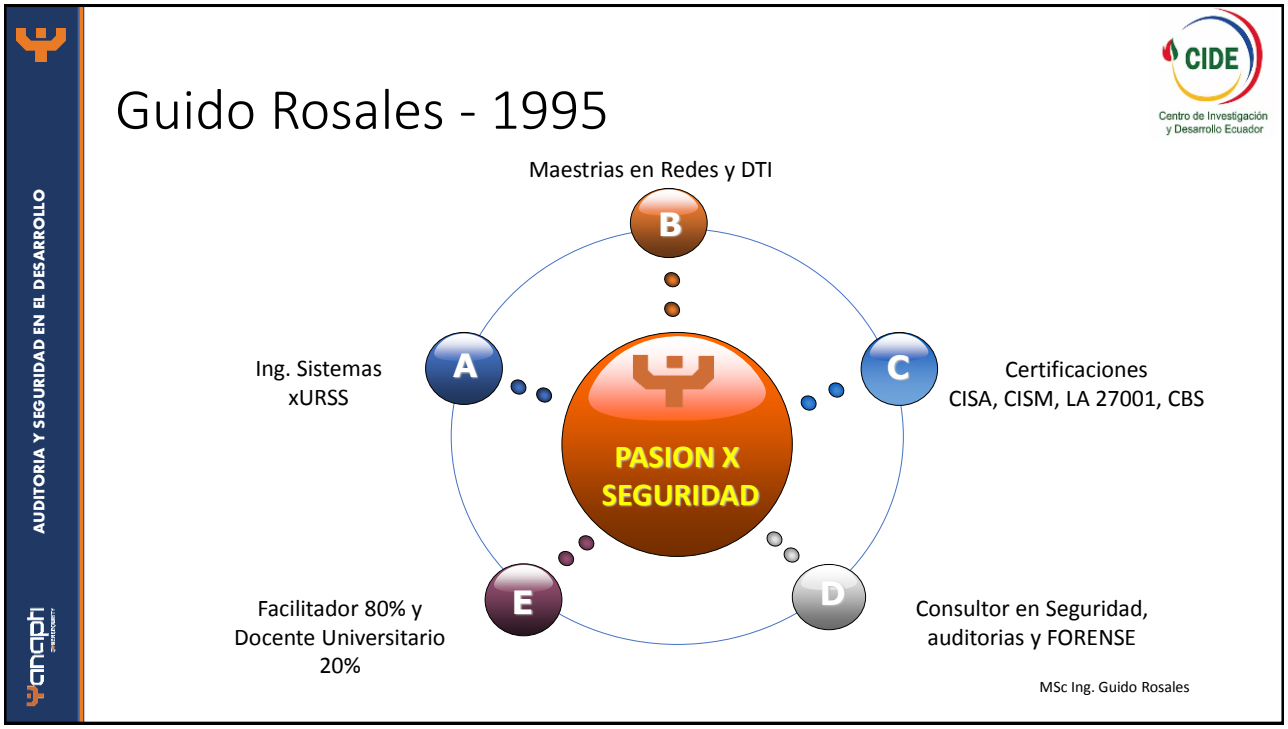
Firmado digitalmente por Guido Rosales
Fecha: 2018.03.13 10:04:49 -04'00'



AUDITORIA Y SEGURIDAD EN EL DESARROLLO

Yanapti

CIDE
Centro de Investigación y Desarrollo Ecuador

Yanapti CYBERSECURITY

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

LA AUDITORIA DE SEGURIDAD EN EL DESARROLLO DE APLICACIONES DE NEGOCIO

CIDE
Centro de Investigación y Desarrollo Ecuador

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

Contenido

1. La Auditoria de Sistemas
2. El Proceso de auditoria
3. Marco de Cumplimiento
4. Herramientas de Auditoria

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador

Contenido

1. La Auditoria de Sistemas
2. El Proceso de auditoria
3. Marco de Cumplimiento
4. Herramientas de Auditoria

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador

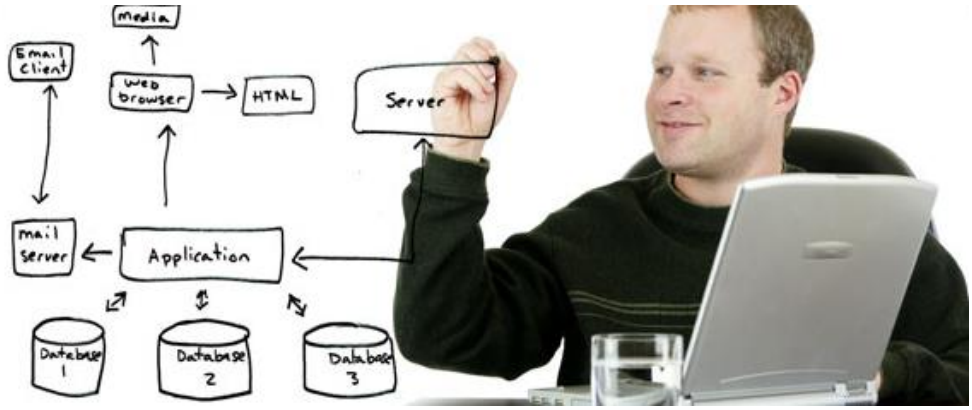
1. LA AUDITORIA DE SISTEMAS

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

AUDITORIA Y SEGURIDAD EN EL DESARROLLO
AUDITOR DE SISTEMAS

AUDITORIA Y SEGURIDAD EN EL DESARROLLO



El ARTISTA DE SISTEMAS

EL CREADOR, EL JEDI, EL SCRUM MASTER

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

EL CREADOR

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

EL auditor?

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

INICIO DE LA AUDITORIA

MSc Ing. Guido Rosales

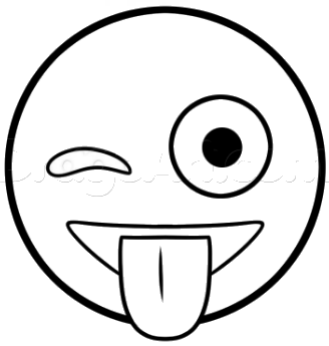
AUDITORIA Y SEGURIDAD EN EL DESARROLLO

PRESENTACION PRELIMINAR DE INFORME

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

PRESENTACION FINAL DE INFORME



MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador

Contenido

1. La Auditoria de Sistemas
2. El Proceso de auditoria
3. Marco de Cumplimiento
4. Herramientas de Auditoria

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

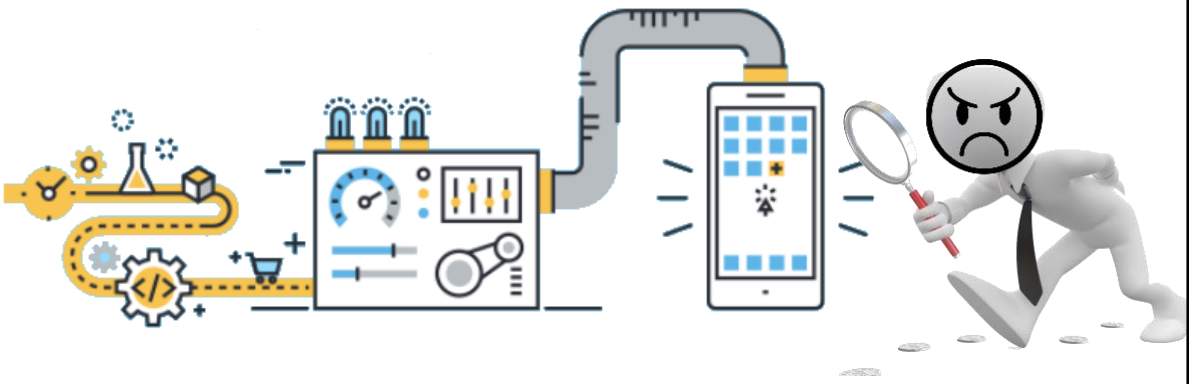
CIDE
Centro de Investigación y Desarrollo Ecuador

