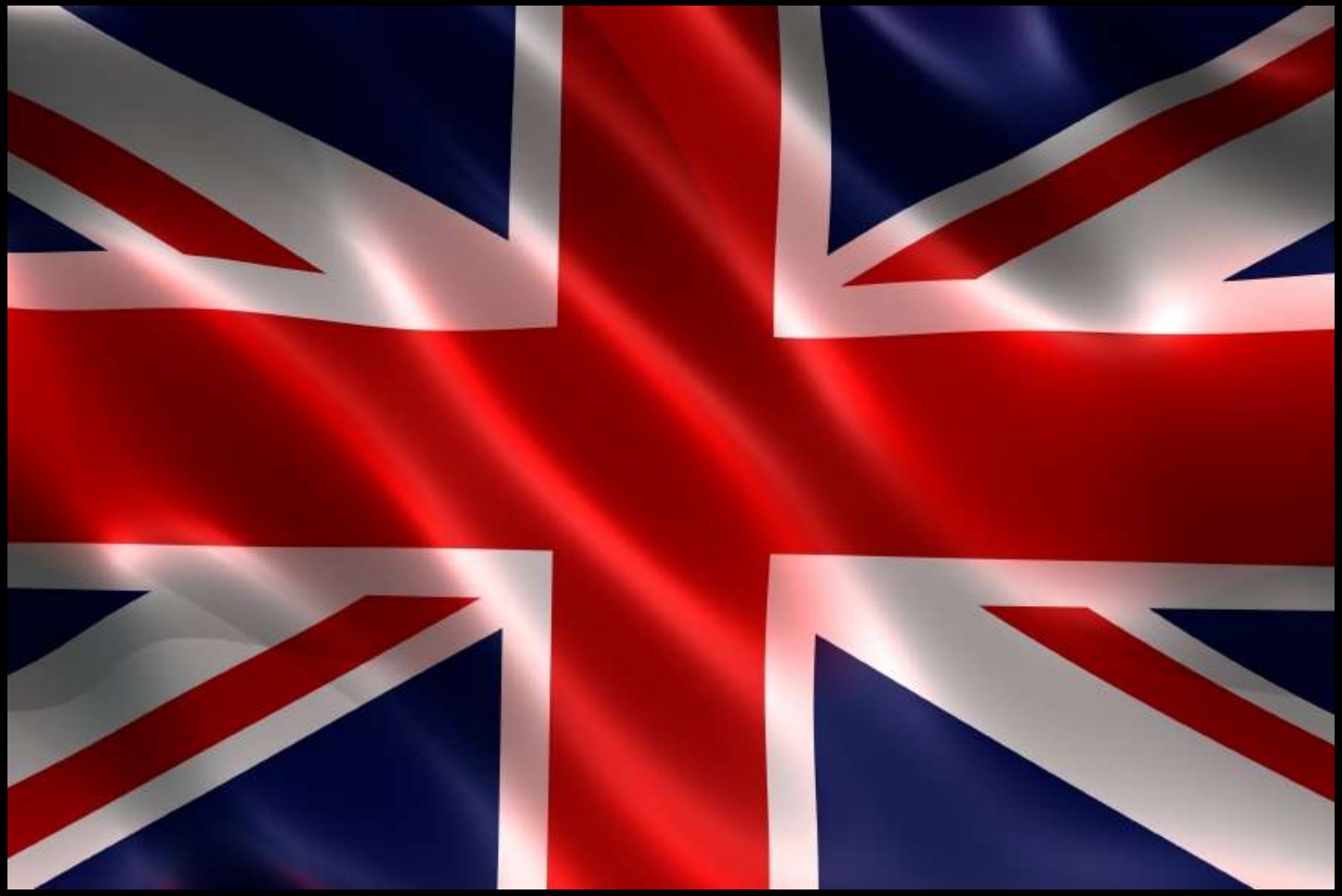
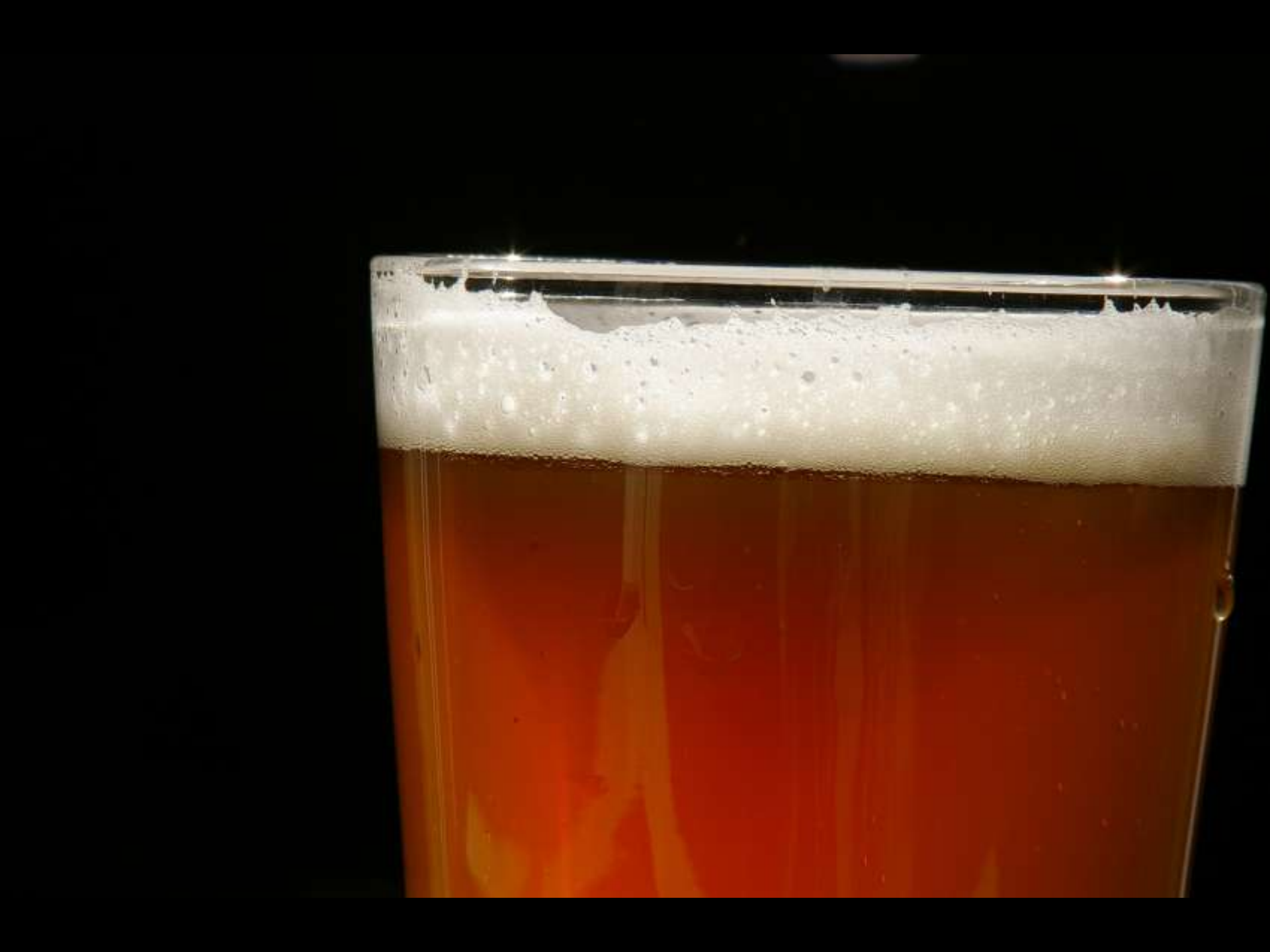
Mark Curphey

