

XIII JORNADAS STIC CCN-CERT



**Padres no hay más
que dos... y los
míos son hackers
(y recelan de las
plataformas tecnológicas)**

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCCNCERT



www.dinosec.com
[@dinosec](https://twitter.com/dinosec)



Mónica Salas
Raúl Siles

Founders & Security Analysts
DinoSec

monica@dinosec.com
raul@dinosec.com

Diciembre 12, 2019



Índice

Venimos a contaros una (o varias) historias..., con su...

- Introducción
- Nudo
- Desenlace

Deberes para estas navidades y para 2020

COMUNIDAD Y CONFIANZA, BASES DE NUESTRA CIBERSEGURIDAD



PLATAFORMAS TECNOLÓGICAS

XIII JORNADAS STIC CCN-CERT





Plataformas tecnológicas (1/2)

- ¿Cuántos tenéis hijos, nietos, sobrinos...?
 - Entonces, creemos que os va a interesar esta ponencia, el resto...
- ¿Cuántos utilizáis plataformas tecnológicas en el ámbito personal?
 - Aplicaciones web y apps móviles con datos personales de los usuarios



Plataformas tecnológicas (2/2)

- ¿Cuántos utilizáis plataformas que os han "impuesto"?
- ¿Tuvisteis opción de haber prescindido de ellas en un principio?
- ¿Podríais dejar de usarlas ahora?

Cultura
Deporte
Ciudadanos
Extraescolares
Actividades
Ocio Educación
Salud

Privadas y públicas



¿Qué tiene de diferente esta ponencia...?

- No surge de la actividad profesional, sino personal
- Limitaciones evidentes a la hora de contar descubrimientos de la parte profesional (ética, NDAs...)
- La experiencia profesional nos lleva a recelar de las plataformas tecnológicas



Deformación profesional



PLATAFORMAS TECNOLÓGICAS EDUCATIVAS

XIII JORNADAS STIC CCN-CERT



En años anteriores...

Plataformas tecnológicas educativas privadas en ámbitos públicos...

La app de **comunicación y pagos**
entre centros educativos, profesores
y padres

 Pruébalo gratis



Download on the
App Store



Get it on
Google play

+10
Países

+450
Ciudades

+4000
Clientes

+500k
Usuarios



SEGURIDAD

Privacidad y **LSSI** (Ley de Protección de
Datos). Los datos personales son
confidenciales.

LSSI

LEY DE SERVICIOS DE LA SOCIEDAD
DE LA INFORMACIÓN Y DEL
COMERCIO ELECTRÓNICO



ESCUELAS INFANTILES



COLEGIOS



UNIVERSIDADES

comunicación entre centros educativos, papás y alumnos. Los mensajes
llegan siempre bajo la **máxima privacidad**, cumpliendo en todo
momento con todas las leyes.



ccn-cert
centro criptológico nacional

El precio de la privacidad en años anteriores...

Today 08:39

Buenos días Raúl. Se ha cancelado la sesión [REDACTED]. Hemos tenido problemas con la plataforma y no ha sido posible solucionarlo. Disculpa el trastorno. Un saludo

En 2019...

- La nueva plataforma educativa deja de ser opcional
 - Motivos: único medio de comunicación, autorizaciones, y mucho más...
- Introducción de sus ventajas y bondades por parte de la dirección
 - "No os preocupéis, ¡la plataforma es muy segura"! ... podemos dormir tranquilos...
 - "... tiene usuario y contraseña"



Seguro que ahora todos estáis pensando...

¡Que esta plataforma no sea la que yo utilizo!



E-mail inicial de invitación a la plataforma

Lunes 22 de julio de 2019 (12:00-13:00h)

Colegio [redacted] Colegio - Bienvenido a Pifias 22 Jul 2019 10:46

Equipo Directivo

A partir de septiembre podrán inscribirse en la plataforma.

[Leer comunicado](#)

Este mensaje incluye un enlace que le proporcionará acceso temporal a su cuenta. No reenviar o responder a este mensaje.

?

Plataforma Internet: Fijo Incluye Agujeros de Seguridad

Colegio

Enviado con

[Pifias](#)

<http://pifias.co>

<https://colegio.api.pifias.es/msg/hs48wxyz987/id/hs48abcd123/link>



Del e-mail a la web... (1/2)

<https://colegio.api.pifias.es/msg/hs48wxyz987/id/hs48abcd123/link>

"... acceso temporal a su cuenta." (e-mail)

Request

Raw Headers Hex
GET / [REDACTED] /hs48 [REDACTED] /link HTTP/1.1
Host: colegio [REDACTED]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:71.0) Gecko/20100101 Firefox/71.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,es;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
DNT: 1
Connection: close
Upgrade-Insecure-Requests: 1

Response

Raw Headers Hex
HTTP/1.1 302 Found
[REDACTED]
location:
[https://colegio \[REDACTED\] ?person=336#/ \[REDACTED\] 42](https://colegio [REDACTED] ?person=336#/ [REDACTED] 42)
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

