Dirigido a:
Eduardo Parraguez
khipu

JULIO
2019

INFORME TÉCNICO

Análisis Perimetral de Vulnerabilidades JULIO 2019

DOCUMENTO CONFIDENCIAL

https://nivel4.com

+56 2 2248 1368
Av Providencia 1208
Oficina 1204
Santiago, Chile.

1 Control de versiones

El siguiente cuadro muestra el historial de cambios sobre el presente documento.

Fecha	Autor	Versión	Comentarios
26-08-2019	Kevin Möller	1.0	Documentación

CONFIDENCIAL

Tabla de contenido

1 Control de versiones 2
2 Resumen ejecutivo 4
3 Ámbito 5
4 Análisis perimetral de vulnerabilidades 6
4.1 Subdominios 6
4.2 Puertos y servicios 8
4.2.1 IP 50.22.89.18 y 50.22.111.181 (Mismo Servidor) 8
4.2.2 IP 50.22.111.178 8
4.2.3 IP 50.22.111.179 9
4.2.4 IP 50.22.111.182 10
4.2.5 IP 184.173.238.18 10
4.2.6 IP 184.173.238.19 10
4.2.7 IP 184.173.238.20 10
4.2.8 IP 184.173.238.22 11
5 Análisis SSL 16
5.1 dev.khipu.com 16
5.2 khipu.com 18
6 Recomendaciones generales 21
Referencias 23
Referencias 23

CONFIDENCIAL

2 Resumen ejecutivo

El análisis de vulnerabilidades consideró dentro de su alcance todo el perímetro de khipu.com. Se enumeraron dominios y subdominios, direcciones y rangos IP, puertos y servicios, y debilidades asociadas a cada uno de los elementos detectados.

Fue posible detectar un total de 23 subdominios de los cuales 16 se encuentran activos y 7 inactivos. Los subdominios activos cuentan con puertos disponibles que se encuentran expuestos a Internet, estos puertos muestran distintos servicios (SSH, HTTP, HTTPS) y de acuerdo con las versiones de estos servicios ninguno tiene vulnerabilidades conocidas que impliquen un riesgo de seguridad.

Por otra parte, durante el análisis SSL se detectó que existen dos certificados válidos para los dominios y subdominios de khipu. El primero es válido para khipu.com, www.khipu.com y bi.khipu.com; el segundo certificado es válido para dev.khipu.com y para www.dev.khipu.com; El resto de los subdominios detectados utilizan certificados que no son válidos, lo que representa un problema de configuración y un potencial riesgo de confidencialidad.

Las direcciones IP 50.22.111.181 y 50.22.89.18 corresponden al mismo servidor, fue posible reconocerlo debido a que ambos servidores SSH presentan las mismas llaves para el servicio. Esto no implica ningún riesgo o inconveniente, solo de manera informativa se indica que ambas direcciones IP se alojan en el mismo servidor por lo que el análisis SSL será idéntico en ambas direcciones IPs

CONFIDENCIAL

3 Ámbito

Las pruebas fueron realizadas sobre https://khipu.com y todo su perímetro.

#	IP	Hostname	Ambiente
1	50.22.89.18	https://khipu.com	Producción

En relación al ámbito se destaca solo khipu.com como objetivo principal ya que es la base del análisis perimetral por lo que debemos tomar este dominio para determinar registros asociados como al dominio como tal obteniendo sub-dominios, direcciones IP, sistemas, etc.

CONFIDENCIAL

4 Análisis perimetral de vulnerabilidades

A nivel de infraestructura se realizó una búsqueda complementaria de todos los subdominios y direcciones IP asociadas a khipu.com, identificándose una cantidad determinada de puertos y servicios que están expuestos a internet.

En análisis se identificaron los puertos y servicios que se encuentras disponibles también las versiones de los sistemas operativos que se ejecutan en estos puestos.

4.1 Subdominios

Se detectaron 15 subdominios activos y 3 subdominios no activos

#	Hostname	Dirección IP	Observaciones
1	app.khipu.com	50.22.89.18	Activo
2	bi.khipu.com	50.22.89.18	Activo
3	demo.khipu.com	50.22.89.18	Activo
4	dev.khipu.com	184.173.238.22	Activo
5	kh04.khipu.com	50.22.111.181	Activo
6	kh06.khipu.com	50.22.111.182	Activo
7	kh07.khipu.com	184.173.238.20	Activo
8	kh08.khipu.com	184.173.238.22	Activo
9	kh09.khipu.com	50.22.111.179	Activo
10	Kh10.khipu.com	50.22.111.178	Activo

11	Kh11.khipu.com	184.173.238.18	Activo
12	kh12.khipu.com	184.173.238.19	Activo
13	khipu.com	50.22.89.18	Activo
14	staging.khipu.com	35.196.64.45	No Activo
15	www.khipu.com	50.22.89.18	Activo
16	kh03.khipu.com	50.22.111.180	No Activo
17	kh05.khipu.com	198.23.126.125	No Activo
18	kauthorizer.khipu.com	35.231.209.46	Activo
19	status.khipu.com	18.234.32.149	Activo
20	magic.khipu.com	No Detectado	No Activo
21	stress.khipu.com	192.168.200.10	No Activo
22	dev.whmcs.khipu.com	No Detectado	No Activo
23	easytaxitopup.khipu.cm	No Detectado	No Activo

CONFI

4.2 Puertos y servicios

4.2.1 IP 50.22.89.18 y 50.22.111.181 (Mismo Servidor)

Puerto	Servicio	Producto	Versión	Observaciones
22	SSH	OpenSSH	7.2p2 Ubuntu 4ubuntu2.8	Sistema Operativo Ubuntu Linux
80	HTTP	HAProxy	1.3.1 o superior	
443	HTTPS	HAProxy	1.3.1 o superior	

4.2.2 IP 50.22.111.178

Puerto	Servicio	Producto	Versión	Observaciones
22	SSH	OpenSSH	7.2p2 Ubuntu 4ubuntu2.8	Sistema Operativo Ubuntu Linux
80	HTTP	HAProxy	1.3.1 o superior	
443	HTTPS	HAProxy	1.3.1 o superior	

CONFIDENCIAL

4.2.3 IP 50.22.111.179

Puerto	Servicio	Producto	Versión	Observaciones
22	SSH	OpenSSH	7.2p2 Ubuntu 4ubuntu2.8	Sistema Operativo Ubuntu Linux
80	HTTP	HAProxy	1.3.1 o superior	
443	HTTPS	HAProxy	1.3.1 o superior	