2. EL PROCESO DE AUDITORIA

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador



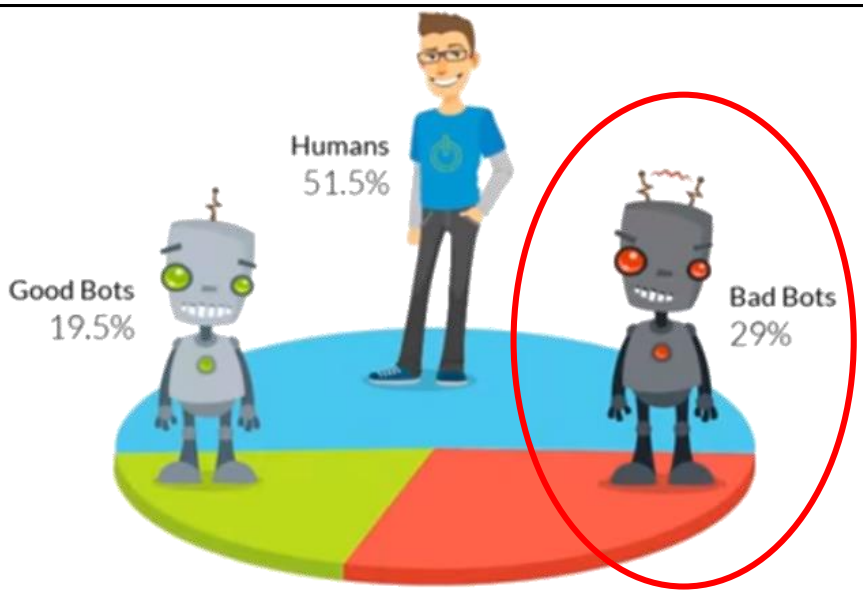
MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador

MSc Ing. Guido Rosales

PRODUCCION



Over **66%** of all bot traffic is malicious.

CIBERCRIMINALES

Good Bots

- Search Engine Crawling
- Website Health Monitoring
- Vulnerability Scanning

Bad Bots

- DDoS
- Site Scraping
- Comment Spam
- SEO Spam
- Fraud
- Vulnerability scanning

MSc Ing. Guido Rosales

BotoPedia
Powered by Incapsula

Directory FAQ About Us Contact Us

BotoPedia

A complete bot identifier

Bot Operator?
Submit your bot to BotoPedia
Add Bot

Botopedia – Bot id checker , User Agent checker

Search by bot name, category, company name or user agent — search

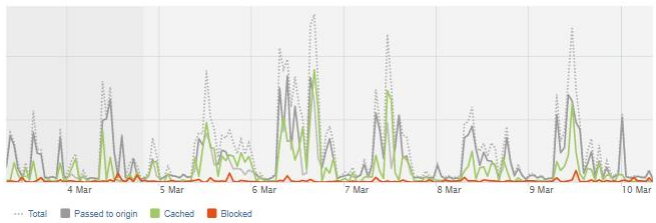
Popular Categories
Search bots
Crawlers
Feed Fetchers
Service Agents
Site Monitors
Social Media Agents
Vulnerability Scaner

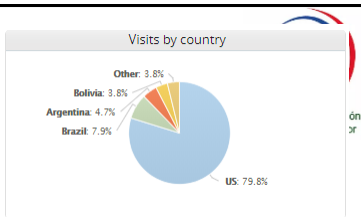
Popular Searches
Search bots

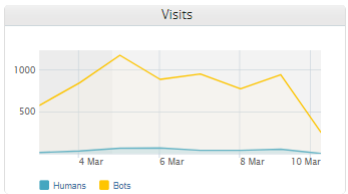
Recently Added
Artmixx Spider Bot
Techmixx Spider Bot
Superfeedr Bot
FeedWordPress Bot

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO





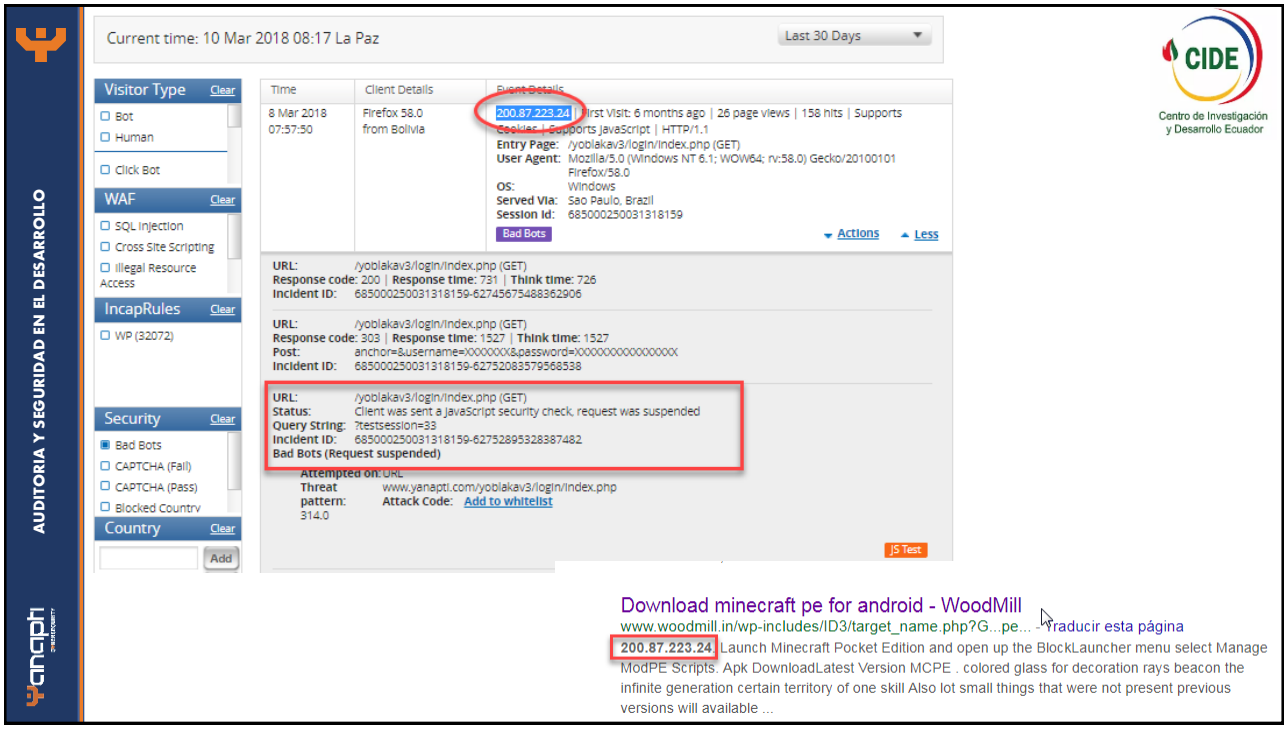


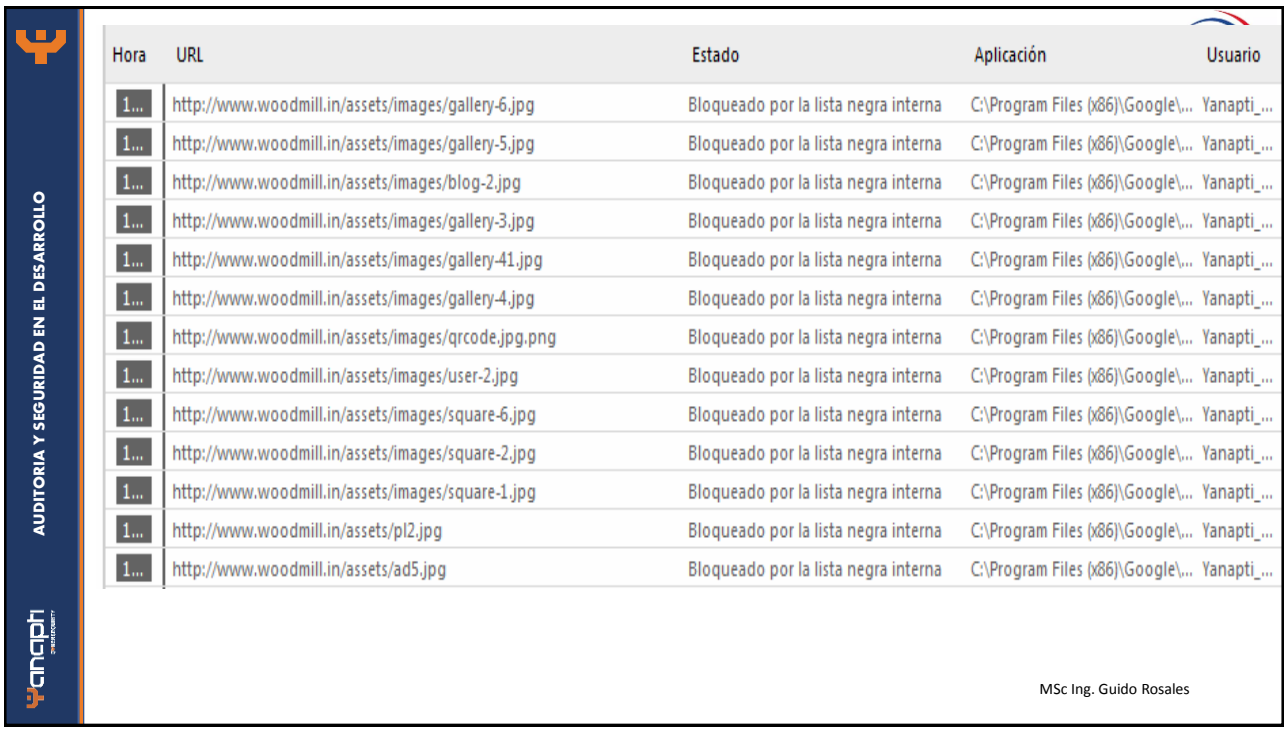
Saturday, March 10, 2018 (La Paz)

