DEBUGGING
ANDROID APPS

@SixP4ck3r
Richard Villca Apaza

OWASP LATAM TOUR 2015

OWASP
The Open Web Application Security Project

About Me

OWASP
The Open Web Application Security Project

Acerca de mi

- Estudiante de Ing. Sistemas
- Developer Android, WP, Python, C++, WebDeveloper, Node.JS
- Independent Security Researcher
- Software Libre
- Autodidacta Empedernido
- > 8 Hacking World

About Me

OWASP
The Open Web Application Security Project

Agenda

- Client Side
- Debugging
- Debugging in Android
- JDB Console
- Demos
- Mitigación
- Despedida

OWASP
The Open Web Application Security Project

DISCLAIMER

Esta presentación es realizada expresamente con fines educativos, tanto OWASP ni el ponente se hacen responsable por los daños que puedan ocacionar a partir de esta información.

Logica de la Aplicación

Logica de la Aplicación

```
<script language="javascript">
/* used for login in my page */
function pasuser(form) {
    if (form.id.value=="JavaScript") {
        if (form.pass.value=="hidude") {
        location="dashboard.php"
        } else {
        alert("Invalid Password")
        }
    } else {
        alert("Invalid UserID")
    }
}
</script>
```

OWASP
The Open Web Application Security Project

Debugging

- Debugging is a methodical process of finding and reducing the number of bugs, or defects, in a computer program or a piece of electronic hardware, thus making it behave as expected. Debugging tends to be harder when various subsystems are tightly coupled, as changes in one may cause bugs to emerge in another.

OWASP
The Open Web Application Security Project

Analisis y Manipulación (Runtime)

- Monitorear el comportamiento.
- Detectar conexiones a protocolos HTTP.
- Entender la logica de la App
- Modificar la App en tiempo de ejecución.

OWASP
The Open Web Application Security Project

¿Que necesitamos?

- Emulador Android
- Binario APK ha ser analisado
- Algun depurardor compatible con Java
- Manos a la obra

OWASP
The Open Web Application Security Project

JDB

The Java Debugger, jdb, is a simple command-line debugger for Java classes. It is a demonstration of the Java Platform Debugger Architecture that provides inspection and debugging of a local or remote Java Virtual Machine.

OWASP
The Open Web Application Security Project

¿Que puedes hacer con JDB?

- Invocar metodos
- Ver los argumentos de los metodos.
- Cambiar variables locales.
- Ver los valores de las variables.
- Monitorear el flujo de los método de la aplicación.
- ...

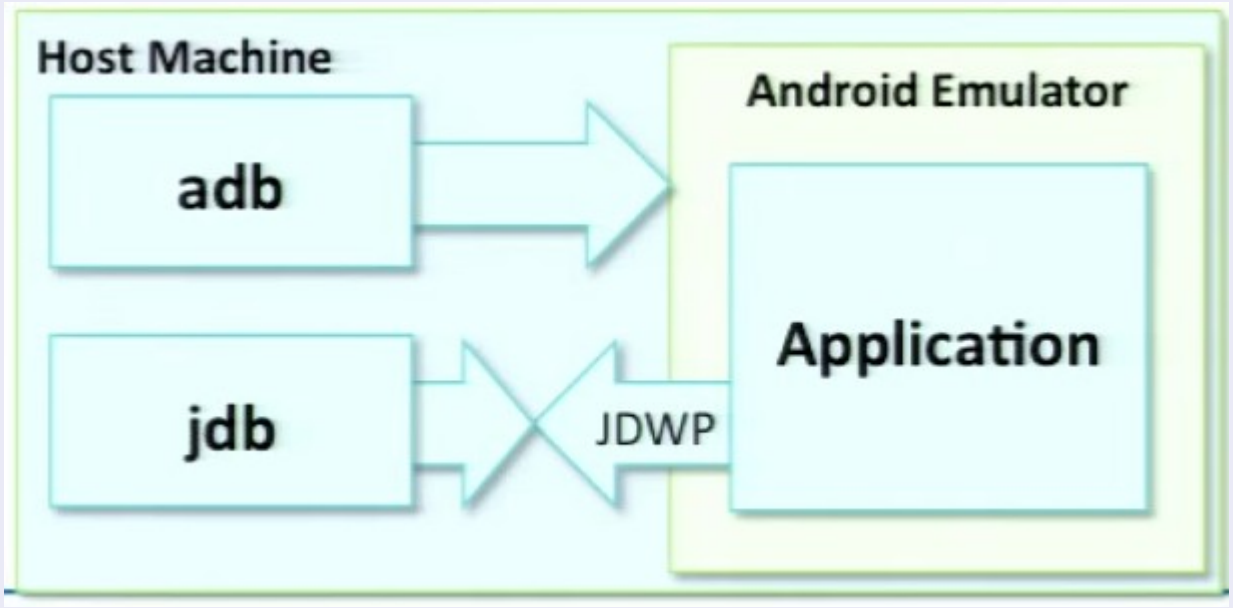
OWASP
The Open Web Application Security Project

Preparando nuestro entorno

$adb -d pull /data/data/com.aplication.apk
$adb -e install com.aplication.apk

Modo depuración
$adb shell ps
$adb forward tcp:8099 jdwp:[id proceso]
Conexión
Jdb -attach localhost:8099

Estructura JDB




DEMO
Time

OWASP
The Open Web Application Security Project

DEMO TIME 2

OWASP
The Open Web Application Security Project

Algunas recomendaciones

- Jamas dejar el modelo de negocios al lado del cliente.
- Usar cierto nivel de ofuscamiento.
- Debugging=False

OWASP
The Open Web Application Security Project

Despedida

Blog: Http://SixP4ck3r.BlogSpot.com/

Twitter: @SixP4ck3r

E-Mail: rithchard<<@>>gmail.com