Kudeaketaren eta Informazio Sistemen Informatikaren Ingeniaritzako Gradua

Maskoten erregistroa

Entrega 2. txostena

Informazio Sistemen Segurtasuna Kudeatzeko Sistemak

Egileak:

Lucia Del Rio, Mikel Eguia
Olatz Elejalde, Asier Las Hayas
Maider Tato, Ainhoa Tomás

Irakaslea:

Mikel Egaña Aranguren

November 7, 2025

Contents

1 Sarrera

Entrega honen helburua 1.zereginean garatutako Web Sistemaren segurtasuna aztertzea da, OWASP ZAP tresnaren metodologia eta OWASP Top 10 informean oinarrituta. Analisi honen bidez, aplikazioan ager daitezkeen ahultasun arruntak identifikatu dira.

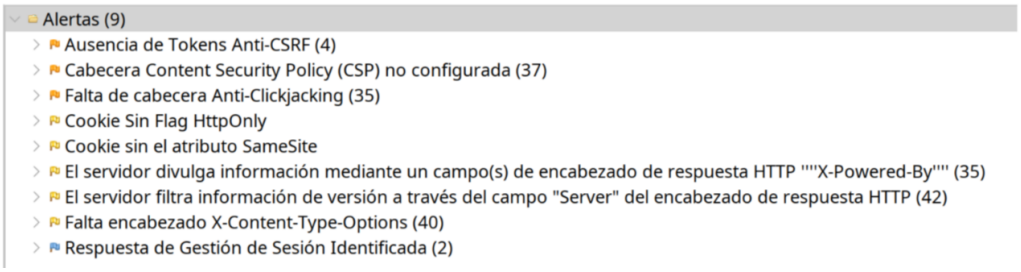
Arazo hauek konpontzea oso garrantzitsua da web sistema seguru mantentzeko eta erabiltzaileen informazioaren segurtasuna erasoen aurka seguru egoteko. Arazo hauek konfidentzialtasuna, integritatea eta erabilgarritasuna arriskuan jartzen dute.

Sistemak 3 puntu garrantzitsuetan ahula da:

- Eskaeren falsifikazioa: Oinarrizko Tokens Anti-CSRF gabezia bat detektatu da, arrisku handikotzat sailkatzen den ahultasun bat, erasotzaileei aukera ematen dielako autentifikatutako erabiltzaileak nahigabeko ekintzak egitera behartzeko, sistemak erabiltzailearen saioan duen konfiantza ustiatuz.
- Goiburuak gogortzea HTTP: Segurtasun-buru modernoak inplementatzeko falta sistemikoa dago. Ahulezia horrek nabigatzailearen defentsak desaktibatzen ditu, Cross-Site Scripting (XSS) eta Clickjacking bezalako erasoek arrakasta izateko probabilitatea handituz.
- Saio ez seguruen kudeaketa: Saioko cookieen konfigurazioak ez ditu barne hartzen HttpOnly eta SameSite funtsezko atributuak. Horrek bide erraza ematen du saioak bahitzeko XSS baten kasuan, eta CSRF erasoak errazten ditu.

2 Segurtasun Ahultasunak

ZAP tresnak 9 alerta identifikatu ditu, horien artean 8 ahultasun.



2.1 Tokens Anti-CSRF ez egotea

2.1.1 OWASP klasifikazioa

- OWASP Top 10 2021: A01 - Sarbide kontrolaren galera
- OWASP Top 10 2017: A05 - Sarbide kontrolaren galera

2.1.2 Ahuleziaren deskribapena

Bidalketa formularioan ez dira Anti-CSRF tokenik aurkitu. Eskaera faltsu bat eraso batean dauden guneen artean, biktima bat konprometitzen eta behartzen duena bere HTTP eskaera jomuga batera bidaltzera, biktima gisa ekintza bat egin ahal izateko haren ezagutzarik edo asmorik gabe. Arrazoi ezkutua aplikazioaren funtzionaltasuna da, URL/formularioko ekintzak erabiliz, behin eta berriz igar daitezkeenak. Erasoaren izaera da CSRGk webgune batek erabiltzaile bati ematen dion konfiantza ustiatzen duela. Aitzitik, gune gurutzatuetako komando-kateek (XSS) erabiltzaile batek webgune batean ematen duen konfiantza ustiatzen dute. XSS bezala, CSRG erasoak ez dira beharrezkoa leku gurutzatuak, baina izan daitezke. CSRF, XSRG, klik bakarreko erasoak, saioa muntatzea, diputatu nahastua eta itsas zabalean nabigatzea ere esaten zaie eskaeren faltsifikazioari.

CSRGren erasoak oso eraginkorrak dira hainbat egoeratan, besteak beste:

- Biktimak saio aktiboa du helmugako lekuan.
- Biktimak baimena du helmugako gunean HTTP autentifikazioa egiteko.
- Biktima helmugako gunearen sare lokal berean dago.