Timeline: Last 7 days

Threats

Threat type	Incidents	Current Settings	
Visitors from blacklisted IPs	0	20 IPs in blacklist	View incidents
Visitors from blacklisted Countries	149	26 countries in blacklist	View incidents
Visitors from blacklisted URLs	0	1 URL in blacklist	View incidents
Bot Access Control	180	Block Request	View incidents
Suspected Bots	3 / 11	CAPTCHA Challenge	View incidents
Remote File Inclusion	0	Block Request	View incidents
SQL Injection	0	Block Request	View incidents
Cross Site Scripting	0	Block Request	View incidents
Illegal Resource Access	0	Block Request	View incidents
DDoS	0	Protected	View incidents
Backdoor Protect	0	Protected	View incidents


AUDITORIA Y SEGURIDAD EN EL DESARROLLO
Current time: 10 Mar 2018 08:17 La Paz
Last 30 Days
CIDE
Centro de Investigación y Desarrollo Ecuador
Visitor Type Clear
Bot
Human
Click Bot
WAF Clear
SQL Injection
Cross Site Scripting
Illegal Resource Access
IncapRules Clear
WP (32072)
Security Clear
Bad Bots
CAPTCHA (Fail)
CAPTCHA (Pass)
Blocked Country
Country Clear
Add
Time
Client Details
Event Details
8 Mar 2018 07:57:50
Firefox 58.0 from Bolivia
200.87.223.24 | First Visit: 6 months ago | 26 page views | 158 hits | Supports Cookies | Supports JavaScript | HTTP/1.1
Entry Page: /yoblakav3/login/index.php (GET)
User Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:58.0) Gecko/20100101 Firefox/58.0
OS: Windows
Served Via: Sao Paulo, Brazil
Session Id: 685000250031318159
Bad Bots
Actions
Less
URL: /yoblakav3/login/index.php (GET)
Response code: 200 | Response time: 731 | Think time: 726
Incident ID: 685000250031318159-62745675488362906
URL: /yoblakav3/login/index.php (GET)
Response code: 303 | Response time: 1527 | Think time: 1527
Post: anchor=&username=XXXXXXX&password=XXXXXXXXXXXXXXX
Incident ID: 685000250031318159-62752083579568538
URL: /yoblakav3/login/index.php (GET)
Status: Client was sent a JavaScript security check, request was suspended
Query String: ?testsession=33
Incident ID: 685000250031318159-62752895328387482
Bad Bots (Request suspended)
Attempted on: URL
Threat pattern: 314.0
www.yanapti.com/yoblakav3/login/index.php
Attack Code: Add to whitelist
JS Test
Download minecraft pe for android - WoodMill
www.woodmill.in/wp-includes/ID3/target_name.php?G...pe... - Traducir esta página
200.87.223.24 | Launch Minecraft Pocket Edition and open up the BlockLauncher menu select Manage ModPE Scripts. Apk DownloadLatest Version MCPE . colored glass for decoration rays beacon the infinite generation certain territory of one skill Also lot small things that were not present previous versions will available ...


AUDITORIA Y SEGURIDAD EN EL DESARROLLO
Hora
URL
Estado
Aplicación
Usuario
http://www.woodmill.in/assets/images/gallery-6.jpg
http://www.woodmill.in/assets/images/gallery-5.jpg
http://www.woodmill.in/assets/images/blog-2.jpg
http://www.woodmill.in/assets/images/gallery-3.jpg
http://www.woodmill.in/assets/images/gallery-41.jpg
http://www.woodmill.in/assets/images/gallery-4.jpg
http://www.woodmill.in/assets/images/qrcode.jpg.png
http://www.woodmill.in/assets/images/user-2.jpg
http://www.woodmill.in/assets/images/square-6.jpg
http://www.woodmill.in/assets/images/square-2.jpg
http://www.woodmill.in/assets/images/square-1.jpg
http://www.woodmill.in/assets/pl2.jpg
http://www.woodmill.in/assets/ad5.jpg
Bloqueado por la lista negra interna
C:\Program Files (x86)\Google\...
Yanapti_...
MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

webcache.googleusercontent.com/search?q=cache:1aWylMR08UsJ:www.woodmill.in/+&cd=1

Aplicaciones GesTor F1 timeanddate.com

CIDE
Centro de Investigación y Desarrollo Ecuador

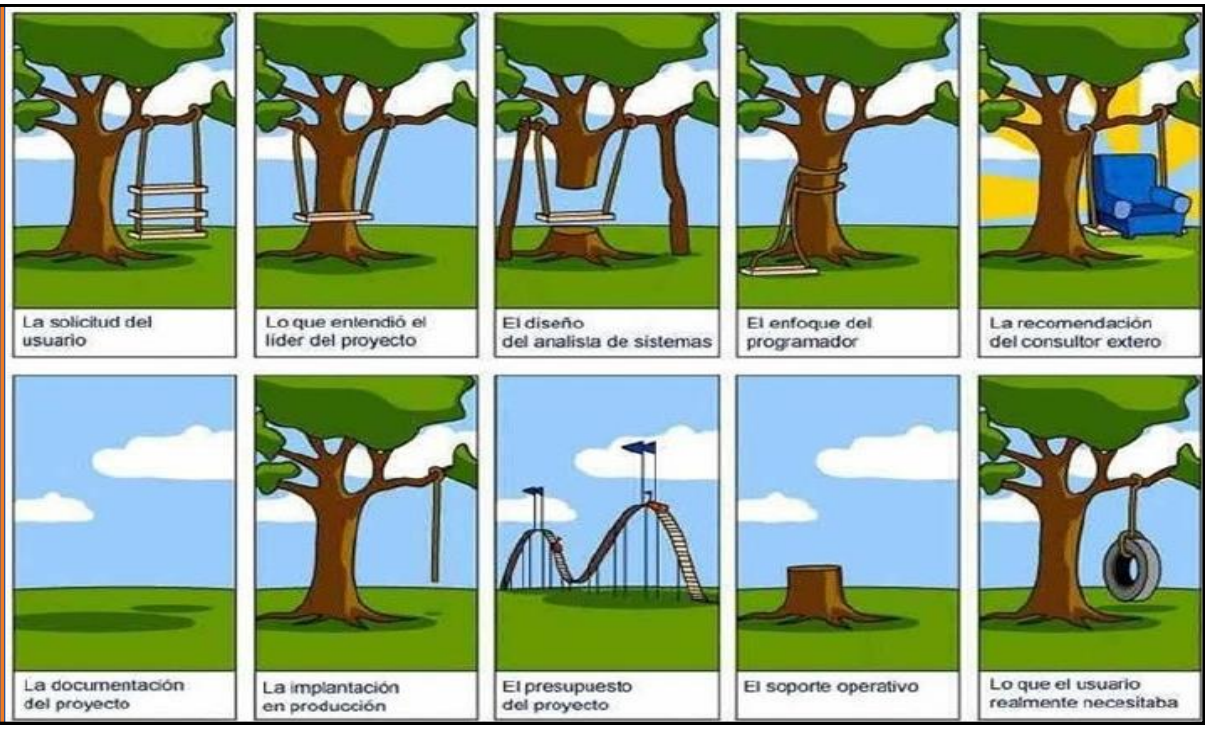
- Home
- About
- Trade
  - Edge band
  - Adhesives
  - Ply Board
- Kitchen components
  - Shutters
  - Sliding
  - Roller Shutters
  - Trap doors
  - Hardware
- Trunkey Sol's
  - Residencies
  - Showrooms
  - Offices
  - Hotels
- Brands
- Contact

