Documentacion Proyecto lewis

FLUID

SECURITY WITHOUT MYSTERY

FLUID

FIN.0037. Cookies generadas de forma insegura

Vulnerabilidad

Las Cookies son generadas en la aplicacin sin las banderas HttpOnly y Secure lo que facilita el compromiso de la sesin del usuario a travs de ataques tipo Cross Site Scripting.

Donde

https//www.countryroad.com.au - SLI - without Secure and HttpOnly Flag - popup_esub_acquisition without Secure and HttpOnly Flag - offerSeen - without Secure and HttpOnly Flag - loggedIn - without Secure and HttpOnly Flag - ki_t - without Secure and HttpOnly Flag - ki_r - without Secure and HttpOnly Flag - iSAMS - without Secure Flag - countryCode - without Secure and HttpOnly Flag - cartCount - without Secure and HttpOnly Flag - cartAbandon - without Secure and HttpOnly Flag - ASP.NET_SessionId - without Secure Flag

https//www.witchery.com.au/ SLI https//www.witchery.com.au/ iSAMS https//www.witchery.com.au/ ASP.NET_SessionId https//www.witchery.com.au/ cartCount https//www.witchery.com.au/ countryCode https//www.witchery.com.au/ ki_r https//www.witchery.com.au/ ki_t https//www.witchery.com.au/ loggedIn https//www.trenery.com.au/ + Cookie ASP.NET_SessionId created without the secure flag + Cookie cartCount created without the secure flag + Cookie cartCount created without the httponly flag + Cookie loggedIn created without the secure flag + Cookie loggedIn created without the httponly flag + Cookie countryCode created without the secure flag + Cookie countryCode created without the httponly flag + Cookie SLI created without the secure flag + Cookie SLI created without the httponly flag + Cookie iSAMS created without the secure flag

https//www.mimco.com.au

- ASP.NET_SessionId, Created without Secure Flag
- SLI, Created without Secure and HttpOnly Flag
- cartCount, Created without Secure and HttpOnly Flag
- countryCode, Created without Secure and HttpOnly Flag

FLUID

- iSAMS, Created without Secure Flag
- loggedIn, Created without Secure Flag

http//outlet.countryroad.com.au/ - Cookie ASP.NET_SessionId created without the httponly flag - Cookie iSAMS created without the httponly flag

Recomendacion

Agregar los atributos HttpOnly y s se est usando SSL en la aplicacin agregar el atributo Secure. = Documentacion Proyecto lewis

FIN.0047. Algoritmo de cifrado inseguro

Vulnerabilidad

El servidor donde se almacena la aplicacin soporta un cifrado inseguro como TLSv1.0 con algoritmos como : RC4 - SHA - MD5.

Donde

- https//www.countryroad.com.au RC4 SHA MD5
- https//outlet.countryroad.com.au RC4 SHA MD5
- https//www.trenery.com.au RC4 SHA MD5
- https//www.witchery.com.au/ RC4 SHA MD5 CBC
- https//www.mimco.com.au/ RC4 SHA , DHE 1024 bits vulnerable a logjam

Recomendacion

Solamente se debe de permitir cifrados seguros con algoritmos seguros como TLSv1.1 o Superior. = Documentacion Proyecto lewis

FLUID

FIN.0039. Mtodos HTTP Inseguros Habilitados

Vulnerabilidad

Mtodos como :

TRACE, HEAD, OPTIONS.

Se encuentran habilitados en el servidor permitiendo al atacante incluir y/o borrar archivos, permite saber cuales otros mtodos son permitidos o usar la depuracin en las pgina que lo permiten.

Donde

- https//www.countryroad.com.au
- TRACE
- http//outlet.countryroad.com.au TRACE

Recomendacion

Configurar los mtodos seguros para las peticiones en el servidor. = Documentacion Proyecto lewis

FIN.0057. Sesiones Concurrentes

Vulnerabilidad

La aplicacin no valida el nmero de sesiones por usuario permitiendole a un usuario iniciar sesin con las mismas credenciales en un mismo momento.

