How a Hacker Sees Your Site

Patrick Laverty
Security Response Engineer
Akamai CSIRT

Patrick Laverty
Akamai Technologies - SIRT
plaverty@akamai.com
http://www.patricklaverty.com
@plaverty9
Organizer of OWASP Rhode Island
BSides Boston Speaker Chair
(Want to present?? Stay til the end!)

Usually 60 mins, got 45, questions after…please

How You See Your Web Site

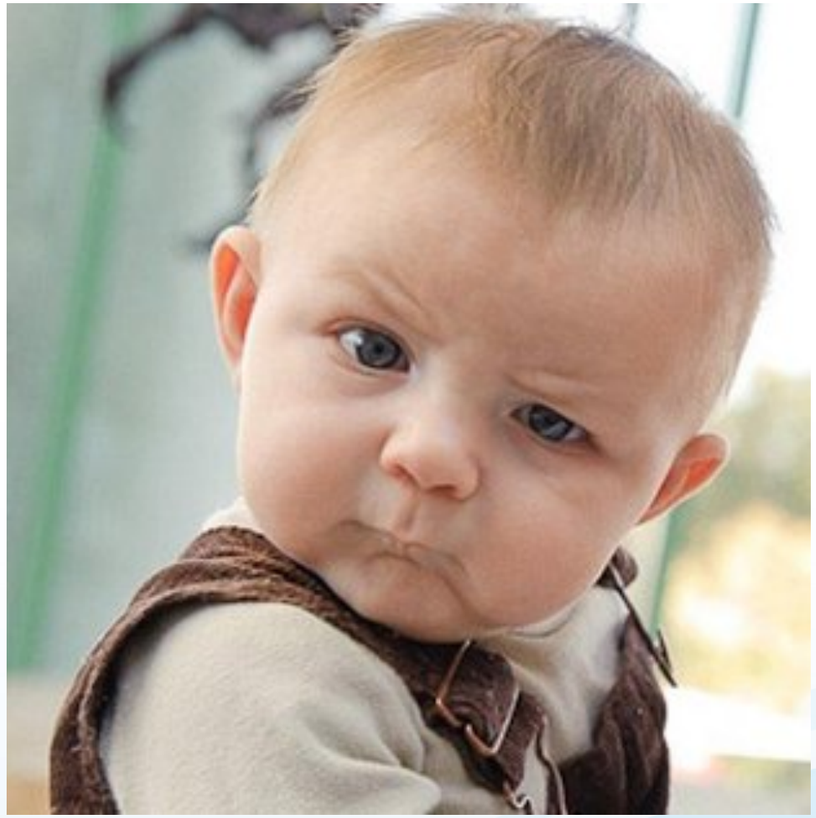
How a Hacker Sees Your Site

Perceived Difficulty To Hack Your Site

How Hard Is It Really?

What Is A Hacker Looking For?

Not all that much…

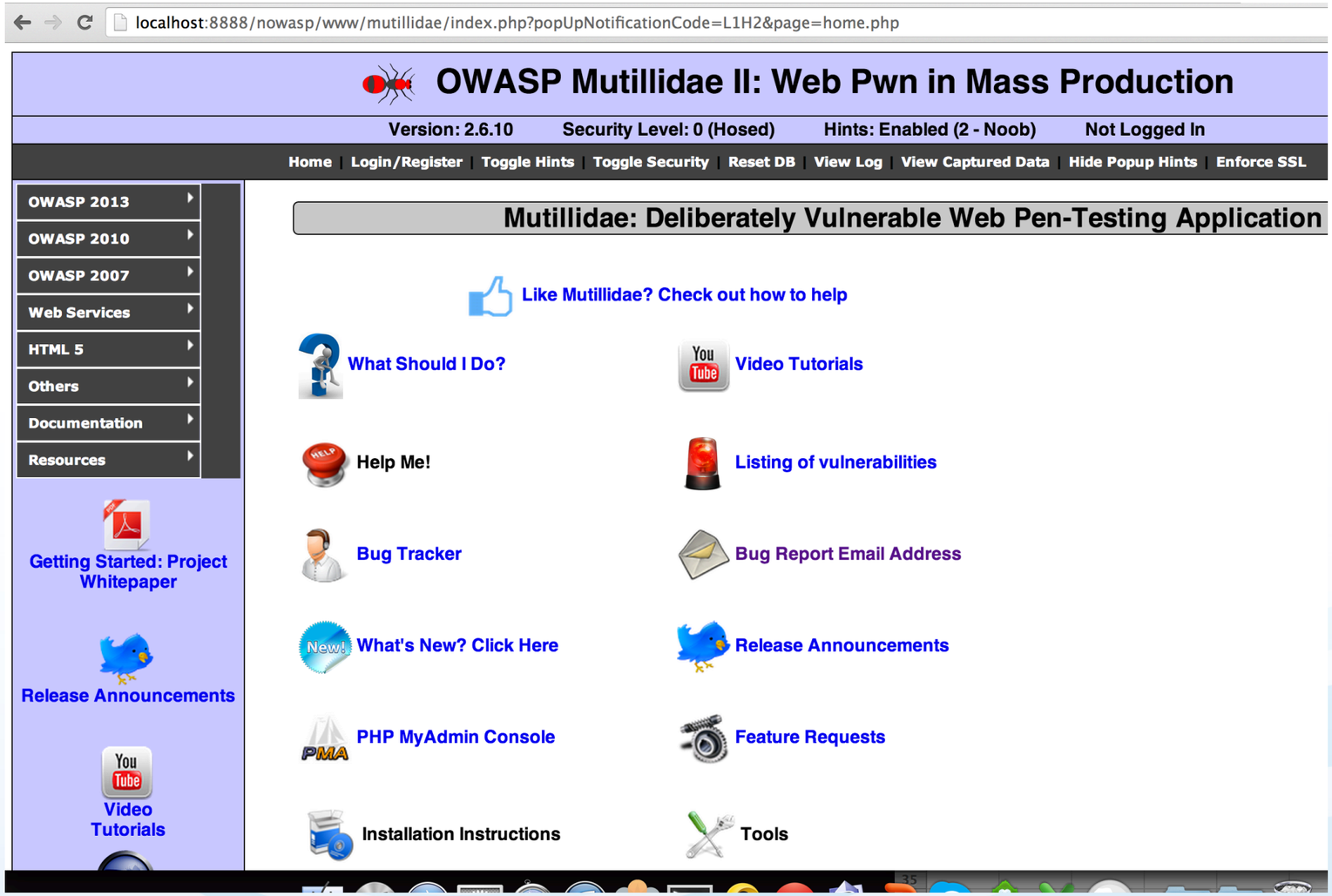


What Is A Hacker Looking For?

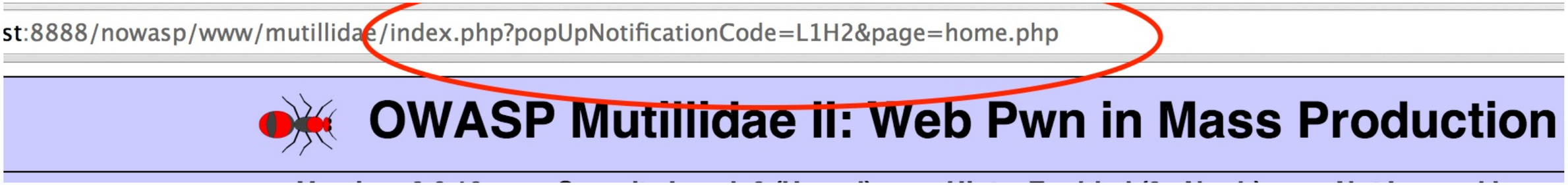
- URL Parameters
- Data Inputs
- 3rd Party Content
- Robots.txt
- Redirects
- Cookies
- Session Data
- Administrator Area/CSRF
- HTML Source Comments
- Weak Passwords
- Weak/Broken SSL
- Old Versions of Site
- Lack of Data Sanitization
- File Uploads
- Business Logic Flaws
- CMS Frameworks
- Company Phone Book
- Company Org Chart
- OSINT
- Outdated Operating System
- Unlocked/Open DNS
- Unnecessary Services

Let’s look at ’em!