WOODMILL™ PRIVATE LIMITED

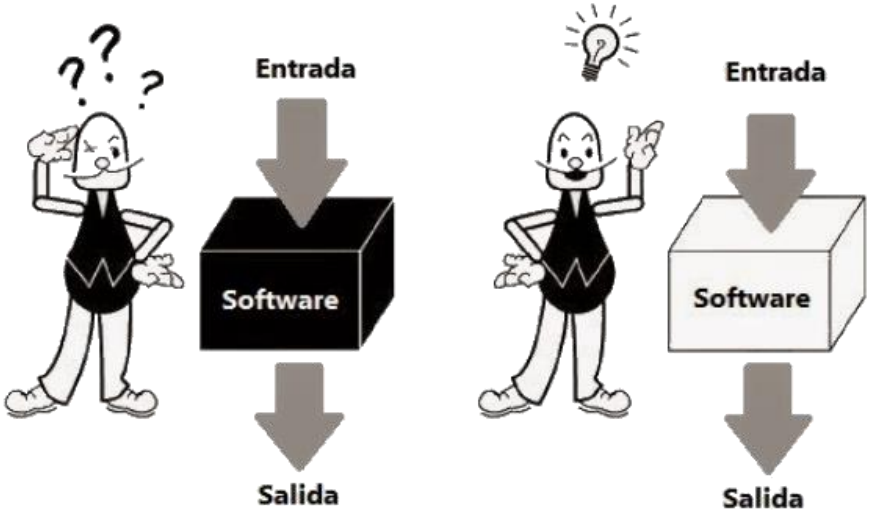
MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

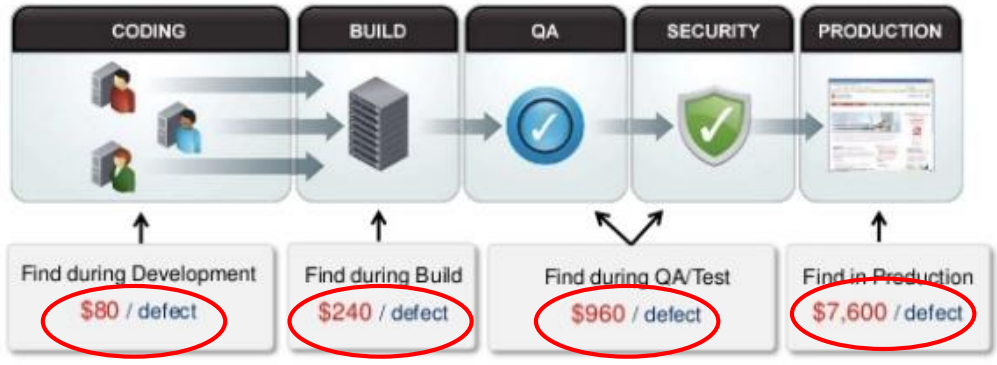
MSc Ing. Guido Rosales



CIDE
Centro de Investigación y Desarrollo Ecuador



MSc Ing. Guido Rosales



80% of development costs are spent identifying and correcting defects!

Source: National Institute of Standards and Technology

- Cost of a Data Breach $7.2M
- 80 days to detect
- More than four months (123 days) to resolve

Source: Ponemon Institute

Contenido

1. El Auditor de Sistemas
2. El Proceso de auditoria
3. **Marco de Cumplimiento**
4. **Herramientas de Auditoria**

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador

3. MARCO DE CUMPLIMIENTO

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

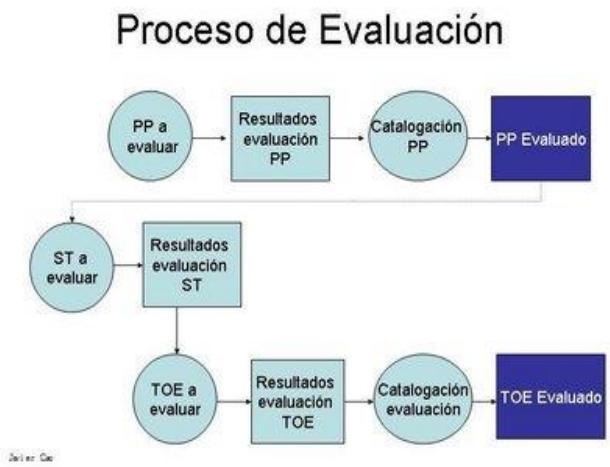
CIDE
Centro de Investigación y Desarrollo Ecuador

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

ISO 15408 - CC

- FAU- Auditoria
- FCO- Comunicaciones
- FCS- Soporte criptográfico
- FDP- Protección de datos de usuario
- FIA- Identificación y autenticación de usuario
- FMT- Gestión de la seguridad
- FPR- Privacidad
- FPT- Protección de las funciones de seguridad
- FRU- Utilización de recursos
- FTA- Acceso al objetivo de evaluación
  FTP- Canales seguros



MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

OWASP

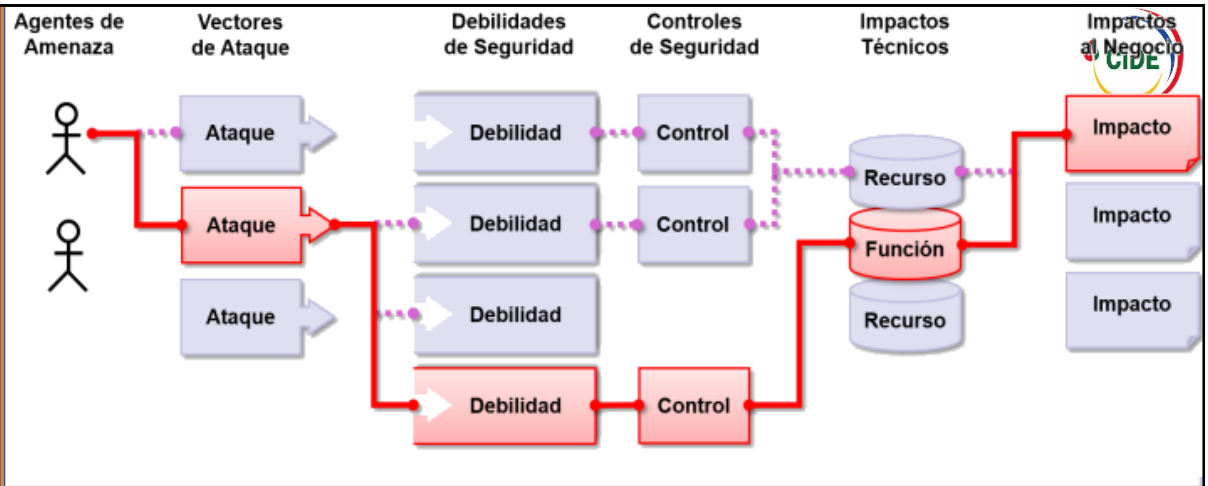
OWASP Top 10 - 2017

Los diez riesgos más críticos en Aplicaciones Web

Centro de Investigación y Desarrollo Ecuador

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO



Agente de Amenaza	Explotabilidad	Prevalencia de Vulnerabilidad	Detección de Vulnerabilidad	Impacto Técnico	Impacto de Negocio
Específico de la Aplicación	Fácil 3	Difundido 3	Fácil 3	Severo 3	Específico del Negocio
	Promedio 2	Común 2	Promedio 2	Moderado 2	
	Difícil 1	Poco Común 1	Difícil 1	Mínimo 1	