Donde

- https//www.countryroad.com.au/default.aspx

- https//www.witchery.com.au/
- https//www.trenery.com.au/
- https//www.mimco.com.au/
- https//outlet.countryroad.com.au/

Recomendacion

El sistema debe restringir el nmero de sesiones concurrentes que puede establecer un usuario. = Documentacion Proyecto lewis

FIN.0038. Cabeceras de seguridad HTTP no establecidas

Vulnerabilidad

El servidor carece de algunos encabezados HTTP que le permiten evitar ataques como el clickjacking y Cross site Scripting a las pginas que estn alojadas en ste.

Donde

https//www.witchery.com.au/ - Cabecera Public-Key-Pins - Cabecera X-Frame-Options - Cabecera X-XSS-Protection - Cabecera X-Content-Type-Options - Cabecera Content-Security-Policy. - Strict-Transport-Security. http//outlet.countryroad.com.au/ - Cabecera Public-Key-Pins - Cabecera X-Frame-Options - Cabecera X-XSS-Protection - Cabecera X-Content-Type-Options - Cabecera Content-Security-Policy. - Strict-Transport-Security. https//www.trenery.com.au - Cabecera Public-Key-Pins - Cabecera X-Frame-Options - Cabecera X-XSS-Protection - Cabecera X-Content-Type-Options - Cabecera Content-Security-Policy. - Strict-Transport-Security. https//www.mimco.com.au -Strict-Transport-Security -Access Control Allow Origin -Cross Domain Meta Policy -X-Frame-Options -X-XSS-Protection -Content Security Policy https//www.countryroad.com.au -Strict-Transport-Security -Access Control Allow Origin -Cross Domain Meta Policy -X-Frame-Options -X-XSS-Protection -ontent Security Policy

FLUID

Recomendacion

Establecer las cabeceras HTTP de seguridad: - Cabecera Public-Key-Pins - Cabecera X-Frame-Options - Cabecera X-XSS-Protection - Cabecera X-Content-Type-Options - Cabecera Content-Security-Policy. - Strict-Transport-Security. = Documentacion Proyecto lewis

FIN.0031. Poltica de credenciales dbiles

Vulnerabilidad

La poltica de credenciales presente en el sistema no cuenta con los parmetros recomendados que son que contengan al menos una maysculas, mnsculas, nmeros y caracteres especiales.

Donde

https//www.witchery.com.au/
https//www.trenery.com.au/
https//outlet.countryroad.com.au/
https//www..mimco.com.au/
https//www.countryroad.com.au/

Recomendacion

Establecer una politica para la creacin de credenciales que involucre el uso de nmeros, caracteres especiales, letras mayusculas y minusculas. = Documentacion Proyecto lewis

FIN.0011. Funcionalidad insegura

Vulnerabilidad

Es posible crear cuentas de usuario sin ninguna validacin alguna.

FLUID

Donde

https//www.trenery.com.au/default.aspx?ZC&rnd7923d3bf-87ec-4642-bbfe-313547c007dd&actiondisplayaccount&pgsubscriber&SIGNUPEMAIL
https//www.witchery.com.au/default.aspx?ZC&rnd9d843dea-a5b7-4daf-87ba-b0f47440d7be&actiondisplayaccount https//www.mimco.com.au/video videosource https//www.mimco.com.au/video/category playlistId https//outlet.countryroad.com.au/default.aspx?ZC&actiondisplayaccount&pgsubscriber
https//www.countryroad.com.au/default.aspx?ZC&actiondisplayaccount&pgsubscriber

Recomendacion

Implementar verificacin de email para evitar la creacin aleatoria de usuarios. = Documentacion Proyecto lewis

FIN.0048. Ausencia de proteccin contra ataques de fuerza bruta

Vulnerabilidad

La aplicacin no tiene proteccin contra ataques automatizados para crear cuentas de usuarios validas.

