ZIBERSEGURTASUNAREN ARLOKO 25 AHULTASUNIK ARRISKUTSUENAK

- **Top 25a baliabide egokia da garatzaileei, ebaluatzaileei eta erabiltzaileei, baita proiektu-kudeatzaileei, segurtasun-ikertzaileei eta hezitzaileei ere, segurtasunean-ahuleziarik larrienei eta berrienei buruzko informazioa ematen laguntzeko.**
- **CWEren 2020 bertsioak Ahultasunen Datu Base Nazional estatubatuarraren (NVD) datuak erabiltzen ditu.**

CWE delakoa (Common Weakness Enumeration) garatzaileen eta profesionalen komunitateek egindako zerrenda bat da, zibersegurtasunarekin zerikusia duten softwareko eta hardwareko ahultasunik ohikoenak biltzen dituena. *Ahultasuna* diogunean, softwarearen eta hardwarearen inplementazioan, kodean, diseinuan eta arkitekturan dauden akats, errore eta kalteberatasunez ari gara. Konpondu ezean, sistemak eta sareak eraso baten aurrean zaurgarri izatea eragin dezakete. CWE zerrenda 2006an argitaratu zen lehengoz, eta hasiera batean software-arazoak baino ez zituen aintzat hartzen.

Hiru urte geroago ahultasunen top 25a eman zen argitara; horretan zerrendatuta zeuden garatzaileei, segurtasun-analistei, ikertzaileei eta hornitzaileei galdetu ondoren jasotako erantzunak. Azkenik, 2019an datu objektiboetan oinarrituriko ikuspuntuari heldu zitzaion, eta hala iritsi zen gaur egungo bertsioa, 2020koa, Ahultasunen Datu Base Nazional estatubatuarraren (NVD) datuak erabiltzen dituena, eta maiztasuna eta batez besteko puntuazio bat bateratuz ezartzen duena sailkapenaren ordena.

Jarraian, 2020ko 25 ahultasunik garrantzitsuenak laburbilduko ditugu:

1. **Inputa modu desegokian neutralizatzea webgunea eratzean (XSS lekuen Scripting-a).** Softwareak ez du erabiltzailearen inputa neutralizatzen (edo gaizki egiten du) eta erasotzaileak gai dira script bat txertatzeko web-aplikazio baten outputean. Hala, script hori bezeroaren nabigatzailean exekutatzen da.
2. **Mugaz kanpo idaztea**. Softwareak aurreikusitako buferraren aurretik edo ondoren idazten ditu datuak, eta horrek datuak hondatzea edo kode bat blokeatzea edo exekutatzea eragin dezake.
3. **Sarrera gaizki balioztatzea**. Aplikazioak sarrerak eta datuak jasotzen ditu, baina ez da gai horiek balioztatzeko, edo okerreko eran egiten du.

info@bcsc.eus | 945 236 636

Parque Tecnológico de Álava
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz

Sarrera-balioztatze hori arriskutsuak izan litezkeen sarrerak egiaztatzeko erabiltzen da, kodearen barruan eta beste osagai batzuekin komunikatzean modu seguruan prozesatuko direla bermatzeko.