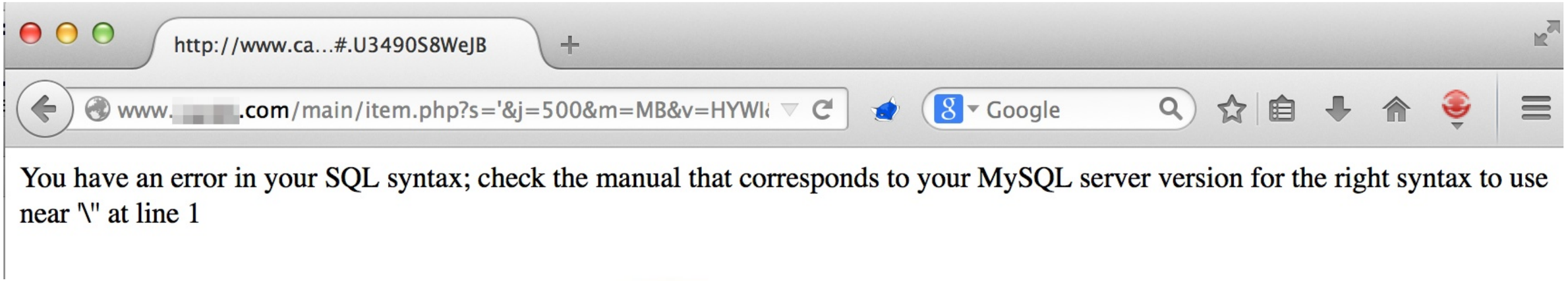
Look At A Web Site

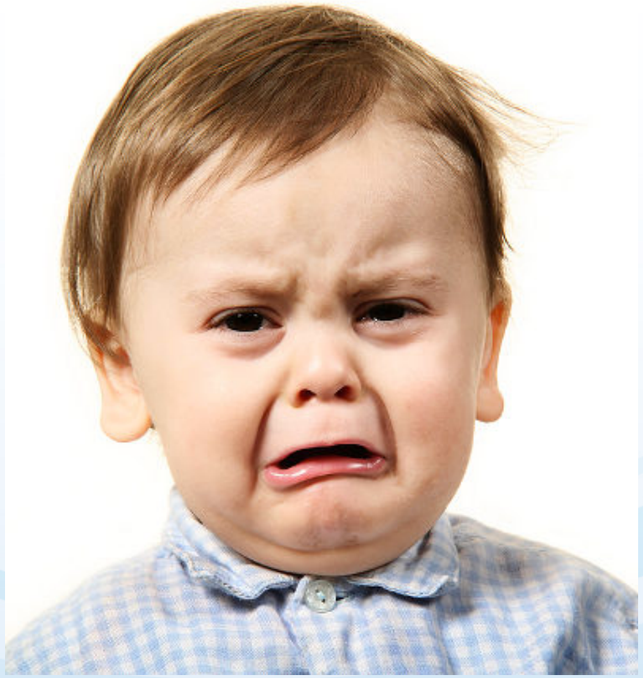


URL Query Parameters

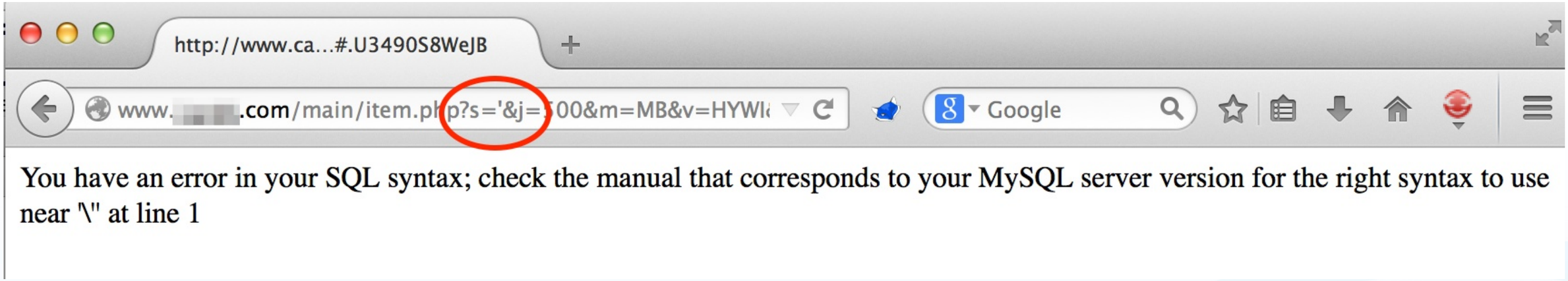


Data Inputs – SQL Injection

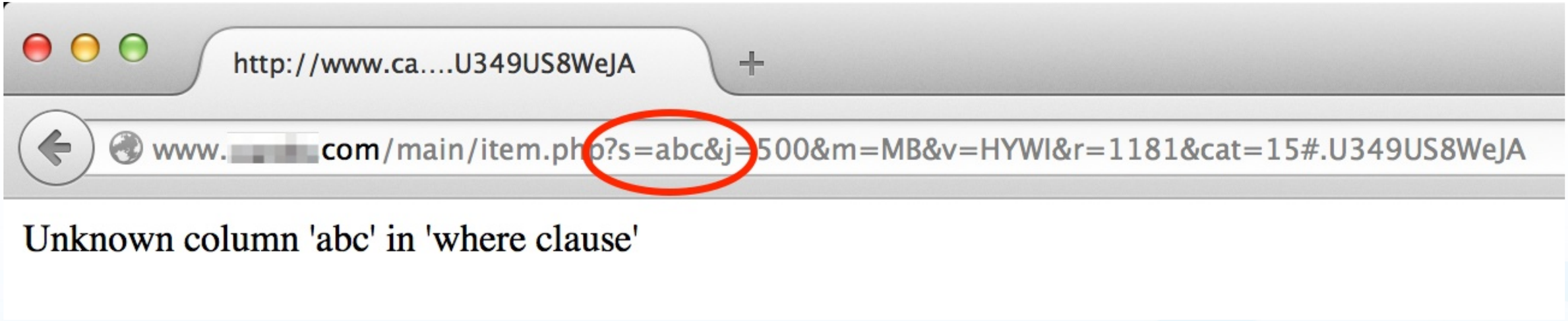




Data Inputs – SQL Injection



Data Inputs – SQL Injection



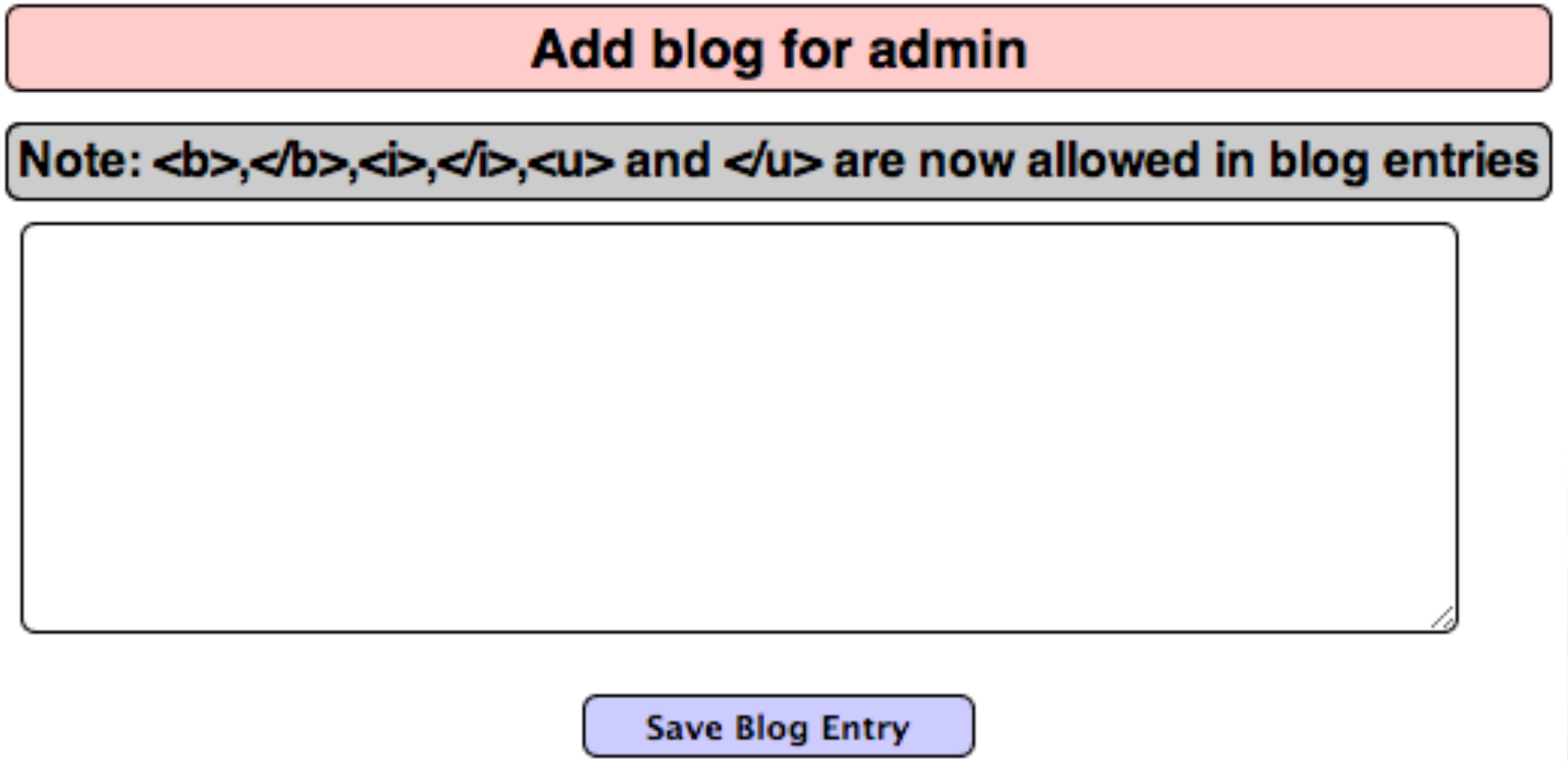
Data Inputs – SQL Injection

Data Inputs – SQL Injection

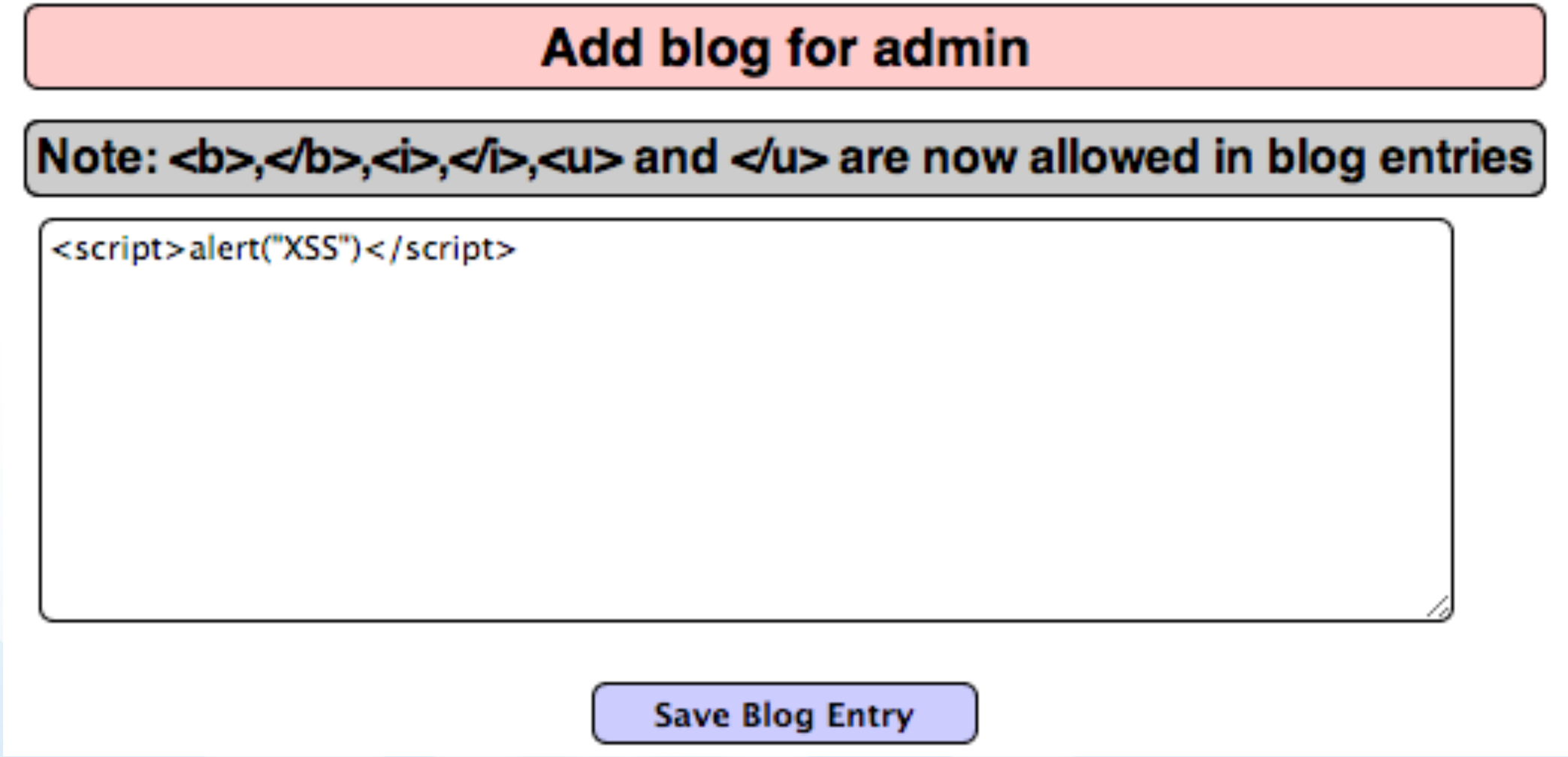
```
sqlmap identified the following injection points with a total of 548 HTTP(s) requests:
---
Place: POST
Parameter: username
    Type: boolean-based blind
    Title: OR boolean-based blind - WHERE or HAVING clause (MySQL comment)
    Payload: username=-1388' OR (3072=3072)#&password=foobar&login-php-submit-button=Login

