





# Diego Ademir Duarte Santana

- Ingeniero de sistemas :: Especialista en Seguridad Informática
- CISO de la Universidad Pontificia Bolivariana Bucaramanga
- Consultor y Docente
- Fundador de SeguTIC :: Soluciones
- He apoyado a OWASP desde el año 2014 cuando fundé el capítulo OWASP-ORIENTE en COLOMBIA
- Distinción WASPY (Web Application Security Person Of the Year) en 2015 en la categoría de Innovation/Sharing para la región Latinoamérica
- ...y amante de la CIBERSEGURIDAD !!!

@dadhimir | [linkedin.com/in/diego-ademir-duarte-santana-8093a71b](https://www.linkedin.com/in/diego-ademir-duarte-santana-8093a71b)

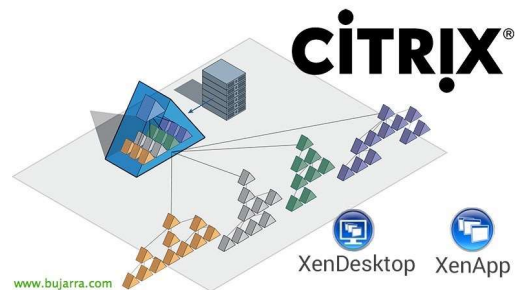


- Open Web Application Security Project.
- <https://owasp.org/>
- Organización internacional sin ánimo de lucro.
- Independiente de Gobiernos.
- Patrocinada por miembros y empresas de manera voluntaria.
- Investigación continua en seguridad informática.

# Algunos tipos de aplicaciones



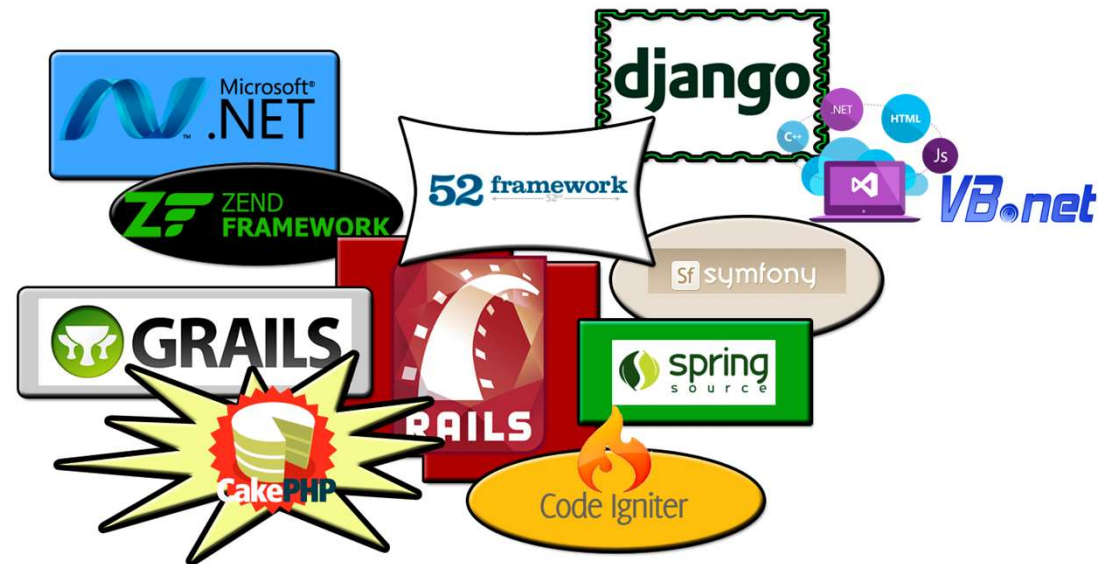
- Toda empresa cuenta con sistemas de información que apoyan los procesos misionales.



# Desarrollos de software propios



- En algunos casos, los desarrollos de software *in-site* son requeridos por que no existe en el mercado una solución focalizada o por “ un tema de costos”.

