
So, U W4nn4 b Hax0R?

Disclaimer

Kiran Karnad

Twitter: ipentest

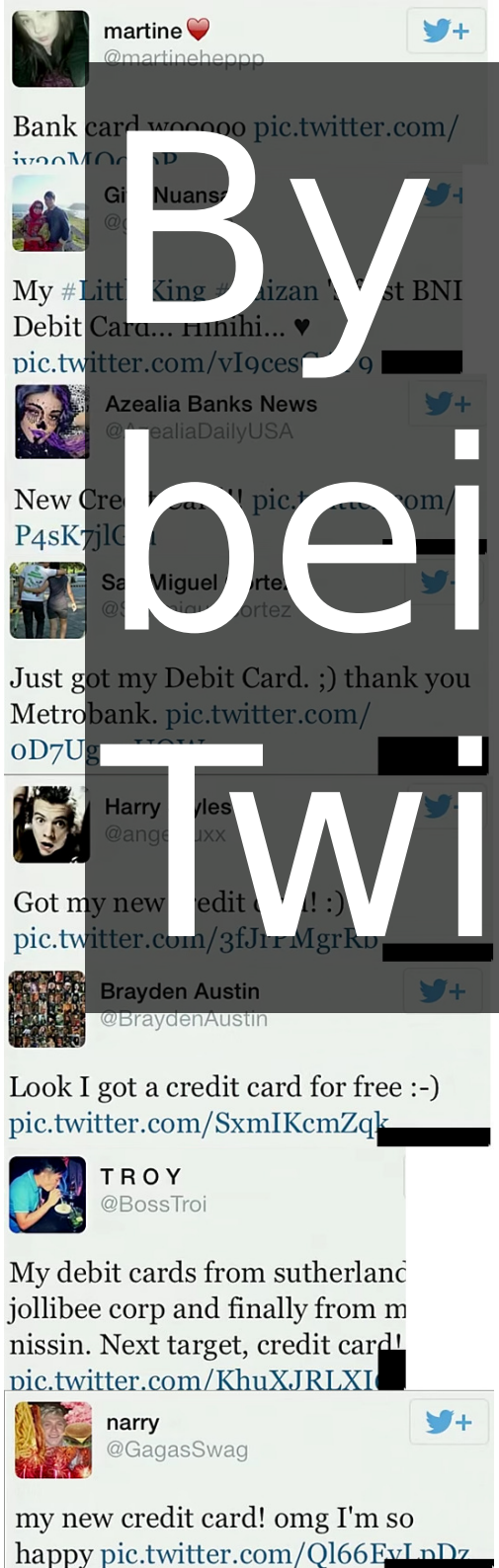
http://www.tinyurl.com/kirankarnad

Love: BC and H1

HoFs: 99+

Non-Tech Hacking


Bank of America
DEBIT CARD
7512 2240 3942
Taplus anak
BNI
DEBIT
6010 0401 9237 5096
6010
HSBC
4659 1234 5678
oyds TSB
8184 9377 6044
08/14
VISA
Taplus anak
BNI
DEBIT
6010 0408 9205 4223
6010
MEMBER SINCE 13
VALID THRU 07/18
KAIZAN DEVIANOS
PLATINUM DEBIT CARD
4342 5629 9329
4342
CUSTOMER SINCE 2013
GOOD THRU 06/16
MIKAYLA S HILL
DEBIT
VISA
Access Card
Interac
VISA
Citizens Bank
1. How did I get these?



By being on Twitter!