ぺちゃくちゃ

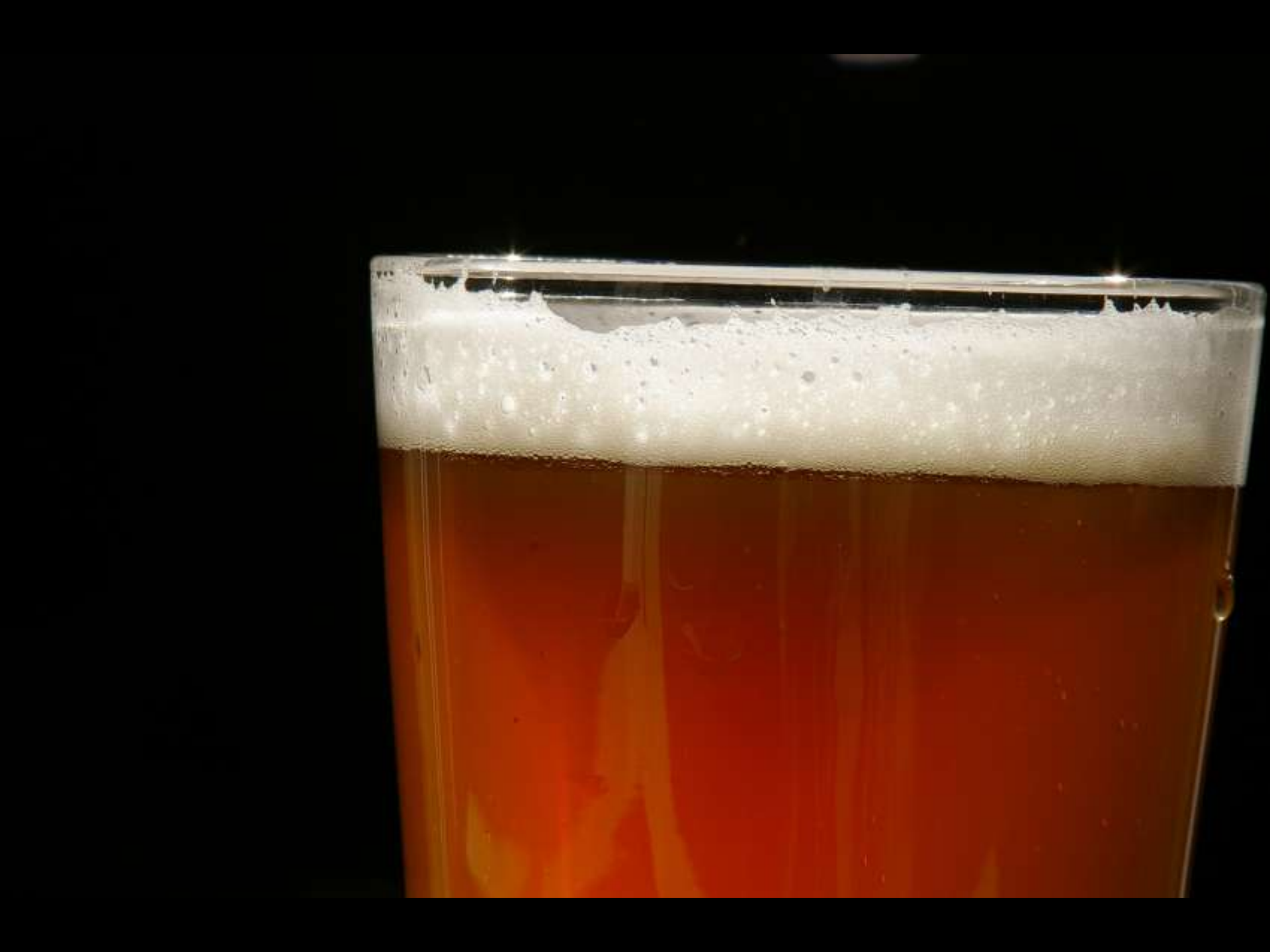
Pecha Kucha

Chatter or chit-chat



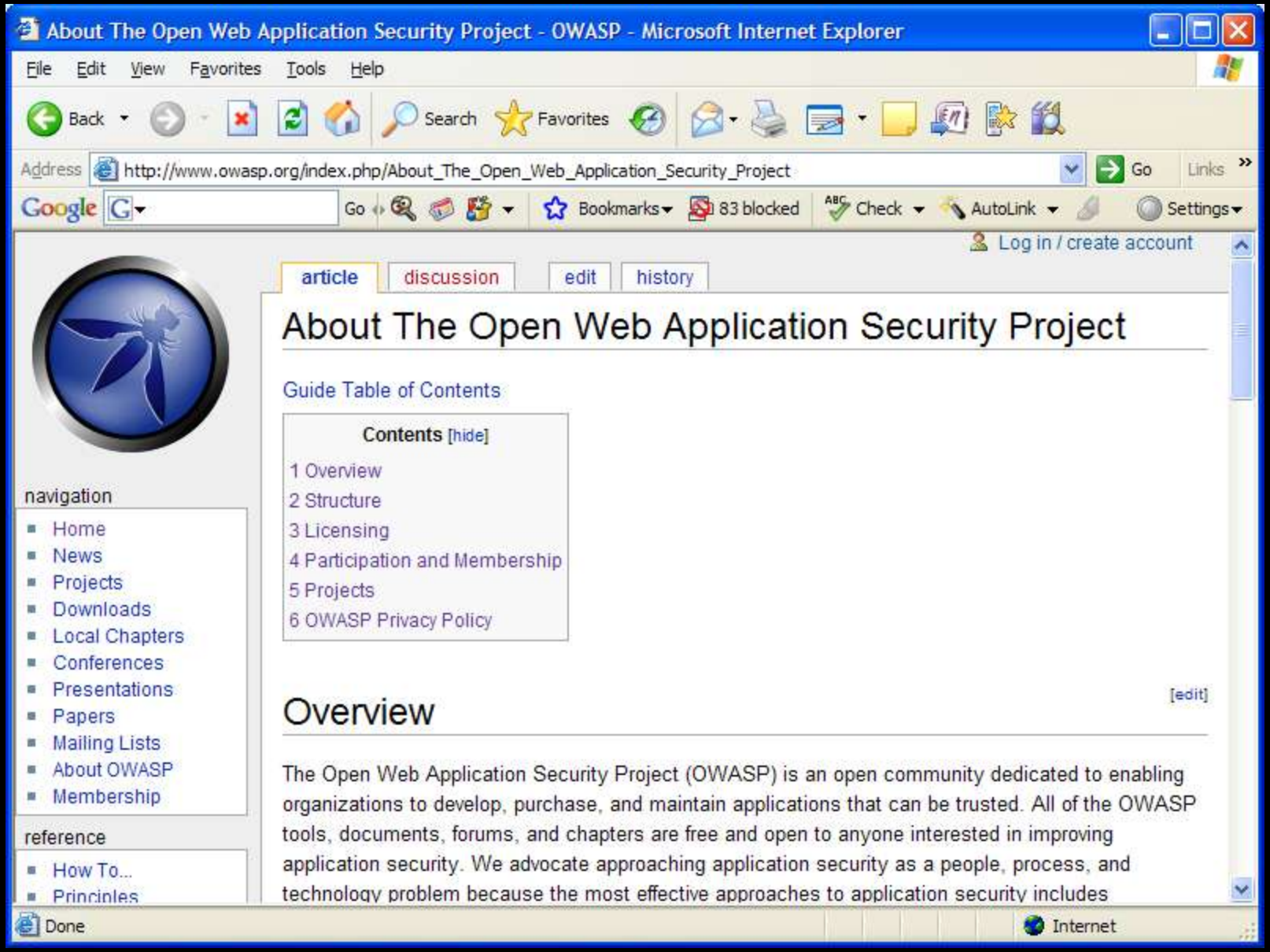



VOLUME
TONE
TONE




.com


charles SCHWAB
NASDAQ


About The Open Web Application Security Project - OWASP - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://www.owasp.org/index.php/About_The_Open_Web_Application_Security_Project
Go Links
Google Go Bookmarks 83 blocked Check AutoLink Settings
Log in / create account
article discussion edit history
About The Open Web Application Security Project
Guide Table of Contents
Contents [hide]
1 Overview
2 Structure
3 Licensing
4 Participation and Membership
5 Projects
6 OWASP Privacy Policy
navigation
Home
News
Projects
Downloads
Local Chapters
Conferences
Presentations
Papers
Mailing Lists
About OWASP
Membership
reference
How To...
Principles
Overview
[edit]
The Open Web Application Security Project (OWASP) is an open community dedicated to enabling organizations to develop, purchase, and maintain applications that can be trusted. All of the OWASP tools, documents, forums, and chapters are free and open to anyone interested in improving application security. We advocate approaching application security as a people, process, and technology problem because the most effective approaches to application security includes
Done
Internet


.com


FOUNDSTONE
KNOW VULNERABILITIES
Managed Security Services
Professional Services
Education
www.foundstone.com

Computerworld | McAfee to buy Foundstone for US$86 million - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Search Favorites

Address http://www.computerworld.com.au/index.php/id;1553486438;relcomp;1 Go Links