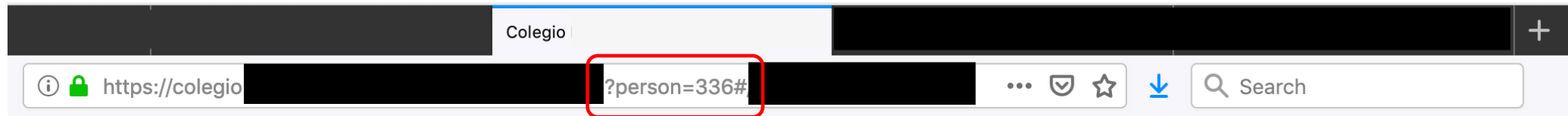
¿A qué puede hacer referencia ese acceso temporal...?

302 Found:

<https://colegio.pifias.es/mensaje?person=336#/hilo/5d357799bb442>



Del e-mail a la web... (2/2)



Usuario

Contraseña

[Olvidé mi contraseña](#)

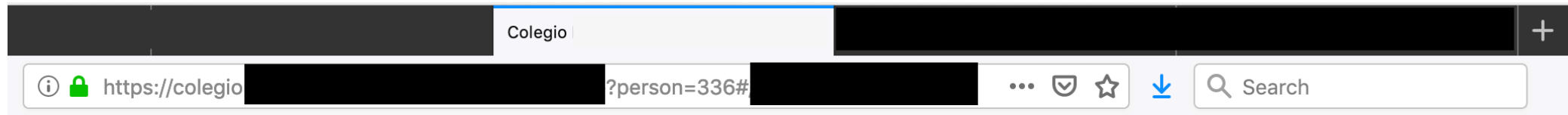
Ingresar

Volver atrás

Recordarme ☐



"A partir de septiembre podrán inscribirse en la plataforma..."



Usuario

Contraseña

[Olvidé mi contraseña](#)

Ingresar

Volver atrás

Recordarme ☐



Recuperando la contraseña...

... ¡y algo más!

Información de acceso

Usuario	Pifi_Aasco
Nueva contraseña	
Repita la nueva contraseña	

• la contraseña debe tener al menos 6 caracteres

Aceptar

1563790024

Timestamp to Human date

Supports Unix timestamps in seconds, milliseconds, micro

Assuming that this timestamp is in **seconds**:

GMT : Monday, July 22, 2019 10:07:04 AM

Your time zone : Monday, July 22, 2019 12:07:04 PM GMT

Recordar contraseña

Escriba a continuación su dirección de correo electrónico.

Email

mi_email@mi_dominio

<https://colegio.pifias.es/usuario/pass/recuperar?person=336&d=1563790024&h=166f02255c39c12d2f98e22bebc74d51>

Aceptar

Revisa tu eMail

Estimado Pifi_Aasco, en pocos minutos recibirá un email a [redacted] con instrucciones para obtener su nueva contraseña.

En caso de no recibirlo póngase en contacto con nosotros al teléfono .

Aceptar

Colegio

Solicitud de nueva contraseña

To: [redacted]

Reply-To: info@[redacted]

Estimado [redacted]:

Si usted ha olvidado su contraseña y desea obtener una nueva, haga click [AQUI](#)

Si usted no ha hecho una solicitud para recibir una nueva contraseña por favor ignore este mensaje.

E-mail

¿Qué chirría en todo este proceso...?

Acceso como usuario autenticado

Usuario y contraseña...

Usuario

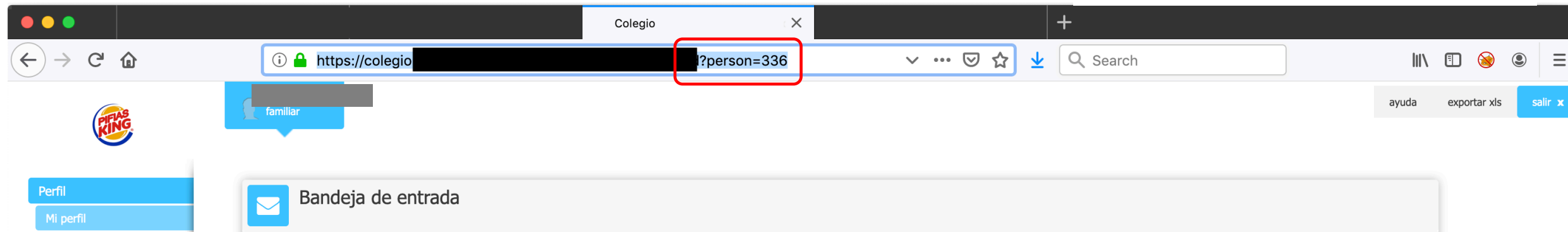
Contraseña

[Olvidé mi contraseña](#)

Ingresar

Volver atrás

Recordarme ☐



- Tras **5 minutos** de interacción con la plataforma como un usuario estándar...
- ... hicimos un parón para reflexionar

¿Cuál sería el siguiente paso...?



