkey=87928942

Information Disclosure (Server-side)

Discover sensitive information from weak authentication process

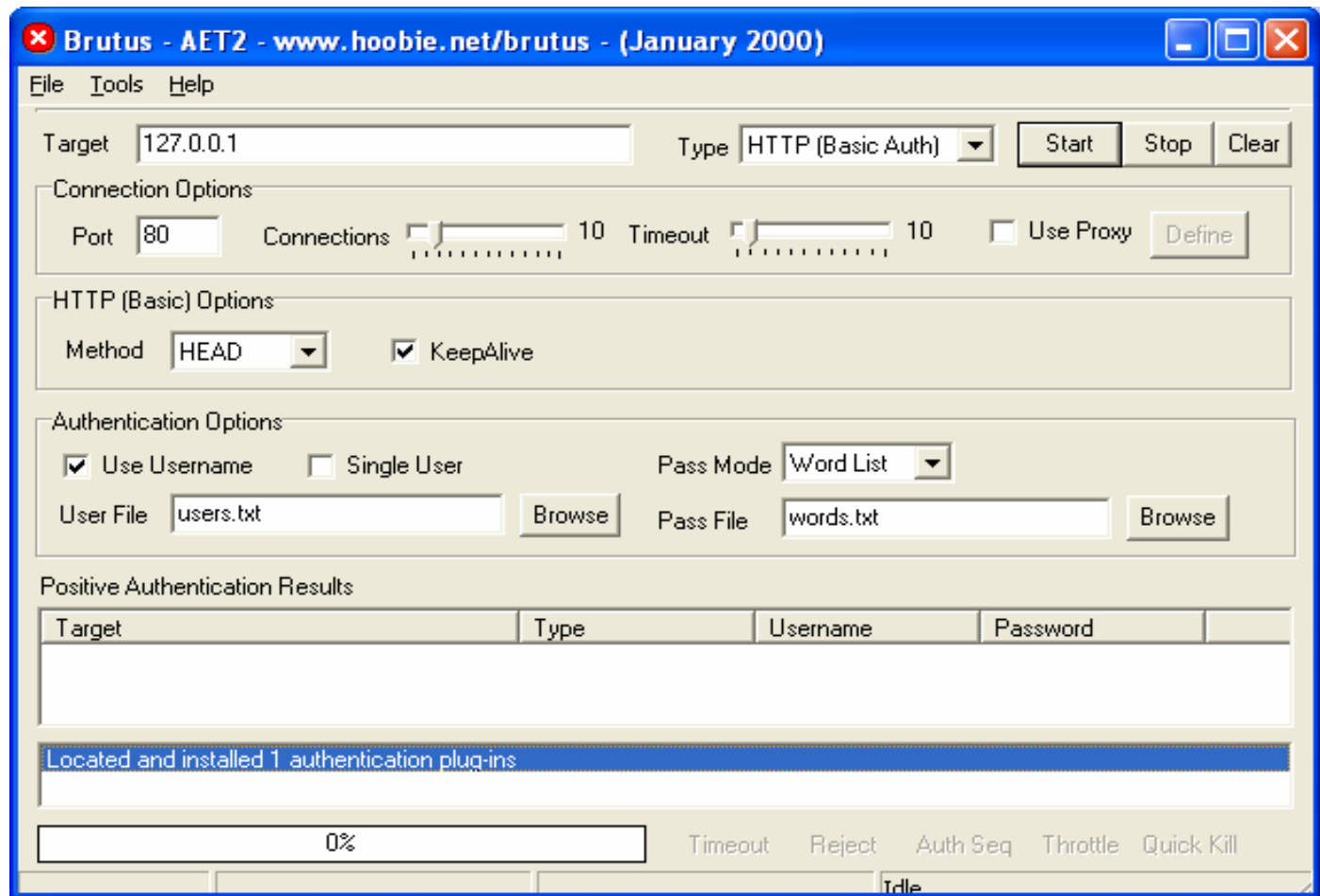
- Impact: Low
- Levels of skills required: Low
- Likelihood of Occurrence: **High**