CONFIDENCIAL

4.2.4 IP 50.22.111.182

Puerto	Servicio	Producto	Versión	Observaciones
22	SSH	OpenSSH	7.2p2 Ubuntu 4ubuntu 4	Sistema Operativo Ubuntu Linux

4.2.5 IP 184.173.238.18

Puerto	Servicio	Producto	Versión	Observaciones
22	SSH	OpenSSH	7.2p2 Ubuntu 4ubuntu2.1	Sistema Operativo Ubuntu Linux
443	HTTPS	HAProxy	1.3.1 o superior	

4.2.6 IP 184.173.238.19

Puerto	Servicio	Producto	Versión	Observaciones
22	SSH	OpenSSH	7.2p2 Ubuntu 4ubuntu2.1	Sistema Operativo Ubuntu Linux
443	HTTPS	HAProxy	1.3.1 o superior	

4.2.7 IP 184.173.238.20

Puerto	Servicio	Producto	Versión	Observaciones
22	SSH	OpenSSH	7.2p2 Ubuntu 4ubuntu2.8	Sistema Operativo Ubuntu Linux

CONFIDENCIAL

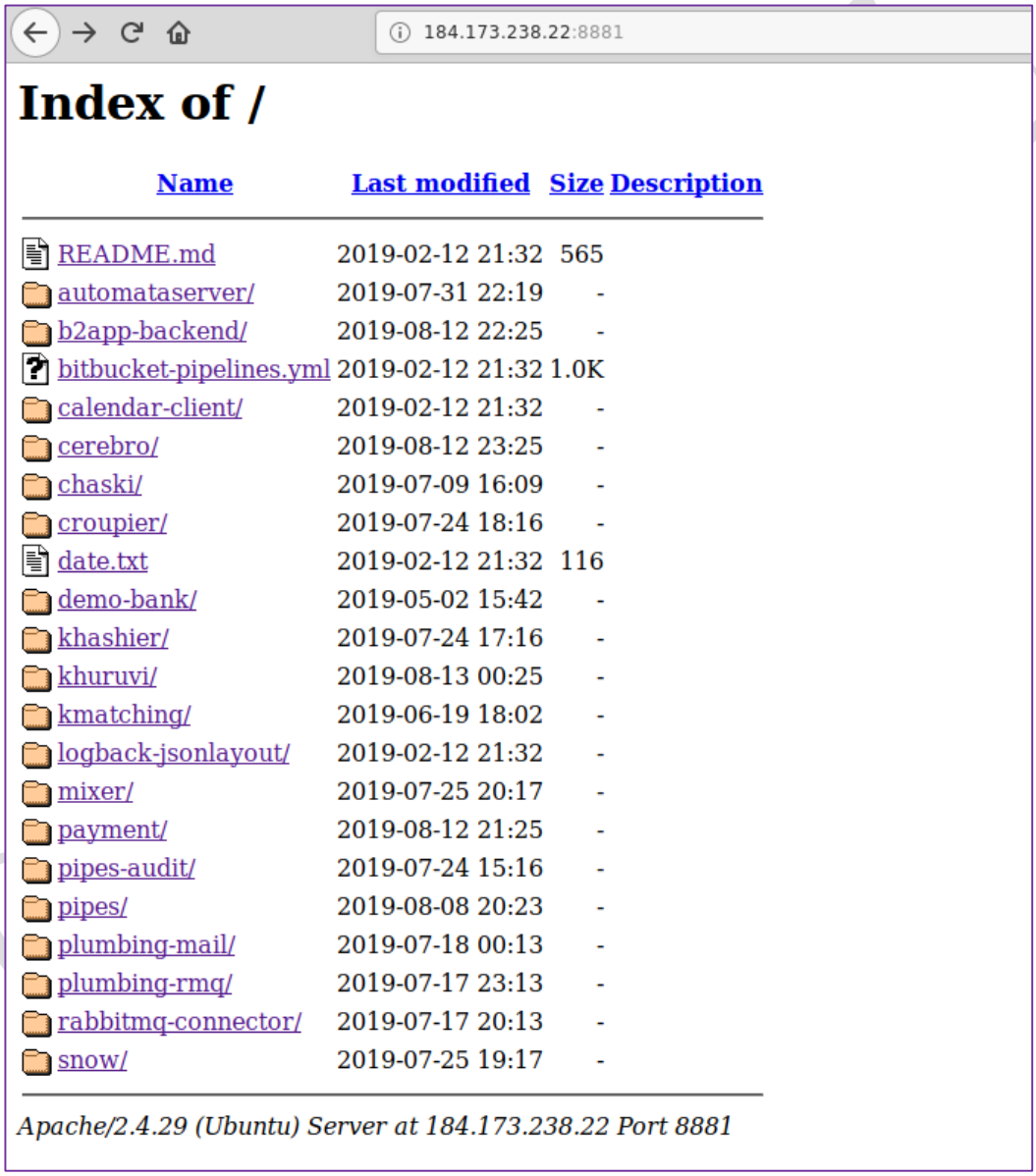
4.2.8 IP 184.173.238.22

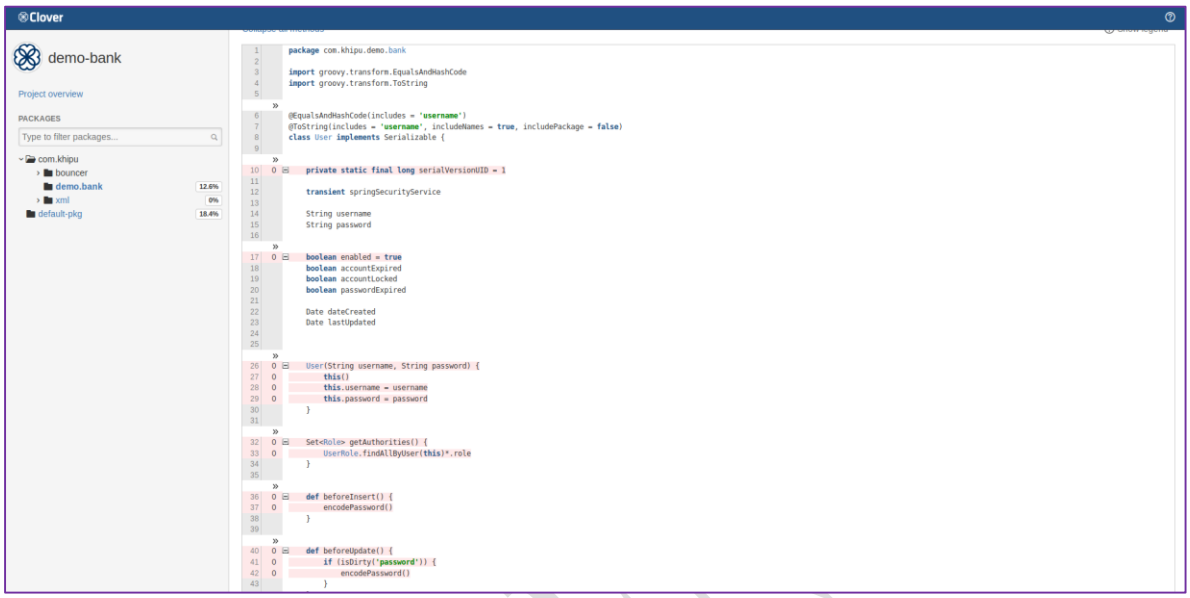
Puerto	Servicio	Producto	Versión	Observaciones
22	SSH	OpenSSH	7.2p2 Ubuntu 4ubuntu2.8	Sistema Operativo Ubuntu Linux
80	HTTP	HAProxy	1.3.1 o superior	
443	HTTPS	HAProxy	1.3.1 o superior	
8881	HTTP	Apache	httpd 2.4.29	

