BISHOP FOX®

If you like it then you shouldn't put a ring3 on it

AN ADVANCED INTRODUCTION TO BREACHING WEB APPLICATIONS

WHO AM I!

Andrew Wilson

- Senior Security Associate (Lead) at Bishop Fox (Assessment Penetration Team)
- *Old man (and grumpy)*

- *Microsoft MVP: Developer Security*

- *OWASP Phoenix*

i hack charities.

THE UTILITY OF PWND

WHY WE DO WHAT WE DO
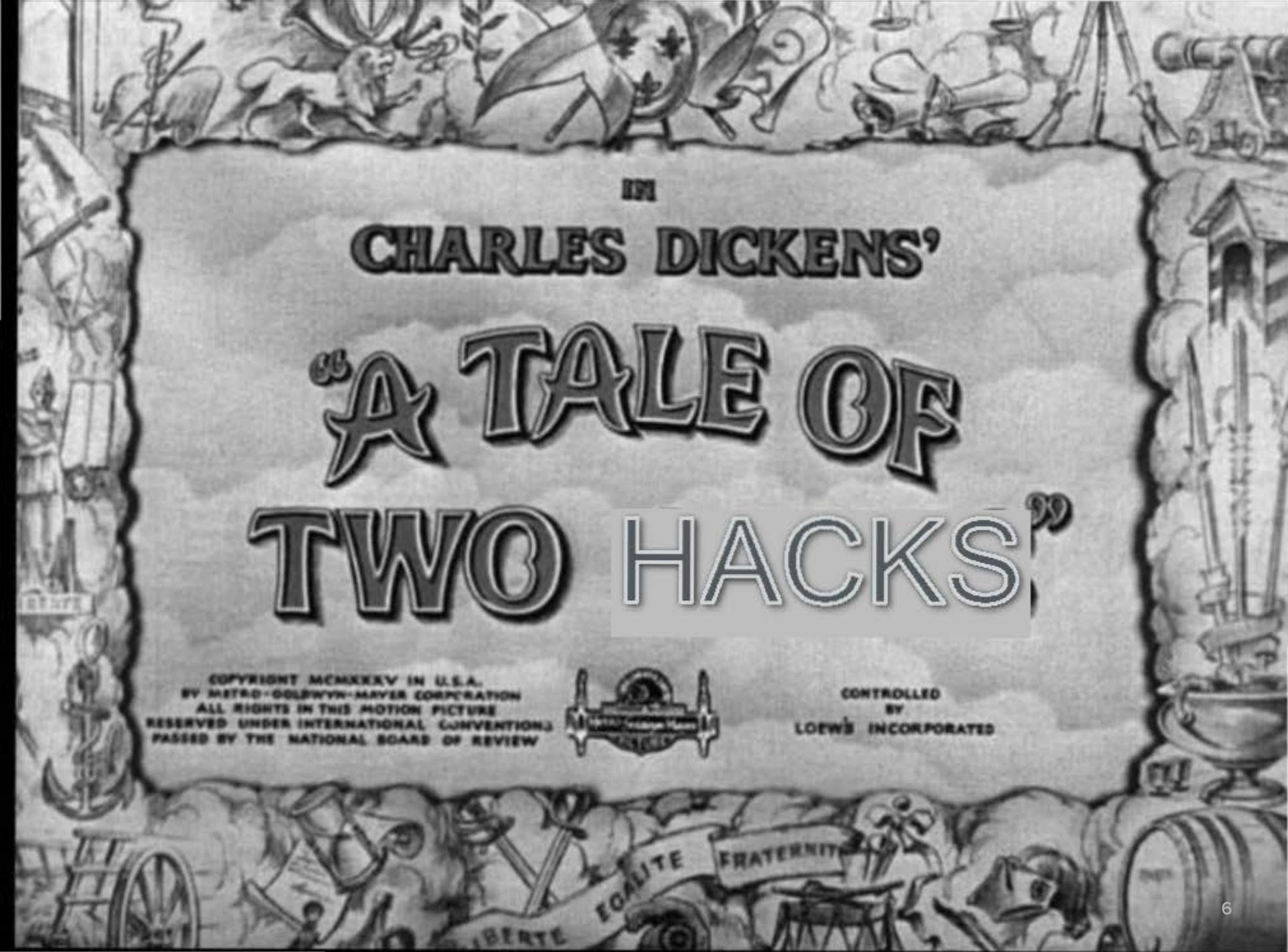
IN

CHARLES DICKENS'

"A TALE OF TWO HACKS"

Why doth thy breach?

