Jan Schaumann
@jschauma

Everything is Awful
(And You’re Not Helping)

An optimistic #infosec talk based on Shamir’s Laws of Security
Everything is Awful.
We've found 198,605 code results

- mathCodingClub/mcc-php-backend
- iPasha/nip
- jinguodong/shell
- andrew78910/otherCodes
- Rakeyjakey/leagueofassassins.co.uk
We've found 198,605 code results

1. mathCodingClub/mcc-php-backend — .README
   ```
   chmod 777 .
   ```

2. iPalash/nlp — compile.sh
   ```
   chmod 777 *
   ```

3. jinguodong/shell — chmod.sh
   ```
   chmod 777 *
   ```

4. andrew78910/otherCodes — chmod
   ```
   chmod 777 *
   ```

5. Rakeyjakey/leagueofassassins.co.uk — .htaccess
   ```
   chmod 777 *
   ```
Showing 351,777 available code results

Robocoder/phpvh – SqlInjectionGet.php
Showing the top two matches. Last indexed on Oct 3, 2015.

```php
<?php
mysql_query("SELECT * FROM table WHERE field='$_GET[query]'");
?>
```

Ewlided/SCARY – xss_and_sql_false_positive2.php
Showing the top two matches. Last indexed on Oct 1, 2015.

```php
<?php
$b="SELECT ".$_GET["id"]; 
$b=htmlspecialchars($b); 
mysql_query($b); # SQL
?>
```
Showing 351,777 available code results

roboCoder/phpv6 - SqlInjectionGet.php
Showing the top two matches. Last indexed on Oct 3, 2015.

```php
<?php
mysql_query("SELECT * FROM table WHERE field='$_GET[query]'");
?>
```

ewield/SCARY - xss_and_sql_false_positive2.php
Showing the top two matches. Last indexed on Oct 1, 2015.

```php
<?php
$b="SELECT ".$_GET['id'];
$b=htmlspecialchars($b);
mysql_query($b); # SQL
?>
```
@jschauma

BSidesSF 2016
<table>
<thead>
<tr>
<th>CVE-2015-2886</th>
<th>Remote</th>
<th>R7-2015-11.1</th>
<th>Predictable Information Leak</th>
<th>iBaby M6</th>
</tr>
</thead>
<tbody>
<tr>
<td>CVE-2015-2882</td>
<td>Local Net</td>
<td>R7-2015-12.1</td>
<td>Backdoor Credentials</td>
<td>Philips In.Sight B120/37</td>
</tr>
<tr>
<td>CVE-2015-2884</td>
<td>Local Net</td>
<td>R7-2015-14.1</td>
<td>Direct Browsing and Internet Viewing</td>
<td>Philips In.Sight B120/37</td>
</tr>
<tr>
<td>CVE-2015-2885</td>
<td>Local Net</td>
<td>R7-2015-15.1</td>
<td>Authentication &amp; Internet Viewing</td>
<td>Philips In.Sight B120/37</td>
</tr>
<tr>
<td>CVE-2015-2881</td>
<td>Local Net</td>
<td>R7-2015-15.2</td>
<td>Backdoor Credentials</td>
<td>Gynoid Wifi &amp; Internet Viewing</td>
</tr>
<tr>
<td>CVE-2015-2880</td>
<td>Device</td>
<td>R7-2015-16.1</td>
<td>Backdoor Credentials</td>
<td>Gynoid Wifi &amp; Internet Viewing</td>
</tr>
</tbody>
</table>
Smart toilet’s bidet hacked via Bluetooth, gives new meaning to ‘backdoor vulnerability’

By Sebastian Anthony on August 5, 2013 at 10:57 am | Comment
Smart toilet’s bidet hacked via Bluetooth, gives new meaning to ‘backdoor vulnerability’

By Sebastian Anthony on August 5, 2013 at 10:57 am | Comment

Attackers could cause the unit to unexpectedly open/close the lid, activate bidet or air-dry functions, causing discomfort or distress to user.
https://v.gd/thingOfTheDay
#Infosec “research”
(aka browsing Shodan)
And You We’re Not Helping.
One of these two people probably has some really interesting OpSec stories to tell...