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE or HAVING clause
    Payload: username=hacker' AND (SELECT 5358 FROM(SELECT COUNT(*),CONCAT(0x7179796e71,(SELECT (CASE
WHEN (5358=5358) THEN 1 ELSE 0 END)),0x7171796d71,FLOOR(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER
_SETS GROUP BY x)a) AND 'jPpV'='jPpV&password=foobar&login-php-submit-button=Login
---
[15:43:12] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.5.10, Apache 2.2.26
back-end DBMS: MySQL 5.0
```

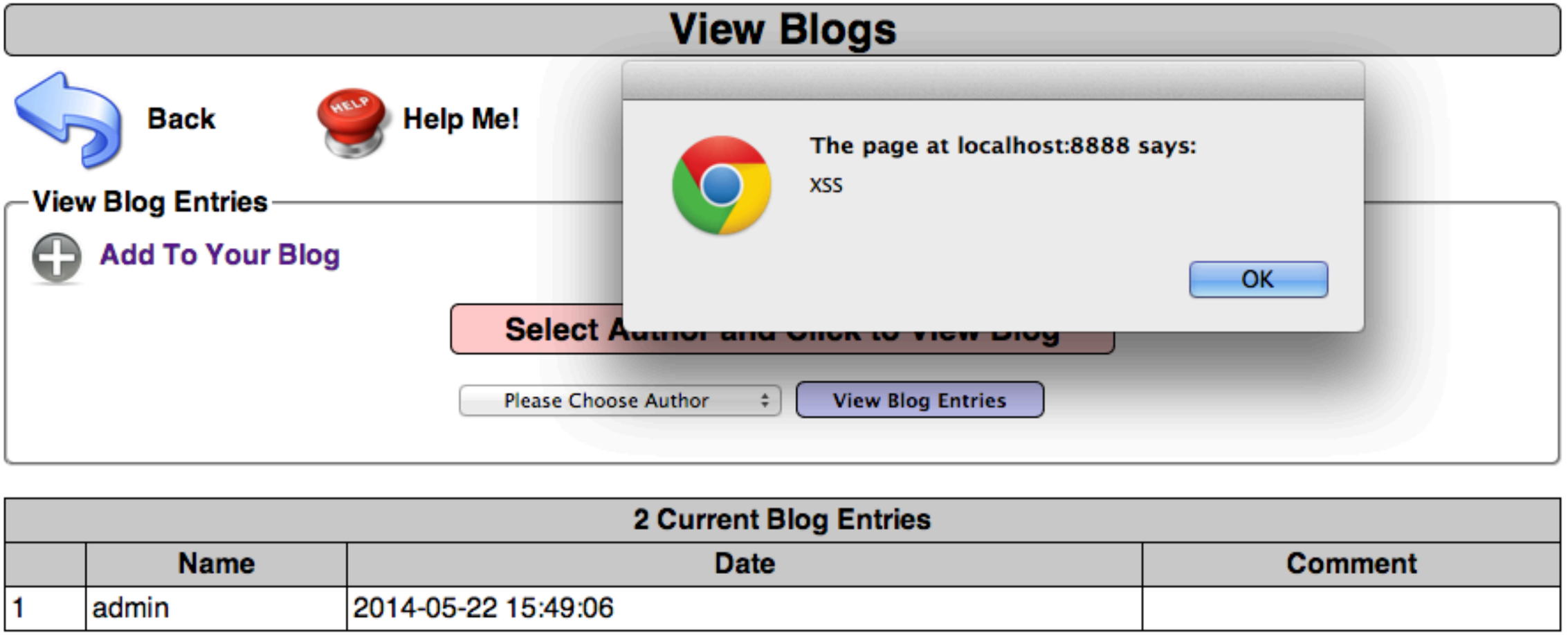
Data Inputs



Data Inputs - XSS



Data Inputs - XSS



Data Inputs - XSS

http://securitypadawan.blogspot.com/2012/08/xss-what-your-momma-didnt-tell-you.html

