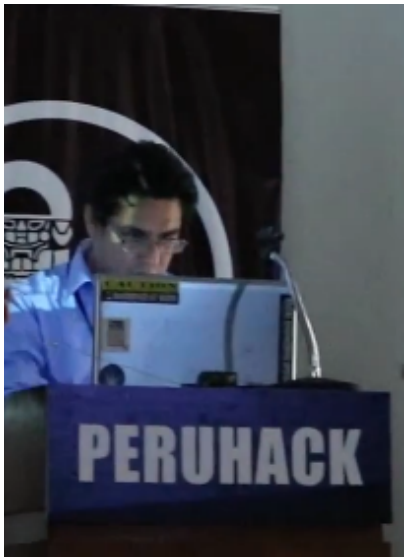
TECNOLÓGICO SUPERIOR CORDILLERA

25 AÑOS

CIDE
Centro de Investigación y Desarrollo Ecuador

SEMINARIO INTERNACIONAL DE SEGURIDAD EN EL DESARROLLO DE SOFTWARE



Attacks In Depth for Web Applications

JUAN OLIVA / @jroliva

- Pentester Security Researcher
- Proyectos de Ethical Hacking en Silcom VoIP & Security Assessment
- Consultor de soluciones de VoIP, enfocadas en seguridad
- Instructor de cursos de Ethical Hacking, Linux y VoIP
- Php y Python lover
- Linux user forever and ever
- Technical writer : Papper “Metasploitable 3 Laboratorios de Práctica”
- Twitter: @jroliva
- Blog: http://jroliva.wordpress.com/