Google Go Bookmarks 83 blocked Check AutoLink Settings

COMPUTERWORLD
THE VOICE OF IT MANAGEMENT

QuickPoll: Are user groups a waste of time?
IT Jobs | Downloads | IDG Registered User Login | Subscribe to emails | Subscribe to print | Subscribe to Digital Edition | Search

Tuesday, 19th September 2006 RSS Feeds | Computerworld Zones | Find an IDG site Find IT Jobs Search

eBusiness | Networking | Linux & Open Systems | Security | Software Development | Storage Solutions | Telecoms | Mobility & Wireless | Whitepapers

HOME

EVENTS
Breakfast Briefing: Strategic Technologies for 2006 & Beyond

LATEST
News
Opinions
Features
Interviews
Reviews
Tutorials
Case Studies

McAfee to buy Foundstone for US$86 million

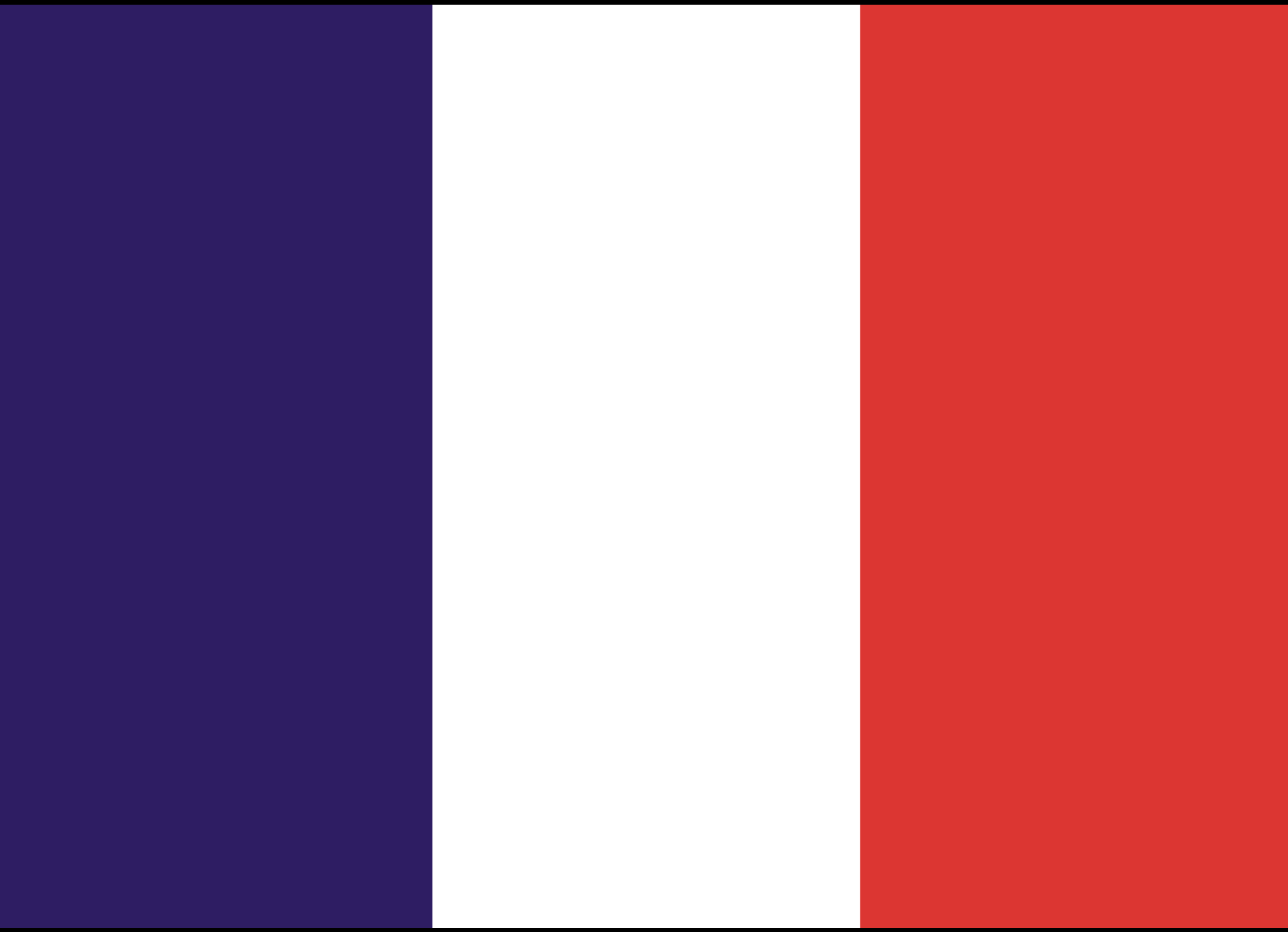
PAUL ROBERTS, IDG NEWS SERVICE

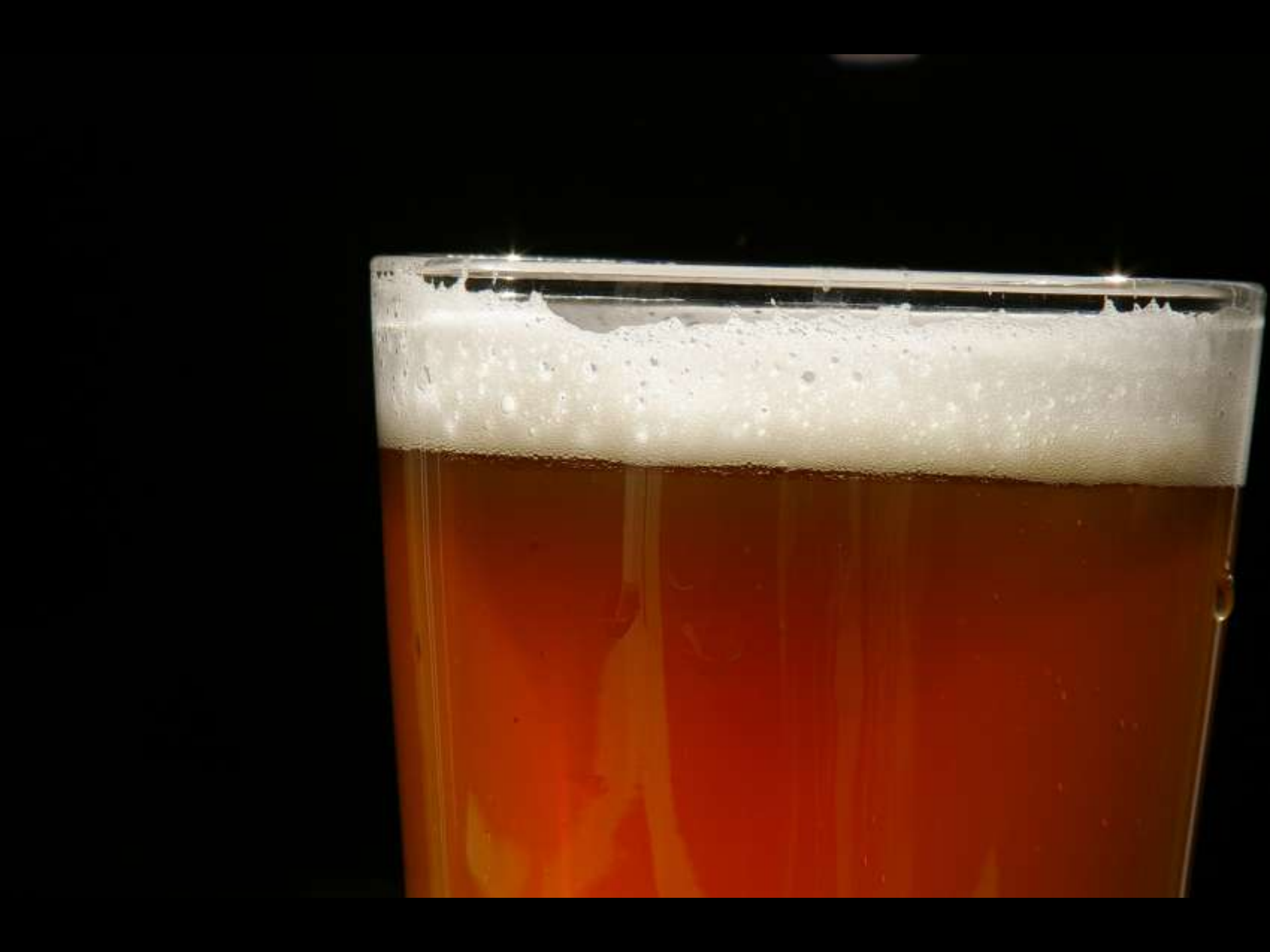
17/08/2004 08:20:52

Antivirus software company, McAfee, is buying Foundstone, which makes software for detecting and managing software vulnerabilities, for $US86 million in cash.

The acquisition will add Foundstone's line of vulnerability management software to McAfee's growing list of security products. McAfee plans to

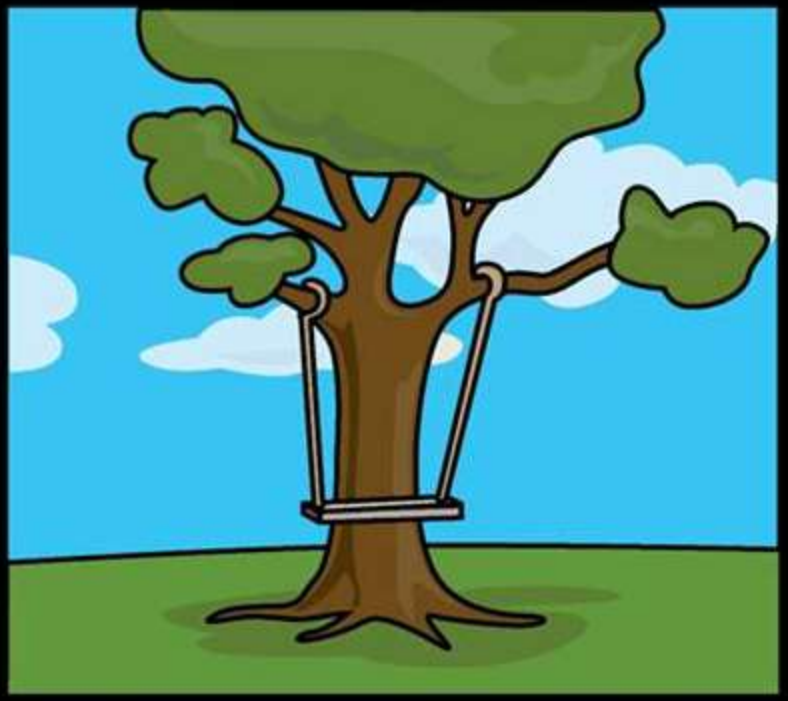
Done Internet





How is Software Built in the Real World?