4. **Mugaz kanpo irakurtzea**. Softwareak aurreikusitako buferraren aurretik edo ondoren irakurtzen ditu datuak. Horrek aukera eman diezaieke gaizkileei informazio konfidentziala irakurtzeko memorian, edo blokeo bat eragiteko.
5. **Eragiketen okerreko murrizketa, memoria-bufer baten mugen barruan**. Normalean, softwareak memoria-bufer batean egin ditu eragiketak, baina gerta daiteke aurreikusitako bufer-mugatik kanpoko kokaleku batean irakurtzea edo idaztea eragiketa horiek. Ondorioz, irakurketa- eta idazketa-eragiketak eman daitezke bestelako aldagai, datu-egitura eta programaren barne-datuei loturiko memoria-kokalekuetan.
6. **SQL komando batean erabilitako elementu bereziak gaizki neutralizatzea (SQL Injekzioa)**. Web-aplikazio bati egindako eraso-mota bat da, web-aplikazio horretan SQL motako sententzia maltzurrak txertatzeko aukera ematen duena. Hala, datu-baseko datu labainetara sartzeko bidea irekiko da, edo zuzenean suntsituko dira datu horiek. Honezkero, SQL injekzioa ohiko arazoa da datu-baseak oinarri dituzten webguneetan. Akatsa erraz atzematen da, baina ustiatzen ere erraza da.
7. **Informazio konfidentziala uztea baimendu gabeko erabiltzaile baten eskura.** Huts horren larritasuna ez da beti berdina, eta aplikazioa erabiltzen den testuinguruaren, agerian jarritako informazio-motaren eta erasotzaileek lor dezaketen onuraren araberakoa izaten da.
8. **Askatutako memoria erabiltzea (use after free)**. Askatutako memoriari erreferentzia egiteak programa bat blokeatzea, ustekabeko balioak erabiltzea eta kode bat exekutatzea ekar ditzake. Hainbat ondorio egon daitezke: datu baliagarriak hondatzea, kode arbitrarioa exekutatzea...
9. **Guneen arteko eskariak faltsutzea (CSRF)**. Web-zerbitzari bat bezero baten eskaria jasotzeko diseinatuta badago, baina ez badu mekanismorik asmo txarrez bidalitakoa dela egiaztatzeko, erasotzaile batek bezero hori engaina dezake web-zerbitzariari eskaera bat egin diezaion URL baten bidez, irudi-karga baten bidez, XML bidez... eta eskari hori benetakotzat joko da.
10. **Sistema eragilearen komando batean erabilitako elementu bereziak modu desegokian neutralizatzea (SEaren komandoaren injekzioa)**. Erasotzaile batek komando arriskutsuak exekuta litzake, zuzenean SEan. Ahultasun hori pribilegioak dituen programa batean badago, gainera, ahalbidetu lezake irisgarriak ez diren komandoak zehaztea, baita ordezko komandoei deitzea ere, erasotzaileak ez dituen pribilegio eta guzti.
11. **Osoek gainezka egitea (Wraparound)**. Balio oso bat handitzen bada, loturiko errepresentazioan gordetzeko handiegi bihurtzeraino, osoek gainezka egiten dute, eta arazoa segurtasunerako oso larria izan daiteke hori erabiltzen bada begizta bat kontrolatzeko, erabaki bat segurtasunez

hartzeko, eta zenbait jokabidetan (memoria esleitzea, kopia, kateamendua, eta abar) lekualdatzea eta tamaina zehazteko.

12. **Murriztutako direktorio baterako ibilbidearen izena modu desegokian mugatzea (Zeharkako ibilbidea)**. Dagokion softwareak kanpo-sarrera bat baliatzen du ibilbide-izen bat sortzeko, eta izen horren egitekoa da murriztutako direktorio nagusi baten azpian dauden fitxategiak eta direktorioak identifikatzea. Haatik, softwareak ez ditu behar bezala neutralizatzen ibilbide-izenaren barruko elementu bereziak. Hala, erasotzaile batek kokaleku murriztutik ihes egin dezake, sistemaren beste alde batzuetan dauden fitxategietara eta direktorioetara sartzeko.
13. **Baliogabeko erakusleari erreferentzia kentzea (NULL)**. Hala gertatzen da aplikazio batek ezabatzen baldin badu baliozkoa izango dela uste den baina baliogabea den erakusle baten erreferentzia. Horrek blokeoa eragin dezake, edo irtetea. Ez programatzeak, besterik gabe, halako arazoak sor ditzake.
14. **Okerreko egiaztatzea**. Hala gertatzen da erabiltzaile batek identitate jakina duela esan eta loturiko softwareak ez badu frogatzen, edo nahikoa ez den eran frogatzen badu, baieztapen hori zuzena dela.
15. **Murrizketarik gabeko fitxategi arriskutsuak kargatzea**. Softwareak aukera ematen dio erasotzaileari produktuaren ingurunean automatikoki prozesa daitezkeen fitxategi arriskutsuak kargatzeko edo transferitzeko.
16. **Baliabide erabakigarrietarako baimenak modu desegokian esleitzea**. Dagokion softwareak baimenak zehazten ditu segurtasun-baliabide erabakigarrietarako, hirugarrengoei baliabide hori irakurtzea eta eraldatzea ahalbidetuko dien modu batean; ondorioz, informazio konfidentziala uzten da agerian, baita baliabidea aldatzeko arriskua sortu ere, nahi ez den eremuetan. Hori oso arriskutsua da baliabideak zerikusia badu konfigurazioarekin, exekutatzearekin edo erabiltzailearen datu konfidentzialen erabilerarekin.
17. **Kodearen sorrera behar bezala ez kontrolatzea (Kode injekzioa)**. Softwareak goranzko osagai baten kodea eraikitzen du kanpotik kontrolatutako sarrerak baliatuz, baina sintaxia eta aurreikusitako kode-segmentuaren jokabidea alda dezaketen hainbat elementu ez ditu neutralizatzen. Kontuan eduki beharra dago prozesuaren exekuzioa eralda daitekeela datu-kanal legitimoetatik kodea bidaliz, beste inolako mekanismorik erabili gabe.
18. **Babes nahikorik gabeko egiaztagiriak**. Aplikazioak egiaztatze-baimenak transmititu edo biltegiratzen ditu, baina segurtasun gutxiko metodoa erabiltzen du, baimenik gabeko erabiltzaileek atzeman dezaketena.
19. **XML erreferentziaren murrizketa okerra**. XML fitxategi bat (URIdun XML entitateak izan ditzakeena) bidaliz, erasotzaile batek lor dezake prozesamendu-aplikazioak artxibo lokal baten edukia irakurtzea, eta hala, aplikazioa behartu dezake erasotzailea zuzenean sartu ezin den zerbitzariei irteerako eskariak bidaltzera. Eskariok firewall-aren murrizketak saihesteko erabil daitezke, baita erasoaren sorburua zein den ezkutatzeko ere.

