CLEÓRBETE SANTOS

cleorbete@gmail.com
www.cleorbete.com
www.twitter.com/cleorbete
www.facebook.com/cleorbete

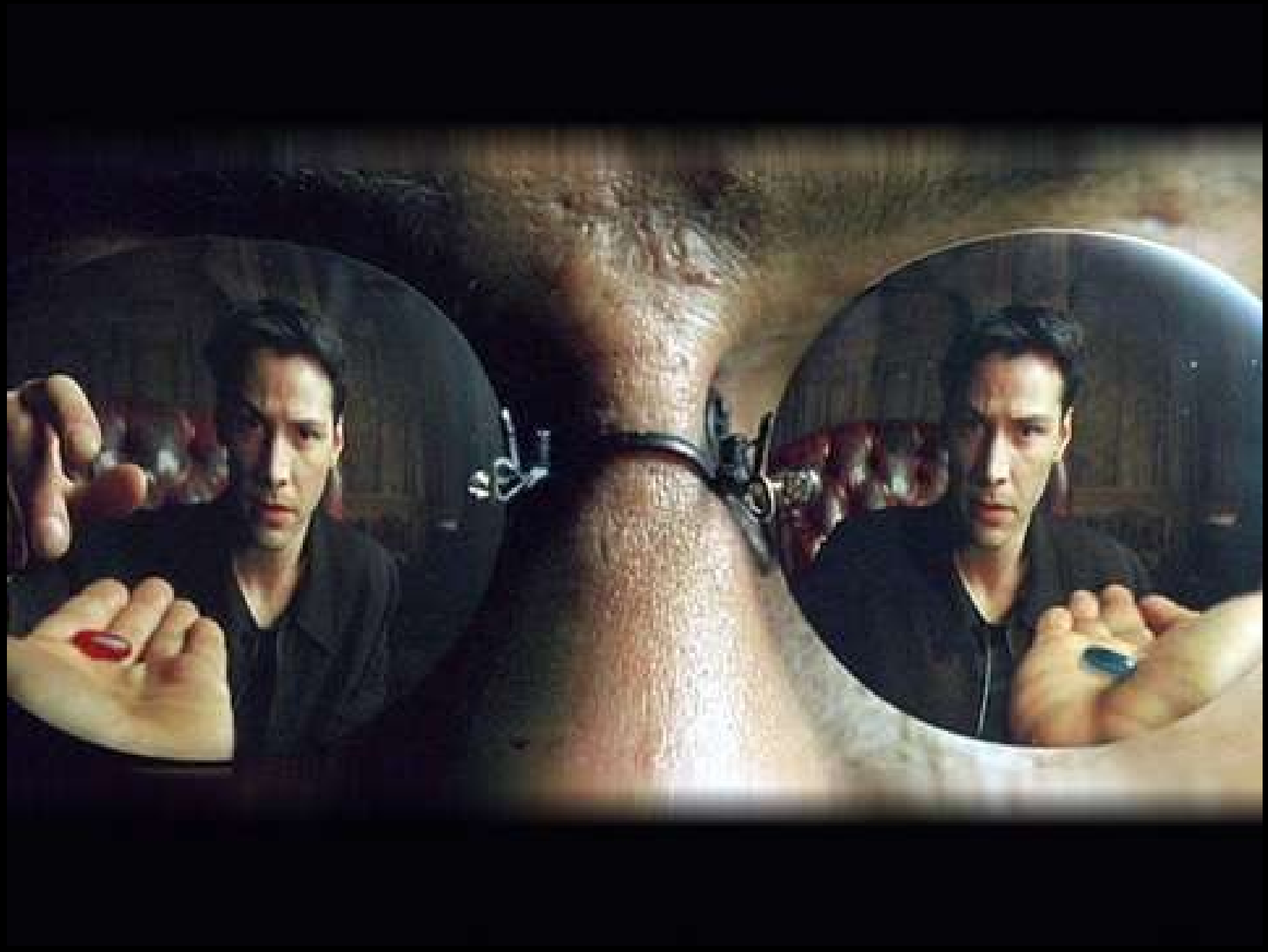
Entre em contato, terei prazer em trocar conhecimentos com você!

SEGURANÇA EM APLICAÇÕES WEB

Cleórbete Santos - www.cleorbete.com
FORTES – Fórum de Tecnologias e Engenharia de Software do Tocantins – www.tre-to.jus.br/fortes

SEGURANÇA EM APLICAÇÕES WEB

ESCOLHI A PÍLULA VERMELHA!



Escolhi a pílula vermelha!

