



# How a Hacker Sees Your Site

Patrick Laverty  
Security Response Engineer  
Akamai CSIRT



# Patrick Laverty

Akamai Technologies - SIRT

[plaverty@akamai.com](mailto: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



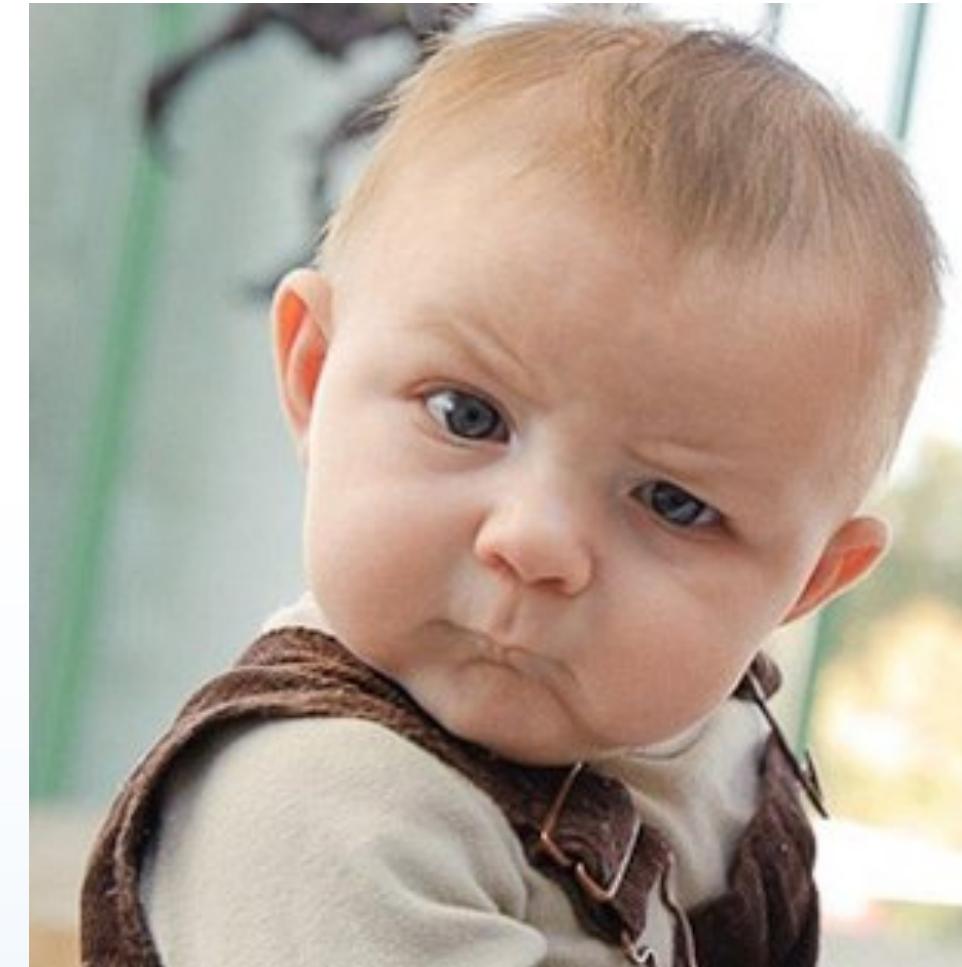
# How Hard Is It Really?



# What Is A Hacker Looking For?



Not all that much...