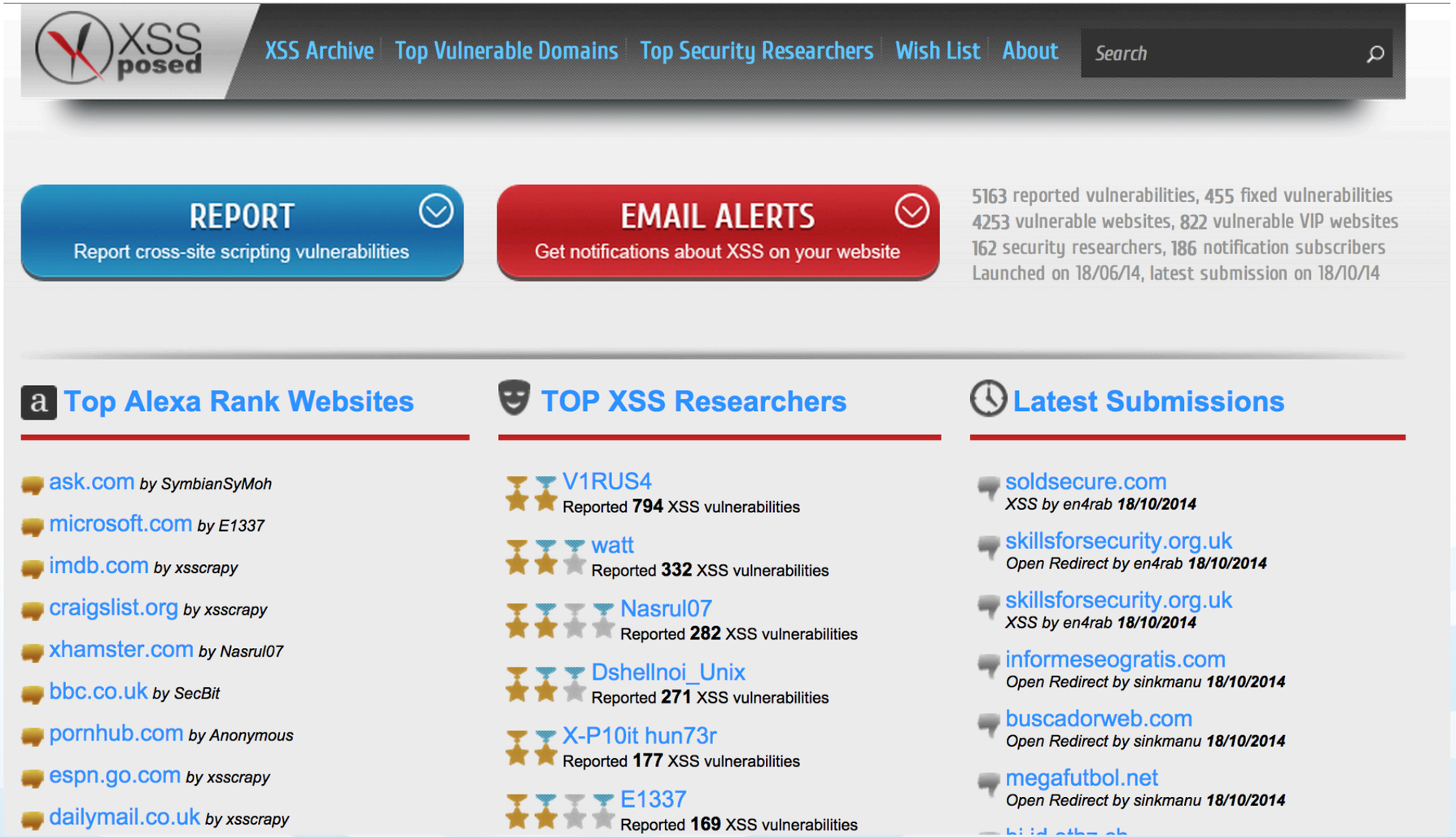
“As a result, metasploit has sent the payload, received a shell back and successfully migrated to a new process so that when the user closes the browser, the shell will not be lost.”

Data Inputs - XSS

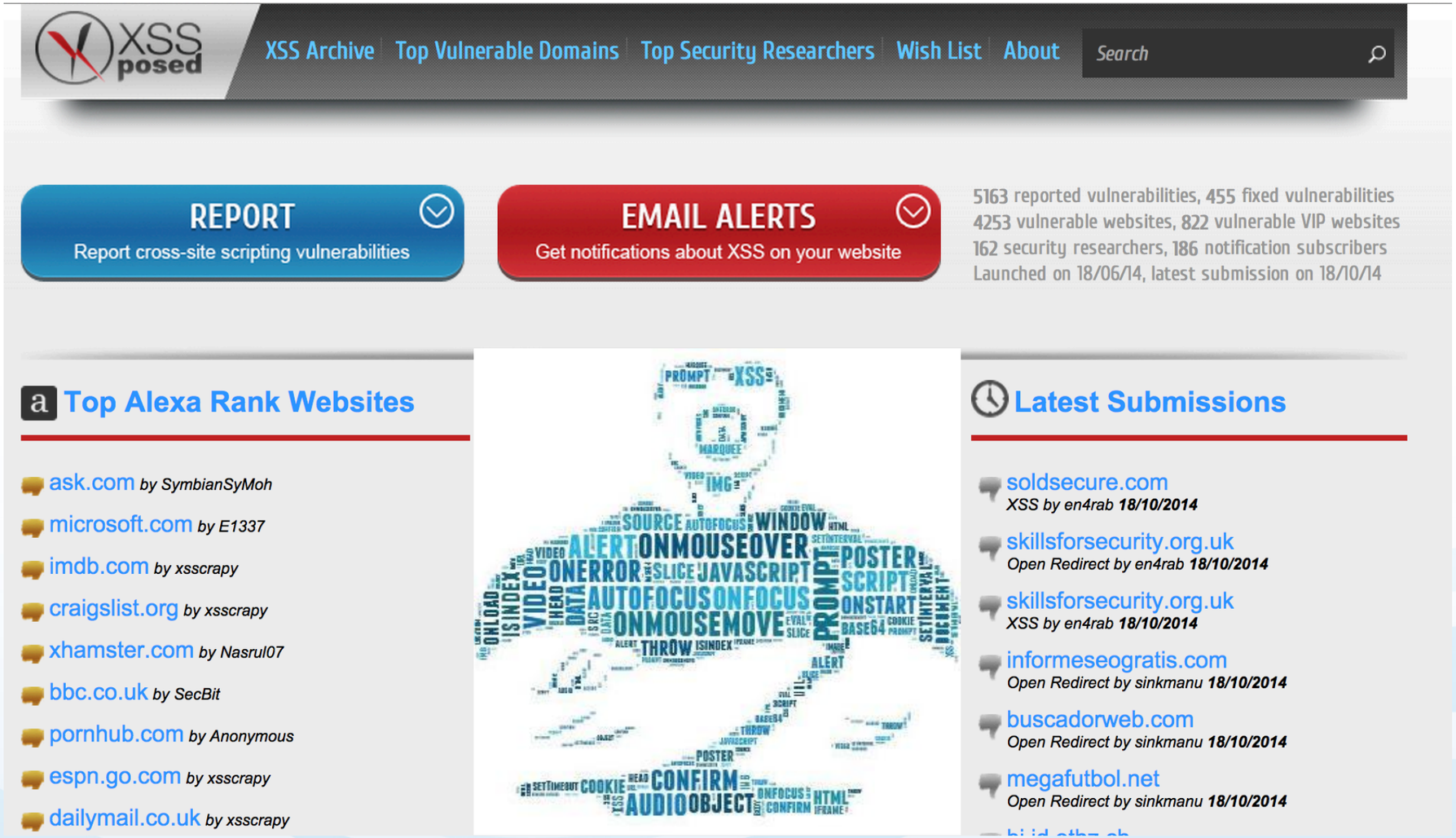
http://securitypadawan.blogspot.com/2012/08/xss-what-your-momma-didnt-tell-you.html

“As a result, metasploit has sent the payload, received a shell back and successfully migrated to a new process so that when the user closes the browser, the shell will not be lost.”