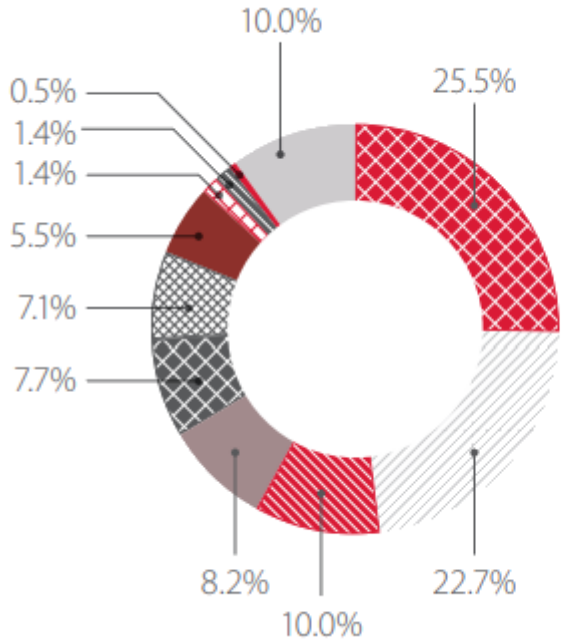
MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

OWASP Top 10 2013	±	OWASP Top 10 2017
A1 – Inyección	→	A1:2017 – Inyección
A2 – Pérdida de Autenticación y Gestión de Sesiones	→	A2:2017 – Pérdida de Autenticación y Gestión de Sesiones
A3 – Secuencia de Comandos en Sitios Cruzados (XSS)	↘	A3:2017 – Exposición de Datos Sensibles
A4 – Referencia Directa Insegura a Objetos [Unido+A7]	∪	A4:2017 – Entidad Externa de XML (XXE) [NUEVO]
A5 – Configuración de Seguridad Incorrecta	↘	A5:2017 – Pérdida de Control de Acceso [Unido]
A6 – Exposición de Datos Sensibles	↗	A6:2017 – Configuración de Seguridad Incorrecta
A7 – Ausencia de Control de Acceso a las Funciones [Unido+A4]	∪	A7:2017 – Secuencia de Comandos en Sitios Cruzados (XSS)
A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF)	☒	A8:2017 – Deserialización Insegura [NUEVO, Comunidad]
A9 – Uso de Componentes con Vulnerabilidades Conocidas	→	A9:2017 – Uso de Componentes con Vulnerabilidades Conocidas
A10 – Redirecciones y reenvíos no validados	☒	A10:2017 – Registro y Monitoreo Insuficientes [NUEVO, Comunidad]

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO



- SQL Injection
- Cross-Site Scripting
- Local File Inclusion
- OS Commanding
- Path Traversal
- Information Leakage
- Cross-Site Request Forgery
- HTTP Verb Tampering
- Predictable Session ID Format
- CSS Injection
- Other

CIDE
Centro de Investigación y Desarrollo Ecuador

MSc Ing. Guido Rosales

AUDITORIA Y SE

A1:2017 Inyección	Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.
A2:2017 Pérdida de Autenticación	Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).
A3:201 Exposición de datos sensibles	Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.
A4:2017 Entidades Externas XML (XXE)	Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).
A5:2017 Pérdida de Control de Acceso	Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc.

CIDE
Centro de Investigación y Desarrollo Ecuador

A1:2017 Inyección	Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.
A2:2017 Pérdida de Autenticación	Las funciones de la aplicación relacionadas a autenticación y gestión de sesiones son implementadas incorrectamente, permitiendo a los atacantes comprometer usuarios y contraseñas, token de sesiones, o explotar otras fallas de implementación para asumir la identidad de otros usuarios (temporal o permanentemente).
A3:201 Exposición de datos sensibles	Muchas aplicaciones web y APIs no protegen adecuadamente datos sensibles, tales como información financiera, de salud o Información Personalmente Identificable (PII). Los atacantes pueden robar o modificar estos datos protegidos inadecuadamente para llevar a cabo fraudes con tarjetas de crédito, robos de identidad u otros delitos. Los datos sensibles requieren métodos de protección adicionales, como el cifrado en almacenamiento y tránsito.
A4:2017 Entidades Externas XML (XXE)	Muchos procesadores XML antiguos o mal configurados evalúan referencias a entidades externas en documentos XML. Las entidades externas pueden utilizarse para revelar archivos internos mediante la URI o archivos internos en servidores no actualizados, escanear puertos de la LAN, ejecutar código de forma remota y realizar ataques de denegación de servicio (DoS).
A5:2017 Pérdida de Control de Acceso	Las restricciones sobre lo que los usuarios autenticados pueden hacer no se aplican correctamente. Los atacantes pueden explotar estos defectos para acceder, de forma no autorizada, a funcionalidades y/o datos, cuentas de otros usuarios, ver archivos sensibles, modificar datos, cambiar derechos de acceso y permisos, etc.

SEGURIDAD EN EL DESARROLLO

A1:2017 Inyección

Las fallas de inyección, como SQL, NoSQL, OS o LDAP ocurren cuando se envían datos no confiables a un intérprete, como parte de un comando o consulta. Los datos dañinos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin la debida autorización.

CIDE
Centro de Investigación y Desarrollo Ecuador

Agente	Vector de Ataque	Debilidades de Seguridad		Impacto	
App. Específica	Explotabilidad: 3	Prevalencia: 2	Detectabilidad: 3	Técnico: 3	¿Negocio?
Casi cualquier fuente de datos puede ser un vector de inyección: variables de entorno, parámetros, servicios web externos e internos, y todo tipo de usuarios. Los defectos de inyección ocurren cuando un atacante puede enviar información dañina a un intérprete.		Estos defectos son muy comunes, particularmente en código heredado. Las vulnerabilidades de inyección se encuentran a menudo en consultas SQL, NoSQL, LDAP, XPath, comandos del SO, analizadores XML, encabezados SMTP, lenguajes de expresión, parámetros y consultas ORM. Los errores de inyección son fáciles de descubrir al examinar el código y los escáneres y *fuzzers* ayudan a encontrarlos.		Una inyección puede causar divulgación, pérdida o corrupción de información, pérdida de auditabilidad, o denegación de acceso. El impacto al negocio depende de las necesidades de la aplicación y de los datos.	

¿La aplicación es vulnerable?

Una aplicación es vulnerable a ataques de este tipo cuando:

- Los datos suministrados por el usuario no son validados, filtrados o sanitizados por la aplicación.
- Se invocan consultas dinámicas o no parametrizadas, sin codificar los parámetros de forma acorde al contexto.
- Se utilizan datos dañinos dentro de los parámetros de búsqueda en consultas *Object-Relational Mapping (ORM)*, para extraer registros adicionales sensibles.
- Los datos dañinos se usan directamente o se concatenan, de modo que el SQL o comando resultante contiene datos y estructuras con consultas dinámicas, comandos o procedimientos almacenados.

Algunas de las inyecciones más comunes son SQL, NoSQL, comandos de SO, *Object-Relational Mapping (ORM)*, LDAP, expresiones de lenguaje u *Object Graph Navigation Library (OGNL)*. El concepto es idéntico entre todos los intérpretes. La revisión del código fuente es el mejor método para detectar si las aplicaciones son vulnerables a inyecciones, seguido de cerca por pruebas automatizadas de todos los parámetros, encabezados, URL, *cookies*, JSON, SOAP y entradas de datos XML.

Las organizaciones pueden incluir herramientas de análisis estático (SAST) y pruebas dinámicas (DAST) para identificar errores de inyecciones recientemente introducidas y antes del despliegue de la aplicación en producción.

Cómo se previene

Para prevenir inyecciones, se requiere separar los datos de los comandos y las consultas.

- La opción preferida es utilizar una API segura, que evite el uso de un intérprete por completo y proporcione una interfaz parametrizada. Se debe migrar y utilizar una herramientas de Mapeo Relacional de Objetos (ORMs).
  Nota: Incluso cuando se parametrizan, los procedimientos almacenados pueden introducir una inyección SQL si el procedimiento PL/SQL o T-SQL concatena consultas y datos, o se ejecutan parámetros utilizando *EXECUTE IMMEDIATE* o *exec()*.
- Realice validaciones de entradas de datos en el servidor, utilizando "listas blancas". De todos modos, esto no es una defensa completa ya que muchas aplicaciones requieren el uso de caracteres especiales, como en campos de texto, APIs o aplicaciones móviles.
- Para cualquier consulta dinámica residual, escape caracteres especiales utilizando la sintaxis de caracteres específica para el intérprete que se trate.
  Nota: La estructura de SQL como nombres de tabla, nombres de columna, etc. no se pueden escapar y, por lo tanto, los nombres de estructura suministrados por el usuario son peligrosos. Este es un problema común en el software de redacción de informes.
- Utilice LIMIT y otros controles SQL dentro de las consultas para evitar la fuga masiva de registros en caso de inyección SQL.