Undeniable Evidence

Immediate Destabilization

Increased Odds of Finding
More Issues

And because it is awesome!

Why doth thy breach?

YOU HACKETH WHAT?
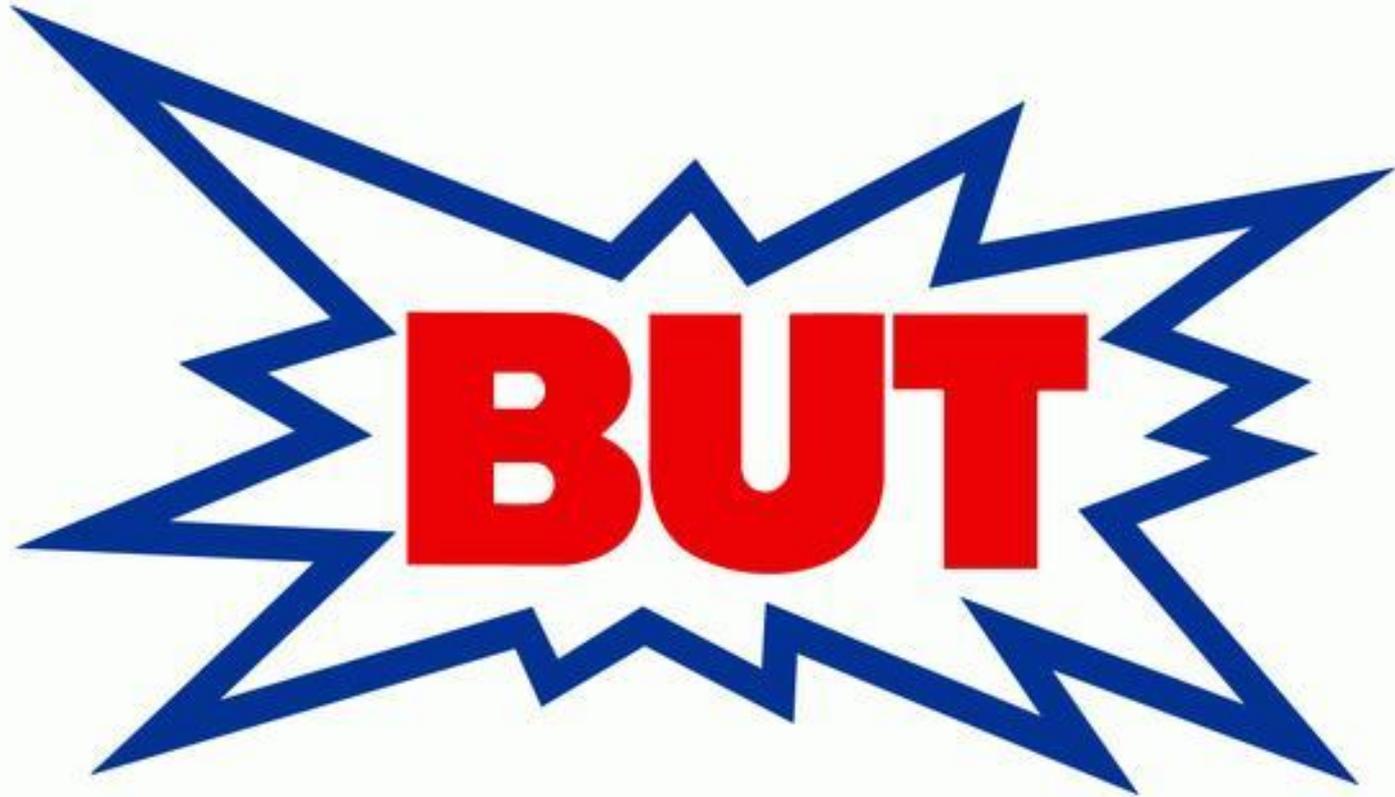
DIRECT VS.
INDIRECT ROUTES

