A ‘Web Application Security’ Challenge

Dinis Cruz, Dec 2010

BIG DISCLAIMER!!!!!!

...this is my **personal opinion** and

I'm not talking on behalf of OWASP
or any of the companies
I work for...

A ‘WEB APPLICATION SECURITY’ CHALLENGE TO PORTUGAL

and others that care about application security

As presented at:

OWASP The Open Web Application Security Project

IBWAS'10

2nd OWASP
Ibero-American
Web Application
Security Conference

16.17 December 2010

ISCTE . Instituto Universitário de Lisboa

LISBOA . PORTUGAL

A NEW Paradigm for Application Security

note: this presentation is designed to be read

Five (5) Proposed Focus

#1) Treat Software and Application Security with the respect and care that it deserves

Proposed Focus

#2) View Application Security as Business Intelligence

Proposed Focus

#3) View Application Security as Competitive Advantage

Proposed Focus

#4) We need to make the Application Security Market ‘work’

Proposed Focus

#5) Use OWASP as an Resource and Enabler

Proposed Focus

Twelve (12) Proposed Actions for Government or Industry

#1) Allow Ethical Hacking

Proposed Action

#2) Publish the results of Security Reviews (Application Score Cards)

Proposed Action

#3) Enhance Security requirements on procurement contracts

Proposed Action

#4) Introduce Liability for Government and Publicly Traded companies

Proposed Action

#5) Create an Independent ‘Vulnerability Disclosure’ agency

Proposed Action

#6) Rewrite Computer Laws

Proposed Action

#7) Pay for Open Source (Application) Security

Proposed Action

#8) Demand the Open Sourcing of widely used ‘Not-Supported / End-Of-Life Applications’ (for example IE6)

Proposed Action

#9) Create an Insurance market for Web Applications' Security

Proposed Action

#10) Reduce the number of Assets (secrets, private data, credit cards info, etc...)

Proposed Action

#11) Improve Journalism coverage and quality (and independence)

Proposed Action

#12) ‘Proper’ SSL support for 50% of websites

Proposed Action

Note that these laws (or recommendations) could be also done at local level

...for example in a local District/Council ...

... remember the impact of
‘California Disclosure laws’

FUD Section

FUD is

Fear,
Uncertainty, and
Doubt

http://en.wikipedia.org/wiki/Fear,_uncertainty_and_doubt

I’m am going to scare you now

...but I'm going to try to be
as pragmatic as possible

...If anything I'm actually being low-key here

...I'm not saying nothing
that has not been said before

Why am I going to scare you?

Because there is a general lack of awareness of how bad is the problem

Why am I going to scare you?

It works (see USA's actions for the past 10 years)

Why am I going to scare you?

If it can be used for government/Corporate agendas, lets see if we can make it use for public health agendas

Everything is Broken!!!

- HTTP is broken
- SSL is broken
- DNS is broken (DNS Rebinding, DNS Chache Poinsoning (Dan Kamisky)
- Browsers are broken
- Websites are broken
- Web Development Frameworks are broken
- Sheer number of Microsoft vulnerabilities (see this month’s MSRC advisories). And Microsoft is one of the BEST vendors (they spend a huge amount of money and resources on Application Security)
- Backdoors in 'secure operating systems' (FreeBSD email)

Its software
everywhere

most (if not all) of you work in ‘software’ companies:

* Supermarkets,
* Construction companies
* Banks,
* Websites
* Government bodies,
* Logistic companies

Your company develops (internally our outsourcing) thousands if not millions of custom lines of code

Your entire life depends on software and more and more these days, on Web Applications

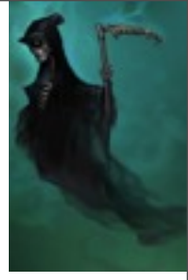
In fact ‘we’ are becoming software

my mom's hearing aid and its ‘advanced features’

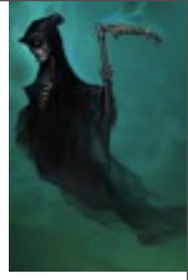
(was there any authentication there?)

Deaths in WebAppSec

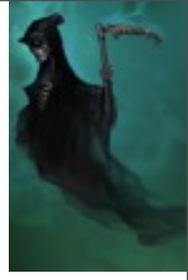
...still on FUD theme...

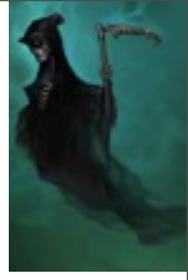
“How many many people will have to die before we take application security seriously?



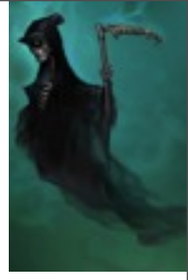
1, 10, 100, 1000, 10000, 100000?



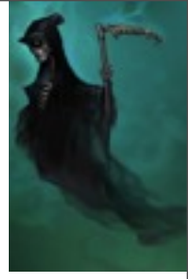
How many Bridges need to fall?



How much money needs to be lost?

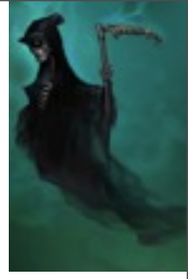


What would be the scenario that would case people or governments to act?

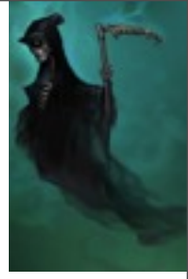


...what about the following 21 scenarios?

...which one(s) would be enough?



1. **Mass supermarket failure (no food, milk, water available)**
2. **Bank or Financial Company collapse**
3. **Fabricated News**
4. **Mass loss, sale and exploitation of Individuals Private information**
5. **Mass Identify Theft!**
    - Can you prove that YOU are YOU?
    - What if the ‘Computer says differently’?
    - What if your picture ‘in the computer’ is different?
    - What if your date-of-birth are family name are different?
    - What if you are shown as DEAD in the system? (how many databases would it take to kill you digitally)
    - What if there is NO record at ALL that you ever existed?
        - in ID database
        - in Financial database
        - in Hospital databases
        - etc...?

