Entering Passwords on a Spyware Infected Machine

Dinei Florencio and Cormac Herley

Microsoft Research

ABSTRACT

We examine the problem of entering sensitive data, such as passwords, from an untrusted machine (i.e., possibly infected with spyware). Using such a machine is obviously undesirable, and yet roaming users often have no choice.

We consider whether it is possible to enter data to confound spyware assumed to be running on the machine in question. The difficulty of mounting a collusion attack on a single user's password makes the problem more tractable than it might appear. We explore several approaches. In the first, we show how the user can embed a password in random keystrokes to confuse spyware, while leaving the actual login unaffected. In the second we employ a proxy server to strip random keys. In the third we again employ a proxy that inverts a key mapping performed by the user. We examine also several potential attacks.

Motivation

- Accessing your accounts when roaming;
- Available terminal (kiosks, internet cafes) may be compromised; keyloggers a common risk.
- “Simply do not use” is not always an option.

Assumption:

- Terminal is running a keylogger.

A simple solution…

- Go to the login page;
- Click on Password (PWD) field;
- Type first character of PWD;
- Click outside PWD field;
- Type random characters (these will be ignored by the browser, but recorded by keylogger);
- Repeat until typing all PWD characters…
- Keylogger gets password interspersed with random characters.

… and a simple attack

- Replace keylogger with one that also records mouse click events …

Assumptions / Requirements

- Attackers record everything you do, and everything on the screen;
- Plug-ins may access whatever goes over a SSL connection;
- No changes to the Bank login server;
- No changes to your daily logins;
- No password uploading/maintaining.

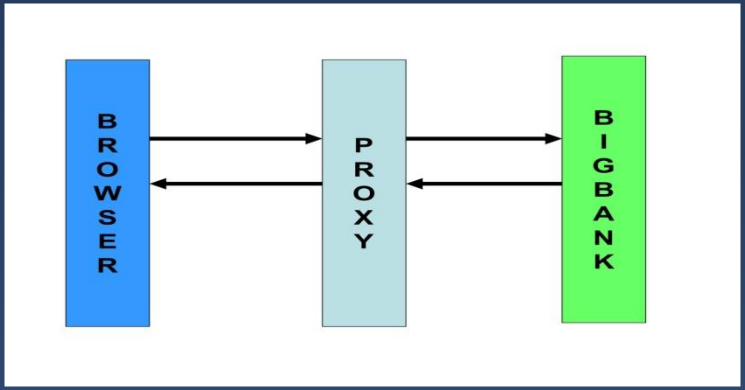
Is the problem possible?

- everything you see on the screen, and everything you type, is available to the attacker…

To our advantage:

- Collusion between different locations is hard;
- We are allowed to use a proxy server;

Basic Idea



- Use a separate channel (e.g., a safe terminal) to set up a **shared secret** with a login proxy server (MITM proxy);
  - NOTE: a *different* unsafe terminal is also ok, as long as we can assume no collusion between terminals.
  - NOTE2: the MITM proxy breaks the SSL connection;
- Use the proxy server to connect you to your desired site. Proxy is going to instruct you on how to modify/code your PWD, based on the shared secret.

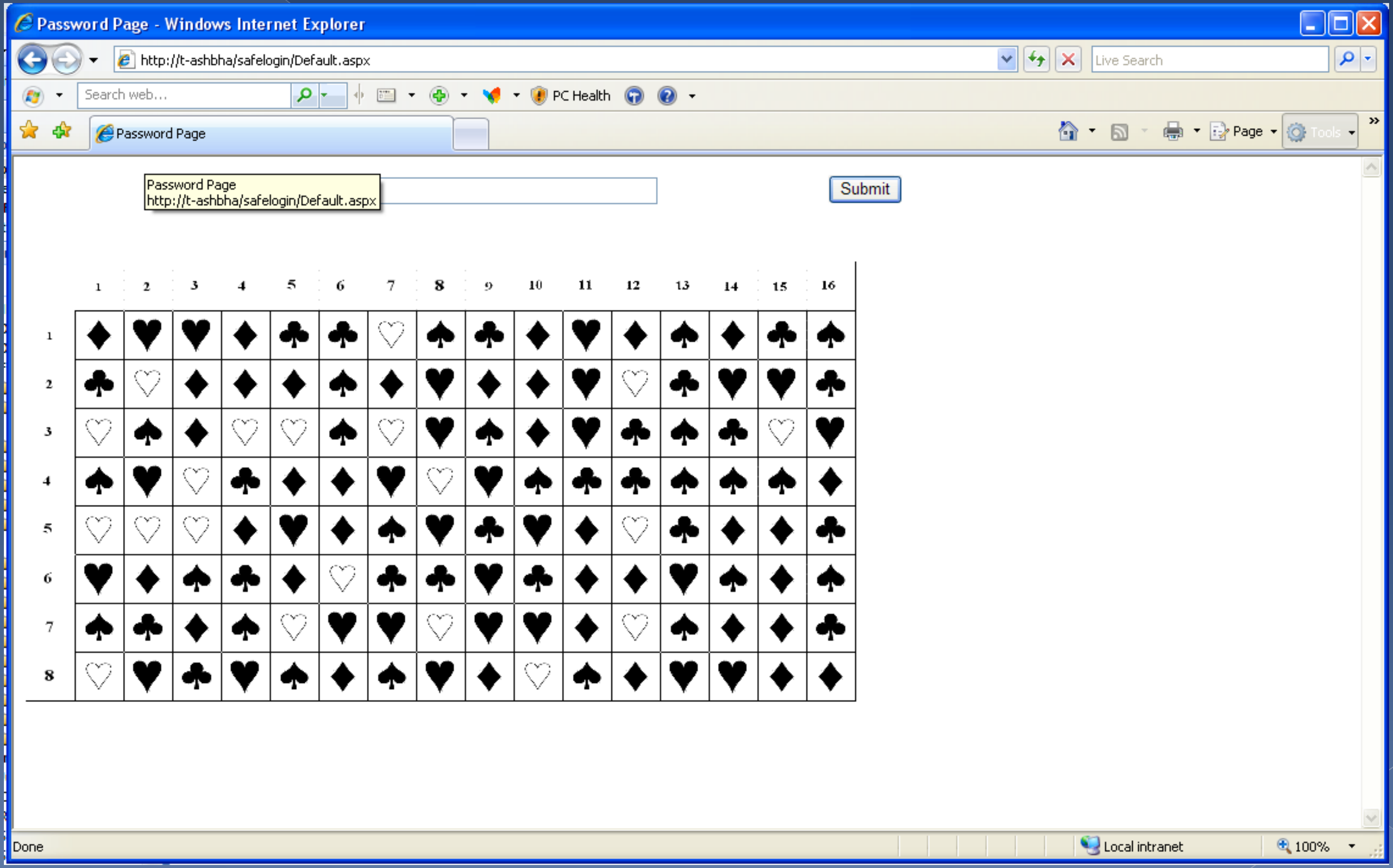
Three alternatives

- METHOD 1: Minimum setup (3A♥).
- METHOD 2: easiest to use (MyPics).
- METHOD 3: maximum security (print table).

METHOD 1 (least initial setup)

- Before using:
  - setup a username (no PWD), and inform any "non-usual" sites you may want to visit
  - Receive (and memorize/keep) a shared secret consisting of a table position and a symbol (e.g., 3A♥)

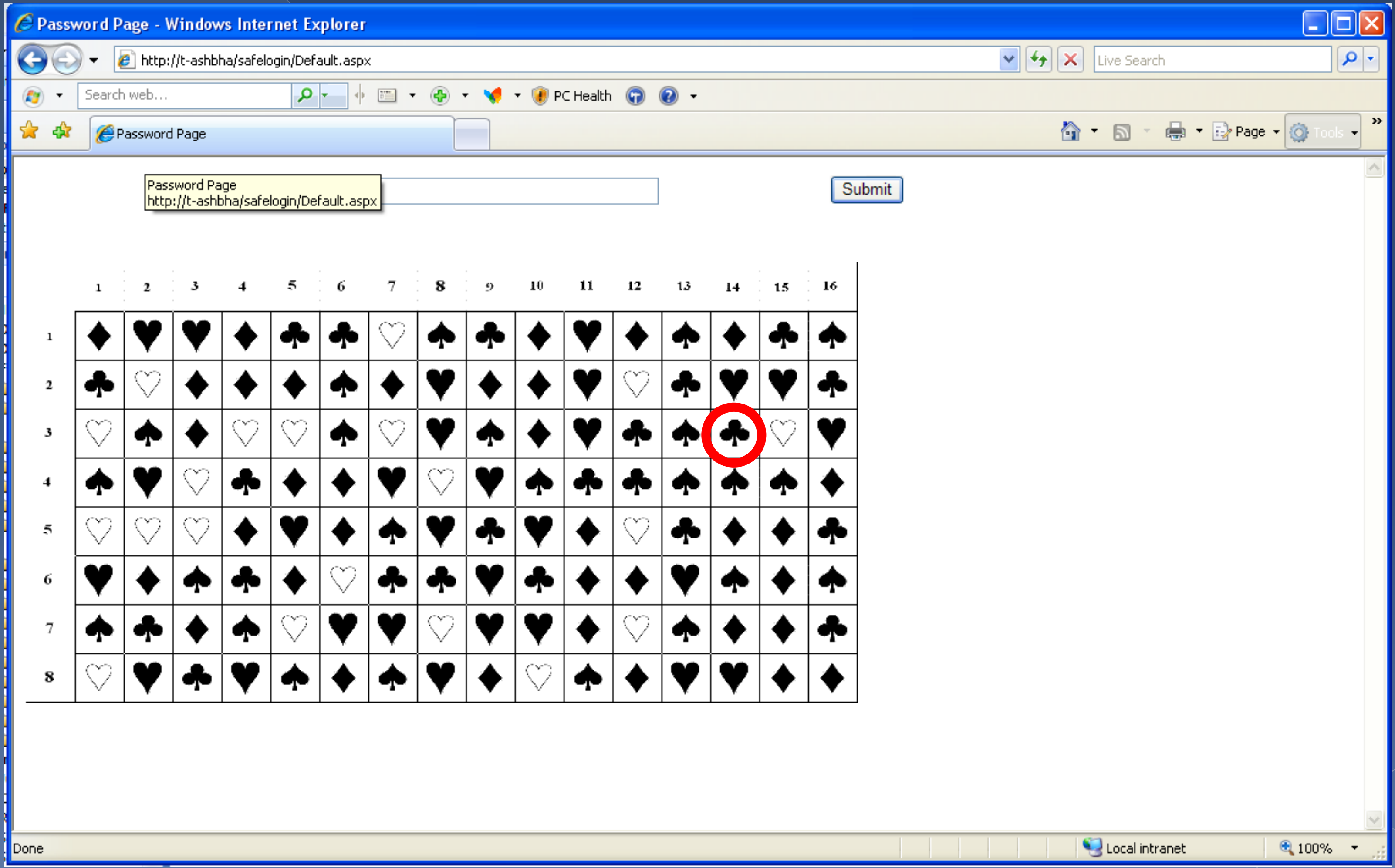
Login w/ method 1



Password Page
http://t-ashbha/safelogin/Default.aspx

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	♦	♥	♥	♦	♣	♣	♡	♠	♣	♦	♥	♦	♠	♦	♣	♠
2	♣	♡	♦	♦	♦	♠	♦	♥	♦	♦	♥	♡	♣	♥	♥	♣
3	♡	♠	♦	♡	♡	♠	♡	♥	♠	♦	♥	♣	♠	♣	♡	♥
4	♠	♥	♡	♣	♦	♦	♥	♡	♥	♠	♣	♣	♠	♠	♠	♦
5	♡	♡	♡	♦	♥	♦	♠	♥	♣	♥	♦	♡	♣	♦	♦	♣
6	♥	♦	♠	♣	♦	♡	♣	♣	♥	♣	♦	♦	♥	♠	♦	♠
7	♠	♣	♦	♠	♡	♥	♥	♡	♥	♥	♦	♡	♠	♦	♦	♣
8	♡	♥	♣	♥	♠	♦	♠	♥	♦	♡	♠	♦	♥	♥	♦	♦