THE SIMPLEST PATH IS THE FASTEST

Direct vs. Indirect Intrusion

Direct Intrusion Points – Attacks can be executed against a system without any third-party arbitrator.

Indirect Intrusion Points – Attacks require a third-party activator (people or process) to be triggered.

System-Based Attacks

MANO E MANO
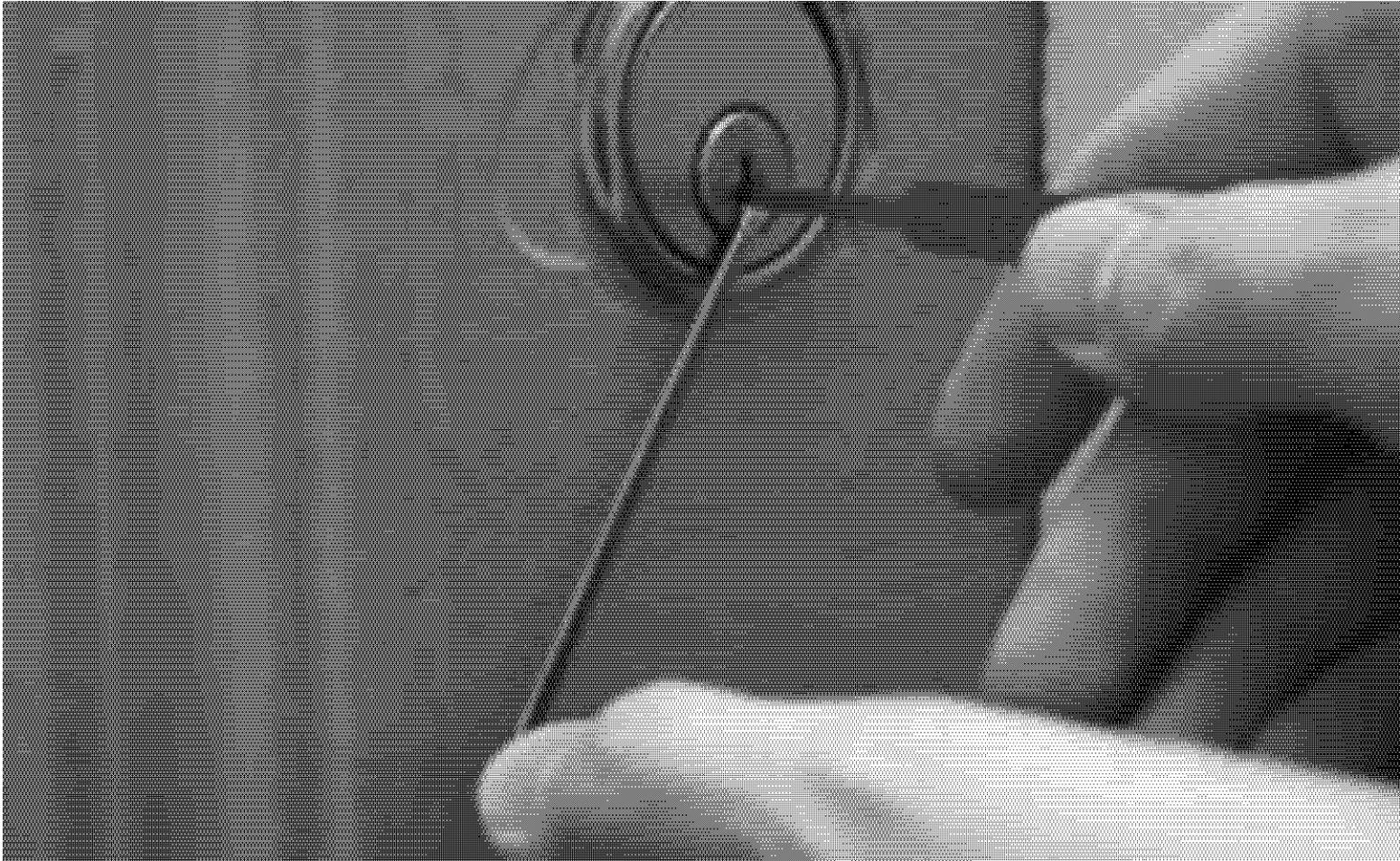
User-Based Attacks
RUBBER HOSE SECURITY

