Trustwave®
SpiderLabs®

Reversing Web Applications

Andrew Wilson
Security Consultant, SpiderLabs

i hack charities.

Trustwave®

SpiderLabs®

Primer

What is reverse engineering?

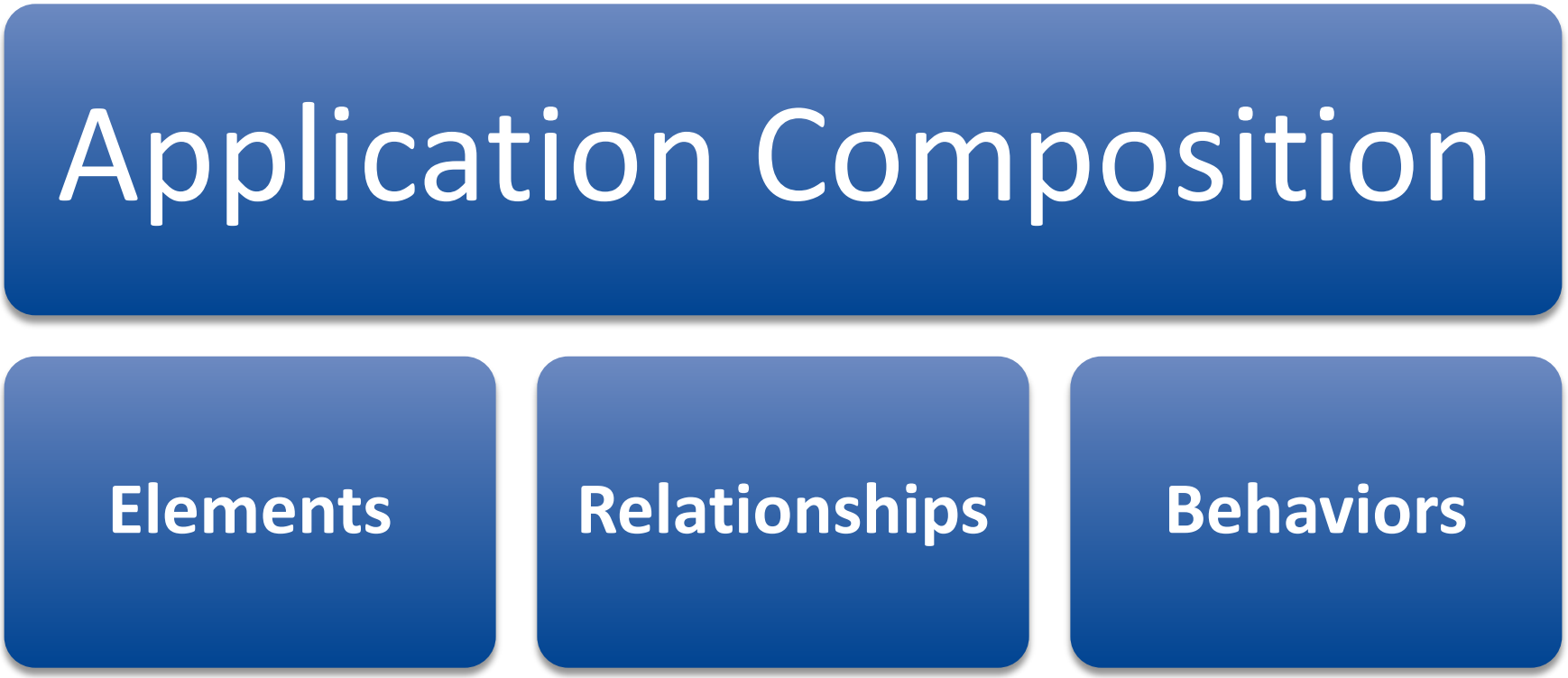
* Do this backwards!

What is Reverse Engineering?

If engineering is the art of designing a body of code…

Reverse engineering is the art of deducing that design from code.

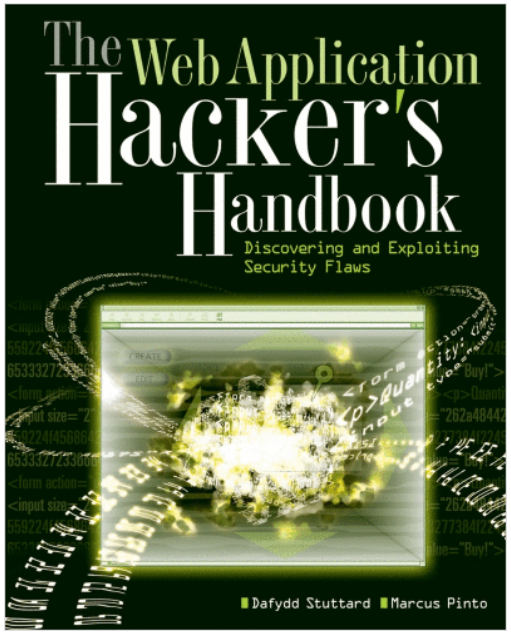
Reversing Goals



http://www.flickr.com/photos/booleansplit/4762692566/sizes/l/in/photostream/

Don’t believe me?

Every methodology says so…



Learn EVERYTHING!

"The first phase in a security assessment is focused on collecting as much information as possible about a target application" – OWASP Testing Guidelines

and I mean, EVERYTHING!

Identify application entry points (OWASP-IG-003)

- Enumerating the application and its attack surface is a key precursor before any attack should commence. This section will help you identify **and map out every area** within the application that should be investigated once your enumeration and mapping phase has been completed.

