From WAF to RASP

Gorka Vicente

Gorka Vicente

co-founder at Hdiv Security & COO

Hdiv

@gorkavicente

hdivsecurity.com

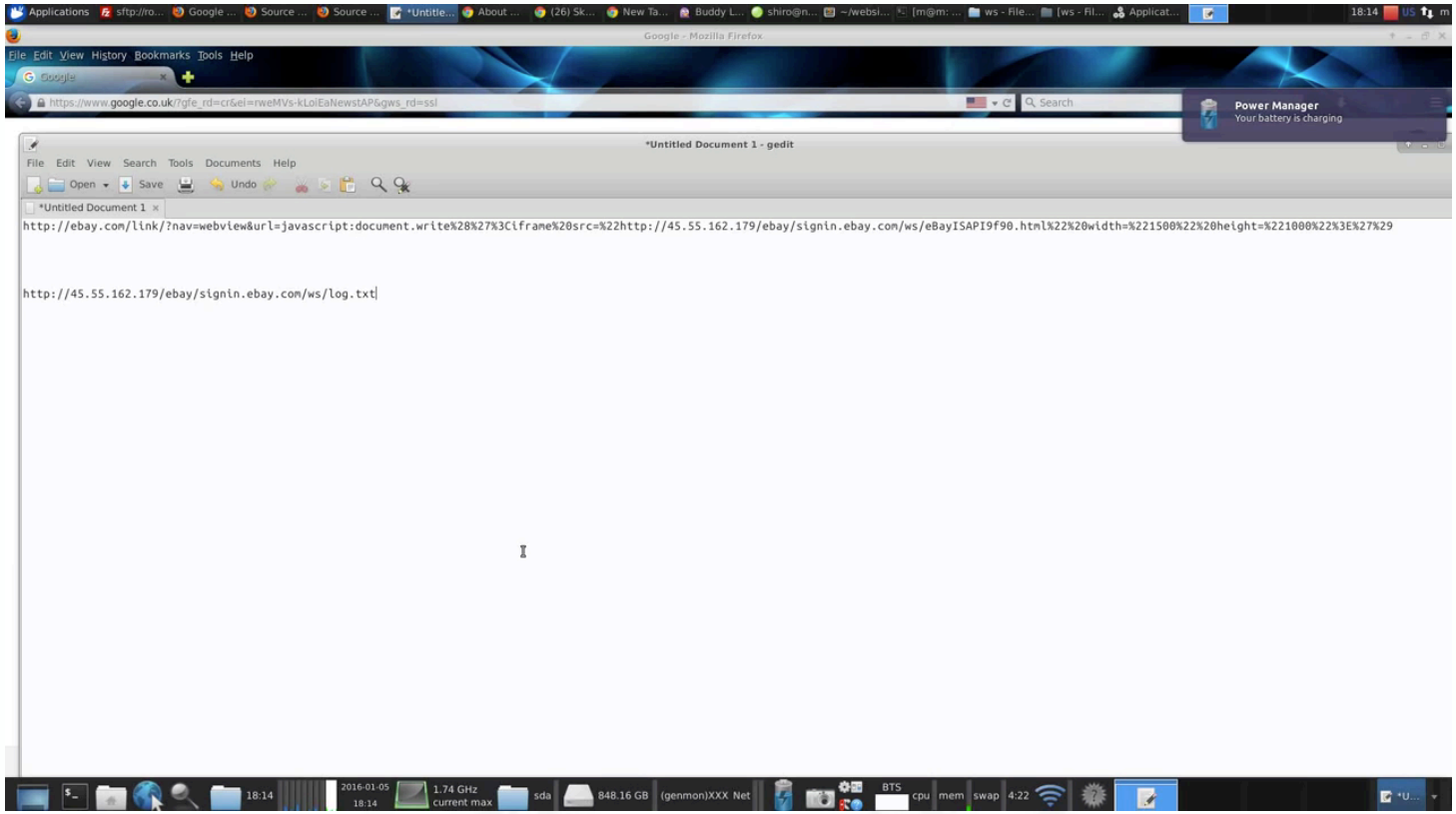
Simple Yet Effective eBay Bug Allows Hackers to Steal Passwords

