

# Amenazas contra la Autenticación Web

## Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: <http://www.ReYDeS.com>

e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)

Jueves 7 de Mayo del 2015

# Presentación

Alonso Eduardo Caballero Quezada es Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Miembro de Open Web Application Security Project (OWASP).

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de doce años de experiencia en el área y desde hace ocho años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz e integra actualmente el Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos en Perú y Ecuador, presentándose también constantemente en exposiciones enfocadas a, Hacking Ético, Informática Forense, GNU/Linux y Software Libre.



@Alonso\_ReYDeS  [www.facebook.com/alonsoreydes](http://www.facebook.com/alonsoreydes) 

[pe.linkedin.com/in/alonsocaballeroquezada/](http://pe.linkedin.com/in/alonsocaballeroquezada/) 

# Amenazas contra la Autenticación Web

La Autenticación juega un rol crítico en la seguridad de una aplicación web, pues las subsecuentes decisiones son hechas en base a la identidad establecida por las credenciales proporcionadas.

A continuación se exponen las formas más prevalentes de autenticación web.

- \* **Nombres de Usuario y Contraseñas.** Debido a su simplicidad es la forma más prevalente de autenticación sobre le Web.
- \* **Autenticación Fuerte.** Muchos sitios web empiezan a utilizar formas más fuertes de autenticación para sus usuarios, incluyendo la utilización de tokens y certificados.
- \* **Servicios de Autenticación.** Muchos sitios web externalizan su autenticación a servicios los cuales implementan gestión de identidad y un protocolo de autenticación, como Microsoft Account u OpenID.

\* [http://en.wikipedia.org/wiki/Microsoft\\_account](http://en.wikipedia.org/wiki/Microsoft_account)

\* <http://en.wikipedia.org/wiki/OpenID>

# Amenazas en los Nombres de Usuario y Contraseñas

Aunque existen numerosas maneras de implementar una autenticación básica utilizando nombres de usuario y contraseña, las implementaciones web caen en el mismo tipo de ataques.

## Enumeración de Nombres de Usuario

Se utiliza principalmente para proporcionar una mayor eficiencia en el ataque para adivinar contraseñas. Existen algunas funcionalidades frecuentemente utilizadas en las aplicaciones web, las cuales permite determinar nombres de usuario.

Resultados de perfilamiento

Mensajes de error en Registros de Ingreso (login)

Mensajes de error en funcionalidades de reajuste de contraseñas

Registro

Bloqueo de cuentas

Ataques basados en el Tiempo

# Amenazas en los Nombres de Usuario y Contraseñas

## Adivinar Contraseñas

Pueden ser utilizados usualmente sin importar el protocolo a autenticación. Esto puede ser realizado de manera manual o automática. Las dos principales técnicas son las siguientes:

Adivinar contraseñas manualmente

Adivinar contraseñas automáticamente

## Interceptación

Cualquier protocolo exponiendo credenciales en tránsito sobre la red es potencialmente vulnerable a ataques de interceptación. Los dos protocolos más populares de autenticación web exponen las credenciales.

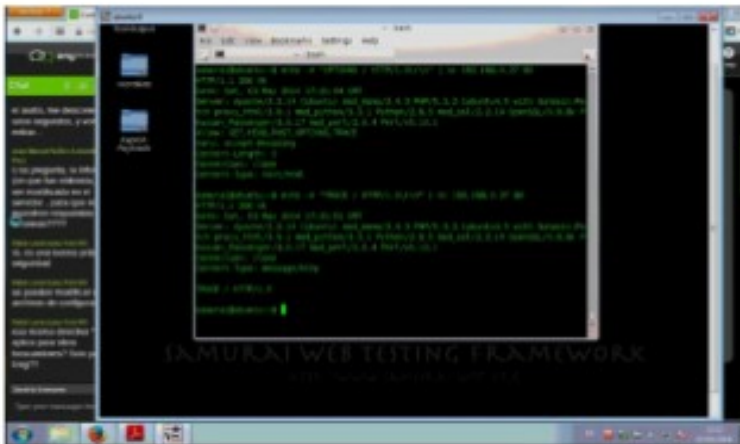
Autenticación “Basic”

Autenticación “Digest”

# Curso Virtual de Hacking Aplicaciones Web

## Curso Virtual de Hacking Aplicaciones Web

2015



### Grupo Sábado:

9, 16, 23 y 30 de Mayo del 2015  
De 3:30pm a 7:15pm (UTC -05:00)

### Grupo Domingo:

10, 17, 24 y 31 de Mayo del 2015  
De 9:00am a 12:45pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:



Más Información: [http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Aplicaciones\\_Web](http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web)  
E-mail: [caballero.alonso@gmail.com](mailto:caballero.alonso@gmail.com) / Sitio Web: <http://www.reydes.com>

# Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

## Curso Virtual de Hacking Ético

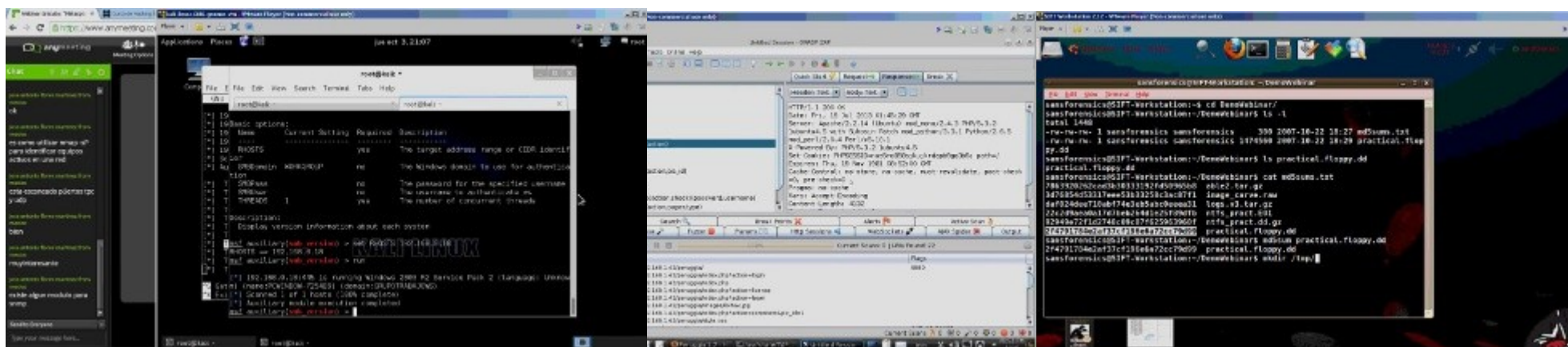
[http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Etico](http://www.reydes.com/d/?q=Curso_de_Hacking_Etico)

## Curso Virtual de Hacking Aplicaciones Web

[http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Aplicaciones\\_Web](http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web)

## Curso Virtual de Informática Forense

[http://www.reydes.com/d/?q=Curso\\_de\\_Informatica\\_Forense](http://www.reydes.com/d/?q=Curso_de_Informatica_Forense)





# Más Contenidos

Videos de 26 Webinars Gratuitos sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

<http://www.reydes.com/d/?q=videos>

Diapositivas utilizadas en los Webinars Gratuitos.

<http://www.reydes.com/d/?q=node/3>

Artículos y documentos publicados

<http://www.reydes.com/d/?q=node/2>

Mi Blog sobre temas de mi interés.

<http://www.reydes.com/d/?q=blog/1>



The screenshot shows the website 'Alonso Caballero Quezada / ReYDeS' with a navigation menu (Documentos, Eventos, Cursos, Blog, Contacto). The main content area features a video player titled 'Servicio Independiente de Hacking Ético' showing a speaker at a podium in front of an audience. Below the video is a 'Presentación' section with a profile picture of Alonso Eduardo Caballero Quezada and a bio: 'Alonso Eduardo Caballero Quezada es Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Miembro de Open Web Application Security Project (OWASP). Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de once años de experiencia en el área y desde hace siete años labora como consultor e Instructor Independiente en las áreas de Hacking'. To the right, there is a 'Cursos' section with a list of courses: 'Curso de Hacking Ético', 'Curso de Hacking Aplicaciones Web', 'Curso de Informática Forense', 'Curso de Hacking con Kali Linux', and 'Curso Forense de Autopsy 3'. Below that is a 'MI Blog' section with a list of blog posts: 'Crear una Puerta Trasera Persistente utilizando Meterpreter', 'Trazado de Rutas en Paralelo utilizando Scapy', and 'Automatizar un Ataque MITM para Recolectar Credenciales utilizando Subterfuge'.



# Demostraciones

The image shows a desktop environment with a Mozilla Firefox browser window and an OWASP ZAP 2.4.0 window. The browser window displays the login page for 'Gruyere' at the URL `192.168.1042115123/login?uid=admin`. The page has a yellow background with a 'Home' link and 'Sign in | Sign up' buttons. Below these are input fields for 'User name:' and 'Password:'. A red circle highlights the 'User name:' field. The OWASP ZAP window shows a request interception for the URL `http://192.168.1042115123/cgi-bin/badstore.cgi?action=moduser`. The response body contains HTML code: `</div>`, `<div class='message'>Invalid user name or password.</div>`, and `<div class='content'>`. The ZAP interface also shows a tree view of the site structure and a table of recent requests.

Browser window: Gruyere: Login - Mozilla Firefox  
URL: 192.168.1042115123/login?uid=admin

OWASP ZAP 2.4.0 window: Untitled Session - OWASP ZAP 2.4.0

Request/Response details:

```
1 HTTP/1.1 200 OK
2 Date: Sat, 11 Apr 2015 02:38:21 GMT
3 Server: BaseHTTP/0.3 Python/2.6.5
4 Content-type: text/html
5 Pragma: no-cache
6 X-XSS-Protection: 0

142 </div>
143
144
145 <div class='message'>Invalid user name or password.</div>
146
147
148 <div class='content'>
```

Id	Req. Timestamp	Method	URL	Code	Reason	RTT	Size Resp...	Highest A...	No...	Tags
163	24/04/15 22:34:46	POST	http://192.168.1042115123/cgi-bin/badstore.cgi?action=moduser	200	OK	3...	3.88 KIB	Medium		Form, Hid...
164	24/04/15 22:34:46	GET	http://192.168.1042115123/cgi-bin/bsheader.cgi	200	OK	1...	1.36 bytes	Medium		

# Amenazas contra la Autenticación Web

¡Muchas Gracias!

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: <http://www.ReYDeS.com>

e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)