Instrucciones 1

Elevation of Privilege Instrucciones

Dibuje un diagrama del modelo de sistema para el que desea modelar amenazas antes de repartir las cartas.

Reparte el mazo a 3-6 jugadores. El juego comienza con el 3 de manipulación. Juega en el sentido de las agujas del reloj y cada jugador, por turno, continúa usando el palo si tiene una carta de ese palo. Si el jugador no tiene una carta de ese palo, puede usar otro palo. Cada ronda se gana con la carta más alta jugada del palo que salió, a menos que se juegue una carta de "Elevation of Privilege" (EoP). En ese caso, gana la tarjeta EoP de alto valor.

Para jugar una carta, léala, anuncie su amenaza y regístrela. Si el jugador no puede vincular la amenaza al sistema, el juego continúa.

El ganador de una mano selecciona la carta (y el palo) para liderar la siguiente mano. Tómate unos minutos entre manos para pensar en las amenazas.

Puntos:
1 por una amenaza en tu carta, +1 por hacer el truco

Elevation of Privilege Instrucciones

Las amenazas deben expresarse de forma clara, comprobable y
abordables. En el caso de que una amenaza lleva a una discusión, puede resolverlo haciendo la pregunta: "¿Aceptaríamos un error procesable, una solicitud de función o un cambio de diseño para eso?" Si la respuesta es sí, se trata de una amenaza real. (Esto no significa que las amenazas fuera de eso no sean reales, es simplemente una forma de centrar la discusión en amenazas procesables). Las preguntas que comienzan con "Hay una manera" eben leerse como "Hay una manera...y así es como..." mientras que las preguntas que comienzan con "Tu código" deben leerse "El código que estamos creando colectivamente...y así es como se hace".

La baraja contiene una serie de cartas especiales: triunfos y amenazas abiertas. Las cartas EoP son triunfos: ganan la baza incluso si tienen un valor menor que el palo que se jugó. El as de cada palo es una carta de amenaza abierta. Cuando se juega, el jugador debe identificar una amenaza que no figura en otra carta.

Cuando se hayan jugado todas las cartas, gana el que tenga más puntos.

¡Recuerda divertirte!

Instrucciones 2

Elevation of Privilege Instrucciones

Variantes opcionales:

- Puedes pasar cartas después del tercer truco. Esto es útil si tiene tarjetas que no puede vincular al sistema. Es posible que alguien más pueda hacerlo.
- Duplica la cantidad de puntos y otorga un punto por las amenazas en las cartas de otras personas.
- Otros jugadores pueden "reflexionar" sobre la amenaza y, si lo hacen, obtienen un punto por cada amenaza adicional.
- Limite los riffs a no más de 60 segundos.
- Marque el diagrama donde ocurre la amenaza.

Las preguntas se enumeran en las cartas de amenaza para ayudar con los ases.

Gracias a Laurie Williams por la inspiración.

Contenido:

• **2** Cartas de instrucciones

• **1** Puedes pasar cartas después del tercer truco. Esto es útil si tiene tarjetas que no puede vincular al sistema. Es posible que alguien más pueda hacerlo.

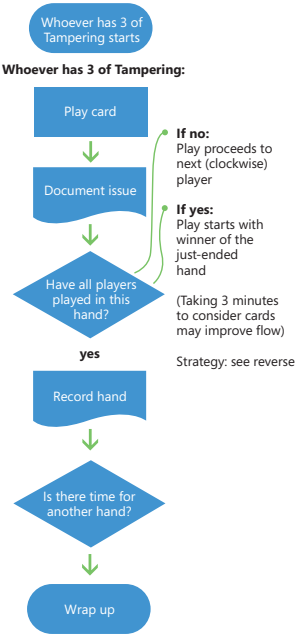
• **6** STRIDE Cartas de amenaza 'palos':

1. Spoofing: 2-K, As
2. Manipulación: 2-K, As
3. Repudio: 2-K, As
4. Divulgación de Información: 2-K, As
5. Denegación de Servicio: 2-K, As
6. Elevación de Privilegios: 2-K, As (Cartas de Triunfo)

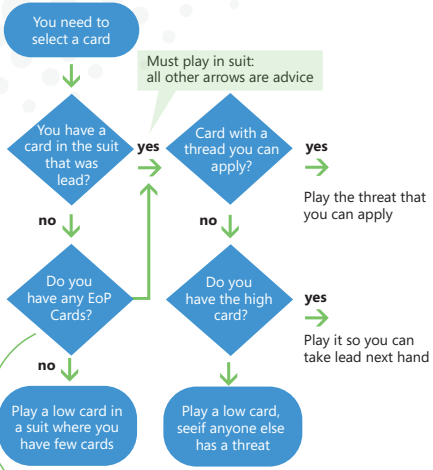
• **6** STRIDE Cartas de Referencia de Amenazas

Context

Play

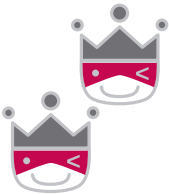


Strategy


You need to select a card
Must play in suit: all other arrows are advice
You have a card in the suit that was lead?
yes
Card with a thread you can apply?
yes
Play the threat that you can apply
no
no
Do you have any EoP Cards?
Do you have the high card?
yes
Play it so you can take lead next hand
no
Play a low card in a suit where you have few cards
Play a low card, seeif anyone else has a threat
Choice: Play EoP or another card. For example, someone else may have played the Jack of EoP, and you only have a 9.

