

Familia de Vulnerabilidades





Testeo de Vulnerabilidades



Índice

- 1. Injection (SQL, NoSQL, LDAP, OS, etc)
- 2. Broken Authentication (auth, session mgmt, etc)
- 3. Sensitive Data Exposure (financiera, credit cards, passwords, etc)
- 4. XML External Entities (XXE Parsers viejos!)

- 5. Broken Access Control
- 6. Security Misconfiguration
- 7. Cross Site Scripting (XSS JS, browser API/HTML, etc)
- 8. Insecure Deserialization

- 9. Using Components
 With Known
 Vulnerabilities (:P)
- 10. Insufficient Logging & Monitoring

Testeo de Caja Blanca / Caja Negra

1

La caja blanca son pruebas estructurales, conociendo el código y siguiendo su estructura lógica, se pueden diseñar pruebas destinadas a comprobar que el código hace correctamente lo que el diseño de bajo nivel indica y otras que demuestren que no se comporta adecuadamente ante determinadas situaciones.

2

En cambio la caja negra conlleva a la verificación de las funcionalidades de la aplicación: Datos que entran, resultados que se obtienen, interacción con los actores, funcionamiento de la interfaz de usuario y en general todo aquello que suponga estudiar el correcto comportamiento que se espera del sistema.

1. Injection (SQL, NoSQL, LDAP, OS, etc)

La finalidad de este ataque es poder modificar del comportamiento de nuestras consultas logrando así falsificar identidades, obtener y divulgar información de la base de datos (contraseñas, correos, información relevante, entre otros), borrar la base de datos, cambiar el nombre a las tablas, anular transacciones, etc.

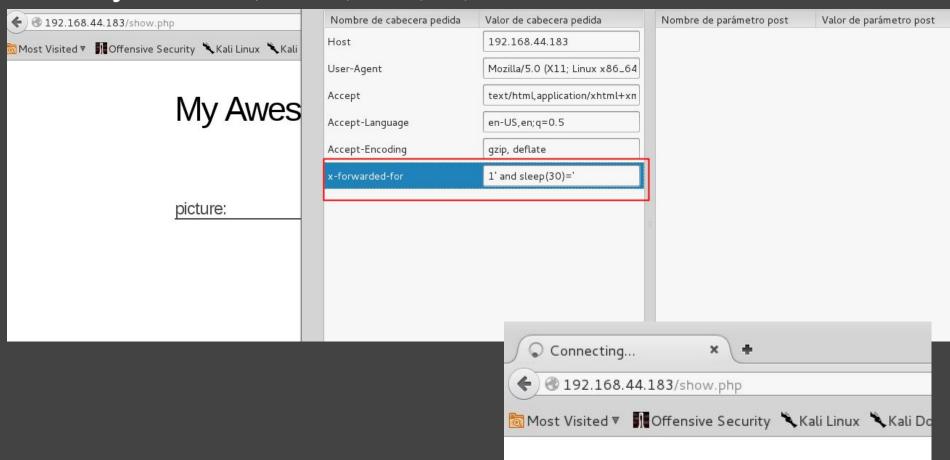
Nivel de Vulnerabilidad: Crítica

1. Injection (SQL, NoSQL, LDAP, OS, etc)

Lesson Instructions EMAIL ADDRESS FINDER: Enter the three digit customer ID to find the customer's email address. Only the first three characters will be recognized. Example: 103 Enter the Customer ID: tt' Find Email! You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near " at line 1

Nivel de Vulnerabilidad: Crítica

1. Injection (SQL, NoSQL, LDAP, OS, etc)



2. Broken Authentication (auth, session mgmt, etc)

Reconocen las acciones que el usuario ha realizado anteriormente, por ejemplo, si se trata de un usuario registrado anteriormente.

Para que la sesión se tenga iniciada el navegador y el servidor de dicho servicio tienen un identificador en cada petición **HTTP** muchas veces mediante las cookies.