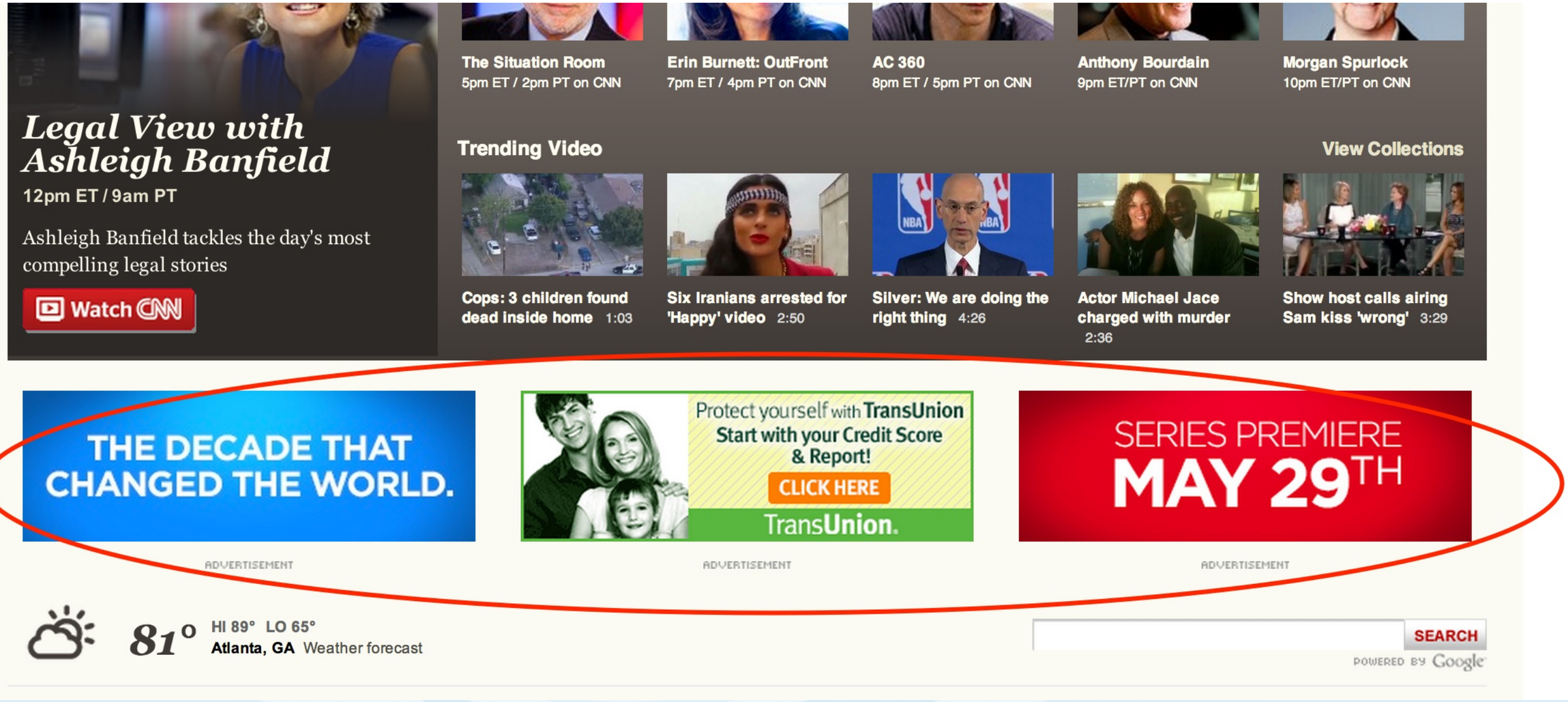
Data Inputs – xssposed.com



Data Inputs – xssposed.com



3rd Party Content



3rd Party Content – s0.2mdn.net?

```
▶ <head>…</head>
▼ <body style="margin:0px;" marginwidth="0" marginheight="0">
  ▼ <div class="GoogleActiveViewClass" id="DfaVisibilityIdentifier_2502805388804862259" style="position: relative;">
    ▼ <a target="_blank" href="http://adclick.g.doubleclick.net/aclk?sa=L&ai=BPsuqUnJ_U9u3H9CNlAeW1YCY…
    urce%3D2095%26utm_medium%3Dbanner%26utm_campaign%3Ddr%26dclid%3D%25edclid!">
        <img src="http://s0.2mdn.net/viewad/2769103/ProtectYourself_NO_2_2014_300x100.gif" alt="Advertisement" border="0" width="300" height=
        "100">
      </a>
    </div>
    <script type="text/javascript" async src="//pagead2.googlesyndication.com/pagead/js/lidar.js"></script>
```

Robots.txt

- Intended to guide search engines
- Show directories/files to ***not*** index - Why?
- What will attackers look for?

Robots.txt

- Intended to guide search engines
- Show directories/files to ***not*** index - Why?
- What will attackers look for?

- Auto-ban at WAF for following?
- Spider Trap

Unvalidated Redirect

Usage:

http://www.site.com/?goto=http://www.google.com

Unvalidated Redirect

Usage:

http://www.site.com/?goto=http://www.google.com

Example:

http://mysite.com/?goto=http://www.evilhackersite.com

Unvalidated Redirect

Usage:

http://www.site.com/?goto=http://www.google.com

Example:

http://mysite.com/rd/?dku=%68%74%74%70%3a%2f%2f1249763400

Unvalidated Redirect

Usage:

http://www.site.com/?goto=http://www.google.com

Example:

http://mysite.com/rd/?dku=%68%74%74%70%3a%2f%2f1249763400

PHISH!!

Cookies & Session Data

Use a plugin!

- **Firefox:** Cookie Manager, Edit Cookies
- **Chrome:** Edit this Cookie, Cookies – app for Chrome
- **Safari:** SafariCookieEditor
- Use a Proxy: Burp, ZAP
- Do it manually!

Cookies & Session Data

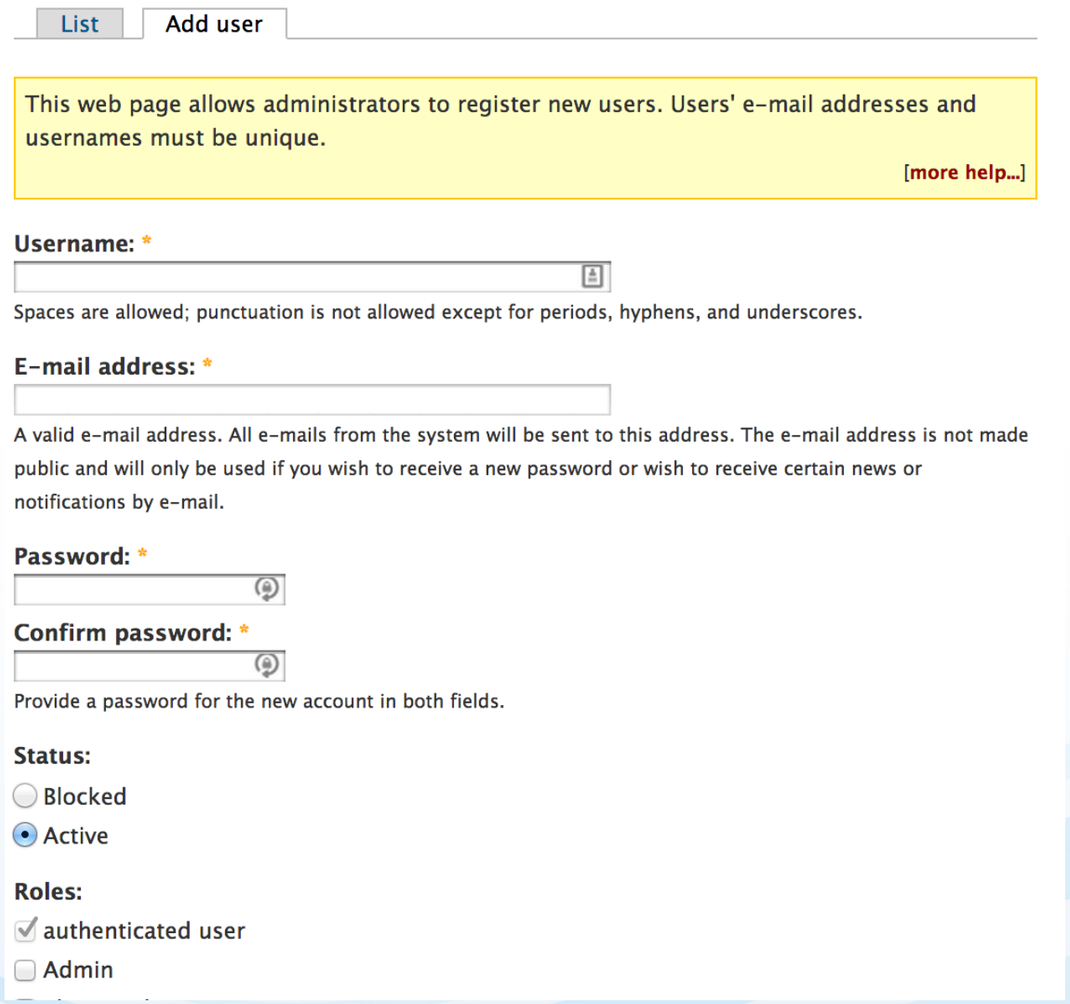
Session replays and Authentication Bypass

Secure flag set?