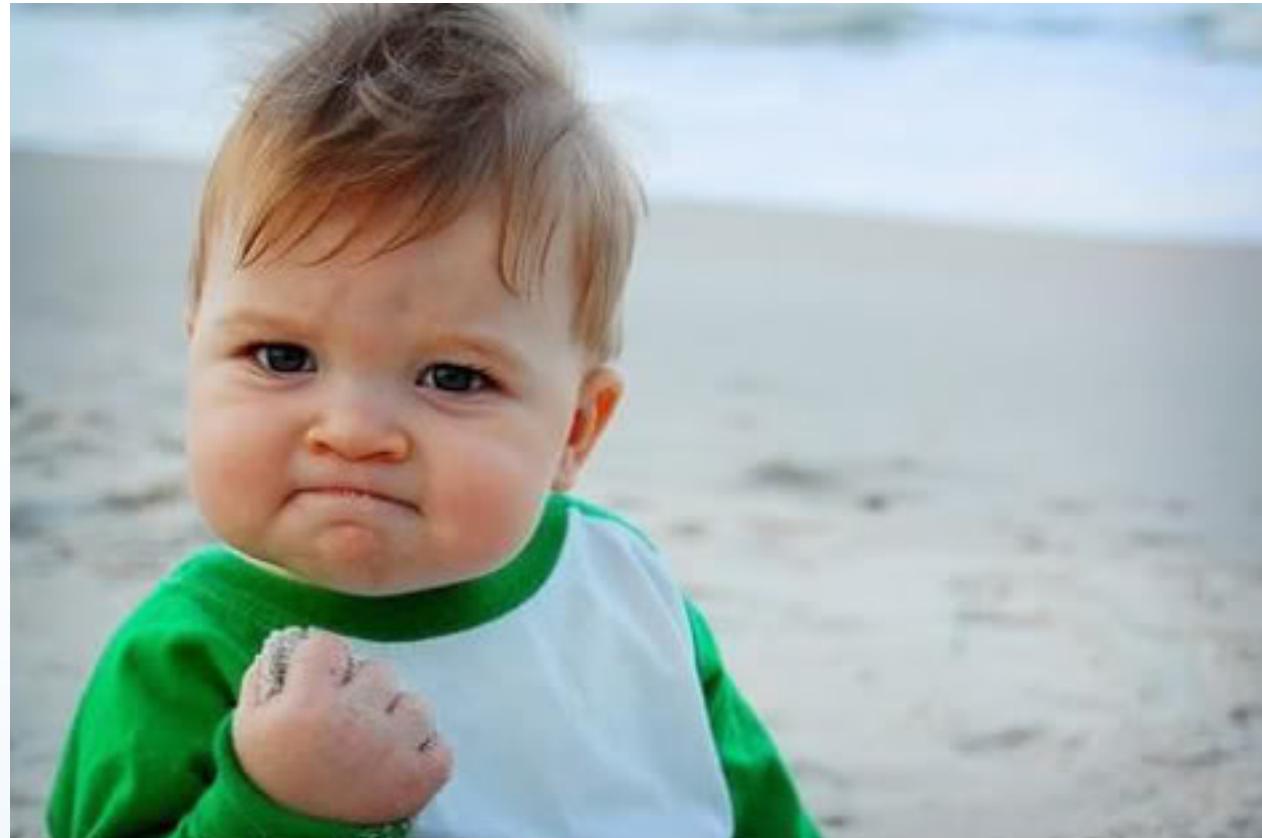


# What Is A Hacker Looking For?



- URL Parameters
- Data Inputs
- 3<sup>rd</sup> 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



localhost:8888/nowasp/www/mutillidae/index.php?popUpNotificationCode=L1H2&page=home.php

## OWASP Mutillidae II: Web Pwn in Mass Production

Version: 2.6.10 Security Level: 0 (Hosed) Hints: Enabled (2 - Noob) Not Logged In

Home | Login/Register | Toggle Hints | Toggle Security | Reset DB | View Log | View Captured Data | Hide Popup Hints | Enforce SSL