Because…

“The more information you are able to gather during this phase, the more vectors of attack you may be able to use in the future.” - PTES

The IG Laundry List:

i. Map visible content
ii. Discover Hidden & default content
iii. Test for debug parameters
iv. Identify data entry points
v. Identify the technologies used
vi. Map the attack surface
vii. Analyze exceptions
viii. Search engine discovery
ix. Test for application fingerprint

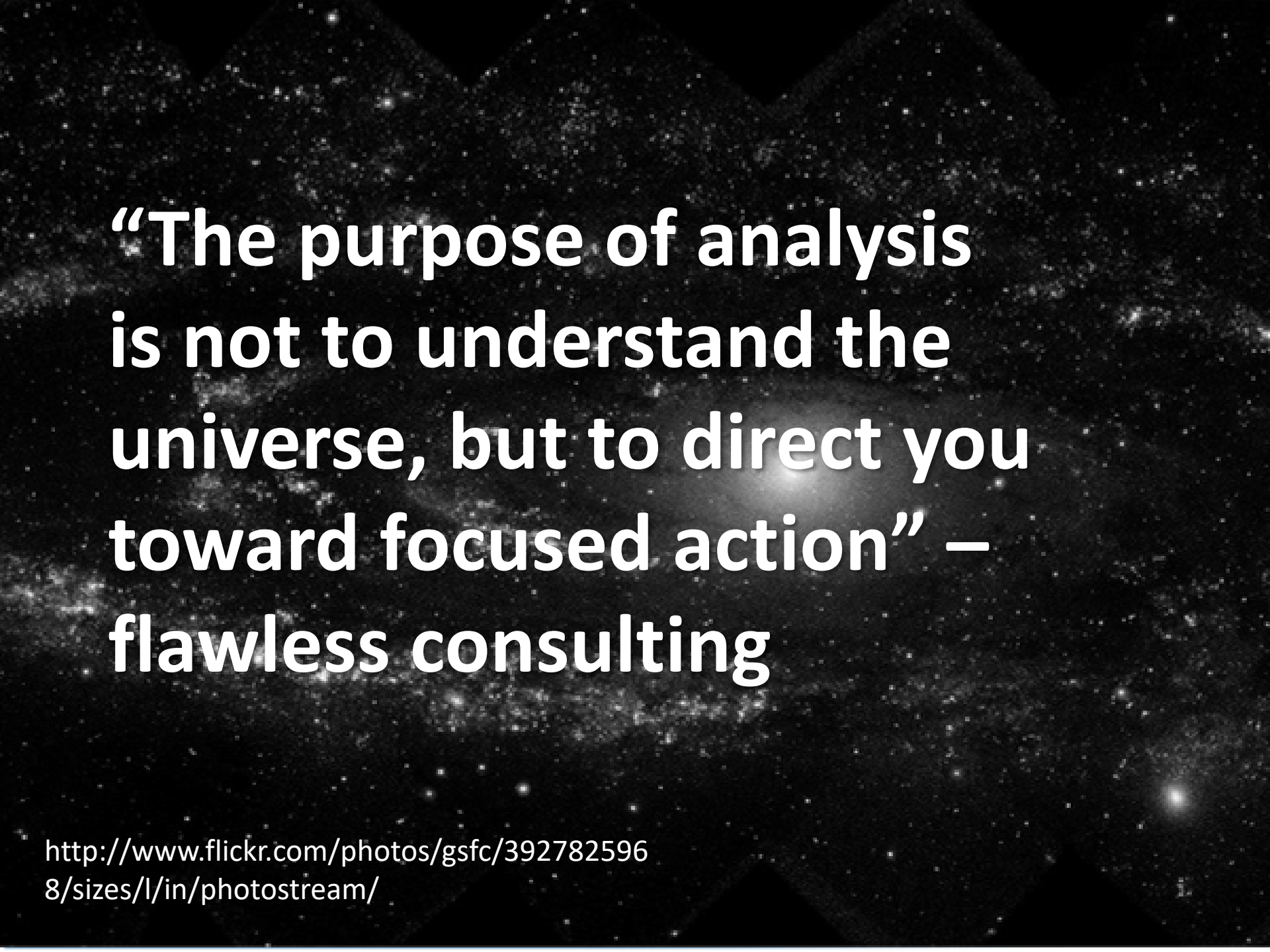
* From web application hackers website outline & OWASP testing guidelines

