For my next trick... hacking Web2.0 (**lite**)

Petko D. Petkov (pdp)
GNUCITIZEN
http://www.gnucitizen.org

OWASP USA
November 2007

The OWASP Foundation
http://www.owasp.org/

powered BY

GNUCITIZEN

http://www.gnucitizen.org

...before we START

- Feel free to ask questions!
- Do ask questions!
- Have fun!

what is WEB2.0?

...

- Marketing buzzword
- Invented by O'Reilly Media in 2003
- Wikis, Blogs, AJAX, Social Networks, Collaboration
- APIs, SOA (Service Oriented Architecture)
- Data in the Cloud
- Applications on Demand

why web2.0 HACKING?

...

- Data Management
- Information Leaks
- Live Profiling
- Information Spamming
- Service Abuse
- Autonomous Agents
- Distribution
- Attack Infrastructures

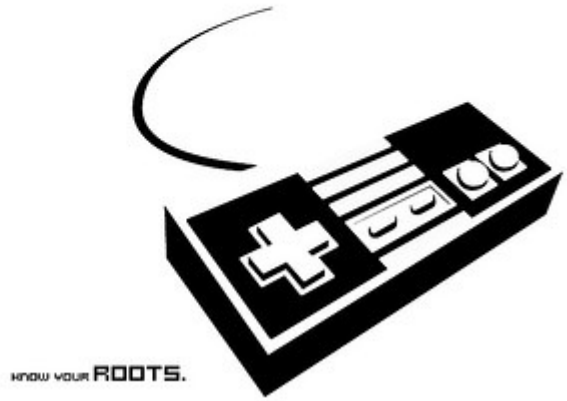
the PAPER

- 5 fictional stories with technology that is real
- Learn by example
- KISS (Keep it Simple Stupid)
- Problems with no solutions
  - I was told that I need to come up with some solutions, otherwise I cannot present at OWASP.

the STORIES

- MPack2.0
  - Attack Infrastructures
- Wormoholic
  - Autonomous Agents
- Bookmarks Rider
  - Distribution
- RSS Kingpin
  - Information Spamming
- Revealing the hidden Web
  - Service Abuse

know your ROOTS



...

what's MPACK?

...

what would it be in the web2.0 WORLD?

hint: Google Mashup Editor

...

who is SAMY?

...

what's a
covert
CHANNEL?

...

...but in the web2.0 WORLD?

...

who's the mechanical TURK?

...

...to MALWARE?

hint: Social Bookmarking

...

can web2.0 malware BROADCAST ?

...

...MD5(DOMAIN + TIME)

...

where are my SCHEDULERS?

...

where are my ACTUATORS ?

...

...data in the CLOUD...

(the malicious one)

...

...applications on DEMAND...

(the malicious ones)

...

what's state
and what's
PERSISTENC
E?

...

riding social bookmarks is FUN!

...

...maybe
make some
money TOO!

...

to splog or not to splog. This is the QUESTION!

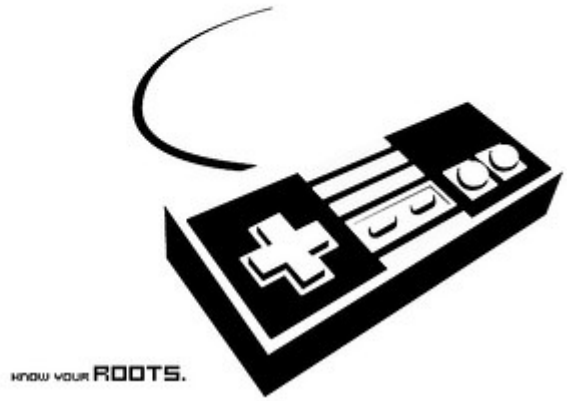
...

call me the rss KINGPIN!

...

service abuse
and the
hidden WEB

know your ROOTS



...more

- Profiling targets by watching their Web activities
- Snoop onto targets
- GEO Position Mobile phones
- GEO Position individuals
- More service abuse
- More vulnerabilities
- More Insecurities

...

solutions and recommendations?

thank YOU

GNUCITIZEN

http://www.gnucitizen.org