2 Spoofing

Un atacante podría apoderarse del puerto o socket que normalmente utiliza el servidor

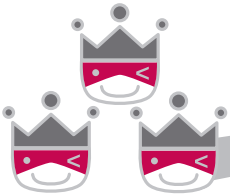


2


Microsoft
elevation of privilege
of

3 Spoofing

Un atacante podría probar una credencial tras otra y no hay nada que las ralentice (en línea o fuera de línea)

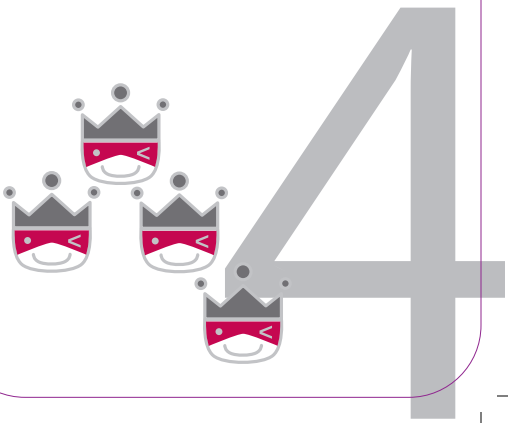


3


Microsoft
elevation of privilege
of

4 Spoofing

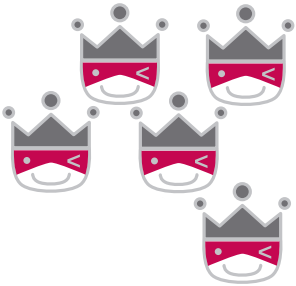
Un atacante puede conectarse de forma anónima porque esperamos que la autenticación se realice en un nivel superior




Microsoft
elevation of privilege
of

5 Spoofing

Un atacante puede confundir a un cliente porque hay demasiadas formas de identificar un servidor

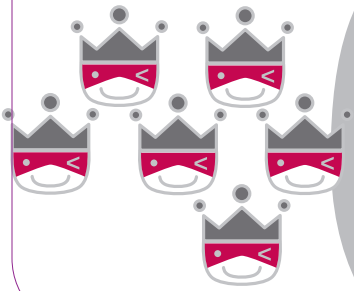


5


Microsoft
elevation of privilege
of

6 Spoofing

Un atacante puede falsificar un servidor porque los identificadores no se almacenan en el cliente y no se verifica su coherencia al volver a conectarse (es decir, no hay persistencia de claves)

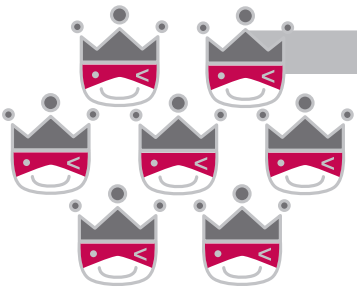


6


Microsoft
elevation of privilege
of

7 Spoofing

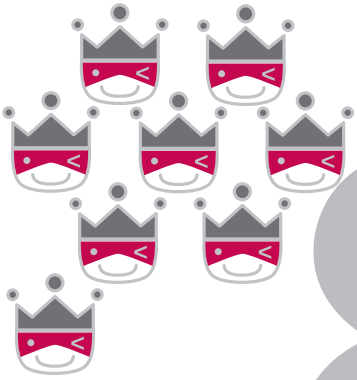
Un atacante puede conectarse a un servidor o a través de un enlace que no está autenticado (ni cifrado)




Microsoft
elevation of privilege
of

8 Spoofing

Un atacante podría robar las credenciales almacenadas en el servidor y reutilizarlas (por ejemplo, una clave se almacena en un

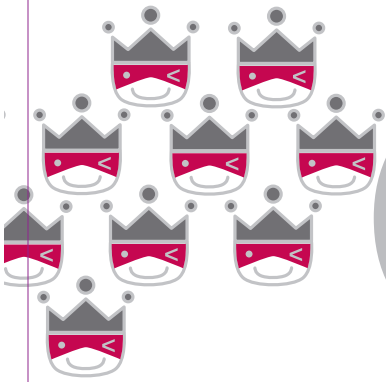


8


Microsoft
elevation of privilege
of

9 Spoofing

Un atacante que obtiene una contraseña puede reutilizarla (use autenticadores más seguros)