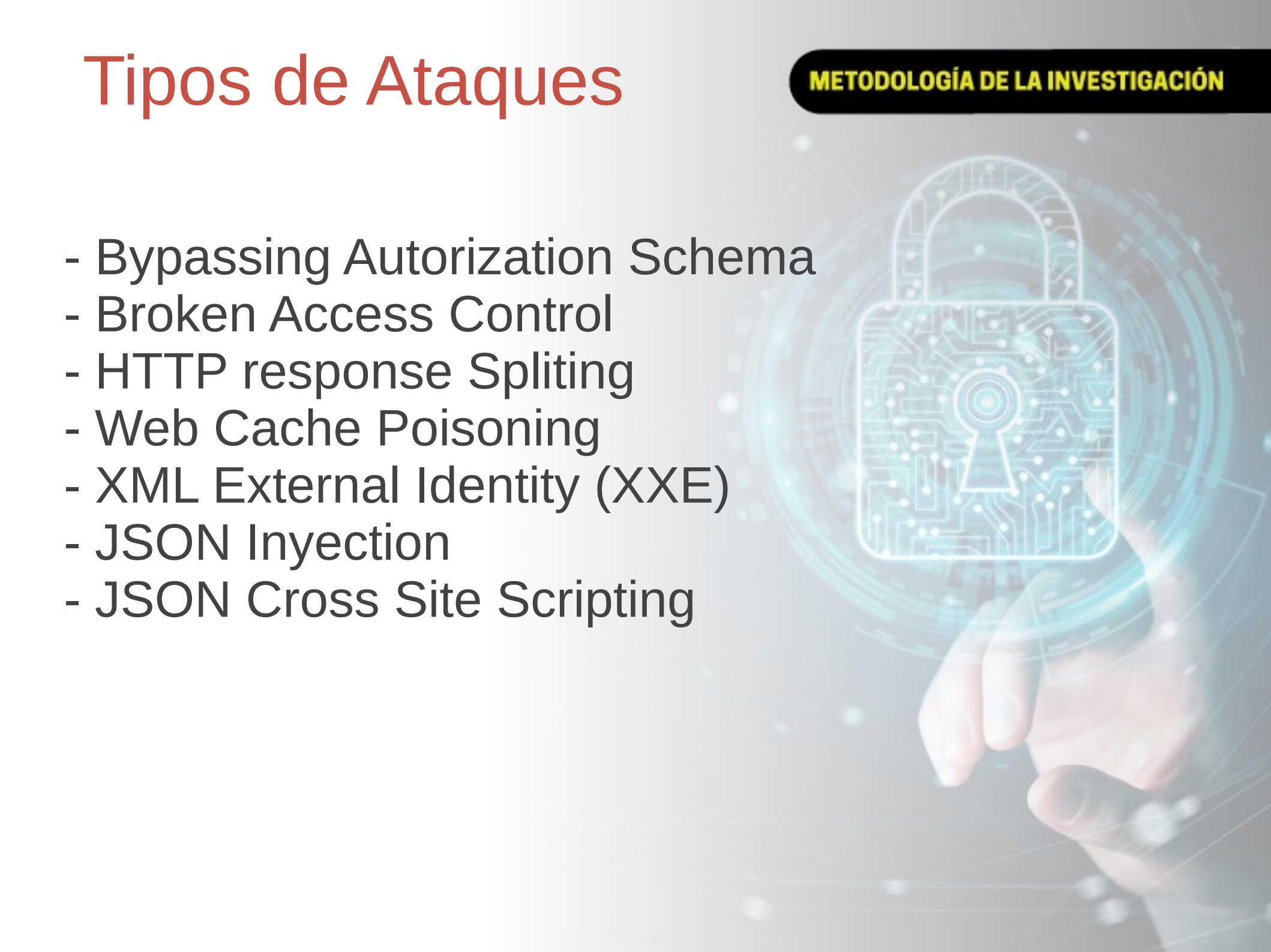
OBJETIVO DE ESTUDIO

Que son Ataques en en profundidad hacia aplicaciones Web

- Existen muchas aplicaciones “modernas”
- Protegidas de vulnerabilidades “comunes”
- Pero, que pasa con las mas rebuscadas poco comunes o mas complejas de explotar ?

Tipos de Ataques

- Bypassing Autorization Schema
- Broken Access Control
- HTTP response Spliting
- Web Cache Poisoning
- XML External Identity (XXE)
- JSON Inyection
- JSON Cross Site Scripting