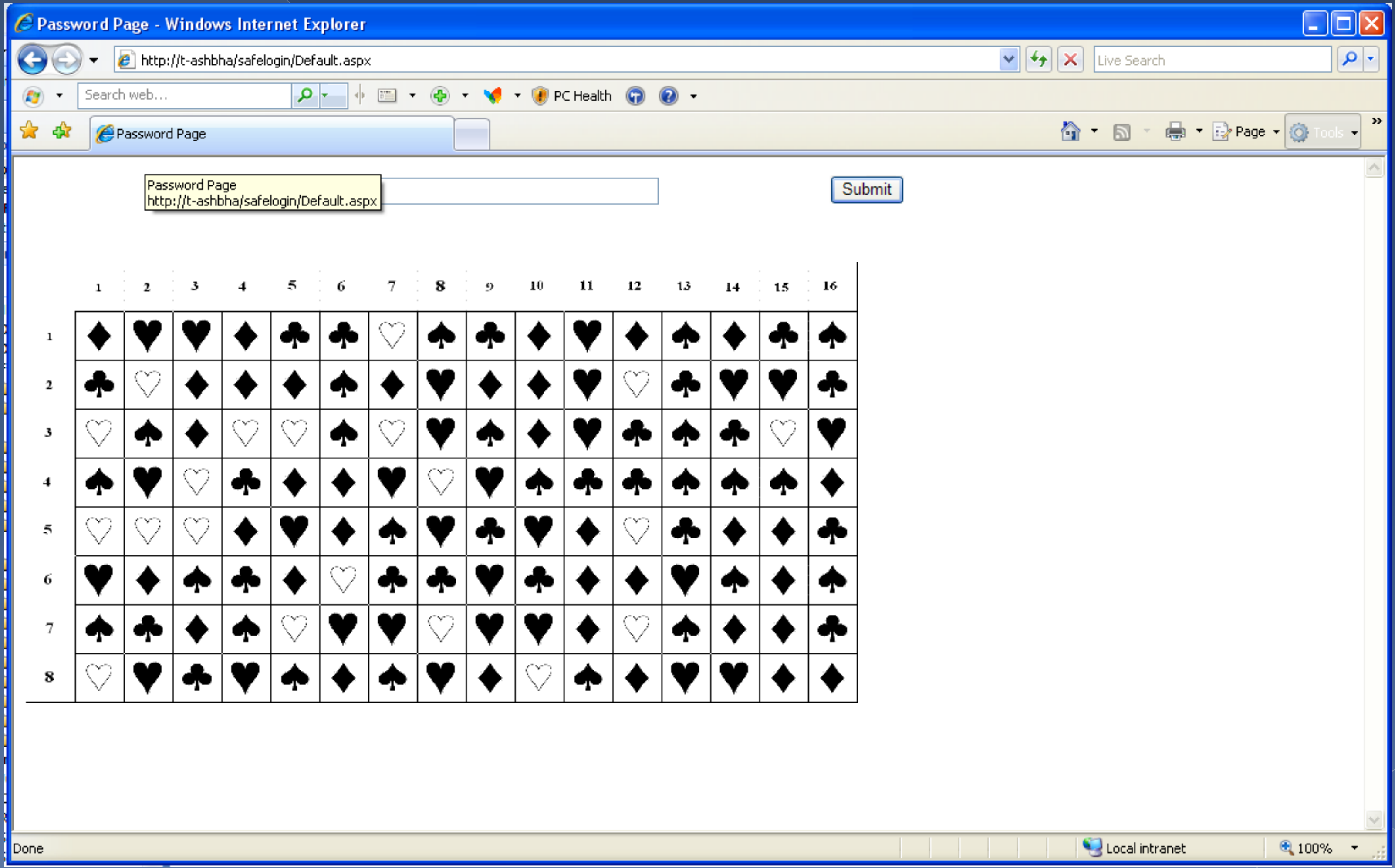
Login w/ method 1



Password Page
http://t-ashbha/safelogin/Default.aspx

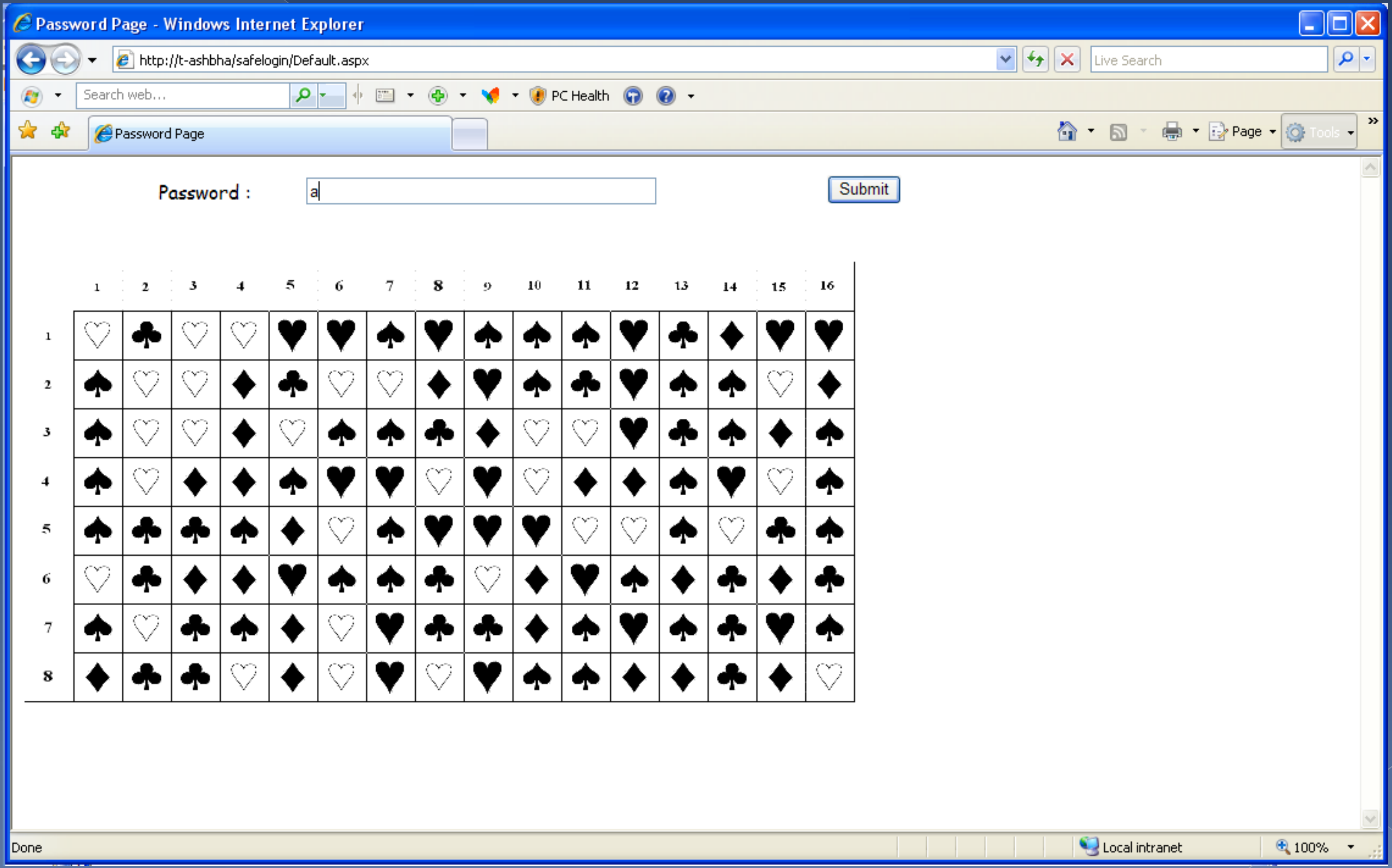
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	♦	♥	♥	♦	♣	♣	♡	♠	♣	♦	♥	♦	♠	♦	♣	♠
2	♣	♡	♦	♦	♦	♠	♦	♥	♦	♦	♥	♡	♣	♥	♥	♣
3	♡	♠	♦	♡	♡	♠	♡	♥	♠	♦	♥	♣	♠	♣	♡	♥
4	♠	♥	♡	♣	♦	♦	♥	♡	♥	♠	♣	♣	♠	♠	♠	♦
5	♡	♡	♡	♦	♥	♦	♠	♥	♣	♥	♦	♡	♣	♦	♦	♣
6	♥	♦	♠	♣	♦	♡	♣	♣	♥	♣	♦	♦	♥	♠	♦	♠
7	♠	♣	♦	♠	♡	♥	♥	♡	♥	♥	♦	♡	♠	♦	♦	♣
8	♡	♥	♣	♥	♠	♦	♠	♥	♦	♡	♠	♦	♥	♥	♦	♦

Login w/ method 1


Password Page - Windows Internet Explorer
http://t-ashbha/safelogin/Default.aspx
Live Search
Search web...
PC Health
Password Page
Page
Tools
Password Page
http://t-ashbha/safelogin/Default.aspx
Submit
Done
Local intranet
100%

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	♦	♥	♥	♦	♣	♣	♡	♠	♣	♦	♥	♦	♠	♦	♣	♠
2	♣	♡	♦	♦	♦	♠	♦	♥	♦	♦	♥	♡	♣	♥	♥	♣
3	♡	♠	♦	♡	♡	♠	♡	♥	♠	♦	♥	♣	♠	♣	♡	♥
4	♠	♥	♡	♣	♦	♦	♥	♡	♥	♠	♣	♣	♠	♠	♠	♦
5	♡	♡	♡	♦	♥	♦	♠	♥	♣	♥	♦	♡	♣	♦	♦	♣
6	♥	♦	♠	♣	♦	♡	♣	♣	♥	♣	♦	♦	♥	♠	♦	♠
7	♠	♣	♦	♠	♡	♥	♥	♡	♥	♥	♦	♡	♠	♦	♦	♣
8	♡	♥	♣	♥	♠	♦	♠	♥	♦	♡	♠	♦	♥	♥	♦	♦

Login w/ method 1


Password Page - Windows Internet Explorer
http://t-ashbha/safelogin/Default.aspx
Live Search
Search web...
PC Health
Password Page
Page
Tools