- Matrix
- Alice no país das maravilhas
- O mito da caverna
- Jean Baudrillard
- Interdisciplinaridade da ITSec

Hacker: “o que muda o que toca”

- Definição confusa
- Década de 50 no MIT
- Filme “Jogos de Guerra” (1983)
- “Eles são crackers!” (1985)
- White, Black, e Gray Hats
- Elite Hackers
- Hacktivistas
- Ethical Hacker

CEH

- CEH – Certified Ethical Hacker
- EC-Council (www.council.org)
- Capacita o FBI, NSA, PF, etc
- Exige curso p/ certificação
- CHFI, além de outros
- Mestrado em Segurança

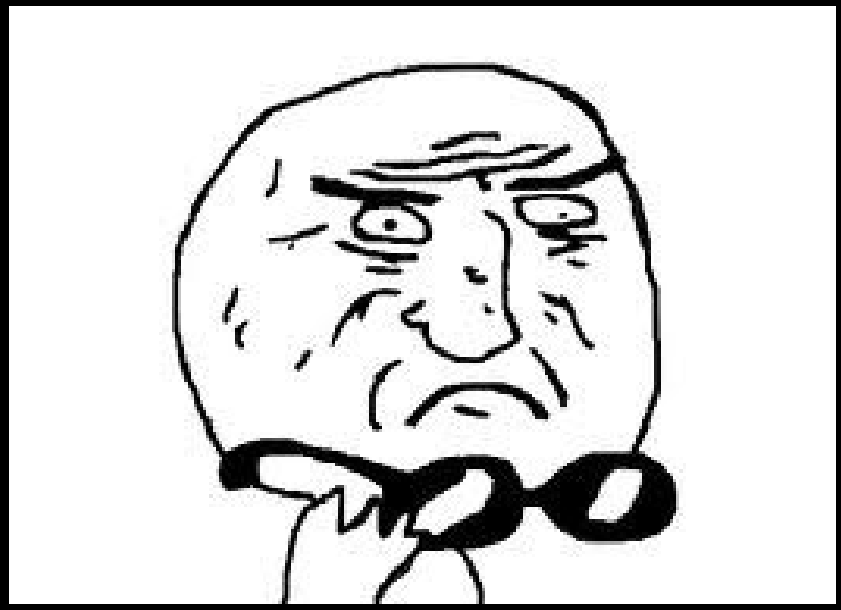
SEGURANÇA EM APLICAÇÕES WEB

THE “D” CEH MASTER

Cleórbete Santos - www.cleorbete.com
FORTES – Fórum de Tecnologias e Engenharia de Software do Tocantins – www.tre-to.jus.br/fortes

SECURITY+

- CompTIA (www.comptia.org)
- Exige curso p/ certificação
- Exige 2 anos de experiência
- A página deles é feita em...
- aspx



CISSP

- Certified Information System Security Professional;
- (ISC)²
- International Information Systems Security Certification Consortium
- www.isc2.org
- Mínimo de 5 anos de experiência
- Entre outros requisitos

TREINAMENTOS NO BRASIL

- www.clavis.com.br
- www.strongsecurity.com.br

ENGENHARIA SOCIAL

- Currículos
- Editais de licitação
- Shoulder surfing
- Códigos em fóruns
- Phishing
- Spear Phishing
- Caso CEZ...
- Caso FORTES...

SEGURANÇA EM APLICAÇÕES WEB

CASO FORTES

Informe seus dados

Até mais, cleorbete. ×

Email

Nome da mãe

Data de Aniversário / (dia/mês)

Enviar dados

OWASP

- Open Web Application Security Project
- www.owasp.org
- Representação em vários países
- OWASP Floripa Day 2012

SEGURANÇA EM APLICAÇÕES WEB

OWASP TOP 10

1 Injection
2 Cross-Site Scripting (XSS)
3 Broken Authentication and Session Management
4 Insecure Direct Object References
5 Cross-Site Request Forgery (CSRF)
6 Security Misconfiguration
7 Insecure Cryptographic Storage
8 Failure to Restrict URL Access

OWASP TOP 10 - continuação

9 Insufficient Transport Layer Protection

10 Unvalidated Redirects and Forwards

DVAW

- http://code.google.com/p/dvwa/

SEGURANÇA EM APLICAÇÕES WEB

10 DICAS PARA SECURE DEV

1. Validar entrada (em todos os lugares)
2. Habilitar alertas do compilador em nível máximo
3. Modelar o sistema pensando na segurança
4. Manter a simplicidade
5. O padrão é negar
6. Princípio do menor privilégio
7. Sanitizar dados que sairão para outros sistemas
8. Combinar práticas de defesa (como programação segura & ambiente seguro)
9. Validar a segurança (Pentest, Auditoria de código, Etc)
10. Adotar um padrão de código seguro (para a linguagem utilizada)

SDL – Security Development Lifecycle (princípios)

- Segurança por Design
- Segurança por Padrão
- Segurança na Implantação
- Segurança na Comunicação

ALÉM DISSO TUDO...

- BSIMM – Maturity Model...
- Políticas de Seg. da Corporação
- Leis, Sarbanes-Oxley, HIPAA, etc
- Normas ISO (27000, etc)
- Outros (PCI DSS, ANSI-x9)

FERRAMENTAS

- Nessus
- Nikto
- w3af
- Acunetix
- Burp
- OWASP ZAP - Zed Attack Proxy Project
- Vega
- Arachni
- Core Impact*
- Metasploit Pro*
- Immunity Canvas*
- HP Webinspect*

LIVROS

- The Secret of Hacking 4
- Hacking Exposed - Web 2.0
- Hacking Exposed - Web Applications 3
- 24 Deadly Sins of Software Security
- The Web Application Hackers Handbook 2
- SafeCode - Fundamentals Practices for Secure Software Development

ENCONTROS

- Defcon (www.defcon.org)
- SegInfo (www.seginfo.com.br)
- ICCYBER (www.iccyber.org)

SEGURANÇA EM APLICAÇÕES WEB

OBRIGADO...