Monday, January 11, 2016

> *This is a common web bug, technically known as a **Cross-Site Scripting (XSS) vulnerability**, in which attackers can exploit the vulnerability to inject malicious lines of code into a legitimate website.*
>
> **Swati Khandelwal**

The Hacker News™
Security in a serious way

http://thehackernews.com/2016/01/ebay-hacking.html



The Hacker News™
Security in a serious way

http://thehackernews.com/2016/01/ebay-hacking.html

threatpost
The Kaspersky Lab Security News Service

September 11, 2015

RESEARCHERS OUTLINE VULNERABILITIES IN YAHOO, PAYPAL, MAGENTO APPS

YAHOO! PayPal Magento eCommerce Platform for Growth

> *Another issue the researchers brought up existed in Gemini,* **Yahoo's marketplace** *for mobile and native ads. If exploited the* ***Cross Site Request Forgery (CSRF) bug*** *could have enabled an attacker to inject malicious code to compromise client-side app to browser requests, along with session data.*

https://threatpost.com/researchers-outline-vulnerabilities-in-yahoo-paypal-magento-apps/114644/

Exposed database allowed read/write access to Microsoft's career portal

February 13, 2016

Microsoft

Configuration errors *exposed data and enabled full control over the website's HTML.*

CSO

http://www.csoonline.com/article/3033154/security/exposed-database-allowed-read-write-access-to-microsofts-career-portal.html

SAP patches three-year-old vulnerability, plus 20 more flaws

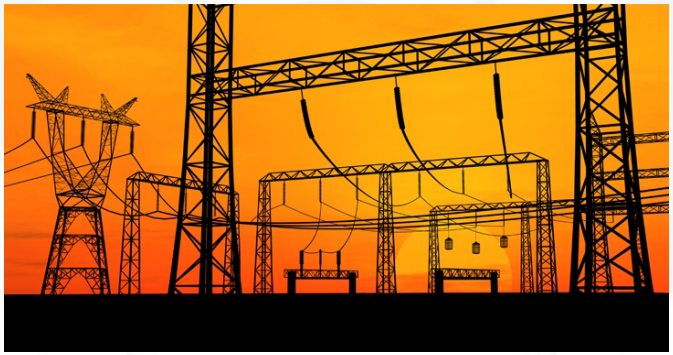
June 16, 2016

> *The 21 total vulnerabilities, four of which were critical, were categorized as follows: five **cross-site scripting**, five **missing authorization**, four **implementation flaws**, two **denial of service**, two **directory traversals**, one **code injection**, one XML external entity, one information disclosure.*

http://www.scmagazine.com/sap-patches-three-year-old-vulnerability-plus-20-more-flaws/article/503720/

Israeli Power Grid Authority Suffers Massive Cyber Attack

January 27, 2016



The Hacker News™
Security in a serious way

http://thehackernews.com/2016/01/power-grid-cyberattack.html

Applications and data are the focus of modern cyber attacks

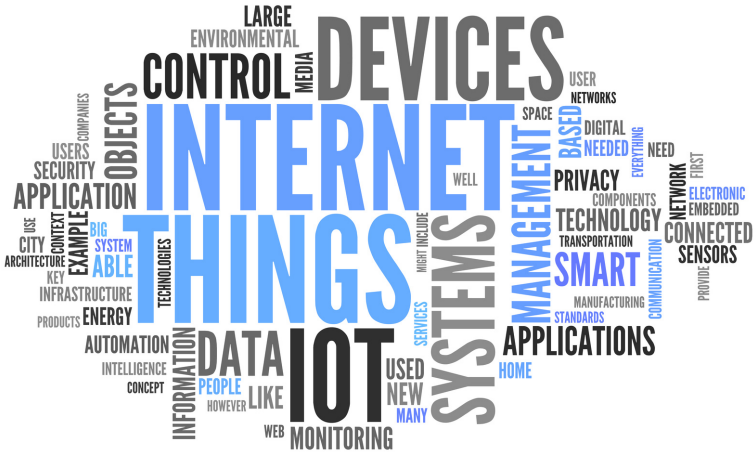
In 2015, companies saw an average of 160 successful cyber attacks per week, more than three times the 2010 average of 50 per week.