2. **Instant** Hacker

3. Distributed **DoS**

3a. **DAAS** - DDoS As A Service

3b. **Stressed Booters** demo

But we prefer **self-service** la

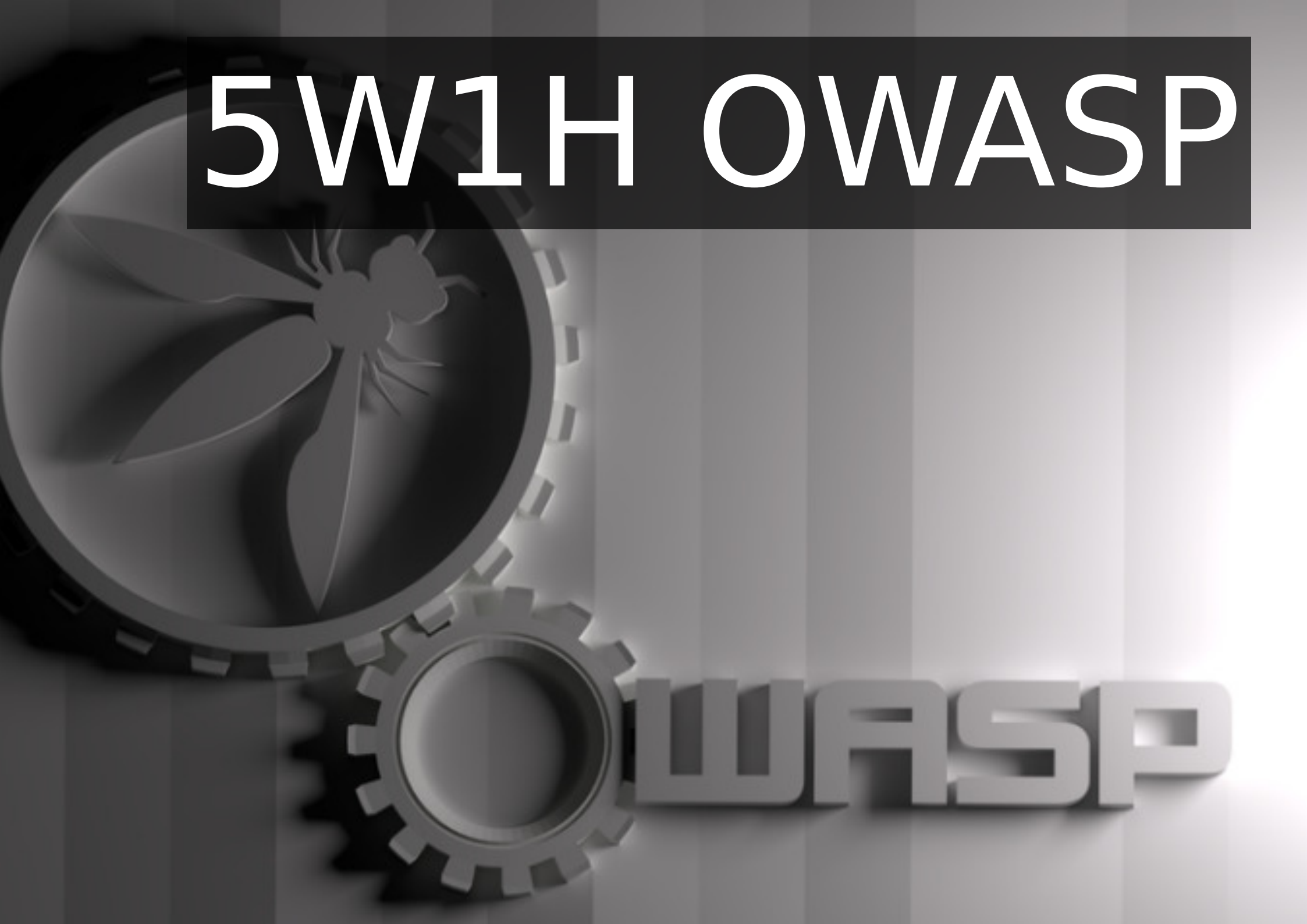

3c. Like LOIC?