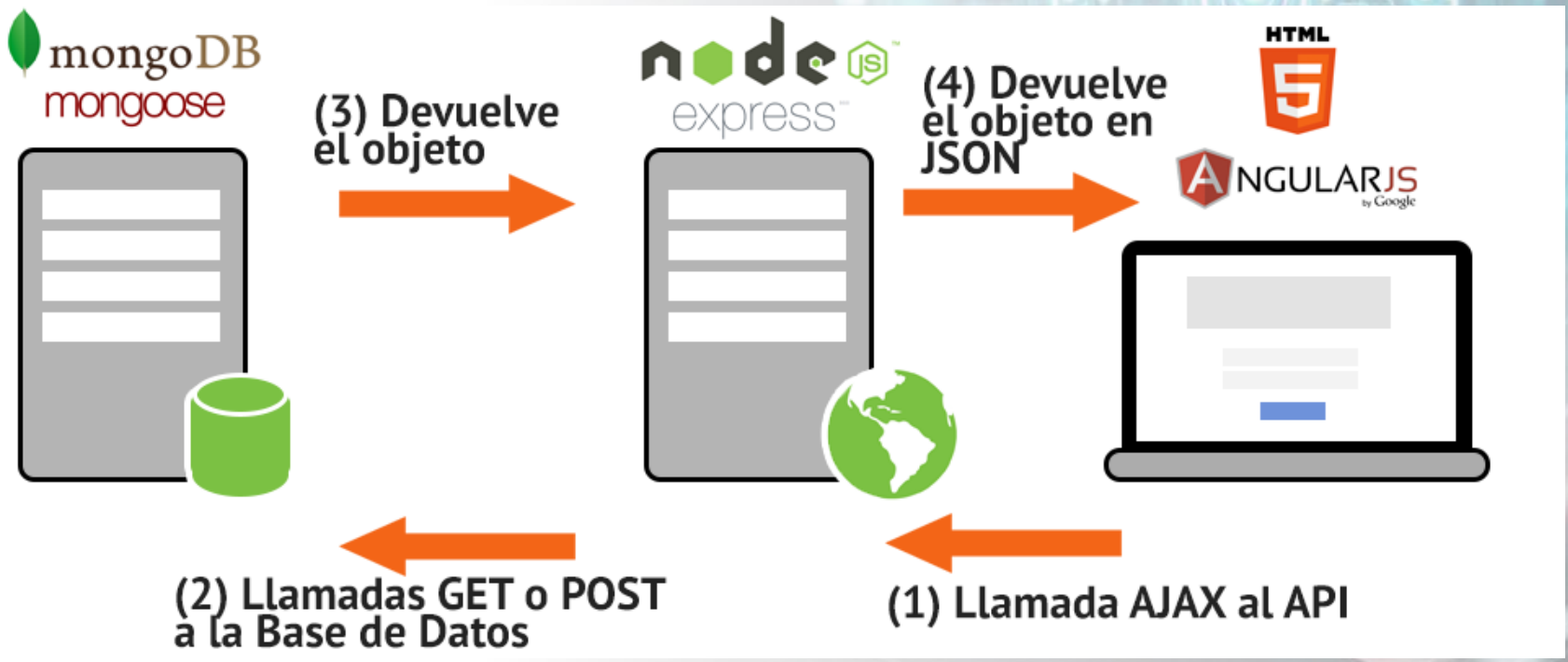
Bypassing Autorization Schema

Este tipo de vulnerabilidad se centra en verificar :

- Cómo se ha implementado el esquema de autorización para cada rol o privilegio
- Obtener acceso a funciones y recursos reservados.

Bypassing Autorization Schema

Servidor con API - REST

- 

Broken Access Control

Este tipo de vulnerabilidad se centra en verificar :

- La forma como la aplicacion otorga acceso a contenido a algunos usuario y no a otros.
- Verificar las reglas que se insertan en en varias ubicaciones en todo el codigo.

HTTP Response Spliting

- Tambien llamadado CRLF (Carriage Return Line Feed) = ataques de retorno de carro o salto de linea.
- Inyectar codigo CRLF en una petificion HTTP (POST/GET) para obtener control sobre el contenido de la respuesta HTTP.
- Generalmente se producen en los procesos de redireccion de paginas.
-

HTTP Response Spliting

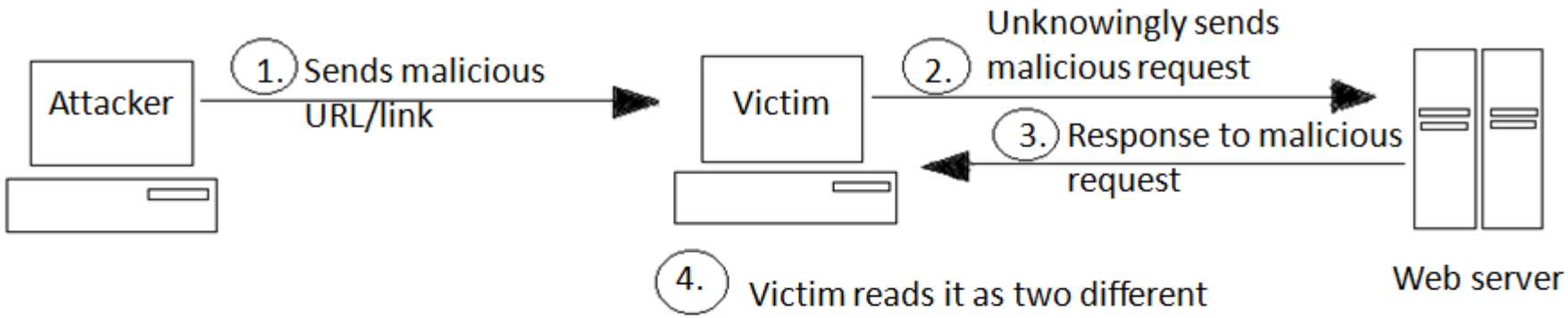
- Peticion del cliente
- www.empresa.com/pagina.jsp?lang=en
-
- Respuesta del servidor
- HTTP/1.0 302 Redirect
- Location:
- www.empresa.com/pagina.jsp?lang=en
- Connection: kee-Alive
- Content-Length: 0