**Mutillidae: Deliberately Vulnerable Web Pen-Testing Application**

Like Mutillidae? Check out how to help

What Should I Do? Video Tutorials

Help Me! Listing of vulnerabilities

Bug Tracker Bug Report Email Address

What's New? Click Here Release Announcements

PHP MyAdmin Console Feature Requests

Installation Instructions Tools

Getting Started: Project Whitepaper

Release Announcements

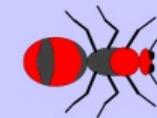
Video Tutorials

A screenshot of a web browser displaying the OWASP Mutillidae II application. The URL in the address bar is localhost:8888/nowasp/www/mutillidae/index.php?popUpNotificationCode=L1H2&page=home.php. The page title is "OWASP Mutillidae II: Web Pwn in Mass Production". The header includes version information (2.6.10), security level (0 Hosed), hints status (Enabled 2 - Noob), and user status (Not Logged In). A navigation menu on the left lists categories like OWASP 2013, OWASP 2010, OWASP 2007, Web Services, HTML 5, Others, Documentation, and Resources. Below this is a sidebar with links to "Getting Started: Project Whitepaper", "Release Announcements", and "Video Tutorials". The main content area features a heading "Mutillidae: Deliberately Vulnerable Web Pen-Testing Application" and a callout "Like Mutillidae? Check out how to help". It contains ten items arranged in two columns, each with an icon and a link: "What Should I Do?" (YouTube icon), "Video Tutorials" (YouTube icon), "Help Me!" (Help icon), "Listing of vulnerabilities" (Warning light icon), "Bug Tracker" (Headset icon), "Bug Report Email Address" (Email icon), "What's New? Click Here" (New icon), "Release Announcements" (Twitter bird icon), "PHP MyAdmin Console" (PMA icon), "Feature Requests" (Gear icon), "Installation Instructions" (Toolbox icon), and "Tools" (Wrench icon). A footer at the bottom shows a decorative pattern of coins and the number 35.

