entrega_2

WebOrrian-ren ahuleziak

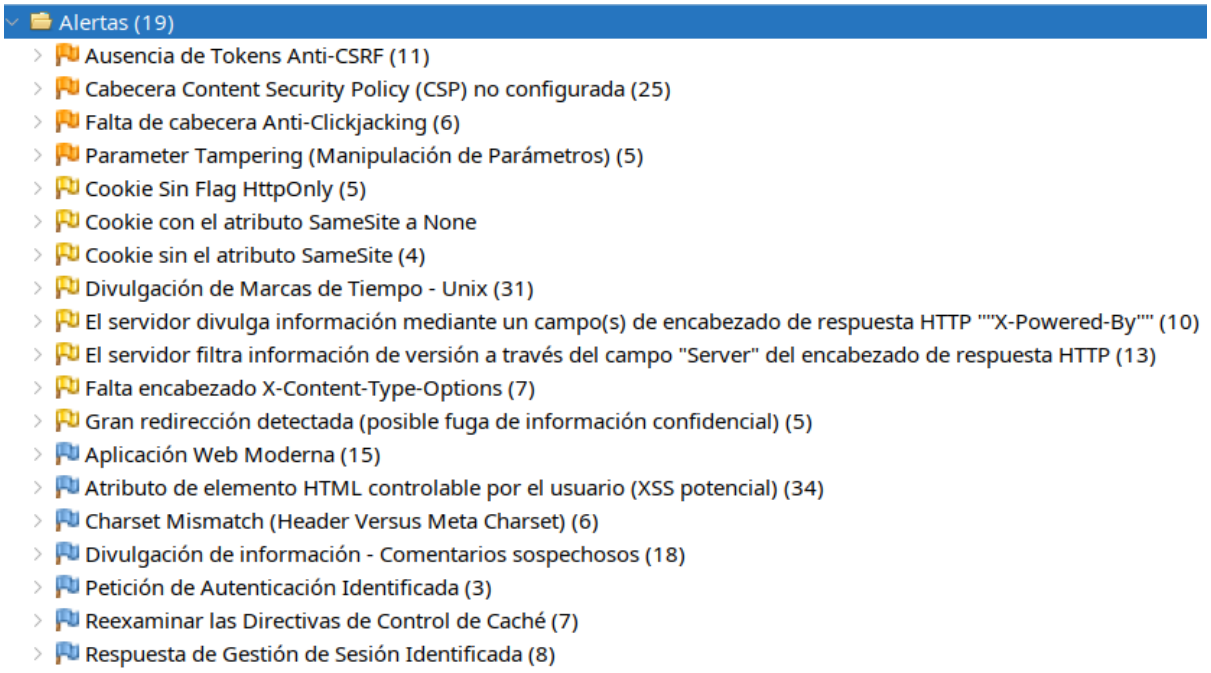
Egileak: Lier Laiseka, Hodei Castro, Andoni Ortiz De Zarate eta Asier Fernández.

