IMPLEMENTATION OF WEB APPLICATION SECURITY ASSESSMENT FOR PUBLIC SERVICE INSTITUTION “AN INDONESIA PERSPECTIVE”

1. DR. HASYIM GAUTAMA, 2. YUDHISTIRA NUGRAHA

Delivered at Annual Computer Security Applications Conference 2011
5-9 December 2011, Orlando, Florida, US
WHY : We Do Web Application Security Assessment??

Vulnerability Assessment Statistic for Public Institution Website, 2010

Number of Government Website

- Connect Method
- HTTP Authentication
- Cross Site Request Forgery
- Delete Method
- PUT Method
- Cross Site Scripting
- Unusual Method HTTP
- Local File Inclulde
- HTTP Directory Listing
- Cookies HTTP Only
- Request Error Handling
- Reflected Cross Site Scripting
- SQL Injection
- Trace Method Enabled
- System Path Disclosure
- HTTP Banner Disclosure
- Autocompleted Enabled

Confidentiality and created by Sholeh
WHAT: we are doing?

- We have adopted ASVS: Application Security Verification Standard

- 4 Verification Level
  - Level 1 – Automated Verification
    - Level 1A – Dynamic Scan
    - Level 1B – Source Code Scan
  - Level 2 – Manual Verification
    - Level 2A – Penetration Test
    - Level 2B – Code Review
  - Level 3 – Design Verification
  - Level 4 – Internal Verification

- Risk Based

- [https://www.owasp.org/index.php/ASVS](https://www.owasp.org/index.php/ASVS)
  *Edition Bahasa Indonesia*
HOW: We Do Web Application Security Assessment

<table>
<thead>
<tr>
<th>ISO-27001:2009</th>
<th>SELF ASSESSMENT</th>
<th>VERIFICATION</th>
</tr>
</thead>
</table>
| • Information Security Index  
  • Role of ICT  
  • Governance  
  • Risk Management  
  • InfoSec Framework  
  • Asset Management  
  • The Use of InfoSec Technology | • 14 Control Objectives  
  • More than 120 Security Control | • External Auditor  
  • Recommendations |
WHO: Involving Stakeholders

Ministry of Communication and Information Technology of Republic of Indonesia
Cq, Directorate of Information Technology

Government Institution (Central & Local Government)

State/Local Owned Enterprise

Other Entities
PROGRESS SUMMARY

INSTITUTIONS
- Directorate of Information Security Ministry of Communication & Information Technology Republic of Indonesia as Policy and Regulatory Body in Indonesia (2011)
- ID-SIRTII and ID-CERT for emergency response team
- Planning for National GOV-CERT
- Certificate of Authority Body for Government Public Key Infrastructure

Policy & Technical Support
- Telecom-Law, Cyber-Law, Public Transparency Law
- Establishing of Management of Information Security Standard based on ISO 27001 on Government Institutions
- Anti-Spam
- Web Security Assessment
- Information Security Governance
- Data Protection
- Critical Information Infrastructure Protection
- National Information Security Index for Government Institutions

HUMAN RESOURCES DEVELOPMENT
- Information Awareness Technical Assistance for Government Staffs
- Information Security Certificates for 7000 Government Staffs
THANK YOU

1. Dr. Hasyim Gautama, 2. Yudhistira Nugraha
Directorate of Information Security
Ministry of Communication and Information Technology of Republic of Indonesia

Please contact us for more inquiries
hasyim.gautama@kominfo.go.id, yudhistira.nugraha@kominfo.go.id
[+] HACKER MANIFESTO [+] 

[+] This is our world now...!!! [+] 
[+] the world of the electron and the switch, the beauty of the baud. [+] 
[+] We make use of a service already existing without paying for what could be dirt-cheap [+] 
[+] if it wasn’t run by profiteering gluttons, [+] 
[+] and you call us criminals...!!! [+] 

[+] We explore... [+] 
[+] and you call us criminals...!!! [+] 
[+] We seek after knowledge... [+] 
[+] and you call us criminals...!!! [+] 
[+] We exist without skin color, without nationality, without religious bias... [+] 
[+] and you call us criminals...!!! [+] 
[+] You build atomic bombs, you wage wars, you murder, cheat, and lie to us [+] 
[+] and try to make us believe it’s for our own good, [+] 
[+] yet we’re the criminals...!!! [+] 

[+] Yes, I am a criminal...!!! [+] 
[+] My crime is that of curiosity...!!! [+] 
[+] My crime is that of judging people by what they say and think, [+] 
[+] not what they look like...!!! [+] 
[+] My crime is that of outsmarting you, [+] 
[+] something that you will never forgive me for...!!! [+] 

[+] I am a hacker, and this is my manifesto. [+] 
[+] You may stop me, but you can’t stop us all...!!! [+]
Deface: http://www.polri.go.id

16 Mei 2011 Mengatasnamakan Mujahidin

Bangkitlah singa-singa Islam!

memperingati hari nakba
mengingat apa yang telah mereka perbuat kepada kaum Muslimin di negeri kaum Muslimin
mengingatkan untuk tidak lupa mendoakan Mujahidin di manapun berada (Allahu A'lam)
harus tetap sadar akan upaya pembusukan Islam & Jihad yang dilakukan intelejen dan pejuang pejuang anti Syari'ah Islam
kami tidak memiliki keterkaitan dengan kelompok manapun, menggunakan media ini untuk mendukung Mujahidin dan menyampaikan pesan

Bangkitlah singa-singa Islam!
www.lemhannas.go.id

11 Januari 2011 – Pelaku : c4ur

Deface : http://www.lemhannas.go.id
Mirror : http://www.zone-h.org/mirror/id/12888872