



#AprenemCiberseguretat

NAVEGACIÓ SEGURA



EL NAVEGADOR ÉS L'EINA FONAMENTAL EN LA CERCA D'INFORMACIÓ I ALTRES SERVEIS A TRAVÉS DELS DIFERENTS DISPOSITIUS (ORDINADORS, TAULETA TÀCTIL I TELÈFON INTEL·LIGENT). N'HI HA DIVERSOS A LA NOSTRA DISPOSICIÓ COM ARA CHROME, FIREFOX, SAFARI O EDGE.

Quins mètodes d'atac existeixen?



Exploit

Programari que s'aprofita de determinada vulnerabilitat per a **injectar codi nociu** en l'equip. Infectarà l'equip amb un agent com ara *ransomware*, troià... L'usuari/ària només ha de visitar una web perquè el seu equip siga compromès.



Ataque de Cross Site Scripting o XSS

inclusió de **codi nociu en el contingut web** o paràmetres de URL. L'objectiu és que aquest codi siga posteriorment interpretat i executat pel navegador de l'usuari/ària afectada.



Extensions i *plugins* maliciosos

Les extensions s'actualitzen automàticament. Aquesta característica fa que una extensió que al principi no realitza cap acció maliciosa, podria modificar-se després d'una actualització per a dur-la a terme.

Desenvolupadors independents d'extensions, poden vendre-les a alguna altra entitat, la qual podria modificar-la perquè duga a terme un altre tipus de tasques no desitjades per l'usuari/ària.

Informació a la qual accedeix el meu navegador web

- Adreça IP.
- Resolució pantalla.
- Valor del camp "User-Agent".
- Quines pàgines es llegeixen i quines no, quantes pàgines s'han visitat i llocs visitats recentment.
- Idioma i zona GMT del sistema operatiu.
- Si s'accepten o no les *cookies*.
- Fonts carregades en el sistema o *plugins* instal·lats i activats.



BONES PRÀCTIQUES

1

FEU ÚS DE HTTPS EN LLOC DE HTTP, fins i tot per a serveis que no manegen informació sensible. Verificar que els certificats remesos per HTTPS que facen servir informació confidencial han sigut emesos per agents de confiança.

ACTUALITZEU NAVEGADOR Y COMPLEMENTOS: extensions y *plugins*.

2

3

PROTEGIU NAVEGADOR Y *PLUGINS* amb solucions *antiexploit* per mitigar atacs d'*exploit*.

DESHABILITEU O ELIMINEU EXTENSIONS en desús.

4

5

Si es navega en pàgines desconegudes, **DESHABILITEU *PLUGINS* JAVA, FLASH I JAVASCRIPT**.

DESCARREGUEU programes, *plugins* y extensions únicament **EN LLOCS OFICIALS Y LEGALS**.

6

7

NO EMMAGATZEMEU SESSIONS associades a serveis web que manegen informació sensible. Tanqueu quan acabe la navegació.

NO EMMAGATZEMEU CONTRASENYES en el navegador. Useu eines més segures per a la seua gestió.

8

9

USEU CONTRASENYES ROBUSTES d'accés a web i doble autenticació.

REVISEU OPCIONS DE SEGURETAT i privacitat del navegador.

10

WWW.UV.ES/UVSTIC