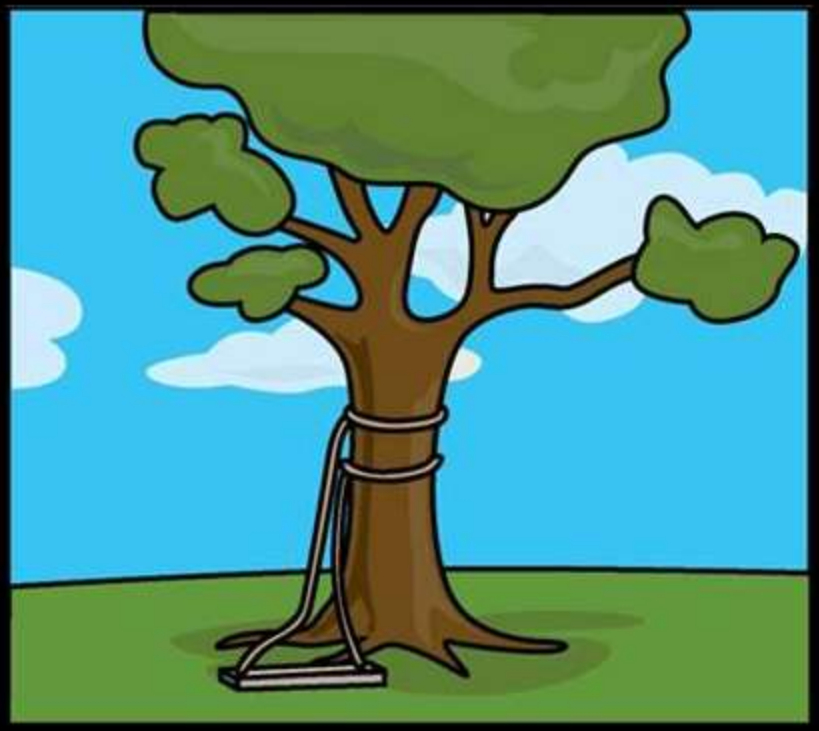
1. What the customer described



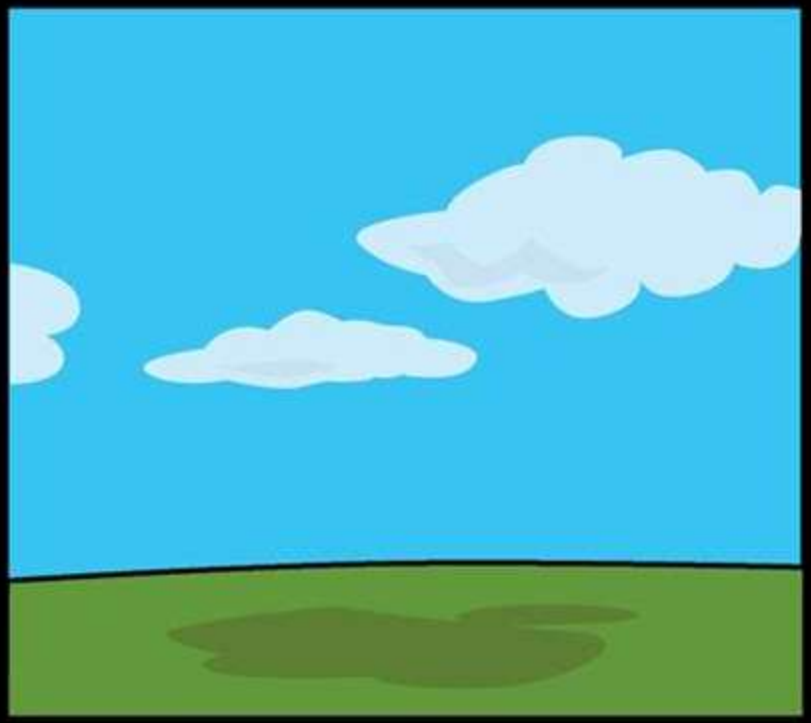
2. How the project manager interpreted it

3. How the business analyst interpreted it

4. How the (expensive) business consultant saw it



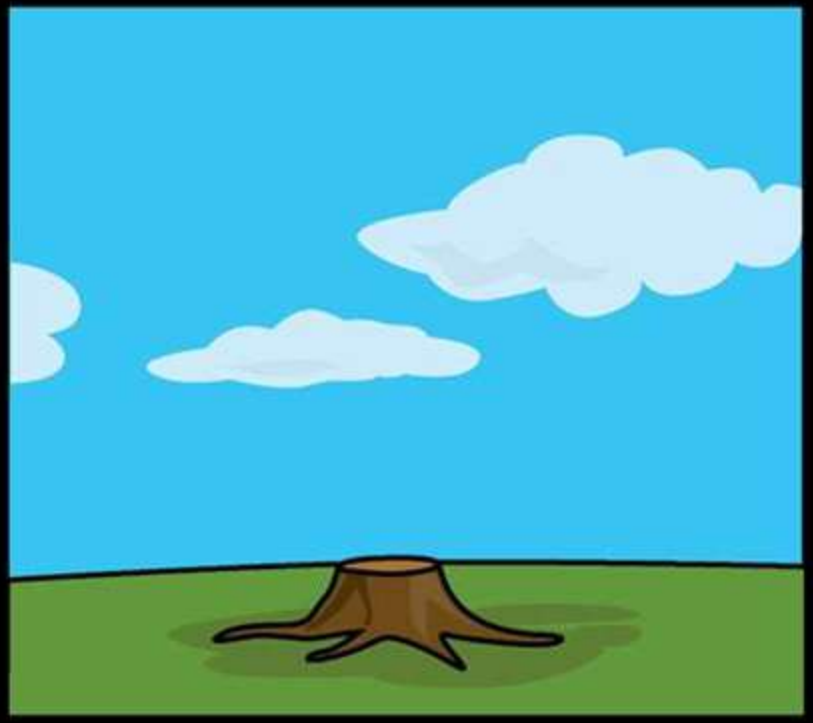
5. How the developer wrote it



6. How the project was documented

7. What operations installed

8. How the consultants billed the project



9. How it was supported

10. What the customer really wanted

Building Software is Hard!

Building Secure Software is Really Hard!

Evaluating Secure Software is REALLY, REALLY, REALLY Hard! (to do it properly)

PCI Data Security Standards?