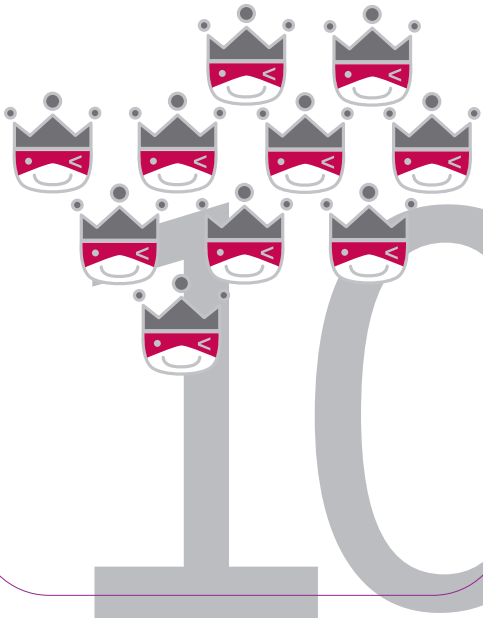


9


Microsoft
elevation of privilege
of

10 Spoofing

Un atacante puede optar por utilizar una autenticación más débil o nula

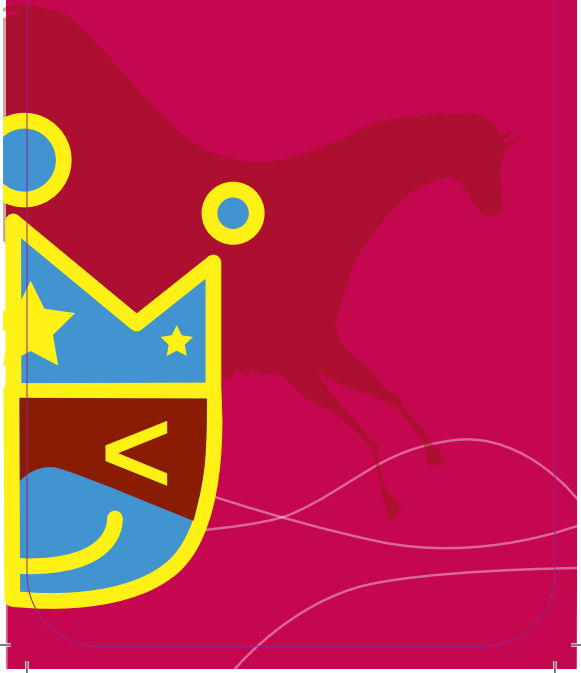



Microsoft
elevation of privilege
of

J

Spoofing

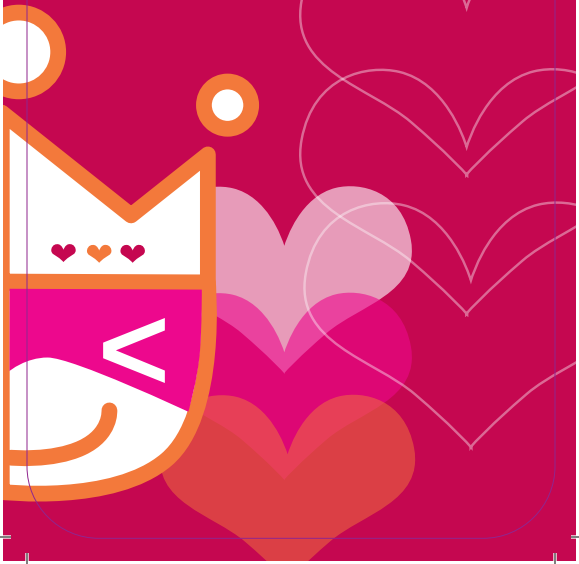
Un atacante podría robar las credenciales almacenadas en el cliente y reutilizarlas




Microsoft
elevation of privilege
of

Q Spoofing

Un atacante podría atacar la forma en que se actualizan o recuperan las credenciales (la recuperación de la cuenta no requiere revelar la contraseña anterior)

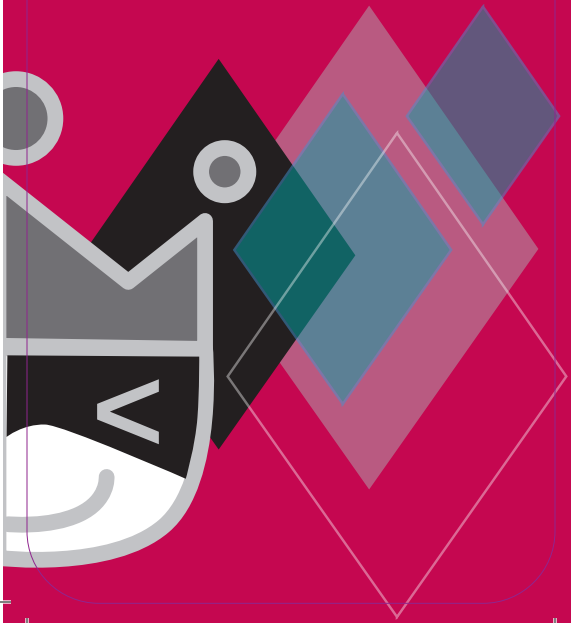



Microsoft
elevation of privilege
of

K

Spoofing

Su sistema viene con una contraseña de administrador predeterminada y no fuerza ningún cambio




Microsoft
elevation of privilege
of

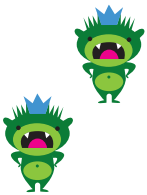
A Spoofing

Has inventado un nuevo ataque de Spoofing


Microsoft
elevation of privilege
of

2 Manipulación

Un atacante puede aprovechar su intercambio de claves personalizado o el control de integridad que usted creó en lugar de usar