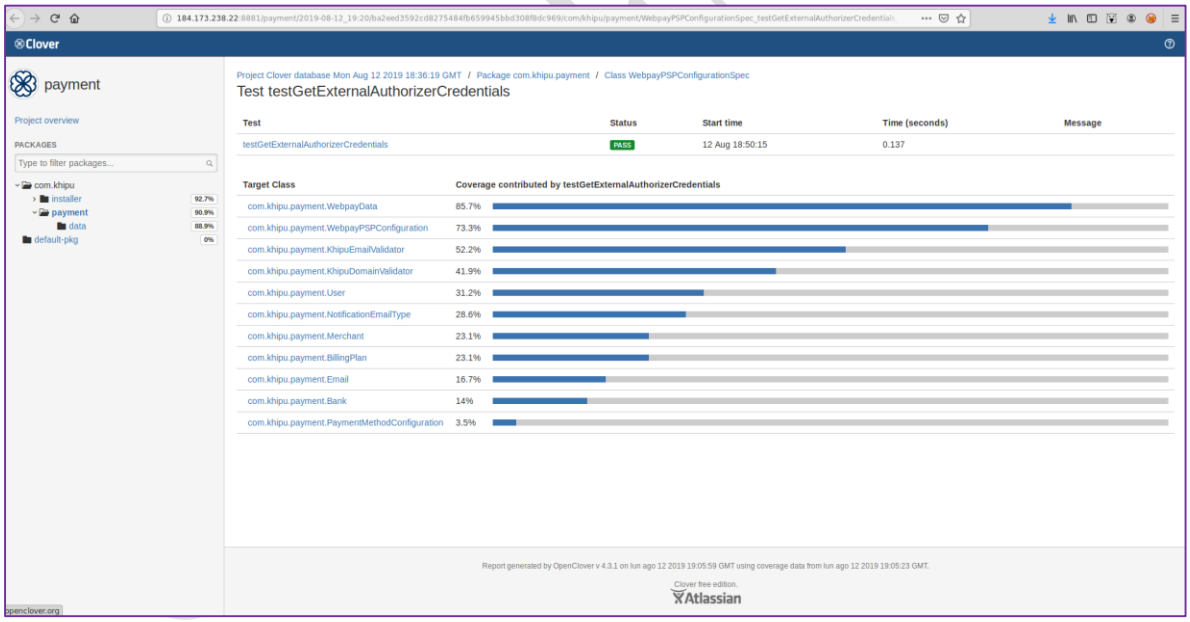
Durante el análisis de los puertos y servicios se ha detectado que la dirección IP 184.173.238.22 en particular en el puerto 8881 cuenta con un listado de directorios los cuales contienen diversa información y pruebas realizadas a la aplicación khipu durante su desarrollo, si bien son archivos de pruebas esta información puede mal utilizarse por parte de un atacante para entender cómo funciona la aplicación, lo cual puede ser considerado un riego, se recomienda filtrar el puerto mencionado o limitar el acceso al listado de directorios.