Password : a

Submit

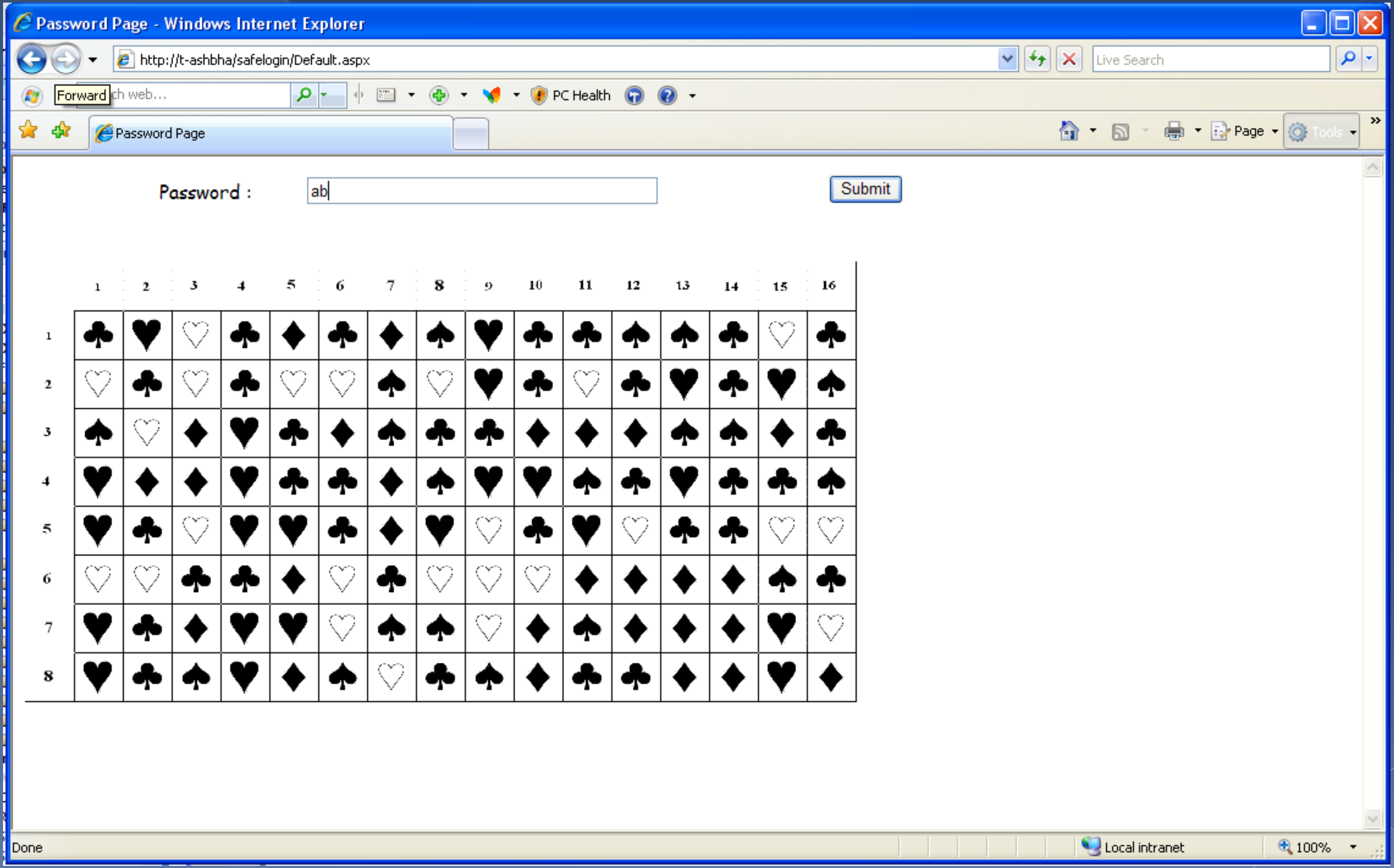
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	♡	♣	♡	♡	♥	♥	♠	♥	♠	♠	♠	♥	♣	♦	♥	♥
2	♠	♡	♡	♦	♣	♡	♡	♦	♥	♠	♣	♥	♠	♠	♡	♦
3	♠	♡	♡	♦	♡	♠	♠	♣	♦	♡	♡	♥	♣	♠	♦	♠
4	♠	♡	♦	♦	♠	♥	♥	♡	♥	♡	♦	♦	♠	♥	♡	♠
5	♠	♣	♣	♠	♦	♡	♠	♥	♥	♥	♡	♡	♠	♡	♣	♠
6	♡	♣	♦	♦	♥	♠	♠	♣	♡	♦	♥	♠	♦	♣	♦	♣
7	♠	♡	♣	♠	♦	♡	♥	♣	♣	♦	♠	♥	♠	♣	♥	♠
8	♦	♣	♣	♡	♦	♡	♥	♡	♥	♠	♠	♦	♦	♣	♦	♡

Done

Local intranet

100%

Login w/ method 1



Password Page - Windows Internet Explorer

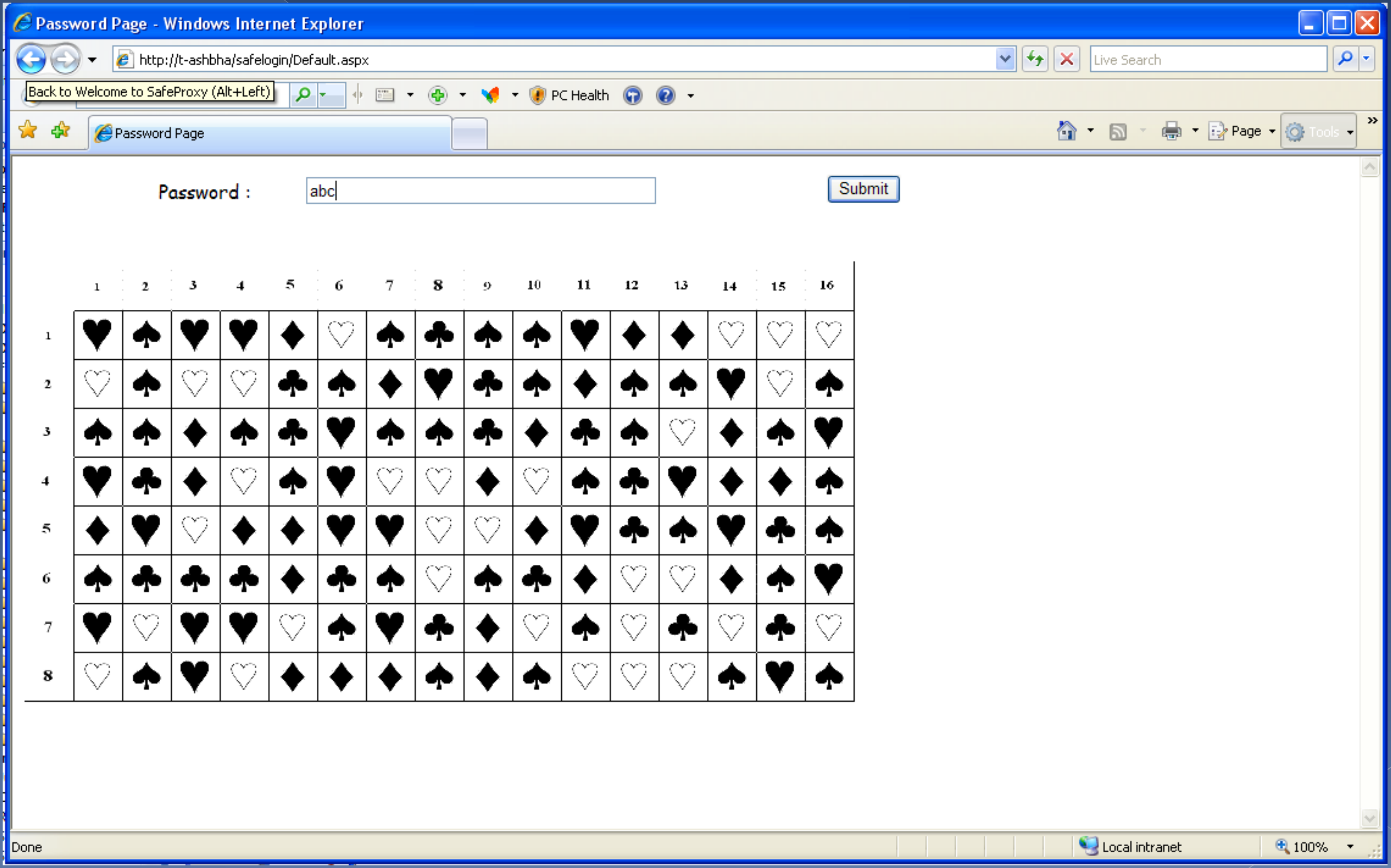
http://t-ashbha/safelogin/Default.aspx

Password : ab

Submit

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	♣	♥	♡	♣	♦	♣	♦	♠	♥	♣	♣	♠	♠	♣	♡	♣
2	♡	♣	♡	♣	♡	♡	♠	♡	♥	♣	♡	♣	♥	♣	♥	♠
3	♠	♡	♦	♥	♣	♦	♠	♣	♣	♦	♦	♦	♠	♠	♦	♣
4	♥	♦	♦	♥	♣	♣	♦	♠	♥	♥	♠	♣	♥	♣	♣	♠
5	♥	♣	♡	♥	♥	♣	♦	♥	♡	♣	♥	♡	♣	♣	♡	♡
6	♡	♡	♣	♣	♦	♡	♣	♡	♡	♡	♦	♦	♦	♦	♠	♣
7	♥	♣	♦	♥	♥	♡	♠	♠	♡	♦	♠	♦	♦	♦	♥	♡
8	♥	♣	♠	♥	♦	♠	♡	♣	♠	♦	♣	♣	♦	♦	♥	♦

Login w/ method 1


Password Page - Windows Internet Explorer
http://t-ashbha/safelogin/Default.aspx
Live Search
Back to Welcome to SafeProxy (Alt+Left)
PC Health
Password Page
Page
Tools
Done
Local intranet
100%

