

GNUCITIZEN

<http://www.gnucitizen.org>

Before We Begin

- Feel free to ask questions!
- Do ask questions!
- Embrace the mindset rather than the tech!
- Have Fun!

CLIENT vs. SERVER

Server-side Issues

- Occurs on the Server!
- Compromises the business logic!
- Compromises the data!
- Compromises the user!
- More severe!
- Less likely to occur!
- Less agile!

Client-side Issues

- Occurs on the Client
- Compromises the client-side business logic!
- Compromises the client-side data!
- Compromises the user!
- Less severe! (individual cases)
- More likely to occur!
- More agile!

Trends



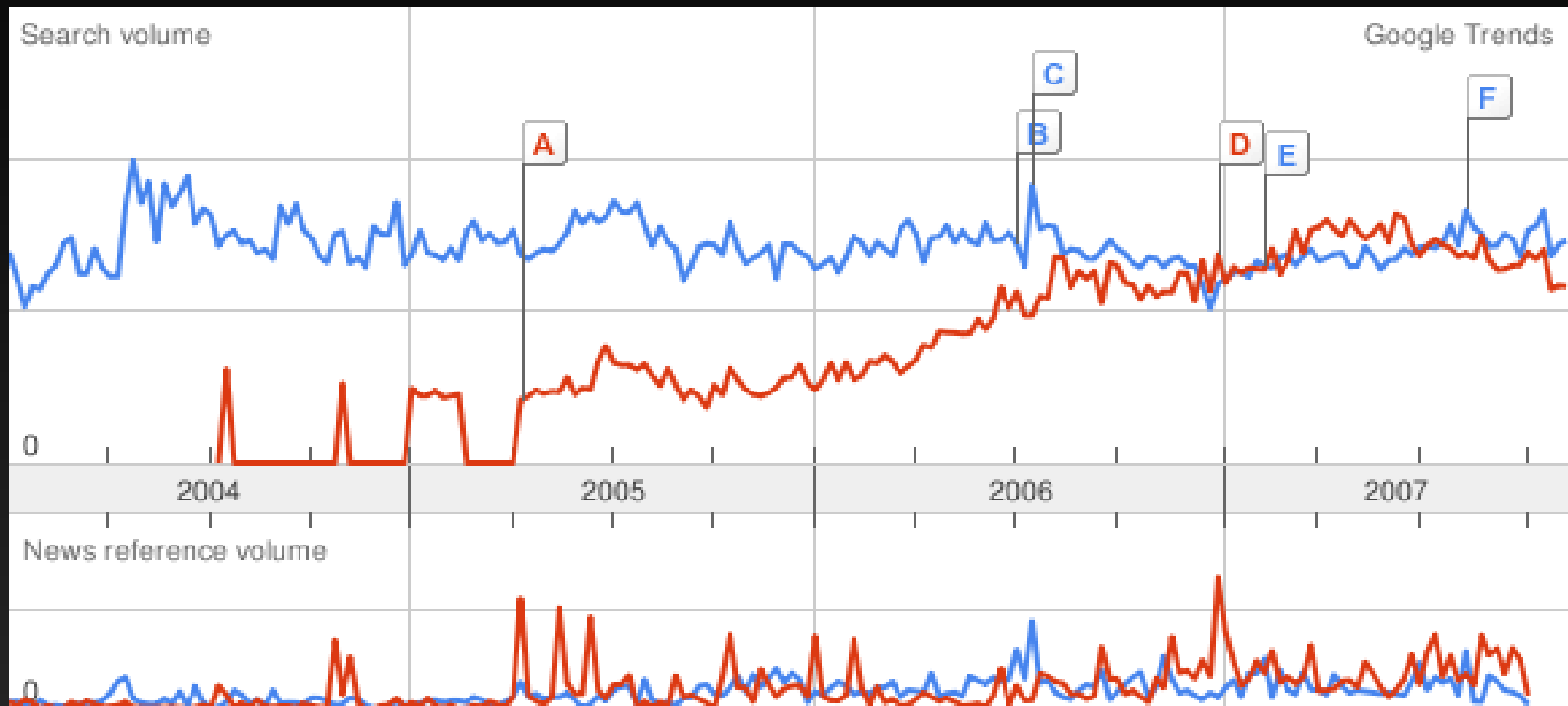
server-side



client-side



Trends



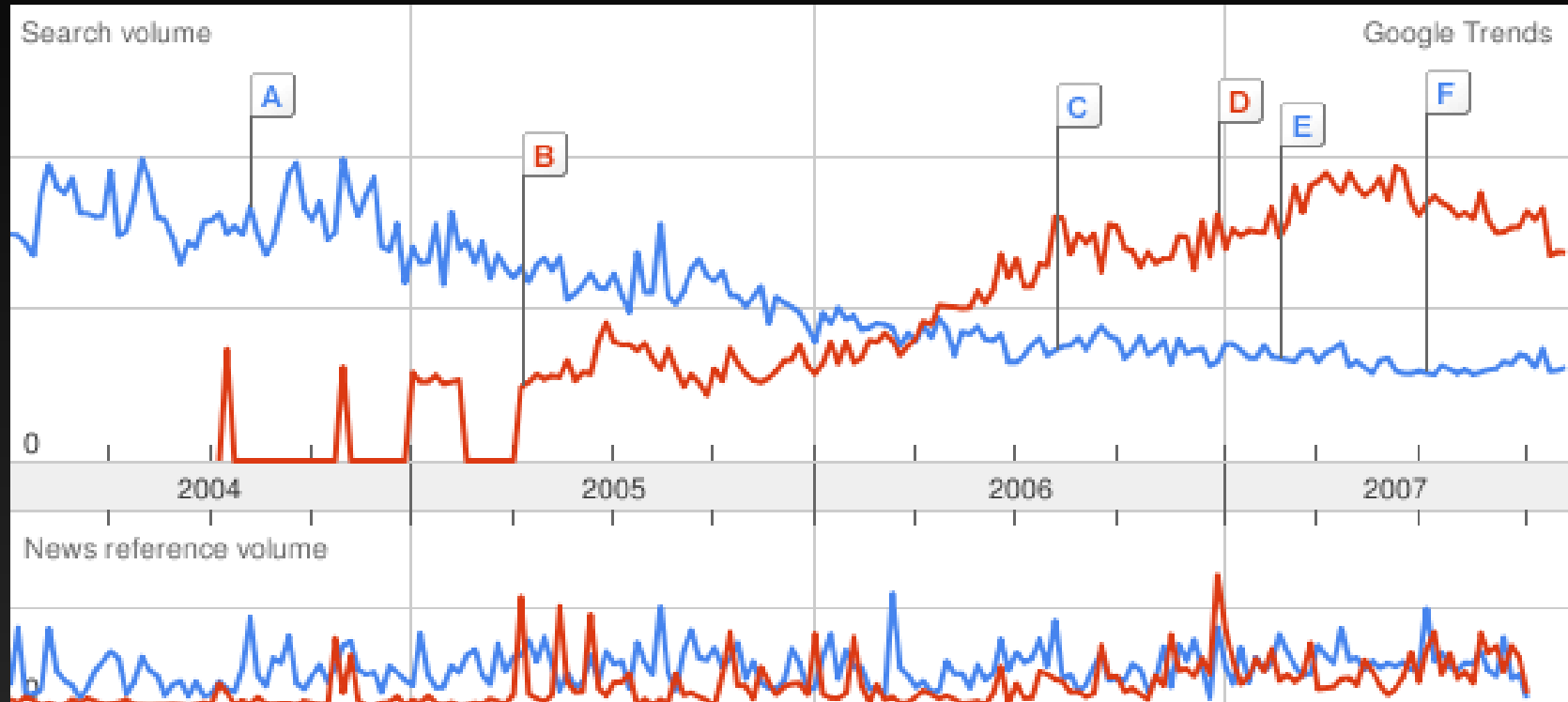
sql injection



xss



Trends



buffer overflow



xss



TYPES OF ISSUES

CSRF (Cross-site Request Forgery)

- Affects unprotected requests!
- Affects both GET and POST!
- JavaScript is not required!
- Can fire from images!
- Can fire from hot-linked resources!
- Huge impact!
- Easy to perform!
- Hard to detect!

XSS (Cross-site Scripting)

- Affects user supplied input!
- Can perform any request to the server!
