presentation date 24/03/2011

Golden Rules to Pen Testing

Jason Flood
Javier Marcos de Prado

- Understand their Business
- Probe the network
  - What are they about?
  - Use Social Media
- Do the boring homework
  - Hacking is only *easy* in Hollywood

Know your enemy!

- Understand who you are!
- This is not fun or treated as such by authorities.
- Set yourself a goal
- Learn on your machine
- Know your limits
  - Stick to them!

Know your own skills!

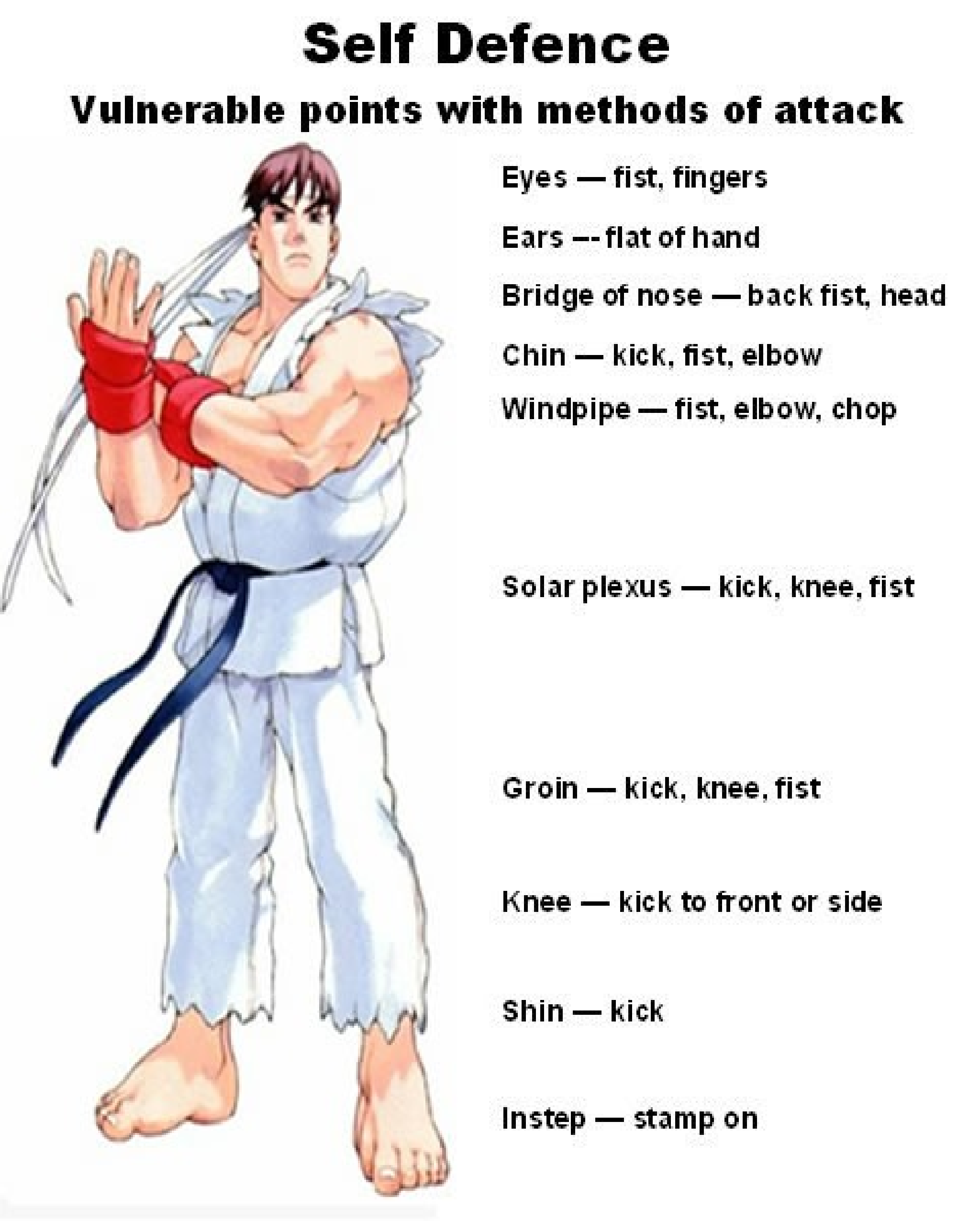
- The bigger the fish, the bigger the stick!
- Can any hacking be called fun?
  - Neighbours wi-fi
  - Will you like what you find out?
- Do you really want to go down this route?

Know the punishment!