Aurkibidea

Guk aurkitutako ahuleziak

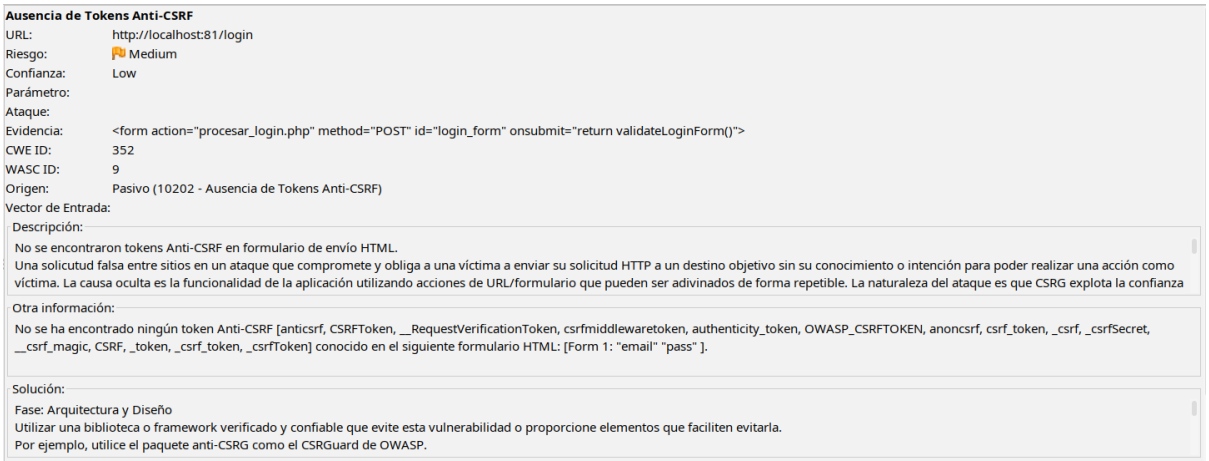
1) Web orria http erabiltzen du. Http erabili beharrean hobeto izango litzateke https, zeren eta, zifraketa seguruagoa da eta SSL zertifikatuak erabiltzen dira zerbitzaria balidatzeko.

ZAP-ek aurkitutako ahuleziak



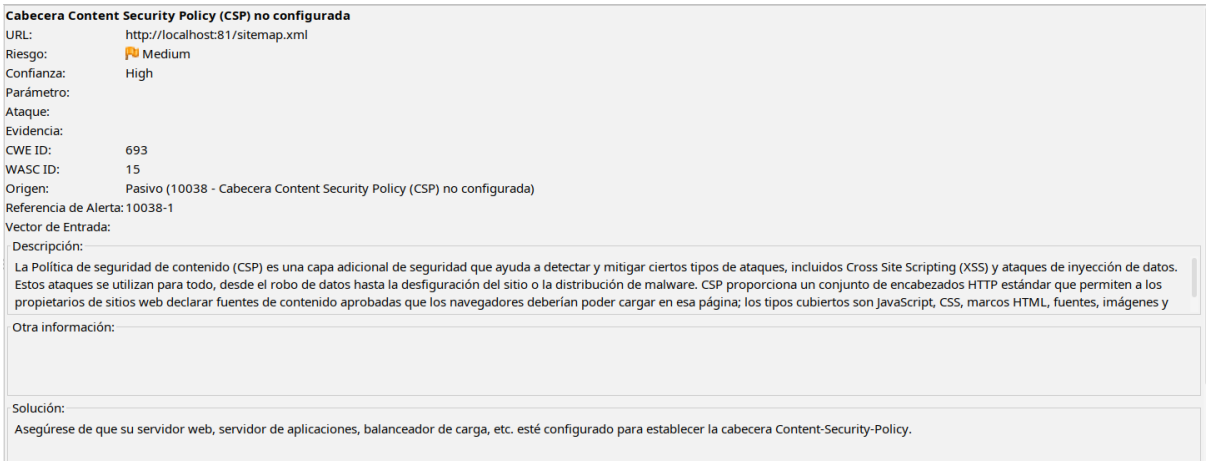
Anti-CSRF aurkako tokenik ez

Token CSRF bat ez dauka, hau eskaerak nahi dugun igorletik datorren edo ez ziurtatzen du. Hau konpontzeko, formulario bakoitzean CSRF token bat gehitu behar da, eta eskaera prozesatu aurretik zerbitzarian balioztatu beharko litzateke.



Content Security Policy (CSP) goiburua ez dago konfiguratuta

Zerbitzariak ez du bidaltzen Content-Security-Policy goiburua, kanpoko zer baliabide kargatu daitezkeen adierazten duena. Hau falta denez, errazagoa da erasotzaile batek kode maltzurra eranztea. CSP politika bat ezarriz baimendutako edukia mugatuko da.