CSRF bereziki erabili da leku objektibo baten aurkako ekintza bat biktimaren pribilegioak erabiliz egin ahal izateko, baina informazioa zabaltzeko teknika berriak azaldu dira, erantzuna eskuratzean. Informazioa zabaltzeko arriskua izugarri handitzen da helmugako gunea XSSrako kaltebera denean; izan ere, XSS CSRFrako plataforma gisa erabil daiteke, eta horrek aukera ematen dio erasotzaileari jatorrizko politika bereko liiten barrutik jarduteko.

2.1.3 Eragin potentziala

Ertaina. Erasotzaile batek saio aktiboa duen erabiltzaile bat behartu dezake ekintza sentikorrak egitera, haren ezagutzarik eta baimenik gabe. Horren barruan sartzen da pasahitzak aldatzea,

profilak aldatzea, erosketak egitea edo, administratuz gero, komandoak exekutatzea. Zuzeneko eragina datuen osotasuna galtzea eta kontuaren konpromisoa da.

2.1.4 Gertatzeko arrazoia

Tokens Nonce ez ezartzea. HTTP formularioa ez du jasotzen egoera-aldaketaren eskaera bakoitzarekin zerbitzarian baliozkotu behar den token balio bakar, sekretu eta aurreikusezinik (nonce).

2.1.5 Gertatzeko probabilitatea

Handia. Ustiategiak eskatzen duen bakarra da biktimak, saio aktibo batekin, webgune maltzur bat bisitatzea, eskaera gune zaurgarrira bidaltzen duen kodea duena. Formularioko ekintza aurreikus badaiteke, erasoa diseinatzearen hutsala da.

2.2 Content Security Policy goiburua konfiguratu gabe

2.2.1 OWASP klasifikazioa

- OWASP Top 10 2021: A05 - Segurtasun konfigurazio okerra
- OWASP Top 10 2017: A06 - Segurtasun konfigurazio okerra

2.2.2 Ahuleziaren deskribapena

Edukiaren segurtasun-politika (CSP) segurtasun-geruza gehigarri bat da, zenbait eraso mota detektatzen eta arintzen laguntzen duena, Cross Site Scripting (XSS) eta datuak injektatzeko erasoak barne. Eraso hauek denetarako erabiltzen dira, datuen lapurretatik hasi eta gunearen desitxuraketaraino edo malware-banaketaraino. CSPk HTTP izenburu estandarren multzo bat eskaintzen du, webguneen jabeei aukera ematen diena onartutako eduki-iturriak adierazteko nabigatzaileek orrialde horretan kargatu ahal izateko; estalitako motak hauek dira: JavaScript, CSS, HTML markoak, iturriak, irudiak eta txertatutako objektuak, hala nola Java appletak, ActiveX, audio- eta bideo-fitxategiak.

2.2.3 Eragin potentziala

Ertaina. CSPrik gabe, erasotzaile batek aplikazioan kode maltzurra (XSS) injektatzea lortzen badu, nabigatzaileak kode hori mugarik gabe kargatu eta exekutatuko du. Horrek saioko cookie-ak lapurtzea, erabiltzaileak birbideratzea edo gunea aldatzea eragin dezake.

2.2.4 Gertatzeko arrazoia

Zerbitzariaren konfigurazioan omisioa. Web-zerbitzaria ez dago konfiguratuta Content-Security-Policy goiburua segurtasun-direktibak dituzten HTTP erantzunetan sartzeko.

2.2.5 Gertatzeko probabilitatea

Ertaina/altua. CSPk XSSa aurreikusten ez duen arren, ustiapena askoz ere zailagoa da, eta, beraz, ez edukitzeak nabarmen handitzen du edozein injekzio-atakek arrakasta izateko probabilitatea.

2.3 Anti-Clickjacking goiburua konfiguratu gabe

2.3.1 OWASP klasifikazioa

- OWASP Top 10 2021: A05 - Segurtasun Konfigurazio okerra
- OWASP Top 10 2017: A06 - Segurtasun konfigurazio okerra

2.3.2 Ahuleziaren deskribapena

HTTP erantzunak ez du Clickjackingen aurkako babes-mekanismorik barne hartzen (klik bahiketa). Clickjacking-ak engainatu egiten du erabiltzailea aplikazioaren elementu sentikor batean klik egin dezan, erasotzailearen orrian klik egiten ari dela uste duenean.

2.3.3 Eragin potentziala

Ertaina. Erasotzaile batek ekintza kritikoko botoietan klik egitera behartu dezake erabiltzailea nahi ez diren ekintzak eta sistemaren osotasun funtzionala galduz.