6.Medical systems exploitation:

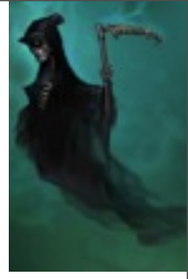
- Wrong medicaments delivered, sold
- Manipulating hospital systems
- Corruption of medial records
- Sale of medial records

7.Car/Plane/Train crashes:

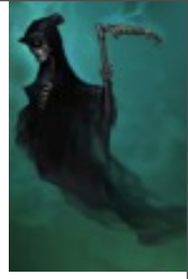
- all lights are made green at the same time
- maintenance records are fiddled or manipulated (Fake parts scam)
- Remote control and manipulation
- Manipulation of traffic guidance systems

8.ID cards/Passport exploits

- Government loses ability to issue new ID cards
- Massive ID Card fraud
- Companies are selling Fake ID carts with no ability to stop them

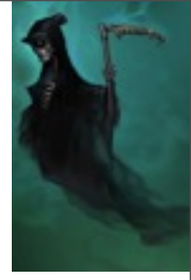
9. **No Cashpoints**
10. **New laws introduced in parliament** (without formal discussion/approval)
11. **Fighter jet fires missile into crowd / building / city**
12. **Mass hysteria at stadium, where a big message on screen says:**
    - *"...RUN!!!!!! The stadium is going to blow in 2 minutes..."*
    - *"...There is a terrorist in the stadium, here is his picture! Find him and kill him!!..."*
13. **Water poisoning**
14. **Manipulation of controls that introduce or remove chemicals in water**
15. **Attacks on electric grid**
16. **Mass compromise of online email systems**
17. **Corruption of Inland Revenue database** (if they did not know who owed what and they could not be able to collect money from taxes)



18. **Government attacks**
    - Paralysis of public bodies (‘IT systems are not working)
    - Mass deletion of Government Emails and documents
    - Creation of fake Government Emails or documents

19. **Websites massively attack users and users are afraid to go online**

20. **Localized or global Internet shutdowns**



just one more to go now....

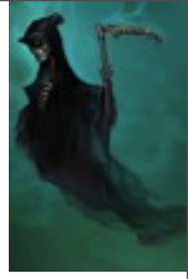
(I could continue but I guess
you are getting the point now....)

21. Hack the Planet

IBM Smart Planet vision is amazing and will deliver really good services, BUT, their entire model is based on increasing connectivity and inter-dependency between our infrastructure (for example smart-grid), and a ‘Smart Planet’ that is not built securely is a recipe for disaster!!!

IBM has the concept that needs to do much more:

http://www.ibm.com/smarterplanet/us/en/business_resilience_management/overview

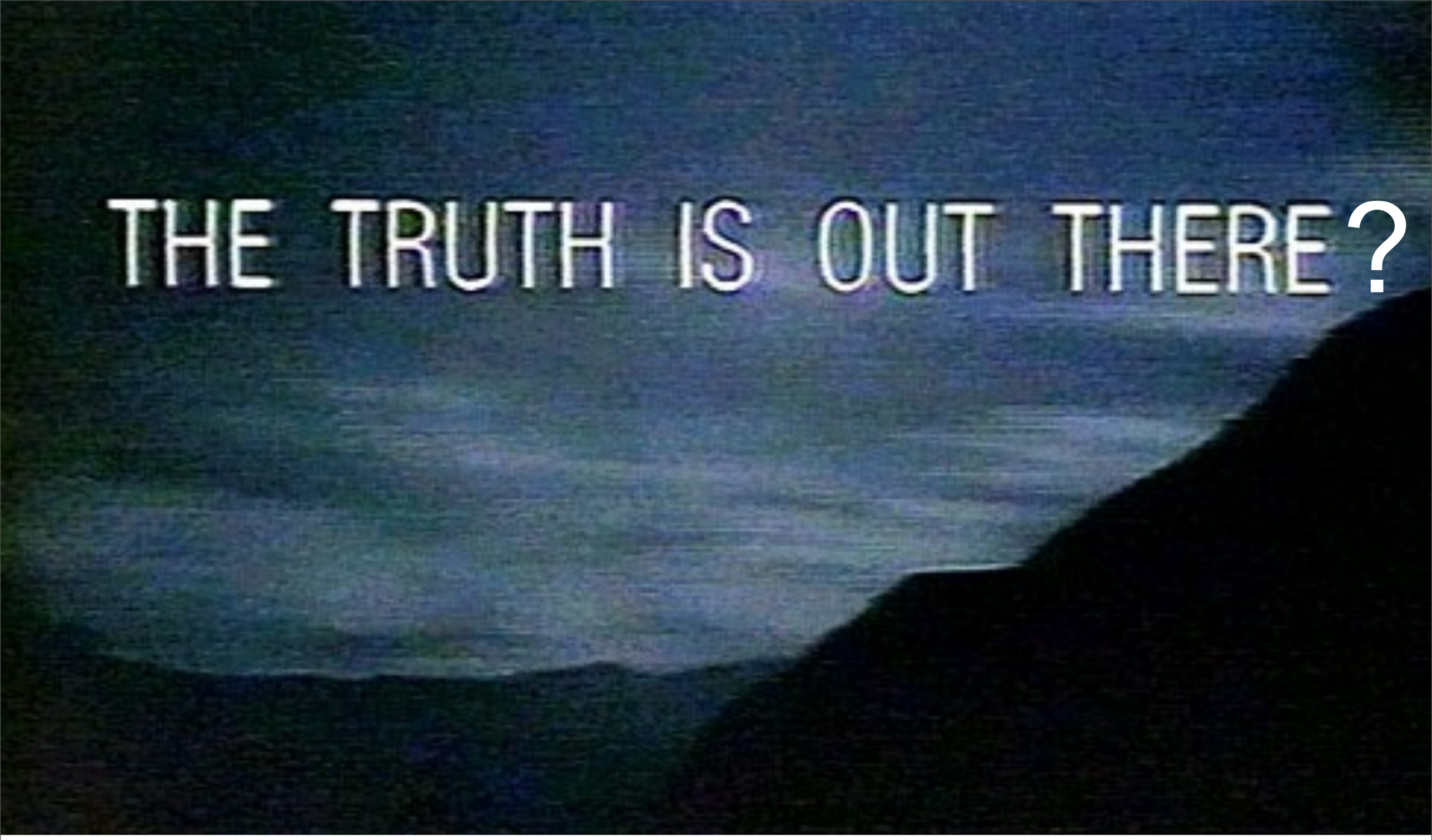


Unfortunately the previous examples are not that hard to technically execute...

... once the base systems are running on software

... and the data is stored in databases

... or word documents sitting on a server



Surely, right?

Current state of disclosure laws

We can’t speak about problems we know!!!