Ejemplos de escenarios de ataque

Escenario #1: la aplicación utiliza datos no confiables en la construcción del siguiente comando SQL vulnerable:

```
String query = "SELECT * FROM accounts WHERE custID='" +
request.getParameter("id") + "'";
```

Escenario #2: la confianza total de una aplicación en su *framework* puede resultar en consultas que aún son vulnerables a inyección, por ejemplo, *Hibernate Query Language (HQL)*:

```
Query HQLQuery = session.createQuery("FROM accounts WHERE
custID='" + request.getParameter("id") + "'");
```

En ambos casos, al atacante puede modificar el parámetro *'id'* en su navegador para enviar: `' or '1'='1`. Por ejemplo:

```
http://example.com/app/accountView?id=' or '1'='1
```

Esto cambia el significado de ambas consultas, devolviendo todos los registros de la tabla *"accounts"*. Ataques más peligrosos podrían modificar los datos o incluso invocar procedimientos almacenados.

Referencias

OWASP

- OWASP Proactive Controls: Parameterize Queries
- OWASP ASVS: V5 Input Validation and Encoding
- OWASP Testing Guide: SQL Injection, Command Injection, ORM injection
- OWASP Cheat Sheet: Injection Prevention
- OWASP Cheat Sheet: SQL Injection Prevention
- OWASP Cheat Sheet: Injection Prevention in Java
- OWASP Cheat Sheet: Query Parameterization
- OWASP Automated Threats to Web Applications – OAT-014

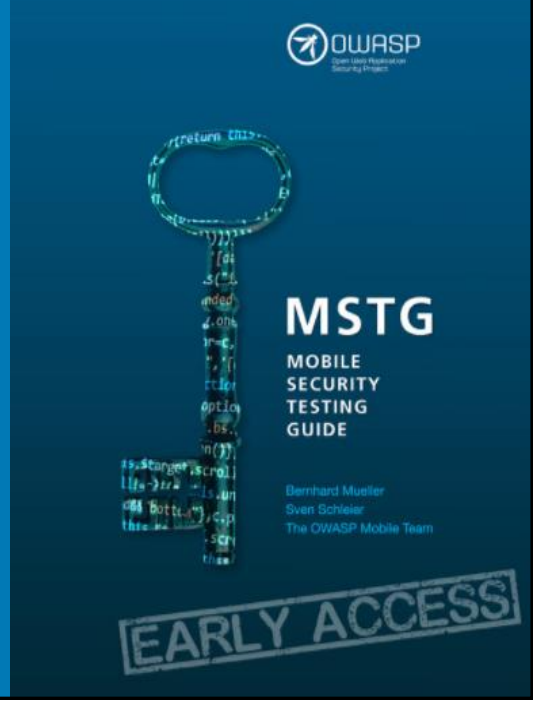
Externos

- CWE-77: Command Injection
- CWE-89: SQL Injection
- CWE-564: Hibernate Injection
- CWE-917: Expression Language Injection
- PortSwigger: Server-side template injection

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

OWASP Open Web Application Security Project | Standard 0.9 pre-release

Mobile AppSec Verification



AUDITORIA Y SEGURIDAD EN EL DESARROLLO

M1 - Improper Platform Usage

M2 - Insecure Data Storage

M3 - Insecure Communication

M4 - Insecure Authentication

M5 - Insufficient Cryptography

M6 - Insecure Authorization

M7 - Client Code Quality

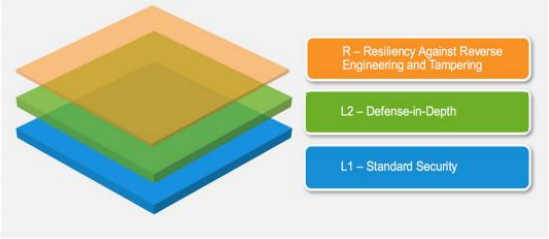
M8 - Code Tampering

M9 - Reverse Engineering

M10 - Extraneous Functionality

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO



#	Description	L1	L2
1.1	All app components are identified and known to be needed.	✓	✓
1.2	Security controls are never enforced only on the client side, but on the respective remote endpoints.	✓	✓
1.3	A high-level architecture for the mobile app and all connected remote services has been defined and security has been addressed in that architecture.	✓	✓
1.4	Data considered sensitive in the context of the mobile app is clearly identified.	✓	✓
1.5	All app components are defined in terms of the business functions and/or security functions they provide.		✓
1.6	A threat model for the mobile app and the associated remote services has been produced that identifies potential threats and countermeasures.		✓
1.7	All security controls have a centralized implementation.		✓
1.8	There is an explicit policy for how cryptographic keys (if any) are managed, and the lifecycle of cryptographic keys is enforced. Ideally, follow a key management standard such as NIST SP 800-57.		✓
1.9	A mechanism for enforcing updates of the mobile app exists.		✓
1.10	Security is addressed within all parts of the software development lifecycle.		✓

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

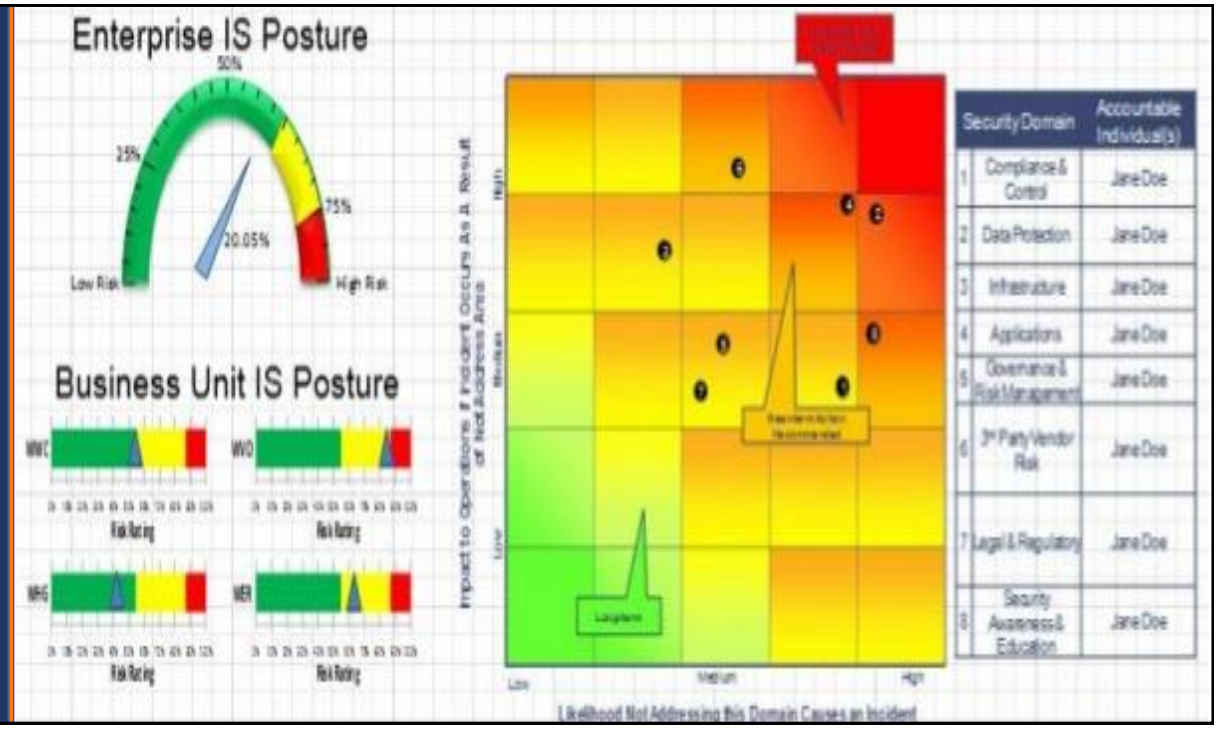
VULNERABILIDADES - Se tienen 34 Vulnerabilidades Analizadas		
Severidad	Debilidad	%
Alta	File unsafe Delete Check	55
Alta	SSL Implementation Check - SSL Certificate Verification	55
Alta	Certificate Pinning	27
Alta	Using activities/improper export of android application activities	9
Alta	Fragment Vulnerability Check	9
Media	Usage of Adb Backup	91
Media	Usage of Native codes	82
Media	Outputting Logs to logCat/ Logging Sensitive information	82
Media	SQLite Journal Information Disclosure Vulnerability	36
Media	WebView addJavascriptInterface Remote Code Execution	18
Media	Usage of Root/Superuser Permission	9
Baja	Usage of Installer verification code	91
Baja	Executing "root" or System Privilege Check	91
Baja	Emulator Detection Check	73
Baja	Unencrypted Credentials in Databases (sqlite db) Vulnerability check	18
Baja	Access Mock Location	9

