

Amenazas contra la Autenticación Web

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: <https://www.ReYDeS.com> :- e-mail: ReYDeS@gmail.com

Jueves 3 de Febrero 2022

Alonso Eduardo Caballero Quezada

EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator Certified, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures Pen Testing, Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist y OSEH.

Más de 18 años de experiencia como consultor e instructor independiente en las áreas de Hacking Ético y Forense Digital. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux.

Redes Sociales

 <https://www.linkedin.com/in/alonsocaballeroquezada/>

 https://twitter.com/Alonso_ReYDeS

 <https://www.youtube.com/c/AlonsoCaballero>

 <https://www.facebook.com/alonsoreydes/>

 https://www.instagram.com/alonso_reydes/

 reydes@gmail.com  <https://www.reydes.com>

 +51 949 304 030  @ReYDeS



Atacar la Autenticación

La autenticación es conceptualmente uno de los mecanismos de seguridad más sencillos empleados dentro de las aplicaciones web. El caso más simple es cuando un usuario proporciona un nombre de usuario y contraseña, luego la aplicación verificará si son correcto. Si lo son, se le permitirá al usuario entrar, caso contrario, no.

También es la base de protección contra ataques maliciosos contra la aplicación. Es la primera línea de defensa contra acceso no autorizado. Si un atacante derrota estas defensas, ganará acceso sin restricción hacia los datos. Sin una autenticación robusta en la cual basarse, ninguno de los otros mecanismos de seguridad serán efectivos.

En la aplicaciones del mundo real, la autenticación suele ser el eslabón más débil, lo cual permite al atacante obtener acceso no autorizado.

Tecnologías para la Autenticación

Existe un amplio rango de tecnologías disponibles para los desarrolladores de aplicaciones web, implementen mecanismos de autenticación:

- Autenticación basada en formularios HTML
- Mecanismos multifactor, como aquellas combinando contraseñas y tokens físicos
- Certificados SSL/TLS para el cliente / o tarjetas inteligentes
- Autenticación HTTP básica (basic) y resumen (digest)
- Autenticación Integrada Windows utilizando NTLM o Kerberos
- Servicios de autenticación

De lejos uno de los mecanismos de seguridad más empleados en las aplicaciones web son los formularios HTML, donde se obtiene el nombre de usuario y contraseña, para luego ser enviado hacia la aplicación.

Fallas de Diseño Mecanismos de Autenticación

- Contraseñas inadecuadas
- Fuerza bruta al login
- Mensajes verbosos de fallas
- Transmisión vulnerable de credenciales
- Funcionalidad para el cambio de contraseña
- Funcionalidad para el olvido de la contraseña
- Funcionalidad de “recordarme”
- Funcionalidad para la suplantación del usuario
- Validación incompleta de credenciales
- Nombres de usuario no únicos
- Nombres de usuario predecibles
- Contraseñas iniciales predecibles
- Distribución insegura de credenciales

Fallas de Implementación en Autenticación

Incluso un mecanismo bien diseñado para la autenticación, puede ser altamente inseguro debido a errores en su implementación. Estos errores pueden conducir hacia fuga de información, evadir completamente el login, o debilitar toda la seguridad del mecanismo diseñado.

Las fallas de implementación tienden a ser más sutiles y difíciles de detectar comparado con los defectos en el diseño.

- Mecanismos de login “Fail-Open”
- Defectos en los mecanismos de login de múltiples etapas
- Almacenamiento inseguro de credenciales

Curso Virtual de Hacking Aplicaciones Web

Domingos 6, 13, 20 y 27 de Febrero del 2022 De 9:00 am a 12:00 pm (UTC -05:00)

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



Presentación

Las aplicaciones web modernas tienen un rol muy importante en todas las organizaciones. Pero si la organización no tiene la capacidad de evaluar y asegurar adecuadamente sus aplicaciones web, los ciberatacantes podrían comprometer estas aplicaciones, afectando el funcionamiento normal de la empresa, como también robar datos sensibles. Desafortunadamente muchas organizaciones operan bajo la errónea percepción, de un escáner de seguridad para aplicaciones web es la manera más fiable de descubrir fallas en sus sistemas. Las ciberdefensas modernas requieren una comprensión realista y profunda de los problemas de seguridad relacionadas con la aplicación web. Cualquiera puede aprender a realizar algunos tipos de ataques contra la web, pero una prueba de penetración efectiva contra aplicaciones web requiere un conocimiento más profundo.



Alonso Eduardo Caballero Quezada. EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement in

Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). He sido instructor, expositor y conferencista en el OWASP LATAM Tour,

Más Información: https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web



e-mail: reydes@gmail.com



Sitio Web: <https://www.reydes.com>

Alonso Eduardo Caballero Quezada :- Sitio web: <https://www.reydes.com> :- e-mail: reydes@gmail.com

Demostraciones

The screenshot shows the OWASP ZAP tool interface. The browser window displays the 'Hackazon' login page with the message 'Please login' and a red error message: 'Username or password are incorrect.' The OWASP ZAP tool window shows the 'Request' tab with the following details:

```
POST http://www.hackazon.info/user/login HTTP/1.1
Host: www.hackazon.info
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101
Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
username=admin&password=qwerty
```

The tool interface also shows a 'Fuzzer' progress bar at 100% and a table of messages sent:

| Tas... | Message Type | Code | Reason | RTT | Size Resp. Header | Size Resp. Body | Highest Alert | State | Payloads |
|--------|--------------|------|--------|------|-------------------|-----------------|---------------|-------|----------|
| 491 | Fuzzed | 200 | OK | 3... | 366 bytes | 24,565 bytes | | | russia |
| 492 | Fuzzed | 200 | OK | 4... | 366 bytes | 24,565 bytes | | | scorpion |
| 493 | Fuzzed | 200 | OK | 1... | 366 bytes | 24,565 bytes | | | rebecca |
| 494 | Fuzzed | 200 | OK | 1... | 366 bytes | 24,565 bytes | | | tester |
| 495 | Fuzzed | 200 | OK | 4... | 366 bytes | 24,565 bytes | | | mistress |

Cursos Virtuales Disponibles en Video

Curso Virtual de Hacking Ético

https://www.reydes.com/d/?q=Curso_de_Hacking_Etico

Curso Virtual de Hacking Aplicaciones Web

https://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web

Curso Virtual de Informática Forense

https://www.reydes.com/d/?q=Curso_de_Informatica_Forense

Curso Virtual Hacking con Kali Linux

https://www.reydes.com/d/?q=Curso_de_Hacking_con_Kali_Linux

Curso Virtual OSINT - Open Source Intelligence

https://www.reydes.com/d/?q=Curso_de_OSINT

Curso Virtual Forense de Redes

https://www.reydes.com/d/?q=Curso_Forense_de_Redde

Y todos los cursos virtuales:

<https://www.reydes.com/d/?q=cursos>



Más Contenidos

Videos de 73 webinars gratuitos

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

Diapositivas de los webinars gratuitos

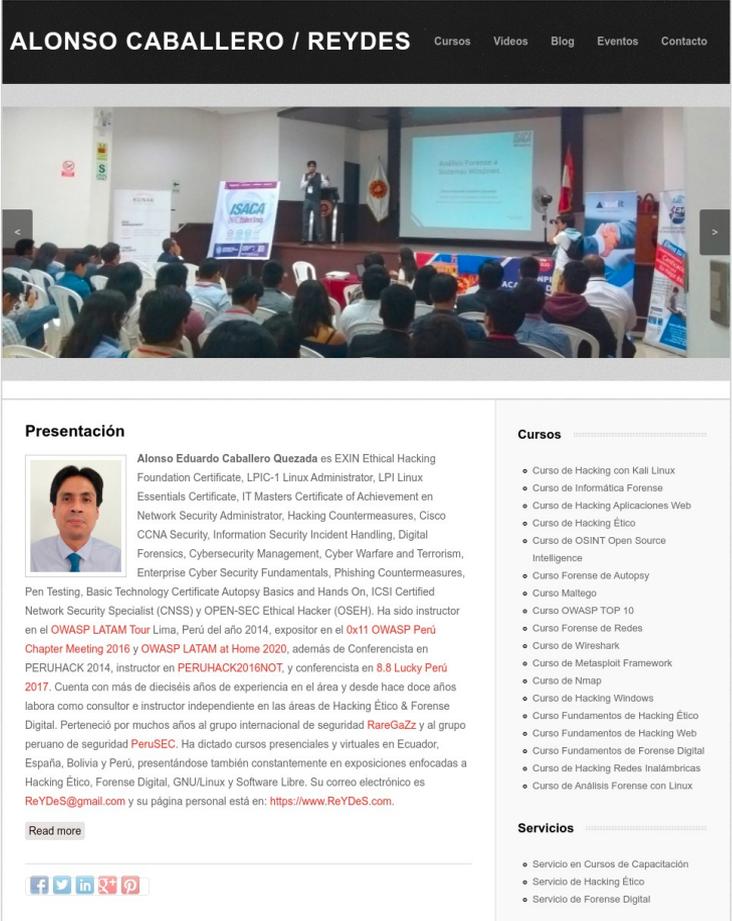
<https://www.reydes.com/d/?q=eventos>

Artículos y documentos publicados

<https://www.reydes.com/d/?q=documentos>

Blog sobre temas de mi interés

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



ALONSO CABALLERO / REYDES Cursos Videos Blog Eventos Contacto

Presentación

 **Alonso Eduardo Caballero Quezada** es EXIN Ethical Hacking Foundation Certificate, LPIC-1 Linux Administrator, LPI Linux Essentials Certificate, IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling, Digital Forensics, Cybersecurity Management, Cyber Warfare and Terrorism, Enterprise Cyber Security Fundamentals, Phishing Countermeasures, Pen Testing, Basic Technology Certificate Autopsy Basics and Hands On, ICSI Certified Network Security Specialist (CNSS) y OPEN-SEC Ethical Hacker (OSEH). Ha sido instructor en el **OWASP LATAM Tour** Lima, Perú del año 2014, expositor en el **0x11 OWASP Perú Chapter Meeting 2016** y **OWASP LATAM at Home 2020**, además de Conferencista en **PERUHACK 2014**, instructor en **PERUHACK2016NOT**, y conferencista en **8.8 Lucky Perú 2017**. Cuenta con más de dieciséis años de experiencia en el área y desde hace doce años labora como consultor e instructor independiente en las áreas de Hacking Ético & Forense Digital. Perteneció por muchos años al grupo internacional de seguridad **RareGazZ** y al grupo peruano de seguridad **PeruSEC**. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Forense Digital, GNU/Linux y Software Libre. Su correo electrónico es ReYDeS@gmail.com y su página personal está en: <https://www.ReYDeS.com>.

[Read more](#)



Cursos

- Curso de Hacking con Kali Linux
- Curso de Informática Forense
- Curso de Hacking Aplicaciones Web
- Curso de Hacking Ético
- Curso de OSINT Open Source Intelligence
- Curso Forense de Autopsy
- Curso Maltego
- Curso OWASP TOP 10
- Curso Forense de Redes
- Curso de WireShark
- Curso de Metasploit Framework
- Curso de Nmap
- Curso de Hacking Windows
- Curso Fundamentos de Hacking Ético
- Curso Fundamentos de Hacking Web
- Curso Fundamentos de Forense Digital
- Curso de Hacking Redes Inalámbricas
- Curso de Análisis Forense con Linux

Servicios

- Servicio en Cursos de Capacitación
- Servicio de Hacking Ético
- Servicio de Forense Digital

Amenazas contra la Autenticación Web

Alonso Eduardo Caballero Quezada

Instructor y Consultor en Hacking Ético, Forense Digital & GNU/Linux

Sitio Web: <https://www.ReYDeS.com> :- e-mail: ReYDeS@gmail.com

Jueves 3 de Febrero 2022