- JavaScript is not required but often used!
- Can fire from anything!
- Enormous impact!
- Often easy to perform!
- 50% of the attacks are easy to detect!
- The other half are undetectable (so far)!

Cross-origin Scripting

- Similar to Cross-site Scripting!
- Affects the Client and its origins!
- Relies on Client-side bugs or design issues!
- JavaScript is required!
- Compromises the security of the entire client!
- Very hard to detect! (executes on the client)

Design Issues

- Session Theft
- CSS History Stealing
- Browser Portscanning
- State Scanning
- Cross-origin communication (flash, java)
- Local files Theft
- DNS Rebinding
- etc...

Client-side BUGS

- Forgeries
- Overflows
- Scripting

LATEST DEVELOPMENTS

Modern Web Client Issues

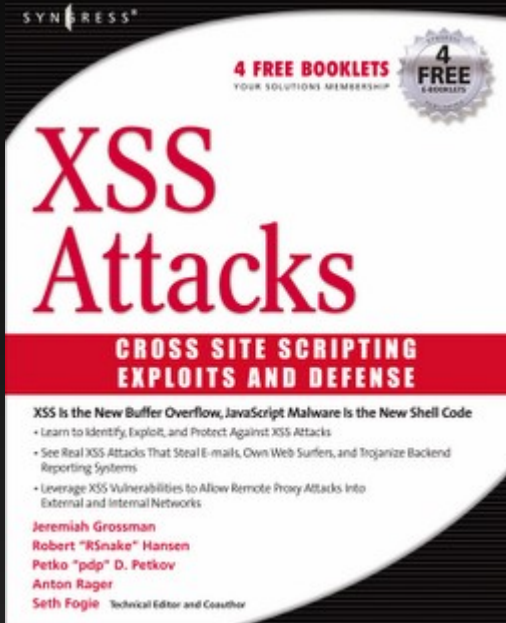
- XSS in Flash
- Scripting in PDF
- Java origin access abuse
 - Trust problems
 - Origin access problems
- ActiveX controllers abuse
- DNS Rebinding
- Browser Bugs

WEB2.0 CONCERNS

Web2.0 Characteristics

- Socially Oriented
- User-supplied Content
- Dynamic
- Huge infrastructures
- Integrated/tangled

Freebies



Q&A

GNUCITIZEN

THANK YOU