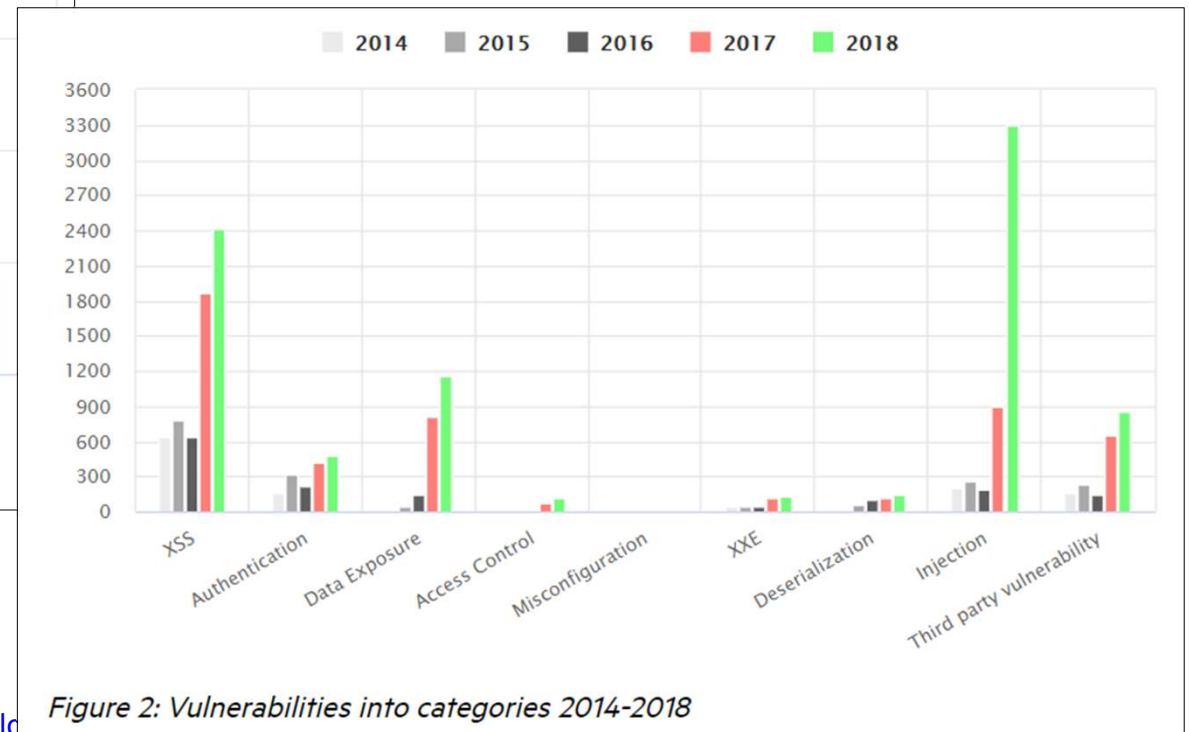
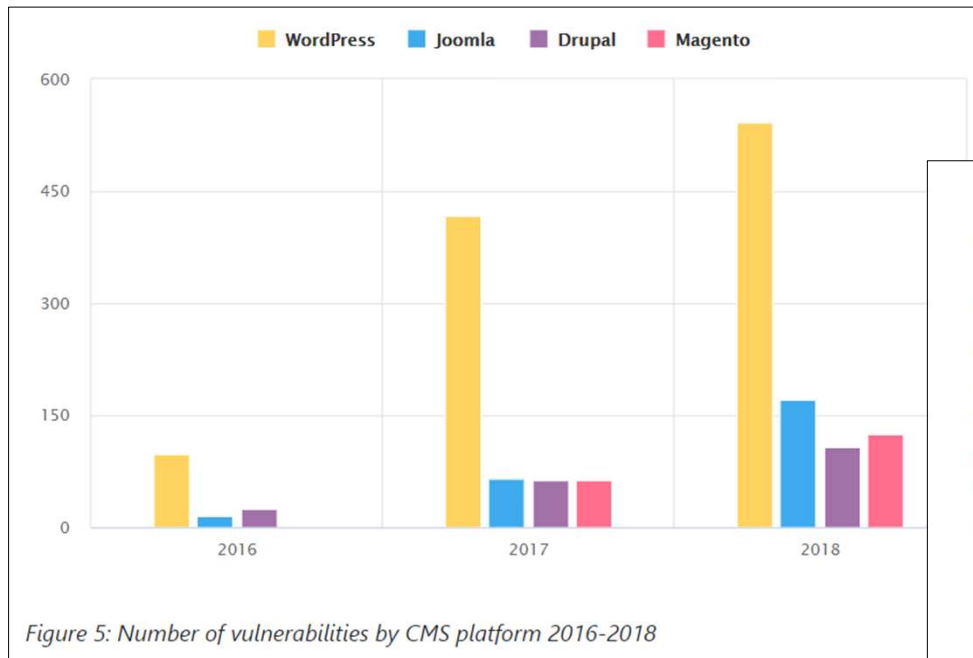


