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

Modulo 16

Modulo 17