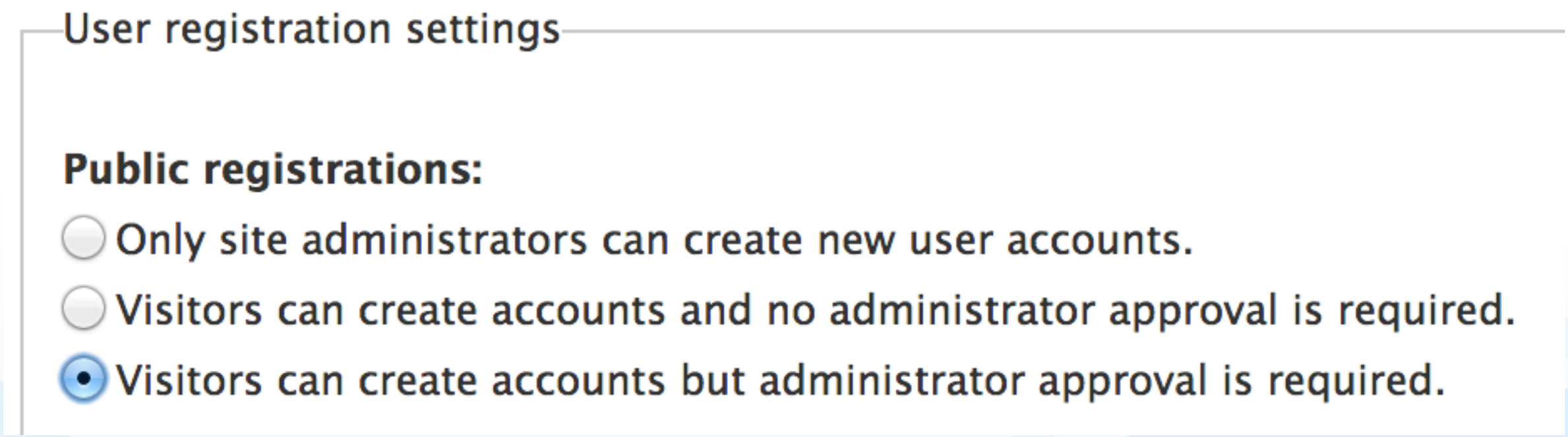
Ars Technica: “Unsafe cookies leave WordPress accounts open to hijacking, 2-factor bypass” – May 26, 2014

Original Research: https://zyan.scripts.mit.edu/blog/wordpress-fail/

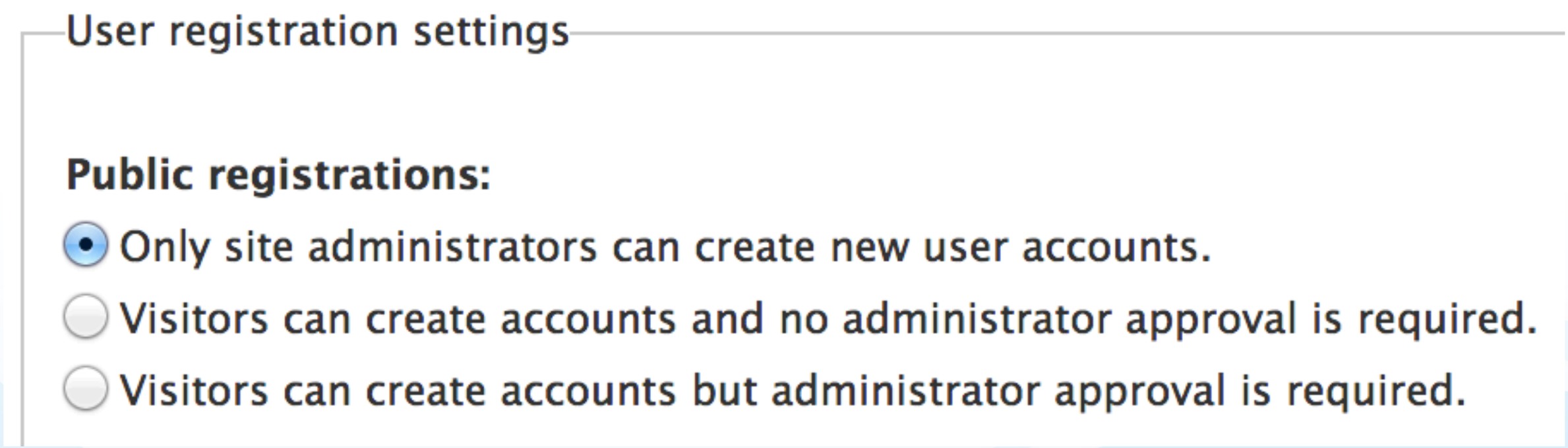
Administrator Area



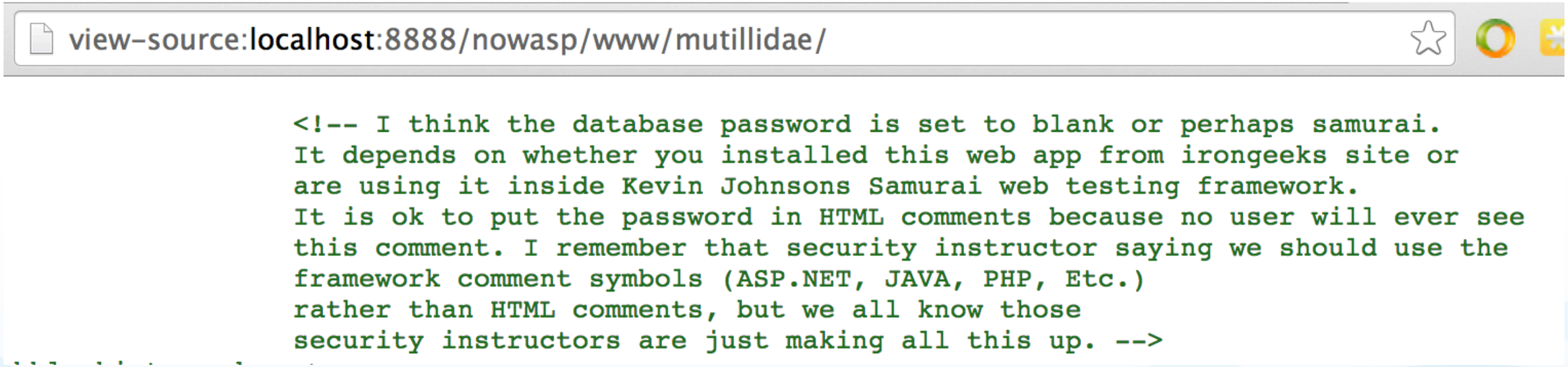
Administrator Area



Administrator Area



HTML Source Comments



NerdyData **Or use NerdyData.com: search “ToDo:”**

Weak/Default Passwords

http://www.cirt.net/passwords

http://resources.infosecinstitute.com/10-popular-password-cracking-tools/

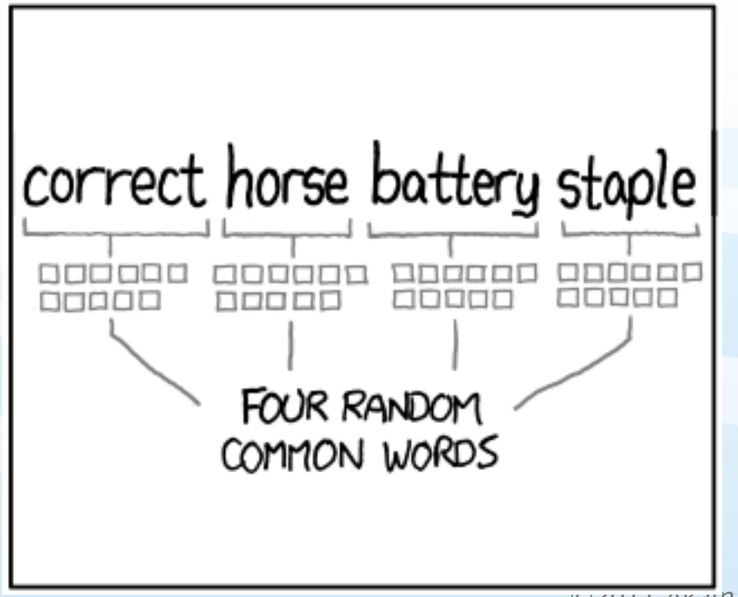
Complex and Long > Length > Complexity

Keyspace ^ length = total # possibilities

http://arstechnica.com/security/2012/12/25-gpu-cluster-cracks-every-standard-windows-password-in-6-hours/

95^8 in just 5 ½ hours, 350B guesses per second

Length of 6, cracks in 2 seconds



Weak/Broken Secure Communications

- Outdated SSL can be broken (http://www.poodletest.com)
- Every secure page must be served via SSL
  - sslstrip by Moxie Marlinspike
- Files requiring authentication must force authentication

Old Versions of Site

File extensions like .old, .bak, .tmp, .svn, .tar, .gz, .git

Example: index.php.old

http://pen-testing.sans.org/blog/pen-testing/2012/12/06/all-your-svn-are-belong-to-us

https://www.google.co.in/search?q=filetype%3Asql+site%3Acom+and+%22insert+into%22+admin+%222014%22&oq=filetype%3Asql+site%3Acom+and+%22insert+into%22+admin+%222014%22&aqs=chrome..69i57j69i58.237j0j9&sourceid=chrome&es_sm=91&ie=UTF-8

File Uploads

- Usually intended to upload attachments, images, etc.
- Specific file type intended

Problems:

- Other file types allowed?
- Executable file types?
- End user control where file goes?