2. Broken Authentication (auth, session mgmt, etc)



😤 Elements 🧓 Resources 💿 Network 🧐 Scripts 💇 Timeline 🐚 Profiles 🔍 Audits 🦙 Console <div id="FB_HiddenContainer" style="position:absolute; top:-10000px; width:0px; height:0px;"></di</pre> ▼ <div id="pagelet_bluebar" data-referrer="pagelet_bluebar"> ▼ <div id="blueBarHolder" class="loggedOut"> ▼ <div id="blueBar" class="viewportLeft viewportRight"> v<div class="loggedout_menubar_container"> ▼ <div class="clearfix loggedout_menubar"> ► _ ▼ <div class="rfloat"> ▼ <div class="menu_login_container"> ▼ <form id="login form" action="https://www.facebook.com/login.php?login attempt=1" met Event.__inlineSubmit(this, event)"> <input type="hidden" autocomplete="off" name="post_form_id" value="a349bc2071e6c4f1.</pre> cinput type="hidden" name="lsd" value="mtHkb" autocomplete="off"> <input type="hidden" autocomplete="off" id="locale" name="locale" value="es LA"> ▼

2. Broken Authentication (auth, session mgmt, etc)

```
v 
  <input type="password" class="inputtext" name="pass" id="pass" tabindex="2">
 F < t d>
         type="text" class="inputtext" name="pass" id="pass" tabindex:
  <input
 _
/tr>
```





Dogistrata



Tipos de ataques

Predicción de sesión (Probar mediante fuerza bruta)

Captura del identificador a través de XSS (puede que envíen la cookie a otro lugar)

Interceptando la comunicación

Fijación de sesión (multifactor authentication)

Errores en el cierre de sesión (entrar mediante el historial de navegación a una cuenta)



3. Sensitive Data **Exposure**

- -Datos financieros
- -Credit cards
- -Passwords
- -Registros de salud
- -Los códigos de las bombas nucleares 🙊



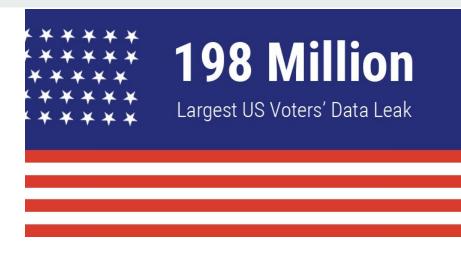
Nivel de Vulnerabilidad: Severo

¿Cuándo sucede esto?

- Los datos son registrados en texto claro en la base de datos o donde se guarden
- Carecen de cifrado
- Están cifrados con algoritmos de encriptación muy antiguos.
- Los datos confidenciales ingresados a través de un formulario son recordados por el navegador (autocompletado)



2015



La base de datos estaba en el servidor de Amazon sin ninguna contraseña

((O:) ▶ dra-dw ▶ dra-dw.s3.amazonaws.com ▶ audiences ▶						K (O:) ▶ dra-dw ▶ dra-dw.s3.amazonaws.com ▶ audiences ▶ exxon_mobile ▶ raw					
n library	Share with ▼ Burn New folder				Share wi	Share with ▼ Burn New folder					
Name	Date modified		fied Type	Name	Name Date m			Туре	Size		
exxon_mobile 6/12/2017 10:18 PM			10:18 PM File folder	(i) audi	ences.yxdb		3/6/2017 1:57 PM	Alteryx Database	11,973,760		
tp_audiences_2017-01-13 6/13/2017 1:04 AM				1:04 AM File folder		onal_exxon_score_fil	le vodh	3/6/2017 2:06 PM	Alteryx Database	25,941,482	
					100		- 56		i.i.		
tp_audiences_2017-01-25 6/13/2017 3:46 AM			3:46 AM File folder		ped_audiences_xon		3/1/2017 1:18 PM	Alteryx Database	20,440 KB		
b tp_audiences_2017-02-02 6/13/2017 5:07 AM			5:07 AM File folder	prep	ped_audiences_xon	n_AL.yxdb	3/1/2017 1:18 PM	Alteryx Database	159,539 KB		
b tp_audiences_2017-02-10 6/13/2017 6:01 AM			6:01 AM File folder	o prep	ped_audiences_xon	n_AR.yxdb	3/1/2017 1:18 PM	Alteryx Database	88,673 KB		
	ields ▼ ✔ Cell Viewer ▼ RNC_RegID	† ↓	FIPS5	CD_NextElection	FirstName	MiddleName	LastName	RegistrationAddr	1 RegCity	RegSta	
1	4519-9E00-AC45AF367C87}	TX	48113	30				, , , , , , , , , , , , , , , , , , , ,	DUNCANVILLE	TX	
2	4EC0-9387-FAD707BF2740}	NC	37127	2	· · · · · · · · · · · · · · · · · · ·				NASHVILLE	NC	
3	417B-AFCB-CC1BEA49D8D5}	SC	45077	3					EASLEY	SC	
4	4870-92C8-700AB66F1D74}	NC	37023	11	·				CONNELLYS SPRINGS		
5	4492-BCDF-5B93F1813066}	PA	42007	12	**********				CONWAY	PA	
6	4030-B1AC-C611A17EACB6}	LA	22109	6			***************************************		HOUMA	LA	
7	4684-A25E-CD67EE63BBDC}	FL	12083	11					OCALA	FL	
8	4FDA-898F-752CC614D27C}	MD	24033	4					CAPITOL HEIGHTS	MD	
9	43D7-A197-C0B89F432A3C}	NV	32031	2					RENO	NV	
10	4F8C-BBE7-3DA5473DB92D}	WA	53017	8			0.000		EAST WENATCHEE	WA	
11	4208-B754-96E90D9EF3F3}	VA	51760	4					RICHMOND	VA	
12	40CB-8B46-556936DEE6C1}	VA	51177	7					SPOTSYLVANIA	VA	
13	44EE-9C00-CD797CB89F47}	IA	19183	2					WASHINGTON	IA.	
2000	4507 0040 40454504603	1011	100005						****		