If we know that the main government XYZ website has massive vulnerabilities and could be malicious exploited (or even that is currently being exploited) we cannot talk about it

"...I wish I could talk about the ***security vulnerabilities in medical systems that I am aware of*** *since if they are exploited they could have* ***serious implications for people's lives****..."*

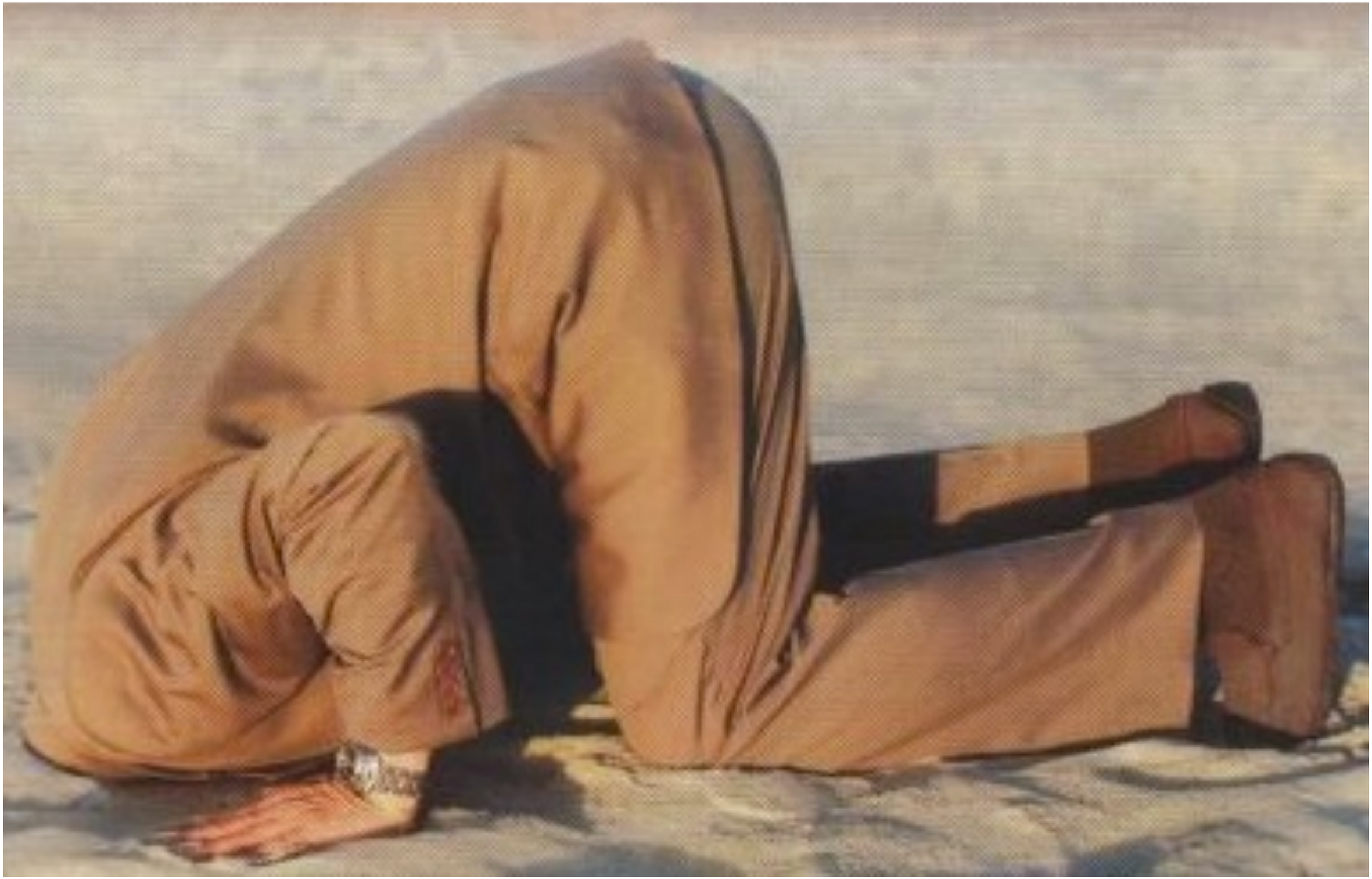
security consultant in this room

who can't even put his name on this phase

Today we promote complacency and reward the inaction

Good thing that there are not enough malicious attackers

Why does my government accepts to be controlled by 3rd party companies and governments (who control the software we run)



We all have the head in the sand

Nothing to do with us...

Really? ....

... what are you going to do next?

If you don’t do anything (after you’ve seen this presentation) you are now an accomplice of the status-quo

This is like knowing about the state of the financial industry (Banks, Madoff, Lehman Brothers) before the crash and not doing anything about it

Good News

We still use the web

We still shop online....

It has not collapsed...

yet

Making progress

- Operating Systems are getting better
- Some companies get it (some industries more than others)
- It is possible to write secure code
- The general awareness is Growing
- When companies care (or are forced to) they do a much better job
- Some clients are starting to demand more secure products applications
- Some Frameworks are able to hide security from developers and make created app ‘not vulnerable’ by default
- OWASP Is working on solutions :)

But, the problem is

- Not enough skilled attackers (with evolved business models) which would build the business case to do something about it
- Most clients/developers don’t care (unless they have been attacked or have a key individual that ‘forces’ security)
  - Writing secure code is:
  - hard
  - expensive
  - time consuming
  - not scalable
  - not appreciated by the business (& paying customer)
  - not user friendly (put screenshot of Abacus)

'Group Think'

en.wikipedia.org/wiki/Groupthink

WIKIPEDIA
The Free Encyclopedia

Article Discussion

Groupthink

From Wikipedia, the free encyclopedia

Groupthink is a type of thought within a deeply cohesive in-group whose members try to minimize conflict and reach consensus without critically testing, analyzing, and evaluating ideas. It is a second potential negative consequence of group cohesion.

Basically....

....‘Group Think’ is when most ‘players’

... say/think that that the

... current status is correct

... which is usually false

*Image by **Design G Productions**.*

... a variation of ‘group think’ is when

....we say YES

... due to ‘market/peer’ pressure

"All those in favour say 'Aye'."