Interacción de 5 minutos con la plataforma como usuario estándar:

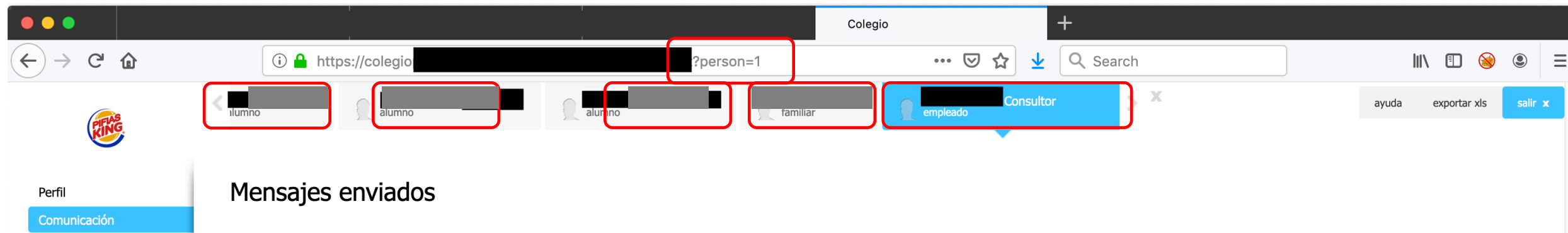
- Sin conocimientos ni herramientas avanzados
- Sin centrarnos en vulnerabilidades específicas y concretas (en las que profundizaremos posteriormente, que ya se veían venir)
- El juicio inicial sobre la condición general de seguridad era demoledor
- "¿Te acuerdas que teníamos pendiente echar un vistazo a la plataforma tecnológica del colegio una vez estuviera disponible...?"
 - "Pues pinta mal... ☹"
- Impacto personal muy elevado: todos los datos familiares



Probando un "LexNET"

10 minutos...

- Funcionamiento esperado de la aplicación...
 - Acceso con el usuario propio
 - Realizar acciones en representación de los hij@s



- Funcionamiento real de la aplicación... (...?person=<id>)
 - Roles de cada usuario: alumno, familiar, empleado...



Impacto del acceso como otro usuario...

Suplantación completa de todos los usuarios

- Por aquel entonces afectaba a:
 - **Comunicaciones: mensajería**
 - Bandeja de entrada (recibidos), enviados, eliminados, redactar mensaje...
 - Formularios
 - Comunidad: calendario de eventos, intercambio de archivos...
 - Perfil del usuario
 - Mi perfil (panel de control)
 - **Información personal**
- Lo que estaba por llegar:
 - **Autorizaciones**: excursiones, salidas fuera de horas, ausencias, personas autorizadas para recoger a los alumnos
 - **Ficha médica**: alergias, enfermedades, medicaciones, datos de emergencia...
 - Seguimientos de enfermería y psicología
 - **Calificaciones académicas** e historial
 - **Tesorería**: cobros y pagos pendientes y recientes... (lista de morosos)



¿A qué información se tenía realmente acceso?

Automatizando peticiones

						Nombre de la persona		Rol	Curso
Request	Payload	Status	Error	Time...	Length	14px;"...	14px;">	
0		200	☐			https://... person=336		Familiar	
1	1	200	☐			https://... person=1		Colaborador	
2	2	200	☐			https://... person=2		Colaborador	
3	3	200	☐			https://... person=3		Colaborador	
4	4	200	☐			https://... person=4		Colaborador	
5	5	200	☐			https://... person=5		Colaborador	
6	6	200	☐			https://... person=6		Colaborador	
7	7	200	☐			https://... person=7		Colaborador	
8	8	200	☐			https://... person=8		Colaborador	
9	9	200	☐			https://... person=9		Colaborador	
10	10	200	☐			https://... person=10		Estudiante	activo en
11	11	200	☐			https://... person=11		Estudiante	activo en
12	12	200	☐			https://... person=12		Estudiante	activo en
13	13	200	☐			https://... person=13		Estudiante	activo en
14	14	200	☐			https://... person=14		Estudiante	activo en
15	15	200	☐			https://... person=15		Estudiante	activo en
16	16	200	☐			https://... person=16		Estudiante	activo en
17	17	200	☐			https://... person=17		Estudiante	activo en

						Nombre de la persona y del alumno asociado		Rol
496	496	200	☐			https://... person=496	person=	Familiar
497	497	200	☐			https://... person=497		Familiar
498	498	200	☐			https://... person=498		Familiar
499	499	200	☐			https://... person=499		Familiar
500	500	200	☐			https://... person=500	person=	Familiar
501	501	200	☐			https://... person=501	person=	Familiar
502	502	200	☐			https://... person=502	person=	Familiar
503	503	200	☐			https://... person=503	person=	Colaborador
504	504	200	☐			https://... person=504	person=	Colaborador

Si te sale el espíritu hacker que llevas dentro...



¿Quién más hace uso de esta plataforma educativa...?

Nuestro colegio no estaba aún plenamente operativo, pero otros sí...



