Web 2.0 Threats Illustrated
About Me

- Robert Hansen - CEO
- SecTheory Ltd
  - Bespoke Boutique Internet Security
    - Web Application/Browser Security
    - Network/OS Security
    - http://www.sectheory.com/
- FallingRock Networks
- Advisory capacity to start-ups
- Founded the web application security lab
  - http://ha.ckers.org/ - the lab
  - http://sla.ckers.org/ - the forum
## Primer on Same Origin Policy

<table>
<thead>
<tr>
<th>URL</th>
<th>Outcome</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.yoursite.com/dir/page.html">http://www.yoursite.com/dir/page.html</a></td>
<td>Success</td>
<td>Same domain</td>
</tr>
<tr>
<td><a href="http://www.yoursite.com/dir2/other-page.html">http://www.yoursite.com/dir2/other-page.html</a></td>
<td>Success</td>
<td>Same domain</td>
</tr>
<tr>
<td><a href="https://www.yoursite.com/">https://www.yoursite.com/</a></td>
<td>Failure (Except Cookies)</td>
<td>Different protocol</td>
</tr>
<tr>
<td><a href="http://www.yoursite.com:8080/">http://www.yoursite.com:8080/</a></td>
<td>Failure (Except Cookies)</td>
<td>Different port</td>
</tr>
<tr>
<td><a href="http://news.yoursite.com/blog/">http://news.yoursite.com/blog/</a></td>
<td>Failure (Except Cookies)</td>
<td>Different host</td>
</tr>
</tbody>
</table>
• Cross domain images/iframes/CSS/JS calls, etc...
• Difference between malicious and benign x-domain requests are almost impossible to tell the difference.
• GET and POST are equally vulnerable.
• Affects nearly all websites – banks, .gov, etc..
CSRF Mitigation

- Check referrer
  - Turn referrer off
  - Meta refresh, https or JS
- Use a nonce (EG: `<input type="hidden" name="nonce" value="5jjkhu431ju1i8d9r14"`>
  - Make the user click on it for me or steal it
- Embed the link in a flash movie
  - Make the user click on it for me or steal it
public function getDateLastUpdated($format = '%x')
{
    if ($this->date_last_updated === null || $this->date_last_edited === null)
        return null;
    elseif (!is_int($this->date_last_updated))
    { // a non-timestamp value was set externally, so we
        $ts = strtotime($this->date_last_updated);
        if ($ts === -1 || $ts === $this->date_last_edited)
            throw new PropertyAccessException('Invalid date: ' . $this->date_last_updated);
    } else {
        $ts = $this->date_last_edited;
    }
    if ($format === null) {
        return $ts;
    } elseif (strpos($format, '%') !== false)
    return strftime($format, $ts);
    else {
        return date($format, $ts);
    }
}
• http://ha.ckers.org/xss.html
Clickjacking 101
Clickjacking 101

- Ronald’s flash settings manager subversion...

This is a non-malicious proof of concept based upon clickjacking, this poc leverages all security settings, which allow cross domain access. Please do notice that once you checked, your Flash settings will allow for cross domain access. To un-check go to this page: undo flash settings credits: Robert Hansen, Jeremiah Grossman, PDF, rydh
Clickjacking 101

- PDP’s version...

All your sites are belong to us!

**Do you allow AJAX?**
AJAX will improve your user experience!

- [ ] Never ask again
  - ![Allow](allow.png)
# Delete User Accounts

<table>
<thead>
<tr>
<th>Name</th>
<th>Member ID/Email Address</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mike Tedlo</td>
<td><a href="mailto:miker@verizon.net">miker@verizon.net</a></td>
<td></td>
</tr>
<tr>
<td>Chris Miller</td>
<td><a href="mailto:chris9441@verizon.com">chris9441@verizon.com</a></td>
<td></td>
</tr>
<tr>
<td>Jan Miller</td>
<td><a href="mailto:jan9441@verizon.com">jan9441@verizon.com</a></td>
<td></td>
</tr>
<tr>
<td>Curran Smith</td>
<td><a href="mailto:curran9721@verizon.com">curran9721@verizon.com</a></td>
<td></td>
</tr>
</tbody>
</table>
Auto-purchase