- I run automated tools – I am a hacker...
  - Can you cover your tracks?
  - These tools have signatures
- Police will knock on your door with a warrant and seize everything.
  - Not a game

Do not Get Caught

Attacks in the real world



Self Defence

Vulnerable points with methods of attack

Eyes — fist, fingers

Ears -- flat of hand

Bridge of nose — back fist, head

Chin — kick, fist, elbow

Windpipe — fist, elbow, chop

Solar plexus — kick, knee, fist

Groin — kick, knee, fist

Knee — kick to front or side

Shin — kick

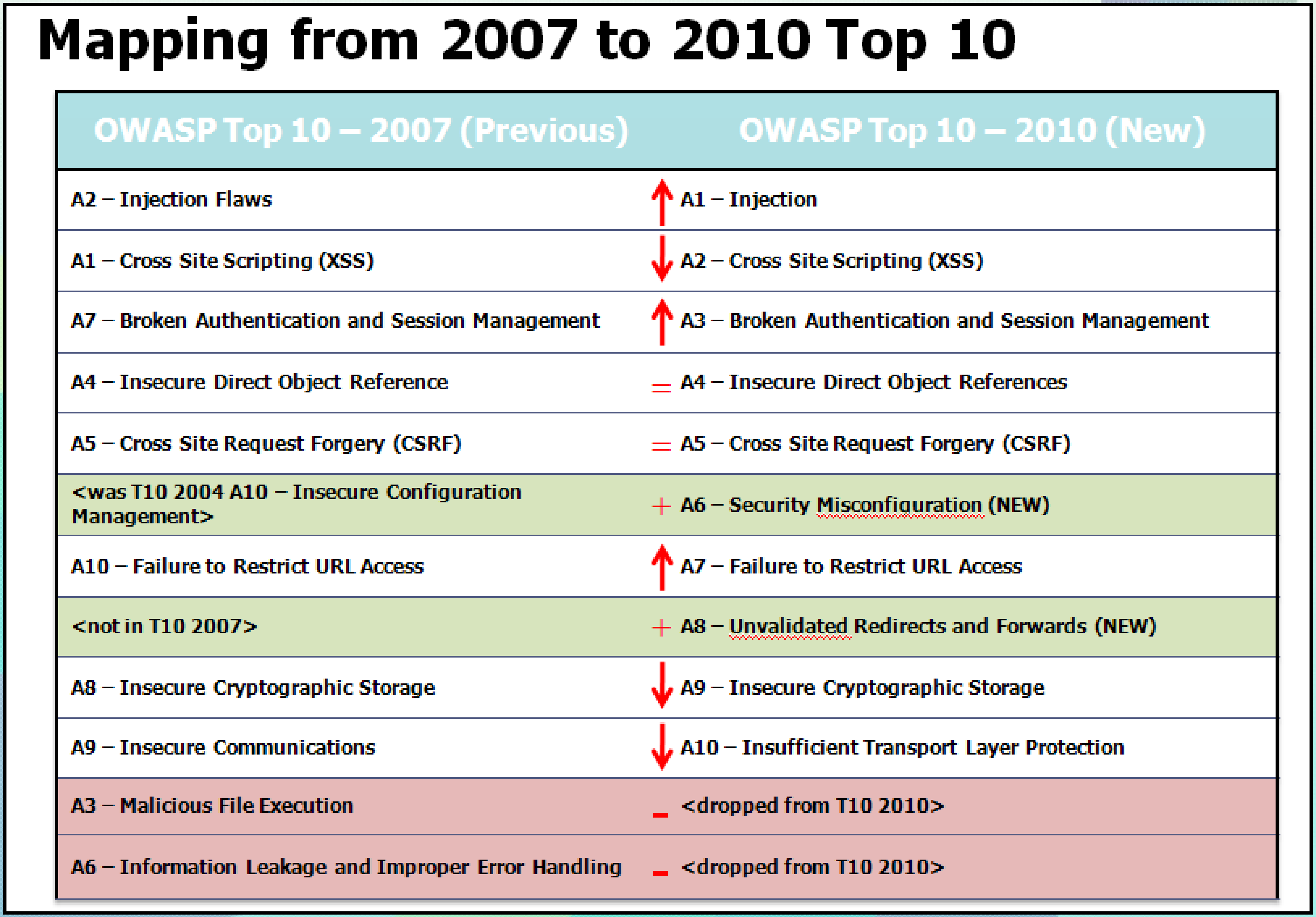
Instep — stamp on

- Do not pick the 7ft 350 lbs ninja to fight (unless your that good)
- Actions have a purpose
  - Random arm/leg movements ineffective.
- What are the consequences.

- Don't attack the 7ft ninja...
- Create a plan
  - Stick to it
  - Step through it
- Take notes as you go
- You will get arrested if you do more then a probe
  - Maybe even then?

- All systems have a fatal flaw
- If you are good enough you may find it.
  - What do you do with this info?
  - Google pay for defects found...
- An attack at this point is illegal
  - Not recommended

See – I told you I could do it!