Brute Force and Dictionary Attack (Server-side)

Gain unauthorized access by trying a large number of possibilities from dictionary or wordlist, or exhaustively working through all possible passwords

- Impact: Low
- Levels of skills required: Medium
- Likelihood of Occurrence: Low

Brute Force and Dictionary Attack (Server-side)





Denial-of-Service (Server-side)

prevent legitimate user's access, by exhausting various computing resource, such as network bandwidth, CPU time, memory, hard disk, etc

- Impact: **High**
- Levels of skills required: Medium
- Likelihood of Occurrence: Medium



Business Logic Vulnerability (Server-side)

Explore the weakness in the business logic design to gain unauthorized access

- Impact: **High**
- Levels of skills required: Medium
- Likelihood of Occurrence: Medium

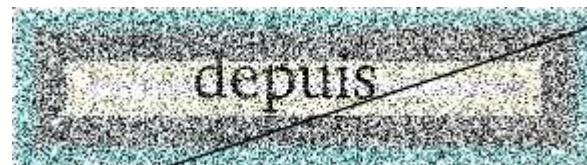


Miscellaneous Vulnerabilities

CAPTCHAs - **C**ompletely **A**utomated **P**ublic **T**uring test to tell **C**omputers and **H**umans **A**part

PWNTcha - <http://sam.zoy.org/pwntcha/>

OCR Research Team <http://www.ocr-research.org.ua/index.php?action=list>



Man-in-the-Middle Attack (Client-side)

Attacker intercept, alter the traffic between two parties without either party knowing that the link between them has been compromised

- Impact: **High**
- Levels of skills required: **High**
- Likelihood of Occurrence: **Low**

Sniffing (Client-side)

Capture the user credentials from network traffic, proxy, caching, etc

- Impact: **High**
- Levels of skills required: **High**
- Likelihood of Occurrence: Medium



Phishing Attack (Client-side)

use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers

- Impact: **High**
- Levels of skills required: High
- Likelihood of Occurrence: **High**

Phishing Attack (Client-side)



From: "Citibank" <antifraud@citibank.com>  Add to Address Book

To:

Subject: your Citibank account [Fri, 9 Jul 2004 07:53:35 +0100]

Date: Fri, 9 Jul 2004 07:53:35 +0100



Dear client of the Citi,

As the Technical service of the Citibank have been currently updating the software, We kindly ask you to follow the reference given below to confirm your data, otherwise your access to the system may be blocked.

https://web.da-us.citibank.com/signin/scripts/login2/user_setup.jsp

We are grateful for your cooperation.

A member of citigroup
Copyright © 2004 Citicorp

Phishing Attack (Client-side)





Key Logger, Screen Logger (Client-side)

Capture user keystroke, mouse click and screen to discover the username and password, even with the on-screen keyboard.

- Impact: **High**
- Levels of skills required: High
- Likelihood of Occurrence: Medium

Key Logger, Screen Logger (Client-side)



Beyond Keylogger ? V 1.78 (only 7 days left to purchase a license)

Beyond Keylogger™

Manual Support

Control Panel

- Settings
 - General Settings
 - Log Maintenance
 - Textual Settings
 - Visual Settings**
 - Media Settings
 - E-Mail Settings
 - FTP Settings
 - Password
 - Advanced
- Commands
 - Stop Logging
 - Hide
- Log Viewer
- Purchase
- Support Email
- Uninstall

? 2006 Supremtec
<http://www.supremtec.com>

Screenshots Settings

Here you can set the screenshots capturing settings

Enable screenshots capturing

This will allow you to set the interval capturing time.

Every 30 seconds. Every 1 minutes.

Capture screen on every mouse click or "Enter" key.

This will allow you to set the image quality.

Small file Big file

This will allow you to reduce the image size for smaller image file.