2.3.4 Gertatzeko arrazoia

Markoaren goiburuak ez aipatzea. Zerbitzariak ez ditu X-Frame-Options goiburukoa edo frame-ancestors direktiba ezartzen Content-Security-Policyren barruan.

2.3.5 Gertatzeko probabilitatea

Ertaina. Nolabaiteko gizarte-ingeniaritza behar du biktima orri maltzurrera erakartzeko, baina helburu-orriak ekintza sentikorrak eta aurreikusteko modukoak baditu, erasoa egingarria da.

2.4 Cookie Flag barik HttpOnly

2.4.1 OWASP klasifikazioa

- OWASP Top 10 2021: A05 - Segurtasun konfigurazio okerra
- OWASP Top 10 2017: A06 - Segurtasun konfigurazio okerra

2.4.2 Ahuleziaren deskribapena

Cookie bat ezarri da HttpOnly flag gabe, eta horrek esan nahi du JavaScript cookiera sar daitekeela. Script maltzur bat orri honetan exekutatu badaiteke, orduan cookiea irisgarria izango da eta beste toki batera transmititu ahal izango da. Saioko cookie bat bada, saioa bahitzea posible izan daiteke.

2.4.3 Eragin potentziala

Baxua. Aplikazioa XSSrako kaltebera bada, erasotzaile batek script bat exekutatu ahal izango du, document.cookie-ra sartzeko, saioko cookiearen balioa lapurtzeko eta bere zerbitzariari bidaltzeko. Horri esker, saioa bahitzen da, eta erasotzaileak biktimaren kontua kontrolatzen du.

2.4.4 Gertatzeko arrazoia

Saioko cookiearen konfigurazio okerra. Web-zerbitzariak edo cookiea ezartzen duen aplikazioaren funtzioak ez du HttpOnly atributua barne hartzen.

2.4.5 Gertatzeko probabilitatea

Ertaina/Altua. Arriskua XSS kalteberatasunaren mende dago, baina baldin badago, cookiearen lapurreta urrats hutsala da erasotzailearentzat.

2.5 Cookie SameSite atributurik gabe

2.5.1 OWASP klasifikazioa

- OWASP Top 10 2021: A01 - Sarbide kontrolaren galera
- OWASP Top 10 2017: A05 - Sarbide kontrolaren galera

2.5.2 Ahuleziaren deskribapena

Cookie bat ezarri da SameSite atributurik gabe, eta horrek esan nahi du cookiea 'cross-site' eskaera baten emaitza gisa bidal daitekeela. SameSite atributua neurri eraginkorra da guneen arteko eskaeren faltsifikazioari, guneen arteko script-ak sartzeari eta sinkronizazio-erasoei aurre egiteko.

2.5.3 Eragin potentziala

Baxua. Ezaugarri hori ez izateak zuzenean errazten ditu CSRFren erasoak, saioaren cookiea automatikoki bidaliko baita erasotzailearen gunetik egindako eskaeretan.

2.5.4 Gertatzeko arrazoia

Cookiean segurtasun-atributua ez ematea. Saioko cookiearen konfigurazioak ez du zehazten SameSite balioa.

2.5.5 Gertatzeko probabilitatea

Altua. CSRFren aurkako lehen mailako defentsa-neurria da hau. Ez egoteak eraso-azalera handitzen du eta cross-site erasoak egitea errazten du.

2.6 Zerbitzariak informazioa zabaltzen du X-Powered-By goiburuaren bidez

2.6.1 OWASP klasifikazioa

- OWASP Top 10 2021: A01 - Ez baimendutako datu sentikorren sustraketa
- OWASP Top 10 2017: A03 - Ez baimendutako datu sentikorren sustraketa

2.6.2 Ahuleziaren deskribapena

Web/aplikazioaren zerbitzaria informazioa zabaltzen ari da HTTP "" X-Powered-By "erantzun-goiburu baten edo gehiagoren bidez. Informazio hori eskuratzeak aukera eman liezaieke erasotzaileei web-aplikazioa mende duten beste esparru/osagai batzuk identifikatzeko, bai eta osagai horiek izan ditzaketen kalteberatasunak identifikatzeko ere.

2.6.3 Eragin potentziala

Baxua. Erasotzaile batek informazio hori erabiltzen du errekonozimendurako, helburuak identifikatzeko behar den ahalegina murriztuz. Framework zehatza ezagutzean, bertsio horri lotutako ahultasun publikoak (CVE) azkar bila ditzakezu eraso zuzen eta eraginkorrago bat diseinatzeko.

2.6.4 Gertatzeko arrazoia

Framework edo aplikazio-zerbitzariaren konfigurazio lehenetsia. Garapen frameworks askok goiburu hau automatikoki barne hartzen dute informazio edo arazketa helburuetarako, eta produkzio etapan ez da ezabaketa konfiguratu.

