SecTheory

Internet Security

About Me

- Robert Hansen – CEO
- SecTheory Ltd
  - Bespoke Boutique Internet Security
    - Web Application/Browser Security
    - Network/OS Security
    - http://www.sectheory.com/
- Advisory capacity to VCs/start-ups
- Founded the web application security lab
    - ~~http://ha.ckers.org/ - the lab~~
    - http://sla.ckers.org/ - the forum

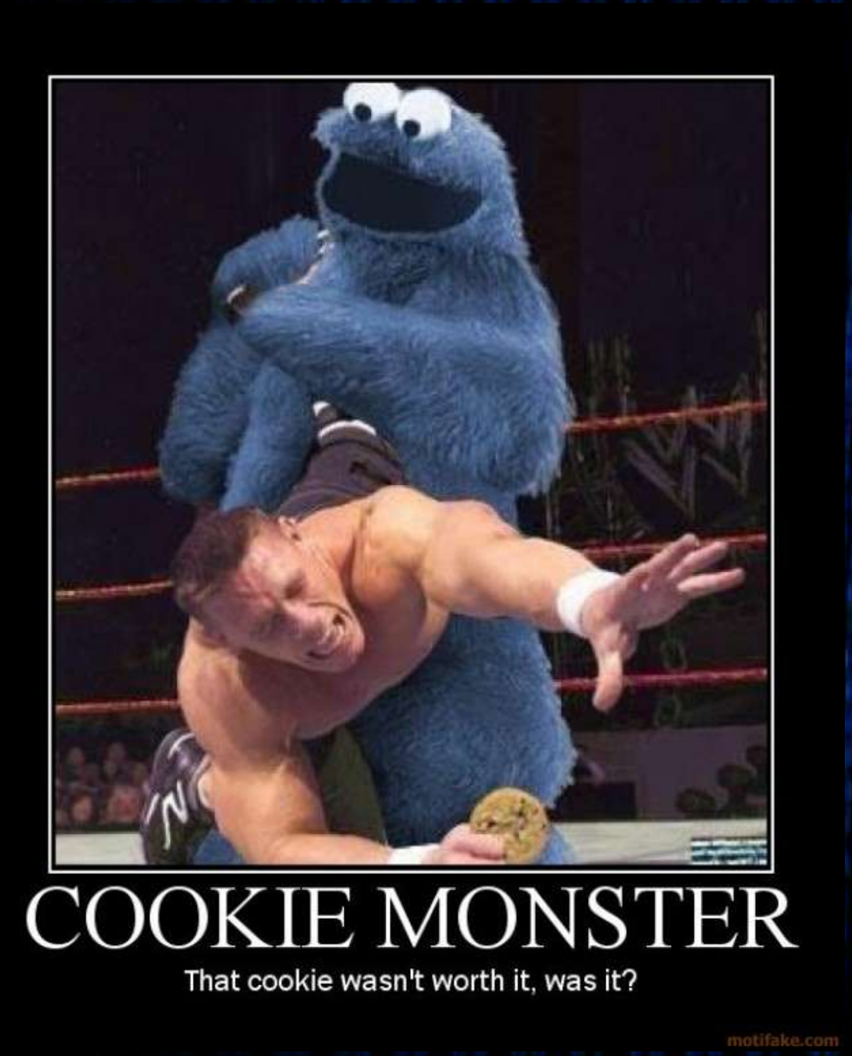
OWASP and Brazil

- Connections committee member
- Brazil could easily become a prototype for the right way to build security
- It starts with the right laws and infrastructure
  - Whistleblower protections
  - Q&A testing/certification
  - Easy takedown processes
  - Software lemon laws
  - Extradition

Let's Go Back To Basics

The humble cookie

Basic Problems



- Aren’t secure by default
- Are being used as a form of tokenized surrogate for passwords (which makes them important)
- Shoddy replacement for a stateful protocol!