Donde

- https/www.countryroad.com.au/default.aspx Campos loginfrm1 Formulario para crear cuentas
- https/www.countryroad.com.au/gift-cards Campos balancecheck, gc-number, gc-pin
- https//www.countryroad.com.au/_admin
- https//www.trenery.com.au Campos emailaddress, password
- https/www.mimco.com.au/default.aspx Campos loginfrm1 Formulario para crear cuentas https//www.mimco.com.au/gift-cards Campos balancecheck, gc-

number, gc-pin

https//www.mimco.com.au/global/api/Stores.asmx - Authenticate
https//www.mimco.com.au/global/api/Products.asmx - Authenticate
https//www.mimco.com.au/global/api/Customers.asmx - Authenticate
https//www.mimco.com.au/global/api/SingleSignOn.asmx - Authenticate
https//www.mimco.com.au/global/api/Orders.asmx - Authenticate
https//www.mimco.com.au/global/api/Dispatch.asmx - Authenticate
https//www.mimco.com.au/global/api/SalesReturns.asmx - Authenticate
https//www.mimco.com.au/global/api/ShoppingCart.asmx - Authenticate
https//www.mimco.com.au/_admin - https//www.trenery.com.au/gift-cards?Zbc Campos balancecheck,gc-number,gc-pin https//outlet.countryroad.com.au Campos emailaddress, password https//www.witchery.com.au/global/api/Stores.asmx - Authenticate https//www.witchery.com.au/global/api/Products.asmx - Authenticate
https//www.witchery.com.au/global/api/Customers.asmx - Authenticate
https//www.witchery.com.au/global/api/SingleSignOn.asmx - Authenticate
https//www.witchery.com.au/global/api/Orders.asmx - Authenticate
https//www.witchery.com.au/global/api/Dispatch.asmx - Authenticate
https//www.witchery.com.au/global/api/SalesReturns.asmx - Authenticate
https//www.witchery.com.au/global/api/ShoppingCart.asmx - Authenticate
https//www.witchery.com.au/_admin
https//www.trenery.com.au/global/api/Stores.asmx - Authenticate
https//www.trenery.com.au/global/api/Products.asmx - Authenticate
https//www.trenery.com.au/global/api/Customers.asmx - Authenticate
https//www.trenery.com.au/global/api/SingleSignOn.asmx - Authenticate
https//www.trenery.com.au/global/api/Orders.asmx - Authenticate
https//www.trenery.com.au/global/api/Dispatch.asmx - Authenticate
https//www.trenery.com.au/global/api/SalesReturns.asmx - Authenticate
https//www.trenery.com.au/global/api/ShoppingCart.asmx - Authenticate

Recomendacion

Implementar un control para evitar este tipo de ataques y que garantice que el acceso no sea de un robot. Ej captcha, bloqueo por retardo en el nmero de intentos fallidos, etc. = Documentacion Proyecto lewis

FLUID

FIN.0007. Cross Site Request Forgery

Vulnerabilidad

La aplicacin permite engaar a un usuario autenticado por medio de links manipulados para ejecutar acciones sobre la aplicacin sin su consentimiento.