2.6.5 Gertatzeko probabilitatea

Baxua. Hori ez da zuzeneko ustiapenaren urrakortasun bat, baizik eta informazioaren filtrazio bat, eraso baten hasierako etapak erraztu eta bizkortzen dituena.

2.7 Zerbitzariak bertsio-informazioa iragazten du "Server" eremuaren bidez

2.7.1 OWASP klasifikazioa

- OWASP Top 10 2021: A05 - Segurtasun konfigurazio okerra
- OWASP Top 10 2017: A06 - Segurtasun konfigurazio okerra

2.7.2 Ahuleziaren deskribapena

Web-zerbitzaria/aplikazioa bertsio-informazioa iragazten ari da HTTP "Server" erantzun-goiburuaren bidez. Informazio hori eskuratzeak aukera eman diezaieke erasotzaileei web zerbitzariak/aplikazioak dituen beste kalteberatasun batzuk identifikatzeko.

2.7.3 Eragin potentziala

Baxua. Aurreko kasuaren antzera, informazio horrek erasotzaile bati bere estrategia fintzen laguntzen dio. Zero eguneko kalteberatasun bat edo zerbitzariaren bertsioarentzat espezifikoa den CVE publiko bat ezagutzen bada, eskalatzeko edo zerbitzua ukatzeko eraso arrakastatsu baten probabilitatea handitu egin daiteke.

2.7.4 Gertatzeko arrazoia

Web zerbitzariaren konfigurazio lehenetsia. Apache edo Nginx bezalako zerbitzariek lehenetsitako bertsioko informazio hori izan ohi dute. Ez da aplikatu hardening-konfiguraziorik xehetasun orokorrak kentzeko edo emateko.

2.7.5 Gertatzeko probabilitatea

Baxua. Aintzatespen-alerta bat da batez ere, eta "defentsa sakonaren" segurtasun-printzipioa urratzen du.

2.8 X-Content-Type-Options goiburua falta da

2.8.1 OWASP klasifikazioa

- OWASP Top 10 2021: A05 - Segurtasun konfigurazio okerra
- OWASP Top 10 2017: A06 - Segurtasun konfigurazio okerra

2.8.2 Ahuleziaren deskribapena

Anti-MIME-Sniffing X-Content-Type-Options goiburua ez da 'nosniff' hizkuntzan ezarri. Horri esker, Internet Explorer eta Chrome-ren aurreko bertsioek MIME-sniffing egiten dute erantzunaren gorputzean, eta horrek eragin dezake gorputzak erantzuna ematea eta adierazitako eduki mota ez den eduki mota gisa interpretatzea eta erakustea. Egungo bertsioek (2014ko printzipioak) eta Firefoxetik heredatutakoek aitortutako eduki mota erabiliko dute (bat ezartzen bada), MIME-sniffing egin beharrean.

2.8.3 Eragin potentziala

Baxua. Nabigatzaile zaharragoetan, edo injekzio-urrakortasun batekin konbinatuta, erasotzaile batek mota exekutagarri gisa interpretatzen den edukia bidal dezake, zerbitzariak text/plain gisa etiketatu badu ere. Horrek kode maltzurra betearaztea ekar lezake.

2.8.4 Gertatzeko arrazoia

Anti-MIME-Sniffing goiburua ez aipatzea. Zerbitzaria ez dago konfiguratuta segurtasun-goiburu hori sartzeko.

2.8.5 Gertatzeko probabilitatea

Ertaina. Arrisku esanguratsua da erasotzaileak erantzunaren edukia kontrola dezakeen orrietan, hala nola errore-orri pertsonalizatuetan edo mezuetan.

2.9 Identifikatutako saioa kudeatzeko erantzuna

2.9.1 Alertaren deskribapena

Emandako erantzunak saioa kudeatzeko token bat duela identifikatu du. 'Other Info' eremuak Header Based Session Management metodoan (goiburuan oinarritutako saioaren kudeaketa) erabil daitezkeen goiburuko token-multzo bat dauka. Eskaera "Auto-Detect" sisteman ezarritako Session Management metodo bat duen testuinguru batean badago, arau horrek saioaren kudeaketa aldatuko du identifikatutako tokenak erabiltzeko.
Alerta hau, berez, ez da ahulezi bat, alerta informatibo bat baizik.

3 Ondorioak

Azterketa egin ondoren, aplikazioak dituen ahultasunak antzeman dira, batez ere saio-kudeaketa eta segurtasun-konfigurazioen arloetan.
3. Entregan, ahultasun horien konponketak egingo dira eta ZAP tresnaren bidez bigarren azterketa egingo da, ezarritako segurtasun-neurriak behar bezala funtzionatzen dutela egiaztatzeko.