4. XML External Entities (XXE - Parsers viejos!)

- 1. Denegación de servicio (DDoS)
- 2. Acceso a archivos y servicios locales o remotos

Consiste en una inyección que se aprovecha de la mala configuración del intérprete XML permitiendo incluir entidades externas, este ataque se realiza contra una aplicación que interpreta lenguaje XML en sus parámetros.



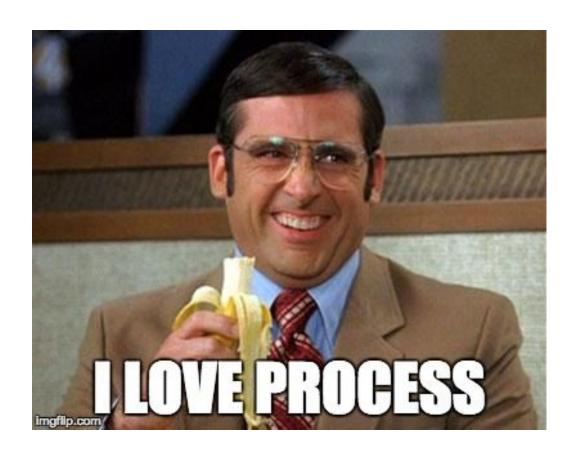
XML-RPC es uno de los protocolos más simples para intercambiar datos de forma segura entre computadoras a través de Internet. Wordpress lo usaba para él y esto sucedió...

Utiliza el método system. **multicall** que permite a una aplicación ejecutar múltiples comandos dentro de una solicitud HTTP.







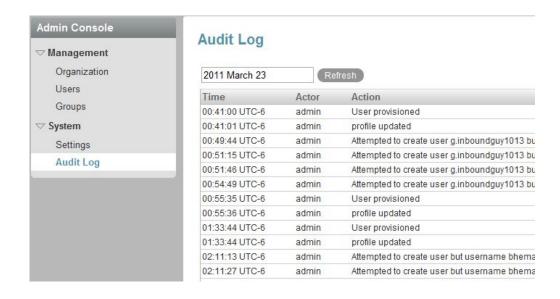


5. Broken Access Control

Los atacantes pueden explotar estos defectos para acceder a funcionalidades y / o datos no autorizados, como acceder a cuentas de otros usuarios, ver archivos confidenciales. modificar datos de otros usuarios, cambiar derechos de acceso, etc.



Ejemplo



6. Security Missconfiguration

Permiten al atacante acceso a áreas restringidas debido a malas prácticas o fallos durante la configuración de la aplicación o de los sistemas asociados.