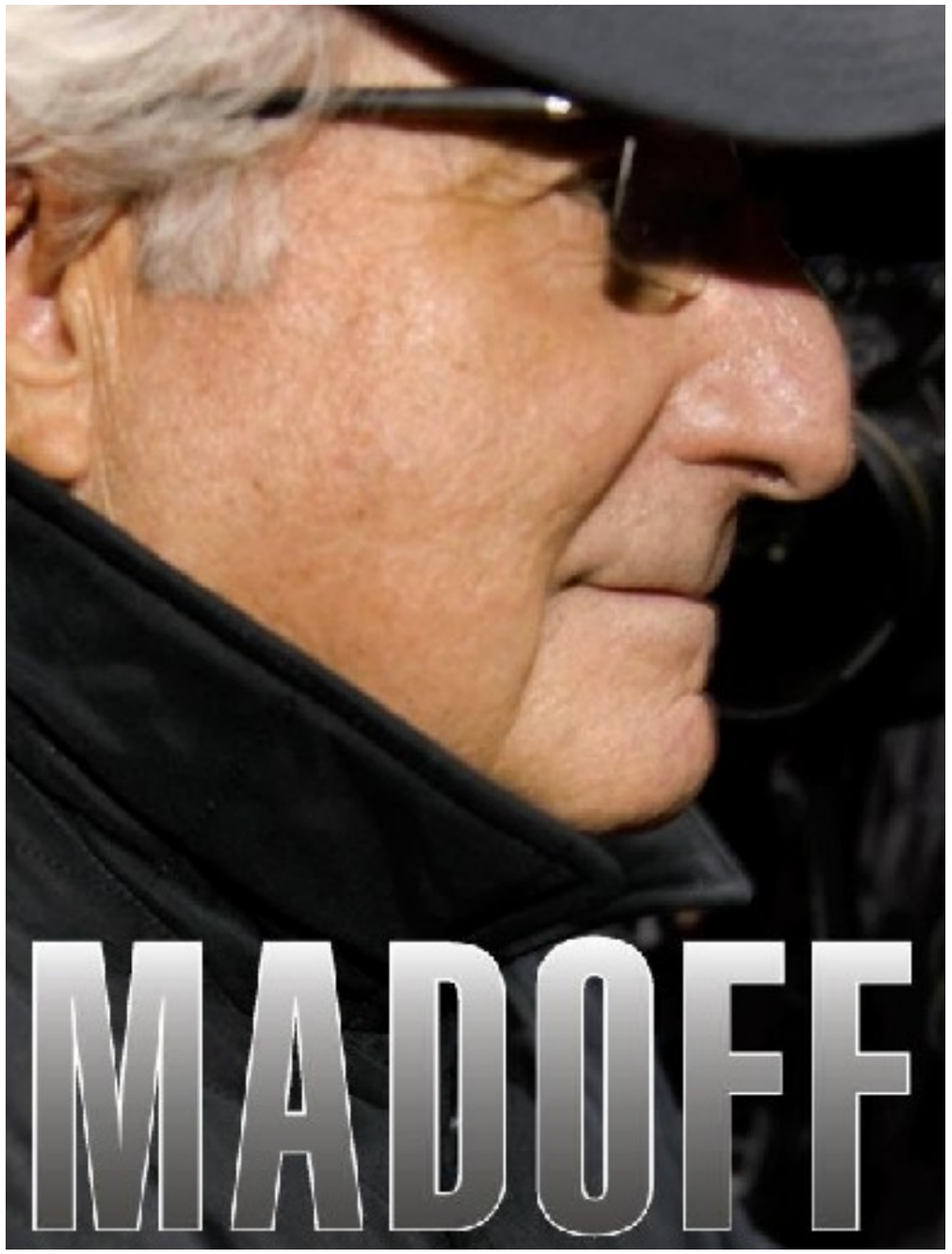
"Aye." "Aye." "Aye." "Aye." "Aye."

Here are some examples of
... recent ‘group-thinks’

... it would be great if we
...could learn from the past

PAST

ENRON



PAST

BUSINESS

Madoff Red Flags Were There All Along

Morning Edition
December 18, 2008 | More on NPR.org

In 2001, a reporter was skeptical of Bernard Madoff's strategy and performance on Wall Street.

‘Markets are efficient’

PAST

The Efficient Markets Hypothesis

September 1, 2009 — *No Comments*

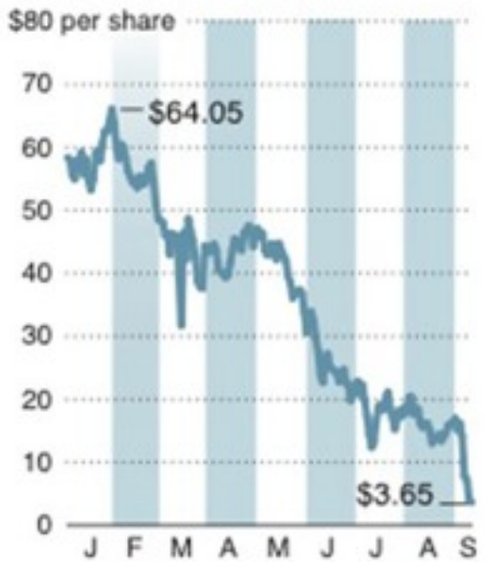
LEHMAN BROTHERS

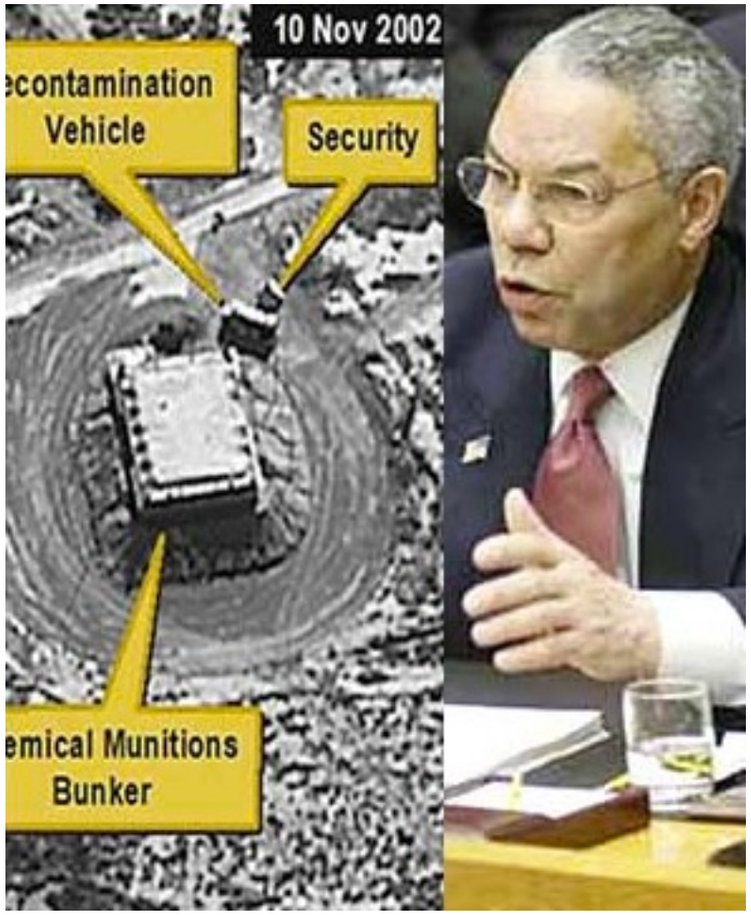
PAST

Lehman losses

Lehman Brothers shares closed below $4 and is down 94.3 percent from its January peak.