Cabecera Content Security Policy (CSP) no configurada

URL: http://localhost:81/sitemap.xml
Riesgo: Medium
Confianza: High
Parámetro:
Ataque:
Evidencia:
CWE ID: 693
WASC ID: 15
Origen: Pasivo (10038 - Cabecera Content Security Policy (CSP) no configurada)
Referencia de Alerta: 10038-1
Vector de Entrada:

Descripción:

La Política de seguridad de contenido (CSP) es una capa adicional de seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y

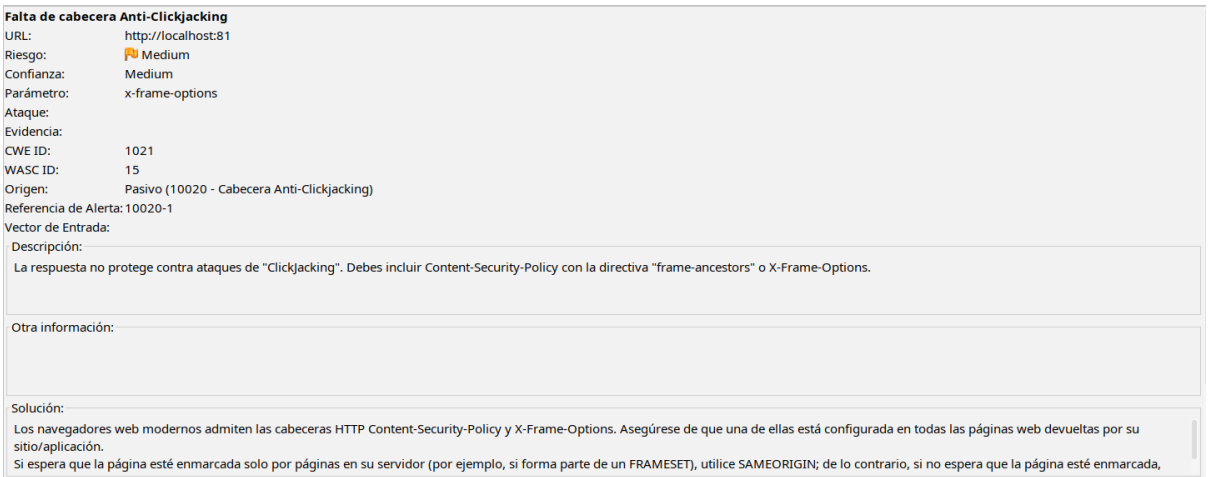
Otra información:

Solución:

Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.

Anti-Clickjacking goiburu falta

Orria iframe baten barruan sar daiteke beste leku batetik, eta horrek clickjacking erasoak egiteko aukera ematen du (hau da, erabiltzaileak klik egin dezake nahigabe ezkutuan dagoen botoi edo link batean). Konpontzeko, gehitu beharko da kanpoko iframeak blokeatuko dituen http goiburua.



Falta de cabecera Anti-Clickjacking

URL: http://localhost:81
Riesgo: Medium
Confianza: Medium
Parámetro: x-frame-options
Ataque:
Evidencia:
CWE ID: 1021
WASC ID: 15
Origen: Pasivo (10020 - Cabecera Anti-Clickjacking)
Referencia de Alerta: 10020-1
Vector de Entrada:

Descripción:

La respuesta no protege contra ataques de "ClickJacking". Debes incluir Content-Security-Policy con la directiva "frame-ancestors" o X-Frame-Options.