Reduce image size by 0 %

[Enter registration code](#)

Key Logger, Screen Logger (Client-side)



Citibank Singapore - Maxthon Browser

File Edit View Favorites Groups Options Tools Window Help

Address https://www.citibank.com.sg/portal/citiwm_home_center.jsp?frameset=centerframeset&framevar1=customerSignInLink1&framevar1=workID

Chinese Rea... 计算机安全... 电子书刊(V... DCR Resear... DBS iBanking Citibank Sing... https://w... Google Powered Key... 007 screen lo... Keylogger - D... Download fre... Schneier on ...

citibank HOME CREDIT CARD READY CREDIT INVESTMENTS & DEPOSITS LOANS INSURANCE FINANCIAL SERVICES

Singapore **log in**

Home
Ranking With Us
CitiGold
CitiBusiness
Open An Account
Change Pin Issuance
Application Forms
Answers Instantly
Contact Us

login to citibank
with your card number and PIN

Card Number
898784848

Please use your mouse to enter your PIN
●●●●

9 6 1 5 0
7 4 8 2 3

Clear

Remember my Card Number

[Need Help?](#)
[Forgot your PIN?](#) **log in**

Need Assistance?
Make your enquiry [Online](#) or call our Internet support officers on 6338-2228

What's New At Citibank Online

Fairy tales do come true... with Citibank Ready Credit [details](#)

Apply online and get your card on the same day! [Apply now](#)

Save \$10 with every 3 trades with Citibank Brokerage [details](#)

Internet Security Notice

At Citibank, we're constantly updating our security technology to protect your privacy and confidentiality. It is as **IMPORTANT** that you take the necessary measures to safeguard yourself.

- **Do not use public or shared computers** such as those at internet cafes for internet banking.
- **Beware of scam emails** that trick you into providing your account information and PIN. Citibank will not send you an email requesting for such information.
- **Always type <http://www.citibank.com.sg>** into your browser address bar before you login to ensure that you are on legitimate Citibank website.

Please access the links below for more online security tips.
[Online Security Tips](#) | [Reporting Incidents](#) | [Your Role & Obligations](#)

Citibank Online, Citicard and CitiPhone Banking are service marks registered and used by Citibank, N.A. and Citicorp throughout the world. Visa is a registered service mark and

Done 2 192.168.190.1 0 bytes 454M 1

start 2 Wi... Citiban... Micros... hack... untile... EN 11:53 PM

Prev Next Slide Show First Last Save Close 8 of 16 - 03/11/2006 23:53:18



Password Discovery (Client-side)


Discover the password from browser cache, history list, memory in client's PC

- Impact: **High**
- Levels of skills required: **High**
- Likelihood of Occurrence: **Low**

Password Discovery (Client-side)



Password Discovery (Client-side)