<-- Colegios públicos
y privados
(nacionales e
internacionales) -->



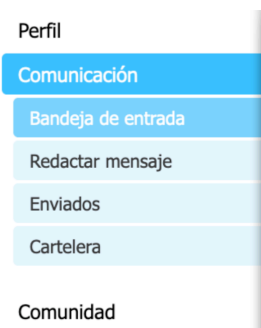
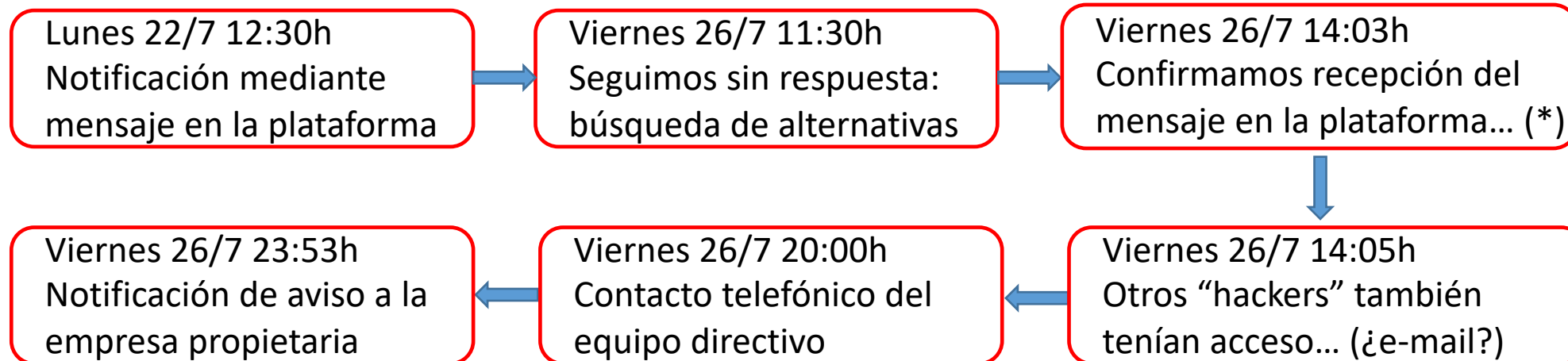
<  >
Previous 1 2 3 4 5 6 7 8 9 10 Next

Ni se nos ocurrió verificar si otros centros eran también vulnerables



Notificación a los responsables

Lunes 22 de julio de 2019: la situación es grave



← mensajes ▾

Q buscar

A partir de septiembre podrán inscribirse en la plataforma.



IMPORTANTE: Seguridad de la plataforma web

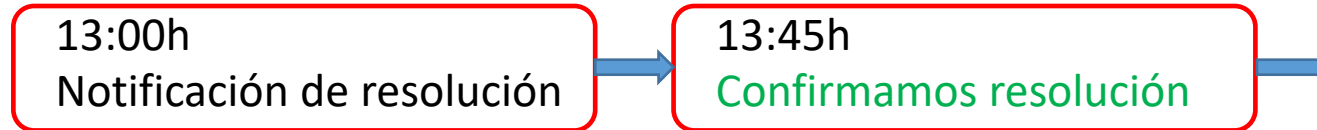
hoy a las 12:30

Buenos días [redacted], Por favor, cuando pueda, póngase en contacto con nosotros a través del teléfono para comentarle un problema importante de seg...



Resolución: Dirección del colegio

Sábado 27 de julio de 2019



Pero...

- ¿Y las comprobaciones antes de la entrada en producción?
- ¿Y los mecanismos de detección de comportamientos anómalos?

Alguien (**no nosotros**) debería analizar el estado de seguridad de la plataforma...

- Reunión en septiembre intentando tranquilizarnos: si alguna vez hubo una auditoría, el auditor debería de estar...



¿Cómo identificar vulnerabilidades de control de acceso?

Burp:

(múltiples
extensiones)

Authorize

The screenshot shows the Burp Suite interface with the 'Authorize' tab selected. The main table lists HTTP requests with columns for ID, Method, URL, and various length fields. The 'Authorization' column shows 'Is enforced??? ... Enforced!'. A red box highlights the 'Authorize' tab in the top navigation bar. Another red box highlights the 'Check unauthenticated' checkbox in the 'Authorization checks' section. A third red box highlights the 'Enforcement Detector' tab in the bottom right section. The 'Enforcement Detector' section shows a filter list with the rule 'Status code equals: 302'.