System-Based Intrusion Points

- SQL Injection

- Directory Traversal

- RCE

- File Upload

- Insecure Direct Object Browsing

- Mass Assignment

- Etc...

User-Based Intrusion Points

- XSS

- CSRF

- Cookie Hijacking (MITM)

- Browser Exploits

- Bad Passwords

- Auto Complete

- Etc…

Goal-Based Testing

WHEN THE RUBBER HITS THE ROAD

Most application
tests won't let
you attack users.

99%

OF USER-BASED
ATTACKS ARE OUT OF
SCOPE.

System-based
attacks FTW!

COMMON
VULNERABILITIES

ONE-HIT WONDERS

The Utility of Vulnerabilities

Common Breaching Vulnerabilities

- Insecure File Upload

- SQL Injection

- Command Execution

- Code Execution

- Local File Inclusion

Likelihood %
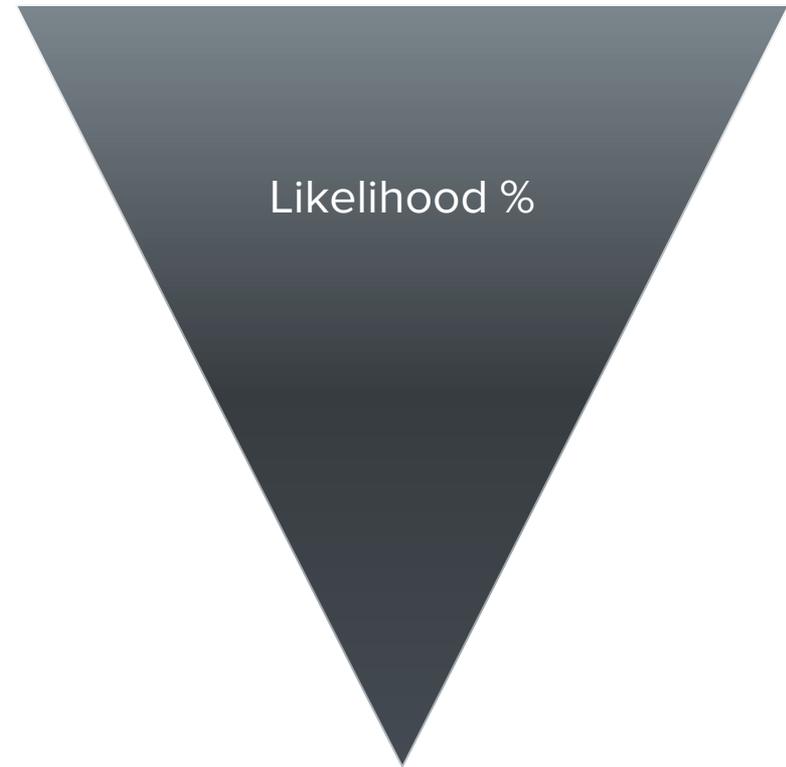
Insecure File Upload
SERVER COMPROMISE ROUTE

- Allowing users to push files to a server is always risky.

- Most frequent route we use to compromise servers.

- Easiest way to compromise a Web server.