Password : abc

Submit

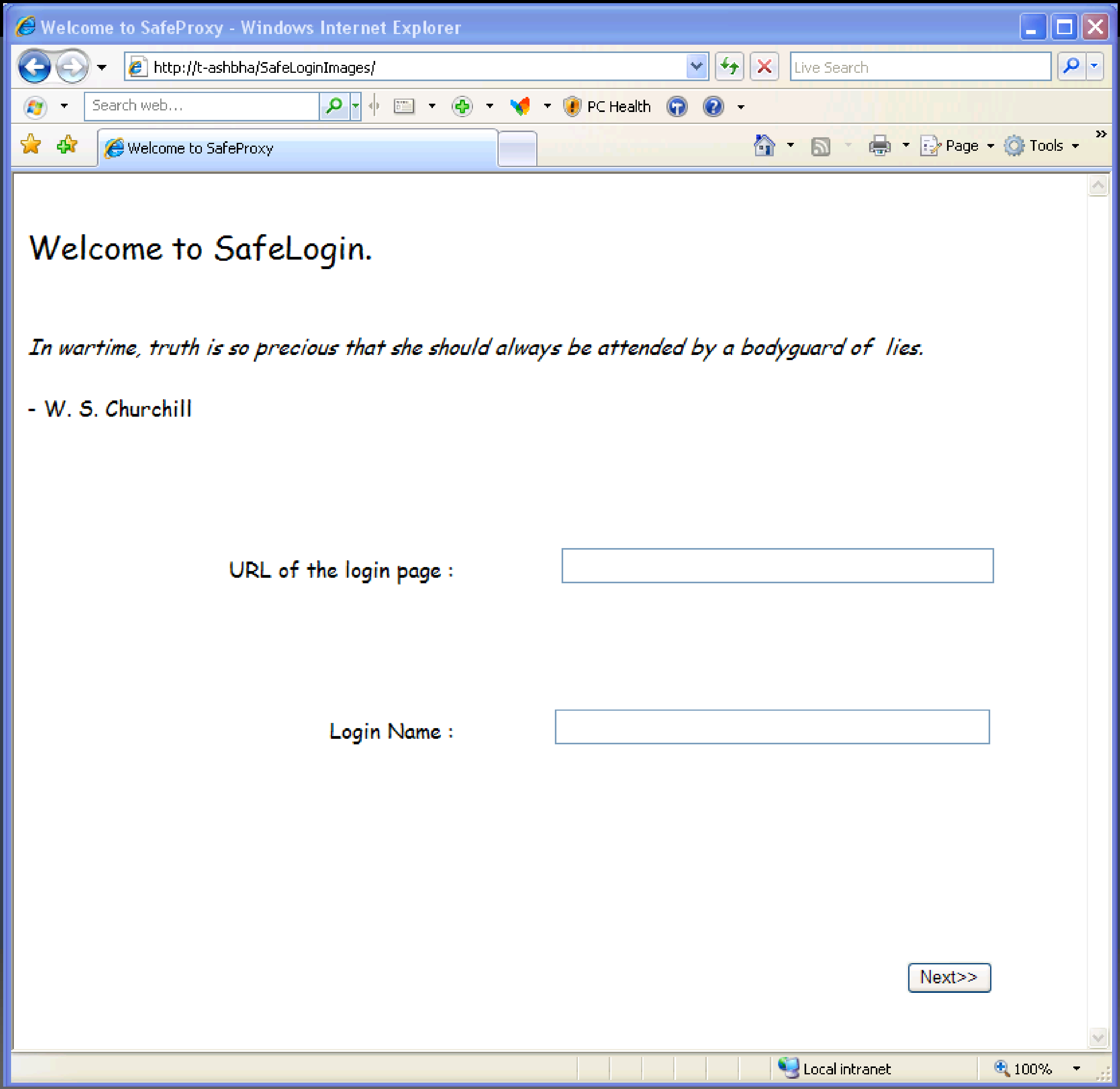
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	♥	♠	♥	♥	♦	♡	♠	♣	♠	♠	♥	♦	♦	♡	♡	♡
2	♡	♠	♡	♡	♣	♠	♦	♥	♣	♠	♦	♠	♠	♥	♡	♠
3	♠	♠	♦	♠	♣	♥	♠	♠	♣	♦	♣	♠	♡	♦	♠	♥
4	♥	♣	♦	♡	♠	♥	♡	♡	♦	♡	♠	♣	♥	♦	♦	♠
5	♦	♥	♡	♦	♦	♥	♥	♡	♡	♦	♥	♣	♠	♥	♣	♠
6	♠	♣	♣	♣	♦	♣	♠	♡	♠	♣	♦	♡	♡	♦	♠	♥
7	♥	♡	♥	♥	♡	♠	♥	♣	♦	♡	♠	♡	♣	♡	♣	♡
8	♡	♠	♥	♡	♦	♦	♦	♠	♦	♠	♡	♡	♡	♠	♥	♠

A few problems with METHOD 1

- Not safe enough: for a 8x16 table with 5 symbols, there are 640 options, entropy or visual inspection on these options may reveal the actual password;
- The Mouse problem: Several users left the mouse pointing at their assigned table location.
- The collusion problem: about 80% of users mistyped the password, and had to retype.

METHOD 2 (easiest to use)

- Before using:
  - setup a username (no PWD), and inform any "non-usual" sites you may want to visit
  - Upload some personal images/pictures



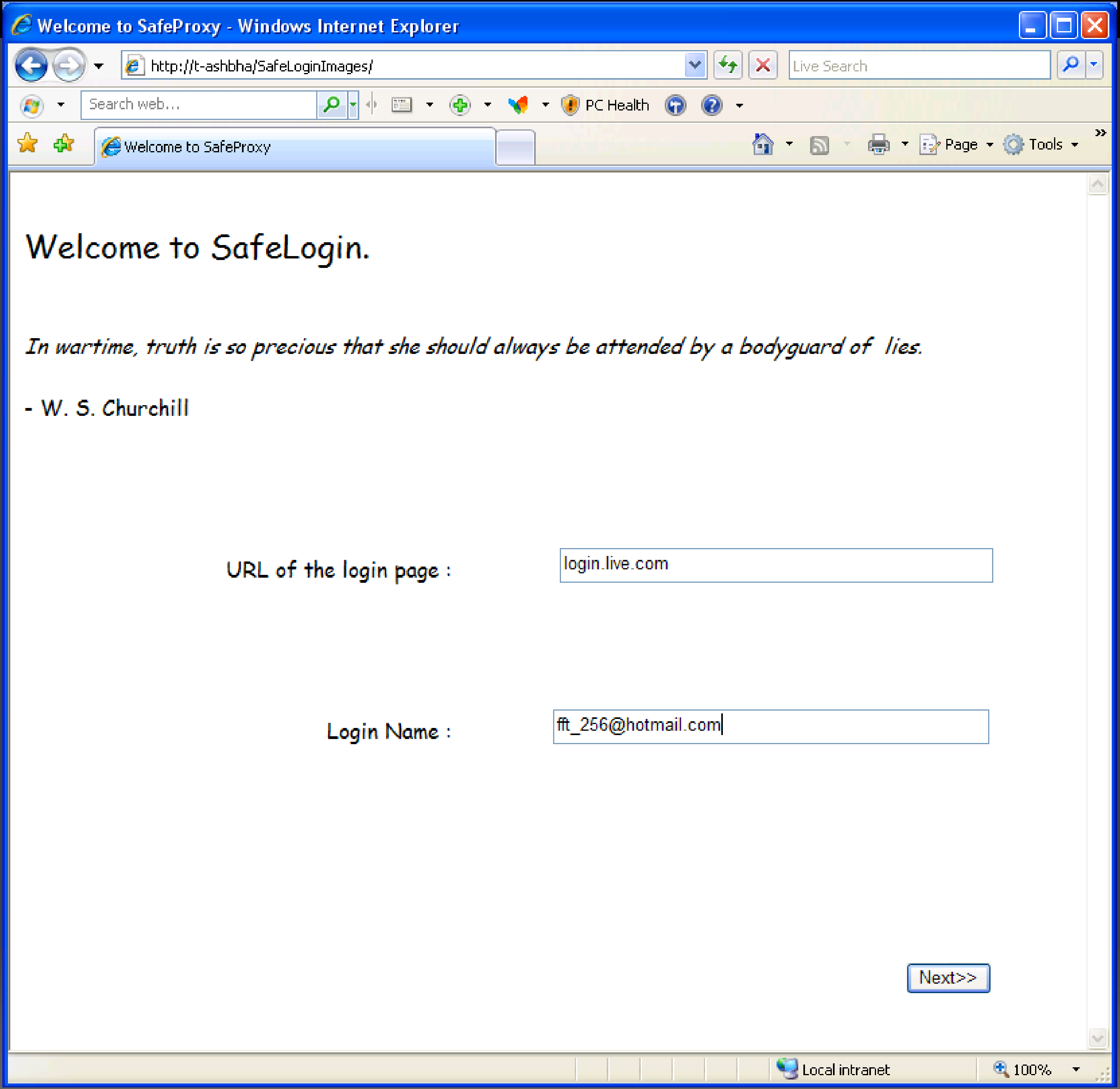
Welcome to SafeLogin.

In wartime, truth is so precious that she should always be attended by a bodyguard of lies.

- W. S. Churchill

URL of the login page :

Login Name :



Welcome to SafeProxy - Windows Internet Explorer
http://t-ashbha/SafeLoginImages/
Live Search
Search web...
PC Health
Welcome to SafeProxy
Page
Tools
Local intranet
100%

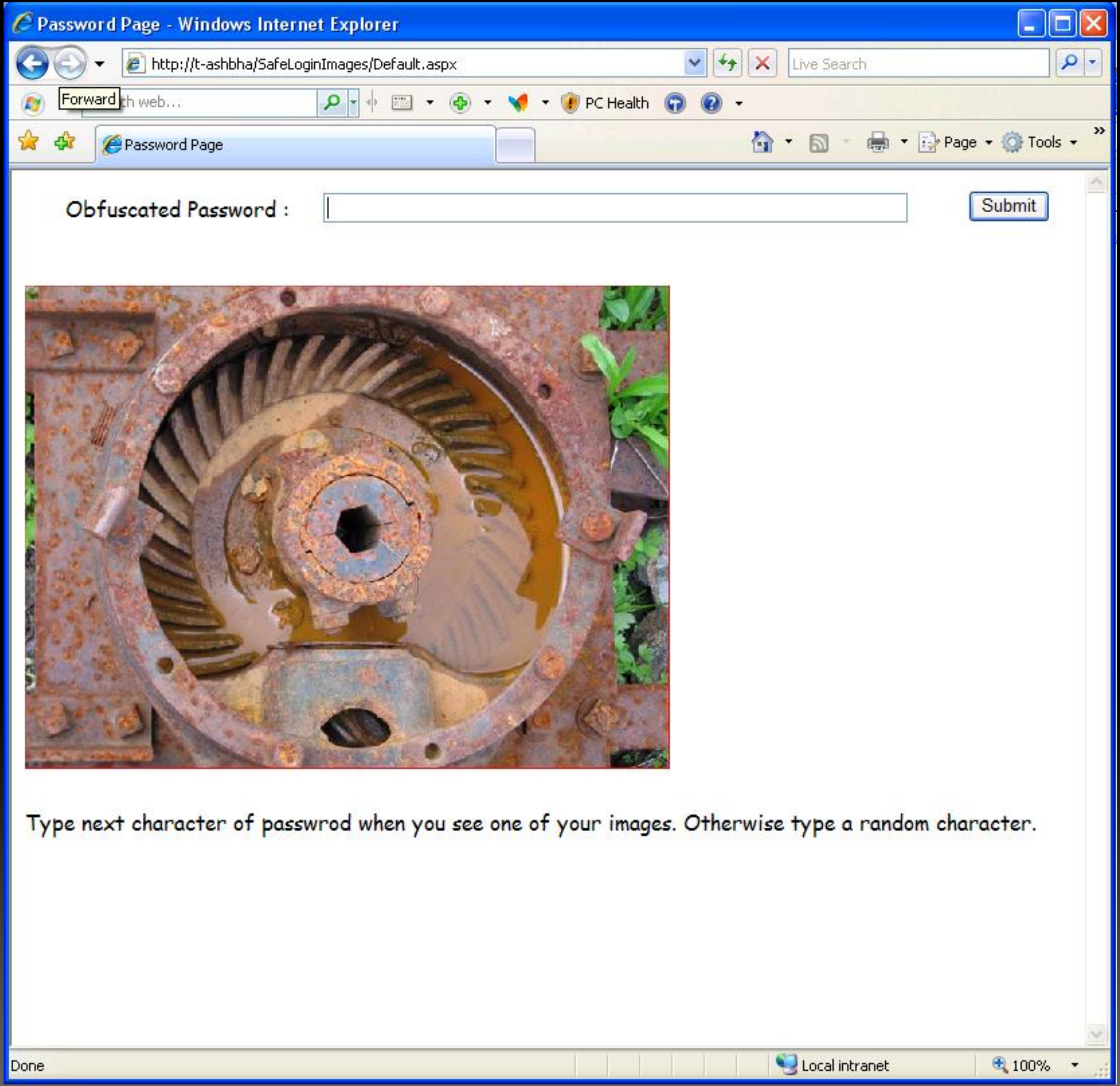
Welcome to SafeLogin.

In wartime, truth is so precious that she should always be attended by a bodyguard of lies.