¿y los **RIESGOS**?



shutterstock.com • 708057346

## ¿y los RIESGOS?



- Tomado de <https://www.imperva.com/blog>

## ¿y los **RIESGOS**?



- De igual forma, *frameworks* de desarrollo pueden ser vulnerados.

### Vulnerabilidad crítica en Spring Framework

Posted: 11 Apr 2018 04:30 AM PDT

El pasado 5 de abril se publicaron tres actualizaciones para Spring. De las tres vulnerabilidades, una de ellas es crítica (CVE-2018-1270) y permite Ejecución Remota de Código (RCE) y permitía a los atacantes ejecutar código arbitrario contra las aplicaciones en las que se ha utilizado el mencionado framework para su construcción. Spring es un framework Open Source para el desarrollo de aplicaciones Java, aunque tiene extensiones para la creación de aplicaciones web sobre la plataforma Java...

Contenido completo del post en <http://blog.segu-info.com.ar> o haciendo clic en el título de la noticia



# ¿y los **RIESGOS**?



- Las aplicaciones móviles pueden incluir servicios web...

```
Applications ▾ Places ▾ Terminal ▾ Wed 16:14 ●
root@sara: ~/Downloads/app-release

File Edit View Search Terminal Help
smali/com/google/firebase/database/ServerValue.smali:.class public Lcom/google/firebase/database/ServerValue;
smali/com/google/firebase/database/ServerValue.smali: sput-object v0, Lcom/google/firebase/database/ServerValue;-->TIMESTAMP
smali/com/google/firebase/database/ServerValue.smali:.class public final Lcom/google/firebase/database/ServerValue;
;
smali/com/google/firebase/database/license/R.smali:.class public final Lcom/google/firebase/database/license/R;
smali/com/google/firebase/provider/FirebaseInitProvider.smali:.method public query(Landroid/net/Uri;[Ljava/lang/String;Ljava/lang/String;Ljava/lang/String;)Landroid/database/Cursor;
smali/com/google/firebase/FirebaseOptions.smali: const-string v3, "firebase_database_url"
smali/com/google/firebase/FirebaseOptions.smali: const-string v1, "databaseUrl"
root@sara:~/Downloads/app-release#
root@sara:~/Downloads/app-release# grep -R "php"
original/META-INF/CERT.SF:SHA1-Digest: fLwy3SRI+KvXlPpPhiI9meUzVE8=
Binary file res/mipmap-xxxhdpi/ic_ubicacion.png matches