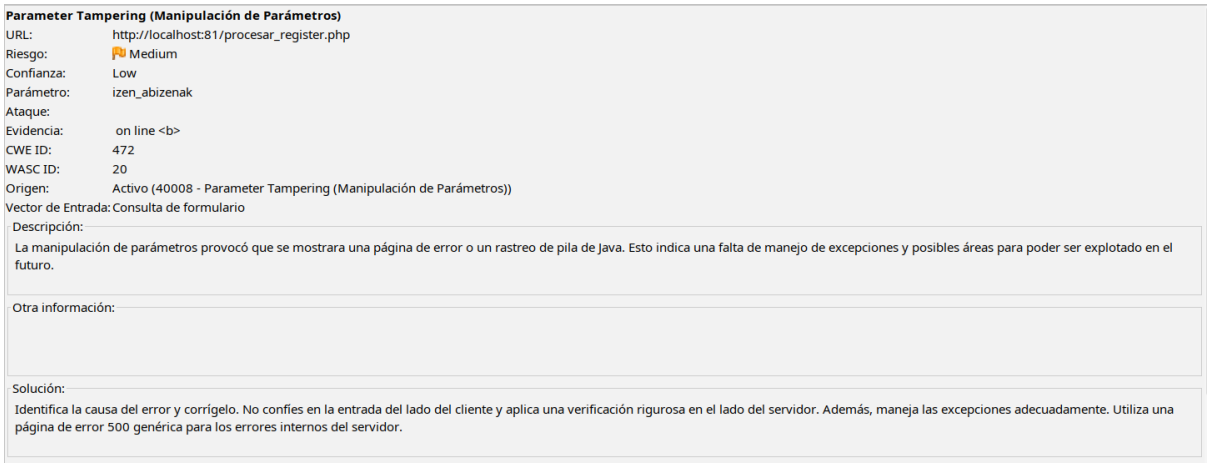
Otra información:

Solución:

Los navegadores web modernos admiten las cabeceras HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que una de ellas está configurada en todas las páginas web devueltas por su sitio/aplicación.
Si espera que la página esté enmarcada solo por páginas en su servidor (por ejemplo, si forma parte de un FRAMESET), utilice SAMEORIGIN; de lo contrario, si no espera que la página esté enmarcada,

Parameter Tampering (Parkametroen manipulatzea)

Zerbitzariak ez ditu behar bezala balioztatzen bezeroak bidalitako datuak, eta erasotzaile batek datu horiek aldatzea posible egiten du, horregatik nahi ez diren erroreak edo portaerak eragin daitezke. Datu guztiak balidatuz zerbitzariaren aldean konponduko da.



Parameter Tampering (Manipulación de Parámetros)

URL: http://localhost:81/procesar_register.php
Riesgo: Medium
Confianza: Low
Parámetro: izen_abizenak
Ataque:
Evidencia: on line <b>
CWE ID: 472
WASC ID: 20
Origen: Activo (40008 - Parameter Tampering (Manipulación de Parámetros))
Vector de Entrada: Consulta de formulario

Descripción:
La manipulación de parámetros provocó que se mostrara una página de error o un rastreo de pila de Java. Esto indica una falta de manejo de excepciones y posibles áreas para poder ser explotado en el futuro.

Otra información:

Solución:
Identifica la causa del error y corrígelo. No confíes en la entrada del lado del cliente y aplica una verificación rigurosa en el lado del servidor. Además, maneja las excepciones adecuadamente. Utiliza una página de error 500 genérica para los errores internos del servidor.

Flag HttpOnly gabeko Cookie-a

Saioko cookie-ak ez du HttpOnly flag-a, eta, horregatik, JavaScriptek irakurri ahal izango du. XSS ahultasun bat badago, erasotzaile batek lapurtu eta saioa bahitu lezake. Cookie-ak HttpOnly atributuarekin konfiguratuz konpondu daiteke.

Cookie Sin Flag HttpOnly

URL: http://localhost:81
Riesgo: Low
Confianza: Medium
Parámetro: PHPSESSID
Ataque:
Evidencia: Set-Cookie: PHPSESSID
CWE ID: 1004
WASC ID: 13
Origen: Pasivo (10010 - Cookie Sin Flag HttpOnly)
Vector de Entrada:

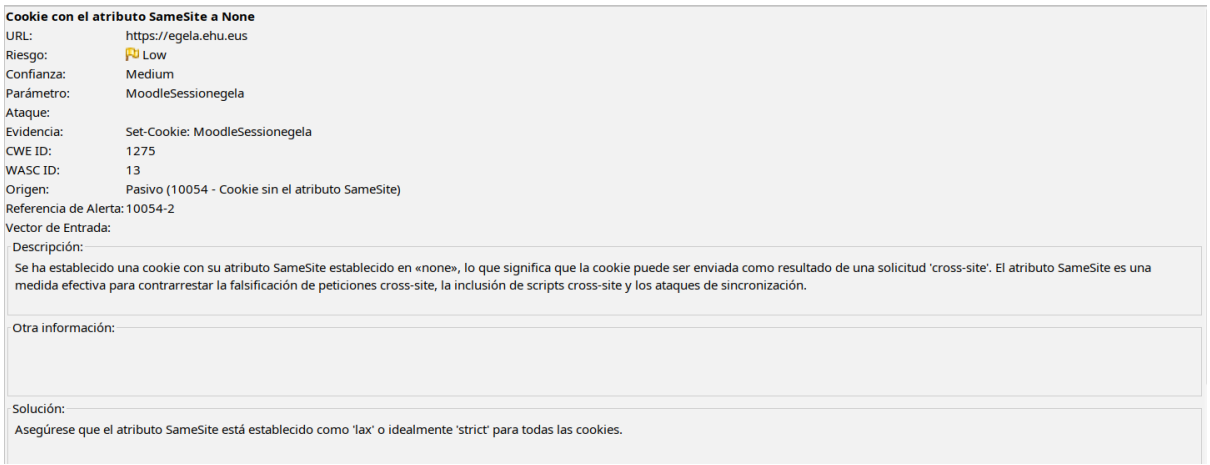
Descripción:
Se ha establecido una cookie sin el flag HttpOnly, lo que significa que JavaScript puede acceder a la cookie. Si un script malicioso puede ser ejecutado en esta página, entonces la cookie será accesible y puede ser transmitida a otro sitio. Si se trata de una cookie de sesión, el secuestro de sesión puede ser posible.

Otra información:

Solución:
Asegúrese de que la flag HttpOnly está establecida para todas las cookies.

SameSite atributua duen Cookie-a = None

SameSite = None atributuak aukera ematen du cookie-a guneen arteko eskaeretan ere bidaltzeko. Horrek CSRF erasoen eraginpean jar dezake Secure-rekin konbinatzen ez bada. Hau konpondu daiteke, soilik SameSite = None erabiltzen beharrezkoa bada eta beti Secure-rekin.



Cookie con el atributo SameSite a None

URL:	https://egela.ehu.eus
Riesgo:	Low
Confianza:	Medium
Parámetro:	MoodleSessionegela
Ataque:	
Evidencia:	Set-Cookie: MoodleSessionegela
CWE ID:	1275
WASC ID:	13
Origen:	Pasivo (10054 - Cookie sin el atributo SameSite)
Referencia de Alerta:	10054-2
Vector de Entrada:	

Descripción:

Se ha establecido una cookie con su atributo SameSite establecido en «none», lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida efectiva para contrarrestar la falsificación de peticiones cross-site, la inclusión de scripts cross-site y los ataques de sincronización.

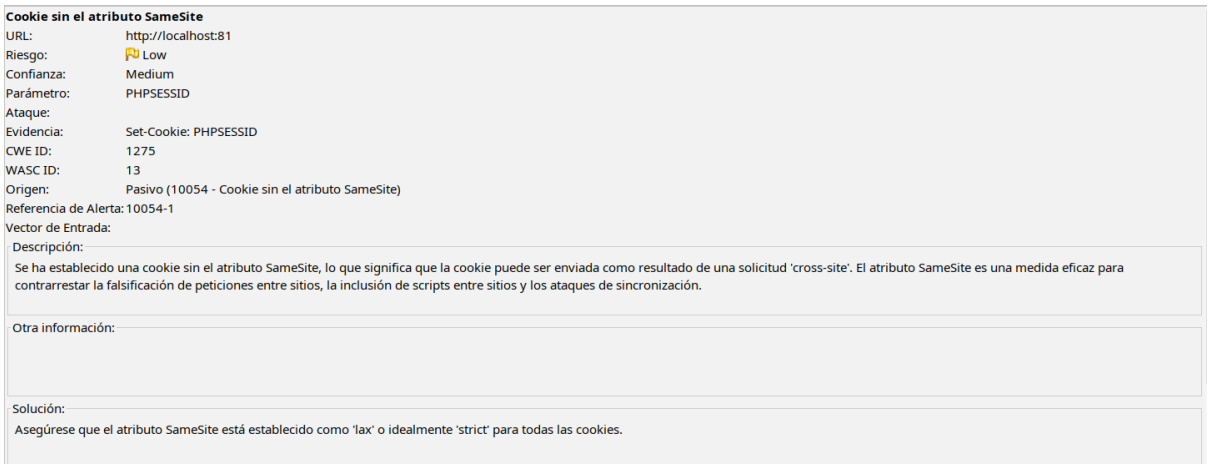
Otra información:

Solución:

Asegúrese que el atributo SameSite está establecido como 'lax' o idealmente 'strict' para todas las cookies.

Cookie SameSite atributua gabe

SameSite definitzen ez bada, nabigatzaileak cookie-a bidali dezake kanpoko eskaeretan, eta horrek CSRF erasoen arriskua areagotzen du. SameSite atributua kasuaren arabera zehazten konponduko da.



Cookie sin el atributo SameSite

URL:	http://localhost:81
Riesgo:	Low
Confianza:	Medium
Parámetro:	PHPSESSID
Ataque:	
Evidencia:	Set-Cookie: PHPSESSID
CWE ID:	1275
WASC ID:	13
Origen:	Pasivo (10054 - Cookie sin el atributo SameSite)
Referencia de Alerta:	10054-1
Vector de Entrada:	

Descripción:

Se ha establecido una cookie sin el atributo SameSite, lo que significa que la cookie puede ser enviada como resultado de una solicitud 'cross-site'. El atributo SameSite es una medida eficaz para contrarrestar la falsificación de peticiones entre sitios, la inclusión de scripts entre sitios y los ataques de sincronización.

Otra información:

Solución:

Asegúrese que el atributo SameSite está establecido como 'lax' o idealmente 'strict' para todas las cookies.

Denbora-marken zabalkundea – Unix

Guneak denbora markak erakusten ditu, sistemaren edo exekuzio une zehatzaren informazioa erakusteko. Horrela, erasotzaile batek bertsioak, jarduerak edo eraso-leihoak ondoriozta ditzake. Hau konpontzeko ez da erakutsiko zerbitzariaren datak edo timestamp-ak erantzunetan. Ez dira sartukos barne-denborarik http goiburuetan eta iturburu-kodean ere ez.

Divulgación de Marcas de Tiempo - Unix

URL: https://egela.ehu.eus/login/index.php?lang=it
Riesgo: Low
Confianza: Low
Parámetro:
Ataque:
Evidencia: 1761633634
CWE ID: 497
WASC ID: 13
Origen: Pasivo (10096 - Divulgación de Marcas de Tiempo)
Vector de Entrada:

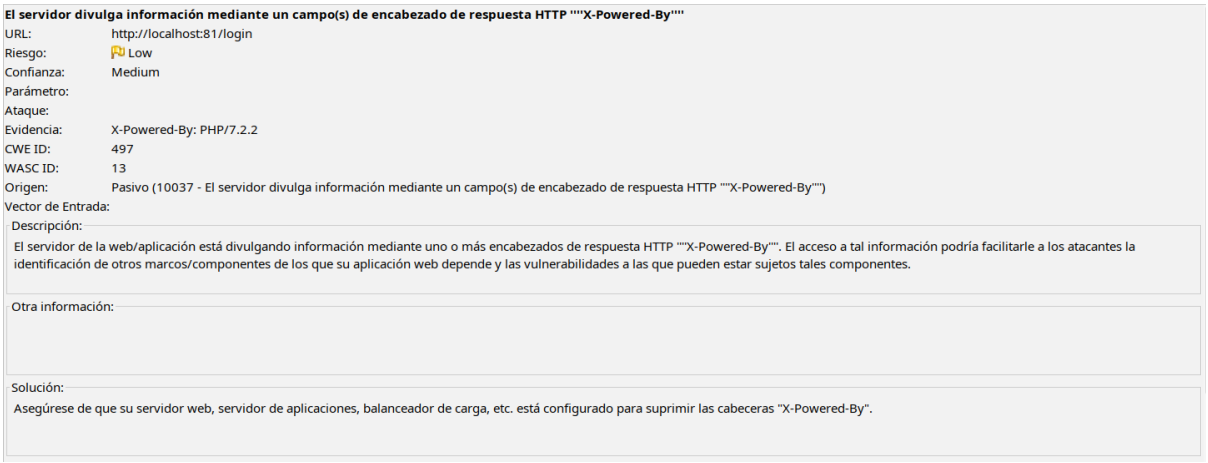
Descripción:
Una marca de tiempo fue revelada por la aplicación/servidor web. - Unix