Donde

https//www.witchery.com.au/default.aspx?ZC&rndc084d244-6fe7-4c65-aefa-a6edd6c8a4d6&actiondisplayaccount
https//www.witchery.com.au//default.aspx?oladditems&zc&actionorderlist&wID71149&[0][pdID]11896&[0][clID]892&[0][szID]100&[0][Quantity]1&_1471544137342
https//www.witchery.com.au /default.aspx?ZC&rnd&actionremoveitem&id
https//www.witchery.com.au/default.aspx?ZC&rnd9a874c36-0087-4343-8229-f5e90c737207&actionorderlist&oldeleteitems&wID71149&[0][ID]526648&[0][pdID]11711&[0][piID]69844&[0][Quantity]1
https//www.witchery.com.au/default.aspx?ZC&rnd07b6eea7-d192-42e9-827d-6e688afb3085&actioncart#
https//www.witchery.com.au/default.aspx?ZC&rnde58cc0d4-365c-41a0-adb4-e6f790d90dd7&actionremoveitem&id6759661 -
http//www.trenery.com.au/default.aspx?oladditems&zc&actionorderlist&wID[ID]&%5B0%5D%5BpdID%5D[pID]&%5B0%5D%5BclID%5D[PID]&%5B0%5D%5BszID%5D[sizeID]&%5B0%5D%5BQuantity%5D[Quanty]&_1471650357377 //add to wishlist
https//www.trenery.com.au/default.aspx?ZC&rnd&actionorderlist&oldeleteitems&wID70664&[0][ID]433540&[0][pdID]6865&[0][piID]12280&[0][Quantity]1 -Delete items from WISHLIST -
https//www.trenery.com.au/default.aspx?ZC&rndF67C410D-C136-47E7-9BD4-BC1017225C21&actionlogout //logout -
https//www.trenery.com.au/default.aspx?ZC&rndf2bffbc3-85d1-4aea-80a8-638b3e955860&actiondisplayaccount&editprofile1 //Edit profile
https//www.trenery.com.au/default.aspx?ZC&rnd //Edit bag
https//www.trenery.com.au/default.aspx?ZC&rnd&actionremoveitem&id //delete from bag https//outlet.countryroad.com.au/default.aspx?ZC&actionlogout
https//outlet.countryroad.com.au/default.aspx?ZC&actionupdateaccount
https//outlet.countryroad.com.au/default.aspx?ZC&actionaddspecif
https//outlet.countryroad.com.au/default.aspx?ZC&actionrecalculate

https//outlet.countryroad.com.au/default.aspx?ZC&actionremoveitem - https//www.trenery.com.au/default.aspxZC&T110353&actionaddspecify&parent[parent]&catID[id]&pdID[ID]&fk_id[product_id]&qs1&addpopup1&clID70&szID2735&size[sizeID]&qty[qty]&wID76152&new&serveasajax&_1471550530249 //add to bag
https//www.mimco.com.au/default.aspx?zc&actionorderlist&oladditems&wID70343&[0][pdID]7054&[0][clID]22&[0][szID]0&[0][Quantity]1&_1471451130845 -Add items to WISHLIST

https//www.mimco.com.au/default.aspx?ZC&rnd&actionorderlist&oldeleteitems&wID70664&[0][ID]433540&[0][pdID]6865&[0][piID]12280&[0][Quantity]1 -Delete items from WISHLIST

https//www.mimco.com.au/default.aspx?ZC&actionlogout - Logout

https//www.mimco.com.au/default.aspx?ZC&rnd944a51b6-ce3a-4204-a5cc-d33826ddf453&profile - Edit Profile

https//www.mimco.com.au/default.aspx?ZC&rnd -Modify Quantity BAG

https//www.mimco.com.au/default.aspx?ZC&rnd&actionremoveitem&id - Delete items from BAG

https//www.countryroad.com.au/default.aspx?ZC&actionlogout
https//www.countryroad.com.au/default.aspx?ZC&actionupdateaccount
https//www.countryroad.com.au/default.aspx?ZC&actionaddspecif
https//www.countryroad.com.au/default.aspx?ZC&actionrecalculate
https//www.countryroad.com.au/default.aspx?ZC&actionremoveitem

Recomendacion

Hacer uso de tokens en los formularios para la verificacin de las peticiones realizadas por usuarios legtimos.

Documentacion Proyecto lewis

FLUID

FIN.0058. Excepciones inseguras

Vulnerabilidad

La aplicacin muestra excepciones por defecto cuando se ingresar a algunas url en este caso Runtime Error, adicionalmente estas excepciones son propias del lenguaje de programacin, lo que permite tener conocimientos tcnicos de la aplicacin.

Lenguaje: ASP.NET.