smali/co/javiermantilla/alejandriaupb/ws/ConsultarWsLibros.smali: const-string v2, "/rest/info.php?uid="
smali/co/javiermantilla/alejandriaupb/ws/ConsultarWsEjemplares.smali: const-string v2, "/rest/ficha.php?uid="
smali/com/google/android/gms/internal/zzcq.smali: const-string v2, "t500bAg0Kquyn7gSVCa5Q5vWaHPXH2npVF5sNuWAC6EtmHNA2fho8fbf
A/7uCoFQc745oA9reYR5AHs474cUNaLWZ5YH04LQ8vcljB0u5gSu+WEsVhYMG0W6wxUSj1XRnqUjuiXS0YPFPcy2/yJPZ2w2SemxxRKwowAmvQcmRurtMlg3+ipwzV
+UFN4u4L+jLMB5ACKvSVeVG6/vd1Wj11k37aF0awntB6928v0egIiTZR50U6fQWMPkv25RKQH7ThUh+v6MoWK9hyDLEIAJD0xjMtXjNzevVMWgX2e0J9QmUhKeK3S
SNDLQWMyahLUE08oQ9VeJ2Mef32EQiaweTEM3QRhxuvTwsUDzrxNN9w5Q4BQHn8Jv1GlnHMV9V2Qswa6/razPDtpE6sZAYp/mV4M5weZbvjgIp3zZD/l27FJzQGc
wCn7Y5A50AswsBEZLFEU5+vCquu1CxR6ndcp4RYyPSALU4r0kdXHYx5B8PgP+PRJ/yidr3jTt2ptK/1RivflxEEmVoSB960NstjjzIls0DA2iDiD/bFVrpPALcuoAL
VzIIXlDRJqn1JR4VxxsazwhxWUIrHEUz0Lxc4hJTftTkXarZUbYk4RxH+tFwXyNcMRZBI2Z7P1XRskkAVabv1NnAW5J/Ku6mRvpp2feWm59l1bdsz6j7os2yX3aj7
p0MCuVQ16EgKaxvaB7pLQ69S3CGyByY3woBhVigiELMBE5KaoLbmrDyyol7jacjyt4B5J9gEMQ99X5S15xzuNLUdqArIerwXUD00Fkle7gaUFSwb06k4SrbVobkFEf
W09mTdlvgLuihfvtS62I2+n5tEGNusHq0TibYEVVzHqbyzHqS+6Zo6S5i7Aqtk7IIMbBLN8f5Vfz80zTEMN7hlfJ1clF3w+GdB1NhCvt2bCa/85AKBARD7lBpBmnNH
```

## ¿y los **RIESGOS**?



- ...y podrían revelar algún tipo de información importante:

```
1  .class public final Lco/javiermantilla/alejandriaupb/BuildConfig;
2  .super Ljava/lang/Object;
3  .source "BuildConfig.java"
4
5
6  # static fields
7  .field public static final APPLICATION_ID:Ljava/lang/String; = "co.javiermantilla.alejandriaupb"
8
9  .field public static final BUILD_TYPE:Ljava/lang/String; = "release"
10
11 .field public static final DEBUG:Z = false
12
13 .field public static final FLAVOR:Ljava/lang/String; = ""
14
15 .field public static final VERSION_CODE:I = 0x1
16
17 .field public static final VERSION_NAME:Ljava/lang/String; = "1.0.1"
18
19
```

## ¿y los **RIESGOS**?



- Falta de gestión de cambio en código fuente.
- Ausencia de ambientes de pre-producción.
- No hay cultura en seguridad informática para *DEVELOPERS*.
- El *PENTESTING* se realiza por el mismo programador.

# La materialización del **RIESGO**



- Caso: *webshell*.