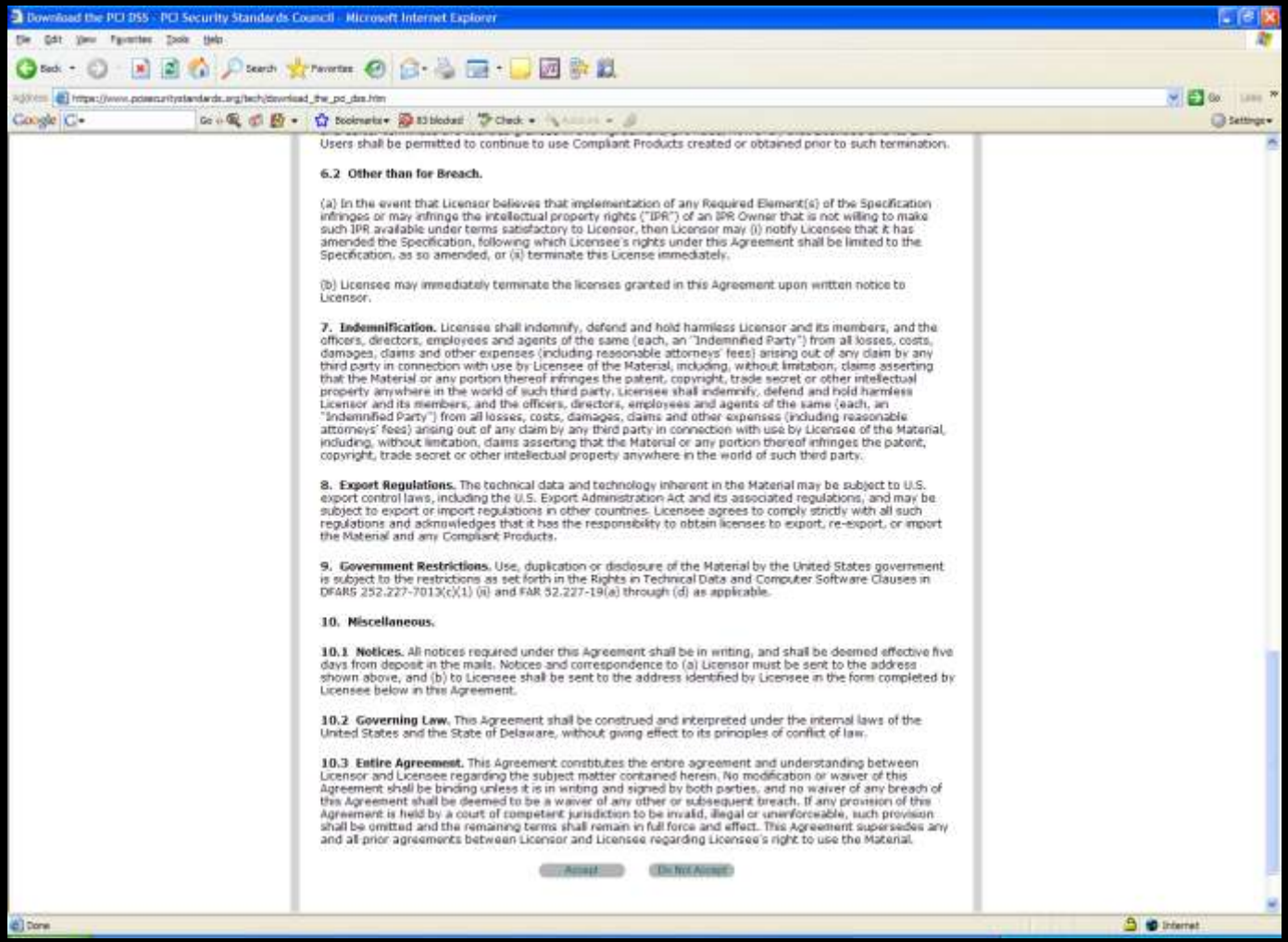
6.6 Ensure that all web-facing applications are protected against known attacks by applying either of the following methods:

- **Having all custom application code reviewed for common vulnerabilities by an organization that specializes in application security**

- **Installing an application layer firewall in front of web-facing applications.**

Note: This method is considered a best practice until June 30, 2008, after which it becomes a requirement.

Full document at
https://www.pcisecuritystandards.org/tech/download_the_pci_dss.htm



……or go straight to the document here!

https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

“……..I Bet I Could Do Better”

Proposal for a Better Scheme
Framework for a Better Scheme
! == Scheme

(Although OWASP May Make It One)

Evaluation - systematic determination of merit, worth, and significance of something.

Certification - attesting to the truth of certain stated facts

Does Anyone Ever Consider the Stakeholders?

External Auditors

Security Consultants

Regulators

CSO’s

Business Managers

System Architects

Operational Managers

Users

Security Architects

System Developers

Internal Auditors

Risk Based Security Assurance (Which Well Talk About Next)

Auditable and Unambiguous Repeatable

High Assurance

(Assurance Levels in Between)

Low Assurance

The Scope of Good Security is People, Process and Technology

Basic and Extended Criteria

People Evaluate and Certify Not Companies

(Auditing the Auditors or Certifying the Certifiers)

Scorecards and Certification

(Share and Share Alike)
(It’s Not a One Time Shot)

Exceptions Happen!