Gartner®

***Web app attacks* represented *40% of breaches* in 2015**

WhiteHat SECURITY

WEB APPLICATIONS SECURITY STATISTICS REPORT 2016



> **86%** of all websites tested had at least **1 serious vulnerability**

WhiteHat SECURITY






Agenda

1. El problema
2. **El porqué**
3. **Soluciones de Seguridad**
4. **Sumario**

Las ***tecnologías*** actuales para el desarrollo de aplicaciones son **inseguras por defecto**

La **seguridad** depende de las **personas**

Las **soluciones de seguridad** *no están resolviendo* el **problema**.

Agenda

1. El problema
2. El porqué
3. **Soluciones de Seguridad**
4. **Sumario**

WAF

Web Application Firewall

¿Qué son?

Dispositivos hardware o software que **analizan el tráfico HTTP y permiten proteger los servidores de aplicaciones** de los ataques a nivel de aplicación (XSS, CSRF, SQL Injection, etc.)

WAF - 1ª generación

Basados en ***detectar patrones de ataque***

WAF - 1ª generación

Basados en ***detectar patrones de ataque***

Todas las peticiones son aceptadas;
excepto las definidas como ***blacklist***.

Protección frente a OWASP TOP 10

OWASP Open Web Application Security Project		WAF *1ª generación*
A1	Injection	✓✗
A2	Broken authentication and session management	✓
A3	XSS	✓✗
A4	Insecure direct object reference	✗
A5	Security misconfiguration	✓✗
A6	Sensitive data exposure	✓✗
A7	Missing function level access control	✗
A8	CSRF	✓✗
A9	Using components with known vulnerabilities	✓✗
A10	Unvalidated redirects and forwards	✗

NIVEL DE PROTECCIÓN **40%**

https://www.owasp.org/index.php/Top_10_2013-Top_10

Protección frente a OWASP TOP 10

OWASP Open Web Application Security Project		WAF *1ª generación*
A1	Injection	✓✗
A2	Broken authentication and session management	✓
A3	XSS	✓✗
A4	Insecure direct object reference	✗
A5	Security misconfiguration	✓✗
A6	Sensitive data exposure	✓✗
A7	Missing function level access control	✗
A8	CSRF	✓✗
A9	Using components with known vulnerabilities	✓✗
A10	Unvalidated redirects and forwards	✗

Vulnerabilidades comunes
Security bugs

NIVEL DE PROTECCIÓN **58%**

https://www.owasp.org/index.php/Top_10_2013-Top_10

Protección frente a OWASP TOP 10

OWASP Open Web Application Security Project		WAF 1ª generación
A1	Injection	⛓
A2	Broken authentication and session management	✓
A3	XSS	⛓
A4	Insecure direct object reference	✗
A5	Security misconfiguration	⛓
A6	Sensitive data exposure	⛓
A7	Missing function level access control	✗
A8	CSRF	⛓
A9	Using components with known vulnerabilities	⛓
A10	Unvalidated redirects and forwards	✗

Vulnerabilidades de negocio

NO siguen un **PATRÓN DE ATAQUE**

NIVEL DE PROTECCIÓN **0%**

https://www.owasp.org/index.php/Top_10_2013-Top_10

WAF - 1ª generación

Inconvenientes

- **No protegen frente a todos los riesgos**
- No cubren los riesgos por conocer (*zero-days*)
- Falsos positivos
- Rendimiento

WAF - 1ª generación

Inconvenientes

- No protegen frente a todos los riesgos
- No cubren los riesgos por conocer (*zero-days*)
- Falsos positivos
- Rendimiento

WAF - 1ª generación

Inconvenientes

- No protegen frente a todos los riesgos
- No cubren los riesgos por conocer (*zero-days*)
- Falsos positivos
- Rendimiento