- W. S. Churchill

URL of the login page : login.live.com

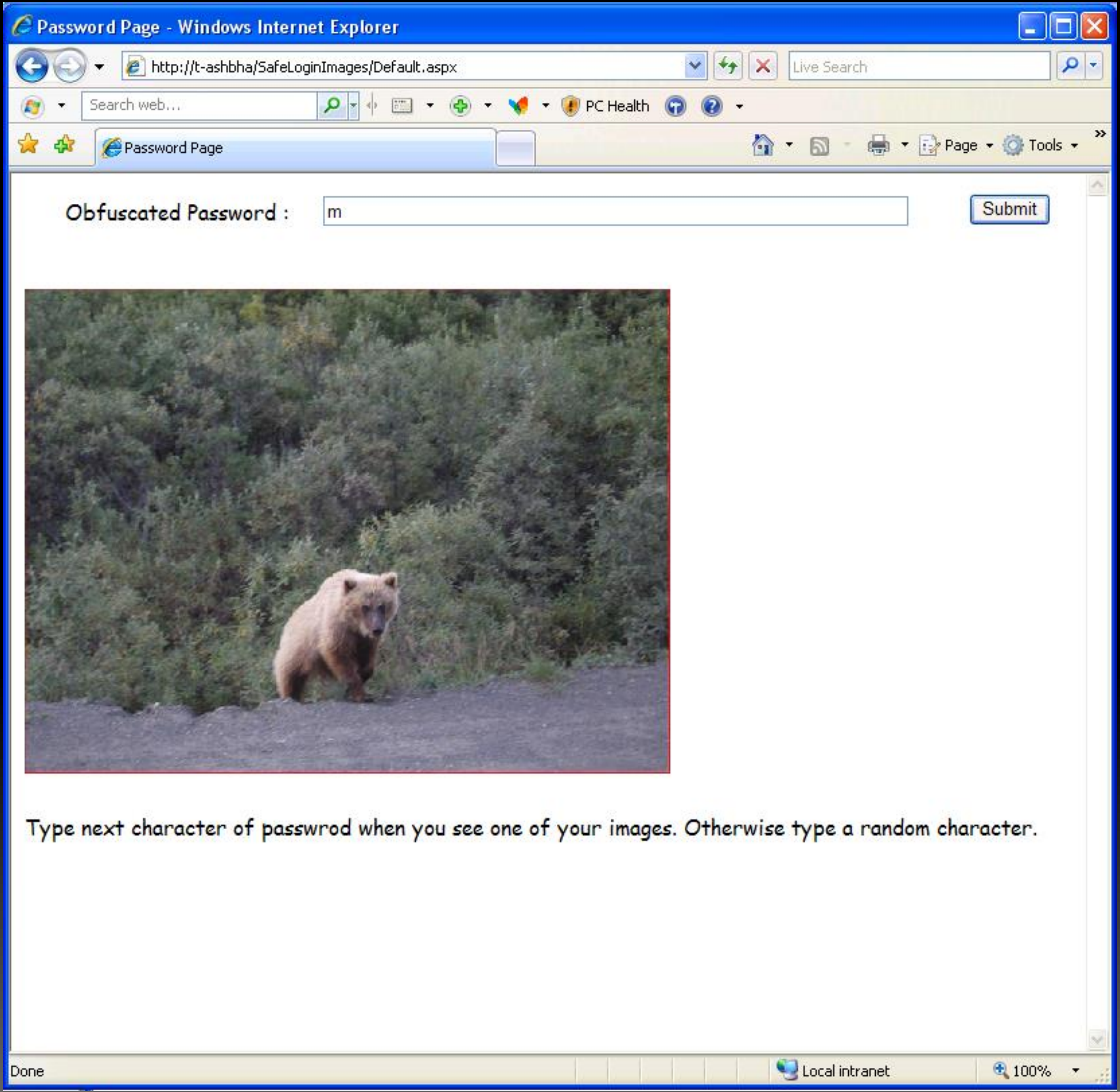
Login Name : fft_256@hotmail.com


Password Page - Windows Internet Explorer
http://t-ashbha/SafeLoginImages/Default.aspx
Live Search
Forward
h web...
PC Health
Password Page
Page
Tools
Done
Local intranet
100%

Obfuscated Password :

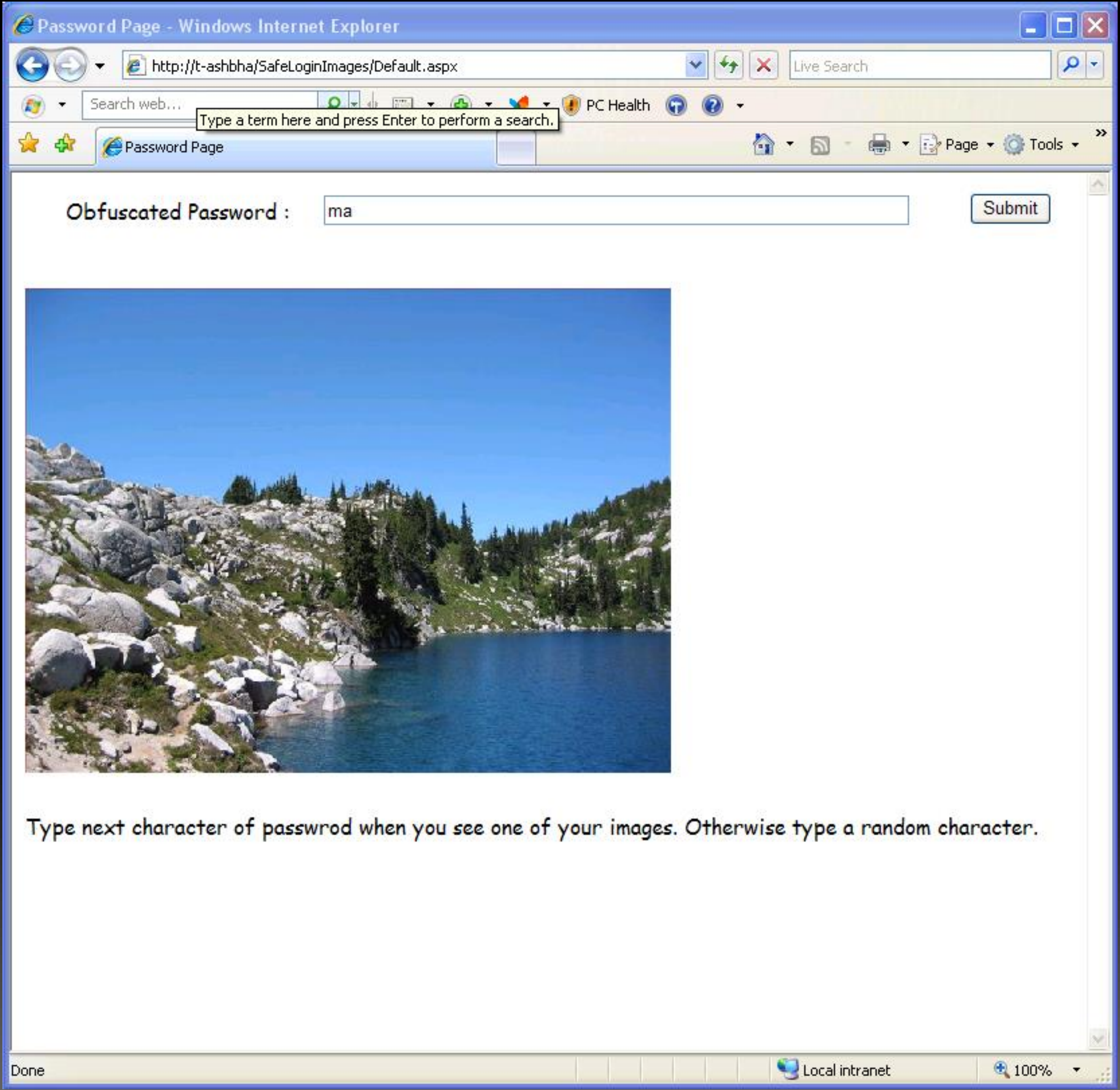
Submit

Type next character of passwrod when you see one of your images. Otherwise type a random character.


Password Page - Windows Internet Explorer
http://t-ashbha/SafeLoginImages/Default.aspx
Live Search
Search web...
PC Health
Password Page
Page
Tools
Submit
Done
Local intranet
100%

Obfuscated Password : m

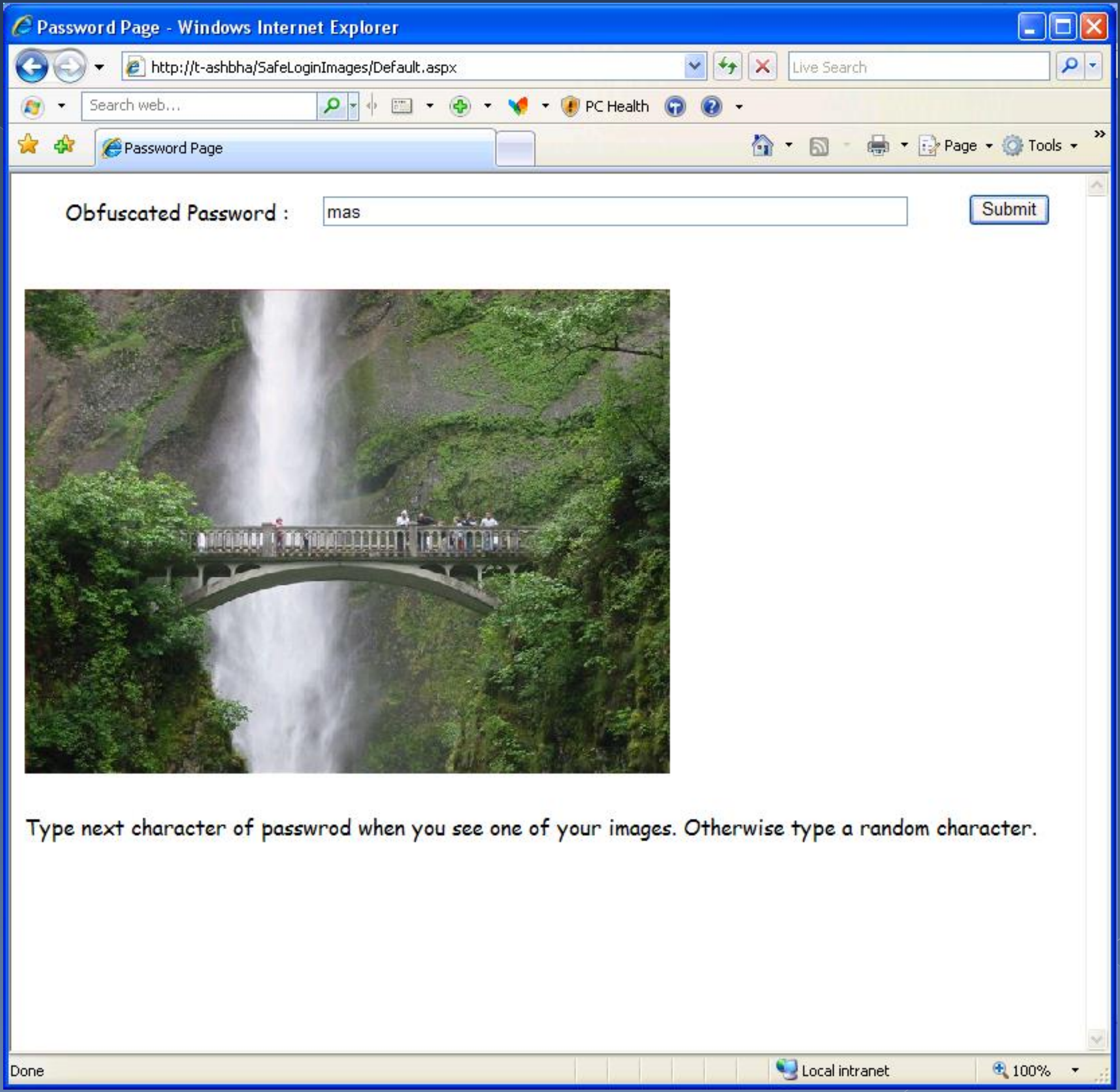
Type next character of passwrod when you see one of your images. Otherwise type a random character.