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

VULNERABILIDADES - Se tienen 34 Vulnerabilidades Analizadas		
Severidad	Debilidad	%
Alta	File unsafe Delete Check	55
Alta	SSL Implemer ion	55
Alta	Certificate Pi	27
Alta	Using activiti n activities	9
Alta	Fragment V	9
Media	Usage of Ad	91
Media	Usage of N	82
Media	Output	82
Media	SQLit	36
Media	Web	18
Media	Usa	9
Baja	Usa	91
Baja	Exe	91
Baja	Emulator Det	73
Baja	Unencrypted Credentials in Databases (sqlite db) Vulnerability check	18
Baja	Access Mock Location	9

MSc Ing. Guido Rosales

MSc Ing. Guido Rosales



AUDITORIA Y SEGURIDAD EN EL DESARROLLO

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador

Contenido

1. El Auditor de Sistemas
2. El Proceso de auditoria
3. Marco de Cumplimiento
4. **Herramientas de Auditoria**

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador

HERRAMIENTAS DE AUDITORIA

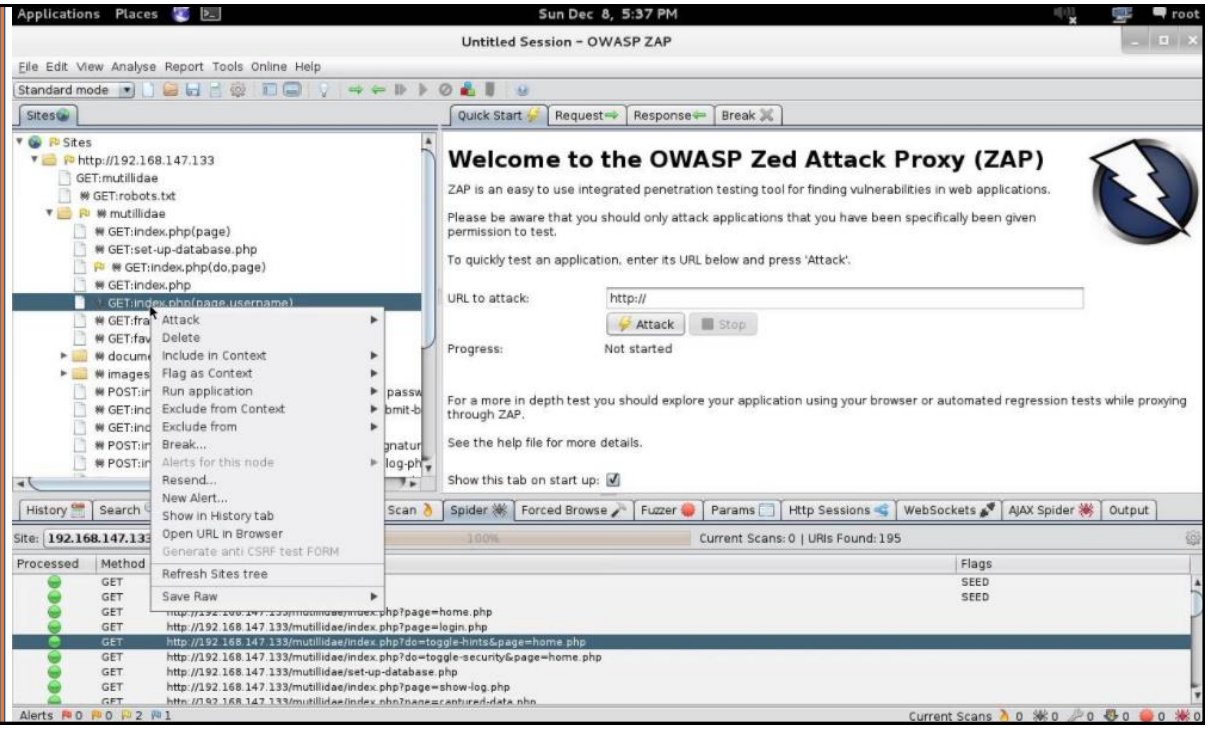
MSc Ing. Guido Rosales

CIDE
Centro de Investigación y Desarrollo Ecuador

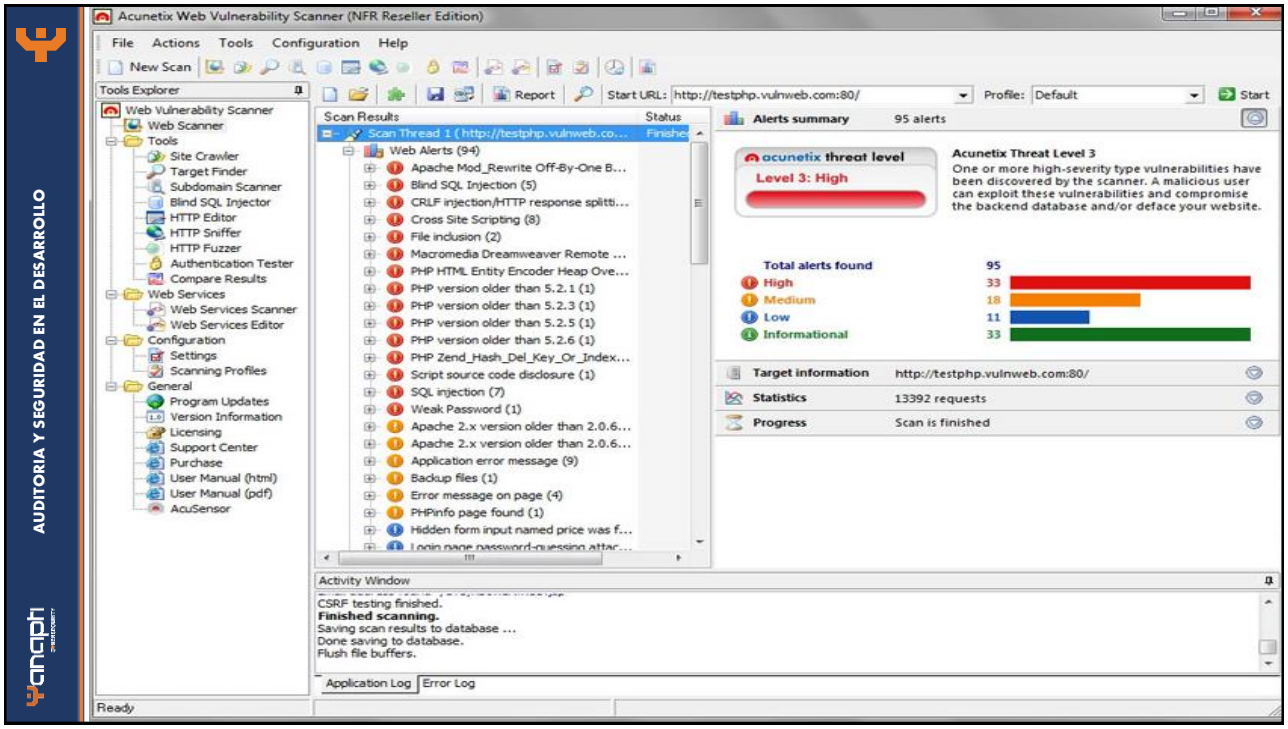
Firmado digitalmente por Guido Rosales
Fecha: 2018.03.10 06:54:06 -04'00'