ID	Method	URL	Orig. Length	Modif. Length	Unauth. Length	Authorization ...	Authorization...
80	GET	https://colegio	4	4	0	Is enforced??? ...	Enforced!
81	GET	https://colegio	2351	2351	0	Is enforced??? ...	Enforced!
82	GET	https://colegio	4	4	4	Is enforced??? ...	Is enforced??? ...
83	GET	https://colegio	832	832	0	Is enforced??? ...	Enforced!
84	GET	https://colegio	25032	25032	0	Is enforced??? ...	Enforced!
85	GET	https://colegio	0	0	0	Is enforced??? ...	Is enforced??? ...
86	GET	https://colegio	6324	0	6324	Enforced!	Is enforced??? ...
87	GET	https://colegio	516594	516594	516594	Is enforced??? ...	Is enforced??? ...
88	POST	https://colegio	0	0	0	Is enforced??? ...	Enforced!
89	GET	https://colegio	33797	397	6431	Is enforced??? ...	Enforced!
90	GET	https://colegio	757	757	757	Is enforced??? ...	Enforced!
91	GET	https://colegio	504	504	504	Is enforced??? ...	Enforced!
92	GET	https://colegio	1014	1014	1014	Is enforced??? ...	Enforced!
93	GET	https://colegio	7429404	7429404	7429404	Is enforced??? ...	Enforced!
94	GET	https://colegio	480	480	480	Is enforced??? ...	Enforced!
95	GET	https://colegio	833	833	833	Is enforced??? ...	Enforced!
96	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Enforced!
97	GET	https://colegio	783	783	783	Is enforced??? ...	Enforced!
98	GET	https://colegio	612	612	612	Is enforced??? ...	Enforced!
99	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Enforced!
100	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Enforced!
101	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Enforced!
102	GET	https://colegio	832	832	0	Is enforced??? ...	Enforced!
103	GET	https://colegio	4	4	4	Is enforced??? ...	Enforced!
104	GET	https://colegio	30	30	30	Is enforced??? ...	Enforced!
105	GET	https://colegio	4	4	0	Is enforced??? ...	Enforced!
106	GET	https://colegio	0	0	0	Is enforced??? ...	Is enforced??? ...
107	GET	https://colegio	6324	0	6324	Enforced!	Is enforced??? ...
108	POST	https://colegio	0	0	0	Is enforced??? ...	Is enforced??? ...
109	GET	https://colegio	33797	397	6431	Is enforced??? ...	Is enforced??? ...
110	GET	https://colegio	7429404	7429404	7429404	Is enforced??? ...	Is enforced??? ...
111	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Is enforced??? ...
112	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Is enforced??? ...
113	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Is enforced??? ...
114	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Is enforced??? ...
115	GET	https://colegio	4	4	4	Is enforced??? ...	Is enforced??? ...
116	GET	https://colegio	832	832	0	Is enforced??? ...	Enforced!
117	GET	https://colegio	30	30	30	Is enforced??? ...	Is enforced??? ...
118	GET	https://colegio	4	4	0	Is enforced??? ...	Enforced!
119	GET	https://colegio	0	0	0	Is enforced??? ...	Enforced!
120	GET	https://colegio	6324	0	6324	Enforced!	Enforced!
121	POST	https://colegio	0	0	0	Is enforced??? ...	Enforced!
122	GET	https://colegio	33797	397	6431	Is enforced??? ...	Enforced!
123	GET	https://colegio	7429404	7429404	7429404	Is enforced??? ...	Enforced!
124	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Enforced!
125	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Enforced!
126	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Enforced!
127	OPTIONS	https://colegio	0	0	0	Is enforced??? ...	Enforced!
128	GET	https://colegio	30	30	30	Is enforced??? ...	Enforced!
129	GET	https://colegio	4	4	4	Is enforced??? ...	Enforced!
130	GET	https://colegio	832	832	0	Is enforced??? ...	Enforced!
131	GET	https://colegio	4	4	0	Is enforced??? ...	Enforced!



Tras el periodo estival...

Viernes 20 de septiembre de 2019

- Reunión al comienzo del curso escolar
- Delicadamente planteamos nuestras reticencias e impresiones
- La dirección seguía estando muy receptiva y agradecida
- ¿Siguen existiendo otras vulnerabilidades?
 - No quisimos seguir indagando desde julio
- Por supuesto, y ya se veían venir desde el principio...
- Comprobada antes de la reunión el **sábado 14 de septiembre de 2019**

¿Qué vulnerabilidad parece existir en el proceso de login?



Vulnerabilidad en el proceso de login (1/3)

Mensajes vía e-mail que redirigen (302) a la página de login...

#	Host	Method	URL	Params	Edited	Status
1	https://colegio[REDACTED]	GET	/[REDACTED]/ic[REDACTED]/ic[REDACTED]/link			302
2	https://colegio[REDACTED]	GET	/[REDACTED]?person=336	✓		200

Request

Response

Raw

Headers

Hex

HTML

```

HTTP/1.1 200 OK
Date: Fri, 13 Sep 2019 11:25:17 GMT
Server: Apache/2.4.18 (Ubuntu)
Set-Cookie: [REDACTED]=ap7cjl8p4frle153msph8rdo3; path=/
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Access-Control-Allow-Origin: *
Vary: Accept-Encoding
Content-Length: 6425
Connection: close
Content-Type: text/html; charset=UTF-8

<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
  "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>

```

<-- Página de login

Vulnerabilidad en el proceso de login (2/3)

Formulario de login: petición...