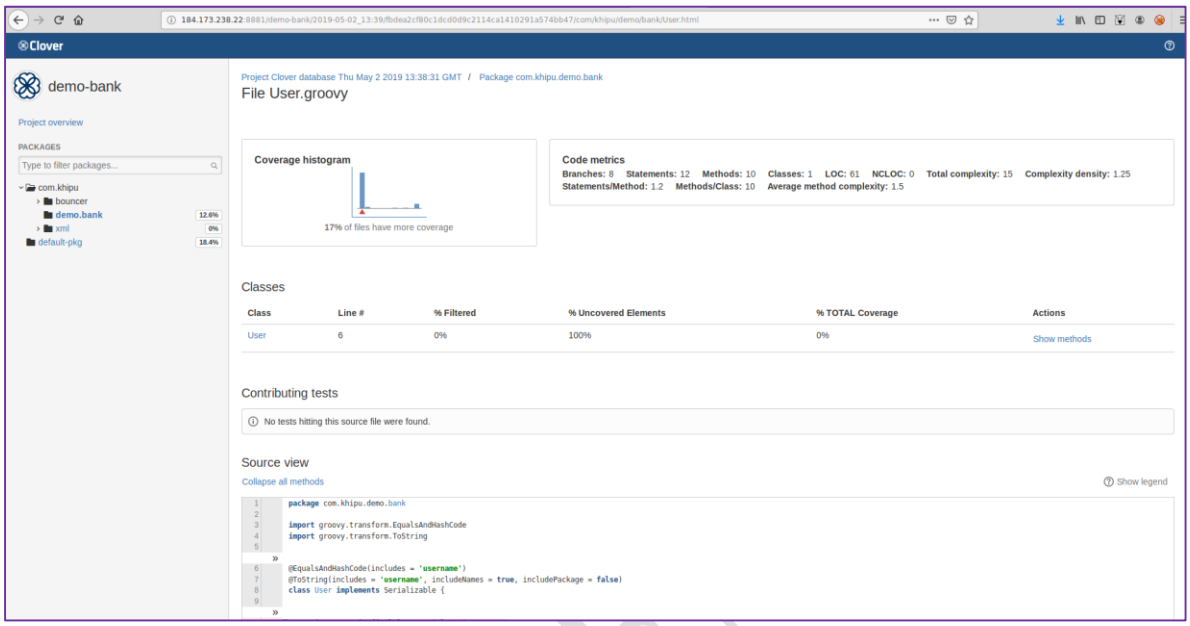
CONFIDENCIAL

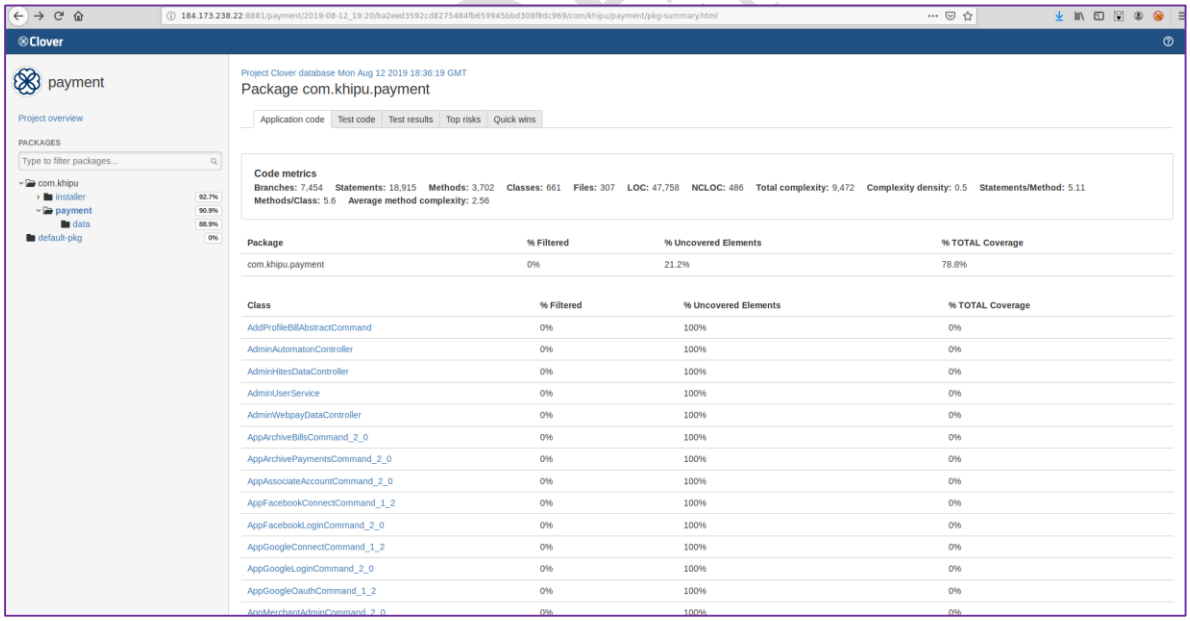
Evidencias:

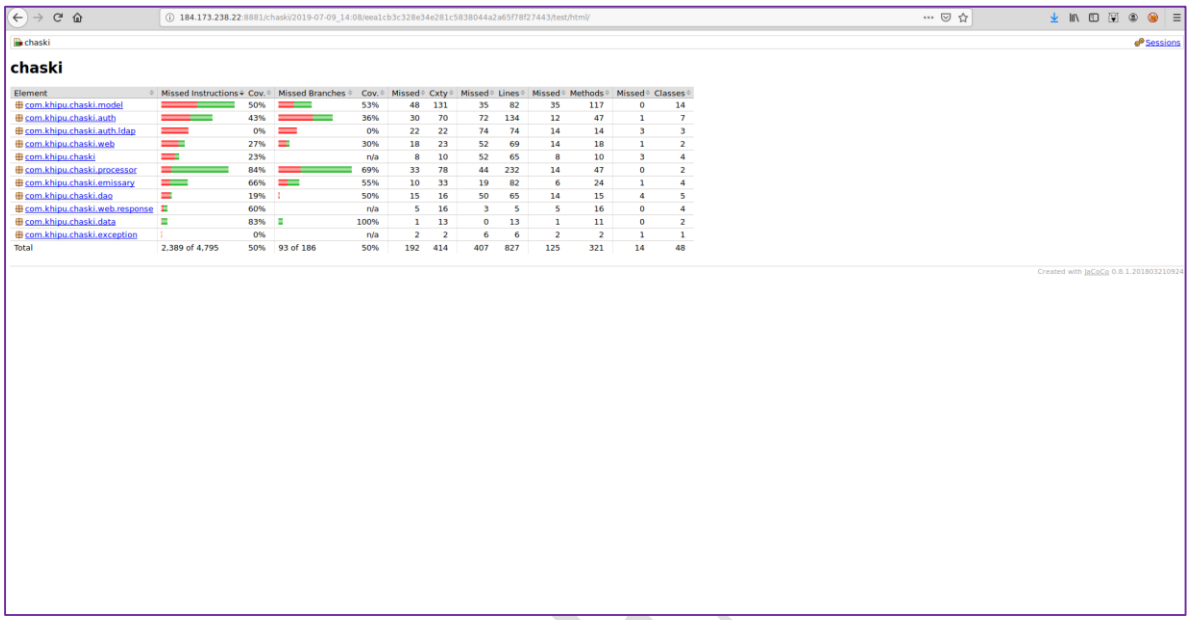

184.173.238.22:8881
Index of /
Name Last modified Size Description
README.md 2019-02-12 21:32 565
automataserver/ 2019-07-31 22:19 -
b2app-backend/ 2019-08-12 22:25 -
bitbucket-pipelines.yml 2019-02-12 21:32 1.0K
calendar-client/ 2019-02-12 21:32 -
cerebro/ 2019-08-12 23:25 -
chaski/ 2019-07-09 16:09 -
croupier/ 2019-07-24 18:16 -
date.txt 2019-02-12 21:32 116
demo-bank/ 2019-05-02 15:42 -
khashier/ 2019-07-24 17:16 -
khuruvi/ 2019-08-13 00:25 -
kmatching/ 2019-06-19 18:02 -
logback-jsonlayout/ 2019-02-12 21:32 -
mixer/ 2019-07-25 20:17 -
payment/ 2019-08-12 21:25 -
pipes-audit/ 2019-07-24 15:16 -
pipes/ 2019-08-08 20:23 -
plumbing-mail/ 2019-07-18 00:13 -
plumbing-rmq/ 2019-07-17 23:13 -
rabbitmq-connector/ 2019-07-17 20:13 -
snow/ 2019-07-25 19:17 -
Apache/2.4.29 (Ubuntu) Server at 184.173.238.22 Port 8881