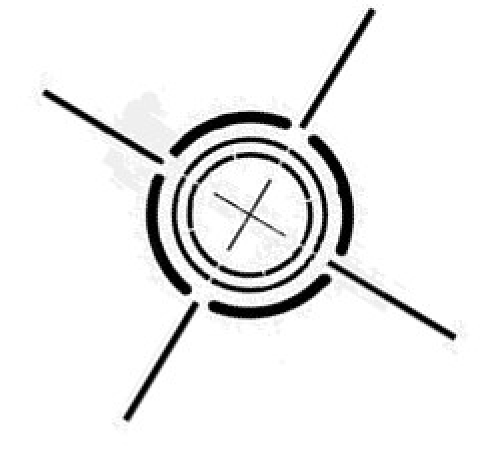
Mapping from 2007 to 2010 Top 10

OWASP Top 10 – 2007 (Previous)		OWASP Top 10 – 2010 (New)
A2 – Injection Flaws	↑	A1 – Injection
A1 – Cross Site Scripting (XSS)	↓	A2 – Cross Site Scripting (XSS)
A7 – Broken Authentication and Session Management	↑	A3 – Broken Authentication and Session Management
A4 – Insecure Direct Object Reference	=	A4 – Insecure Direct Object References
A5 – Cross Site Request Forgery (CSRF)	=	A5 – Cross Site Request Forgery (CSRF)
<was T10 2004 A10 – Insecure Configuration Management>	+	A6 – Security Misconfiguration (NEW)
A10 – Failure to Restrict URL Access	↑	A7 – Failure to Restrict URL Access
<not in T10 2007>	+	A8 – Unvalidated Redirects and Forwards (NEW)
A8 – Insecure Cryptographic Storage	↓	A9 – Insecure Cryptographic Storage
A9 – Insecure Communications	↓	A10 – Insufficient Transport Layer Protection
A3 – Malicious File Execution	−	<dropped from T10 2010>
A6 – Information Leakage and Improper Error Handling	−	<dropped from T10 2010>

What does all this mean?

Select target

- Pick a suitable target, there are several criteria you can apply.
- Attacks should not be random events
- Pick a victim within your capabilities
- Improve your skills constantly
- READ READ READ READ
- Sign up to security blog sites,
- Keep up to date on zero days and version update releases



What would a white hat do here? *Test what he is allowed to access*
What would a black hat do here? *Scan to gather as many victims as possible*

Golden Rule: 1

Justify benefit

- There must be a gain in your action
- Less and less common to attack with aim of destruction
- Be sure you will be happy with the result if you get your wish?

What would a white hat do here? *Find the problem and report it*
What would a black hat do here? *Fun and profit!*

Golden Rule: 2

Learn application flow

- Discover the business logic
- Figure out what the application wants you to do and document it.
- Be able to describe action/response for every click

What would a white hat do here? *Learn about the allowed area*
What would a black hat do here? *Learn as much as possible and share it*

Golden Rule: 3

Probe architecture and design

- Figure out what components are used
- Get details on version numbers and products
- Check for default usernames and password
- Check ports

What would a white hat do here? *Stick to the allowed areas*
What would a black hat do here? *Go to town... Do everything, everywhere...*

Golden Rule: 4

Identify entry points based on components

- Map on paper the application as you understand it
- Compose potential attack vectors
- Decide the best route to achieve the predetermined goal

What would a white hat do here? *Stick to the testplan...*
What would a black hat do here? *Everything, everywhere...*

Golden Rule: 5

Chart attack vector matrix on each component

- Using a predefined attack matrix, select attacks suitable for component.
- Generate a complete list and develop a testing plan.

What would a white hat do here? *"You are supposed to test only this..."*
What would a black hat do here? *"w0w! Machines all over the place!..."*

Golden Rule: 6

Carry out simplified to complex probes

- Starting with the most simple test cases develop an attack story
- Treat the results of simple test as clues to the next step
- Gradually increase the complexity of the probes.

What would a white hat do here? *No problems found in the allowed areas*
What would a black hat do here? *Nothing in that service, but there I hit the spot!*

Golden Rule: 7

Analyse results

- Chart out the results you are getting
- Do they help you achieve the goal
- if not, why not?
- Was you testing methodology sufficient to achieve the goal based on your findings?
- Should you relook at how you achieve goal
    - link in chain V one time hit.

What would a white hat do here? *The goal is to find a problem*
What would a black hat do here? *while 1; FUN_AND_PROFIT!*

Golden Rule: 8

Build valid attacks based on derived benefit

- Based on your finding derive clean and clear steps to reproduce the issue.
- Stabilize the attack
- Look for variants that give the same result.

What would a white hat do here? *Theoretical attacks on allowed services*
What would a black hat do here? *A bunch of exploits all over the place!*

Golden Rule: 9

Contact Admin – let them know.

- It is important that you contact the owners of the application to let them know about the issue.
- Currently it is recommended that 180 days is enough notice (Responsible Disclosure)
    - This notice period is not legal protection for you
- You should not post the defect on any forums.
- If you are lucky the admins will fix the issue and after that give you credit publicly. Without contacting law enforcement.

What would a white hat do here?	*Responsible disclosure...*
What would a black hat do here?	*Carry on the hack, expose it to others (forums, hacktivism, trading, fun and profit!)*

Golden Rule: 10

The Golden Rules

- Select target
- Justify benefit
- Learn application flow
- Probe architecture and design
- Identify entry points based on components
- Chart attack vector matrix on each component
- Carry out simplified to complex probes
- Analyse results
- Build valid attacks based on derived benefit
- Contact Admin – let them know.

- Do you take the white or the black pill?
  - How deep into the rabbit hole do you want to go?

Best person to ensure