Top down approach implies it only happens once. It doesn't

S-L-O-W

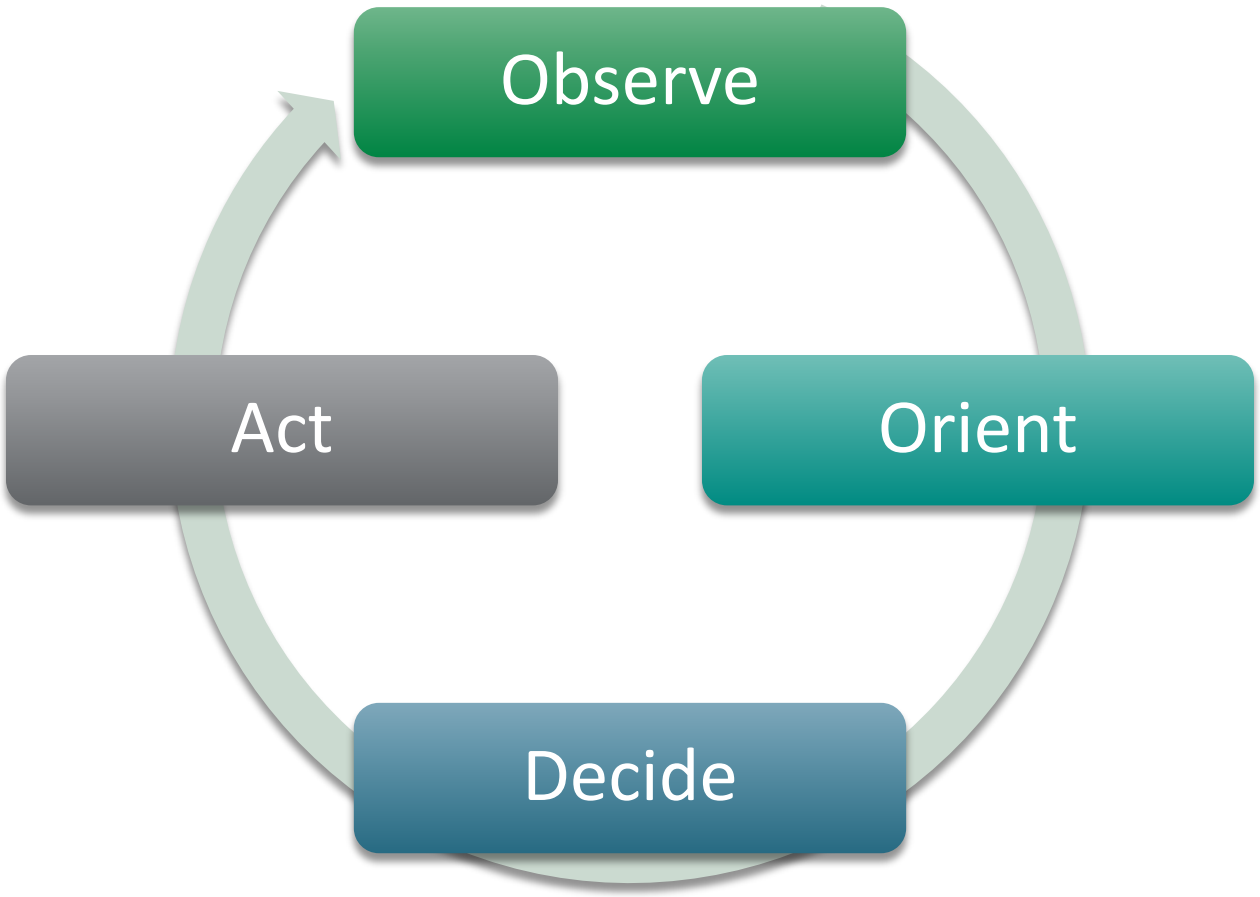
Information Overload

http://www.flickr.com/photos/kb35/1644548833/sizes/z/in/photostream/



http://www.flickr.com/photos/gsfc/3927825968/sizes/l/in/photostream/

OODA / Iterative testing



Caveats

- **Not a 1:1 relationship to compiled binary reversing**
- **People do silly things.**

Trustwave®

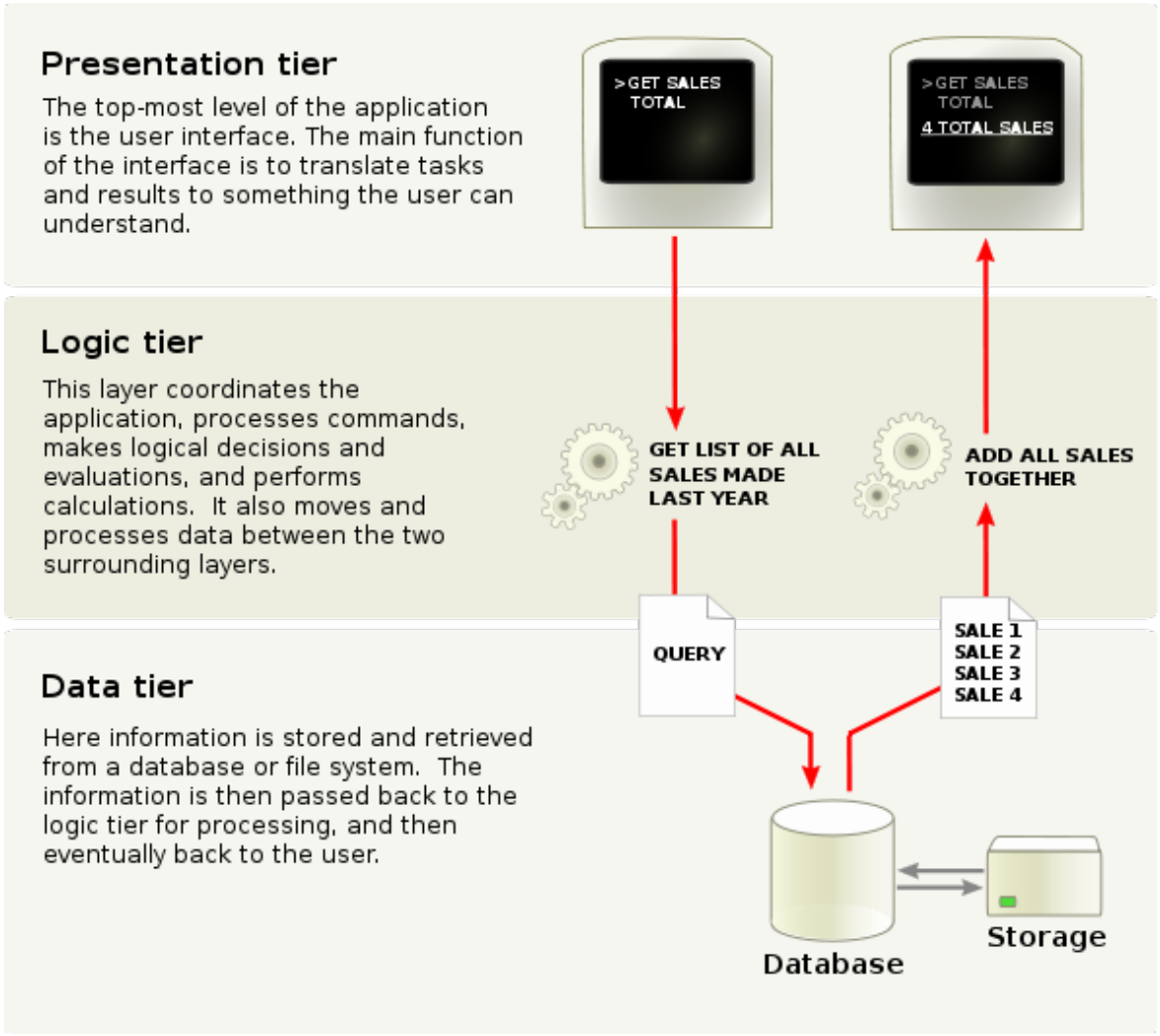
SpiderLabs®

Decomposing Applications

“Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him.” – Locard Exchange Principle

http://www.flickr.com/photos/pagedooley/2422430207/sizes/l/in/photostream/

Identifying Compositions



http://en.wikipedia.org/wiki/File:Overview_of_a_three-tier_application_vectorVersion.svg

Passive Testing

Techniques which:

- don’t connect to system
- appear as normal / public use

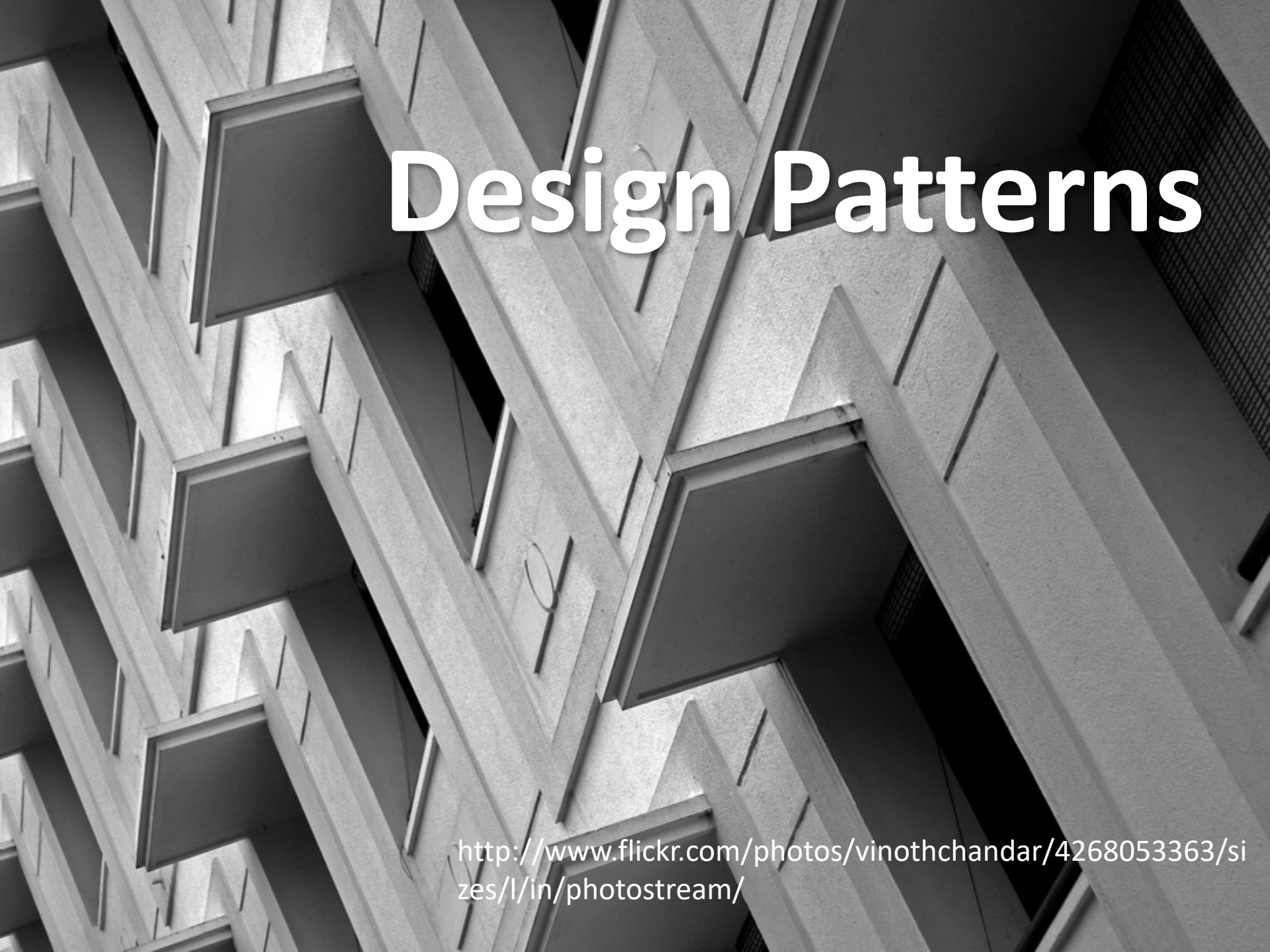
Example (google dorks, shodan, regular traffic)

Active Testing

…The opposite of the last slide.

Active vs. Passive Testing

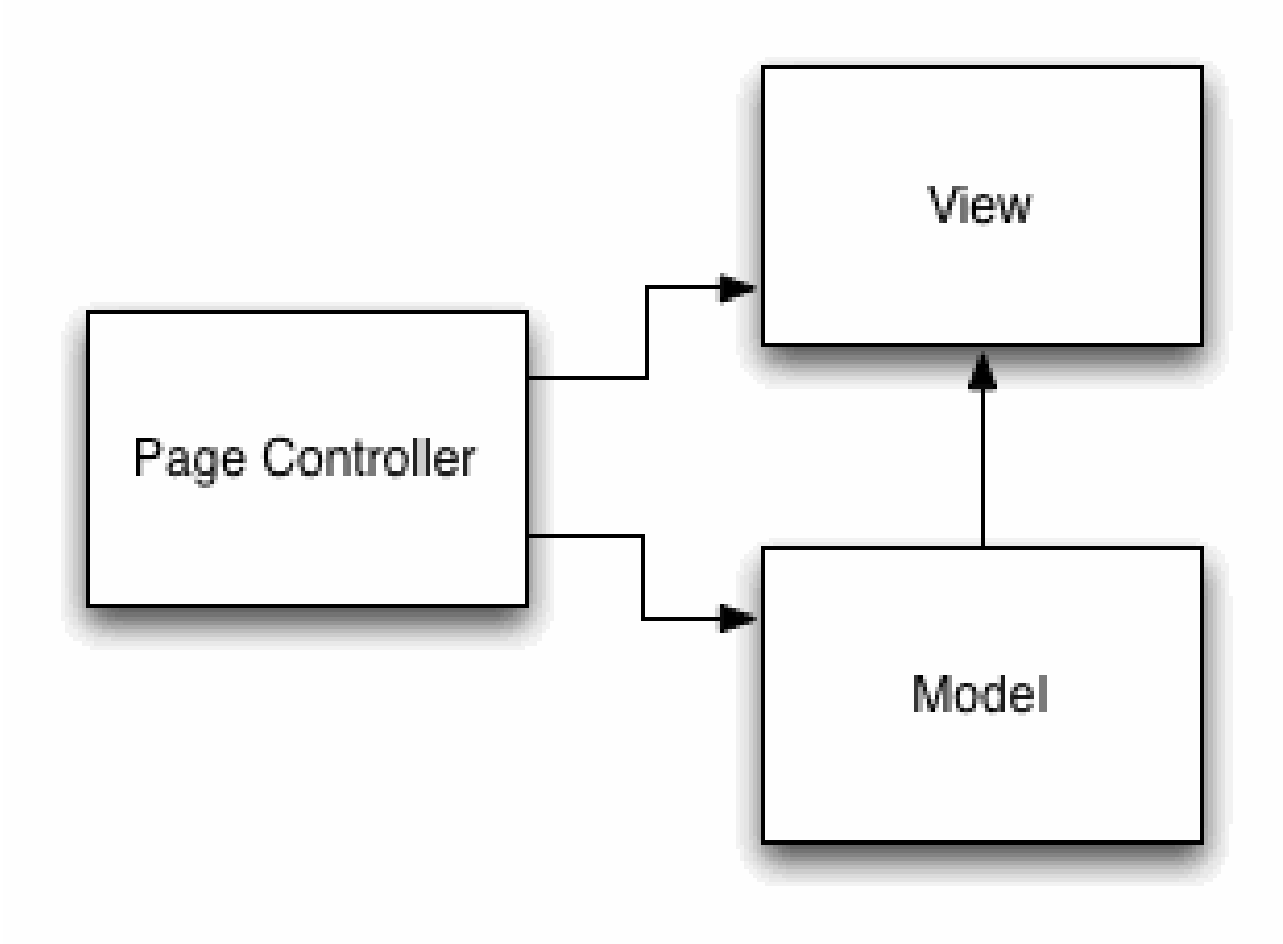
- **Passive testing reveals “happy path”**
- **Active testing reveals how optimistic the developers were.**