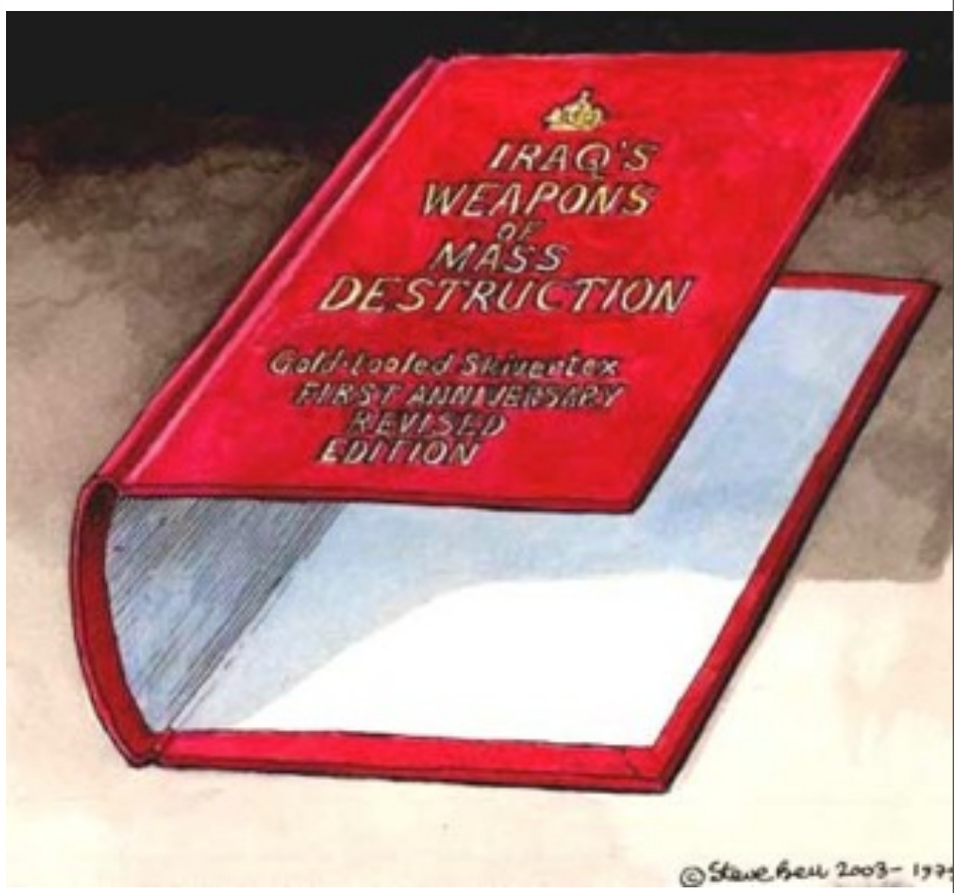
Lehman Brothers (LEH)





PAST

... WMDs in Iraq



.... so what is Application Security ‘group think’

There is nothing majorly wrong with:

'*The state of Application security world*'

... Nothing has happened (so far)

... There has been no major disruption (so far)

but...

apps (including ‘security products’) have

massive vulnerabilities

and (most) vendors and clients

are not motivated/interested in fixing them

(until there is an attack)

Unfortunately ...

... Strong NDAs & no Disclosure Laws
(prevent current knowledge
from being known)

So we don’t reward who does it right....

... and invests in security

But wont disclosure of information make it more dangerous?

won't the the attackers benefit
from knowing this information?

... don’t worry ...

.... they already have that information

It’s just like
Health and Safety

We expect water, restaurants,cars, planes, food, drink, medicaments, chairs, tables, roofs to have a minimum level of quality

We have laws that regulate them

We have laws that mandate disclosure of known problems

But, we have very little (if anything) in software and web applications

(PCI / DSS is an rare example)

Software and Web Application licenses gives

the client no rights
(he clicked on the EULA)

and gives the vendor no
liability and responsibility

We know disclosure works (public 0-days get patched quickly)

Non disclosure of application security information does not make us more secure, it just promotes complacency

The risk of a attack driven by the disclosure of the information is offset by the improvement of security

And any malicious attacker will have access to that information

In fact most malicious attackers today care more about your system than you (and in fact in a lot of cases they will protect and maintain the systems they compromise (its bad for their business to have other malicious attackers also compromising those boxes))

XSSed

Public XSS disclosure forum

The information is already out there.....

http://www.xssed.org

The XSSed project was created in early February 2007 by KF and DP. It provides information on all things related to cross-site scripting vulnerabilities and is the largest online **archive** of XSS vulnerable websites.

We started this project with the scope of increasing security and privacy on the web. Professional and amateur webmasters and web developers are notified about any cross-site scripting vulnerability affecting their online properties. The importance of securing their web applications is emphasized through the informational and educational content which we provide.

What we do is to simply validate all the submitted XSS vulnerable websites and then publish them on the archive. We actively assist all website owners to remediate the cross-site scripting issues by bringing them up to their attention on a timely manner. You will be helped by us for any problems you may face when trying to correct the XSS flaws. Please **contact** us.

XSS on portuguese websites

Results for "**.pt**" (limited to 20 entries per section)

XSS:

www.chip7.pt XSS vulnerability notified by **iNs4n3.PT**
www.ptu.ac.in XSS vulnerability notified by **APS**
www1.esec.pt XSS vulnerability notified by **Juza**
www.uevora.pt XSS vulnerability notified by **Juza**
www.regiao-sul.pt XSS vulnerability notified by **Juza**
beiratv.pt XSS vulnerability notified by **Juza**
ciberia.aeiou.pt XSS vulnerability notified by **Juza**
amizade.aeiou.pt XSS vulnerability notified by **Juza**
autosport.aeiou.pt XSS vulnerability notified by **Juza**
aeiou.caras.pt XSS vulnerability notified by **Juza**
aeiou.exameinformatica.pt XSS vulnerability notified by **Juza**
www.mygames.pt XSS vulnerability notified by **Juza**
www.meteo.pt XSS vulnerability notified by **Juza**
aeiou.escape.expresso.pt XSS vulnerability notified by **Juza**
www.infopedia.pt XSS vulnerability notified by **Juza**
www.cp.pt XSS vulnerability notified by **Juza**
olhares.aeiou.pt XSS vulnerability notified by **Juza**
www.alvorada.pt XSS vulnerability notified by **Fatal Attack**
www.ubi.pt XSS vulnerability notified by **Juza**
www.axa.pt XSS vulnerability notified by **TurKPoweR**

Evora's university

</xssed>
xss attacks information

Home | News | Articles | Adv. | Submit | Alerts | Links | XSS info | About | Contact

XSS Archive | XSS Archive ★ | TOP Submitters | TOP Submitters ★ | TOP Pagerank | search