20. **Kodetutako baimenak erabiltzea**. Software batean kodetutako baimenek huts eginez gero ate bat sor daiteke, erasotzaileari aukera emango diona softwarearen administratzaileak konfiguratu duen egiaztatze-metodoa saihesteko.
21. **Konfiantzazkoak ez diren datuei serie-kodifikazioa kentzea**. Aplikazioak serie-kodifikazioa kentzen die konfiantzazkoak ez diren datuei, behar bezain ongi egiaztatu gabe lortzen diren datuak baliagarriak ote diren. Babesteko kriptografia erabili ezean, datu horiek eraldatu egin daitezke.
22. **Pribilegioak modu desegokian kudeatzea**. Softwareak ez ditu erabiltzaile baten pribilegioak egokiro esleitzen, aldatzen, bilatzen ezta egiaztatzen ere, eta ondorioz erabiltzaile horren kontroletik at dagoen eremu bat sortzen da.
23. **Kontrolik gabeko baliabide-kontsumoa**. Dagokion softwareak ez ditu behar bezala kontrolatzen baliabide mugatu baten esleipena eta mantentzea. Horrek aukera ematen du kontsumitutako baliabideen kantitatean eragiteko, eta azkenik, agortu egiten dira baliabide erabilgarriak.
24. **Funtzio erabakigarrietarako egiaztatzerik eza**. Programak ez du egiaztatzerik egiten frogatzeko moduko erabiltzaile-nortasun bat eskatzen duten funtzionalitateetarako, edo baliabide-kantitate esanguratsua kontsumitzen du.
25. **Desagertutako baimena**. Softwareak ez ditu baimenak egiaztatzen erabiltzaile bat baliabide batera iristen edo ekintza bat gauzatzen saiatzen denean, eta hala, sarbidea errazten du baimendu gabekoak beharko luketen datu eta ekintzetarako. Horrek hainbat arazo sortzen ditu: informazioa agerian uztea, zerbitzua ukatzea eta kode arbitrarioa exekutatzea.

Oso top 25 baliagarria zibersegurtasunaren alorreko profesionalentzat

CWE zerrendan balizko 700 errore baino gehiago badaude ere, atera daitekeen ondorioa da horietatik zortzik baino ez dutela arriskua eragiten. Hau da, eraso bat arrakastaz egiteko balia daitekeen akatsik izatekotan, zortzi errore hauetako bat egongo da tartean:

- Datuak irakurtzea.
- Datuak aldatzea.
- Zerbitzua ukatzea (DOS). Ez fidatzeko moduko exekutatzea.
- Zerbitzua ukatzea (DOS). Baliabide-kontsumoa.
- Baimendu gabeko kodeak edo komandoak exekutatzea.
- Pribilegioak eskuratzea edota besteren nortasuna hartzea.
- Bypassa babesteko mekanismoak.
- Jarduerak ezkutatzea.

Azken batean, softwarea eta hardwarea garatzen dute enpresek, baita segurtasunaren arloko profesionalek ere, ahultasunak atzemateko, deuseztatzeko eta arintzeko erabiltzen dute gaur egun CWE lanabesa. CWE

zerrenda doako baliabidea da, kanpoko eraso bat eragin dezaketen programazio-errore zabalduenak identifikatzen dituena. Halako hutsak erraz aurkitu ohi dira, baina ziberkriminalentzat ere erraza da haietaz baliatzea.

.

info@bcsc.eus | 945 236 636

Parque Tecnológico de Álava
Albert Einstein. 46-3ª – Ed. E7 01510
Vitoria-Gasteiz