Shopping Cart Contents
1 x Heritage Grunge Clikit  
- Zip Part 1: Download

Sub-Total: $3.50
Free Shipping: $0.00
Discount Coupons: couponcode: -$3.50
Total: $0.00

Shipping Method: Free Shipping
Payment Method:

Final Step
- continue to confirm your order. Thank you!
Buy stocks

Confirm Order

Date: 06/06/2007
Time: 07:38 AM
Order Status: AUTO
Preferred ECII

Details

Buy PCU 1 Share
Market: N/A
Buy Southern Copper Corporation Common Stock (PCU:NYSE)
Bid: 78.26  Ask: 91.73  Last trade: 91.73

Estimated total cost: $91.73

Quote

CANCEL ORDER  SEND ORDER
Router Reset

D-Link DFL-700 Network Security Firewall

Restart / Reset
- Quick restart: reset interfaces and re-read configuration
- Full restart: restart from power-on state

Reset to factory defaults

You can restore the unit to factory defaults. This means that all configuration parameters will be wiped, and all firmware upgrades removed.

On the next start-up, its LAN IP address will be 192.168.1.1, and the web GUI will begin with the setup wizard. It will not accept connections on any interface other than the LAN interface.

Reset to Factory Defaults
### Delete Firewall Rules

#### Firewall > Access Rules

<table>
<thead>
<tr>
<th>Priority</th>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Action</th>
<th>Options</th>
<th>Enable</th>
<th>Configure</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>WLAN</td>
<td>192.168.168.168 (LAN)</td>
<td>HTTP Management</td>
<td>Allow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>LAN</td>
<td>192.168.168.168 (LAN)</td>
<td>HTTPS Management</td>
<td>Allow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>LAN</td>
<td>192.168.168.168 (LAN)</td>
<td>HTTP Management</td>
<td>Allow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>WLAN</td>
<td>192.168.168.168 (LAN)</td>
<td>HTTPS Management</td>
<td>Allow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>*</td>
<td>192.168.168.168 (LAN)</td>
<td>Key Exchange (IKE)</td>
<td>Allow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>192.168.168.168 (LAN)</td>
<td>*</td>
<td>Key Exchange (IKE)</td>
<td>Allow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>WLAN</td>
<td>WLAN</td>
<td>Any</td>
<td>Allow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>WLAN</td>
<td>WLAN</td>
<td>Any</td>
<td>Allow</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>WAN</td>
<td>WLAN</td>
<td>Any</td>
<td>Deny</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>LAN</td>
<td>*</td>
<td>Any</td>
<td>Allow</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>*</td>
<td>LAN</td>
<td>Any</td>
<td>Deny</td>
<td></td>
<td>✔️</td>
<td></td>
</tr>
</tbody>
</table>

Make Your Profile Public

Who Can View My Full Profile

- My Friends Only
- Public
- Only Users Over 18

Privacy Settings

- Friend Requests - Require email or last name
- Comments - approve before posting
- Hide Online Now
- Show My Birthday to my Friends
- Photos - No Forwarding
- Block Comments - Friends Only
- Friend Requests - No Bends
- Block Users Under 18 From Contacting Me
Deactivate Wordpress Plugins

Plugin Management

Plugins extend and expand the functionality of WordPress. Once a plugin is installed, you may activate it or deactivate it here.