Donde

- https//www.trenery.com.au/wa/perth/lpt9
- https//www.trenery.com.au/lightwidget.com/widgets/lpt9
- https//outlet.countryroad.com.au/wa/perth/lpt9

Recomendacion

Validar adecuadamente todas las excepciones y no dejar excepciones por defecto. = Documentacion Proyecto lewis

FIN.0072. Cdigo funcional comentado

Vulnerabilidad

Existe cdigo comentado en ambiente de produccin, lo que aumenta la probabilidad de que en ambientes de desarrollo, puedan remover los comentarios de este cdigo y desplegarlo en produccin.

Donde

https//www.countryroad.com.au/assets/cr_scripts_7.js
https//www.countryroad.com.au/images/assetimages/countryroad_custom.js

https//www.countryroad.com.au/default.aspx
https//outlet.countryroad.com.au/assets/cr_map.js
https//outlet.countryroad.com.au/assets/outlet.js

Recomendacion

Eliminar todas las lneas de cdigo funcional comentado en el cdigo fuente de la aplicacin.

Documentacion Proyecto lewis

FIN.0013. Mtodo de autenticacin inseguro

Vulnerabilidad

Uso de mtodos de autenticacin inseguros como Basic HTTP.

Donde

https//www.countryroad.com.au/_admin https//www.countryroad.com.au/__admin https//www.mimco.com.au/_admin

Recomendacion

Implementar mecanismos de autenticacin ms seguros cmo aquellos basados en formularios. = Documentacion Proyecto lewis

FLUID

FIN.0061. Falta de validacin de datos

Vulnerabilidad

La aplicacin no valida en algunos formularios, el tipo de datos que se ingresan y quedan almacenados en la BD, esto incrementa el riesgo de ataques del tipo de inyeccin o XXS.

Donde

- https//www.trenery.com.au/default.aspx?ZC&rnd5cb14068-8a39-41c3-b96b-14f76c8f68bc&actiondelivery campos company1, uburb1, street1, postcode1, Bill-firstname, bill-lastname, address1, address2
- https//outlet.countryroad.com.au/default.aspx?ZC&actiondisplayaccount&editprofile1 firstname lastname address address2
- https//outlet.countryroad.com.au/default.aspx?ZC&actiondelivery firstname lastname address address2
- https//outlet.countryroad.com.au/default.aspx?ZC&deliveryd card_name
- https//www.mimco.com.au card_name, address, address2

Recomendacion

Validar en el lado del cliente los tipos de datos que se ingresan a distintos tipos de campos en la aplicacin. = Documentacion Proyecto lewis

FIN.0038. Webservices expuestos

Vulnerabilidad

El servidor contiene expuestos los webservices de la aplicacin, lo que permite visualizar todos sus mtodos, documentacin e instrucciones de uso.