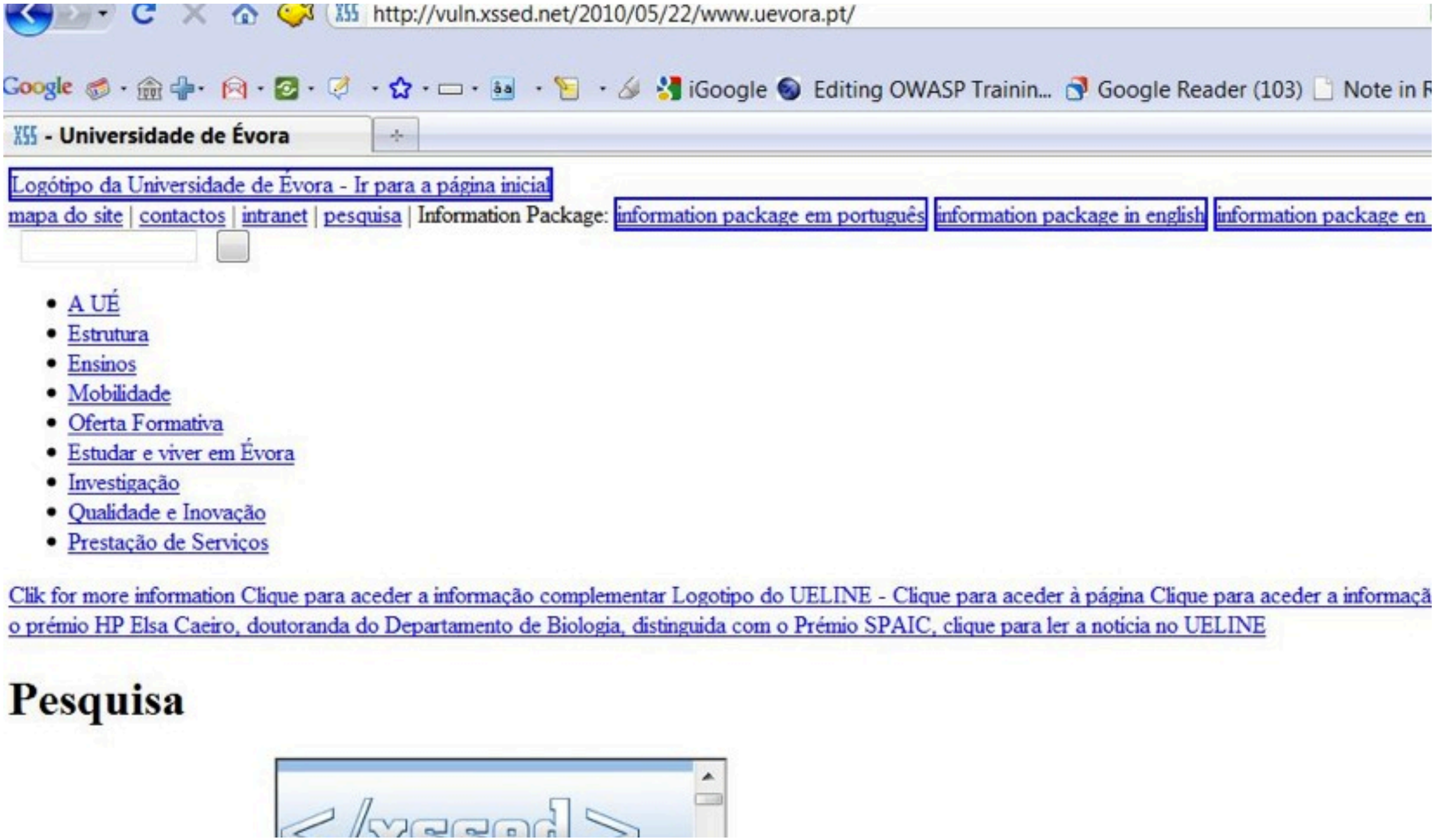
Security researcher Juza, has submitted on 22/05/2010 a cross-site-scripting (XSS) vulnerability affecting www.uevora.pt, which at the time of submission ranked 94944 on the web according to Alexa.
We manually validated and published a mirror of this vulnerability on 06/07/2010. It is currently unfixed.
If you believe that this security issue has been corrected, please send us an e-mail.

Date submitted: 22/05/2010	**Date published: 06/07/2010**	Fixed? Mail us!	**Status: ✗ UNFIXED**
Author: Juza	**Domain: www.uevora.pt**	**Category: XSS**	**Pagerank: 94944**

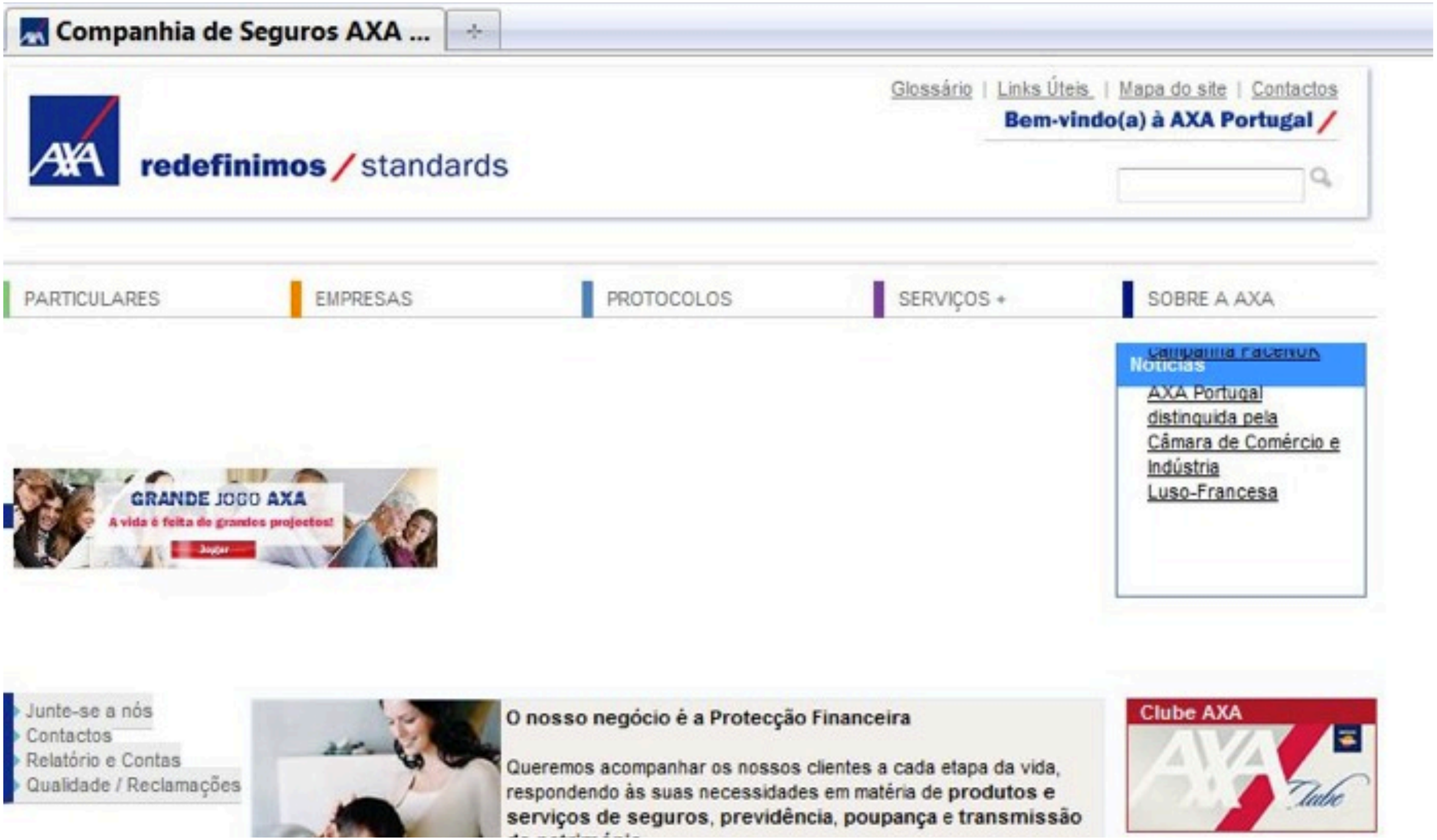
URL: http://www.uevora.pt/pesquisa/resultado?query=%3E%22%3E%3Ciframe+src%3D%22http%3A%2F%2Fxssed.com%22%3E