Por ejemplo: usuarios y contraseñas por defecto, páginas en desuso o de administración accesibles, vulnerabilidades conocidas sin parchear, ficheros y directorios sin proteger, etc



2013: 100,000 tv's, refrigeradores, tablets, routers hackeados

750,000 correos de spam enviados

Escribe aquí tu texto

25%

tenían contraseñas predeterminadas

Escribe aquí tu texto

80%

No tenían seguridad óptima

Escribe aquí tu texto

45%

No tenía contraseña

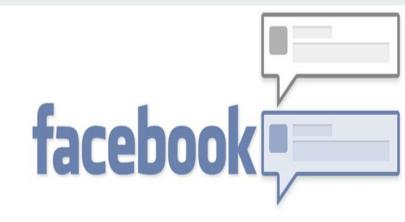
7. Cross Site Scripting (XSS - JS, browser API/HTML, etc)

XSS es un ataque de inyección de código malicioso para su posterior ejecución que puede realizarse a sitios web, aplicaciones locales e incluso al propio navegador.

Sucede cuando un usuario mal intencionado envía código malicioso a la aplicación web y se coloca en forma de un hipervínculo para conducir al usuario a otro sitio web, mensajería instantánea o un correo electrónico.

Ejemplo 2013 ChatBox

La GUI se utiliza para presentar la publicación de enlace usando un parámetro, es decir, [archivo adjunto] [título], archivo adjunto [parámetros] [urlInfo] [final]