Insecure File Upload

Insecure file upload

Filesystem

Database

Type confusion

Evasions

No protection

Poisoned files

Incorrect headers

System

User

SQL Injection

SQL Injection *occasionally* allows malicious users to execute system functions and/or push files to the system.

Its greatest strength in breaching servers is most likely to be data loss leading to account takeover.

SQL Injection

DIRECT AND SUPPLEMENTAL
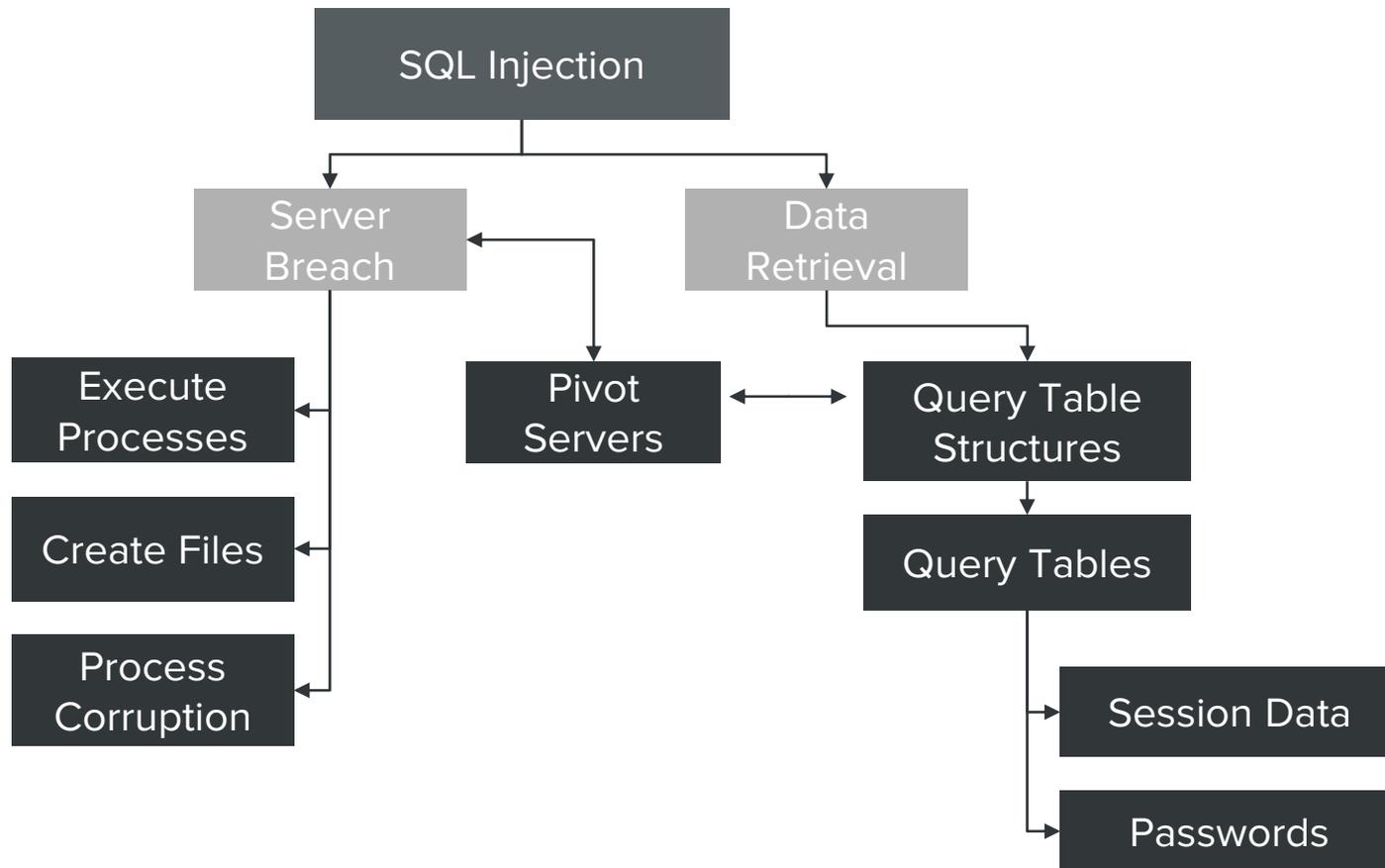
Command Injection

Command injection attacks occur whenever an application executes system processes using a loosely defined boundary.