#	Host	Method	URL	Params	Edited	Status
22	https://colegio[REDACTED]	POST	/[REDACTED]	?person=336	✓	200

Request

Response

Raw

Params

Headers

Hex


```
POST /[REDACTED]?person=336 HTTP/1.1
Host: colegio[REDACTED]
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.14; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,es;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Referer: https://colegio[REDACTED]
Content-Type: application/x-www-form-urlencoded
Content-Length: 53
DNT: 1
Connection: close
Cookie: [REDACTED]=[REDACTED]=ap7cjl f8p4frle153msph8rdo3; __utma=[REDACTED]
__utmz=[REDACTED]; __utmt=1
Upgrade-Insecure-Requests: 1

_width=[REDACTED]&_height=[REDACTED]
```



Vulnerabilidad en el proceso de login (3/3)

Formulario de login: **respuesta...**

#	Host	Method	URL	Params	Edited	Status
22	https://colegio [REDACTED]	POST	/ [REDACTED]	?person=336	✓	200

Request	Response
---------	----------

Raw	Headers	Hex	HTML
-----	---------	-----	------

Date: Fri, 13 Sep 2019 11:34:22 GMT
Server: [REDACTED]
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Vary: Accept-Encoding
Access-Control-Allow-Origin: *
Content-Length: 4297
Connection: close
Content-Type: text/html; charset=UTF-8