HTTP Response Spliting

- Peticion del cliente
- www.empresa.com/pagina.jsp?lang=en**%0A**Content-Length**%3A%200%0A%0A**HTTP%2F1.1%20200%20OK%0AContent-Type**%3A%20text%2F**html%0AContent-Length%3A%2031**%0A%**3Chtml%3Ehttp%20Splitting%20test%20by%20%23PERUHACK2018**%20%3C%2F**html%3E
-
- Respuesta del servidor

- HTTP/1.0 302 Moved Temporaly
- Location:
- www.empresa.com/pagina.jsp?lang=en
- Content-Length: 0
- HTTP/1.0 200 OK
- Content-Type: text/html
- Content-Length: 19
- <html>http Splitting test by #PERUHACK2018 </html>

HTTP Response Spliting



Es el uso malisioso de caracteres CR y LR (%0d%0a) para quebrar la ejecucion del Programa y sustituir la pagina de respuesta Esperada.

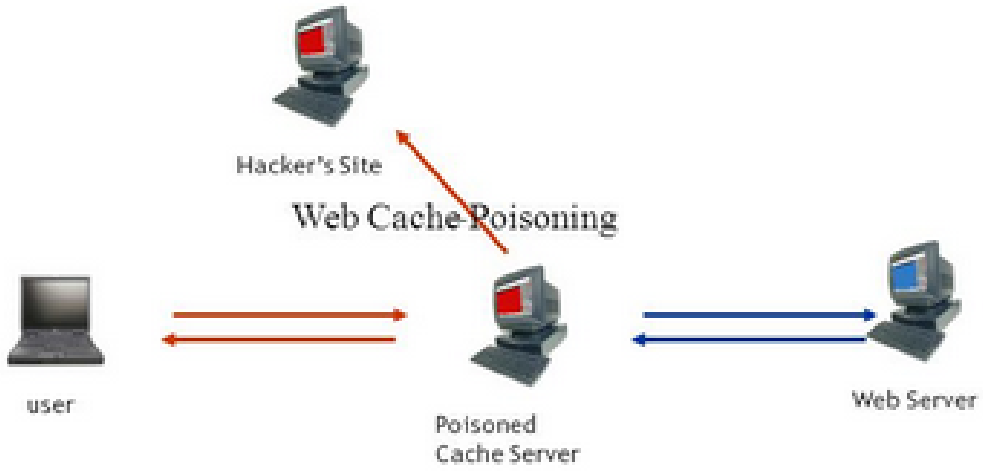
Web Cache poisoning

- Cache web es usado para mejorar el rendimiento del comsumo del ancho de banda
- Por lo general no existen mecanismos para validar la integridad de la cache del lado del servidor.
- Esto representa una oportunidad de vulnerabilidad que es posible explotar
- Una vez que la cache sea envenenada, los usuarios reciben el contenido ilegitimo o acceden a una URL modificada
- Consite en modificar el parametro que contiene la fecha de actualizacion de la pagina, de tal forma que el proxy nunca va actualizar la pagina en su cache.
-
-