Click here to view the mirror

Evora's university



AXA.pt


Companhia de Seguros AXA ...
Glossário | Links Úteis | Mapa do site | Contactos
Bem-vindo(a) à AXA Portugal
redefinimos / standards
PARTICULARES
EMPRESAS
PROTOCOLOS
SERVIÇOS +
SOBRE A AXA
Notícias
AXA Portugal distinguida pela Câmara de Comércio e Indústria Luso-Francesa
GRANDE JOGO AXA
A vida é feita de grandes projectos!
Jogar
Junte-se a nós
Contactos
Relatório e Contas
Qualidade / Reclamações
O nosso negócio é a Protecção Financeira
Queremos acompanhar os nossos clientes a cada etapa da vida, respondendo às suas necessidades em matéria de produtos e serviços de seguros, previdência, poupança e transmissão
Clube AXA

AXA.pt

</xssed>
xss attacks information

Home | News | Articles | Adv. | Submit | Alerts | Links | XSS info | About | Contact

XSS Archive | XSS Archive ★ | TOP Submitters | TOP Submitters ★ | TOP Pagerank | search

Security researcher TurKPoweR, has submitted on 03/07/2009 a cross-site-scripting (XSS) vulnerability affecting www.axa.pt, which at the time of submission ranked 1149905 on the web according to Alexa.
We manually validated and published a mirror of this vulnerability on 20/06/2010. It is currently unfixed.
If you believe that this security issue has been corrected, please send us an e-mail.

Date submitted: 03/07/2009	Date published: 20/06/2010	Fixed? Mail us!	Status: ✗ UNFIXED
Author: TurKPoweR	Domain: www.axa.pt	Category: XSS	Pagerank: 1149905

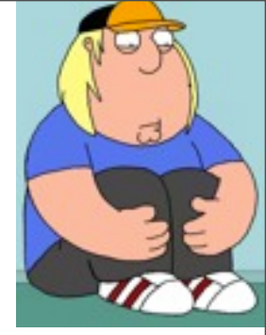
URL: http://www.axa.pt/mapeamento_log_internet.asp?log=>"><ScRiPt%20%0a
%0d>alert(/XSS%20By%20TurKPoweR%20
-%20FROM%20TURKEY/)%3B</ScRiPt><h1>XSS%20By%20TurKPoweR%20-%20FROM%20TURKEY</h1>

Click here to view the mirror

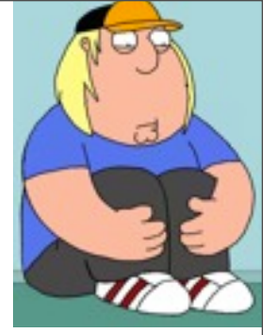
AXA.pt


Ficheiro Editar Ver Histórico Marcadores Ferramentas Ajuda
http://vuln.xssed.net/2009/07/03/www.axa.pt/
Google
iGoogle
Editing OWASP Trainin...
Google Reader (103)
Note in Rea
http://vuln.xs...3/www.axa.pt/
Ocorreu um erro ->>">
XSS By TurKPoweR - FROM TURKEY

Why am I so worried?



- There is no urgency today that we should be tacking this problem
- If we have to solve this problem after a major security incident we will be much worse of (see what happened in America after 9/11 with the massive over reaction that happened there)
- because I want to solve the web application security problem before it gets too serious
- the real problem with cyber security and malicious attacks are organised crime (i.e. criminals that are focused on making money who have the: intent, funding, technical ability, profit-focus and no ethical boundaries)
- Today some of the best distributed networks in the world are maintained by criminals groups (the botnets)
  - When was the last time you saw a commercial solution that is able to successful maintain a network of millions of computers?



- One day these criminals, if they get big enough, will realize that the biggest threat to their business model is us, the security focused people (i.e. the people in this room)

- That day they will be motivated to put a bullet in our heads, or just blow up (or poison the coffee) at one of our conferences!

- Question: what would happen if all of us DIED now? What do you think would be security impact on your company's Security profile?

- If I wanted to attack you company/sector, wouldn't it make sense to kill you first? (since you would be the ones tried to detect and stop the attack?)

OK ....

ENOUGH TALK ABOUT PROBLEMS!!!!

Lets look at some solutions

Security as pollution

David Rice’s amazing presentation at OWASP AppSec USA

If you haven't seen David Rice's Presentation at OWASP AppSec USA ....

... you HAVE to see it ASAP....

http://vimeo.com/15506033

"... chocolate-brown, oily, bubbling subsurface gases, it oozes rather than flows."

Time Magazine

August [illegible]


Cuyahoga River fire.

EXHIBIT 1

THE ROAD TO SUSTAINABLE ENTERPRISE

1945-60s

POLLUTION DENIAL

"SMELL OF MONEY" [BALANCE]

OBLIGATION

1970-80s

END-OF-PIPE REGULATION

"PAY TO REDUCE NEGATIVE IMPACT" [TRADE-OFF]

OPPORTUNITY

MID 1980s-90s

GREENING

1_ POLLUTION PREVENTION
2_ PRODUCT STEWARDSHIP
3_ ECO-EFFICIENCY [WIN-WIN]

REORIENTATION

LATE 90s-PRESENT

BEYOND GREENING

1_ CLEAN TECHNOLOGY
2_ BASE OF THE PYRAMID
3_ ECO-EFFECTIVENESS [POSITIVE IMPACT]

THE ROAD TO SUSTAINABLE SECURITY

1950s-2003

POLLUTION DENIAL

"No such thing as perfect software"

OBLIGATION

2003 - Current

END-OF-PIPE REGULATION

"Mandatory firewalls, anti-malware, etc..."

PCI DSS, SOX, data breach laws...

OPPORTUNITY

???

SUSTAINABILITY

RE-ORIENTATION

Current - ?

BUILD SECURITY IN

"Pollution" Prevention

Product Stewardship (SDLC)

Security Efficiency (Monitoring)

> People are so focused on feature marketing that they do not stop to think about bugs until it is too late. After generations of this, and of the problem getting worse all the time, end users have developed a sort of Stockholm Syndrome with regard to buggy software. They believe it is normal, expected, and inescapable.