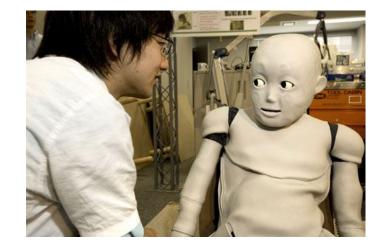


fb dtsg-kGBDMcRxxhpc context-homesxhpc ismeta-14xhpc timeline-sxhpc composerid-u O vaxhpc litestand-14xhpc targetid-1021051560sxhpc message text-http%l4%15 www.breakmec.comixhpc mexmace=http%1A%2Fwww.breakmer.comiaktion=post(app id=11050f0772iattachment[params][uriInfo][canonical]=http%1A%2F%2Fwww.breakmer.com/ If sattachment[params] (urlinfo] (final) =http://breaksec.com/aftachment(params) (urlinfo) (user) =http://breaksec.com/Iffattachment(params) (setaTagMap) [B] [http-equiv] =content-typeiattachment[params] [metaTagMap] [0] [content] =text%lFhtml%lB%lOcharmet%lDutf=Siattachment[params] [metaTagMap] [1] [charmet] =UTF-Siatt achment[params][metaTagMap][2][name]=demoriptionsattachment[params][metaTagMap][2][content]=Breakt20Securityt20specializedt20int20securityt20functionst20and \$2Sapplication\$2Cassessments\$201;ke\$2Openetration\$20testing\$2C\$2Ccode\$2Oreviev\$2C\$2Oclient-side\$2Oand\$2Orobile\$2Openetration\$2Otesting.fattachment(parama)[m etaTagHap [3] [property] =ogN3AlocaleSattachment[params] [metaTagHap] [3] [content] =en USSattachment[params] [metaTagHap] [4] [property] =ogN3AttitleSattachment[params s) [netaTagMap] [4] [content] = Break 10 Security attachment [params] [netaTagMap] [5] [property] = og 1) Adescriptions attachment [params] [netaTagMap] [5] [content] = Break 100 Security%2Ompecialized%2Oin%2Omecurity%2Ofunctions%2Omnd%2Omplication%2Ommensa42Olike%2Openetration%2Otenting%2C%2Ocode%2Oreview%2C%2Oclient-mide%2Om dk10mobilek10penetrationk10testing.sattachment[parame][metaTagMap][6][property]=ogklAurlsattachment[parame][metaTagMap][6][content]=httpklAk1F4lFwww.breakse c.com2f(attachment(parama)(metaTagMap)(7)(property)=og%3anite mame(attachment(parama)(metaTagMap)(7)(content)=Break*105ecurityiattachment(parama)(metaTagMa n) [8] [property] = on litype sattachment[parame] [metaTaqHan] [8] [content] = article sattachment[parame] [metaTaqHan] [9] [name] = generator sattachment[parame] [metaTaqHan] [19][content]=WordPresst200.5.1&attachment[params][metaTagm][description]=Breakt2OSecurityt2Ospecializedt2Oint2Omecurityt2Ofunctionst2Oand ssessments 2011ke 20 menetration 20 testing 10 10 20 de 10 review 20 10 20 de 10 review 20 10 20 de 10 review 20 10 20 de 10 20 d]=WordPress1301.5. idatachwent(params) (og info)[properties][0][0]=og43Alocaledattachwent(params) (og info)[properties][0][1]=en USdattachwent(params) (og info [properties][1][0] *ogt lattice attachment [params][og info][properties][1][1] *Breakt lose unity Lattachment [params][og info][properties][2][0] *ogt lates ription 4attachment[params][og info][properties][2][1]=Breakt30Securityt2Ospecializedt2Oint2Osecurityt2Ofunctionst3Oandt2Oapplicationt2Oassessmentst3Oliket3Openetra tion\20testing\2C\20code\20revie\2C\20client-side\20and\20and\20and\20antiesting.&attachment[params][og info][properties][3][0]-og\3&url&attachment [parame][og info][properties][3][1] *http://latif/parame][og info][properties][4][0] *og.blaite namesattachment[parame][og info]] [properties] [4] [1] = Sreakt20Security interpreted [or info] [properties] [5] [0] = ogt liktype interpreted [or info] [properties] [5] [1] = article interpreted [or info] [properties] [5] [1] = article interpreted [or info] [properties] [5] [1] = article interpreted [or info] [or in [quesees] [of info] [queses] [O] [O] [organisation in the contraction of the contraction 1)[0]=ogt3&titleiattachment(params)(og info)[guennes)[1][1]=Breakt20Securityiattachment(params)(og info)[guennes][2][0]=ogt3&descriptioniattachment(params)[og info] (guesses) [2] [1] *Breakt/20Securityt/20specializedt/20int/20securityt/20functionst/20andt/20applicationt/20assessmentst/20liket/20penetrationt/20testingt/20t/20cod ekIGreviewkICkIGclient-widekIGandkiGnobilekIGpenetrationkIGtenting.iattachment(parame) [og info] [guesses) [3] [8] =ogklkinageiattachment(parame) [og info] [guesse s)[3][1]=http%3AV2F42Fbreaksec.com*1Fvp-content%1Fuploads%1F2013%1F03%2FClient-Side.pnpsattachment[params][og_info][quesses][4][0]=og%1Ainagesattachment[par arm)[og info][quesses][4][1]=http%)A%2F%2Foreaksec.com%2Fup-content%2Fuploads%2F2013%2F0%2FRobile2.jpg4attachment[params][og info][quesses][5][0]=og\$3Aimag etattachment(parame)(og info)(guesses)(5)(1)=http%3ACF%2F203.104.105.145ACF%p-content%2Fuploads%2F2013%2F03%2Fces slider 3 1.jpg4attachment(parame)(og info [guesses][6][0] *ogklkinagetattachment[params][og info][quesses][6][1] *httpAlkAFFAPF301.124.105.14542Fvp-content%Fuploads%FF201342F0342Falide img 3-copy.pn giattachment[parame][og_info][quesses][7][0]=ogt3Aimageiattachment[parame][og_info][quesses][7][1]=httpt5A42F42F203.124.105.14552Fep-content%2Fuploads%2F201 3%2F03%2Fslide img 11.phgsattachment(parame)[og info][queeses][8][0]-og%3%imagesattachment(parame)[og info][queeses][8][1]-http%3%%2F%2F03.124.105.145%2Fwp



9. Using Components With Known Vulnerabilities

Usando componentes o cosas en nuestros programas que sabemos que son o muy vulnerables o ya son muy antiguos.



10. Insufficient Logging & Monitoring

- Las aplicaciones emplean varios componentes y, en general, los registros no se crean o se comparten con otros componentes.
- Difícil de detectar ya que junto con las herramientas automatizadas, el análisis manual es esencial para diversas condiciones de error

Recomendación: LLevar un registro de todo lo que se hace en la app y que es lo que cubrimos y que nos falta.