Web Cache poisoning

Web Cache Poisoning

- Coming soon to a phishing pond near you

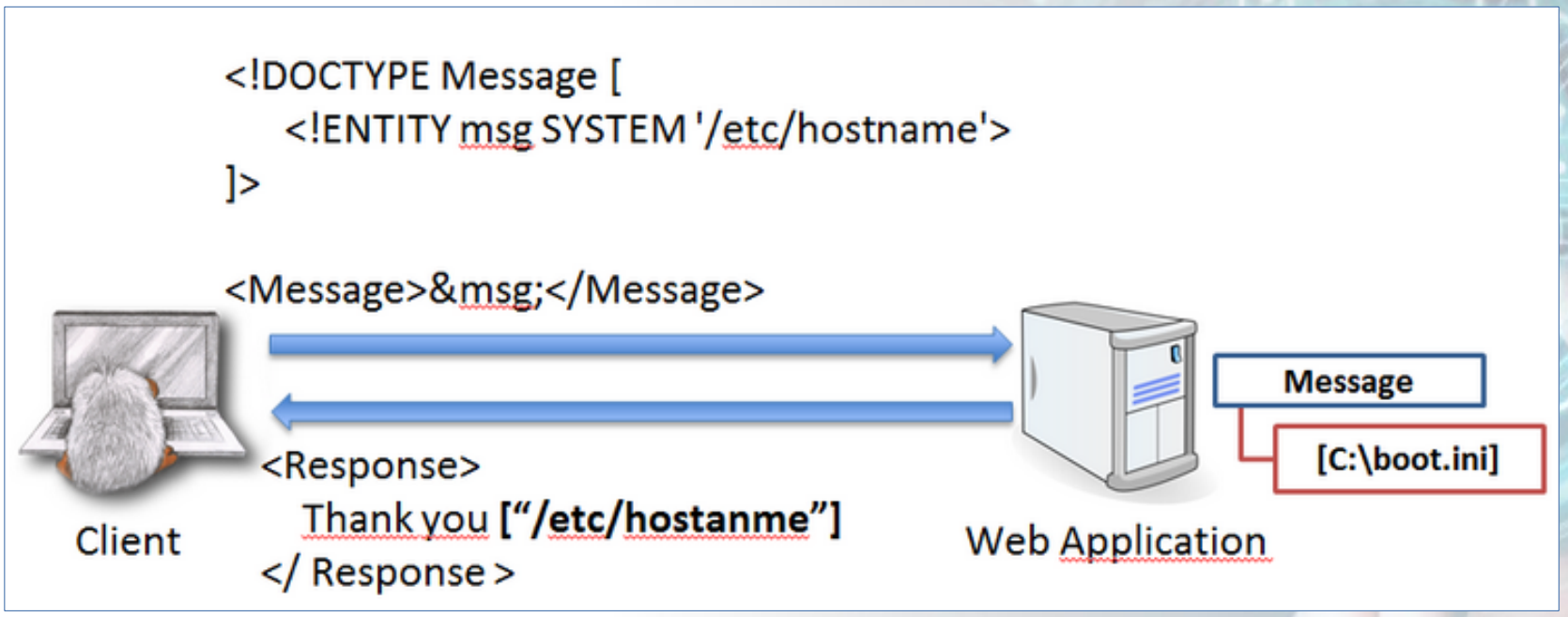


XML External Identity (XXE)

Este tipo de vulnerabilidad se centra en verificar :

- La mala configuracion de la pagina que interpreta XML
- Con el objetivo de invocar entidades externas, como funciones internas o archivos del sistema.
-

XML External Identity (XXE)



JSON INYECTION

- JSON se usa para almacenar datos o enviar mensajes. Cuando se utiliza para almacenar datos, JSON a menudo trata los datos almacenados en la caché del cliente.
- Lo cual permite ingresar entradas sin validar en JSON que permita inyectar atributos o elementos arbitrarios en la entidad JSON.
-
-

JSON INYECTION

JSON XSS

Este tipo de vulnerabilidad se centra en verificar :

- La mala configuracion de la pagina que interpreta XML
- Con el objetivo de invocar entidades externas, como funciones internas o archivos del sistema.
-

JSON XSS

```
<script>
    var JSONResponseString = '{"movies":[{"response":"HINT: our master really loves Marvel movies :)"}]}';

    // var JSONResponse = eval ("(" + JSONResponseString + ")");
    var JSONResponse = JSON.parse(JSONResponseString);

    document.getElementById("result").innerHTML=JSONResponse.movies[0].response;

</script>
```

"}]}';</script><script>prompt('CIDEECUADOR')</script>

Gracias !!!

Juan Oliva
Consultor en Ethical Hacking
joliva@silcom.com.pe

Hangouts :jroliva@gmail.com
Twiter : @jroliva
Blog : http://jroliva.net/


TECNOLÓGICO SUPERIOR
CORDILLERA
25 años
CIDE
Centro de Investigación
y Desarrollo Ecuador
SEMINARIO INTERNACIONAL DE
SEGURIDAD
EN EL DESARROLLO DE
SOFTWARE
WWW.CIDECUADOR.COM
Una vez finalizado el evento esta presentación
sera publicada en su respectiva página web