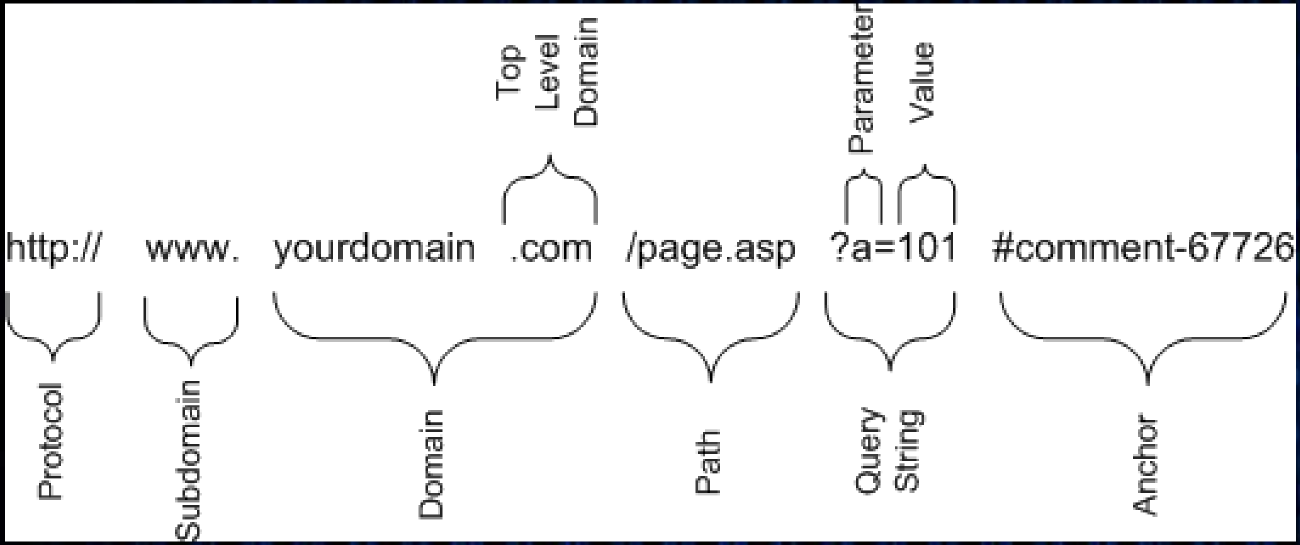
What the f*©% are Cookies?

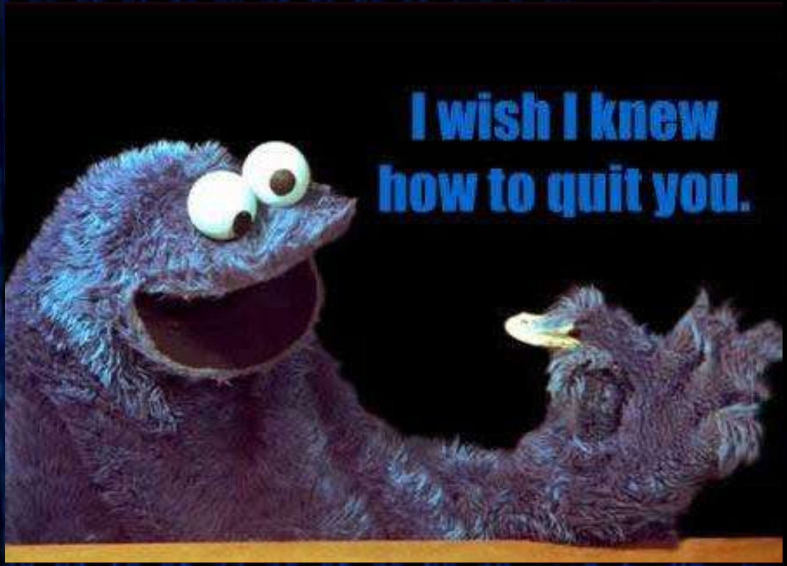
```
HTTP/1.1 200 OK
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: PHP/5.2.3,ASP.NET
Set-Cookie: user=bob; path/
Date: Wed, 18 Aug 2010 14:24:49 GMT
Connection: close

GET / HTTP/1.1
User-Agent: Mozilla/4.0…
Cache-Control: no-cache
Host: www.example.com
Cookie: user=bob;
Accept-Encoding: gzip, deflate
Connection: Keep-Alive
```

Cookie Structure

- a=b;
- a=b; Path=/;
- a=b; Expires=Fri, 31-Dec-2010 23:59:59 GMT; Max-Age=10000; Path=/;
- a=b; Expires=Fri, 31-Dec-2010 23:59:59 GMT; Max-Age=10000; Path=/; domain=.example.org;
- a=b; Expires=Fri, 31-Dec-2010 23:59:59 GMT; Max-Age=10000; Path=/; domain=.example.org; HttpOnly; Secure