Otra información:
1761633634, que se evalúa como: 2025-10-28 07:40:34.

Solución:
Confirmar que los datos encontrados de información sobre la marca de tiempo no son sensibles, ni se pueden usar en patrones explotables de divulgación.

Zerbitzariak informazioa zabaltzen du erantzun-goiburuko HTTP eremu baten bidez ‘’’’’’X-Powered-By’’’’’’’

Zerbitzariak erabilitako teknologia adierazten du, eta horrek zer ahultasun egon litezkeen adierazten die erasotzaileei. Goiburu hori desgaituz konponduko da.



El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By""

URL: http://localhost:81/login
Riesgo: Low
Confianza: Medium
Parámetro:
Ataque:
Evidencia: X-Powered-By: PHP/7.2.2
CWE ID: 497
WASC ID: 13
Origen: Pasivo (10037 - El servidor divulga información mediante un campo(s) de encabezado de respuesta HTTP ""X-Powered-By"")
Vector de Entrada:

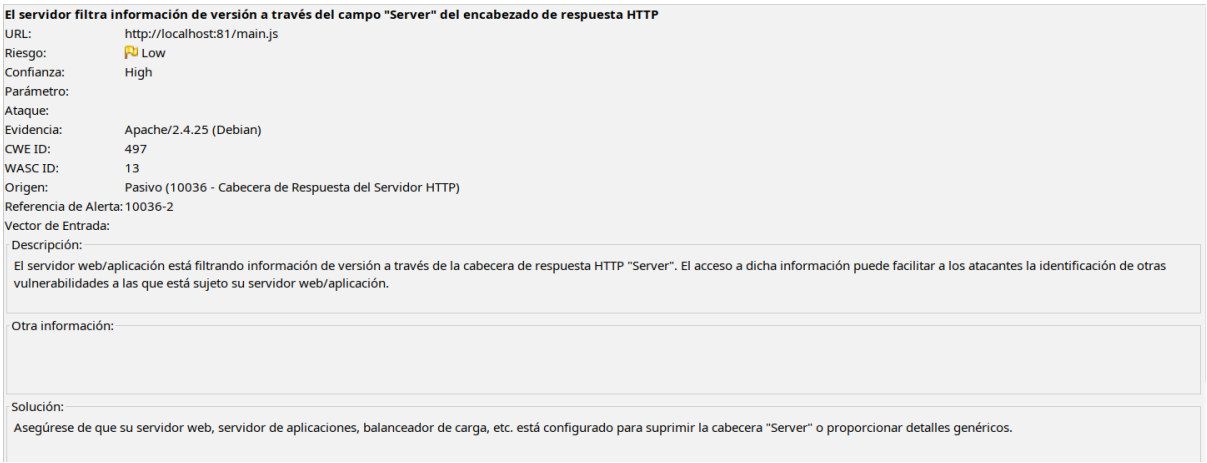
Descripción:
El servidor de la web/aplicación está divulgando información mediante uno o más encabezados de respuesta HTTP ""X-Powered-By"". El acceso a tal información podría facilitarle a los atacantes la identificación de otros marcos/componentes de los que su aplicación web depende y las vulnerabilidades a las que pueden estar sujetos tales componentes.

Otra información:

Solución:
Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. está configurado para suprimir las cabeceras "X-Powered-By".