WinHex

File Edit Search Position View Tools Specialist Options File Manager Window Help

Case Data

File Edit

lexplore: Primary Memory

Texplore: Primary Memory

Offset	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	
10023A80	01	00	00	00	B8	31	02	10	01	00	00	00	A0	02	3C	161.....<..
10023A90	00	00	00	00	00	00	00	00	01	00	00	00	90	94	02	16
10023AA0	B0	3A	02	10	00	00	00	00	00	00	00	00	00	00	00	00	*.....
10023AB0	01	00	00	00	C8	03	3C	16	01	00	00	00	68	3A	02	10E.<.....h:..
10023AC0	01	00	00	00	60	86	65	16	68	31	02	10	60	E4	01	10 e.h ...ä..
10023AD0	01	00	00	00	05	80	00	00	01	00	00	00	C0	94	65	16Ä e..
10023AE0	60	A6	09	10	68	31	02	10	00	00	00	00	01	01	00	00	...h
10023AF0	01	00	00	00	40	9D	65	16	F0	E9	01	10	00	00	00	00	...@ e.šé.....
10023B00	01	00	00	00	58	F3	04	16	01	00	00	00	F0	E9	01	10	...Xó.....šé..
10023B10	01	00	00	00	58	F3	04	16	00	00	00	00	00	00	00	00	...Xó.....
10023B20	01	00	00	00	D8	2D	04	16	B8	3B	02	10	06	00	00	00	0-.....
10023B30	00	00	00	00	00	00	00	00	01	00	00	00	90	03	01	16
10023B40	06	00	00	00	32	00	32	00	33	00	34	00	37	00	37	00	...2.2.3.4.7.7..
10023B50	01	00	00	00	E0	85	01	16	38	3B	02	10	00	00	00	00	...à
10023B60	06	00	00	00	00	00	00	00	01	00	00	00	90	03	01	16	...à
10023B70	16	00	00	00	32	00	32	00	33	00	34	00	37	00	37	00	...2.2.3.4.7.7..
10023B80	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
10023B90	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
10023BA0	01	00	00	00	E0	85	01	16	68	3B	02	10	00	00	00	00	...à ...h:..
10023BB0	06	00	00	00	00	00	00	00	01	00	00	00	90	03	01	16
10023BC0	16	00	00	00	FF	00	FF	00	FF	00	FF	00	FF	00	FF	00	...ý.ý.ý.ý.ý.ý..
10023BD0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
10023BE0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
10023BF0	01	00	00	00	90	06	01	16	08	00	00	00	FF	FF	FF	FFyyyy
10023C00	FF	FF	FF	FF	00	00	00	00	01	00	00	00	90	06	01	16	yyyy..... ...
10023C10	08	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	00	00	00	...yyyyyyyyyy...
10023C20	01	00	00	00	90	06	01	16	08	00	00	00	FF	FF	FF	FFyyyy
10023C30	FF	FF	FF	FF	00	00	00	00	01	00	00	00	90	06	01	16	yyyy..... ...
10023C40	10	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	...yyyyyyyyyyyyyy
10023C50	FF	FF	FF	FF	00	00	00	00	01	00	00	00	90	06	01	16	yyyy..... ...
10023C60	10	00	00	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	...yyyyyyyyyyyyyy
10023C70	FF	FF	FF	FF	00	00	00	00	01	00	00	00	D8	2D	04	16	yyyy.....0-..
10023C80	48	A6	02	10	10	00	00	00	00	00	00	00	00	00	00	00	H
10023C90	01	00	00	00	90	03	01	16	10	00	00	00	43	00	46	00C.F..
10023CA0	31	00	32	00	30	00	32	00	39	00	42	00	32	00	36	00	1.2.0.2.9.B.2.6.
10023CB0	34	00	46	00	37	00	33	00	36	00	31	00	00	00	00	00	4.F.7.3.6.1.....

Data Interpreter

8 Bit (±): 50
16 Bit (±): 50
32 Bit (±): 3276850

Page 44443 of 79901 Offset: 10023B74 = 50 Block: n/a Size: n/a

Primary Memory [unregistered]

Process: lexplore

Range size: 43.9 MB
46,022,656 bytes

Base address: 00010000

[Read-only mode]

Window #: 1
No. of windows: 1

Mode: Text
Character set: ANSI ASCII
Offsets: virtual
Bytes per page: 36x16=576

Clipboard: available

TEMP folder: 6.2 GB free
IE~1\BoonHoo\LOCALS~1\Temp

Password

Password Discovery (Client-side)

- For example, an online banking application stored the password in memory like the following:

```
FEFFFEFF750076007700780031003200330  
03400FEFFFEFF
```

- The password “uvwxyz1234” is encoded by Unicode and stored in memory with “FEFFFEFF” as delimiters. It is simple to search for FEFFFEFF to find the password.



Denial-of-Service Attack (Client-side)

prevent legitimate users' access to the web application, by sabotage the users' computer

- Impact: High
- Levels of skills required: High
- Likelihood of Occurrence: Low

A person's hands are shown holding a large, bright yellow egg. The egg is the central focus of the image, and the person's hands are positioned around it, one near the top and one near the bottom. The background is dark and out of focus.