Cookies != SOP

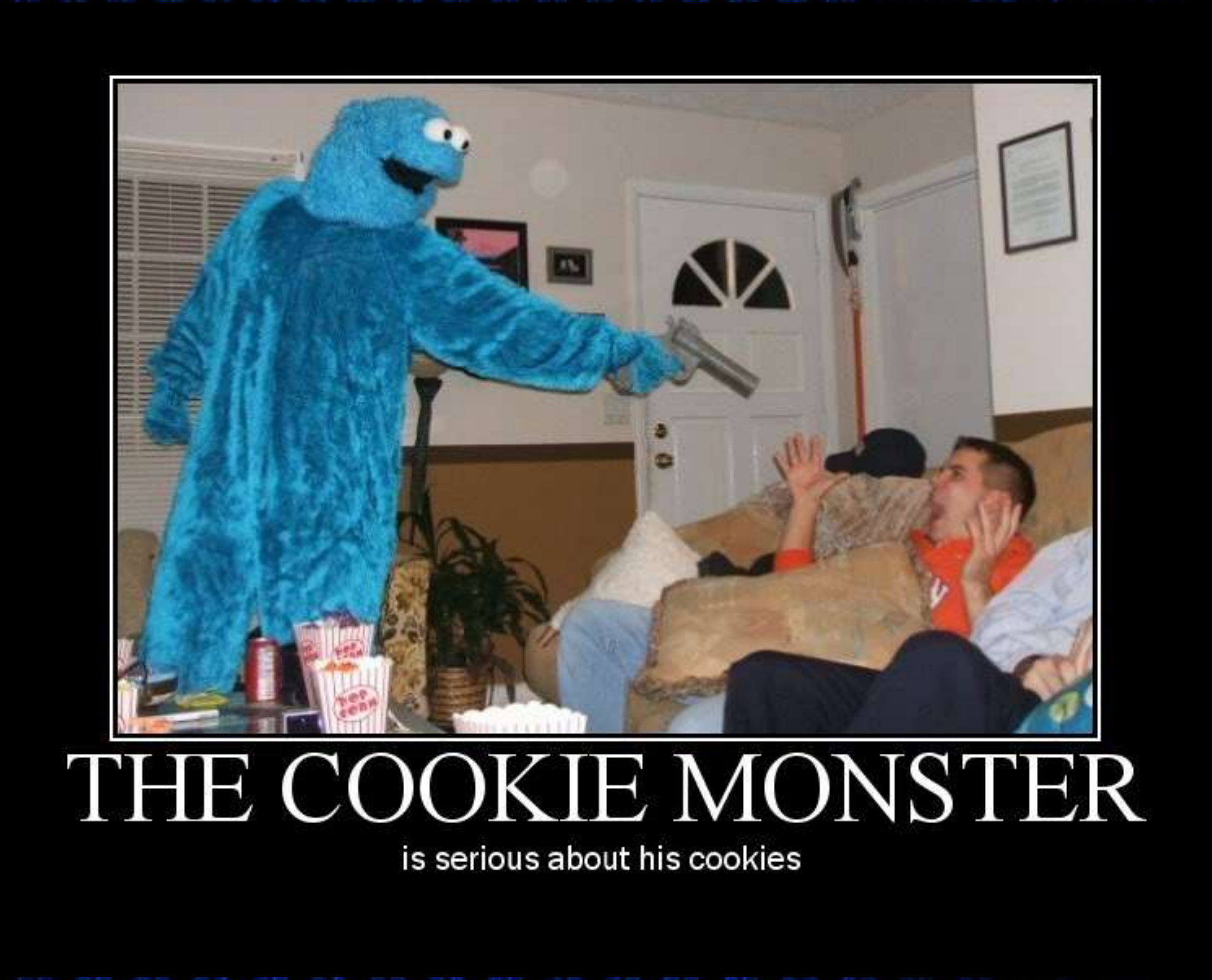




URL	Outcome	Reason
http://www.yoursite.com/dir/page.html	Success	Same domain
http://www.yoursite.com/dir2/other-page.html	Success	Same domain
https://www.yoursite.com/	Failure (Except Cookies)	Different protocol
http://www.yoursite.com:8080/	Failure (Except Cookies)	Different port
http://news.yoursite.com/blog/	Failure (Except Cookies)	Different sub-domain

Olllld Cookie Issues

- Doesn’t follow the semi-sane JS SOP
- Cross Site Cooking
- Max-age doesn’t work in IE
- XHR could bypass HTTPOnly
- Client side removal doesn’t actually remove the cookies



Olllld Cookies Issues 2

- CSRF (to create/change cookies)
- XSS (to create/change/steal cookies)
- Session fixation (known cookie variant)