Zerbitzariak bertsio-informazioa iragazten du, HTTP erantzun-goiburuko “Server” eremuaren bidez.

Server goiburuak softwareari eta bertsioari buruzko informazioa ematen du, eraso espezifikoetarako erabilgarria dena. Konpontzeko, goiburua kendu beharko da.

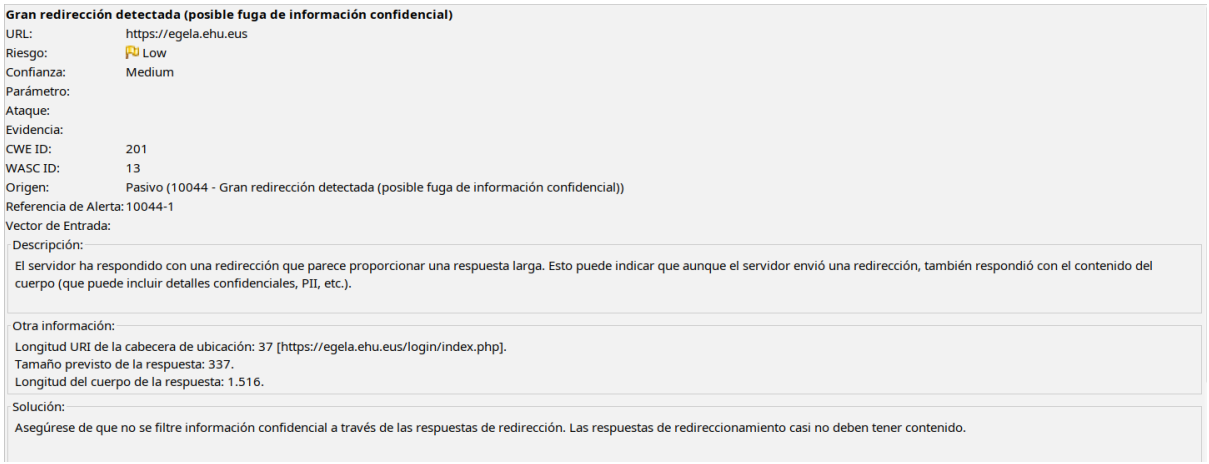


X-Content-Type-Options goiburu falta

Nabigatzailea eduki mota asmatzen saia daiteke, eta horrek kode maltzurra exekutatzea ekar dezake. Http goiburu hau sartuz konponduko da: “X-Content-Type-Options: nosniff”

Birbideratze handia detektatu da (informazio konfidentzialak ihes egin dezake)

Guneak birbideratzeak egiten ditu parametro sentikorrekin URL-an, eta hori erregistroetan. Hauek nabigatzailearen historian edo kanpoko sistemetan ikus daitezke. Datu sentikorrak URL-etan edo birbideratzeetan ez sartuz konpondu daiteke. Birbideratzek berrikusten, beharrezkoak ez diren parametroak ezabatu beharko dira ere hau konpontzeko.



Gran redirección detectada (posible fuga de información confidencial)

URL: https://egela.ehu.eus
Riesgo: Low
Confianza: Medium
Parámetro:
Ataque:
Evidencia:
CWE ID: 201
WASC ID: 13
Origen: Pasivo (10044 - Gran redirección detectada (posible fuga de información confidencial))
Referencia de Alerta: 10044-1
Vector de Entrada:

Descripción:

El servidor ha respondido con una redirección que parece proporcionar una respuesta larga. Esto puede indicar que aunque el servidor envió una redirección, también respondió con el contenido del cuerpo (que puede incluir detalles confidenciales, PII, etc.).

Otra información:

Longitud URI de la cabecera de ubicación: 37 [https://egela.ehu.eus/login/index.php].
Tamaño previsto de la respuesta: 337.
Longitud del cuerpo de la respuesta: 1.516.

Solución:

Asegúrese de que no se filtre información confidencial a través de las respuestas de redirección. Las respuestas de redireccionamiento casi no deben tener contenido.