Browser address bar: [\[redacted\]hell/dondon.php](#)

```
Uname: [redacted] #142-Ubuntu SMP Tue Apr 28 10:12:19 UTC 2015 x86_64
User: 33 ( www-data ) Group: 33 ( www-data )
Php: 5.3.2-1ubuntu4.30 Safe mode: OFF [ phpinfo ] Datetime: 2018-04-10 15:27:41
Hdd: 49.21 GB Free: 333.88 MB (0%)
Cwd: [redacted]hell/ drwxr-xr-x [ home ]
```

File manager

Name	Size	Modify
[ .. ]	dir	2018-03-14 12:36:12
dadhemirshell.bak	52.38 KB	2012-04-25 10:41:36
dadhemirshell.php	52.38 KB	2017-06-02 14:10:43
dk.php	61.40 KB	2016-02-05 11:06:12
dondon.php	49.13 KB	2015-04-15 09:11:44
file.php	61.40 KB	2014-04-03 17:01:28
indexbak.html	53 B	2012-03-29 17:26:55
indexhack.htm	742 B	2011-04-06 13:59:24
injected.php	44 B	2016-02-16 15:47:55
shell.php	1.44 KB	2017-06-02 13:54:30

Copy [v] >>

Change dir: [redacted] >>

Make dir: (Not writable) >>

Execute: >>

# La materialización del **RIESGO**



- Caso: Plataformas de desarrollo desactualizadas y/o con problemas en configuración.

Asunto: [PL-532078] Phishing redirect(s) hosted on industrial.upbbga.edu.co

Hello,

My name is Charles McLemore and I work for PhishLabs. We investigate computer crime incidents on behalf of other organizations.

During an investigation of fraud, we have identified phishing redirect content which is hosted on your network and attempting to defraud the customers of **Apple ID**.

The following URL(s) are the redirect file(s) which are part of this phishing campaign:

**hXXp://industrial.upbbga.edu.co/images/up.php**

First detection of malicious activity: 05-07-2017 20:02:23 UTC Most recent observation of malicious activity: 05-09-2017 08:21:11 UTC Associated IP Address: 207.248.81.6 Hostname of Server: upbbga.edu.co

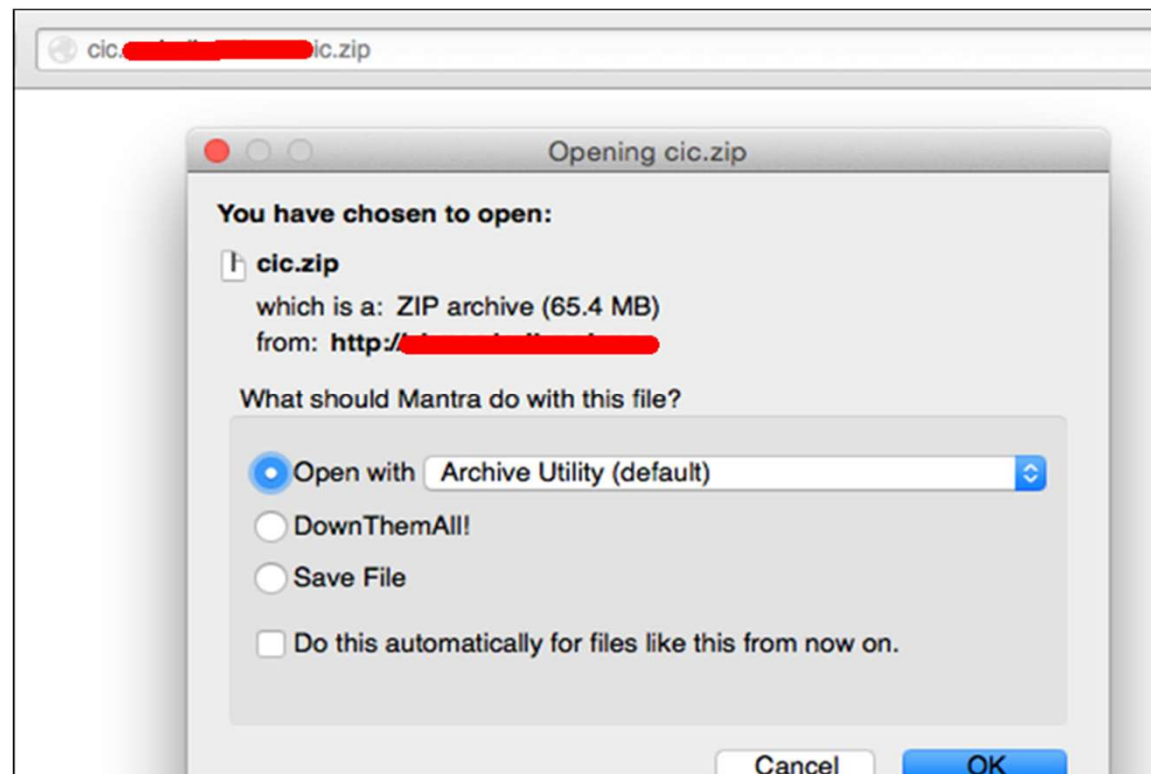
If you agree that this is malicious, we kindly request that you take steps to have the content removed as soon as possible. It is likely that the intruder who set up this phishing site has also left additional fraudulent material on this server.