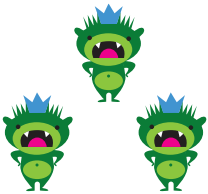


2


Microsoft
elevation of privilege
of

3 Manipulación

Un atacante puede modificar su sistema de compilación y producir compilaciones firmadas de su software

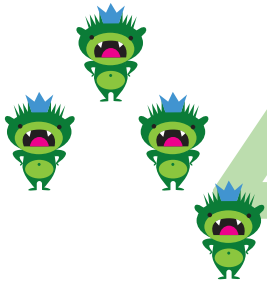


3


Microsoft
elevation of privilege
of

4 Manipulación

Su código toma decisiones de control de acceso en todas partes, en lugar de hacerlo con un núcleo de seguridad

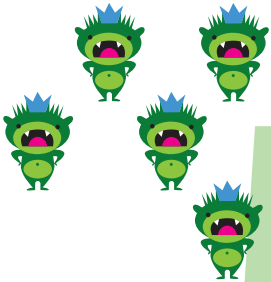


4


Microsoft
elevation of privilege
of

5 Manipulación

Un atacante puede reproducir datos sin ser detectado porque su código no proporciona marcas de tiempo ni números de

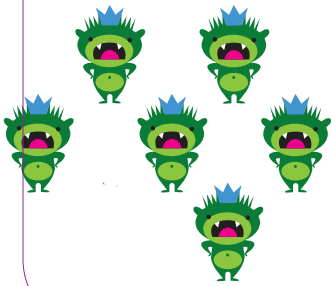


5


Microsoft
elevation of privilege
of

6 Manipulación

Un atacante puede escribir en un almacén de datos en el que se basa su código

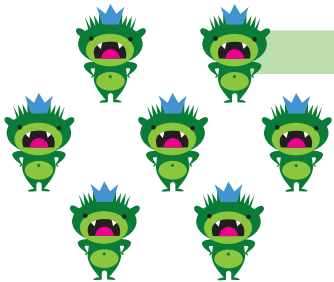


6


Microsoft
elevation of privilege
of

7 Manipulación

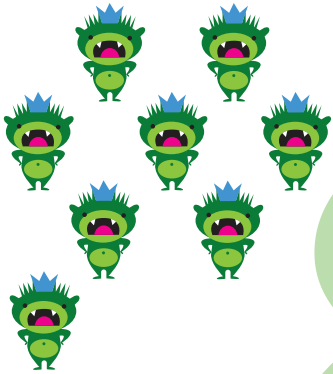
Un atacante puede eludir los permisos porque no convierte los nombres en canónicos antes de verificar los permisos de acceso




Microsoft
elevation of privilege
of

8 Manipulación

Un atacante puede manipular datos porque no existe protección de integridad para los datos en la red

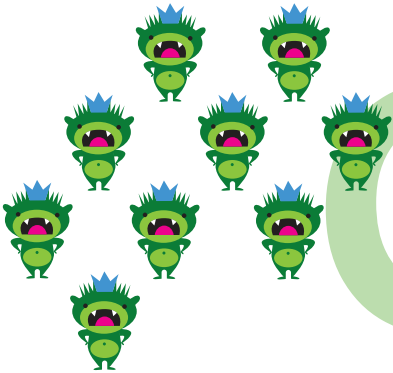


8


Microsoft
elevation of privilege
of

9 Manipulación

Un atacante puede proporcionar o controlar información de estado




Microsoft
elevation of privilege
of

10 Manipulación

Un atacante puede alterar la información en un almacén de datos porque tiene permisos débiles/abiertos o incluye un grupo que es equivalente a todos (“cualquier persona con una cuenta de Facebook”)


Microsoft
elevation of privilege
of

J Manipulación

Un atacante puede escribir en algún recurso porque se otorgan permisos al mundo o no hay ACL


Microsoft
elevation of privilege
of

Q Manipulación

Un atacante puede cambiar los parámetros más allá de un límite de confianza y después de la validación (por ejemplo, parámetros importantes en un campo oculto en HTML o pasar un puntero a una memoria crítica)


Microsoft
elevation of privilege
of

K Manipulación

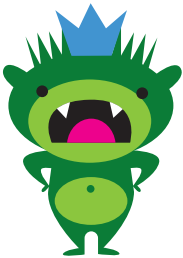
Un atacante puede cargar código dentro de su proceso a través de un punto de extensión


Microsoft
elevation of privilege
of

A

Manipulación

Has inventado un nuevo ataque de manipulación

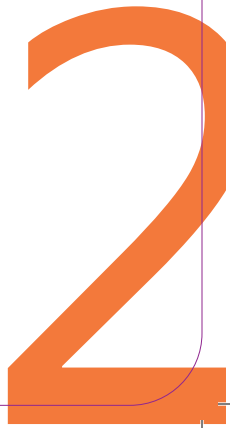


A


Microsoft
elevation of privilege
of

2 Repudio

Un atacante puede pasar datos a través del registro para atacar a un lector de registros, y no hay documentación sobre qué tipo de validación se realiza




Microsoft
elevation of privilege
of

3 Repudio

Un atacante con privilegios bajos puede leer información de seguridad interesante en los registros