FLUID

Donde

https//www.witchery.com.au/global/api/Stores.asmx
https//www.witchery.com.au/global/api/Products.asmx
https//www.witchery.com.au/global/api/Customers.asmx
https//www.witchery.com.au/global/api/SingleSignOn.asmx
https//www.witchery.com.au/global/api/Orders.asmx
https//www.witchery.com.au/global/api/Dispatch.asmx
https//www.witchery.com.au/global/api/SalesReturns.asmx
https//www.witchery.com.au/global/api/ShoppingCart.asmx
https//www.witchery.com.au/api/state https//www.witchery.com.au/api/pricing
https//www.mimco.com.au/global/api/Stores.asmx
https//www.mimco.com.au/global/api/Products.asmx
https//www.mimco.com.au/global/api/Customers.asmx
https//www.mimco.com.au/global/api/SingleSignOn.asmx
https//www.mimco.com.au/global/api/Orders.asmx
https//www.mimco.com.au/global/api/Dispatch.asmx
https//www.mimco.com.au/global/api/SalesReturns.asmx
https//www.mimco.com.au/global/api/ShoppingCart.asmx
https//www.mimco.com.au/api/state https//www.mimco.com.au/api/pricing
https//www.countryroad.com.au/global/api/Stores.asmx
https//www.countryroad.com.au/global/api/Products.asmx
https//www.countryroad.com.au/global/api/Customers.asmx
https//www.countryroad.com.au/global/api/SingleSignOn.asmx
https//www.countryroad.com.au/global/api/Orders.asmx
https//www.countryroad.com.au/global/api/Dispatch.asmx
https//www.countryroad.com.au/global/api/SalesReturns.asmx
https//www.countryroad.com.au/global/api/ShoppingCart.asmx
https//www.countryroad.com.au/api/state
https//www.countryroad.com.au/api/pricing
https//www.trenery.com.au/global/api/Products.asmx
https//www.trenery.com.au/global/api/Customers.asmx
https//www.trenery.com.au/global/api/Stores.asmx
https//www.trenery.com.au/global/api/SingleSignOn.asmx
https//www.trenery.com.au/global/api/Orders.asmx
https//www.trenery.com.au/global/api/Dispatch.asmx
https//www.trenery.com.au/global/api/SalesReturns.asmx
https//www.trenery.com.au/global/api/ShoppingCart.asmx
https//www.trenery.com.au/api/state
https//outlet.countryroad.com.au/global/api/Stores.asmx
https//outlet.countryroad.com.au/global/api/Products.asmx

https//outlet.countryroad.com.au/global/api/Customers.asmx
https//outlet.countryroad.com.au/global/api/SingleSignOn.asmx
https//outlet.countryroad.com.au/global/api/Orders.asmx
https//outlet.countryroad.com.au/global/api/Dispatch.asmx
https//outlet.countryroad.com.au/global/api/SalesReturns.asmx
https//outlet.countryroad.com.au/global/api/ShoppingCart.asmx
https//outlet.countryroad.com.au/api/state
https//outlet.countryroad.com.au/api/pricing

Recomendacion

Implementar autenticacin para visualizar los webservices o en su defecto eliminar su acceso pblico. = Documentacion Proyecto lewis

FIN.0066. Tiempo lmite de inactividad inseguro

Vulnerabilidad

La sesin de usuario de la aplicacin no expira despus de 5 minutos de inactividad.

Donde

https//www.witchery.com.au/
https//www.trenery.com.au
https//www.countryroad.com.au
https//outlet.countryroad.com.au
https//www.mimco.com.au

Recomendacion

Cerrar las sesiones cuando permanezcan inactivas ms de 5 minutos

FLUID

Documentacion Proyecto lewis

FIN.0064. Cdigo JavaScript sin ofuscar

Vulnerabilidad

El sistema tiene cdigo javascript que contiene informacin del negocio sin ofuscar, lo que le permite a un atacante identificar rutas, validaciones y parmetros que ste utiliza.

Donde

- https//www.countryroad.com.au/assets/cr_scripts_7.js
- https//www.countryroad.com.au/images/assetimages/countryroad_custom.js
- https//www.trenery.com.au/assets/CountryRoad_GiftCards.js
- https//www.trenery.com.au/assets/Trenery.js
  https//outlet.countryroad.com.au/assets/cr_map.js
  https//outlet.countryroad.com.au/assets/outlet.js

Recomendacion

Realizar un proceso de ofuscacin al cdigo expuesto en las aplicaciones web. = Documentacion Proyecto lewis

FIN.0008. Inyeccin de cdigo (XSS)

Vulnerabilidad

Los campos de la aplicacin permiten inyectar scripts en la base de datos de la aplicacin para que estos sean ejecutados posteriormente en el momento que los

usuarios consulten la funcionalidad afectada permitiendo el robo de informacin o la distribucin de software malicioso.

Los campos de la aplicacin permiten inyectar cdigo Javascript haciendo posible a un atacante comprometer la sesin del usuario.