<table>
<thead>
<tr>
<th>Plugin</th>
<th>Version</th>
<th>Description</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Akismet</td>
<td>2.1.4</td>
<td>Akismet checks your comments against the Akismet web service to see if they look like spam or not. You need a WordPress API key to use it. You can review the spam it catches under &quot;Comments.&quot; To show off your Akismet stats just put <code>&lt;php akismet_count(); ?&gt;</code> in your template. See also: <a href="https://www.wordpress.com/plugins/wp-stats/">WP Stats plugin</a> By Matt Mullenweg.</td>
<td>Activate, Edit</td>
</tr>
<tr>
<td>Hello Dolly</td>
<td>1.5</td>
<td>This is not just a plugin, it symbolizes the hope and enthusiasm of an entire generation summed up in two words sung most famously by Louis Armstrong. Hello, Dolly. When activated you will randomly see a lyric from Hello, Dolly in the upper right of your admin screen on every page. By <a href="https://www.wordpress.com/plugins/hello-dolly/">Matt Mullenweg</a>.</td>
<td>Deactivate, Edit</td>
</tr>
</tbody>
</table>

If something goes wrong with a plugin and you can't use WordPress, delete or rename that file in the `wp-content/plugins` directory and it will be automatically deactivated.
Digg
MySpace

HTML, CSS, and JavaScript may size, follow the mouse and make transparent third-party IFRAME content.
Google Bowling to the Extreme

- Slowloris...
- DNS Cache Poisoning is fixed...
  - Or is it?
  - Spoof static.competitor.com and include malware
- Persistent XSS
PHP File includes

- Robot pulls requests a page
- Page requests the file from www.hacked-site.com which contains a simple echo statement.
- Site executes the content if it’s vulnerable.
- If robot sees the echo’d statement of the file it requests a new file with the real payload at [www.hacked-site.com/realpayload.txt](http://www.hacked-site.com/realpayload.txt)
- Site executes new payload and bot propagates.
- Simple to turn into a worm...
- Modify some 404s instead of entire site.
I find that the best way to overcome a destructive temptation is to stare it in the face, without yielding to it. Some people find this approach crazy, even torturous. They’d rather throw away the carrot—the Blackberry, the chocolate, the pornography—than throw on the chastity belt and sleep with it. They feel that if the attraction is physically unattainable, they naturally can’t attain it, and their resolution is met.
Malvertizing

- Sell ads on behalf of name brand companies
- Time of day
- Geo IP
- Redirect to malware or offer malware for sale under the guise of security software
Future of Spamming

- Personas
  - Age
  - Demographic
  - Marital status
  - Interests
  - Zodiac
  - Birth date
  - Friends
  - Perfect weather
  - Locale
  - Etc...
Clouds of Insecurity

Hi,

Thank you for contacting us about payment processing services. If your credit cards or bank accounts don’t have to. If you have any questions about our Payment Service and our pricing, please don’t hesitate to ask.

As for PCI level 2 compliance, it is possible for you to build a PCI level 2 compliant infrastructure. And you have a data breach, you can take steps to mitigate the impact. From a business perspective, I recommend building a robust defense and risk management processes. If you have any questions on-site auditing; that is when you have a business on your risk management process.

Regard,

Cindy S.
Amazon Web Services
http://aws.amazon.com

Google Apps Security Questioned After Twitter Leak

Analysis: Twitter suffers a significant security breach, brought on by a Twitter employee's Google Apps account being hacked.

Seth H. Weintraub, Computerworld

Twitter uses Google Docs for information sharing. How do I know this? Well, it seems Twitter Inc. has had a pretty significant security breach, which was brought on by a Twitter employee's Google Apps account being hacked. Have a look below at one of the screenshots the hacker has sent to various news sites.

DoS, failure to segment data, access controls, going out of business… etc… etc…
Lots Of Other Stuff

- Inter-protocol exploitation
- SQL injection
- History stealing
- DNS rebinding
- RFC1918 cache poisoning
- Etc..
Thank you!

- Robert Hansen
  - http://www.sectheory.com – the company
  - http://ha.ckers.org – the lab
  - http://sla.ckers.org – the forum
  - Detecting Malice – the eBook
  - XSS Exploits – the book
  - robert@sectheory.com – the email