More Obscure Cookie Issues

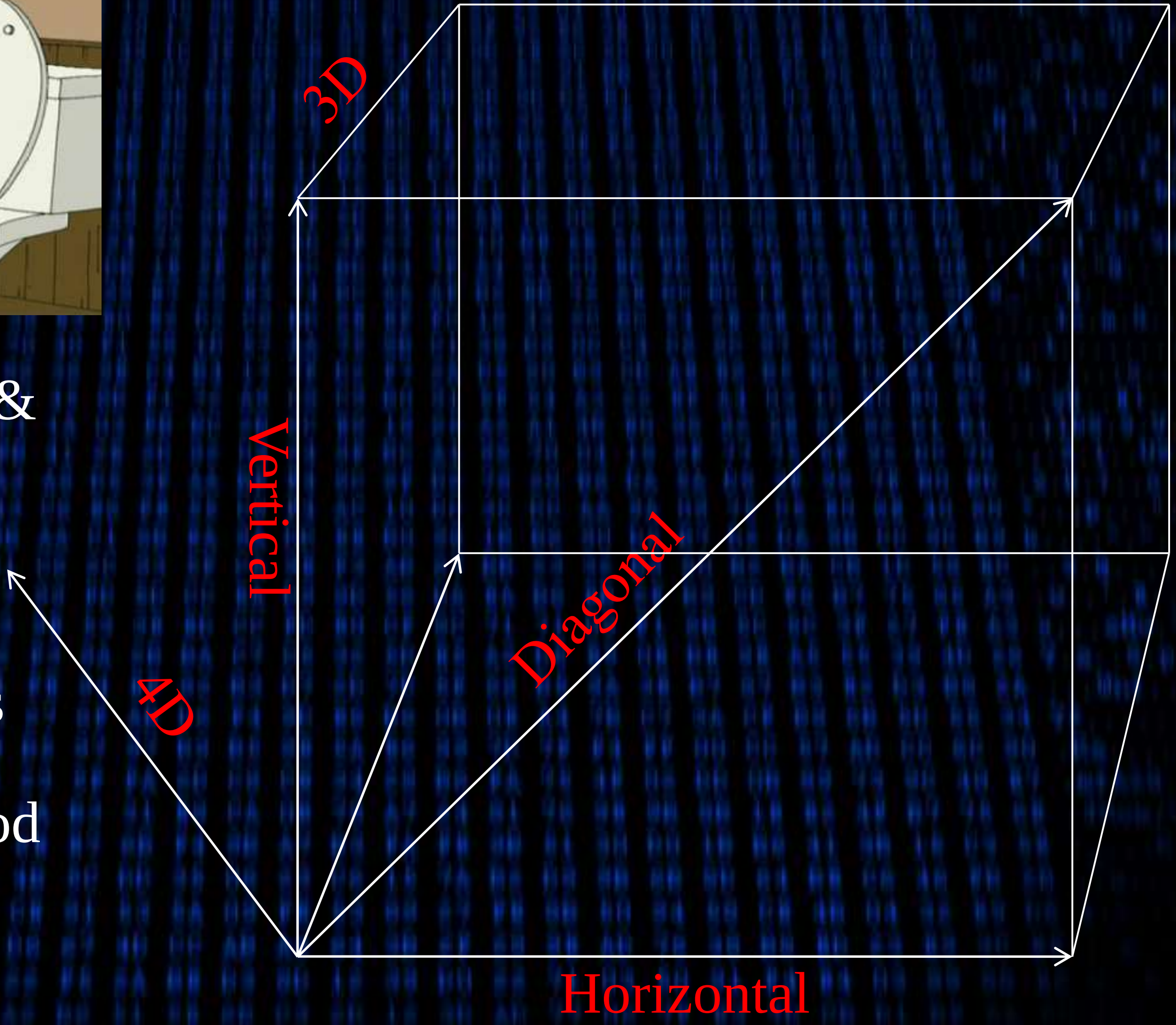
- Predictable cookie names
- DNS Rebinding
- IE8 doesn’t remove cookies until reboot but IE9 beta is soooo much worse…
- Lack of Cookie Consolidation Issues
- MITM cookie clobber
- MITM XSS introduction
- MITM login detection
- NoScript Cookies

Wrath of the Cookie!