If we have contacted you in error, or if there is a better way for us to report this incident, please let us know so that we may continue our investigation.

# La materialización del **RIESGO**



- Caso: *backups* de código fuente en el mismo servidor de aplicaciones.





Mitigación de Riesgos

# **CONTROLES :: PROYECTO ASVS**

## **APPlication SECURITY VERIFICATION STANDARD**



## Proyectos de OWASP (Madurez)





# ASVS :: un proyecto actualizado!



- Clasificación y gestión de cambio

Tools [Health Check January 2017] [editar]

- OWASP Zed Attack Proxy 🍏
- OWASP Web Testing Environment Project 🍏
- OWASP OWTF 🍏
- OWASP Dependency Check 🍏
- OWASP Security Shepherd 🍏

Code [Health Check January 2017] [editar]

- OWASP ModSecurity Core Rule Set Project 🍏
- OWASP CSRFGuard Project 🍏
- OWASP AppSensor Project 🍏

Documentation [Health Check January 2017] [editar código]

- OWASP Application Security Verification Standard Project 🍏
- OWASP Software Assurance Maturity Model (SAMM) 🍏
- OWASP AppSensor Project 🍏
- OWASP Top Ten Project 🍏
- OWASP Testing Project 🍏

OWASP PROJECTS CHAPTERS EVENTS AB

## OWASP Application Security Verification Standard

Main [News and Events](#) Acknowledgements Glossary ASVS Users

owasp flagship project Stars ASVS 848 Follow 603

### News and Events

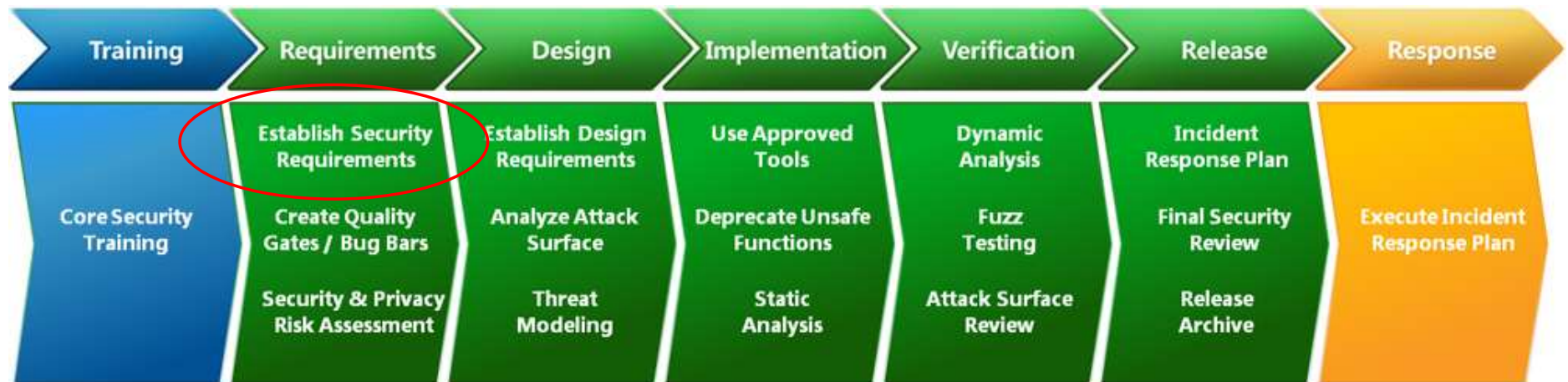
- [2 March 2019] [ASVS 4.0.1](#) released!
- [9 March 2018] [OWASP ASVS 3.1 Spreadsheet](#) created by August Detlefsen
- [29 June 2016] Version 3.0.1 released
- [16 Oct 2015] Version 2.0 released