Password Page - Windows Internet Explorer
http://t-ashbha/SafeLoginImages/Default.aspx
Live Search
Search web...
PC Health
Password Page
Page
Tools
Submit
Done
Local intranet
100%

Type a term here and press Enter to perform a search.

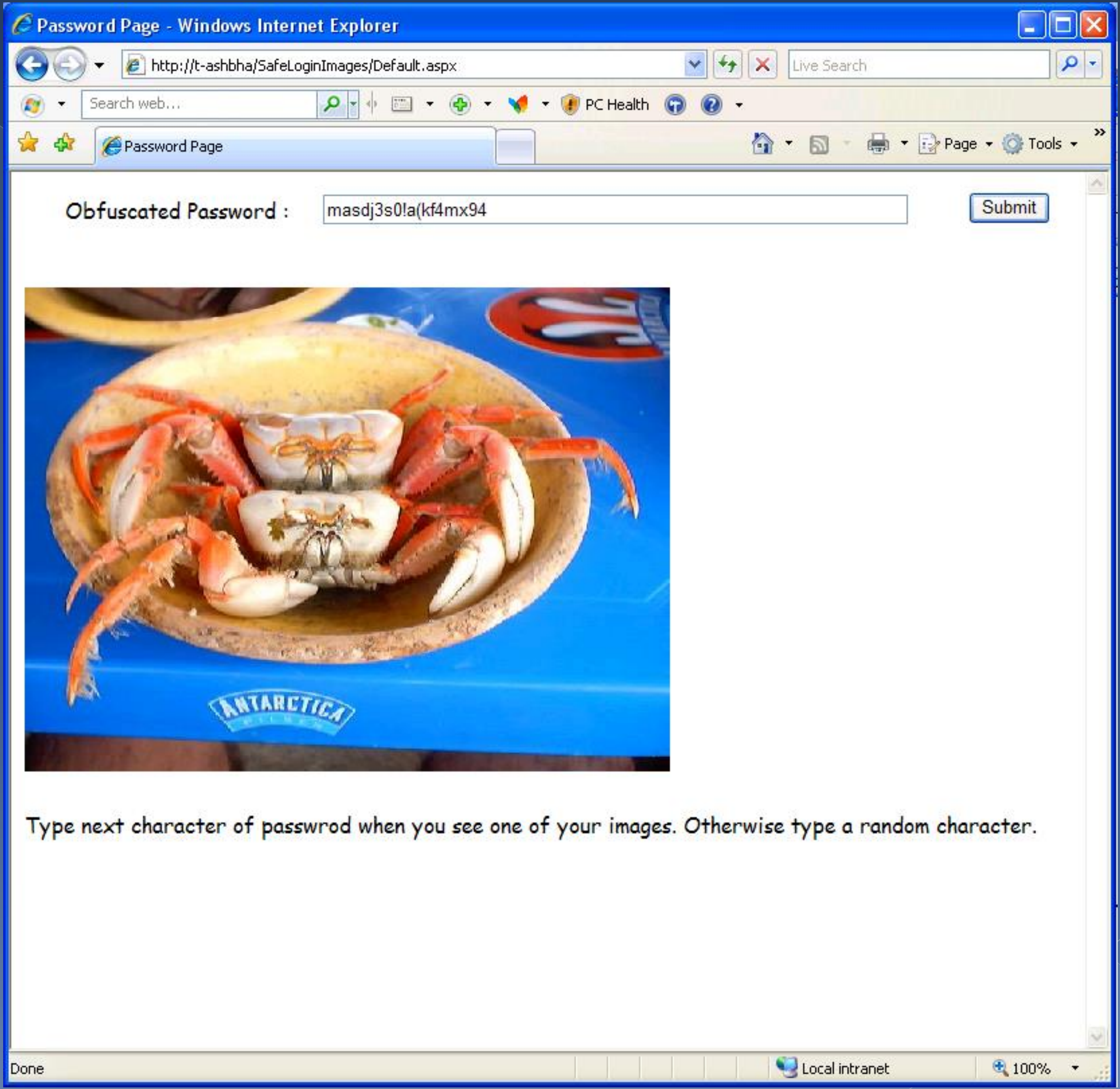
Obfuscated Password : ma

Type next character of passwrod when you see one of your images. Otherwise type a random character.


Password Page - Windows Internet Explorer
http://t-ashbha/SafeLoginImages/Default.aspx
Live Search
Search web...
PC Health
Password Page
Page
Tools
Submit
Done
Local intranet
100%

Obfuscated Password : mas

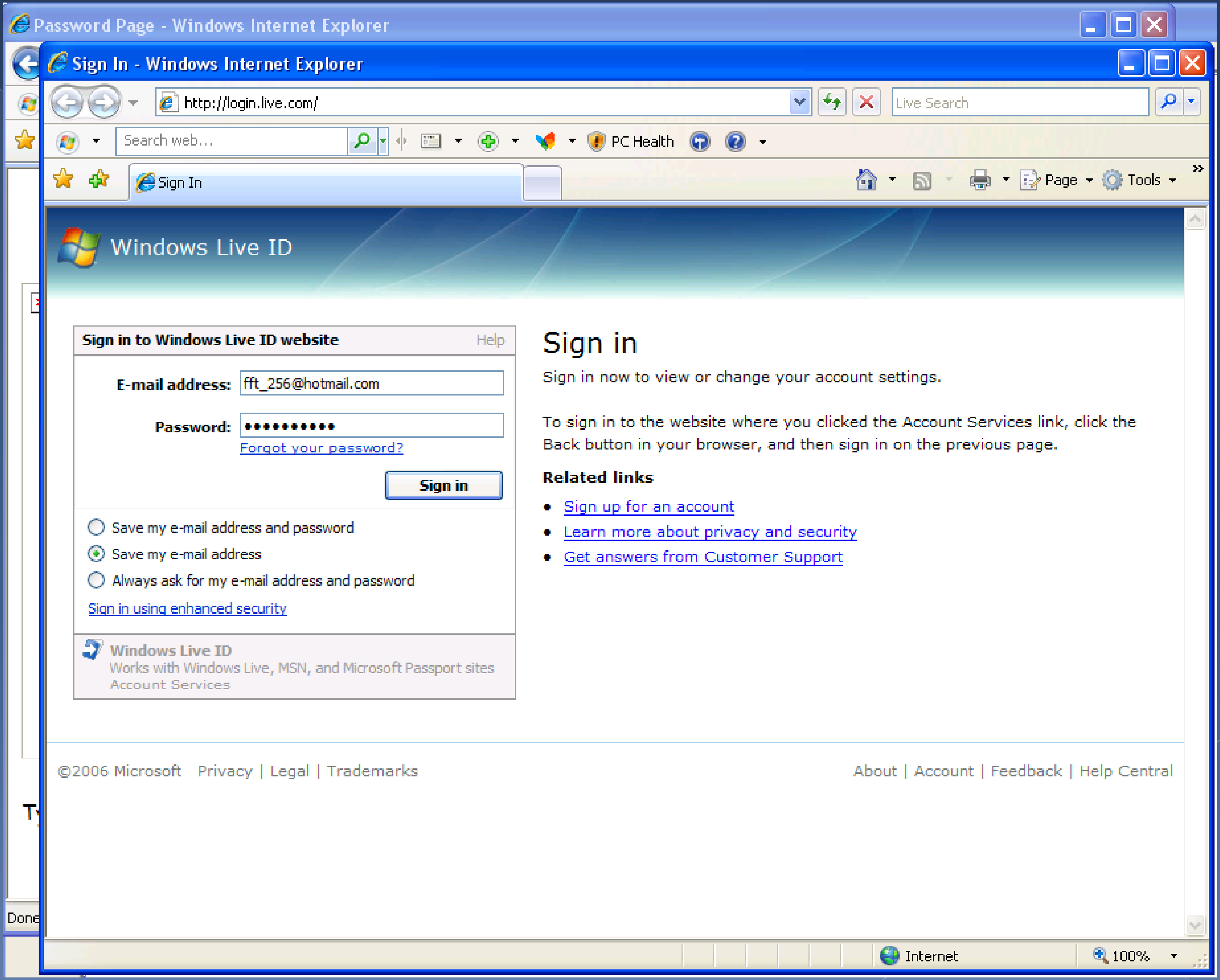
Type next character of passwrod when you see one of your images. Otherwise type a random character.



http://t-ashbha/SafeLoginImages/Default.aspx

Obfuscated Password : masdj3s0!a(kf4mx94

Type next character of passwrod when you see one of your images. Otherwise type a random character.



Password Page - Windows Internet Explorer

Sign In - Windows Internet Explorer

http://login.live.com/

Windows Live ID

Sign in to Windows Live ID website

E-mail address: fft_256@hotmail.com

Password: ••••••••••

Forgot your password?

○ Save my e-mail address and password
● Save my e-mail address
○ Always ask for my e-mail address and password

Sign in using enhanced security

Windows Live ID
Works with Windows Live, MSN, and Microsoft Passport sites
Account Services

Sign in

Sign in now to view or change your account settings.

To sign in to the website where you clicked the Account Services link, click the Back button in your browser, and then sign in on the previous page.

Related links

- Sign up for an account
- Learn more about privacy and security
- Get answers from Customer Support

©2006 Microsoft Privacy | Legal | Trademarks About | Account | Feedback | Help Central

A few points about METHOD 2

- Safer than Method 1, but entropy still not as high as original password (only need to figure out which characters are part of password, about ~3bits per character);
- Success rate above 95%.

METHOD 3 (safest)

- Before using:
  - Request a UserNumber, and inform any "non-usual" sites you may want to visit;
  - Download and print an encryption table for future use.