WAF - 1ª generación

Inconvenientes

- No protegen frente a todos los riesgos
- No cubren los riesgos por conocer (*zero-days*)
- Falsos positivos
- Rendimiento

WAF - 2ª generación

Basados ***whitelist + blacklist***

WAF - 2ª generación

Basados ***whitelist + blacklist***

1. **Procesos de aprendizaje**

WAF - 2ª generación

Basados ***whitelist + blacklist***

1. **Procesos de aprendizaje**
2. **Parseo de contenido en tiempo real**

WAF - 2ª generación

Basados ***whitelist + blacklist***

1. **Procesos de aprendizaje**
2. **Parseo de contenido en tiempo real**

No es posible aprender contenidos dinámicos

Protección frente a OWASP TOP 10

OWASP Open Web Application Security Project		WAF *1ª generación*	WAF *2ª generación*
A1	Injection	✓✗	✓✗
A2	Broken authentication and session management	✓	✓
A3	XSS	✓✗	✓✗
A4	Insecure direct object reference	✗	✓
A5	Security misconfiguration	✓✗	✓✗
A6	Sensitive data exposure	✓✗	✓✗
A7	Missing function level access control	✗	✓
A8	CSRF	✓✗	✓
A9	Using components with known vulnerabilities	✓✗	✓✗
A10	Unvalidated redirects and forwards	✗	✓
NIVEL DE PROTECCIÓN		**40%**	**75%**

https://www.owasp.org/index.php/Top_10_2013-Top_10

Protección frente a OWASP TOP 10

OWASP Open Web Application Security Project		WAF *1ª generación*	WAF *2ª generación*
A1	Injection	✗	✗
A2	Broken authentication and session management	✓	✓
A3	XSS	✗	✗
A4	Insecure direct object reference	✗	✓
A5	Security misconfiguration	✗	✗
A6	Sensitive data exposure	✗	✗
A7	Missing function level access control	✗	✓
A8	CSRF	✗	✓
A9	Using components with known vulnerabilities	✗	✗
A10	Unvalidated redirects and forwards	✗	✓
NIVEL DE PROTECCIÓN		**0%**	**100%**

https://www.owasp.org/index.php/Top_10_2013-Top_10

Teniendo estos niveles de ***protección***,

¿por qué nuestras apps siguen siendo vulnerables?

WAF - 2ª generación

Inconvenientes

Falsos positivos

Costo de implantación

¿Por qué no **hacer** las **apps seguras**?

¡No esperemos a que alguien tenga que venir después a protegerlas!

> *Stop Protecting Your Apps;*
> *It's Time for Apps to Protect Themselves*

Gartner, Inc. Maveric Research: Stop Protecting Your Apps; It's Time for Apps to Protect Themselves, 25th September 2014 by Joseph Feiman

Gartner®

RASP

Runtime Application Self Protection

Detección + Protección

de vulnerabilidades ***mediante acciones proactivas***

Evolución de los AST (*Application Security Testing*)

Los AST son herramientas que ayudan a los desarrolladores a encontrar vulnerabilidades en código fuente pero no automatizan la creación de aplicaciones seguras.

RASP

Runtime Application Self Protection

Efectivos para *detectar y proteger* sobre las vulnerabilidades comunes

A1	**Injection**
A2	Broken authentication and session management
A3	**XSS**
A4	Insecure direct object reference
A5	Security misconfiguration
A6	Sensitive data exposure
A7	Missing function level access control
A8	CSRF
A9	Using components with known vulnerabilities
A10	Unvalidated redirects and forwards

RASP

Runtime Application Self Protection

Efectivos para ***detectar y proteger*** sobre las vulnerabilidades comunes

NO *protegen* frente a vulnerabilidades de negocio

	A1	**Injection**
	A2	Broken authentication and session management
	A3	**XSS**
✗	A4	**Insecure direct object reference**
	A5	Security misconfiguration
	A6	Sensitive data exposure
✗	A7	**Missing function level access control**
	A8	CSRF
	A9	Using components with known vulnerabilities
✗	A10	**Unvalidated redirects and forwards**

Aunque el **enfoque** es ***interesante***, los RASP actuales **no están solventando el problema.**

No controlan el tráfico HTTP entre peticiones (*arquitectura sin estado*)

Es **necesario** controlar el
flujo completo de los datos
con un enfoque diferente al de los WAF

Tecnologías de Desarrollo

Ciberseguridad


ANGULARJS by Google
Microsoft .NET
php
Java
Security By Design
Tecnologías de Desarrollo
Ciberseguridad

Security by Design

Seguridad dentro de las apps (embedded security)

Eliminación de los **procesos de aprendizaje** y el **parseo de contenido**

Integración durante la **fase de Desarrollo**.