Donde

- https//www.countryroad.com.au/CR_StoredPayments.ashx card_name
- https//www.trenery.com.au/CR_StoredPayments.ashx campo card_name
- https//witchery.com.au/CR_StoredPayments.ashx card_name
- https//outlet.countryroad.com.au/CR_StoredPayments.ashx card_name
- https//www.mimco.com.au/CR_StoredPayments.ashx card_name

Recomendacion

Filtrar la informacin que recibe y enva la aplicacin por medio de listas blancas

Documentacion Proyecto lewis

FIN.0074. Manejo inseguro de sesin

Vulnerabilidad

El sitio almacena las credenciales en una cookie insegura, la cual no tiene la flag de issecure, la sesin nunca expira si el usuario no la cierra, lo que permite que un atacante mediante acceso al equipo ya sea fsico o por medio de un malware pueda robar la cookie para robar las credenciales y la sesin del usuario.

FLUID

Donde

https//www.witchery.com.au/ iSAMS https//outlet.countryroad.com.au/ iSAMS https//www.trenery.com.au/ ISAMS https//www.mimco.com.au/ ISAMS https//www.countryroad.com.au/ ISAMS

Recomendacion

Las credenciales deben de almacenarse del lado del servidor y no en las cookies. = Documentacion Proyecto lewis

FIN.0035. Fuga de informacin tcnica

Vulnerabilidad

A travs de mtodos pasivos de Footprinting se puede recolectar informacin importante de la aplicacin y el servidor, esto incluye el S.O, el lenguaje de programacin, el servicio HTTP, APIS y el CDN, adems de las versiones en las que corren. Esto facilita la tarea a un atacante de buscar vulnerabilidades conocidas en dichos recursos para posteriormente explotarlas.

Donde

- https://www.trenery.com.au

Recomendacion

Configurar adecuadamente los servicios y los banners para que no den ms informacin de la necesaria a los usuarios. = Documentacion Proyecto lewis

FLUID

FIN.0024. Enumeracin de usuarios

Vulnerabilidad

Debido a una mala prctica en la configuracin se pueden enumerar los usuarios vlidos en la aplicacin.

Donde

https//www.mimco.com.au/default.aspx?ZC&rnd -profile editions -Forgot Password -join https//www.witchery.com.au/ -profile editions -Forgot Password -join https//www.trenery.com.au -profile editions -Forgot Password -join https//outlet.countryroad.com.au -profile editions -Forgot Password -join https//www.countryroad.com.au -profile editions -Forgot Password -join

Recomendacion

Implementar mensajes de error genricos que no le permitan a un atacante discernir la existencia del usuario en el sistema a travs de los errores HTTP (500 o 404) . = Documentacion Proyecto lewis

FIN.0045. Enumeracin automtica de informacin

Vulnerabilidad

Es posible enumerar de forma automatizada las tarjetas de regalo (giftcards) disponibles en el servidor mediante una funcin, permitiendo as saber cuales estn activas y cules se pueden consumir.

Donde

- https//www.countryroad.com.au/gift-cards?Zbc Campos balancecheck,gc-number,gc-pin
- https//www.mimco.com.au/gift-cards?Zbc Campos balancecheck,gc-

number,gc-pin

- https//www.witchery.com.au/gift-cards?Zbc Campos balancecheck,gc-number,gc-pin
- https//www.trenery.com.au/gift-cards?Zbc Campos balancecheck,gc-number,gc-pin

Recomendacion

Establecer alguna proteccin contra enumeracin automatizada de tarjetas de regalo (giftcards) validas como bloquear ip despues de n intentos o retardos incrementales. = Documentacion Proyecto lewis

FIN.0063. Cach en formulario

Vulnerabilidad

El formulario no deshabilita la caracterstica de autocompletado, por lo que informacin quedar almacenada en el cach del navegador.

Donde

https//outlet.countryroad.com.au/ -emailaddress https//www.trenery.com.au/ campo emailaddress https//www.witchery.com.au/ -emailaddress https//www.countryroad.com.au/ -emailaddress https//www.mimco.com.au

Recomendacion

Agregar el atributo HTML autocomplete = off, en los campos de texto del formulario.