# URL Query Parameters

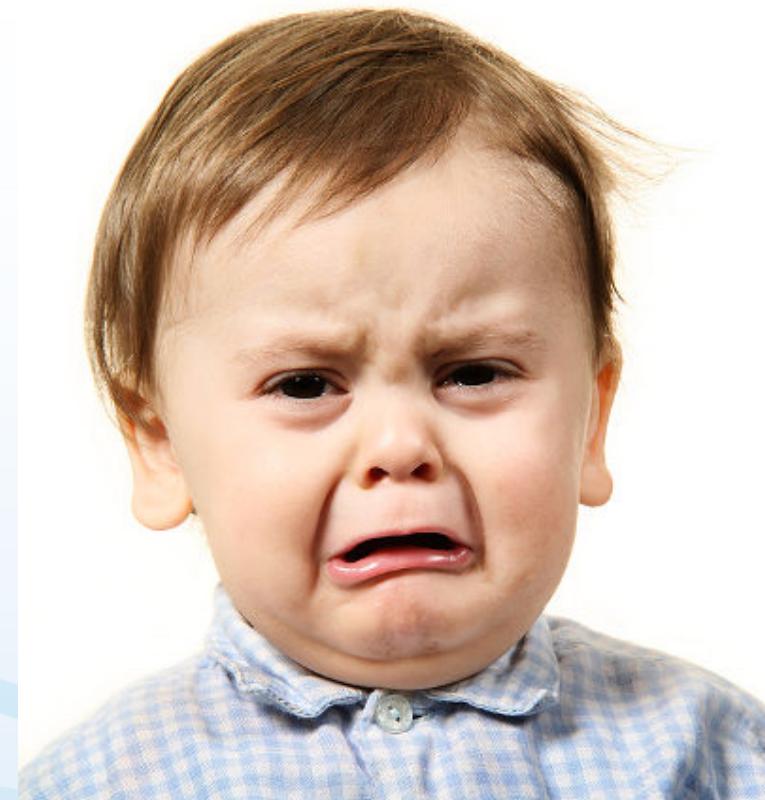


st:8888/nowasp/www/mutillidae/index.php?popUpNotificationCode=L1H2&page=home.php

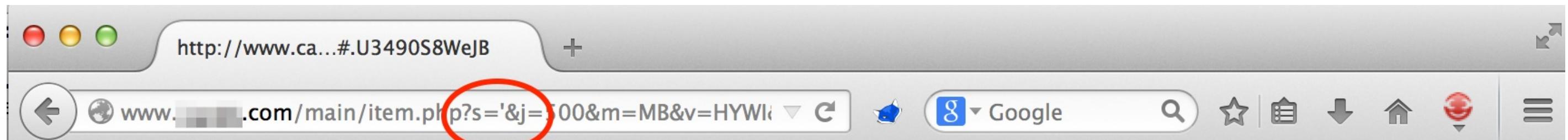


**OWASP Mutillidae II: Web Pwn in Mass Production**

# Data Inputs – SQL Injection

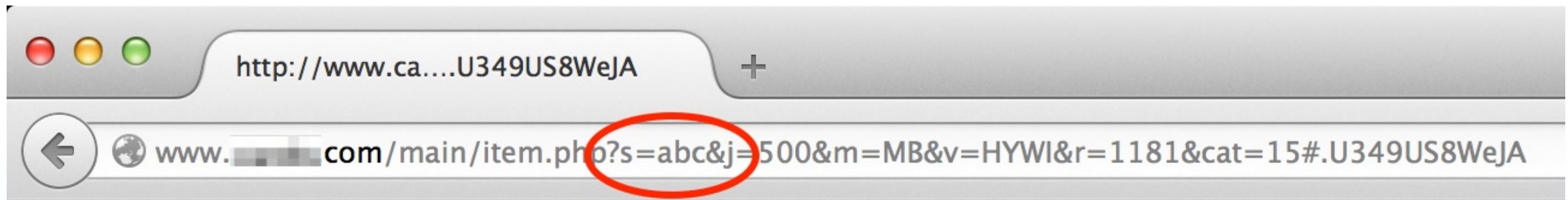


# Data Inputs – SQL Injection



You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '\" at line 1

# Data Inputs – SQL Injection



Unknown column 'abc' in 'where clause'

# 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
```

## Add blog for admin

**Note: <b>,</b>,<i>,</i>,<u> and </u> are now allowed in blog entries**

Save Blog Entry

## Add blog for admin

**Note: <b>,</b>,<i>,</i>,<u> and </u> are now allowed in blog entries**