Business Logic Flaws

- Not scannable
- Know how site should work
- Usually due to unvalidated user input

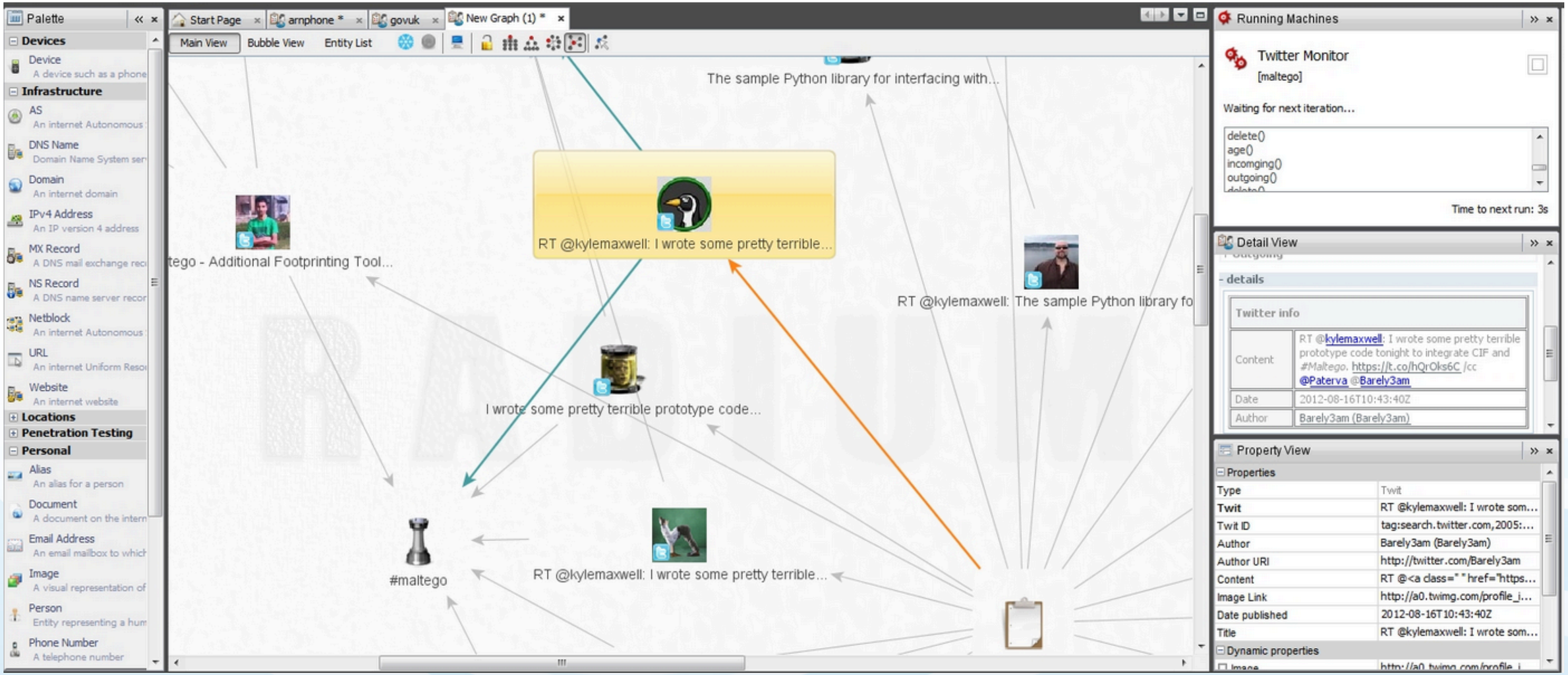
CMS Frameworks

- Wordpress, Drupal, Joomla
- Set it and forget it
- Easy to set up, requires frequent maintenance/updates
- Plugins/modules/custom code
- Templates/themes
- Oct 15, 2014: https://www.drupal.org/SA-CORE-2014-005

Company/Employee Information

- Phone book
- Organizational Chart
- OSINT
- Facebook/Twitter/Blogs/Cat pages
- Maltego
- Social Engineering!

Company/Employee Information



Outdated Operating System

http://www.exploit-db.com

http://www.cvedetails.com/

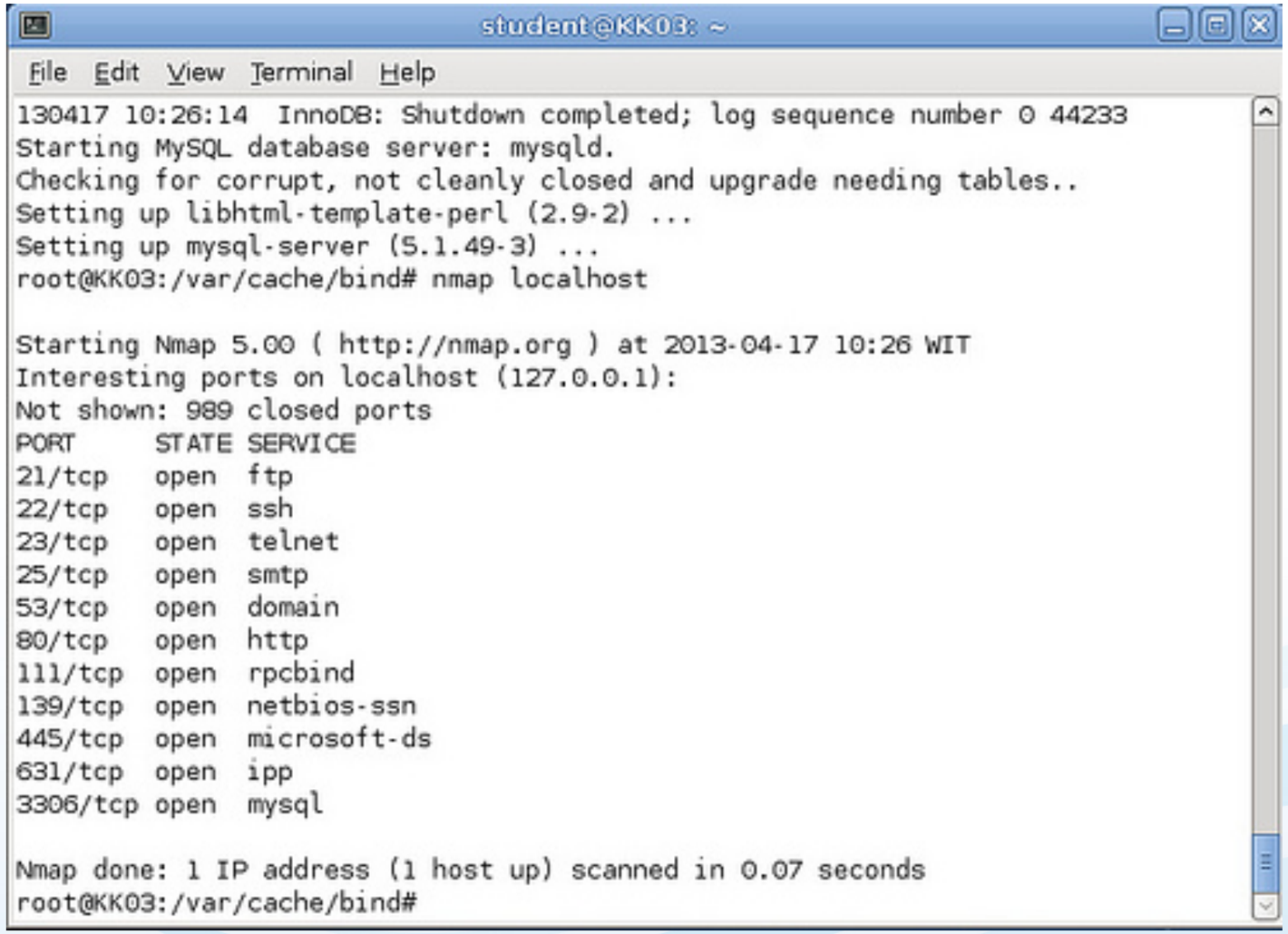
Many others!