Design Patterns

http://www.flickr.com/photos/vinothchandar/4268053363/sizes/l/in/photostream/

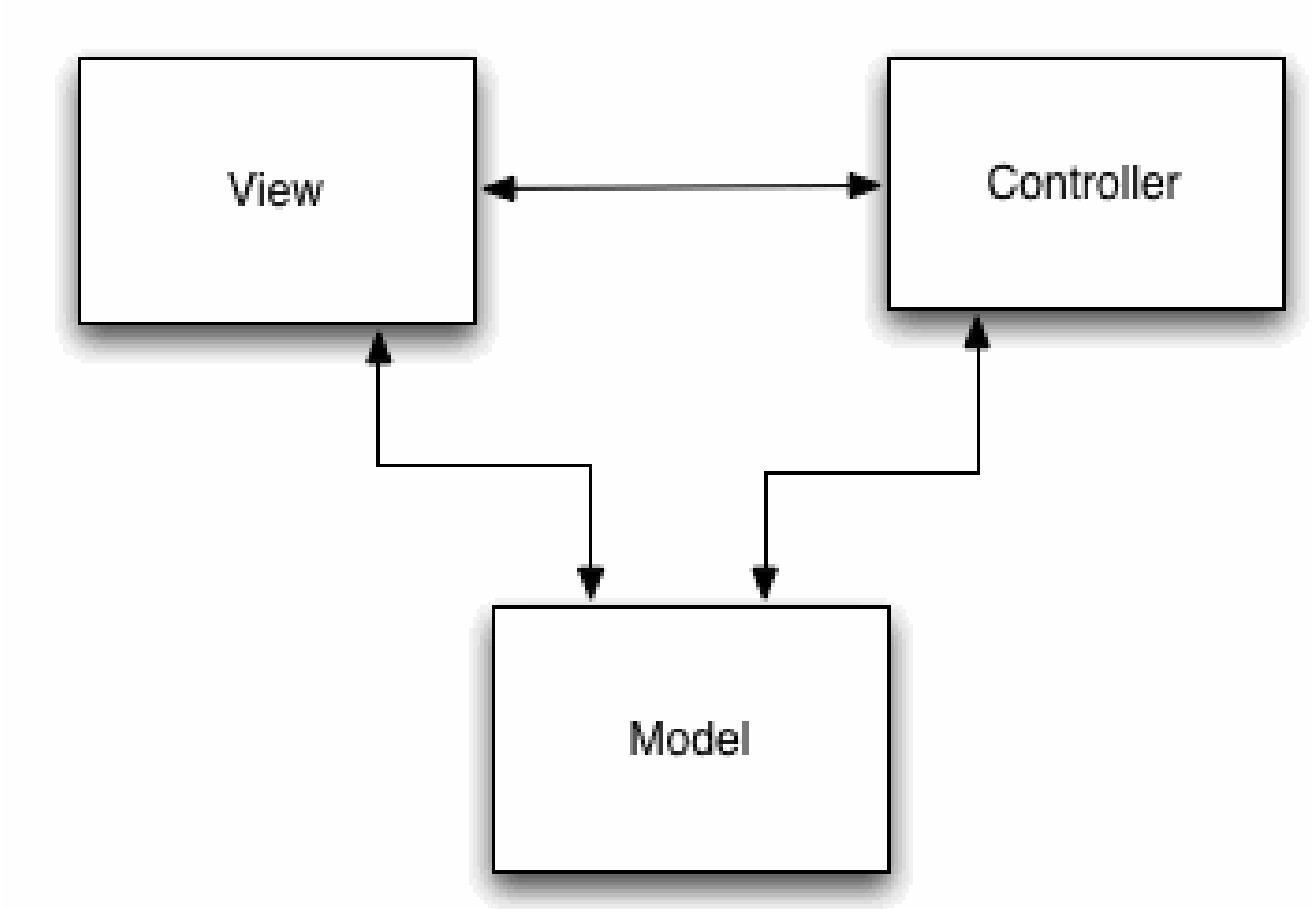
Display Patterns: Page Controller



Display Patterns: Page Controller

- Lots of single “action” pages
- Lots of client controlled variables
- .php file extension ☺