```
<script>alert("XSS")</script>
```

Save Blog Entry

# Data Inputs - XSS



## View Blogs

Back      Help Me!

**View Blog Entries**

**Add To Your Blog**

The page at localhost:8888 says:  
XSS

OK

Select Author and Click to View Blog

Please Choose Author      View Blog Entries

2 Current Blog Entries			
	Name	Date	Comment
1	admin	2014-05-22 15:49:06	

# 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



XSSposed

XSS Archive | Top Vulnerable Domains | Top Security Researchers | Wish List | About | Search

REPORT Report cross-site scripting vulnerabilities

EMAIL ALERTS Get notifications about XSS on your website

5163 reported vulnerabilities, 455 fixed vulnerabilities  
4253 vulnerable websites, 822 vulnerable VIP websites  
162 security researchers, 186 notification subscribers  
Launched on 18/06/14, latest submission on 18/10/14

---

a Top Alexa Rank Websites

- ask.com by SymbianSyMoh
- microsoft.com by E1337
- imdb.com by xsscrappy
- craigslist.org by xsscrappy
- xhamster.com by Nasrul07
- bbc.co.uk by SecBit
- pornhub.com by Anonymous
- espn.go.com by xsscrappy
- dailymail.co.uk by xsscrappy

---

TOP XSS Researchers

RANK	RESEARCHER	VULNERABILITIES REPORTED
1	V1RUS4	794
2	watt	332
3	Nasrul07	282
4	Dshellnoi_Unix	271
5	X-P10it hun73r	177
6	E1337	169

---

Latest Submissions

- soldsecure.com XSS by en4rab 18/10/2014
- skillsforsecurity.org.uk Open Redirect by en4rab 18/10/2014
- skillsforsecurity.org.uk XSS by en4rab 18/10/2014
- informeseogratis.com Open Redirect by sinkmanu 18/10/2014
- buscadorweb.com Open Redirect by sinkmanu 18/10/2014
- megafutbol.net Open Redirect by sinkmanu 18/10/2014

# Data Inputs – XSSposed.com



 XSS  
posed

XSS Archive | Top Vulnerable Domains | Top Security Researchers | Wish List | About | Search

# 3rd Party Content



**Legal View with Ashleigh Banfield**  
12pm ET / 9am PT  
Ashleigh Banfield tackles the day's most compelling legal stories

**Watch CNN**

**The Situation Room**  
5pm ET / 2pm PT on CNN

**Erin Burnett: OutFront**  
7pm ET / 4pm PT on CNN

**AC 360**  
8pm ET / 5pm PT on CNN

**Anthony Bourdain**  
9pm ET/PT on CNN

**Morgan Spurlock**  
10pm ET/PT on CNN

**Trending Video**

Cops: 3 children found dead inside home 1:03

Six Iranians arrested for 'Happy' video 2:50

Silver: We are doing the right thing 4:26

Actor Michael Jace charged with murder 2:36

Show host calls airing Sam kiss 'wrong' 3:29

**View Collections**

ADVERTISEMENT

**THE DECADE THAT CHANGED THE WORLD.**

ADVERTISEMENT

Protect yourself with **TransUnion**  
Start with your Credit Score & Report!  
**CLICK HERE**  
**TransUnion.**

ADVERTISEMENT

**SERIES PREMIERE**  
**MAY 29<sup>TH</sup>**

**81°** HI 89° LO 65°  
Atlanta, GA Weather forecast

**SEARCH**  
POWERED BY Google

# 3<sup>rd</sup> 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/aclick?sa=L&ai=BPsuqUnJ_U9u3H9CNlAeW1YCY...
      urce%3D2095%26utm_medium%3Dbanner%26utm_campaign%3Ddr%26dclid%3D%25edclid!">
        
      </a>
    </div>
    <script type="text/javascript" async src="//pagead2.googlesyndication.com/pagead/js/af/dar.js"//></script>
```

# Robots.txt



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

- 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!!**



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!

## 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



List Add user

This web page allows administrators to register new users. Users' e-mail addresses and usernames must be unique. [\[more help...\]](#)

**Username:** \*  (

Spaces are allowed; punctuation is not allowed except for periods, hyphens, and underscores.

**E-mail address:** \*

A valid e-mail address. All e-mails from the system will be sent to this address. The e-mail address is not made public and will only be used if you wish to receive a new password or wish to receive certain news or notifications by e-mail.

**Password:** \*  (

**Confirm password:** \*  (

Provide a password for the new account in both fields.

**Status:**  
 Blocked  
 Active

**Roles:**  
 authenticated user  
 Admin

## User registration settings

### Public registrations:

- Only site administrators can create new user accounts.
- Visitors can create accounts and no administrator approval is required.
- Visitors can create accounts but administrator approval is required.

## User registration settings

### Public registrations:

- Only site administrators can create new user accounts.
- Visitors can create accounts and no administrator approval is required.
- Visitors can create accounts but administrator approval is required.

# HTML Source Comments



```
<!-- I think the database password is set to blank or perhaps samurai.  
It depends on whether you installed this web app from irongeeks site or  
are using it inside Kevin Johnsons Samurai web testing framework.  
It is ok to put the password in HTML comments because no user will ever see  
this comment. I remember that security instructor saying we should use the  
framework comment symbols (ASP.NET, JAVA, PHP, Etc.)  
rather than HTML comments, but we all know those  
security instructors are just making all this up. -->  
....
```



Or use [NerdyData.com](http://NerdyData.com): search “ToDo:”