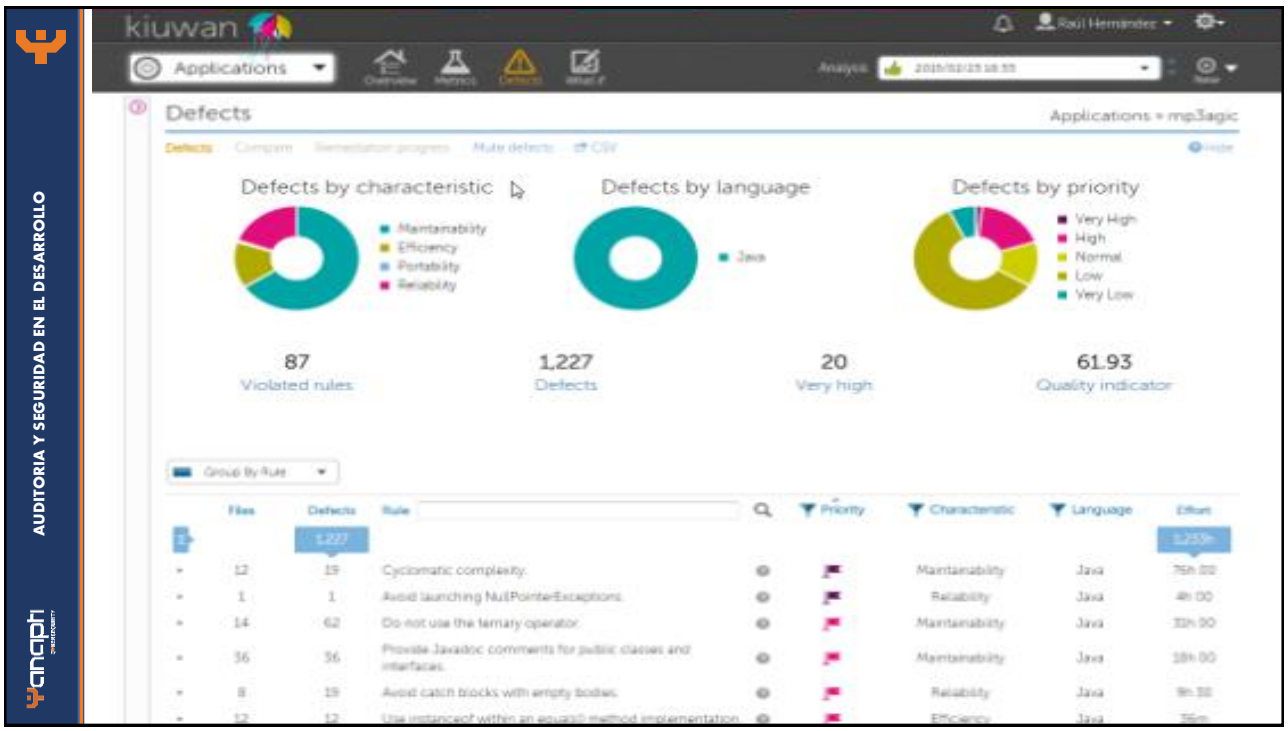
MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO



AUDITORIA Y SEGURIDAD EN EL DESARROLLO

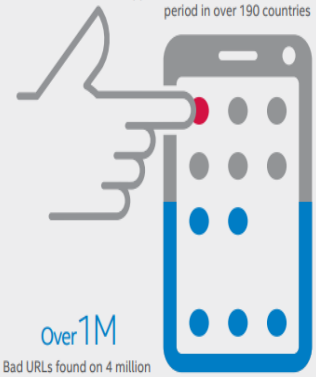

Acunetix Web Vulnerability Scanner (NFR Reseller Edition)
File Actions Tools Configuration Help
New Scan
Tools Explorer
Web Vulnerability Scanner
Web Scanner
Tools
Site Crawler
Target Finder
Subdomain Scanner
Blind SQL Injector
HTTP Editor
HTTP Sniffer
HTTP Fuzzer
Authentication Tester
Compare Results
Web Services
Web Services Scanner
Web Services Editor
Configuration
Settings
Scanning Profiles
General
Program Updates
Version Information
Licensing
Support Center
Purchase
User Manual (html)
User Manual (pdf)
AcuSensor
Report
Start URL: http://testphp.vulnweb.com:80/
Profile: Default
Start
Scan Results
Status
Scan Thread 1 (http://testphp.vulnweb.co...
Finished
Web Alerts (94)
Apache Mod_Rewrite Off-By-One B...
Blind SQL Injection (5)
CRLF injection/HTTP response splitti...
Cross Site Scripting (8)
File inclusion (2)
Macromedia Dreamweaver Remote ...
PHP HTML Entity Encoder Heap Ove...
PHP version older than 5.2.1 (1)
PHP version older than 5.2.3 (1)
PHP version older than 5.2.5 (1)
PHP version older than 5.2.6 (1)
PHP Zend_Hash_Del_Key_Or_Index...
Script source code disclosure (1)
SQL injection (7)
Weak Password (1)
Apache 2.x version older than 2.0.6...
Apache 2.x version older than 2.0.6...
Application error message (9)
Backup files (1)
Error message on page (4)
PHPinfo page found (1)
Hidden form input named price was f...
Alerts summary
95 alerts
acunetix threat level
Level 3: High
Acunetix Threat Level 3
One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.
Total alerts found 95
High 33
Medium 18
Low 11
Informational 33
Target information http://testphp.vulnweb.com:80/
Statistics 13392 requests
Progress Scan is finished
Activity Window
CSRF testing finished.
Finished scanning.
Saving scan results to database ...
Done saving to database.
Flush file buffers.
Application Log
Error Log
Ready


kiuwan
Applications
Raul Hernandez
Defects
Applications » mp3agic
Defects by characteristic
Maintainability
Efficiency
Portability
Reliability
Defects by language
Java
Defects by priority
Very High
High
Normal
Low
Very Low
87
Violated rules
1,227
Defects
20
Very high
61.93
Quality indicator
Group By Rule
Files
Defects
Rule
Priority
Characteristic
Language
Effort
Cyclomatic complexity
Avoid launching NullPointerExceptions
Do not use the ternary operator
Provide Javadoc comments for public classes and interfaces
Avoid catch blocks with empty bodies
Use instanceof within an equals() method implementation

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

Inside McAfee Labs: The Magic Numbers Behind the App Stores

150M
Apps scanned on client in last three month period in over 190 countries



9M Malwares

9M Suspicious apps

3M Devices were affected over 6 months

1M Apps with bad trust score

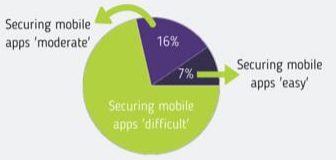
Over 1M Bad URLs found on 4 million devices over 6 months

37M Total count of malware detected over 6 months

Source: McAfee Labs 2016

CIDE
Centro de Investigación y Desarrollo Ecuador

Mobile App Insecurity



77% say securing mobile apps is a difficult task

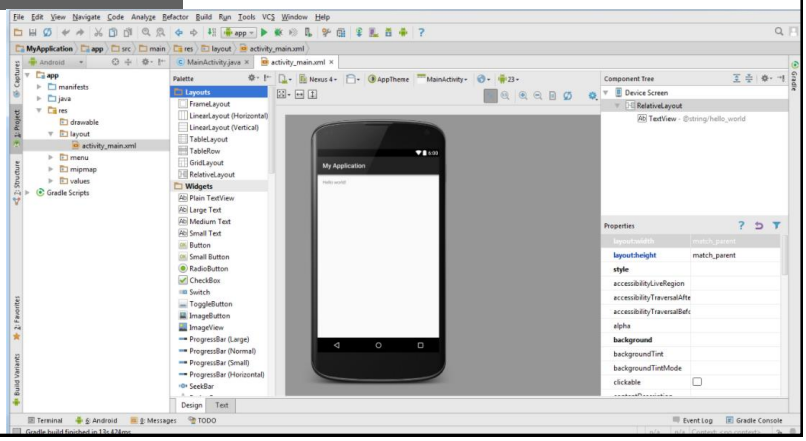
50% of organizations do not allocate budget to mobile security testing

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL

CIDE
Centro de Investigación y Desarrollo Ecuador

Android Studio



AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador

CONCLUSIONES

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO


CIBERCRIMINALES
6".0"
5".0"
4".0"
3".0
Hacker_
Black Hats_
Hacktivistas_
Script Kiddies_


COMO NOS VEN LOS USUARIOS
COMO VEMOS A LOS USUARIOS
UGH!
OOGA!
UG UG!!

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

AUDITORIA Y SEGURIDAD EN EL DESARROLLO

CIDE
Centro de Investigación y Desarrollo Ecuador

DISFRUTEN Y APROVECHEN EL EVENTO!!

MSc Ing. Guido Rosales

AUDITORIA Y SEGURIDAD EN EL DESARROLLO