



Familia de Vulnerabilidades

Jorge Súchite
315365994





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 el 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)

EMAIL ADDRESS FINDER:

[Lesson Instructions](#)

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:

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)

192.168.44.183/show.php

Most Visited
 Offensive Security
 Kali Linux
 Kali

My Awes

picture:

Nombre de cabecera pedida	Valor de cabecera pedida
Host	192.168.44.183
User-Agent	Mozilla/5.0 (X11; Linux x86_64
Accept	text/html,application/xhtml+xml
Accept-Language	en-US,en;q=0.5
Accept-Encoding	gzip, deflate
x-forwarded-for	1' and sleep(30)='

Nombre de parámetro post	Valor de parámetro post
--------------------------	-------------------------

Connecting...

192.168.44.183/show.php

Most Visited
 Offensive Security
 Kali Linux
 Kali Do



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)

Dirección de correo electrónico

Contraseña

jonathan@teknoplof.com

☐ No cerrar sesión

¿Olvidaste tu contraseña?

Entrar

Regístrate

```

Elements Resources Network Scripts Timeline Profiles Audits Console
<div id="FB_HiddenContainer" style="position:absolute; top:-1000px; width:0px; height:0px;"></div>
▼<div id="pagelet_bluebar" data-referrer="pagelet_bluebar">
  ▼<div id="blueBarHolder" class="loggedOut">
    ▼<div id="blueBar" class="viewportleft viewportRight">
      ▼<div class="loggedout_menubar_container">
        ▼<div class="clearfix loggedout_menubar">
          ▶<a class="lfloat" href="/" title="Ir a la página de inicio de Facebook">_</a>
          ▼<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.
                  <input type="hidden" name="lsd" value="mt/kb" autocomplete="off">
                  <input type="hidden" autocomplete="off" id="locale" name="locale" value="es_LA">
                ▼<table cellpadding="0">

```

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

```
▼ <td>  
  <input type="password" class="inputtext" name="pass" id="pass" tabindex="2">  
  </td>  
  <td>_</td>  
</tr>
```

```
▶ <td>_</td>  
▼ <td>  
  <input type="text" class="inputtext" name="pass" id="pass" tabindex="2">  
  </td>  
▶ <td>_</td>  
</tr>
```



Dirección de correo electrónico

jonathan@teknoplof.com

☐ No cerrar sesión

Contraseña

JonathanTP2874\$\$

[¿Olvidaste tu contraseña?](#)

Entrar

Regístrate

The Netflix logo is shown in its characteristic red, bold, sans-serif font. It is superimposed on a graphic of bright orange and yellow flames rising from the bottom, with thick, dark grey smoke billowing upwards behind the text. The entire scene is set against a light grey background.

NETFLIX



Tipos de ataques

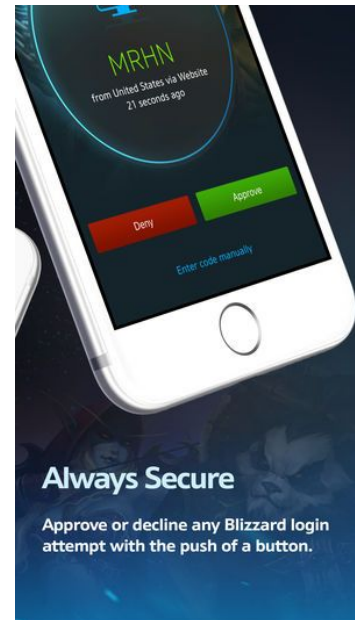
Predicción de sesión (Probar mediante fuerza bruta)

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)



- 



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)



Ejemplo

2015

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



198 Million

Largest US Voters' Data Leak



K (O:) > dra-dw > dra-dw.s3.amazonaws.com > audiences >

Name	Date modified	Type
exon_mobile	6/12/2017 10:18 PM	File folder
tp_audiences_2017-01-13	6/13/2017 1:04 AM	File folder
tp_audiences_2017-01-25	6/13/2017 3:46 AM	File folder
tp_audiences_2017-02-02	6/13/2017 5:07 AM	File folder
tp_audiences_2017-02-10	6/13/2017 6:01 AM	File folder

K (O:) > dra-dw > dra-dw.s3.amazonaws.com > audiences > exon_mobile > raw

Name	Date modified	Type	Size
@ audiences.yxdb	3/6/2017 1:57 PM	Alteryx Database	11,973,760 ...
@ national_exxon_score_file.yxdb	3/6/2017 2:06 PM	Alteryx Database	25,941,482 ...
@ prepped_audiences_xom_AK.yxdb	3/1/2017 1:18 PM	Alteryx Database	20,440 KB
@ prepped_audiences_xom_AL.yxdb	3/1/2017 1:18 PM	Alteryx Database	159,539 KB
@ prepped_audiences_xom_AR.yxdb	3/1/2017 1:18 PM	Alteryx Database	88,673 KB