# Weak/Default Passwords



<http://www.cirt.net/passwords>

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

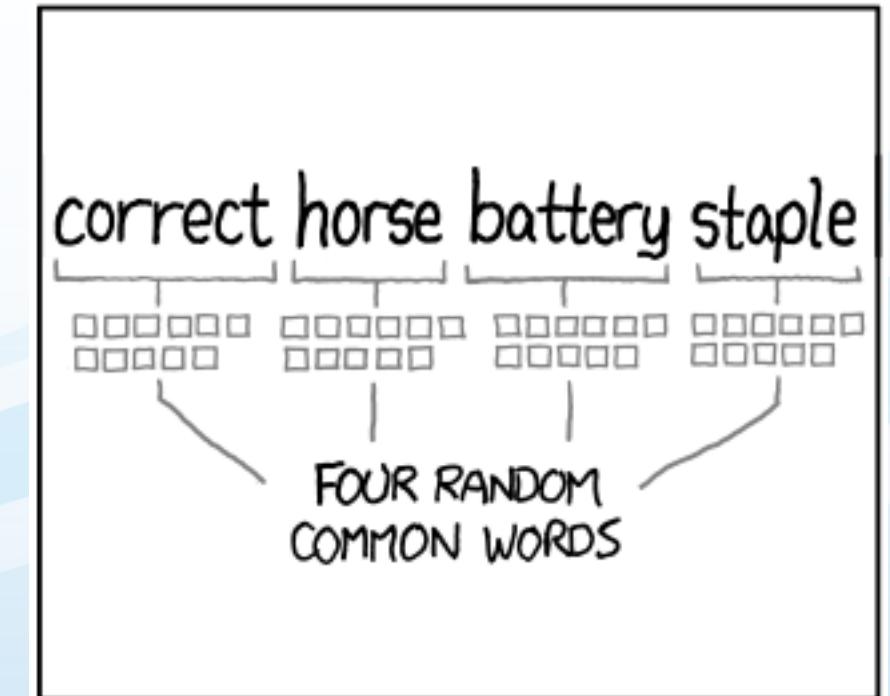
Complex and Long > Length > Complexity

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](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



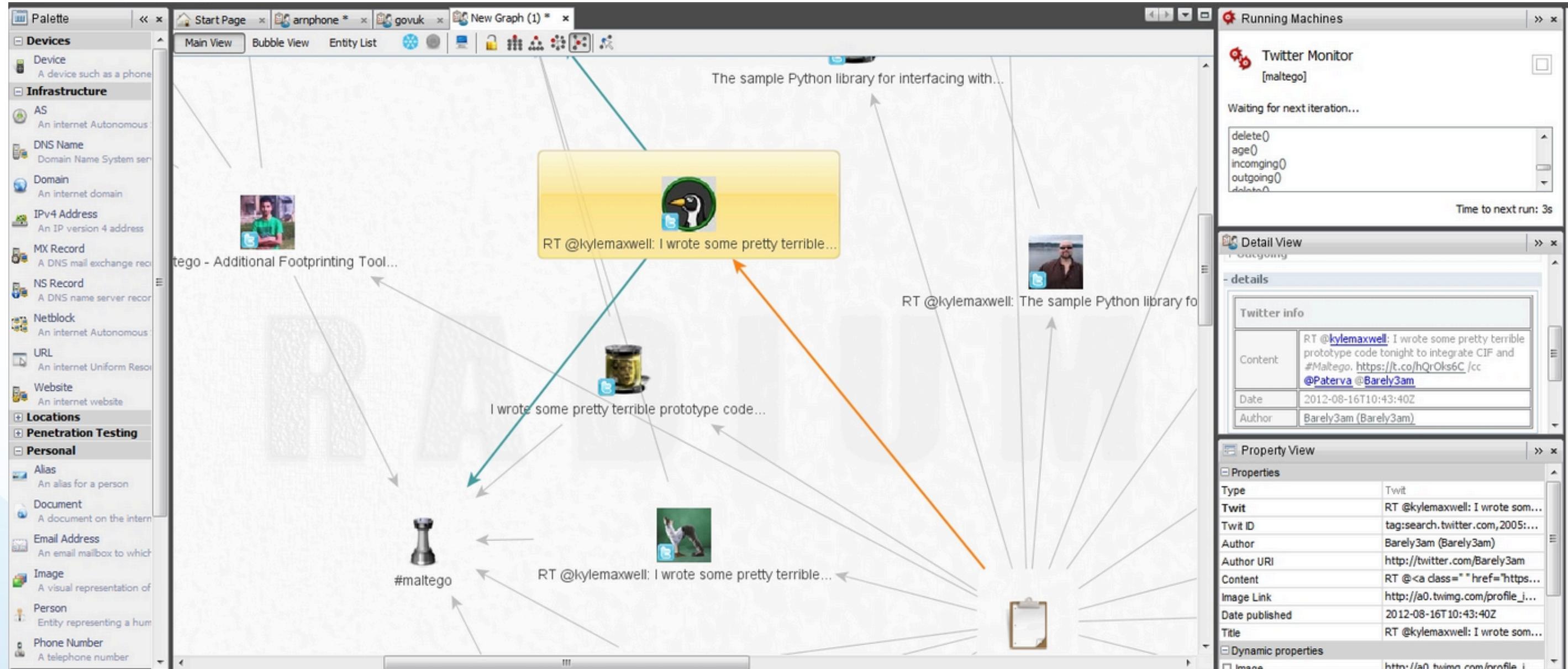
- Wordpress, Drupal, Joomla
- Set it and forget it
- Easy to set up, requires frequent maintenance/updates
- Plugins/modules/custom code
- Templates/themes
- Oct 15, 2014: <https://www.drupal.org/SA-CORE-2014-005>