Real-time Attacks

4. **Social Engineering**


TIME ZONES OF THE WORLD
Greenland
(DENMARK)
CANADA
UNITED STATES
MEXICO
RUSSIA
CHINA
INDIA
BRAZIL
AUSTRALIA
INDONESIA
ALGERIA
LIBYA
EGYPT
SAUDI ARABIA
IRAN
KAZAKHSTAN
MONGOLIA
NORTH ATLANTIC OCEAN
NORTH PACIFIC OCEAN
SOUTH PACIFIC OCEAN
SOUTH ATLANTIC OCEAN
INDIAN OCEAN
ARCTIC OCEAN
Tech Hacking

5W1H OWASP



OWASP Top 10 – 2010 (Previous)	OWASP Top 10 – 2013 (New)
A1 – Injection	A1 – Injection
A3 – Broken Authentication and Session Management	A2 – Broken Authentication and Session Management
A2 – Cross-Site Scripting (XSS)	A3 – Cross-Site Scripting (XSS)
A4 – Insecure Direct Object References	A4 – Insecure Direct Object References
A6 – Security Misconfiguration	A5 – Security Misconfiguration
A7 – Insecure Cryptographic Storage – Merged with A9 →	A6 – Sensitive Data Exposure
A8 – Failure to Restrict URL Access – Broadened into →	A7 – Missing Function Level Access Control
A5 – Cross-Site Request Forgery (CSRF)	A8 – Cross-Site Request Forgery (CSRF)
<buried in A6: Security Misconfiguration>	A9 – Using Known Vulnerable Components
A10 – Unvalidated Redirects and Forwards	A10 – Unvalidated Redirects and Forwards
A9 – Insufficient Transport Layer Protection	Merged with 2010-A7 into new 2013-A6

OWASP Top 10

5. OWASP Live Demos


A1. Injection


A1.1. HTML Injection Demo

A1.2. **SQL** Injection Demo

A2. **BASM** Demo

A3. XSS

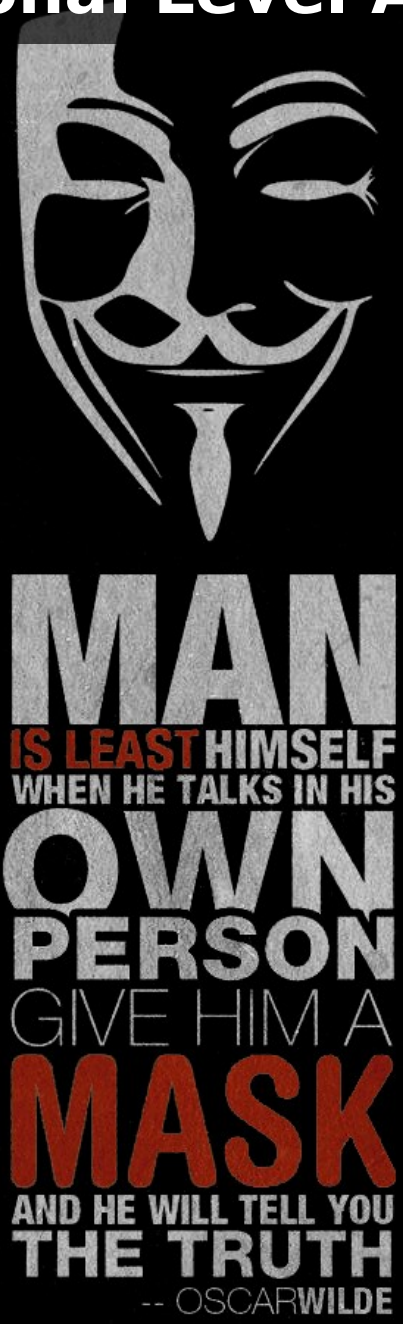
The HS Demo

A4. **IDOR** Demo


A5. Security **Misconfiguration** Demo

A6. Sensitive **Data Exposure** Demo

A7. Missing **Functional Level Access Control** Demo




Skipping A8. to A10, but you get the point right!

Thanks for the opportunity

Thank You, Any FAQs?