Protección frente a OWASP TOP 10

OWASP Open Web Application Security Project		RASP
A1	Injection	✓
A2	Broken authentication and session management	✓
A3	XSS	✓
A4	Insecure direct object reference	✓
A5	Security misconfiguration	✓/✗
A6	Sensitive data exposure	✓/✗
A7	Missing function level access control	✓
A8	CSRF	✓
A9	Using components with known vulnerabilities	✓/✗
A10	Unvalidated redirects and forwards	✓

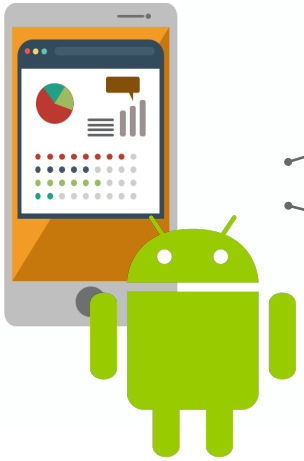
NIVEL DE PROTECCIÓN **85%**

Protección frente a OWASP TOP 10

OWASP Open Web Application Security Project		RASP	WAF *1ª generación*	WAF *2ª generación*
A1	Injection	✓	✓✗	✓✗
A2	Broken authentication and session management	✓	✓	✓
A3	XSS	✓	✓✗	✓✗
A4	Insecure direct object reference	✓	✗	✓
A5	Security misconfiguration	✓✗	✓✗	✓✗
A6	Sensitive data exposure	✓✗	✓✗	✓✗
A7	Missing function level access control	✓	✗	✓
A8	CSRF	✓	✓✗	✓
A9	Using components with known vulnerabilities	✓✗	✓✗	✓✗
A10	Unvalidated redirects and forwards	✓	✗	✓
NIVEL DE PROTECCIÓN		**85%**	**40%**	**75%**

	RASP	WAF *2ª generación*
Instalación y Mantenimiento	1 día	Varias semanas
Latencia	1-3 ms.	< 5 ms
Portabilidad	✓	-
Forma de reportar el error en la aplicación	✓	-
Plataformas	Dependiente de tecnología	Independiente
Entornos	Todos	Producción

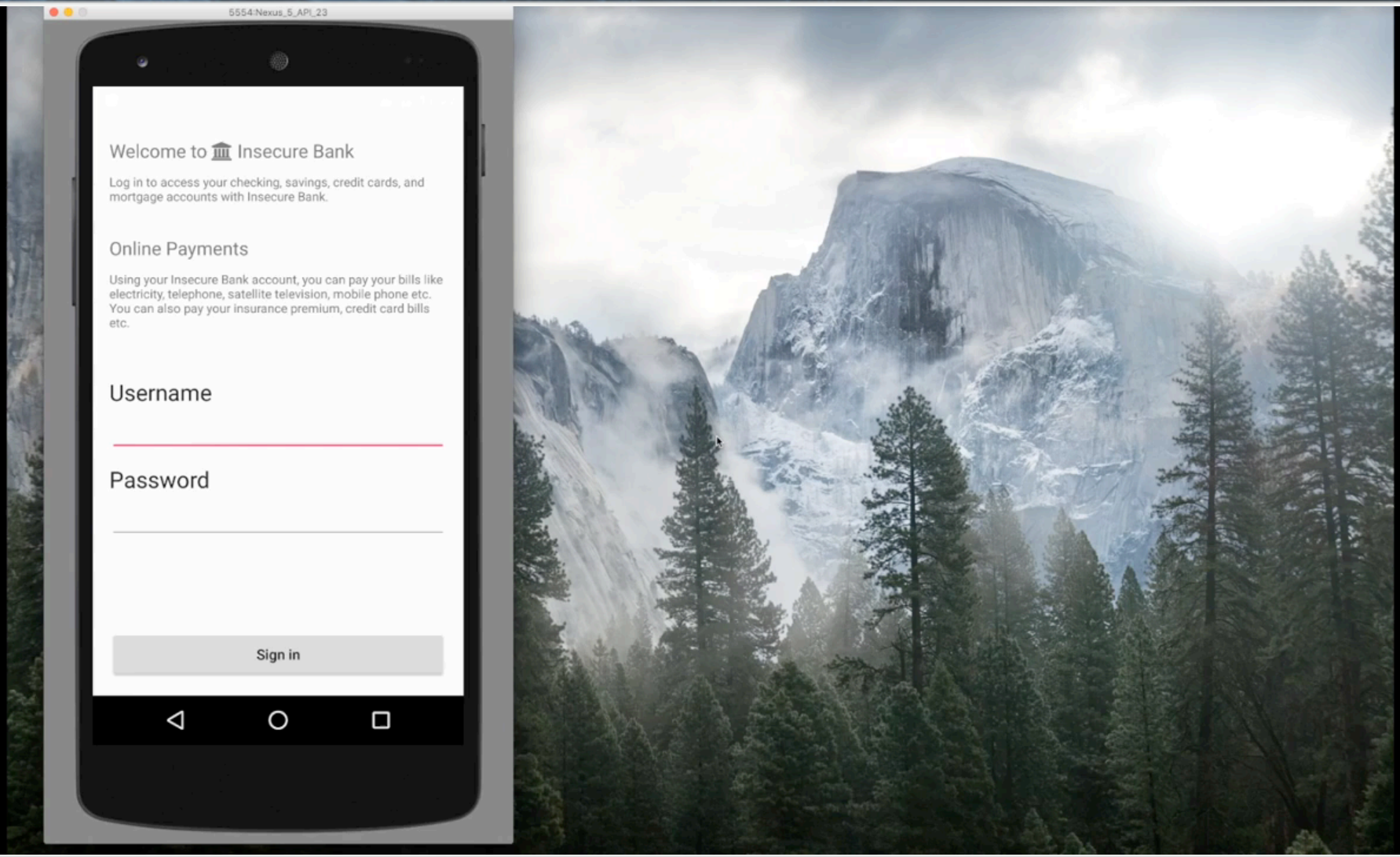
Hdiv DEMO



Ataques de integridad
Parameter Tampering

Ataques contra datos editables
SQL Injection

https://youtu.be/XulSxkEROpE


5554:Nexus_5_API_23
Welcome to Insecure Bank
Log in to access your checking, savings, credit cards, and mortgage accounts with Insecure Bank.
Online Payments
Using your Insecure Bank account, you can pay your bills like electricity, telephone, satellite television, mobile phone etc. You can also pay your insurance premium, credit card bills etc.
Username
Password
Sign in

Hdiv

Basado en hechos reales

Top Retail Bank, US

Hdiv makes it easy for developers to secure their applications once Hdiv is added to the application development process. It has been working phenomenally well for fixing my security issues.

CONFIDENTIAL

Large Federal Agency, US

We wanted to rely on the protection of the application itself without totally relying on external devices. We wanted stronger security but we didn't want to compromise application performance or generate lots of false positives. Hdiv is what we wanted.

CONFIDENTIAL

Agenda

1. El problema
2. El porqué
3. Soluciones de Seguridad
4. **Sumario**

Sumario

- El **enfoque tradicional** de seguridad **no ha resuelto adecuadamente el problema**.
- Todavía vemos que los **WAF van a tener un papel importante**.
- Consideramos que **la seguridad integrada dentro de las aplicaciones (RASP) es necesaria** para cambiar esta realidad.

Ruegos & Preguntas

Eskerrik asko

gorka@hdivsecurity.com
hdivsecurity.com