It isn't super common, but certain language features or business features can expose this risk in an application.

Command Injection

SERVER COMPROMISE ROUTE

Common Locations

- Photo editing

- Email

- LDAP

- Administrative features

Remote Code Execution

Remote code execution attacks occur when data is confused as code and executed as such.

This is pretty rare in applications, but in certain 'robust' applications it can be a feature!

Remote Code Execution
THE FRINGE

```
                    ┌─────────────────────┐
                    │  Remote Code Exec   │
                    └─────────────────────┘
                        │             │
              ┌─────────────────┐  ┌──────────────────┐
              │  Language Based │  │ Corruption-based │
              └─────────────────┘  └──────────────────┘
                      │                      │
    ┌─────────────────┐                  ┌──────────┐
    │  Cached objects │◄─                ─►│ Interop  │
    └─────────────────┘                  └──────────┘
    ┌──────────────────┐                 ┌────────────────────┐
    │ DSL/Micro language│◄─             ─►│ Framework failure  │
    └──────────────────┘                 └────────────────────┘
    ┌──────────────────┐
    │ Banned functions │◄─
    └──────────────────┘
```
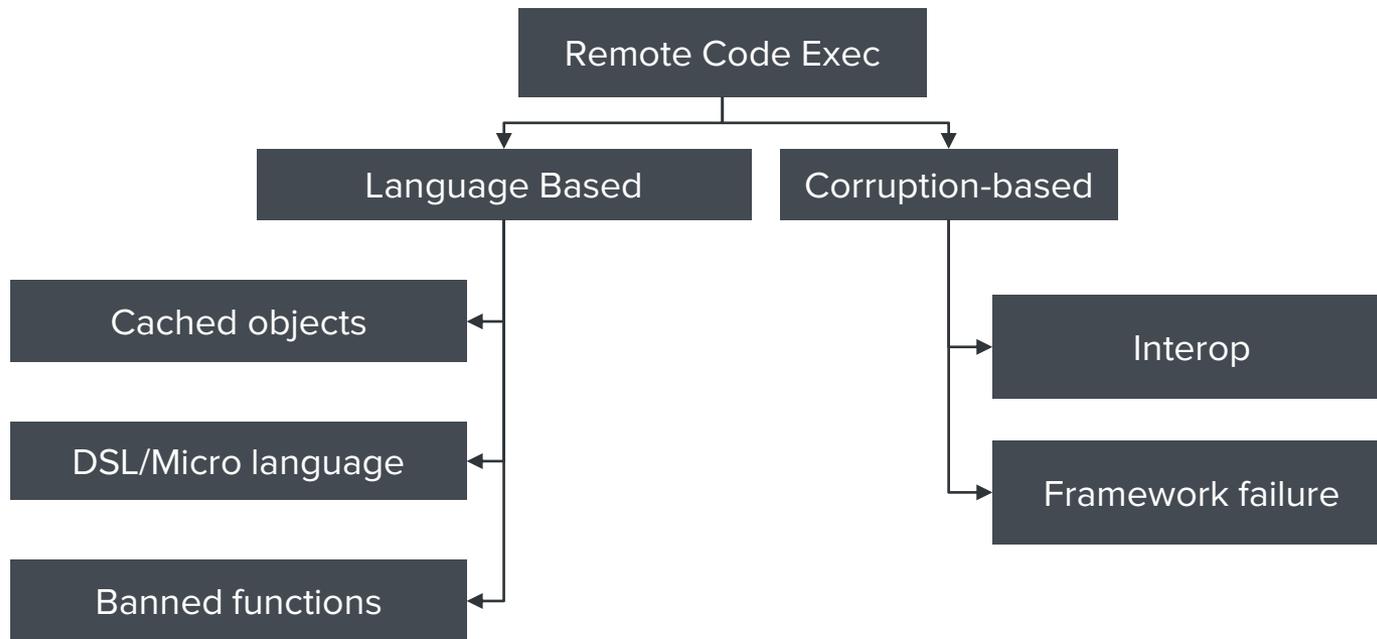
Local File Inclusion

Local file inclusion attacks occur when you can dynamically include files to be executed inside of an application.