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
    "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html>
  <head>
```

<-- Acceso a la cuenta del usuario



Ejemplo de otra vulnerabilidad más

- Fijación de sesión (conocida desde 2002)
 - Black Hat EU (marzo 2011): <https://www.dinosec.com/en/lab.html#SAPBH2011>
- ¿Cuál es el peor caso posible de fijación de sesión?
 - Por parte de un usuario no autenticado
 - No es necesario disponer de un usuario en la plataforma
 - Sin ni siquiera interactuar con la plataforma
 - Cualquier valor válido para la cookie de sesión
- De nuevo, desvela la condición general de seguridad de la plataforma
 - Evidencias enviadas el **viernes 20 de septiembre a las 15:28h**

¿Esta vulnerabilidad fue también resuelta diligentemente?



PLATAFORMAS TECNOLÓGICAS CULTURALES

XIII JORNADAS STIC CCN-CERT



HTTP Everywhere

Incluyendo el formulario de autenticación (muy de los años 2000)

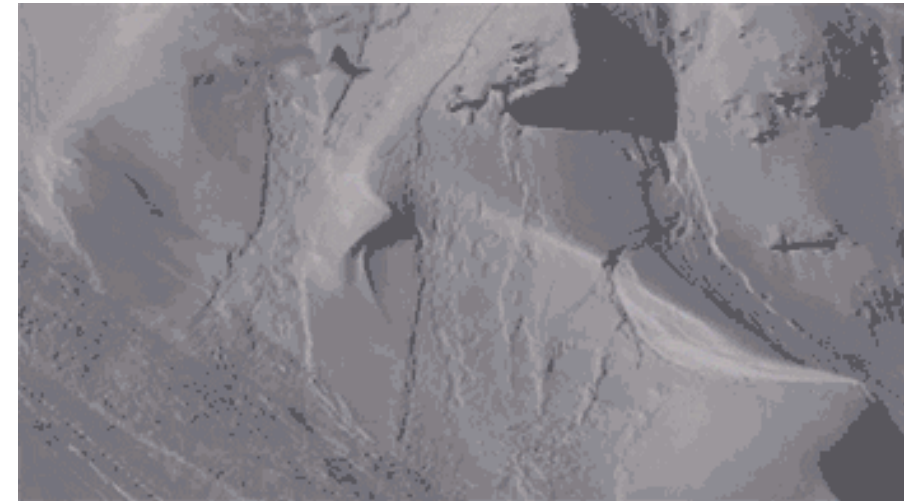


- Múltiples accesos diferentes
- Datos personales (de miles a millones)
- Utilización de SSO (Single Sign On)
 - Credenciales compartidas con otros servicios con acceso a contenidos digitales...



Proceso de notificación

- Inicial: finales de septiembre
- Seguimiento: finales de octubre
- Dificultad en encontrar al equipo y/o persona responsable de seguridad
- Persecución activa a través de dos frentes
 - Individual y vía el CCN-CERT
- Lunes-Miércoles 4-6 de noviembre de 2019
 - Informe detallado oficial



Preocupación principal: RGPD (¿prevenir o curar?)

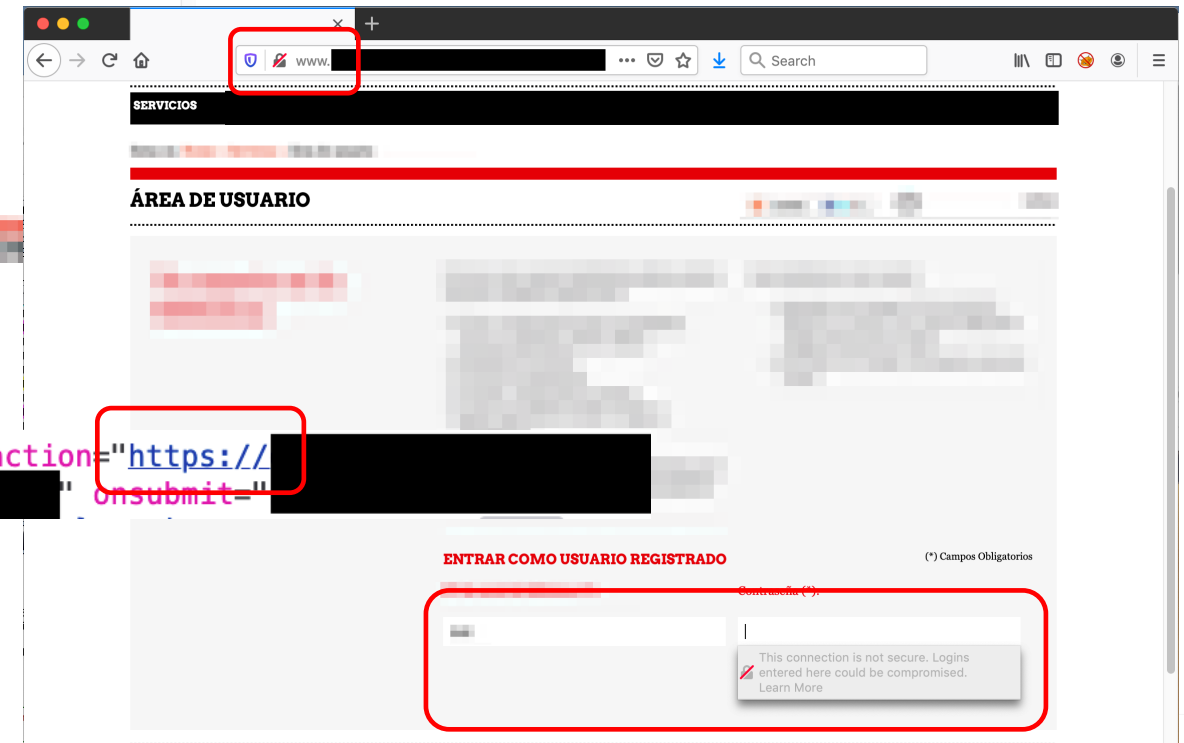
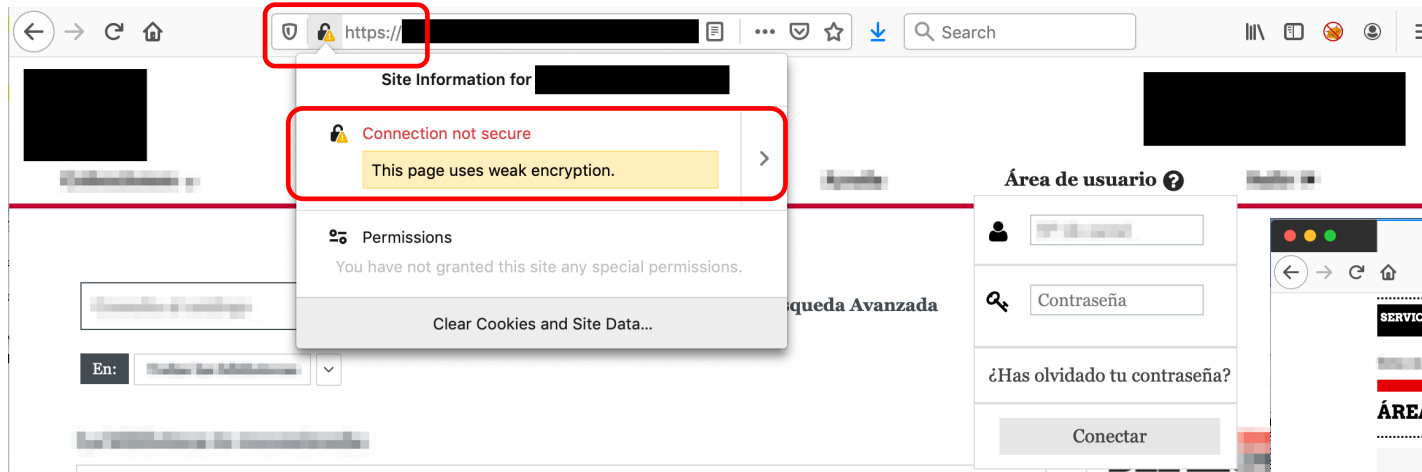


Resolución

Technical Details

Broken Encryption (TLS_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.0)

TLS 1.0: Enero de 1999