# 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



```
student@KK03: ~
File Edit View Terminal Help
130417 10:26:14 InnoDB: Shutdown completed; log sequence number 0 44233
Starting MySQL database server: mysqld.
Checking for corrupt, not cleanly closed and upgrade needing tables..
Setting up libhtml-template-perl (2.9-2) ...
Setting up mysql-server (5.1.49-3) ...
root@KK03:/var/cache/bind# nmap localhost

Starting Nmap 5.00 ( http://nmap.org ) at 2013-04-17 10:26 WIT
Interesting ports on localhost (127.0.0.1):
Not shown: 989 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@KK03:/var/cache/bind#
```

# Running Unnecessary Services



```
student@KK03: ~
File Edit View Terminal Help
130417 10:26:14 InnoDB: Shutdown completed; log sequence number 0 44233
Starting MySQL database server: mysqld.
Checking for corrupt, not cleanly closed and upgrade needing tables..
Setting up libhtml-template-perl (2.9-2) ...
Setting up mysql-server (5.1.49-3) ...
root@KK03:/var/cache/bind# nmap localhost

Starting Nmap 5.00 ( http://nmap.org ) at 2013-04-17 10:26 WIT
Interesting ports on localhost (127.0.0.1):
Not shown: 989 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp ←
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@KK03:/var/cache/bind#
```

# Running Unnecessary Services



```
student@KK03: ~
File Edit View Terminal Help
130417 10:26:14 InnoDB: Shutdown completed; log sequence number 0 44233
Starting MySQL database server: mysqld.
Checking for corrupt, not cleanly closed and upgrade needing tables..
Setting up libhtml-template-perl (2.9-2) ...
Setting up mysql-server (5.1.49-3) ...
root@KK03:/var/cache/bind# nmap localhost

Starting Nmap 5.00 ( http://nmap.org ) at 2013-04-17 10:26 WIT
Interesting ports on localhost (127.0.0.1):
Not shown: 989 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
631/tcp   open  ipp
3306/tcp  open  mysql <-----
Nmap done: 1 IP address (1 host up) scanned in 0.07 seconds
root@KK03:/var/cache/bind#
```

# 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](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 Lavery

@plaverty9

plaverty@akamai.com