Alteryx Designer x64 - national_exxon_score_file.yxdb

182,746,897 records displayed, 19 fields, , 25 GB

Record...	RNC_RegID	State	FIP55	CD_NextElection	FirstName	MiddleName	LastName	RegistrationAddr1	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	NC
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					EAST WENATCHEE	WA
11	4208-B754-96E90D9EF3F3}	VA	51760	4					RICHMOND	VA
12	40CB-8B46-556936DEE6C1}	VA	51177	7					SPOTSVYLVANIA	VA
13	44EE-9C00-CD797CB89F47}	IA	19183	2					WASHINGTON	IA

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.

Ejemplo 2015

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.



Ataque de fuerza bruta

Con cuatro solicitudes HTTP podían probar miles y miles de veces las contraseñas eludiendo todos los protocolos de seguridad!!!!





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

Admin Console

Management

Organization

Users

Groups

System

Settings

Audit Log

Audit Log

Refresh

Time	Actor	Action
00:41:00 UTC-6	admin	User provisioned
00:41:01 UTC-6	admin	profile updated
00:49:44 UTC-6	admin	Attempted to create user g.inboundguy1013 bu
00:51:15 UTC-6	admin	Attempted to create user g.inboundguy1013 bu
00:51:46 UTC-6	admin	Attempted to create user g.inboundguy1013 bu
00:54:49 UTC-6	admin	Attempted to create user g.inboundguy1013 bu
00:55:35 UTC-6	admin	User provisioned
00:55:36 UTC-6	admin	profile updated
01:33:44 UTC-6	admin	User provisioned
01:33:44 UTC-6	admin	profile updated
02:11:13 UTC-6	admin	Attempted to create user but username bhema
02:11:27 UTC-6	admin	Attempted to create user but username bhema



6. Security Misconfiguration

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



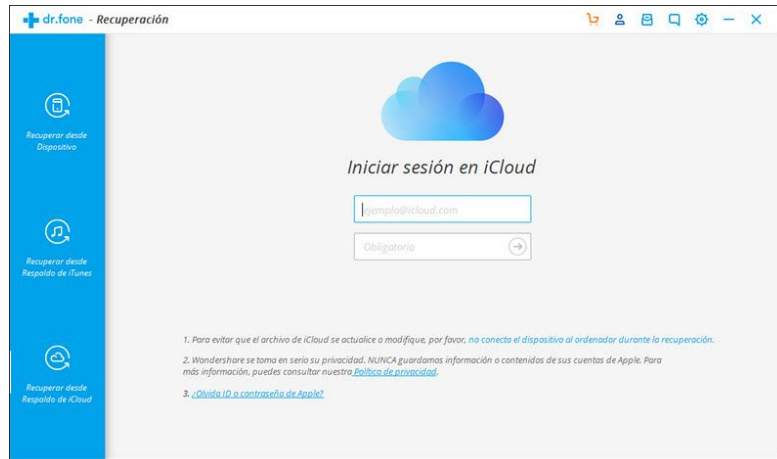
7. Cross Site Scripting (XSS - JS, browser API/HTML, etc)

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]

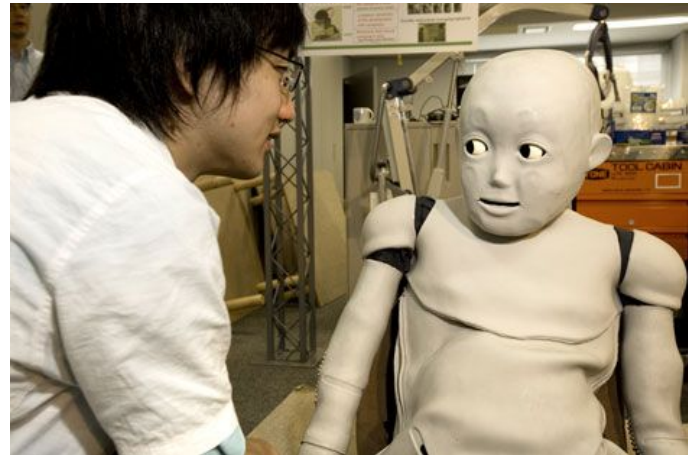






9. Using Components With Known Vulnerabilities

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.



Gracias.