Clover
demo-bank
Project overview
PACKAGES
Type to filter packages...
com.khipu
bouncer
demo.bank 12.6%
xml 0%
default-pkg 18.4%
package com.khipu.demo.bank
import groovy.transform.EqualsAndHashCode
import groovy.transform.ToString
@EqualsAndHashCode(includes = 'username')
@ToString(includes = 'username', includeNames = true, includePackage = false)
class User implements Serializable {
private static final long serialVersionUID = 1
transient springSecurityService
String username
String password
boolean enabled = true
boolean accountExpired
boolean accountLocked
boolean passwordExpired
Date dateCreated
Date lastUpdated
User(String username, String password) {
this()
this.username = username
this.password = password
}
Set<Role> getAuthorities() {
UserRole.findAllByUser(this)*.role
}
def beforeInsert() {
encodePassword()
}
def beforeUpdate() {
if (isDirty('password')) {
encodePassword()
}


184.173.238.22:8881/payment/2019-08-12_19:20/ba2eed3592cd8275484fb659945bbd308f8dc969/com/khipu/payment/WebpayPSPConfigurationSpec_testGetExternalAuthorizerCredentials
Clover
payment
Project overview
PACKAGES
Type to filter packages...
com.khipu
installer 92.7%
payment 90.9%
data 88.9%
default-pkg 0%
Project Clover database Mon Aug 12 2019 18:36:19 GMT / Package com.khipu.payment / Class WebpayPSPConfigurationSpec
Test testGetExternalAuthorizerCredentials
Test | Status | Start time | Time (seconds) | Message
testGetExternalAuthorizerCredentials | PASS | 12 Aug 18:50:15 | 0.137
Target Class | Coverage contributed by testGetExternalAuthorizerCredentials
com.khipu.payment.WebpayData 85.7%
com.khipu.payment.WebpayPSPConfiguration 73.3%
com.khipu.payment.KhipuEmailValidator 52.2%
com.khipu.payment.KhipuDomainValidator 41.9%
com.khipu.payment.User 31.2%
com.khipu.payment.NotificationEmailType 28.6%
com.khipu.payment.Merchant 23.1%
com.khipu.payment.BillingPlan 23.1%
com.khipu.payment.Email 16.7%
com.khipu.payment.Bank 14%
com.khipu.payment.PaymentMethodConfiguration 3.5%
Report generated by OpenClover v 4.3.1 on lun ago 12 2019 19:05:59 GMT using coverage data from lun ago 12 2019 19:05:23 GMT.
Clover free edition.
Atlassian
openclover.org


Clover
demo-bank
Project overview
PACKAGES
Type to filter packages...
com.khipu
bouncer
demo.bank 12.6%
xml 0%
default-pkg 18.4%
Project Clover database Thu May 2 2019 13:38:31 GMT / Package com.khipu.demo.bank
File User.groovy
Coverage histogram
17% of files have more coverage
Code metrics
Branches: 8 Statements: 12 Methods: 10 Classes: 1 LOC: 61 NCLOC: 0 Total complexity: 15 Complexity density: 1.25
Statements/Method: 1.2 Methods/Class: 10 Average method complexity: 1.5
Classes
Class | Line # | % Filtered | % Uncovered Elements | % TOTAL Coverage | Actions
User | 6 | 0% | 100% | 0% | Show methods
Contributing tests
No tests hitting this source file were found.
Source view
Collapse all methods
Show legend
package com.khipu.demo.bank
import groovy.transform.EqualsAndHashCode
import groovy.transform.ToString
@EqualsAndHashCode(includes = 'username')
@ToString(includes = 'username', includeNames = true, includePackage = false)
class User implements Serializable {


Clover
payment
Project overview
PACKAGES
Type to filter packages...
com.khipu
installer 92.7%
payment 90.9%
data 88.9%
default-pkg 0%
Project Clover database Mon Aug 12 2019 18:36:19 GMT
Package com.khipu.payment
Application code
Test code
Test results
Top risks
Quick wins
Code metrics
Branches: 7,454 Statements: 18,915 Methods: 3,702 Classes: 661 Files: 307 LOC: 47,758 NCLOC: 486 Total complexity: 9,472 Complexity density: 0.5 Statements/Method: 5.11
Methods/Class: 5.6 Average method complexity: 2.56
Package | % Filtered | % Uncovered Elements | % TOTAL Coverage
com.khipu.payment | 0% | 21.2% | 78.8%
Class | % Filtered | % Uncovered Elements | % TOTAL Coverage
AddProfileBillAbstractCommand | 0% | 100% | 0%
AdminAutomatonController | 0% | 100% | 0%
AdminHitesDataController | 0% | 100% | 0%
AdminUserService | 0% | 100% | 0%
AdminWebpayDataController | 0% | 100% | 0%
AppArchiveBillsCommand_2_0 | 0% | 100% | 0%
AppArchivePaymentsCommand_2_0 | 0% | 100% | 0%
AppAssociateAccountCommand_2_0 | 0% | 100% | 0%
AppFacebookConnectCommand_1_2 | 0% | 100% | 0%
AppFacebookLoginCommand_2_0 | 0% | 100% | 0%
AppGoogleConnectCommand_1_2 | 0% | 100% | 0%
AppGoogleLoginCommand_2_0 | 0% | 100% | 0%
AppGoogleOauthCommand_1_2 | 0% | 100% | 0%



184.173.238.22:8881/chaski/2019-07-09_14:08/eea1cb3c328e34e281c5838044a2a65f78f27443/test/html/

chaski

Sessions

chaski

Element	Missed Instructions +	Cov.	Missed Branches	Cov.	Missed	Cxty	Missed	Lines	Missed	Methods	Missed	Classes
com.khipu.chaski.model		50%		53%	48	131	35	82	35	117	0	14
com.khipu.chaski.auth		43%		36%	30	70	72	134	12	47	1	7
com.khipu.chaski.auth.ldap		0%		0%	22	22	74	74	14	14	3	3
com.khipu.chaski.web		27%		30%	18	23	52	69	14	18	1	2
com.khipu.chaski		23%		n/a	8	10	52	65	8	10	3	4
com.khipu.chaski.processor		84%		69%	33	78	44	232	14	47	0	2
com.khipu.chaski.emissary		66%		55%	10	33	19	82	6	24	1	4
com.khipu.chaski.dao		19%		50%	15	16	50	65	14	15	4	5
com.khipu.chaski.web.response		60%		n/a	5	16	3	5	5	16	0	4
com.khipu.chaski.data		83%		100%	1	13	0	13	1	11	0	2
com.khipu.chaski.exception		0%		n/a	2	2	6	6	2	2	1	1
Total	2.389 of 4,795	50%	93 of 186	50%	192	414	407	827	125	321	14	48

Created with JaCoCo 0.8.1.201803210924

CONFIDE

5 Análisis SSL

A continuación, se lista el detalle del análisis de cada certificado con sus respectivas propiedades y debilidades.