Microsoft
elevation of privilege
of

4 Repudio

Un atacante puede alterar las firmas digitales porque el sistema de firma digital que está implementando es débil o usa MAC donde debería usar una firma


Microsoft
elevation of privilege
of

5 Repudio

Un atacante puede alterar los mensajes de registro en una red porque carecen de controles de integridad sólidos


Microsoft
elevation of privilege
of

6 Repudio

Un atacante puede crear una entrada de registro sin una marca de tiempo (o ninguna entrada de registro tiene una marca de tiempo)


Microsoft
elevation of privilege
of

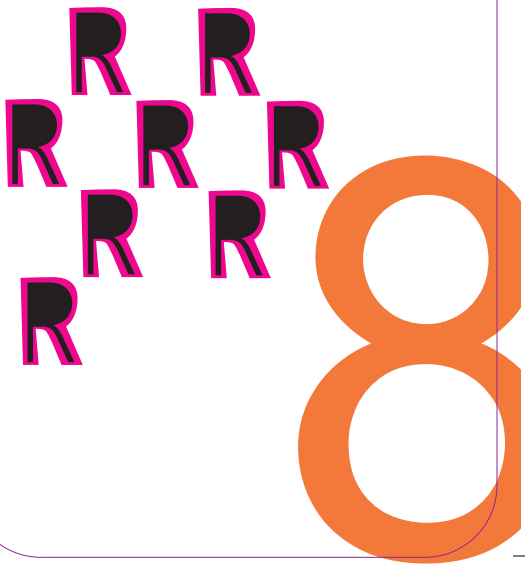
7 Repudio

Un atacante puede hacer que los registros se retuerzan y pierdan datos


Microsoft
elevation of privilege
of

8 Repudio

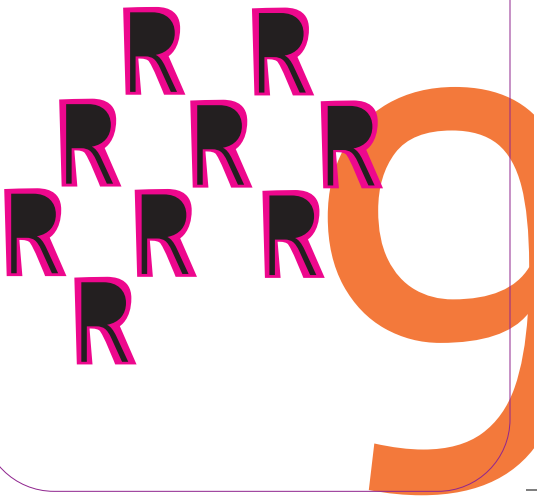
Un atacante puede hacer que un registro se pierda o confunda información de seguridad




Microsoft
elevation of privilege
of

9 Repudio

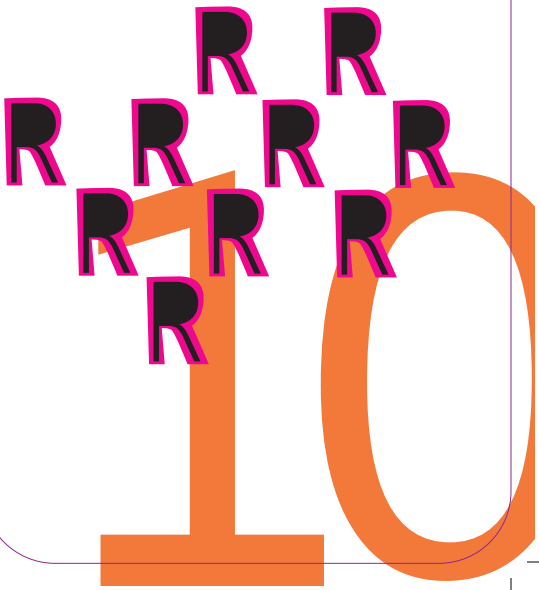
Un atacante puede utilizar una clave compartida para autenticarse como principales diferentes, confundiendo la información en los registros




Microsoft
elevation of privilege
of

10 Repudio

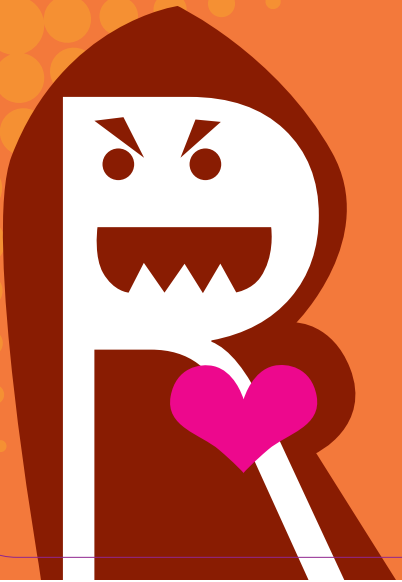
Un atacante puede obtener datos arbitrarios a registros de personas externas no autenticadas (o débilmente autenticadas) sin validación




Microsoft
elevation of privilege
of

J Repudio

Un atacante puede editar registros y no hay forma de saberlo (quizás porque no hay una opción de latido para el sistema de registro)