Technology Controls

Category Name	Basic Controls	Extended Controls
Infrastructure Management	N/A	N/A
User Management	10	4
Authentication	3	4
Session Management	7	0
Authorization	TBD	TBD
Data Validation	5	3
Preventing Specific Attacks	11	0
Data Protection	5	1
Privacy	2	1
Security Monitoring	2	0
Miscellaneous	2	0

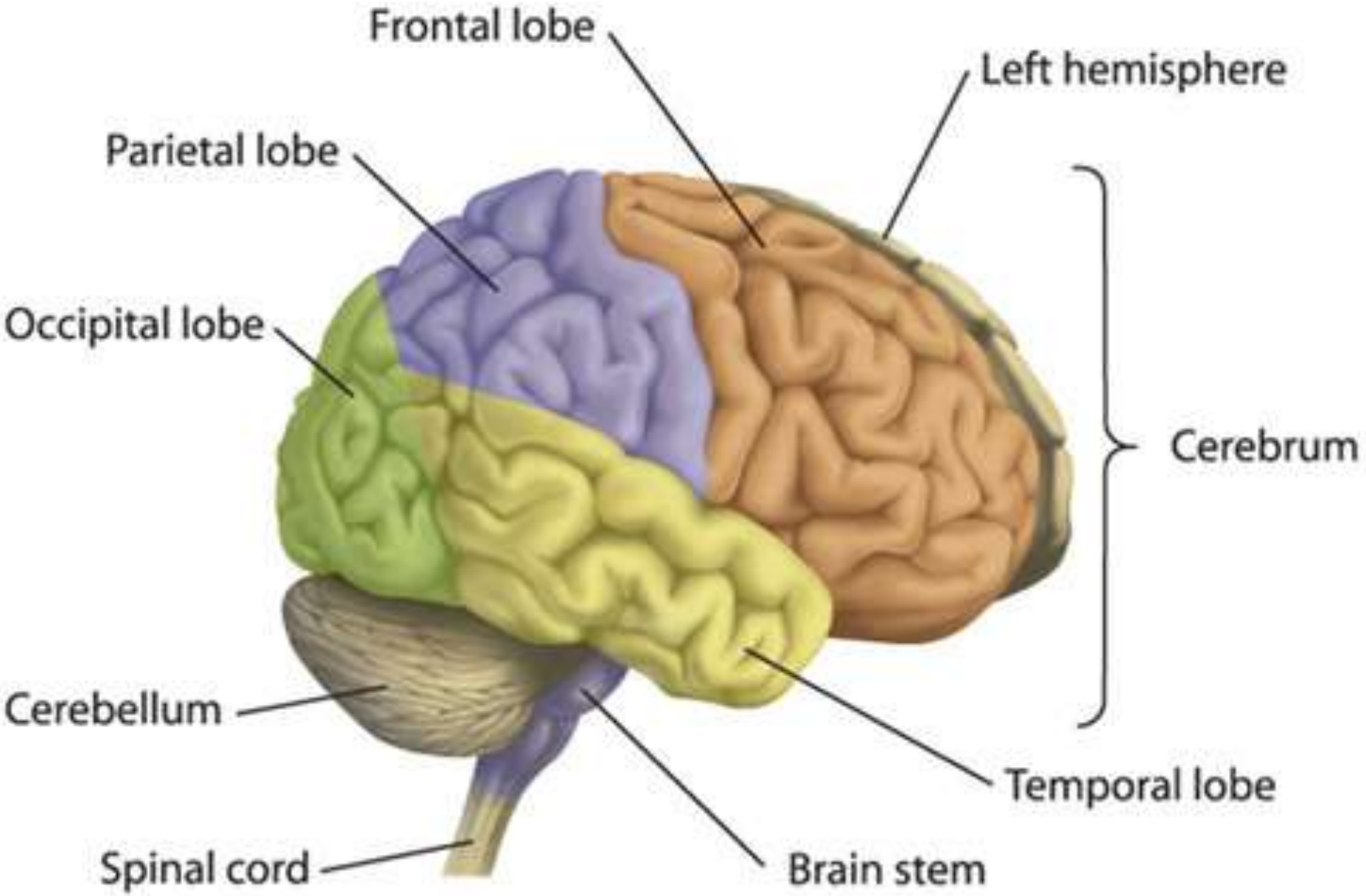
User Management

Reference	Name	Control Type
USERMAN-001	Username Format	Basic
USERMAN-002	Unique Usernames	Basic
USERMAN-003	Username Format (Extended)	Extended
USERMAN-004	Account Management Activity over SSL	Basic
USERMAN-005	Password Strength	Basic
USERMAN-006	Password Expiry	Extended
USERMAN-007	Password Lockout	Basic
USERMAN-008	Password History	Extended
USERMAN-009	Password Storage	Basic
USERMAN-010	Password Reset: Secret Question and Answer	Basic
USERMAN-011	Password Reset: Secondary Chanel	Basic
USERMAN-012	Password Reset: Out of Band Chanel	Extended
USERMAN-013	User Logout	Basic
USERMAN-014	User Management Presentation	Basic

USERMAN-009 – Password Storage

Number	USERMAN -009
Name	**Password Storage**
Description	Passwords should be stored in an encrypted form.
Requirement	Encrypted passwords be enforced. <Scheme implementer to insert details here> <Suggestions: Specify algorithm, key length, key management specs>
Criteria Type	Basic
High Assurance	<To Be Completed by Scheme Implementer>
Medium Assurance	<To Be Completed by Scheme Implementer>
Low Assurance	<To Be Completed by Scheme Implementer>
Very Low Assurance	<To Be Completed by Scheme Implementer>
Evaluation Notes	<To Be Completed By Inspector>
Score	<Pass or Fail : To Be Completed By Inspector>

Introducing the only tool in the world that really works effectively today……


Frontal lobe
Left hemisphere
Parietal lobe
Occipital lobe
Cerebrum
Cerebellum
Temporal lobe
Spinal cord
Brain stem

News for people who run tools

A fool with a tool

….is still a fool

China!

China!

China!

People

Process

Technology

The First Draft Will be Completed by Next Friday, I Promise (Fingers Crossed!)

Thanks For Listening!