## ASVS :: Objetivo



- The Application Security Verification Standard is a list of application security requirements or tests that can be used by architects, developers, testers, security professionals, tool vendors, and consumers to define, build, test and verify secure applications.

# ASVS :: Alineado con los modelos de desarrollo de software



- Tomado de <https://social.technet.microsoft.com/wiki/contents/articles/7100.the-security-development-lifecycle.aspx>

# ASVS :: Niveles



	Applicability	Building			Building, Configuration, Deployment Assurance and Verification			Assurance and Verification	
Level 1	All apps		Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Penetration Testing	DAST
Level 2	All apps	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
Level 3	High Assurance	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
	Legend	Acceptable	Suitable						

ASVS Level 1 is for low assurance levels, and is completely penetration testable

ASVS Level 2 is for applications that contain sensitive data, which requires protection and is the recommended level for most apps

ASVS Level 3 is for the most critical applications - applications that perform high value transactions, contain sensitive medical data, or any application that requires the highest level of trust.

## ASVS :: Nivel 1 :: Lo Básico

- Contiene 136 controles
- Mejor que OWASP TOP 10
- Aseguramiento mínimo aceptable
- INSUFICIENTE para construir una aplicación segura



## ASVS :: Nivel 2 :: El Recomendado

- Contiene 267 controles
- Algunos controles se aplican UNA SOLA VEZ
  - Promover un SDLC seguro
  - Utilizar controles de revisión de código fuente
  - Usa un *defect tracker*
- Incluye SDLC y Arquitectura



## **ASVS :: Nivel 3 :: Aplicaciones que pueden matarte o afectar la economía**



- Contiene 286 controles
- Aplicables para:
  - Aplicaciones médicas y dispositivos
  - Vehículos automatizados
  - Tecnología operacional: energía, agua, plantas químicas, nucleares, etc.
  - Software de control
  - Aplicaciones financieras
- Nivel de aseguramiento ALTO
- Nivel de paranoia ALTO

# ASVS :: Grupos de requerimientos



**V1: Architecture, Design and Threat Modeling Requirements**

**V2: Authentication Verification Requirements**

**V3: Session Management Verification Requirements**



# ASVS :: Grupos de requerimientos



V4: Access Control Verification Requirements

V5: Validation, Sanitization and Encoding Verification Requirements.

V6: Stored Cryptography Verification Requirements

# ASVS :: Grupos de requerimientos



**V7: Error Handling and Logging Verification Requirements.**

**V8: Data Protection Verification Requirements**

**V9: Communications Verification Requirements**

# ASVS :: Grupos de requerimientos



**V10: Malicious Code Verification Requirements**

**V11: Business Logic Verification Requirements.**

**V12: File and Resources Verification Requirements**

# ASVS :: Grupos de requerimientos



**V13: API and Web Service Verification Requirements**

**V14: Configuration Verification Requirements**

# ASVS :: Ejemplos de aplicación



🔒 No es seguro | [redacted]maescolar.com.co



# COLEGIO MIL

Aprobado por MINE

Usuario:

Contraseña:

**2.2.1** Verify that anti-automation controls are effective at mitigating breached credential testing, brute force, and account lockout attacks. Such controls include blocking the most common breached passwords, soft lockouts, rate limiting, CAPTCHA, ever increasing delays between attempts, IP address restrictions, or risk-based restrictions such as location, first login on a device, recent attempts to unlock the account, or similar. Verify that no more than 100 failed attempts per hour is possible on a single account.