Microsoft
elevation of privilege
of

Q Repudio

Un atacante puede decir "Yo no hice eso" y no habría forma de demostrar que está equivocado


Microsoft
elevation of privilege
of

K

Repudio

El sistema no tiene registros

logs = 0


Microsoft
elevation of privilege
of

A

Repudio

Has inventado un nuevo ataque de repudio


Microsoft
elevation of privilege
of

2 Divulgación de Información

Un atacante puede cifrar archivos con fuerza bruta porque no existe ninguna defensa (defensa por ejemplo, extensión de contraseña)

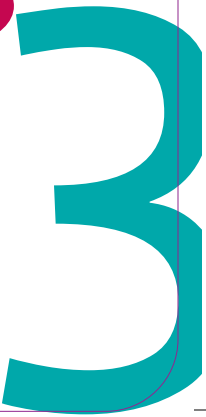
2


Microsoft
elevation of privilege
of

3

Divulgación de Información

Un atacante puede ver mensajes de error con contenido sensible a la seguridad




Microsoft
elevation of privilege
of

4 Divulgación de Información

Un atacante puede leer contenido porque los mensajes (por ejemplo, un correo electrónico o una cookie HTTP) no está encriptado incluso si el canal está encriptado


Microsoft
elevation of privilege
of

5 Divulgación de Información

Un atacante puede ser capaz de leer un documento o datos porque están encriptados con un algoritmo no estándar


Microsoft
elevation of privilege
of

6 Divulgación de Información

Un atacante puede leer datos porque están ocultos u ocluidos (para deshacer o cambiar el seguimiento) y el usuario puede olvidar que está ahí


Microsoft
elevation of privilege
of

7 Divulgación de Información

Un atacante puede actuar como un "intermediario" porque no autentica los puntos finales de una conexión de red


Microsoft
elevation of privilege
of

8 Divulgación de Información

Un atacante puede acceder a la información a través de un indexador de búsqueda, un registrador u otro mecanismo similar


Microsoft
elevation of privilege
of

9 Divulgación de Información

Un atacante puede leer información confidencial en un archivo con permisos permisivos


Microsoft
elevation of privilege
of

10 Divulgación de Información

Un atacante puede leer información en archivos o bases de datos sin controles de acce


Microsoft
elevation of privilege
of

J

Divulgación de Información

Un atacante puede descubrir la clave fija que se utiliza para cifrar


Microsoft
elevation of privilege
of

Q

Divulgación de Información

Un atacante puede leer el canal completo porque el canal (por ejemplo, HTTP o SMTP) no está encriptado.


Microsoft
elevation of privilege
of

K

Divulgación de Información

Un atacante puede leer información de la red porque no se utiliza criptografía


Microsoft
elevation of privilege
of

A

Divulgación de Información

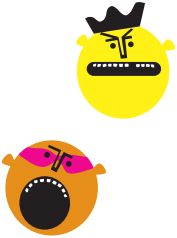
Has inventado un nuevo ataque de divulgación de información


Microsoft
elevation of privilege
of

2

Denegación de Servicio

Un atacante puede inutilizar o dejar de estar disponible su sistema de autenticación



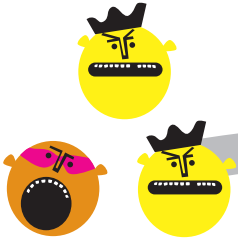
2


Microsoft
elevation of privilege
of

3

Denegación de Servicio

Un atacante puede agotar nuestra batería fácilmente reemplazable **(batería, temporal)**



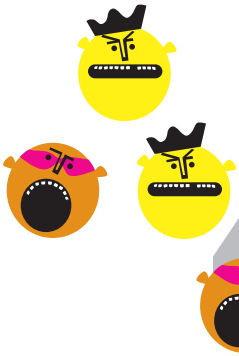
3


Microsoft
elevation of privilege
of

4

Denegación de Servicio

Un atacante puede agotar una batería que es difícil de reemplazar **(sellada en un teléfono, en un dispositivo médico implantado o en un lugar de difícil acceso)** (batería,

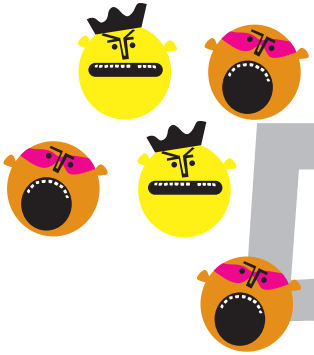


4


Microsoft
elevation of privilege
of

5 Denegación de Servicio

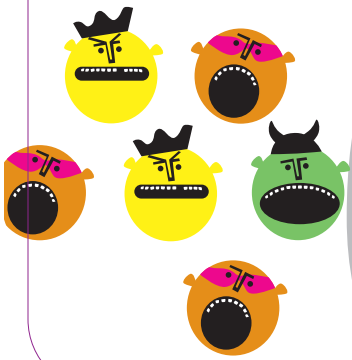
Un atacante puede gastar nuestro presupuesto en la nube **(presupuesto, persistir)**




Microsoft
elevation of privilege
of

6 Denegación de Servicio

Un atacante puede hacer que un servidor no esté disponible o sea inutilizable sin siquiera autenticarse, pero el problema desaparece cuando el atacante se detiene **(servidor, anónimo, temporal)**