Display Patterns: Model View Controller



Display Patterns: Model View Controller

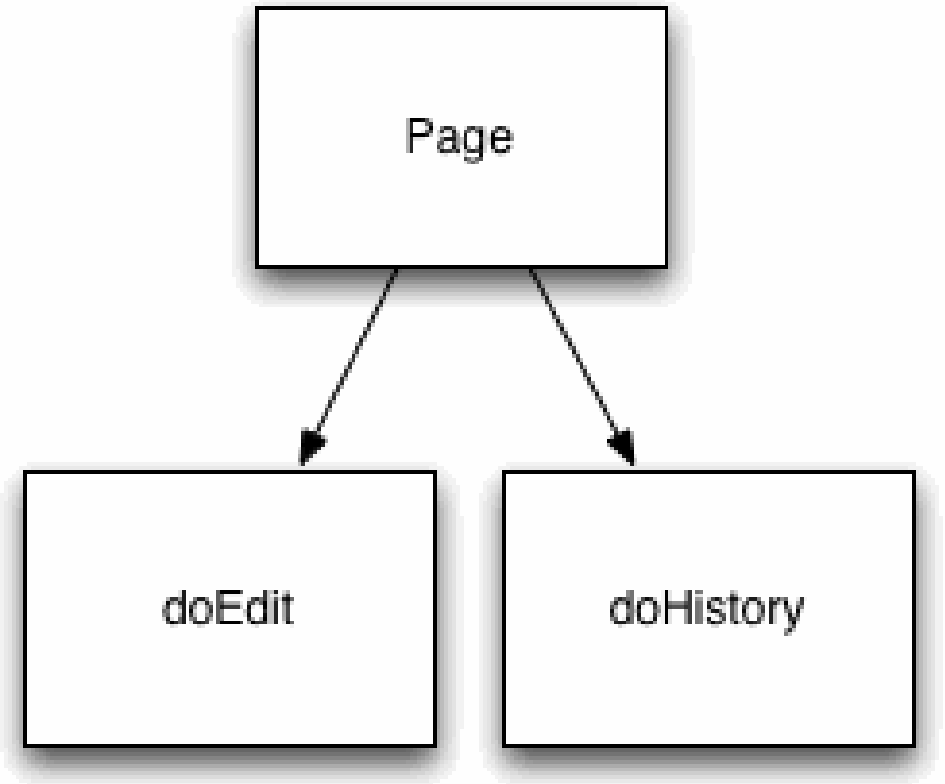
URL Structure:

/controller/action/id
/controller/ <- default-action
/id <- default controller & action

Wont see many parameters in query string

Popular in certain languages

Display Patterns: Front Controller



/index.php?title=Installation&action=history
/index.php?title=installation&action=edit

Display Patterns: Examples

Pattern	Page
Page Controller	doQuery.asp?x=params
Front Controller	index.asp?action="doQuery"&x=params
MVC	/Query/Param/SubParam

Data Access

Concatenated Strings

"select * from table where value = " + value;

Prepared Statements

query = "select * from table where value = ?"; query.Properties.add(value);

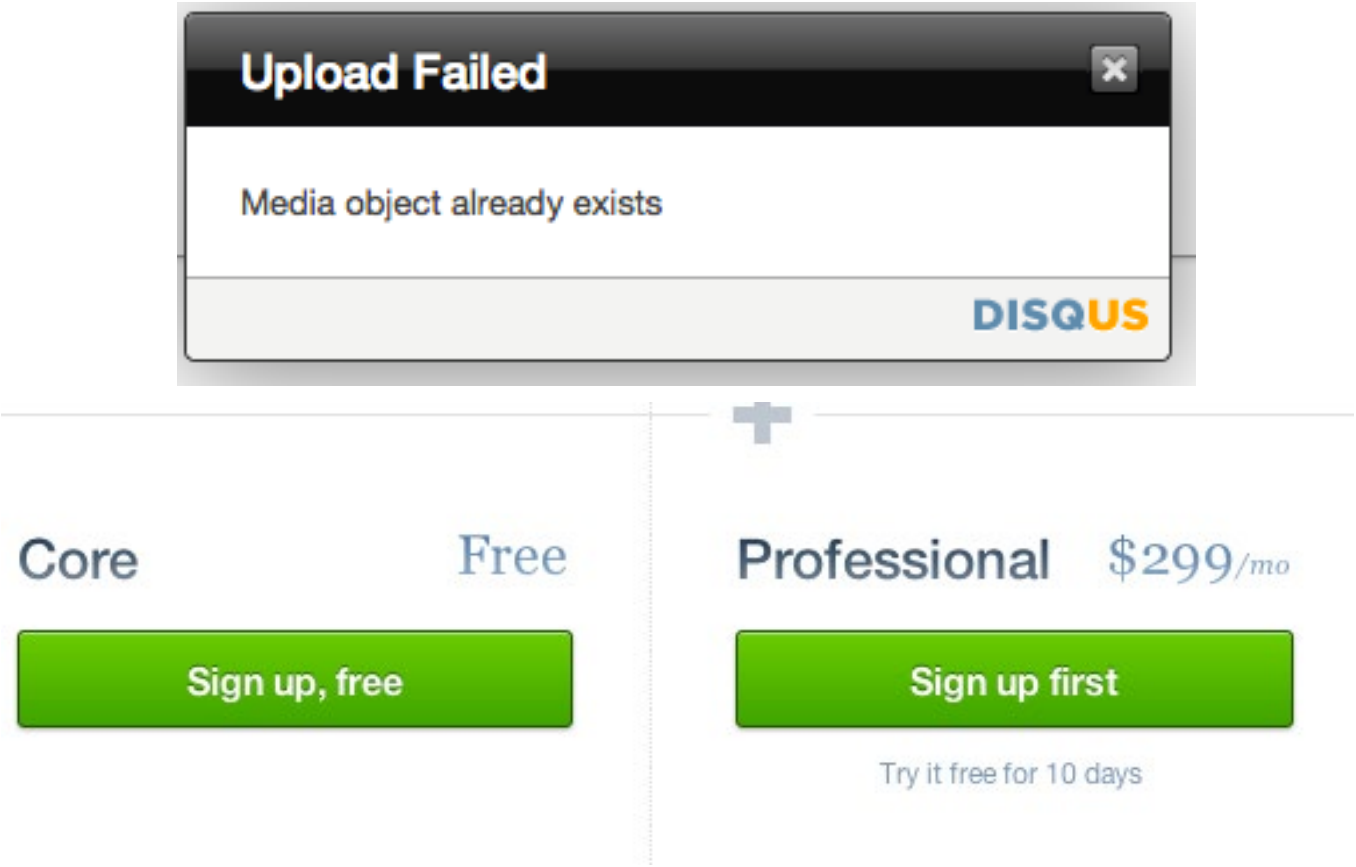
Stored Procedures

Be wary of inconsistencies

- **Sometimes URL re-writing rules can "appear" as MVC**
- **However frameworks still generate front-controller links.**

Cheat

If you can, download the framework locally.



http://www.flickr.com/photos/jmurawski/4992 78540/sizes/z/in/photostream/

Leveraging Infrastructure

- Anything they say, can and should be used against them.
- Each pattern has strength's & weaknesses.
- View patterns can imply underlying data access pattern(s).

http://www.flickr.com/photos/futureshape/2614476028/sizes/l/in/photostream/

Application psychoanalysis.