5.1 dev.khipu.com

Host / IP / Puerto	16.ee.adb8.ip4.static.sl-reverse.com./ 184.173.238.22/ 443
Expiración	27/12/2019
Válido para	dev.khipu.com www.dev.khipu.com
Información Adicional	Huella SHA256 **4A6364F0817D55D4C140828C16E711246D0FFBF0B041F55E2C5F3C9F33FB5B57** Nombres Comunes **dev.khipu.com** Nombres Alternativos **dev.khipu.com www.dev.khipu.com**

Vulnerabilidad	Identificador	Estado	Observaciones
Heartbleed	CVE-2014-0160	✓	No vulnerable
CCS	CVE-2014-0224	✓	No vulnerable
Ticketbleed	CVE-2016-9244	✓	No vulnerable
ROBOT	CVE-2017-17382	✓	No vulnerable
Secure Renegotiation	CVE-2009-3555	✓	No vulnerable
Secure Client-Initiated Renegotiation	CVE-2011-1473	✓	No vulnerable

CRIME	CVE-2012-4929	✓	No vulnerable
BREACH	CVE-2013-3587	✓	No vulnerable
POODLE	CVE-2014-3566	✓	No vulnerable
TLS_FALLBACK_SCSV	RFC 7507	✓	No vulnerable
SWEET32	CVE-2016-2183	✓	No vulnerable
FREAK	CVE-2015-0204	✓	No vulnerable
DROWN	CVE-2016-0703	✓	No vulnerable
LOGJAM	CVE-2015-4000	✓	No vulnerable
BEAST	CVE-2011-3389	✗	Potencialmente Vulnerable
LUCKY13	CVE-2013-0169	✓	No vulnerable
RC4	CVE-2013-2566 CVE-2015-2808	✓	No vulnerable

CONFI

5.2 khipu.com

Host / IP / Puerto	12.59.1632.ip4.static.sl-reverse.com / 50.22.89.18 / 443
Expiración	28/01/2021
Válido para	khipu.com www.khipu.com
Información Adicional	Huella SHA256 **1958D3CEF2160C7D7DC0DA34CF189E088CB5911B3A7193C9807C222538365AC8** Nombres Comunes **khipu.com** Nombres Alternativos **khipu.com www.khipu.com**

Vulnerabilidad	Identificador	Estado	Observaciones
Heartbleed	CVE-2014-0160	✓	No vulnerable
CCS	CVE-2014-0224	✓	No vulnerable
Ticketbleed	CVE-2016-9244	✓	No vulnerable
ROBOT	CVE-2017-17382	✓	No vulnerable
Secure Renegotiation	CVE-2009-3555	✓	No vulnerable
Secure Client-Initiated Renegotiation	CVE-2011-1473	✓	No vulnerable
CRIME	CVE-2012-4929	✓	No vulnerable
BREACH	CVE-2013-3587	✗	**Potencialmente Vulnerable**
POODLE	CVE-2014-3566	✓	No vulnerable

TLS_FALLBACK_SCSV	RFC 7507	✓	No vulnerable
SWEET32	CVE-2016-2183	✓	No vulnerable
FREAK	CVE-2015-0204	✓	No vulnerable
DROWN	CVE-2016-0703	✓	No vulnerable
LOGJAM	CVE-2015-4000	✓	No vulnerable
BEAST	CVE-2011-3389	✗	**Potencialmente Vulnerable**
LUCKY13	CVE-2013-0169	✓	No vulnerable
RC4	CVE-2013-2566 CVE-2015-2808	✓	No vulnerable

La implementación de SSL/TLS para el dominio dev.khipu.com y khipu.com se encuentra con un nivel óptimo, si bien se detectaron nuevamente vulnerabilidades como BREACH y BEAST estos por su complejidad y falta de “exploits” conocidos se consideran potencialmente vulnerables ya que su reproducción es de alta complejidad.

CONFIDE

Adicionalmente se detectó que 4 subdominios que utilizan un certificado válido para otros dominios.

Dirección IP	Dominios	Válido para
50.22.111.181	kh04.khipu.com	khipu.com www.khipu.com
50.22.111.178	Kh10.khipu.com	khipu.com www.khipu.com
50.22.111.179	kh09.khipu.com	khipu.com www.khipu.com
184.173.238.22	Kh08.khipu.com	dev.khipu.com www.dev.khipu.com

CONFIDENCIAL

6 Recomendaciones generales

En términos generales, el perímetro de kiphu.com mantiene un acotado número de puertos y servicios expuestos a internet.

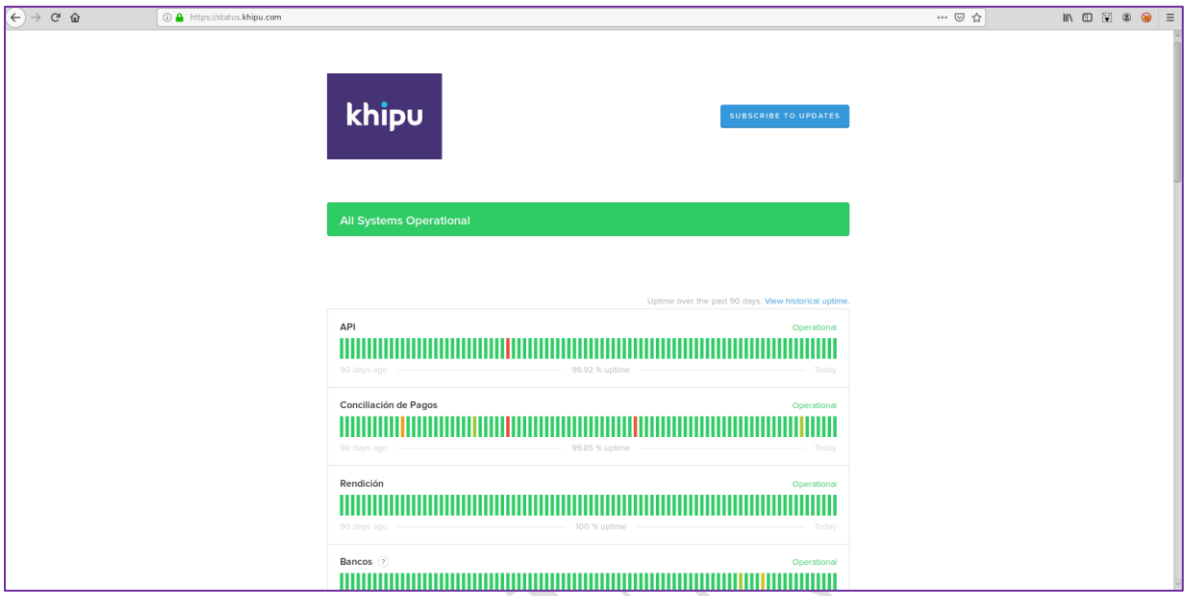
Se ha detectado que el subdominio en este nuevo análisis que kh08.khipu.com usa un certificado valido para otro sitio (dev.khipu.com) por lo que el navegador alerta de que la conexión se considera insegura y niega el acceso, es necesario modificar el certificado implementado en este subdominio para evitar problemas de seguridad.