Consideration for Authentication Security

- Security requirement
- Risk assessment and/or threat modeling
- User acceptance
- Application performance
- Compatibility
- Cost of implementation

A person's hands are shown holding a large, bright yellow egg. The egg is the central focus of the image, and the person's hands are positioned around it, one at the top and one at the bottom. The background is a soft, out-of-focus light color.

Principles for Authentication Security

- Proper input validation and output verification
- Always use “post” for form variable submission
- Non-cache and immediately expire all the web pages
- Manage user sessions and transaction sessions properly
- Use strong session management mechanism

Real World Case Study



login to citibank
with your card number and PIN

Card Number

Please use your mouse to enter your PIN

8	2	4	6	0
5	3	9	7	1

Remember my Card Number

[Need Help?](#)
[Forgot your PIN?](#)


Real World Case Study




Login


Access Code: ?


PIN: ?

 For added security, please use our [On-Screen Keyboard](#) ?

Secured area  [I have forgotten my password](#)

[I have problems logging on.](#) | [How do I log on?](#)

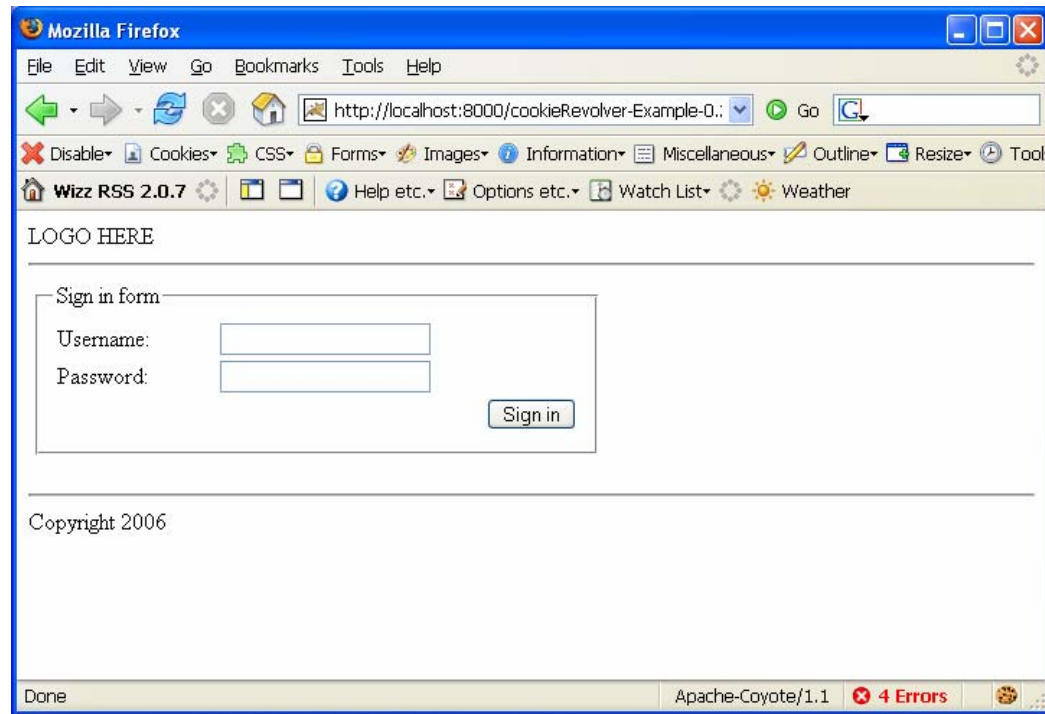
 **Security Alert**

 **Security and Privacy**
Learn how to safeguard yourself
[click here](#)

~	!	@	#	\$	%	^	&	*	()	_	+
`	1	2	3	4	5	6	7	8	9	0	-	=
	Q	W	E	R	T	Y	U	I	O	P	{	}
"	A	S	D	F	G	H	J	K	L	:	;	\
'	Z	X	C	V	B	N	M	{	}	,	.	/
?	CAP	SPACE	<	>	CLEAR							

CookieRevolver

<http://sourceforge.net/projects/cookie-revolver>



A person's hands are shown holding a large, bright yellow egg. The egg is the central focus of the image on the left side of the slide. The person is wearing a dark jacket. The background is a plain, light color.