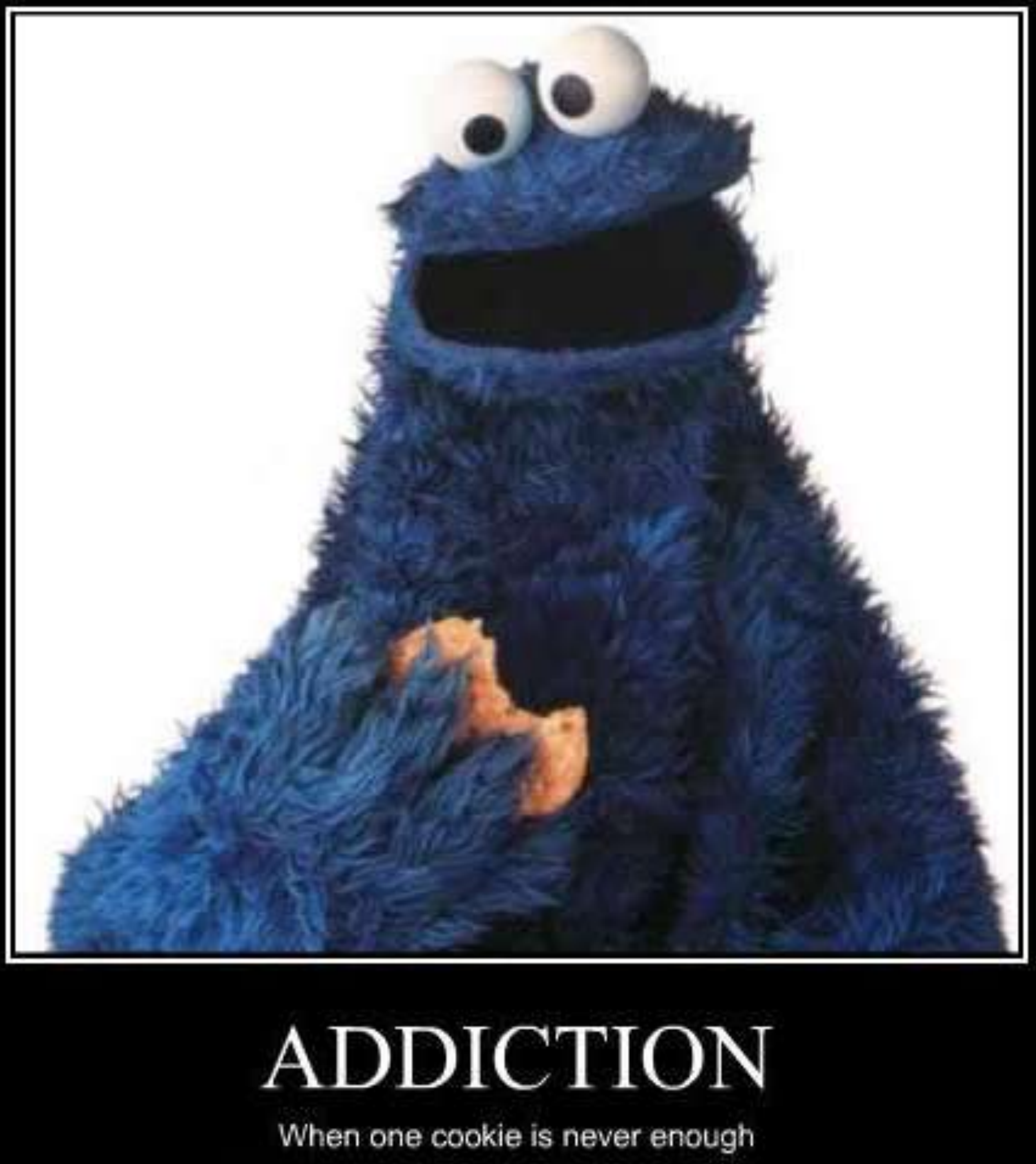
C.O.W. #170 - THE REAL COOKIE MONSTER - MFRANK

- Double DNS Rebinding
- Cookies cause DoS
- Overflowing cookie jar
- Affiliate protections
- Session prediction/brute force (Samy)

- Vertical = 1 username & many passwords
- Horizontal = 1 pass & many usernames
- Diagonal = many usernames & passwords
- 3D = Many IPs
- 4D = Over a long period of time
- Credential



Ultimately…



- Makes multi sub-domain sites much less safe
- Makes browsers easy to track, & hard to defend.
- We need to kick the cookie addition and build better forms of auth.

JOIN
THE
DARKSIDE
and get a free cookie...

Thank you!

- Robert Hansen
  - www.fallingrocknetworks.com/ - hosting
  - www.sectheory.com – the company
  - ~~http://ha.ckers.org – the lab~~
  - http://sla.ckers.org – the forum
  - Detecting Malice – the book
    - www.detectmalice.com
  - XSS Exploits – the book
  - robert_aT_sectheory_d0t_org – the email