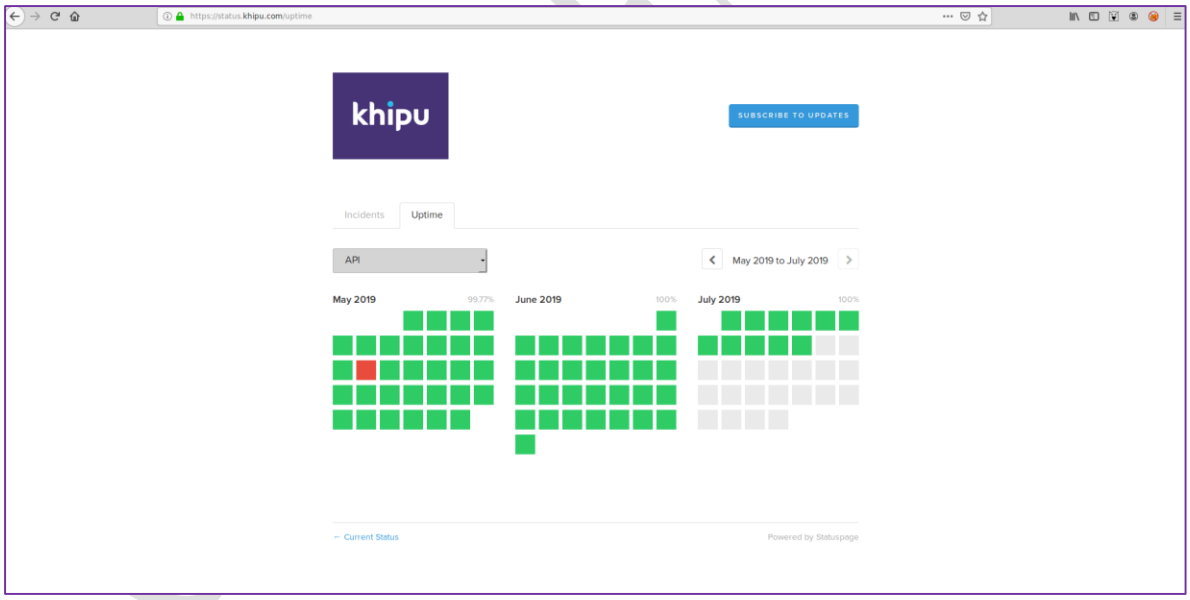
Fue posible detectar 4 nuevos sub-dominios (stress.khipu.com) (dev.whmcs.khipu.com) (www.magic.khipu.com) y (easytaxitopup.khipu.com) los cuales no se encuentran activos.Se recomienda comprobar si estos dominios pertenecen a khipu.

En temas de la implementación SSL el certificado implementado en dev.khipu.com y en khipu.com, se detectó que son potencialmente vulnerables al ataque de BEAST, se recomienda para mitigar este problema no hacer uso ni ofrecer el protocolo TLS 1.0. También fue posible detectar que el certificado de khipu.com es potencialmente vulnerable a BREACH, se recomienda deshabilitar la compresión HTTP. Se recomienda también en ambos certificados SSL hacer uso del protocolo más reciente que se encuentra disponible TLS 1.3

Durante el análisis también fue posible detectar nuevamente el dominio https://status.khipu.com/ un servicio web del “uptime” de algunos de los sistemas de khipu, se recomienda validar si este sistema debe estar expuesto a internet.

CONFIDENCIAL





Evidencias de la url status.khipu.com

Referencias

http://breachattack.com/

https://kb.iweb.com/hc/es/articles/230268628-Vulnerabilidades-SSL-TLS-Ataques-POODLE-BEAST-SWEET32-y-la-muerte-de-SSLv3-Aviso-de-Seguridad-Open-SSL

https://www.wolfssl.com/docs/tls13

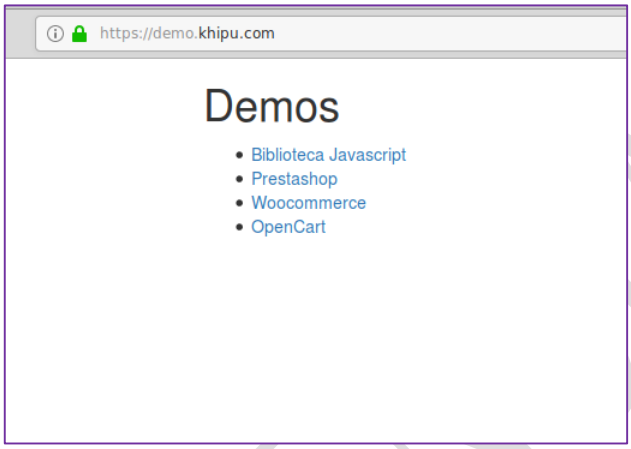
Por último, se detectaron nuevamente aplicaciones instaladas sobre el servidor demo.khipu.com estas aplicaciones se encuentran expuestas a internet sin mantenimiento alguno, esto se considera un riesgo de seguridad y podrían manchar la imagen de khipu como organización si un atacante logra ejecutar un ataque sobre estos aplicativos. Se realizó una nueva prueba de seguridad sobre estos sistemas logrando ejecutar la misma vulnerabilidad de manera exitosa el ataque de Cross-Site Scripting (XSS) en uno de los procesos de pago de prueba.