CookieRevolver

The first time a system is used by a browser, this is the process

- Browser gets a new machine-id cookie
- User authenticates with username/password
- User answers preset security question
- Browser gets a new certificate cookie
- User is redirected to the site main page

For most interaction with a CookieRevolver secured site, this is the process

- Browser sends machine-id cookie
- User authenticates with username/password
- Browser sends and gets a new certificate cookie
- User is redirected to the site main page

Cookie Revolver

Cookie

- certtest001=EtDPWHDLhISEt5NxkqPZVmWFVWNZRkXHuYYcSOqJ27611qtyuYKA%2BknmKdAzxPcEsnaKJI8hFdFd%0D%0AZ00pOEeklxuiUCDSHe%2BqpIKIY4inQdiZ%2F2VACue8DbL8rvQNgjpXnHqBOEo7f6%2BbTx3dALjmZ8G2%0D%0Aqv4EJa075Tt2Cg%2BwL74%3D; JSESSIONID=74D44E606788EF36AF174C2BBF7E7E92
- {machine='36d5c75f-a064-4ae3-86eb-b727f0e95ee0'(homepc),userName=test001,loginFailures='0',cert='id=8a8aac01-dd3e-4bd9-be5c-8ec8e39d6a05&userID=test001'}

CookieRevolver



Test Case	Impact	Risk rating	Finding
Server Side			
Authentication Bypass	N/A	N/A	No
Authentication Replay	N/A	N/A	No
Session Attack	N/A	N/A	No
Information Disclosure	N/A	N/A	No
Brute Force and Dictionary Attack	N/A	N/A	No
Denial-of- Service Attack	N/A	N/A	No
Business Logic Vulnerabilities	N/A	N/A	No
Client Side			
Man-in-the-Middle Attack	Medium	Low	Vulnerable but difficult to explore
Sniffing	Medium	Low	Vulnerable but difficult to explore
Phishing Attack	Medium	Low	Vulnerable but difficult to explore
Key and screen Logger	Low	Low	Vulnerable but difficult to explore
Password Discovery	Low	Low	Vulnerable but difficult to explore
Denial-of-Service Attack	Low	Low	Vulnerable but can be fixed

Reference

- Directory traversal http://www.imperva.com/application_defense_center/glossary/directory_traversal.html
- Phishing <http://www.antiphishing.org/>
- Discussion on browser refresh security issues <http://seclists.org/lists/webappsec/2003/Jul-Sep/0084.html>
- Application Denial of Service (DoS) Attacks <http://www.corsaire.com/>
- Open Source Web Application Security Project (OWASP) <http://www.owasp.org>
- Dos and Don'ts of Client Authentication on the Web <http://cookies.lcs.mit.edu>

Reference

- http://www.schneier.com/blog/archives/2006/02/doityours elf_ke.html
- **Osk.exe - On-screen keyboard in Windows**
- <http://www.mykeylogger.com/>
- <http://www.supremtec.com/> Captures All KeyStrokes. Records Instant Messengers. Monitors Application Usage. Captures Desktop Activity. Captures Screen shots. Quick Search over the log. Sends Reports by e-Mail.
- **My Little Spy** is intended for recording a file of everything that is entered from the keyboard. My Little Spy works with out being seen, and can be recalled by a combination of keys. My Little Spy records all email, chats conversations, instant messengers (ICQ, MSN, Yahoo, AIM ...), usernames and passwords, all keystrokes typed, in one word, everything. It records all text that has been on the clipboard (copy/paste), window titles and takes pictures of the screen as well.



- zhusec005@yahoo.com
- www.ebizsec.com