✓ ✓ ✓ 307

# ASVS :: Ejemplos de aplicación



```
Origin: http://[redacted]
Connection: close
Referer: http://[redacted]login.aspx
Cookie:
ext-gxui20-RegistroFactura-Grid1=ot3Awidth%3Dn%253A795%5Ecolumns%3Dn%25253Agxui20-RegistroFactura-Grid1-col-TRANUNITARIO%25255Ewidth%25253Dn%2525253A69%255Eot%25253Aid%25253Ds%2525253Agxui20-RegistroFactura-id1-col-VALORIVA%25255Ewidth%25253Dn%2525253A68%255Eot%25253Aid%25253DsASP.NET_SessionId=sicfis35b3ocd4053qilqcyw

vUSUARIOUSUARIO=[redacted]&vUSUARIOCONTRASENIA=124578&BUTTON1=Iniciar%22%3A%22%22%2C%22vIP%22%3A%22%22%2C%22vPUERTO%22%3A%220%22%2C%22vIP%22%2C%22GX_AJAX_KEY%22%3A%228C6F51263DEC54CB032CC18B83D0ECF3%22%2C%22X_CMP_OBJS%22%3A%227B%22%2C%22sCallerURL%22%3A%22%22%2C%22GX_RES_PROVIDE%22%3A%22%22%2C%22IsModified%22%3A%221%22%2C%22SCAMESSAGE1_Width%22%3A%22MESSAGE1_Animationtype%22%3A%22fade%22%2C%22SCAMESSAGE1_Delayuntilclose%22%3A%22TopRight%22%2C%22SCAMESSAGE1_Niftyanimationtype%22%3A%22Niftymessage%22%3A%22%22%2C%22SCAMESSAGE1_Niftybuttontext%22%3A%22buttoncolor%22%3A%2210823707%22%2C%22SCAMESSAGE1_Niftybuttononhovercolor%22%3A%22Verdana%22%20Arial%22%2C%22SCAMESSAGE1_Message1_Dialogdefaultmessagetitle%22%3A%22Me
```

3.3.2	If authenticators permit users to remain logged in, verify that re-authentication occurs periodically both when actively used or after an idle period. (C6)	30 days	12 hours or 30 minutes of inactivity, 2FA optional	12 hours or 15 minutes of inactivity, with 2FA	613
-------	---	---------	--	--	-----


# ASVS :: Ejemplos de aplicación








## Out-of-date Version (jQuery UI Dialog)

Certainty :   
URL : [http://\[redacted\]shared/jqueryui/jquery-ui-1.9.1.js](http://[redacted]shared/jqueryui/jquery-ui-1.9.1.js)  
Identified Version : 1.9.1  
Latest Version : 1.12.1 (in this branch)  
Vulnerability Database : Result is based on 10/21/2019 08:00:00 vulnerability database content.

## Out-of-date Version (Highcharts)

Certainty :   
URL : [http://\[redacted\]erres.aspx](http://[redacted]erres.aspx)  
Identified Version : 2.1.6  
Latest Version : 7.2.0 (in this branch)  
Vulnerability Database : Result is based on 10/21/2019 content.

**3.4.2** Verify that cookie-based session tokens have the 'HttpOnly' attribute set.    1004  
(C6)

**14.1.3** Verify that server configuration is hardened as per the recommendations of the application server and frameworks in use.   16

**Gracias por su asistencia !**



[slides.app.goo.gl/eNEbe](https://slides.app.goo.gl/eNEbe)

