¿Conoces la vulnerabilidad Cross Site Request Forgery?

Es muy habitual escuchar en los medios de comunicación ataques llevados a cabo por ciberdelincuentes que buscan la forma de lucrarse a costa del resto de usuarios. Este tipo de amenazas en Internet están a la orden del día, y que sea muy importante que los usuarios se protejan con todos los medios que tengan a su alcance, ya no sólo en sus equipos informáticos, sino también en sus dispositivos móviles, unos elementos que cada vez tienen más importancia dentro de la sociedad.

Por desgracia, hoy en día nos podemos encontrar un gran número de amenazas en Internet, desde los ya clásicos virus o troyanos, hasta el Cross-Site Scripting (XSS). Hoy nos centraremos en otro que quizá no conozcáis. Se trata del Cross Site Request Forgery (CSRF), y a lo largo de este WhitePaper intentaremos explicaros en qué consiste y cómo protegernos de él.

¿Qué es el ataque Cross Site Request Forgery?

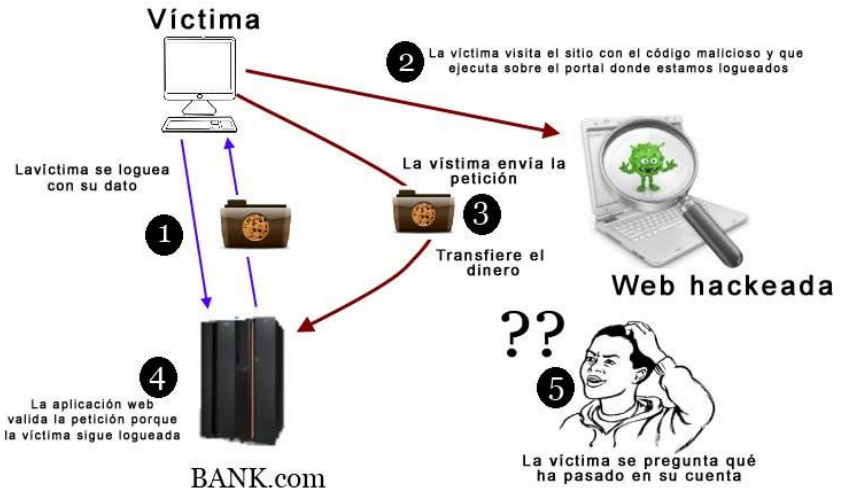
Los mecanismos utilizados por los atacantes para llevar a cabo sus planes, son cada vez más sofisticados, y en muchas ocasiones, imperceptible para las personas, que pueden estar navegando por cualquier sitio web sin saber que están sufriendo un ataque en ese mismo momento, y lo peor de todo, que ellos mismos, con sus acciones son los que lo han provocado.

Dentro de este tipo de ataques sofisticados podemos incluir el ataque que hoy os vamos a explicar. Se trata de la técnica llamada “Falsificación de petición en sitios cruzados”, más conocida con su nombre en versión inglés “Cross Site Request Forgery”, aunque también es conocida como “Session Riding”.

El objetivo principal que busca el atacante mediante el uso de la técnica CSRF es utilizar esas situaciones en las que los usuarios no cierran de forma correcta las sesiones de alguna aplicación web (banco, correo electrónico, panel de control de gestión de dominios…) y que siguen activas mientras estamos visitando otras páginas, sitios donde pueden haber insertado algún tipo de código malicioso que ejecute alguna instrucción.

Por medio de este tipo de ataque el hacker puede llevar a cabo multitud de operaciones, dependiendo del tipo de aplicación sobre la que se ejecutará la acción. Por ejemplo, si actúa sobre un webmail podría crear algún filtro en el correo para que todos los emails que reciba una determinada cuenta de correo sean enviados a otra dirección, o si se trata de un portal bancario, podría transferir una determinada cantidad de dinero a una de sus cuentas.

¿Cómo funciona el ataque Cross Site Request Forgery?



Por si la explicación anterior no ha quedado clara, vamos a desgranar cómo funciona este tipo de ataques. Lo primero que debe ocurrir para que se lleve a cabo un ataque CSRF, es que el atacante, sea capaz de hackear un determinado servidor o portal web, donde insertar el código malicioso con el que llevará a cabo sus acciones. Este código puede ser desde un simple enlace a una determinada url, hasta un formulario de apariencia normal, pero en el que al pulsar el botón 'Enviar' ejecutará una url encargada de llevar a cabo la acción maliciosa.

Lo siguiente que debe ocurrir es que el usuario acceda a una aplicación web y se loguee con sus credenciales. Esta aplicación será totalmente diferente de la primera donde el atacante ha introducido el código malicioso, y por lo general no tendrán ningún tipo de relación.

Si ahora la víctima visita el primer sitio que ha sido infectado sin cerrar la sesión del otro sitio, y ejecuta sin querer el código malicioso que actúa sobre el segundo portal, entonces se llevará a cabo el ataque sin que el usuario se entere.

Por poner un ejemplo. Un atacante hackea el portal web "portalhackeado.com" e inyecta código malicioso que actúa sobre la web "mibanco.com" mediante la ejecución de un enlace que ordena que se transfiera dinero de nuestra cuenta hacia la del atacante. Si la víctima accede a su perfil en el portal del banco, y sin cerrar la sesión se pone a visitar el portal "portalhackeado.com" y ejecuta sin querer ese código malicioso, hará que de forma inmediata su banco transfiera parte de sus ahorros hacia la cuenta del hacker, ya que al estar aún logueado, la petición es totalmente válida. Esto no ocurriría, si hubiera cerrado la sesión con su entidad bancaria.

Recomendaciones para protegernos contra el ataque Cross Site Request Forgery

Ahora que ya tenemos una idea de en qué consiste este tipo de ataques, es hora de nombrar algunas prácticas recomendadas que podemos aplicar para no sufrir el ataque CSRF.

- El principal consejo que os podemos dar para prevenir este tipo de ataques es hacer una sólo cosa a la vez mientras estemos logueados en algún sitio web. Una vez que hayamos terminado de hacer nuestras cosas, es muy importante cerrar la sesión, algo que podemos hacer con un simple clic de ratón.
- No sirve con cerrar la pestaña en cuestión, ya que algunas webs mantienen la sesión abierta, opción que podemos deshabilitar.
- Otra buena práctica es hacer uso del "modo incógnito" que ofrece los navegadores hoy en día para acceder a los sitios más críticos, o configurar el navegador para que no almacene nuestros usuarios y contraseñas.
- Si usamos complementos que bloqueen la ejecución de scripts, aquellos formularios que hagan uso del método POST para el envío, no lo podrán hacer sin el consentimiento del usuario.
- Ya más orientado a los programadores, lo que se suele hacer para evitar este tipo de ataques es introducir un "token" dinámico en las solicitudes del cliente que se asocia a la sesión y que se añade a todas las peticiones. Si la petición no tiene asociado ningún token o si este no coincide con el del usuario, entonces no se llevará a cabo la petición. Esta técnica la vienen implementando algunos CMS como WordPress y los principales frameworks de programación con Symfony 2.

Cómo habéis podido observar, se trata de un ataque que difícilmente los usuarios podemos detectar, pero siempre tenemos armas para evitar caer en las garras de los atacantes.