These are pretty rare, and often require other vulnerabilities to occur before you can exploit it.

SUPPLEMENTARY VULNERABILITIES

VISIBILITY IS KING

"The real voyage of discovery consists not in seeking new landscapes, but in having new eyes."

— Marcel Proust

Source Exposure

SUPPLEMENTAL DOESN'T MEAN LESSER THAN

This is an easy thing to check:
https://github.com/evilpacket/DVCS-Pillage

Don't discount error messages that leak stack traces.

Some apps are built on top of other frameworks, which you can find online.

Authentication Bypass
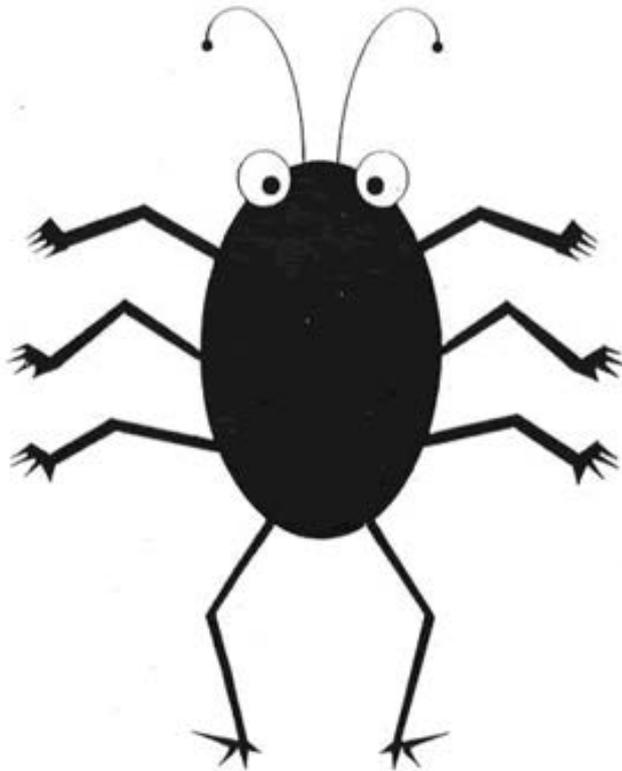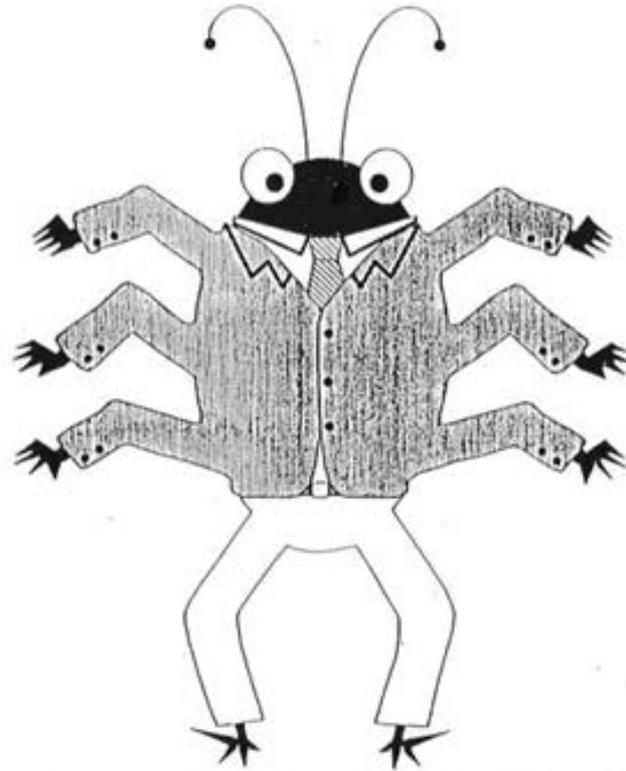
BUG   FEATURE