-Chad Perrin
TechRepublic


Patching
Spam
Configuration
Botnets
Audits
Weak Defaults
Weak Crypto
DDoS
XSS
SQL Injection
Assessments
Malware
Buffer Overf
CSRF
Focus of U.S.
Cyber Strategy
Cybercrime

If we can make the case that *'Web Application Security can help with Effectiveness and increase Competitive Advantage'* we will finally be in a position to change the market dynamics

Business case for Application Security

You (and governments and companies) need to embrace application security, not because you care, but because it can be made to be an competitive advantage

With application security (when used as business intelligence) you will be able to:

* understand how your application work
* be more productive
* be more efficient and effective
* be faster to market
* have a better brand
* sell more

Proposed revised

Computer Crime LAW

- Focus on Intent
- Make cyber crimes to have direct mapping to real world laws (that we already have): Theft, Destruction, Blackmail
- Allow (and encourage) Ethical Hacking
- Mandate disclosure of known security vulnerabilities (Health and Safety model)
    - This could be done privately first with a time limit for public disclosure
- Promote/encourage the development of application security technology (for both attacking and defending)
- Mandate higher standards for public bodies

It’s our turn

- The government had 10 years to do anything about it, and so far, their actions (laws and regulations) are not working
  - So let us (the experts) try in now, give us a change to make it work
  - We (the experts) care because we are the ones that will have to clean up the mess
  - We (the experts) care because we are the ones that are becoming targets
  - Note that the current system is not working (how many software/ application prosecutions and arrests have happened in the last 10 years?)

Let us Hack you!

There is enough talent in this room to bring down most (if not all) web infrastructure of Portugal (and that would probably the ‘least’ damaging scenario’)

It is scary that a small number of individuals can bring down (or seriously damage) significant parts of our infrastructure

Do you want to bet?

Would you bet your website againts the OWASP Leaders Team that are here?

Unfortunately the processing power that we have here in this room, we can bring down a very large number of websites (using basic attacks)

If you don’t think that this is real,

why don’t you let us do it?

Lets play the game of:

“Bring the internet down for a day”

(think of it like a country wide fire-drill)

What would happen in Portugal if the Internet was down for 1 hour, 1 day, 1 week?

Question: who do you want to be attacked by?

- a kid that defaces your website and puts a big banner saying “You’re hacked”
- a kid that sends so much traffic to your site that you know something wrong is going on and you do something about it
- a criminal that exploits your weakness slowly (i.e. undetected) and creates big financial (or operational) damage to your company/organization or clients
- a criminal that corrupts your database
- a security professional, that knows what he/she is doing and can help you to fix the problem?

Portugal and Brazil

- My Frustration with Portugal
- Big on “Soft Corruption” (not mafia style but as damaging)
- Nobody respects government and authority (I live in London were we still do (a bit :))
- The mood is that if a person doesn’t take advantage of a situation (but could), he/she is viewed as stupid
  - The rules of engagement are not clear
  - The people who just want to get on with their jobs and make a difference have to deal with government bodies that have very little transparency, independence and openness in their decision making process
- In a lot of cases we have government bodies that are the worse of both worlds:
  - they are run like monopolies
  - they don’t allow some private enterprises compete fairly with them
  - they allow other private enterprises/sectors to define/control the rules of engagement
  - very little transparency and openness into the decision making process

The government expects the people to be corrupt, threats them with suspicion, creates draconian to catch the ‘abuses’ and they end up creating a ‘self fulfilling prophecy’

My argument is that application security can be (one of the solutions) for Portugal by showing how an open, vibrant, ethical, multi-cultural industry can work and flourish

Why Portugal?

Because portugal has nothing to lose (it is already rock-bottom)

What I’m asking doesn’t cost any money

It only takes courage, focus and commitment

I don’t want to play politics, so if Portugal is not interested, then I’ve done my bit

By ‘Portugal’ I mean the ‘Portugal as a Community’ , i.e. you (which includes the government)

The Brazilians are kicking our asses!!

- They believe more in Portuguese Language than we do
- Most Portuguese (including young ones) still have a very ‘demeaning’ view of Brazil (they are the ones on top now, not us)
- Same thing for Angola
- They are focused, have energy and are doing something about it (are they a better partner for OWASP?)
- This should be a great PLOP (Paises Lingual Official Portuguesa) project, one that would unify the people and build relationships
- It is embarrassing from me (as a Portuguese) the current lack of collaboration and focus that Portugal has on our culture and countries that have massive historical connections

PORTUGAL is
Depressed :(

... Portugal is such a depressed country today ...

... and really needs new ideas

.... and business models

... SO ...

... let us show how one sector can do it right

... with energy, passion and focus

Portugal could become the **‘Switzerland of Hacking’**

- lots of talent would be developed here
- lots of talent would come to portugal
- new business would appear
- new business models would appear
- Portugal would become a technology power house
- We have the raw talent that is needed
- We are actually quite good at technology
- Out IT systems (telecoms, banking, government) are actually quite good (at least from a usability point of view (can’t comment on security :))

OWASP PORTUGAL

What is OWASP is doing for Portugal

- 150, 000 USD invested in the OWASP Summit 2008 (Algarve)
- 100,000 USD already invested (more under negotiation) in the next OWASP Summit in (Feb 2011)
- 5,000 currently invested in a Brazilian Event Management company to manage the ‘Brazilian Delegation’ to the Summit 2011
- Paulo Coimbra Salary (OWASP Project Manger)
- Sandra Paiva Consulting agreement (OWASP Training and OWASP Academies)
- Translation of OWASP Top 10 book to Portuguese
- OWASP Academies and UMIC
- Samy Tour (150 people in ESCTE)

in conclusion ....

I’m proposing a

NEW Paradigm for Application Security

---

recapping to the ideas previously presented

5 Proposed Focus

1. Treat Software with the respect and care that it deserves
2. View Application Security as Business intelligence
3. View Application Security as Competitive advantage
4. We need to make the Application Security market ‘work’
5. Use OWASP as an Resource and Enabler

12 Proposed Actions for Government or Industry

1. Allow Ethical Hacking
2. Publish the results of Security Reviews (Application Score Cards)
3. Enhance Security requirements on procurement contracts
4. Introduce Liability for Government and Publicly Traded companies
5. Create an Independent ‘Vulnerability Disclosure’ agency
6. Rewrite Computer Laws
7. Pay for Open Source (Application) Security
8. Demand the Open Sourcing of widely used ‘Not-Supported / End-Of-Life Applications‘ (for example IE6)
9. Create Insurance Market for Web Applications’ Security
10. Reduce the number of Assets (secrets, private data, credit cards info)
11. Improve journalism coverage and quality (and independence)
12. ‘Proper’ SSL support for 50% of websites

I’ve done my bit

your turn .....

Thanks