We are concerned with what an application does.

And what it doesn't.


Where did my data go?
http://www.flickr.com/photos/59937401@N07/5858002158/sizes/l/in/photostream/

And how did it get there?

- How did the data move: POST, query string, cookie?
- Was the data encoded when I retrieve it?
- Was there a redirection?

Identifying Types

- **There are only two types of types. Basic and Complex**

- **In both cases, you want to know:**
  - Is it required?
  - What does it do?

Basic types

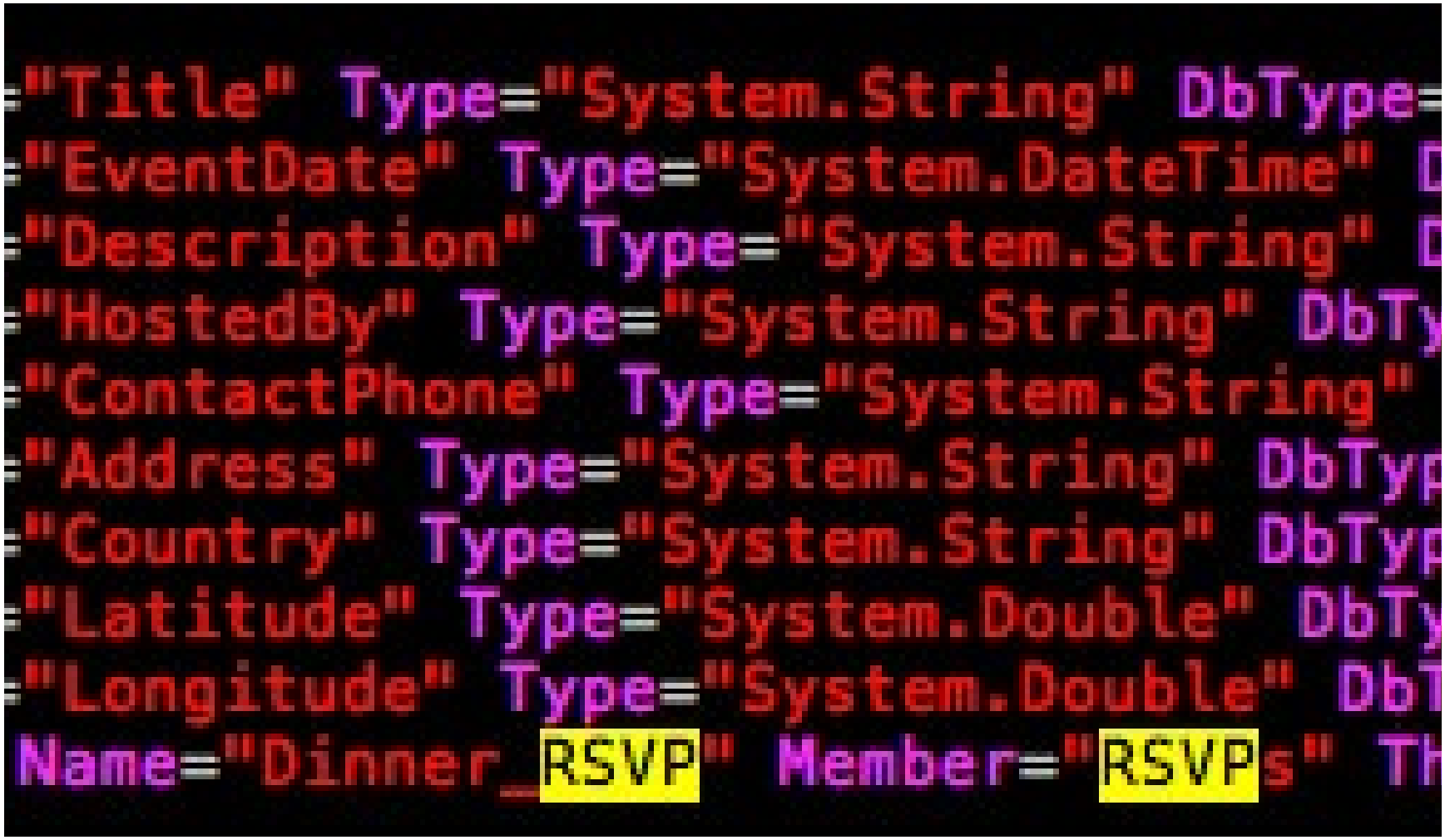
- Exist in: Forms, query strings, cookies, and URL composition.
- Strings, Numeric, Guids

Complex types

Sometimes obvious:

body	DinnerID	0
body	Title	e
body	EventDate	10%2F13%2F2011+3%3A00%3A47+PM
body	Description	e
body	HostedBy	e
body	ContactPhone	e
body	Address	e
body	Country	USA
body	Latitude	51.57954025268555
body	Longitude	0.00288999869746923
body	HostedById	

Which matches pretty close to:



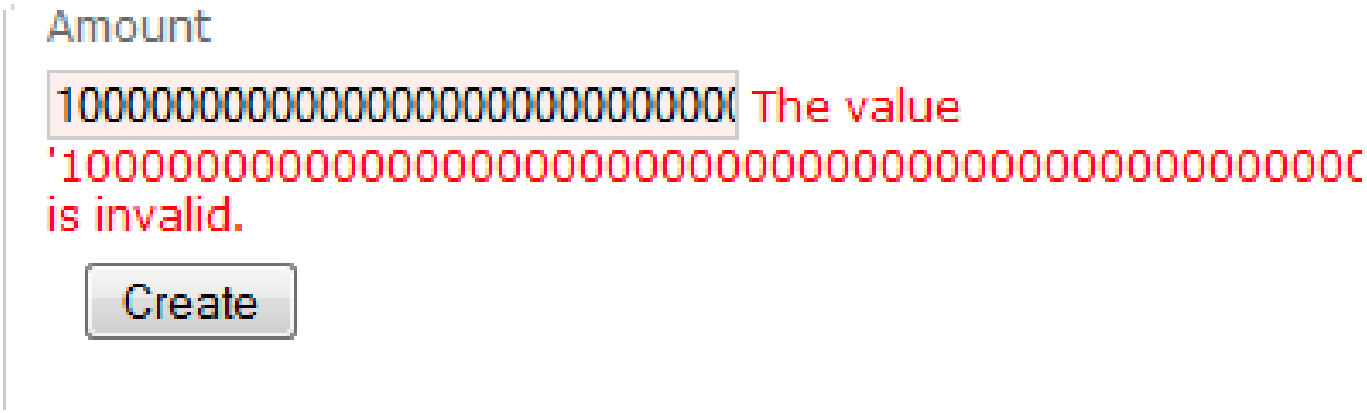
I 

EXCEPTIONS!

Learning from Exceptions

Discovering field type from error messages:

- To determine type of number, attempt:
  - Negative integers
  - Large numbers



Learning from Exceptions

- **You can also learn if a field is dynamic or static:**

- **i.e: value=1+1, 1-1, etc..**

New errors are better than old ones

- **Getting new errors means you are making progress.**

- **Applications will fail in various places, and can sometimes be cheated to not fail.**

Taking their time

- Blind SQL injection is based, most often, on timing attacks.

- How long a response takes, can sometimes tell you how far it got in a process.

Pro Tips:

- **What an application says, or doesn't say is very revealing.**

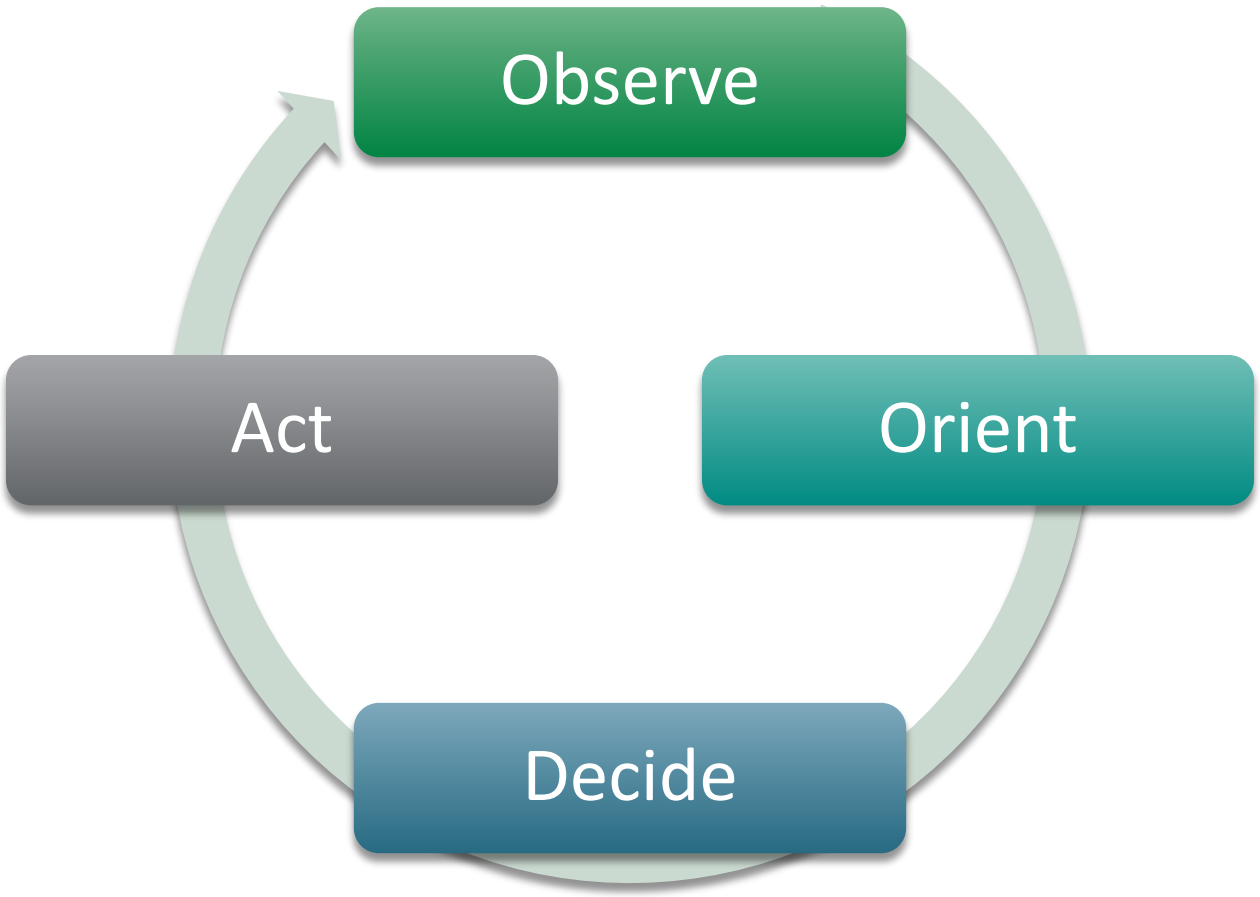
- **Don't trust tools too much.**

Trustwave®

SpiderLabs®

Final thoughts (by Jack Handy)

OODA / Iterative testing



Let the application be your guide.

Ask lots of questions.

If you ask properly– it will likely tell you.

Learn to listen

Listen to the application is saying and make informed decisions

“Wherever he steps, whatever he touches, whatever he leaves, even unconsciously, will serve as a silent witness against him.” – Locard Exchange Principle

http://www.flickr.com/photos/pagedooley/2422430207/sizes/l/in/photostream/

http://www.flickr.com/photos/marcelekkel/4456101492/sizes/o/in/photostream/

Trustwave®

SpiderLabs®

Questions?