... the other one keynotes RSAC.
Being really good at one thing does *not* make you an expert in *all* things.
#Infosec != Real World
Welcome to #Infosec,

where Hanlon’s Razor is dull.
Why Glenn can’t encrypt.
Hackers steal a hospital in Hollywood

https://v.gd/hackersStealHospital
Signature Needed

Please sign below using attached pen.

After signing, touch box below.

Butthole

https://v.gd/ccSignatureFun
MEET OUR DIGITAL PARENTING DASHBOARD

The All-inclusive Tool for Monitoring Your Child’s Digital and Mobile Activities
MEET OUR DIGITAL PARENTING DASHBOARD

uKnowKids.com database error exposed sensitive information on 1,700 kids

In violation of the Children's Online Privacy Protection Act (COPPA), uKnowKids.com gave public access to over 6.8 million private text messages, nearly 2 million images (many depicting children), and more than 1,700 detailed child profiles. This includes first and last names, email addresses, dates of birth, gps coordinates, social media access credentials, and more.
New Hampshire bill allows public libraries to run Tor in the face of federal challenges

https://libraryfreedomproject.org/
Don’t fuck with librarians.

https://v.gd/FreedomToRead
Everything is Awful.
And We’re Not Helping.
The “S” in RSA... 
...does not stand for Sean Penn.
Absolutely secure systems do not exist.
Absolutely secure systems do not exist.

To halve your vulnerability, you have to double your expenditure.
Absolutely secure systems do not exist.

To halve your vulnerability, you have to double your expenditure.

Cryptography is typically bypassed, not penetrated.
Absolutely secure systems do not exist.
Absolutely secure systems do not exist.
Keep calm, that’s fine.

Raising the cost of an attack is often sufficient.
Know your Threat Model.
HTTPS

Essential Complexity:
• exposes port 443
• uses TLS
• speaks HTTP

Accidental Complexity:
• weak Ciphers enabled
• 30 different versions of at least 5 different TLS libraries deployed
• apache, nodejs, nginx, Tomcat, ...
Reducing complexity reduces attack surface.
Data is your friend.
Preferred order list:
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-SHA384
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES256-SHA
AES128-GCM-SHA256
AES256-GCM-SHA384
AES128-SHA256
AES256-SHA256
AES128-SHA
AES256-SHA
DES-CBC3-SHA
ECDHE-RSA-RC4-SHA
RC4-SHA
Preferred order list:
ECDHE-RSA-AES128-GCM-SHA256
ECDHE-RSA-AES256-GCM-SHA384
ECDHE-RSA-AES128-SHA256
ECDHE-RSA-AES256-SHA384
ECDHE-RSA-AES128-SHA
ECDHE-RSA-AES256-SHA
AES128-GCM-SHA256
AES256-GCM-SHA384
AES128-SHA256
AES256-SHA256
AES128-SHA
AES256-SHA
SSL Report: search.yahoo.com (98.137.250.95)
Assessed on: Wed, 24 Feb 2016 20:20:46 UTC | Clear cache

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

This server supports TLS_FALLBACK_SCSV to prevent protocol downgrade attacks.

This site supports HTTP Strict Transport Security with long duration. Grade set to A+. MORE INFO »
Data is your friend.
Avg payout
Cumulative payout by vuln.
Data is your friend.
Why not “APT breaking our cryptos”?
Cryptography is typically bypassed, not penetrated.
US gov risk management
US gov risk management
US gov risk management

#infosec focus

- SQLi
- Keys on GitHub
- XSS

“APT” breaking our cryptos
Dat APT, tho.
Dat APT, tho.