Sample Table

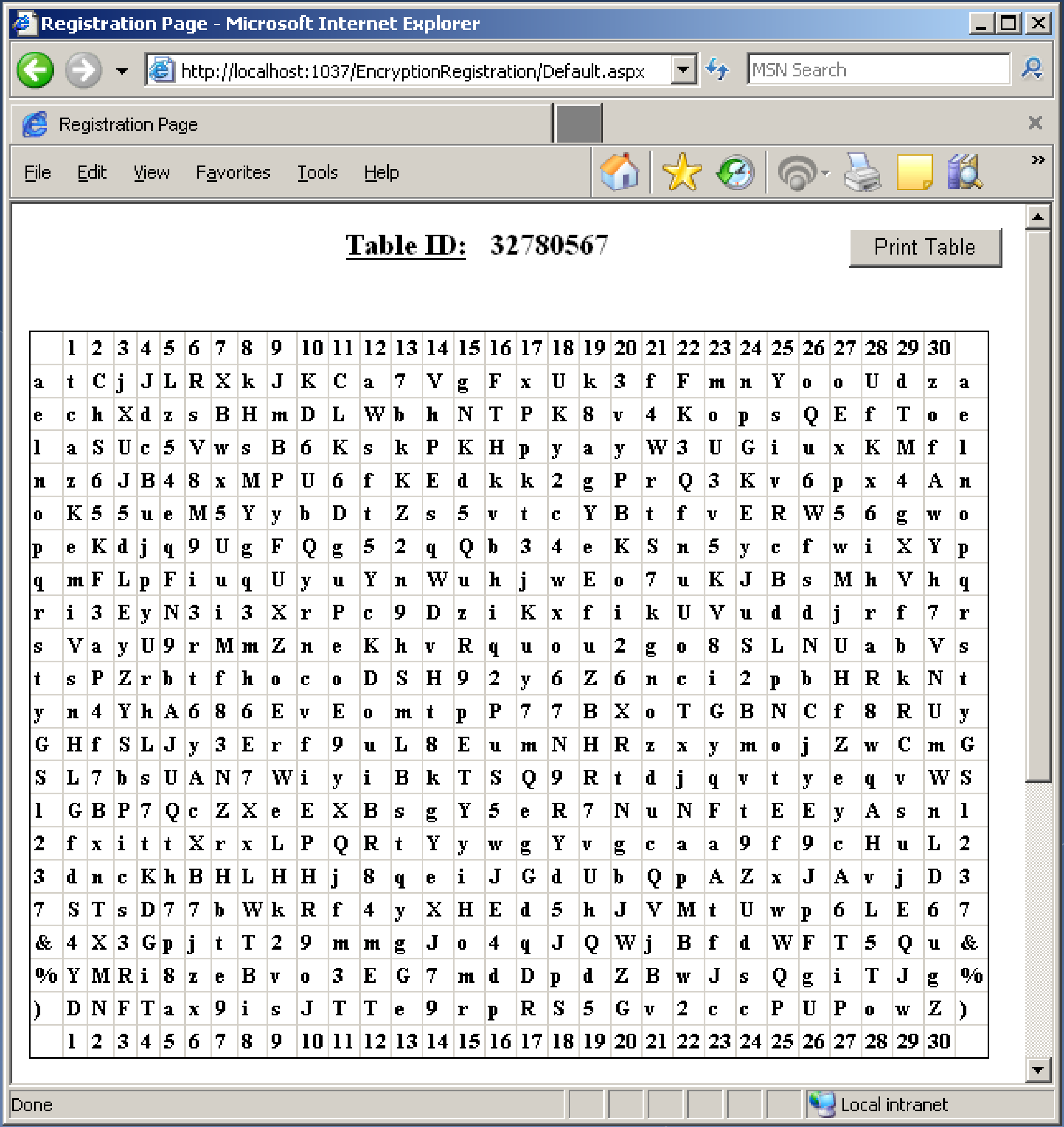

Registration Page - Microsoft Internet Explorer
http://localhost:1037/EncryptionRegistration/Default.aspx
MSN Search
Registration Page
File
Edit
View
Favorites
Tools
Help
Print Table
Done
Local intranet

Table ID: 32780567

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
a	t	C	j	J	L	R	X	k	J	K	C	a	7	V	g	F	x	U	k	3	f	F	m	n	Y	o	o	U	d	z	a
e	c	h	X	d	z	s	B	H	m	D	L	W	b	h	N	T	P	K	8	v	4	K	o	p	s	Q	E	f	T	o	e
l	a	S	U	c	5	V	w	s	B	6	K	s	k	P	K	H	p	y	a	y	W	3	U	G	i	u	x	K	M	f	l
n	z	6	J	B	4	8	x	M	P	U	6	f	K	E	d	k	k	2	g	P	r	Q	3	K	v	6	p	x	4	A	n
o	K	5	5	u	e	M	5	Y	y	b	D	t	Z	s	5	v	t	c	Y	B	t	f	v	E	R	W	5	6	g	w	o
p	e	K	d	j	q	9	U	g	F	Q	g	5	2	q	Q	b	3	4	e	K	S	n	5	y	c	f	w	i	X	Y	p
q	m	F	L	p	F	i	u	q	U	y	u	Y	n	W	u	h	j	w	E	o	7	u	K	J	B	s	M	h	V	h	q
r	i	3	E	y	N	3	i	3	X	r	P	c	9	D	z	i	K	x	f	i	k	U	V	u	d	d	j	r	f	7	r
s	V	a	y	U	9	r	M	m	Z	n	e	K	h	v	R	q	u	o	u	2	g	o	8	S	L	N	U	a	b	V	s
t	s	P	Z	r	b	t	f	h	o	c	o	D	S	H	9	2	y	6	Z	6	n	c	i	2	p	b	H	R	k	N	t
y	n	4	Y	h	A	6	8	6	E	v	E	o	m	t	p	P	7	7	B	X	o	T	G	B	N	C	f	8	R	U	y
G	H	f	S	L	J	y	3	E	r	f	9	u	L	8	E	u	m	N	H	R	z	x	y	m	o	j	Z	w	C	m	G
S	L	7	b	s	U	A	N	7	W	i	y	i	B	k	T	S	Q	9	R	t	d	j	q	v	t	y	e	q	v	W	S
l	G	B	P	7	Q	c	Z	X	e	E	X	B	s	g	Y	5	e	R	7	N	u	N	F	t	E	E	y	A	s	n	l
2	f	x	i	t	t	X	r	x	L	P	Q	R	t	Y	y	w	g	Y	v	g	c	a	a	9	f	9	c	H	u	L	2
3	d	n	c	K	h	B	H	L	H	H	j	8	q	e	i	J	G	d	U	b	Q	p	A	Z	x	J	A	v	j	D	3
7	S	T	s	D	7	7	b	W	k	R	f	4	y	X	H	E	d	5	h	J	V	M	t	U	w	p	6	L	E	6	7
&	4	X	3	G	p	j	t	T	2	9	m	m	g	J	o	4	q	J	Q	W	j	B	f	d	W	F	T	5	Q	u	&
%	Y	M	R	i	8	z	e	B	v	o	3	E	G	7	m	d	D	p	d	Z	B	w	J	s	Q	g	i	T	J	g	%
)	D	N	F	T	a	x	9	i	s	J	T	T	e	9	r	p	R	S	5	G	v	2	c	c	P	U	P	o	w	Z	)
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	

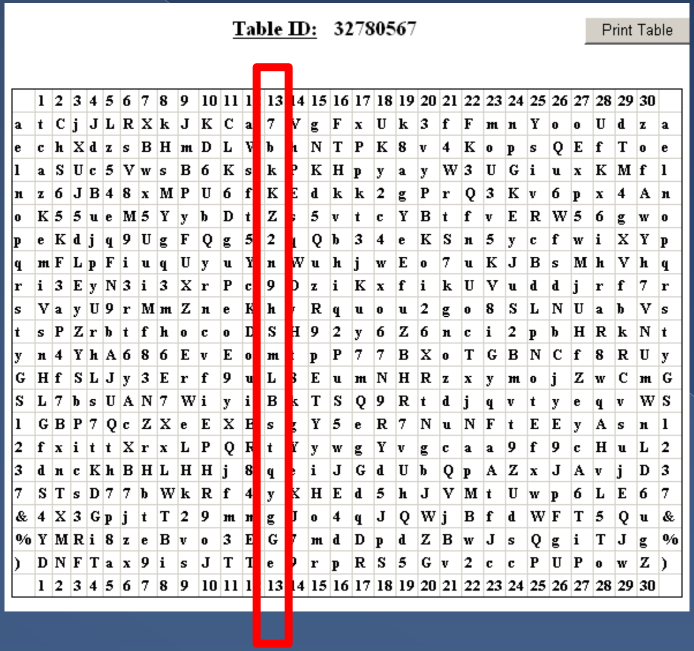
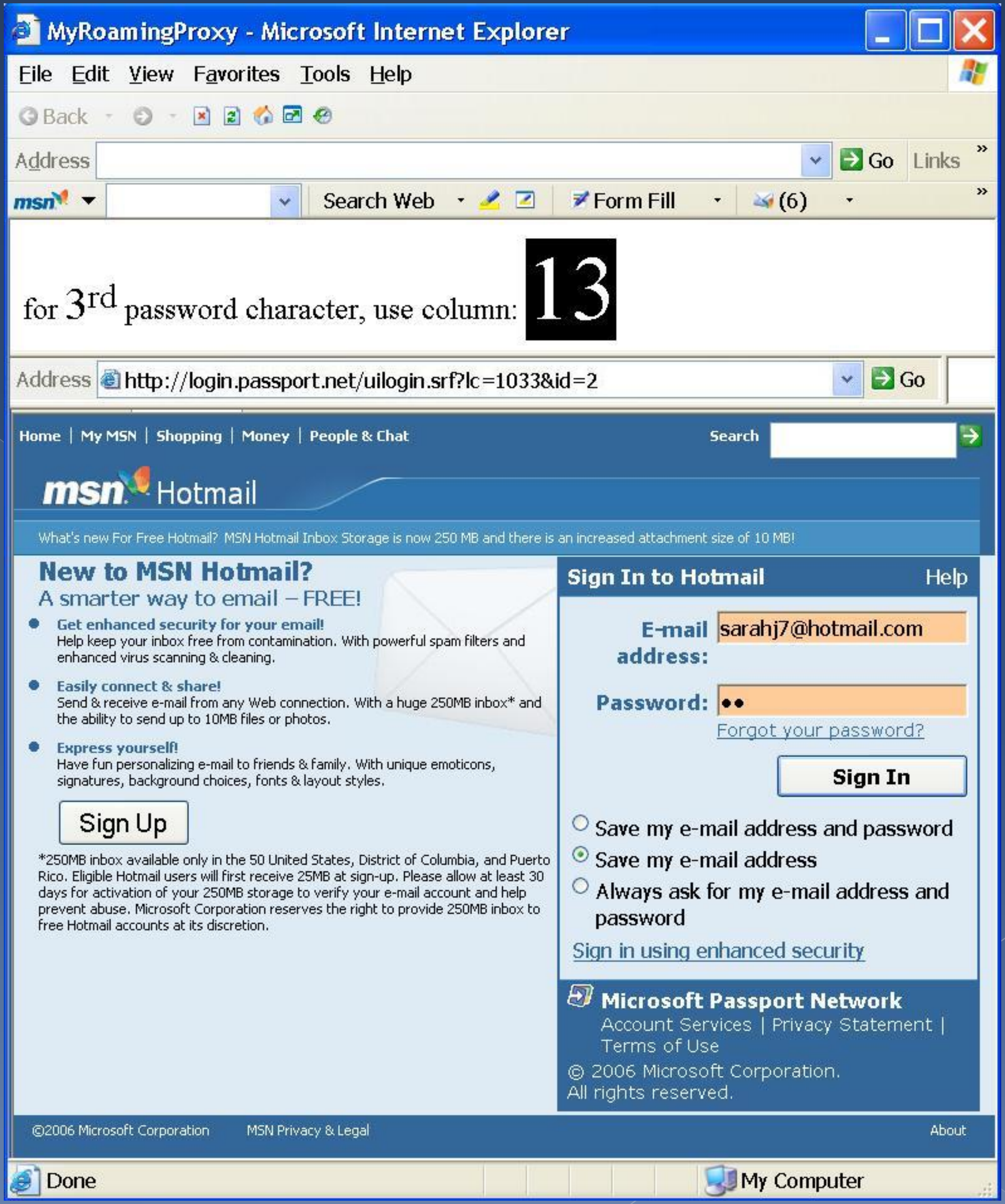