```
<form id="[redacted]" class="[redacted]" action="https://[redacted]" method="post" target="_blank" name="[redacted]" onsubmit="[redacted]"
```

¿Siguen existiendo otras vulnerabilidades?

CONCLUSIONES

XIII JORNADAS STIC CCN-CERT



COMUNIDAD Y CONFIANZA, BASES DE NUESTRA CIBERSEGURIDAD

Conclusiones (1/2)

“Tener confianza” es distinto de “ser confiado”

- Usuario final:
 - Exigir informes sobre controles aplicados, auditorías de seguridad, funcionamiento...
- Sector Público y Sector Privado (SPs):
 - Establecer un mínimo marco normativo:
 - ¿Qué controles se deben aplicar y qué análisis se deben realizar antes de poner estas plataformas tecnológicas en producción?
 - Notificaciones de seguridad: security.txt
 - <https://securitytxt.org>
 - Aplicar buenas prácticas de seguridad
 - Cabeceras HTTP de seguridad
 - Plataformas tecnológicas horizontales (educación)



#Retos2020

Evaluación continua
(OB/2) & inicial...

Aplicaciones web y aplicaciones móviles (iOS y Android)



OWASP Top 10 - 2017

OWASP Top 10 - 2013	→	OWASP Top 10 - 2017
A1 – Injection	→	A1:2017-Injection
A2 – Broken Authentication and Session Management	→	A2:2017-Broken Authentication
A3 – Cross-Site Scripting (XSS)	↘	A3:2017-Sensitive Data Exposure
A4 – Insecure Direct Object References [Merged+A7]	U	A4:2017-XML External Entities (XXE) [NEW]
A5 – Security Misconfiguration	↘	A5:2017-Broken Access Control [Merged]
A6 – Sensitive Data Exposure	↗	A6:2017-Security Misconfiguration
A7 – Missing Function Level Access Contr [Merged+A4]	U	A7:2017-Cross-Site Scripting (XSS)
A8 – Cross-Site Request Forgery (CSRF)	⊗	A8:2017-Insecure Deserialization [NEW, Community]
A9 – Using Components with Known Vulnerabilities	→	A9:2017-Using Components with Known Vulnerabilities
A10 – Unvalidated Redirects and Forwards	⊗	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project



Conclusiones (2/2)

- Propietario y/o desarrollador de una plataforma tecnológica:
 - Asegúrate de que entre los alumnos... ¡ninguno tiene padres *hackers*!



Nueva plataforma del CCN-CERT en el 2020

SOLUCIONES

AMPARO

ANA

ATENEA

CARMEN

CCNDroid

CLARA

CLAUDIA

ELISA

EMMA

GLORIA

INES

LORETO

LUCIA

MARIA

MARTA

PILAR

REYES

ROCIO

VANESA



Aplica Minuciosamente Buenas
Recomendaciones Objetivas de
Seguridad Inmediata y Ampliamente

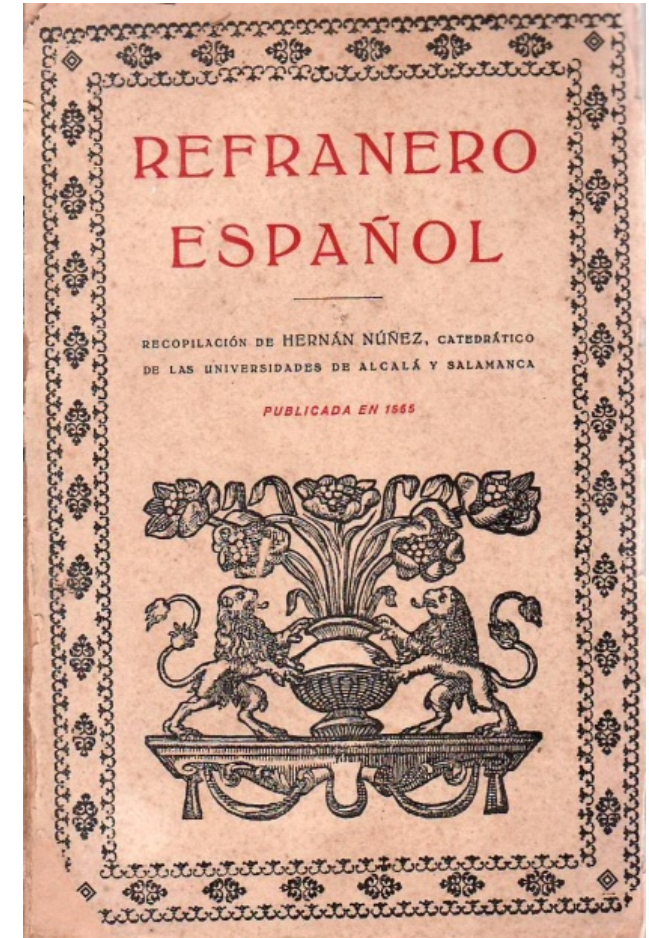


El refranero español

“Ojos que no ven...
plataforma que te cuelan...
¡y todos tus datos vuelan!



“Lo que me cuentan no creo,
sino solo lo que veo”





www.dinosec.com
@dinosec

Mónica Salas
monica@dinosec.com

Raúl Siles
raul@dinosec.com



¡Muchas gracias! ¿Preguntas?



www.dinosec.com
[@dinosec](https://twitter.com/dinosec)



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional