Apuntes SinCara sesión 4

Modulo 14 : Hacking Web Applications

- OWASP
  - OWASP Top 10
    - https://owasp.org/Top10/es - OWASP Top 10 2021
    - https://www.incibe.es/empresas/blog/top-10-vulnerabilidades-web-2021 - Resumen
  - OWASP Web Security Testing Guide (WSTG)
    - https://thehackerway.com/2021/03/22/conoce-el-owasp-web-security-testing-guide-wstg/ - WSTG
    - https://owasp.org/www-project-web-security-testing-guide/ - guía de 465 páginas.
      - https://github.com/OWASP/wstg/releases/download/v4.2/wstg-v4.2.pdf - PDF
  - OWASP Zed Attack Proxy (ZAP)
    - https://www.zaproxy.org/ - En septiembre de 2024, ZAP se van a Checkmarx, pero previamente, en 2023 se habían ido a la Fundación Linux
- Análisis de seguridad de aplicaciones web
  - https://www.incibe.es/protege-tu-empresa/blog/analiza-seguridad-tu-web-y-protege-tu-empresa - Analiza la seguridad de tu web y protege tu empresa. Interesante artículo del INCIBE con enlaces a muchas herramientas.
  - https://portswigger.net/research/top-10-web-hacking-techniques - Varios artículos recopilando las técnicas de hacking de Webs más usadas a lo largo de los años.
- Nomenclatura, Conceptos
  - https://seguridad.prestigia.es/que-son-las-herramientas-sast-y-dast/ - SAST vs DAST
  - https://blog.segu-info.com.ar/2022/06/introduccion-al-fuzzing-como-buscar.html - Introducción al fuzzing: cómo buscar bugs de manera automatizada
  - https://www.hackplayers.com/2021/02/vulnerabilidades-XXE-y-contramedidas.html - XXE
  - https://es.wikipedia.org/wiki/C%C3%B3digo_porciento - Lenguaje código porciento o URL.
  - https://www.welivesecurity.com/la-es/2017/08/11/watering-hole-espera-potenciales-victimas/ - Watering Hole
  - https://okitup.com/blog/que-es-y-como-funciona-el-cors/ - CORS: Qué es y cómo funciona el Cross-Origin Resource Sharing
  - https://www.cronup.com/que-es-rasp/ - Qué es RASP
  - DNS Rebinding
    - El atacante registra un dominio el cual delega a un servidor DNS que él controla.
    - El servidor está configurado para responder con un parámetro TTL muy corto, que previene que la respuesta sea cacheada.
    - Se envía una URL, con un código (JavaScript o el que sea), que interactua con ese dominio.
    - El usuario ejecuta esa URL en su navegador.
    - La primera respuesta contiene la dirección IP del servidor con el código malicioso, que descarga y ejecuta en el navegador de la víctima.
    - Las consiguientes respuestas contienen direcciones IP existentes en las redes privadas de la víctima. Esto hace que ahora ejecute ese código contra IPs internas.
    - Dado que las dos son respuestas DNS completamente válidas, autorizan al script el acceso a hosts dentro de la red privada.
    - Cómo la conexión ya estaba previamente establecida con el servidor remoto malicioso inicial, las consiguientes respuestas del código JavaScript ejecutándose contra IPs internas, se envían al servidor.
    - Dicho código accede a recursos internos, inyecta código en ellos, recopila información y la envia al servidor remoto.
    - RESUMEN: Básicamente, haces que te pidan algo, les das un mapeo de nombre-TTL corto a IP, inyectas algo de JavaScript en su navegador que hace peticiones maliciosas, y luego cambias la IP a través de la actualización de DNS de tu lado para que apunte a todas las IPs

de destino detrás de su firewall.
        - https://es.wikipedia.org/wiki/DNS_rebinding - DNS Rebinding
        - https://www.websecurity.es/que-es-dns-rebinding/ - Qué es DNS Rebinding
- REST, SOAP
    - https://www.redhat.com/es/topics/integration/whats-the-difference-between-soap-rest - Diferencias entre REST y SOAP
    - https://es.stackoverflow.com/questions/76615/qu%C3%A9-diferencia-hay-entre-soap-y-rest - Tablita con las diferencias
    - https://www.nts-solutions.com/blog/saml-que-es.html - Qué es SAML
    - SOAP, UDDI y WSDL
        - SOAP (Simple Object Access Protocol) es un protocolo estándar que define cómo dos objetos en diferentes procesos pueden comunicarse entre si, preguntando a UDDI por su localización, y por medio de intercambio de datos XML (documentos WSDL).
        - UDDI son las siglas del catálogo de servicios denominado Universal Description, Discovery and Integration. UDDI se comunica intercambiando archivos WSDL. Un servidor (o proveedor del servicio) debe realizar el registro de su servicio en UDDI para que sea localizable.
        - WSDL (Web Services Description Language), es un formato (XML) que se utiliza para describir servicios web (WS).
        - https://txikiboo.wordpress.com/2013/11/11/relacion-soap-wsdl-uddi/ - Artículo sobre SOAP
- APIs
    - https://owasp.org/www-project-api-security/ - OWASP API Security Top 10 2023
    - https://www.campusmvp.es/recursos/post/que-son-los-webhooks-en-que-se-diferencian-de-una-api-rest-y-por-que-deberias-conocerlos.aspx - Webhook vs API
- Más info, Noticias
    - https://blog.elhacker.net/2022/06/herramienta-YODA-encuentra-miles-plugins-maliciosos-en-wordpress.html - Encuentran 47.300 plugins maliciosos de WordPress instalados en 24.900 sitios
    - https://blog.segu-info.com.ar/2023/04/mas-de-un-millon-de-sitios-wordpress.html - Más de un millón de sitios WordPress infectados
    - &pct-off=60-99 - Truco para añadir a la URL de amazon para ver los productos con un descuento dado.
    - https://derechodelared.com/investigando-url-maliciosa/ - Investigando una URL maliciosa

Tools

- Burp Suite
    - https://portswigger.net/burp - Descarga. Hay tres versiones:
        - Burp Suite Community Edition (gratis): https://portswigger.net/burp/communitydownload
        - Burp Suite Professional (349$ / año)
        - Burp Suite Enterprise Edition (a partir de 6000$ / año)
    - https://portswigger.net/web-security - Academy, formación gratuita, pero requiere cuenta.
    - https://portswigger.net/web-security/all-labs - Labs gratuitos, aunque requieren tener cuenta.
    - https://www.youtube.com/playlist?list=PL4TbrTdoQBY_dZQ9XI9NKwb5evvyfYQNQ - Un curso en video de Burp Suite, en español, que está bastante bien. Para novatos. Sacado de https://sniferl4bs.com/2020/06/curso-burp-suite-desde-0-presentaci%C3%B3n/
    - https://github.com/alphaSeclab/awesome-burp-suite/blob/master/Readme_en.md - Recopilación de recursos de Burp Suite
    - https://www.google.com/search?q=meme+%22burp+suite%22&tbm=isch - Memes de Burp Suite

Modulo 15 - SQL Injection

- https://owasp.org/www-community/attacks/SQL_Injection - Recursos en Inglés
- FUN:
    - https://es.xkcd.com/strips/exploits-de-una-madre/ - SQL Injection

    - https://xkcd.com/1253/ - Otro SQL Injection
    - https://computerhoy.com/noticias/life/pone-nombre-null-matricula-hacerse-invisible-cobran-12000-dolares-multas-defectuosas-473645 - Le pone a su matricula «NULL» y le caen decenas de multas pendientes de cobrar.
    - https://www.xataka.com/otros/internet-tu-nombre-puede-convertirse-tu-peor-pesadilla-1 - Jennifer Null
    - https://i.kinja-img.com/gawker-media/image/upload/s--UzcqSr8_--/c_fill,fl_progressive,g_center,h_900,q_80,w_1600/18mpenleoksq8jpg.jpg - SQL Injection
- https://sqlpd.com/ - Para aprender SQL jugando
- https://github.com/digininja/DVWA/blob/master/README.es.md - Damm Vulnerable Web Application
- https://portswigger.net/web-security/sql-injection/union-attacks - Cómo detectar número de columnas en una query, para poder utilizar el operador UNION

Modulo 16 - Hacking Wireless Networks

WIFI

```
-------------------------------------------------------------------------------
-----------------------------
Generation     IEEE Standard       Maximum Linkrate
Wi-Fi 7     802.11be          46 Gbit/s
Wi-Fi 6E    802.11ax          11 Gbit/s  Añade la banda de los 6GHz
Wi-Fi 6     802.11ax          11 Gbit/s  2,4GHz y 5GHz
Wi-Fi 5     802.11ac    680–6933 Mbit/s  2,4GHz y 5GHz
Wi-Fi 4     802.11n       72–600 Mbit/s  2,4GHz y 5GHz
Wi-Fi 3     802.11g         3–54 Mbit/s  2,4GHz
Wi-Fi 2     802.11b    1.5 to 54 Mbit/s  2,4GHz
Wi-Fi 1     802.11a      1 to 11 Mbit/s  3,7GHz y 5GHz
-------------------------------------------------------------------------------
-----------------------------
```

- Futuro
    - https://bandaancha.eu/articulos/como-funciona-wifi-6-mejoras-ofdma-1024-9846 - Qué es WiFi 6 y por qué la velocidad no es su mejor característica
    - https://www.genbeta.com/actualidad/detectar-movimiento-e-incluso-nuestra-frecuencia-respiratoria-asi-funcionaran-routers-nuevo-estandar-wifi-802-11bf - Detectar el movimiento e incluso nuestra frecuencia respiratoria: así funcionarán los routers con el nuevo estándar WiFi 802.11bf
        - https://github.com/Marsrocky/Awesome-WiFi-CSI-Sensing - Awesome Wi-Fi Sensing
- Canales WiFi
    - https://www.redeszone.net/tutoriales/redes-wifi/bandas-frecuencias-wi-fi/ - Canales WiFi
    - https://bandaancha.eu/articulos/orange-movistar-limitan-wifi-routers-9808 - Acerca de los canales WIFI
    - https://www.syscomblog.com/2016/02/que-es-dfs-dynamic-frequency-selection.html - ¿Qué es DFS (Dynamic Frequency Selection)?
    - https://bandaancha.eu/articulos/baja-velocidad-cortes-audio-desconexion-10264 - Colisiones entre Wifi y Bluetooth
- Algoritmos:

```
-------------------------------------------------------------------------------
-------------------------------------------
Tecn.      <-------- IV ---------->      Alg.      Longitud key     Int. Check
Alg.      Key Management     Año
WEP       RC4  24 bits   EAP  40/104 bits    CRC-32       No              1997
WPA       RC4  48 bits   TKIP    128 bits  MA & CRC-32    4way Handshake  1999
```

```
WPA2      AES  48 bits   CCMP    128 bits   CBC-MAC       4way Handshake  2004
WPA3  AES-256 1-64 bits  GCMP    192 bits  BIP-GMAC-256   ECDH and ECDSA  2018
------------------------------------------------------------------------------
-------------------------------------------
```

- Ataques Wireless:
  - https://es.wikipedia.org/wiki/KRACK - Ataque KRACK
    - https://www.krackattacks.com/ - Página dedicada a KRACK
  - https://unaaldia.hispasec.com/2018/07/nuevos-ataques-contra-el-protocolo-de-red-lte-4g-y-posible-afeccion-a-5g.html - aLTEr Attack
    - https://alter-attack.net/ - Página dedicada a aLTEr
- Otros enlaces de redes wireless:
  - https://www.redeszone.net/reportajes/tecnologias/sidewalk-que-es-wifi-amazon-como-funciona/ - La nueva red de Amazon, y también describe otras menos conocidas: Zigbee, LoRa, etc...
  - https://www.redeszone.net/tutoriales/redes-wifi/wps-que-es-como-funciona/ - Qué es el WPS de los routers, cómo funciona y por qué deberías desactivarlo
  - https://www.incibe.es/sites/default/files/docs/guia_router/osi-guia-tu-router-tu-castillo.pdf - Guía de configuración de routers del INCIBE
  - https://www.redeszone.net/tutoriales/redes-wifi/metodos-crackear-wps-routers-wifi/ - Cómo crackear el WPS
  - https://www.wifislax.com/ - Distro española especializada en redes. Es la más actualizada en cuanto a drivers de tarjetas wifi.
  - https://wigle.net/ - Buscador de Wifis geolocalizadas.
- WarShipping
  - https://www.helpnetsecurity.com/2019/08/07/warshipping/ - WarShipping, escaneo de redes mediante paquetería postal.
  - https://www.incibe.es/empresas/blog/historias-reales-paquete-postal-y-redes-wifi-combinacion-perfecta-el - Historia real en España
- Enlaces variados:
  - https://www.lavanguardia.com/tecnologia/20220222/8074390/hombre-deja-internet-toda-ciudad-hijo-utilice-tablet-pmv.html - Un padre que usó un inhibidor de señal para dejar sin wifi a su hijo corta internet a todo un pueblo (en Francia)
  - https://computerhoy.com/noticias/moviles/papeleras-espia-rastrean-transeuntes-londres-5593 - Rastreo de viandantes siguiendo las MACs de sus dispositivos, en Londres.
  - https://www.design1st.com/impact-5g-on-iot-product-development/ - Telefonía 5G
  - https://en.wikipedia.org/wiki/List_of_interface_bit_rates - Magnífica página con todo tipo de estándares, y las velocidades que tienen.

Modulo 17 - Hacking Mobile Platforms

- https://www.owasp.org/index.php/OWASP_Mobile_Top_10 - Top 10 OWASP para Móviles.
- https://www.osi.es/es/guia-para-configurar-dispositivos-moviles - Guías del INCIBE para configurar nuestros móviles.
- Hacking
  - https://blog.segu-info.com.ar/2020/01/asi-hackearon-el-movil-de-jeff-bezos.html - Así hackearon el móvil de Jeff Bezos a través de NSO/Pegasus
  - https://www.elconfidencial.com/espna/2019-09-26/arrimadas-intento-hackeo-whatsapp-rivera-sms-denuncia_2254663/ - Hackeo por Whassap de Albert Rivera.
  - https://blog.segu-info.com.ar/2020/08/sdk-chino-espio-mas-de-1200.html - SDK chino, espió en más de 1200 apps de iOS
- Ataques Bluetooth:
  - https://www.redeszone.net/tutoriales/seguridad/principales-riesgos-seguridad-bluetooth/ - Ataques Bluetooth
  - https://github.com/engn33r/awesome-bluetooth-security - Awesome Bluetooth Security

    - Bluesmacking: Ataque de tipo DoS via Bluetooth.
    - Bluejacking: Mandar mensajes no solicitados.
    - Blue Snarfing: Robo de Información usando Bluetooth.
    - BlueSniff: Wardriving pero con dispositivos Bluetooth.
    - Bluebugging: Obteniendo control sobre el dispositivo a través de Bluetooth.
    - BluePrinting: Equivalente al Footprinting, recopilando información sobre los dispositivos bluetooth: MAC, fabricante, modelo, firmware…
    - MAC Spoofing Attack: Falsificando la MAC del Bluetooth.
    - Man-in-the-Middle / Impersonation Attack: Ataque MitM con Bluetooth.
- SIMS
    - https://www.redeszone.net/noticias/seguridad/metodos-hackear-tarjeta-sim/ - Métodos para hackear (duplicar) una tarjeta SIM.
    - https://blog.segu-info.com.ar/2020/08/sim-utilizadas-por-los-delincuentes.html - SIMs rusas o SIMs blancas
    - https://blog.segu-info.com.ar/2021/03/como-conseguir-los-sms-de-cualquiera.html - Cómo conseguir los SMS de cualquiera por U$S16 y porqué NO usar SMS como 2FA
    - https://bandaancha.eu/articulos/orange-informara-bancos-cuando-9775 - Estandar Mobile Connect de la GSM, permite que las entidades financieras puedan saber cuándo se hizo el último duplicado de SIM.
        - Si has pedido un duplicado de SIM de forma legítima, puedes encontrarte con que no puedes realizar transacciones en tu banco durante unos días. La GSMA recomienda un plazo de 48 h. para que los bancos denieguen operaciones de riesgo tras un duplicado.
        - https://mobileconnect.io/about/ - Según la página del estandar, en España están adheridos Telefónica, Vodafone y Orange.
- Android
    - ROMs
        - https://www.xatakandroid.com/sistema-operativo/estamos-2021-sigo-instalando-roms-personalizadas - ROMs personalizadas para móviles Android
        - https://www.kali.org/kali-linux-nethunter/ - Kali NetHunter, versión de Kali para smartphones Android.
        - https://desktop.firmware.mobi/ - ROMs para rootear móviles con Android
        - https://calyxos.org/ - Android mobile operating system that puts privacy and security
    - Apps
        - https://www.osi.es/es/conan-mobile - Aplicación móvil del Incibe para securizar Android
        - https://play.google.com/store/apps/details?id=com.eakteam.networkmanager.pro - App potente de networking (6€)
    - https://www.xatakandroid.com/roms-android/android-x86-proyecto-independiente-android-para-escritorio-llega-a-version-9-0-pie - Android para escritorio.
        - https://www.android-x86.org/
    - https://blog.segu-info.com.ar/2021/08/guias-de-seguridad-para-android.html - Guías de securización de Android
    - Malware
        - https://andro4all.com/noticias/apps-android/descubren-varios-fallos-de-seguridad-en-una-de-las-apps-android-mas-descargadas-del-mundo - Descubren varios fallos de seguridad en una de las apps Android más descargadas del mundo
        - https://blog.segu-info.com.ar/2020/08/evil-droid-framework-para-infectar-apk.html - Evil-Droid: framework para infectar APK
        - https://blog.phonehouse.es/2018/08/27/malware-fortnite-android/ - Malware en Android a través de una tienda de apps externa
        - https://blog.segu-info.com.ar/2021/03/tapjacking-y-otros-enganos-en-android.html - Tapjacking y otros engaños en Android
    - https://blog.segu-info.com.ar/2020/01/50-organizaciones-firman-una-carta.html - 50 organizaciones firman una carta abierta contra el Bloatware en Android.
        - https://bandaancha.eu/articulos/operadoras-fabricantes-estaran-obligados-9756 - Operadoras y fabricantes estarán obligados a permitir que su bloatware pueda ser desinstalado