Table ID: 32780567

Print Table

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
a	t	C	j	J	L	R	X	k	J	K	C	a	7	V	g	F	x	U	k	3	f	F	m	n	Y	o	o	U	d	z	a
e	c	h	X	d	z	s	B	H	m	D	L	W	b	n	N	T	P	K	8	v	4	K	o	p	s	Q	E	f	T	o	e
l	a	S	U	c	5	V	w	s	B	6	K	s	k	P	K	H	p	y	a	y	W	3	U	G	i	u	x	K	M	f	l
n	z	6	J	B	4	8	x	M	P	U	6	f	K	E	d	k	k	2	g	P	r	Q	3	K	v	6	p	x	4	A	n
o	K	5	5	u	e	M	5	Y	y	b	D	t	Z	s	5	v	t	c	Y	B	t	f	v	E	R	W	5	6	g	w	o
p	e	K	d	j	q	9	U	g	F	Q	g	5	2	q	Q	b	3	4	e	K	S	n	5	y	c	f	w	i	X	Y	p
q	m	F	L	p	F	i	u	q	U	y	u	Y	n	W	u	h	j	w	E	o	7	u	K	J	B	s	M	h	V	h	q
r	i	3	E	y	N	3	i	3	X	r	P	c	9	D	z	i	K	x	f	i	k	U	V	u	d	d	j	r	f	7	r
s	V	a	y	U	9	r	M	m	Z	n	e	K	h	v	R	q	u	o	u	2	g	o	8	S	L	N	U	a	b	V	s
t	s	P	Z	r	b	t	f	h	o	c	o	D	S	H	9	2	y	6	Z	6	n	c	i	2	p	b	H	R	k	N	t
y	n	4	Y	h	A	6	8	6	E	v	E	o	m	t	p	P	7	7	B	X	o	T	G	B	N	C	f	8	R	U	y
G	H	f	S	L	J	y	3	E	r	f	9	u	L	B	E	u	m	N	H	R	z	x	y	m	o	j	Z	w	C	m	G
S	L	7	b	s	U	A	N	7	W	i	y	i	B	k	T	S	Q	9	R	t	d	j	q	v	t	y	e	q	v	W	S
l	G	B	P	7	Q	c	Z	X	e	E	X	B	s	g	Y	5	e	R	7	N	u	N	F	t	E	E	y	A	s	n	l
2	f	x	i	t	t	X	r	x	L	P	Q	R	t	Y	y	w	g	Y	v	g	c	a	a	9	f	9	c	H	u	L	2
3	d	n	c	K	h	B	H	L	H	H	j	8	q	e	i	J	G	d	U	b	Q	p	A	Z	x	J	A	v	j	D	3
7	S	T	s	D	7	7	b	W	k	R	f	4	y	X	H	E	d	5	h	J	V	M	t	U	w	p	6	L	E	6	7
&	4	X	3	G	p	j	t	T	2	9	m	m	g	J	o	4	q	J	Q	W	j	B	f	d	W	F	T	5	Q	u	&
%	Y	M	R	i	8	z	e	B	v	o	3	E	G	7	m	d	D	p	d	Z	B	w	J	s	Q	g	i	T	J	g	%
)	D	N	F	T	a	x	9	i	s	J	T	T	e	9	r	p	R	S	5	G	v	2	c	c	P	U	P	o	w	Z	)
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	



MyRoamingProxy - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address
Go
Links
msn
Search Web
Form Fill
(6)

for 3rd password character, use column: 13

Address http://login.passport.net/uilogin.srf?lc=1033&id=2

Go
Home | My MSN | Shopping | Money | People & Chat
Search
msn Hotmail

What's new For Free Hotmail? MSN Hotmail Inbox Storage is now 250 MB and there is an increased attachment size of 10 MB!

New to MSN Hotmail?

A smarter way to email – FREE!

- **Get enhanced security for your email!** Help keep your inbox free from contamination. With powerful spam filters and enhanced virus scanning & cleaning.
- **Easily connect & share!** Send & receive e-mail from any Web connection. With a huge 250MB inbox* and the ability to send up to 10MB files or photos.
- **Express yourself!** Have fun personalizing e-mail to friends & family. With unique emoticons, signatures, background choices, fonts & layout styles.

*250MB inbox available only in the 50 United States, District of Columbia, and Puerto Rico. Eligible Hotmail users will first receive 25MB at sign-up. Please allow at least 30 days for activation of your 250MB storage to verify your e-mail account and help prevent abuse. Microsoft Corporation reserves the right to provide 250MB inbox to free Hotmail accounts at its discretion.

Sign In to Hotmail Help

E-mail address: sarahj7@hotmail.com

Password: ●●

Forgot your password?

○ Save my e-mail address and password
● Save my e-mail address
○ Always ask for my e-mail address and password

Sign in using enhanced security

Microsoft Passport Network

Account Services | Privacy Statement | Terms of Use

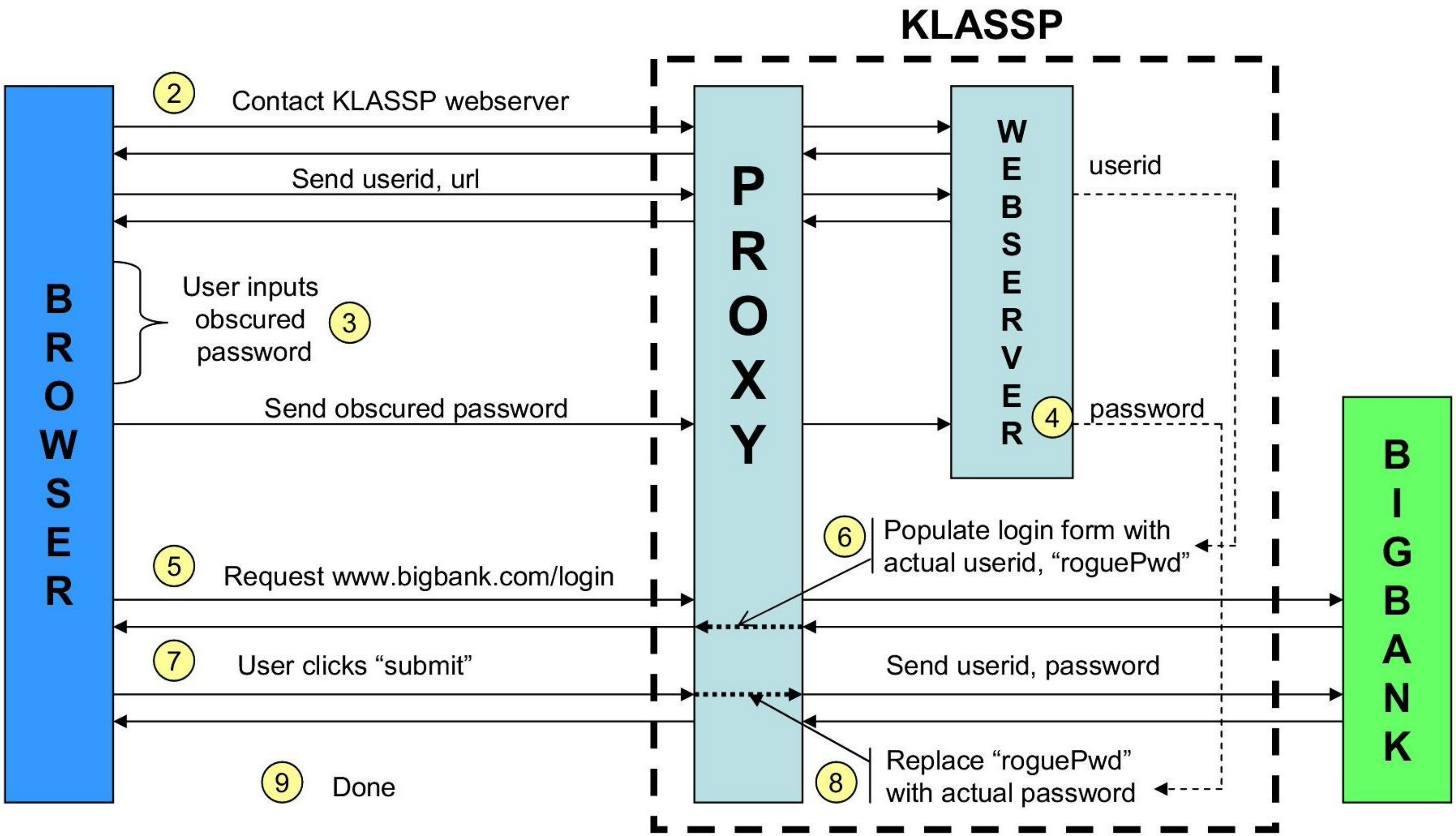
© 2006 Microsoft Corporation. All rights reserved.

©2006 Microsoft Corporation MSN Privacy & Legal About

A few points about METHOD 3

- Entropy ~ as high as original password;
- Success rate around 75%, but collision not a problem anymore;
- Harder to use of all three;
- Requires pre-printing encryption table.

Implementation



Future work

- Implement as reverse proxy, ie, be able to type http://proxy:port/www.cnn.com to go to cnn through the proxy.

- NOTE: right now need to change the settings in the browser to point at the proxy.

Conclusions

- Shared-secret Proxy helps make it harder to capture passwords.
- No prior uploading of PWDs;
- Little setup or maintenance;
- Never 100% safe.

References

(back- and forward-pointing references)

[1] Dinei Florencio and Cormac Herley, KLASSP: Entering Passwords on a Spyware Infected Machine Using a Shared-Secret Proxy, Association for Computing Machinery, Inc., December 2006.

[2] Dinei Florencio and Cormac Herley, Password Rescue: A New Approach to Phishing Prevention, USENIX, July 2006.

[3] Dinei Florencio and Cormac Herley, How to Login from an Internet Cafe Without Worrying about Keyloggers, Association for Computing Machinery, Inc., July 2006.

[4] Dinei Florencio and Cormac Herley, Stopping a Phishing Attack, Even when the Victims Ignore Warnings, MSR Tech Report, October 2005.

[5] Dinei Florencio and Cormac Herley, Analyzing and Improving Anti-Phishing Schemes," *Security and Privacy in Dynamic Environments*. Springer US, 2006. 148-157.

[6] Dinei Florencio and Cormac Herley, A Large-Scale Study of Web Password Habits, in *preparation*.

[7] Dinei Florencio, Cormac Herley, and Baris Coskun, Do Strong Web Passwords Accomplish Anything?, in *preparation*.

[8] Dinei Florencio and Cormac Herley, Evaluating a Trial Deployment of Password Re-Use for Phishing Prevention, in *preparation*.

[9] Dinei Florencio and Cormac Herley, One Time Password Access to Any Server without Changing the Server, Springer Verlag, September 2008.

[10] Cormac Herley and Dinei Florencio, Protecting Financial Institutions from Brute-Force Attacks, in *Proc. 23rd International Information Security Conference (SEC 2008)*, Springer-Verlag, September 2008.

[11] Cormac Herley and Dinei Florencio, A Profitless Endeavor: Phishing as Tragedy of the Commons, in *Proc. New Security Paradigms Workshop*, Association for Computing Machinery, Inc., September 2008.

[12] Dinei Florencio and Cormac Herley, Where Do Security Policies Come From?, in *SOUPS*, June 2010.

[13] Cormac Herley and Dinei Florencio, Phishing and Money Mules, in *WIFS*, 2010.

[14] Ziqing Mao, Dinei Florencio, and Cormac Herley, Painless Migration from Passwords to Two Factor Authentication, in *WIFS*, IEEE SPS, 29 November 2011.

[15] D. Florencio and C. Herley, "Where Do All the Attacks Go?" WEIS 2011

[16] D. Florencio and C. Herley, "Sex, Lies and Cyber-crime Surveys," [slides] WEIS 2011

[17] Dinei Florencio and Cormac Herley, Is Everything We Know About Password Stealing Wrong?, in *IEEE Security and Privacy magazine*, 2012.

[18] Dinei Florencio, Cormac Herley, and Paul C. van Oorschot, An Administrator's Guide to Internet Password Research, in *Usenix LISA*, USENIX – Advanced Computing Systems Association, November 2014.

[19] Dinei Florencio, Cormac Herley, and Paul C. van Oorschot, Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts, in *Usenix Security*, August 2014.

[20] Dinei Florencio, Cormac Herley, and Adam Shostack, FUD: A Plea for Intolerance, in *Communications ACM*, June 2014.