From: John Doe
To: John Doe
Cc: 
Subject: ILOVEYOU

kindly check the attached LOVELETTER

LOVE-LETTER-FOR-Y

coming from me. OU.TXT.vbs

The Cyber Mafia
"If you think your problems can be solved by cryptography, you're probably wrong."

-- Robert Morris
<table>
<thead>
<tr>
<th>T</th>
<th>Key</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>INC0570977:</td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td></td>
<td>[S0]-201</td>
<td>Credentials Available on GitHub</td>
</tr>
<tr>
<td>!</td>
<td>IT-12560</td>
<td>[Security Issue - S0] Github Information Disclosure</td>
</tr>
<tr>
<td>!</td>
<td>IT-2716</td>
<td>[Security Issue S0] Credentials exposed on github</td>
</tr>
<tr>
<td>!</td>
<td>IT-2727</td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td>!</td>
<td>IT-2703</td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td>!</td>
<td>V-4300</td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td>!</td>
<td></td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td>T</td>
<td>Key</td>
<td>Summary</td>
</tr>
<tr>
<td>---</td>
<td>-----</td>
<td>---------</td>
</tr>
<tr>
<td>![ ]</td>
<td>INC0570977: [Security Issue S0] Credentials exposed on GitHub</td>
<td></td>
</tr>
<tr>
<td>![ ]</td>
<td>[S0] -201</td>
<td>Credentials Available on GitHub</td>
</tr>
<tr>
<td>![ ]</td>
<td>IT-12560</td>
<td>[Security Issue - S0] Github Information Disclosure</td>
</tr>
<tr>
<td>![ ]</td>
<td>[Security Issue S0]</td>
<td>Credentials Available on GitHub</td>
</tr>
<tr>
<td>![ ]</td>
<td>IT-2716</td>
<td>[Security Issue S0] Credentials exposed on github</td>
</tr>
<tr>
<td>![ ]</td>
<td>IT-2727</td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td>![ ]</td>
<td>[Security Issue S0]</td>
<td>Credentials exposed on GitHub</td>
</tr>
<tr>
<td>![ ]</td>
<td>IT-2703</td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td>![ ]</td>
<td>V-4300</td>
<td>[Security Issue S0] Credentials exposed on GitHub</td>
</tr>
<tr>
<td>![ ]</td>
<td>[Security Issue S0]</td>
<td>Credentials exposed on GitHub</td>
</tr>
</tbody>
</table>
Everything is Awful.
And We’re Not Helping.
Everything is Awful.
(Keep calm, that’s fine.)
Is the internet on fire?

Previously

txt dig +short txt istheinternetonfire.com [json]

Probably.

OpenSSL update coming on March 1st,
will fix several security defects with maximum severity "high".

@isthenetonfire

Made by @jschauma. See other Signs of Triviality.
The internet is always going to be on fire.

CVE-2014-6271: shellshock remote code execution through bash
CVE-2014-0160: Heartbleed
Don’t waste your time on busy work. Measure your impact.

Prioritize.
Don’t waste your time on busy work. Measure your impact.

Understand your threat model.

Prioritize.
Don’t waste your time on busy work. Measure your impact.

Have a *threat model*.

Prioritize.
Threats you know about.
Threats you decided to defend against.
Threats you can defend against.
Threats you care about.

A Threat Model
Venn Diagram

- Time, money, effort sadly wasted. Plus: you're mad.
- Outside your threat model. You're ok here.
- Make this bigger.
- Difficult, but correct decision.
- Accepted risk.
- Just because. (Ok, if cheap.)
- Here be dragons.
Measure your impact.

Prioritize.

Help others take responsibility.
Guide them.
Everybody else's job is more complicated than you think.
Measure your impact.

Prioritize.

Be helpful.

Teach. Listen.
Measure your impact.

Prioritize.

Be helpful.

Teach. Listen.

...and stop with the fucking Sun Tzu quotes.
Measure your impact.

Prioritize.

Be helpful.

Teach. Listen.

…and stop with the fucking Sun Tzu quotes.