DNS Hijacking

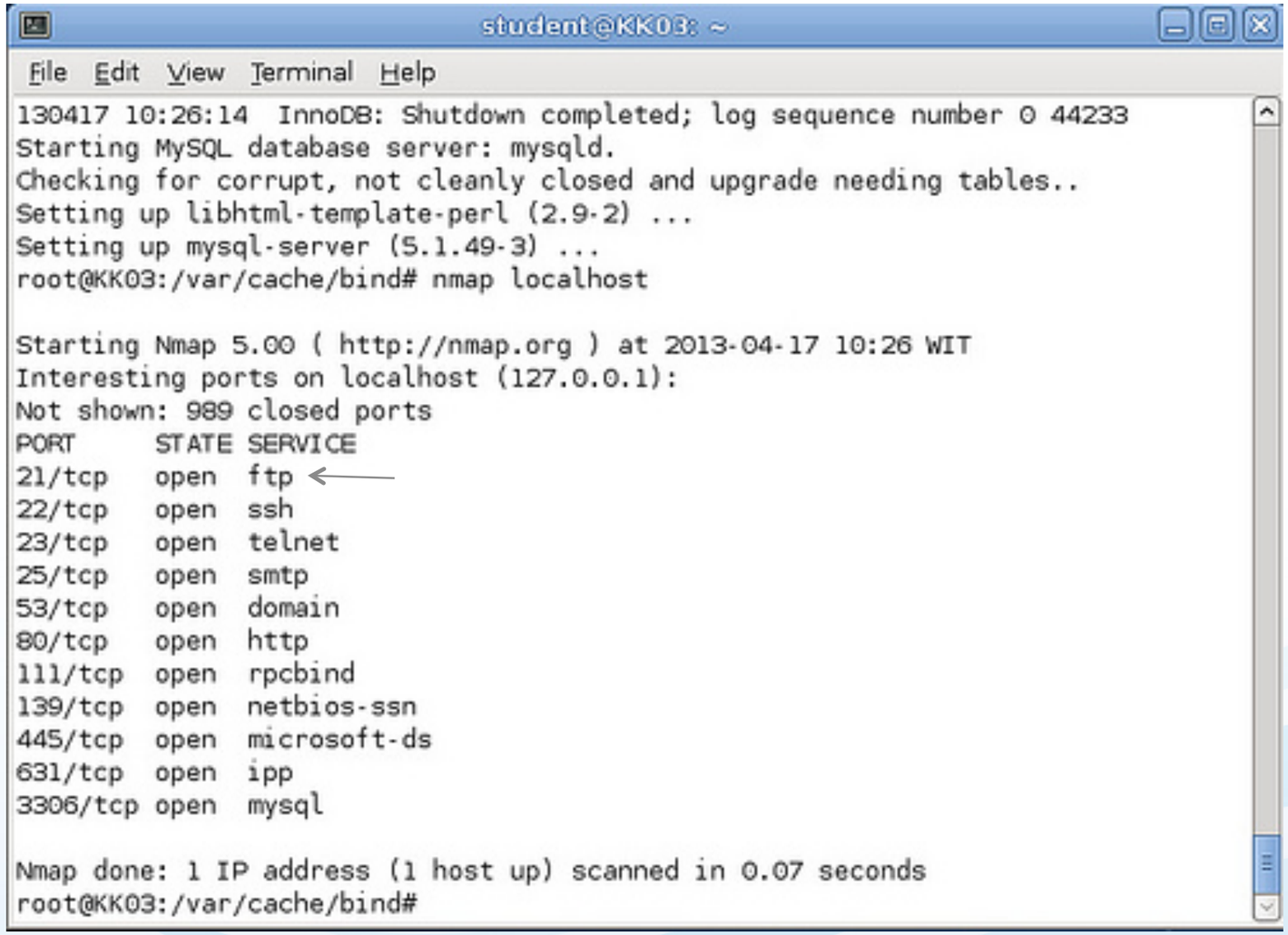
Set locks at two levels:

- Client
  - ClientTransferProhibited
  - ClientDeleteProhibited
  - ClientUpdateProhibited
- Server
  - ServerTransferProhibited
  - ServerDeleteProhibited
  - ServerUpdateProhibited

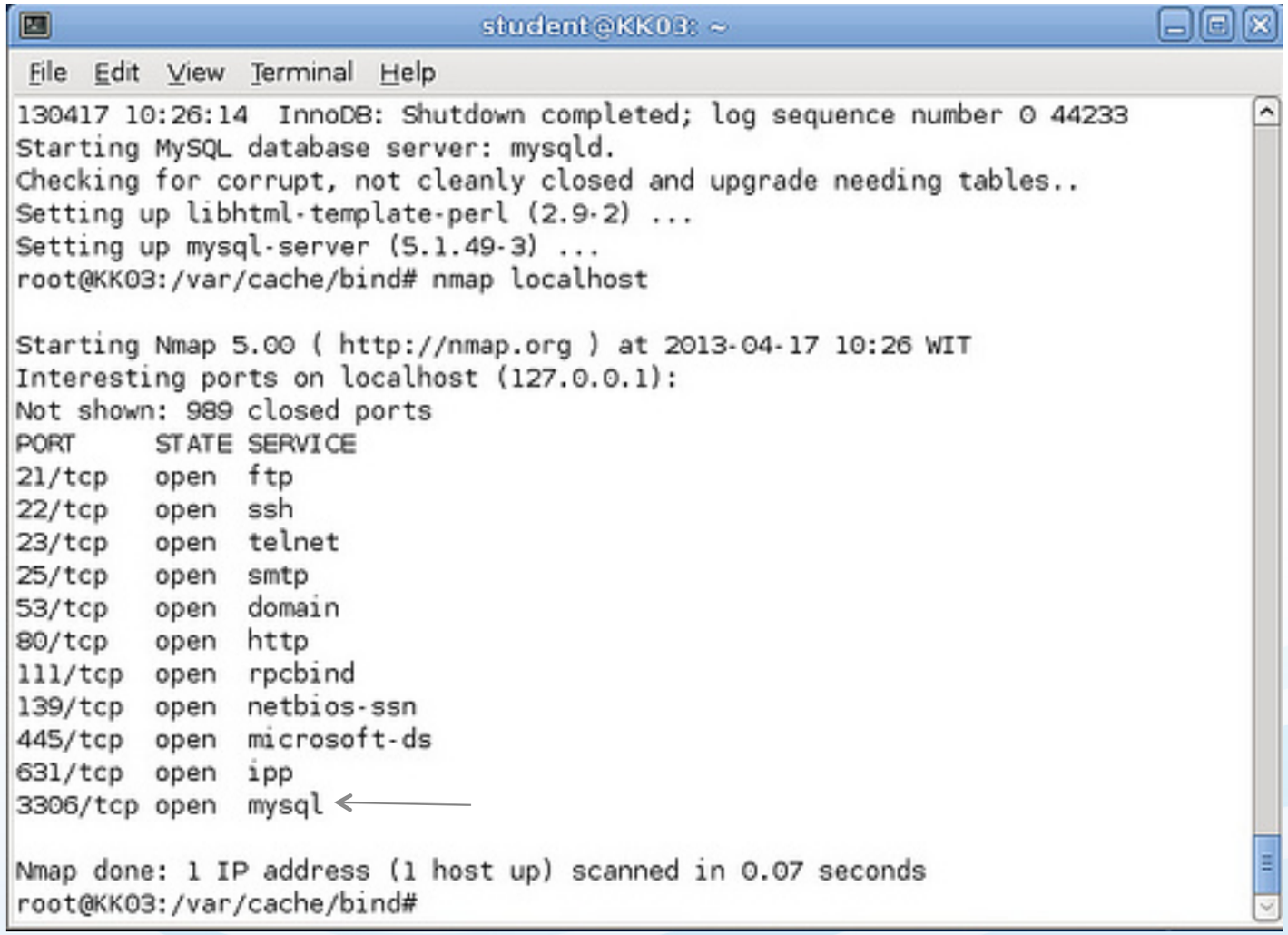
Running Unnecessary Services



Running Unnecessary Services



Running Unnecessary Services



Scanners!

“Web Application Vulnerability Scanners are the automated tools that scan web applications to look for known security vulnerabilities such as cross-site scripting, SQL injection, command execution, directory traversal and insecure server configuration.”

- https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools

Examples:

- Acunetix
- Nikto
- Nessus
- NTOSpider
- AppScan
- WebInspect

Questions?

Oh and…

https://goo.gl/25jV8d

Contact:

Patrick Laverty

@plaverty9

plaverty@akamai.com