ATTACK STRATEGIES

THE NEW HOTNESS

Attack Theory: Jeet Kun Do

BE LIKE WATER, MY FRIENDS

1.) Direct Attack

2.) Combination Attack

3.) Progressive Indirect Attack

4.) ~~Trapping~~

5.) ~~Drawing~~

Attack Theory: Hack Foo Do

BECAUSE WE CAN!

1.) Direct Attacks

Attack Theory: Hack Foo Do
BECAUSE WE CAN!

1.) Direct Attacks

2.) Combination Attacks

Direct Combinations

Combo Attacks – Attacks achieve new privileges, exposing additional attacks.

Conditional Attacks

Branch Analysis – Test the various execution paths an application could take in order to uncover broken rules and/or security weaknesses.

Examples:

- Inconsistent application of logic/authentication

- Incomplete business rules

- Really weird bugs/exploits

Attack Chaining

AKA: EXECUTION PATH TESTING

Chained Attacks – The use of n-attacks to produce an otherwise unattainable attack.

Attack Theory: Hack Foo Do

BECAUSE WE CAN!

1.) Direct Attacks (Low-Hanging Fruit)

2.) Combination Attacks

- Conditional

- Chained

3.) Indirect Progressive

- Second-Order

Second-Order Attacks

Second-Order – The use of combined attacks to undermine and/or circumvent a countermeasure or security feature.

Example:

- Input validation weaknesses

CLOSING THOUGHTS

BY JACK HANDY

Takeaways

- Vulnerabilities are just video game cheat codes.

- If you can access the functionality, then you don't need vulnerabilities.

- Attacks against users are valid, but not often in scope.

45

Takeaways (Part Deux)

- 5 attacks lead to Web server compromise.

- Supplemental attacks provide invaluable insight for exploits.

- Combination strategies achieve results.

Thank You

bishopfox.com

awilson@bishopfox.com

@azwilsong

Page of Attribution: Photos

- Marines photo - http://www.flickr.com/photos/marine_corps/7294795902/in/photostream/

- Bruce Lee – http://www.officialpsds.com/images/thumbs/Bruce-Lee-psd93556.png

- BS! - http://www.flickr.com/photos/70938871@N05/6420020339/

- Doggy bag: http://www.womansday.com/cm/womansday/images/2m/05-doggie-bag-lgn.jpg

- Game genie: http://www.beachbayonet.com/wp-content/uploads/2014/04/game_genie-jpg.jpg

- User attack : http://3.bp.blogspot.com/-1E40OaAb4TI/UgOEeylUsRI/AAAAAAAAnVw/grCrnYsMorQ/s1600/ALI+BABA+LOOEY+4.png

- Lock pick: http://images.askmen.com/fashion/how_to_300/374_how_to_flash.jpg

- But….: http://www.dsprel.com/wp-content/uploads/2014/05/but-meubles-electromenager-saint-herblain-1309252625.jpg

- Broken heart: http://upload.wikimedia.org/wikipedia/commons/thumb/b/bb/Broken_heart.svg/2000px-Broken_heart.svg.png

- *A Tale of Two Cities*: http://allthingsd.com/files/2012/08/tale-of-two-cities-title-still.jpeg

- Shell shock: http://i.nextmedia.com.au/News/shellshock-bug.png
- Bug vs. feature: http://alexander-windbichler.com/wp-content/uploads/2009/03/bug_vs_feature.gif
- Combo! http://comboattackpodcast.files.wordpress.com/2010/08/bonus-round-logo.jpg
- Chains: http://www.marinewarehouse.net/images/anchoring/acco/acco%20chain.jpg

BISHOP FOX®