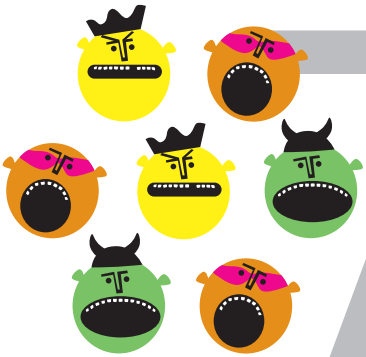
6


Microsoft
elevation of privilege
of

7

Denegación de Servicio

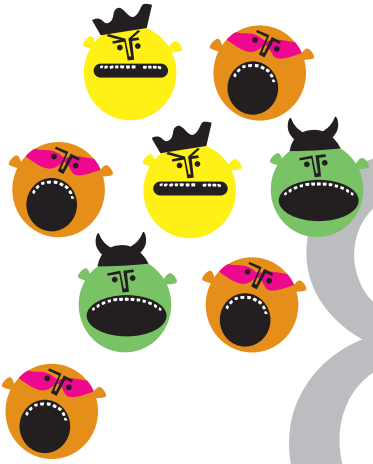
An attacker can make a client unavailable or unusable and the problem persists after the attacker goes away **(cliente, autenticación, persistir)**




Microsoft
elevation of privilege
of

8 Denegación de Servicio

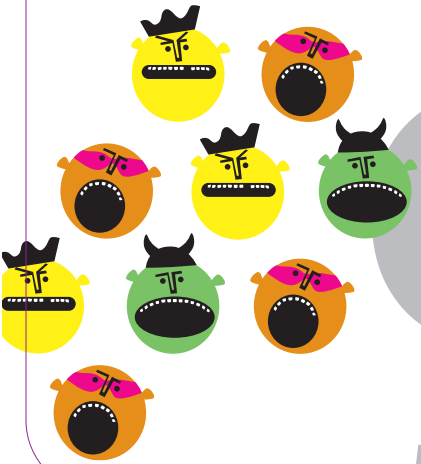
Un atacante puede hacer que un servidor no esté disponible o sea inutilizable y el problema persista después de que el atacante desaparezca **(servidor,**




Microsoft
elevation of privilege
of

9 Denegación de Servicio

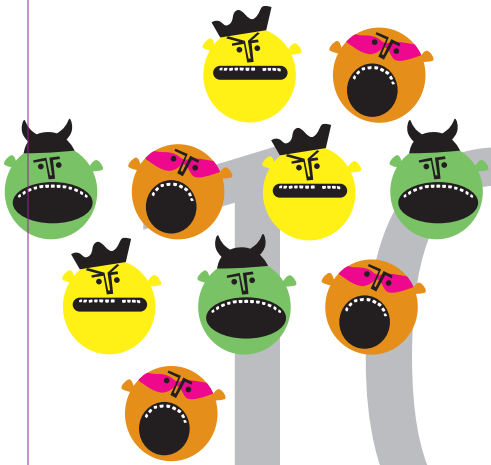
Un atacante puede hacer que un cliente no esté disponible o sea inutilizable sin siquiera autenticarse y el problema persiste después de que el atacante desaparece **(servidor, autenticación, persistir)**




Microsoft
elevation of privilege
of

10 Denegación de Servicio

An attacker can make a server unavailable or unusable without ever authenticating and the problem persists after the attacker goes away **(servidor, anónimo, persistir)**




Microsoft
elevation of privilege
of

J

Denegación de Servicio

Un atacante puede hacer que el subsistema de registro deje de funcionar


Microsoft
elevation of privilege
of

Q

Denegación de Servicio

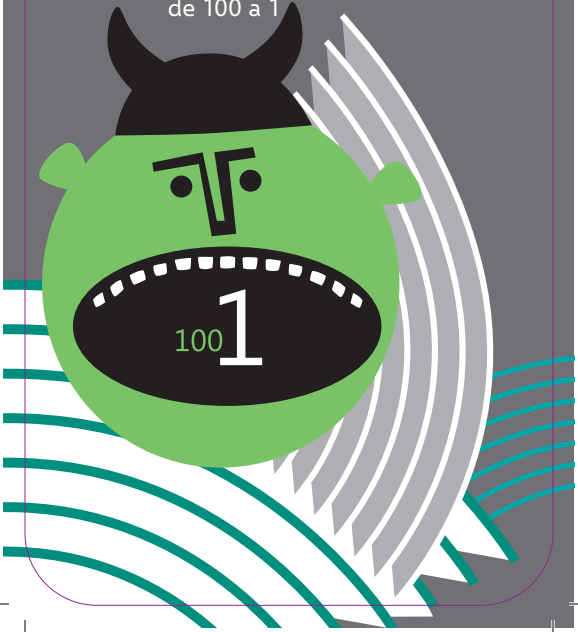
Un atacante puede amplificar un ataque de denegación de servicio a través de este componente con una amplificación del orden de 10 a 1


Microsoft
elevation of privilege
of

K

Denegación de Servicio

Un atacante puede amplificar un ataque de denegación de servicio a través de este componente con una amplificación del orden de 100 a 1