Referencias

https://www.owasp.org/index.php/Cross-site_Scripting_(XSS)

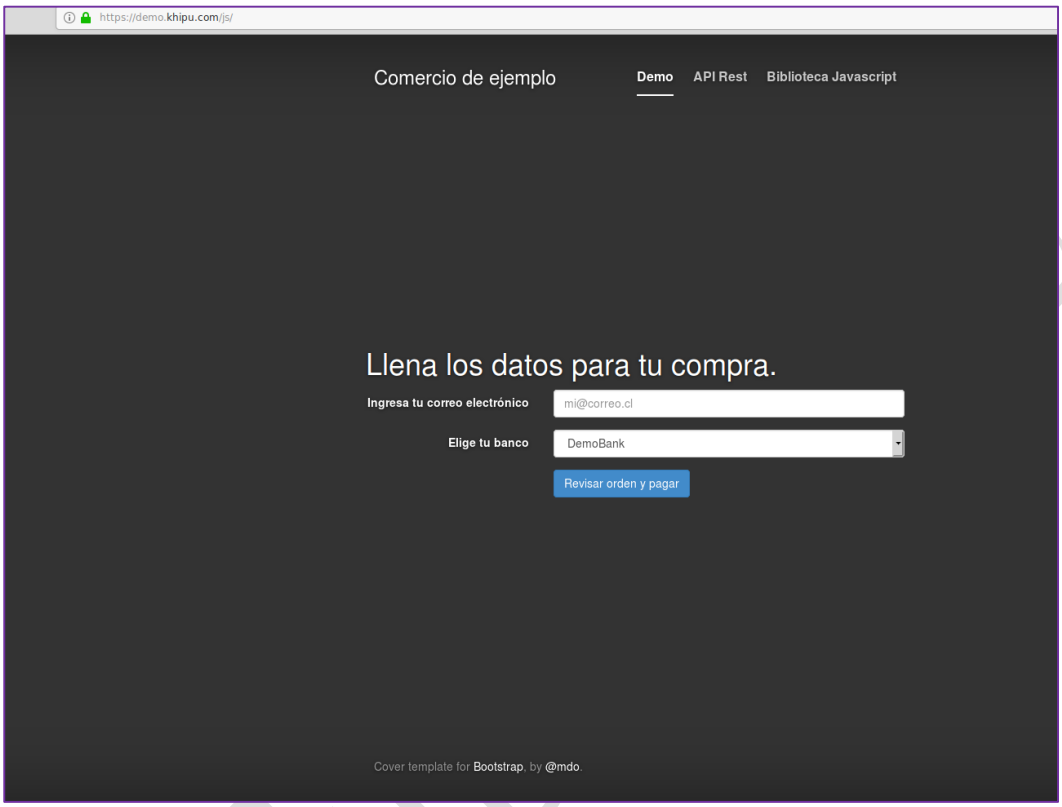
CONFIDENCIAL

A continuación, se detallan las evidencias:



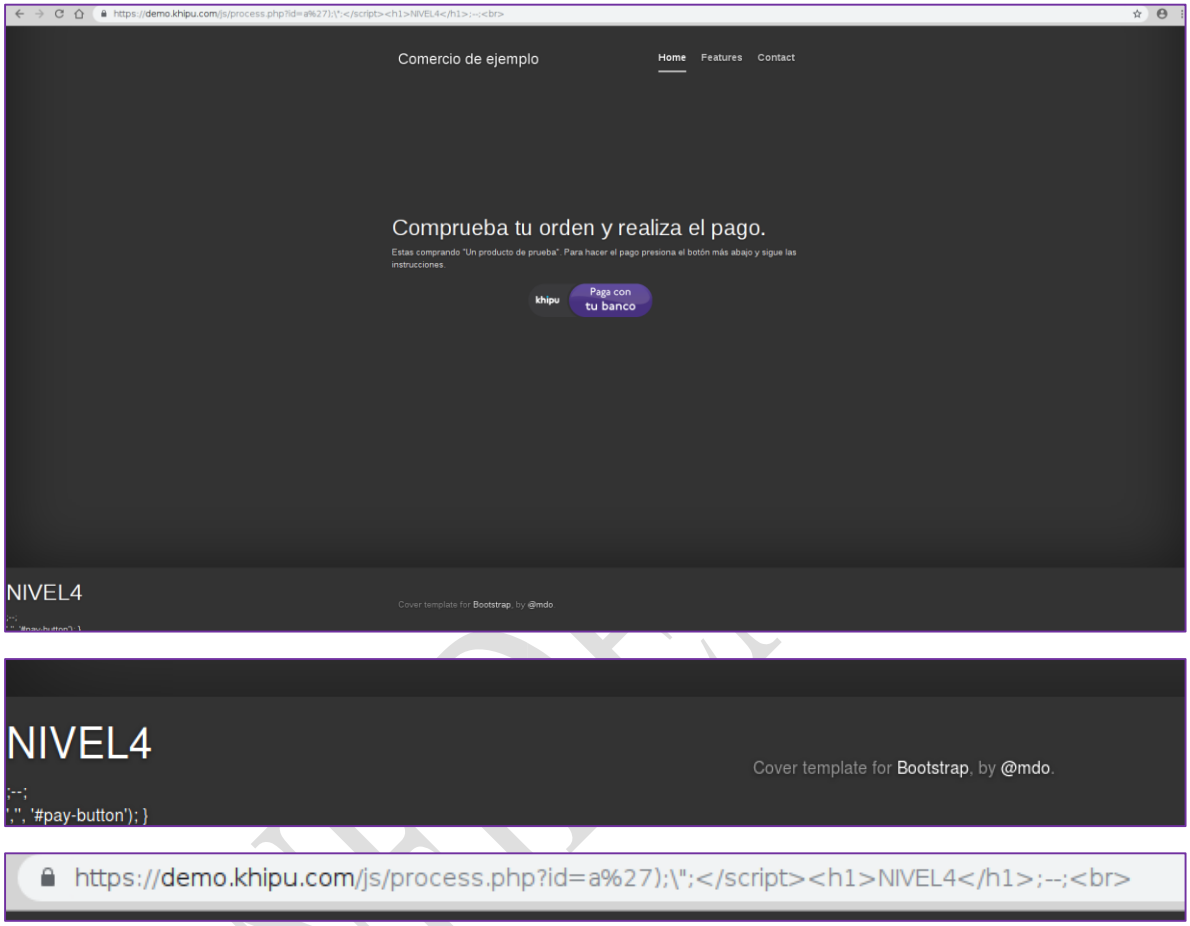
Url de las aplicaciones expuestas a internet demo.khipu.com

CONFIDENCIAL



Aplicación afectada por ataque de Cross-site Scripting (XSS)

CONFI



Ataque de Cross-site Scripting (XSS) ejecutado con éxito