    - https://bandaancha.eu/articulos/cuatro-usuarios-android-demandan-google-9771 - Usuarios de Android demandan a Google, por usar más de 9MB de datos diarios con el móvil en reposo.
    - https://blog.segu-info.com.ar/2024/09/caso-cmg-socio-de-negocio-de-rrss.html - Caso CMG: socio de negocio de RRSS admite que los micrófonos escuchan a la gente hablar para «ofrecer mejores anuncios»
- Fuchsia
    - https://es.wikipedia.org/wiki/Google_Fuchsia - Fuchsia, el nuevo Sistema Operativo de Móviles de Google, en desarrollo desde 2016.
    - https://www.muylinux.com/2021/02/17/fuchsia-os-aplicaciones-android-linux/ - Google quiere que Fuchsia OS pueda ejecutar aplicaciones de Android y Linux
- Vega
    - https://www.muylinux.com/2023/11/10/amazon-android-linux/ - Amazon abandonará Android en favor de su propio sistema operativo basado en Linux
- iOS
    - https://www.welivesecurity.com/la-es/2021/08/13/jailbreak-que-debes-saber-realizar-pentesting-aplicaciones-ios/ - Tipos de Jailbreaking en iOS
        - Jailbreak Tethered (atado): Temporal, se pierde al reiniciar el dispositivo, pero no arranca por si solo, necesitaremos conectarlo a un ordenador para arrancarlo.
        - Jailbreak Semi-Tethered: Temporal, se pierde al reiniciar el dispositivo, pero arranca por si solo.
        - Jailbreak Semi-Untethered: Al igual que el anterior, al reiniciar el dispositivo se pierde el Jailbreak, pero se puede volver a activar mediante alguna app previamente instalada cuando estaba «Jailbroken», es decir, sin necesidad de conectarlo a un ordenador.
        - Jailbreak Untethered: Permanente, al reiniciar el dispositivo sigue «Jailbroken». Este el tipo de Jailbreak más deseado.
    - https://www.theapplewiki.com/ - Todos los dispositivos de Apple
    - https://www.passfab.es/products/remove-activation-lock.html - Software para desbloquear dispositivos
    - https://br.atsit.in/es/?p=133917 - Malware que finje un apagado del móvil. Puede acceder al micrófono y a la cámara con el móvil «aparentemente» apagado.
        - https://blog.elhacker.net/2022/03/falso-reinicio-ataque-noreboot-para-mantener-persistencia-iOS.html - Otro artículo, este en castellano
- https://gendersec.tacticaltech.org/wiki/index.php/Funda_de_Faraday_para_el_tel%C3%A9fono_m%C3%B3vil - Fundas de Faraday.
    - https://www.amazon.es/Faraday/s?k=Faraday - Artículos en Amazon de fundas de Faraday.
- https://www.kimovil.com/es - Comparador de móviles y tablets.
- https://www.hackplayers.com/2024/10/tu-smarttv-te-vigila-el-impune-acr.html - Spyware en TVs
- https://bandaancha.eu/articulos/como-funcionan-donde-salen-codigos-10853 - Códigos MMI
- SS7
    - https://blog.segu-info.com.ar/2020/10/explotan-vulnerabilidades-en-ss7-para.html - SS7
    - https://blog.segu-info.com.ar/2023/09/explotar-vulnerabilidades-ss7-en.html - Explotar vulnerabilidades SS7 en iPhones y Android
- https://www.amazon.es/s?k=usb+condom - Condón USB
- https://www.infobae.com/america/mexico/2020/07/08/conoce-los-puntos-de-la-ley-que-te-podria-llevar-a-la-carcel-si-modificas-tus-dispositivos-electronicos-en-mexico/ - En México es ilegal modificar los aparatos electrónicos que hayas comprado
- https://www.geeknetic.es/Noticia/33919/Espana-prohibira-las-llamadas-desde-el-extranjero-con-numeracion-espanola-falsificada.html - España prohibirá las llamadas desde el extranjero con numeración española falsificada
- https://www.xda-developers.com/ - Página Web y foros sobre Móviles

From:
https://matebcn.eu/ - **miguel angel torres egea**

Permanent link:
https://matebcn.eu/info:cursos:pue:ethical-hacker:sesion4:sincara

Last update: **26/02/2025 10:51**