Ethical Hacker : sesión 4

- Ethical Hacker : sesión 4

clase

- Modulo 14
- Modulo 15
- Modulo 16
- Modulo 17

Modulo 14: Hacking Web Applications

- Amenazas
- OWASP - https://owasp.org
    - asociación sin ánimo de lucro
    - proyectos relacionados con seguridad
    - Coraza - ModSecurity - set reglas programables
    - web security testint guide
- Componentes de terceros con problemas: https://blog.elhacker.net/2022/06/herramienta-YODA-encuentra-miles-plugins-maliciosos-en-wordpress.html
- Falta de monitorización
- Ataques a aplicaciones web
    - ataque transversal directorio
    - https://certifiedhacker.com/<portales/
        - se pueden escanear, permitido
        - ejemplos de vulnerabildiades
    - manipulación campos ocultos (via POST/GET)
        - amazon: `&pct-off=60-99` - Truco para añadir a la URL de amazon para ver los productos con un descuento dado.
    - pass-the-cookie
        - robar cookies para logearse en una web
    - same-site
    - command injection
        - shell
        - html
        - file
    - LDAP injection
    - XSS en comentarios (tipo 2)
    - evasión filtros XSS
    - Timing attacks
        - direct timing: deducir por la respuesta si el usuario existe o no
        - cross-site timing: paquetes de solictud manipulados usando javascript
        - browser-based timing: estimar el tiempo que tarda el server en procesar para saber si es correcto o no
    - XXE
        - invocación desde XML a una petición de fichero/recurso externo
    - redirecciones / reenvios inválidos
    - Magecart (web skimming): componentes de terceros desactualizados
    - Watering Hole (abrevadero): espera de potenciales víctimas, emboscada
    - CSRF

- Manipulación / envenenamiento de cookies
- Deserialización insegura
- Ataques a servicios web
  - apuntes Fernando:
    - **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).
      - https://txikiboo.wordpress.com/2013/11/11/relacion-soap-wsdl-uddi/ - Artículo sobre SOAP
    - **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).
- XML Poisoning
- DNS Rebinding
  - saltarse restricciones de seguridad
  - controlar DNS secundario, bajar TTL
  - primera petición legítima, la siguiente manipulada
- ...

Module 15: SQL Injection

Module 16: Hacking Wireless Networks

Module 17: Hacking Mobile Platforms