Microsoft
elevation of privilege
of

A

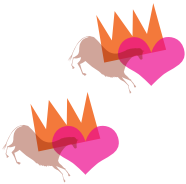
Denegación de Servicio

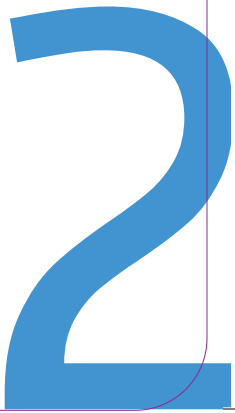
Has inventado un nuevo ataque de denegación de servicio


Microsoft
elevation of privilege
of

2 Elevación de Privilegios

Un atacante ha comprometido a un proveedor de tecnología clave

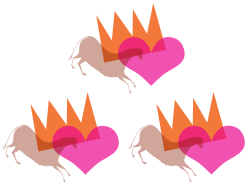





Microsoft
elevation of privilege
of

3 Elevación de Privilegios

Un atacante puede acceder al servicio en la nube que gestiona sus dispositivos

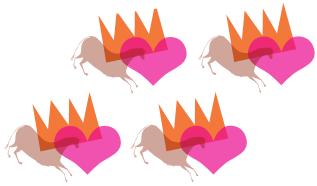


3


Microsoft
elevation of privilege
of

4 Elevación de Privilegios

Un atacante puede escapar de un contenedor u otra zona de pruebas

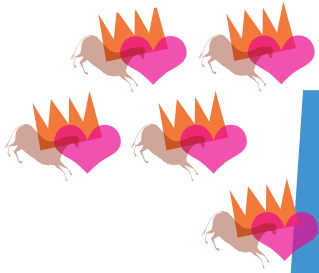


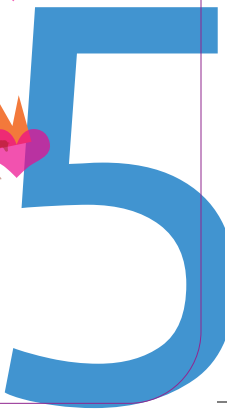
4


Microsoft
elevation of privilege
of

5 Elevación de Privilegios

Un atacante puede forzar los datos a través de diferentes rutas de validación que dan resultados diferentes

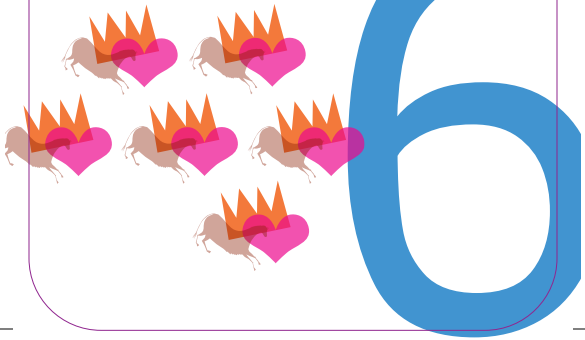





Microsoft
elevation of privilege
of

6 Elevación de Privilegios

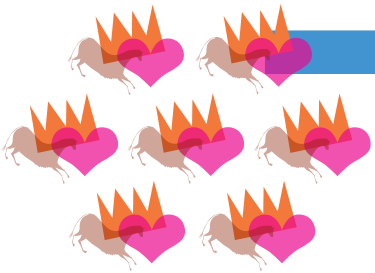
Un atacante podría aprovechar los permisos que usted establece, pero no utiliza




Microsoft
elevation of privilege
of

7 Elevación de Privilegios

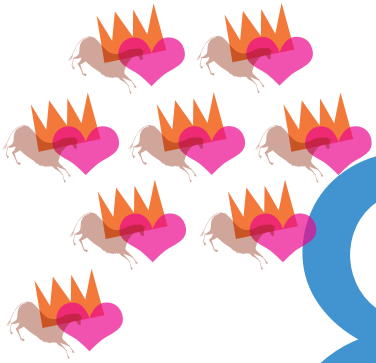
Un atacante puede proporcionar un indicador a través de un límite de confianza, en lugar de datos que puedan validarse

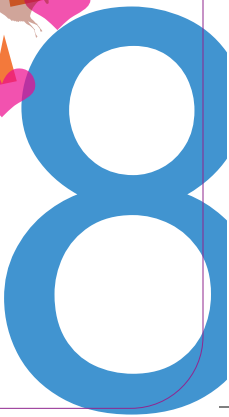



Microsoft
elevation of privilege
of

8 Elevación de Privilegios

Un atacante puede ingresar datos que se verifican mientras aún están bajo su control y se usan más tarde al otro lado de un límite de

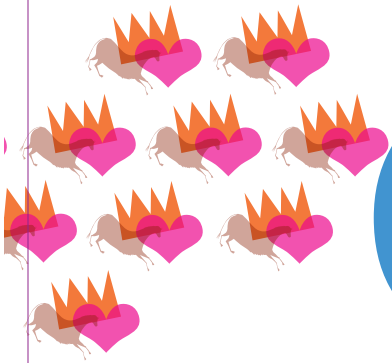


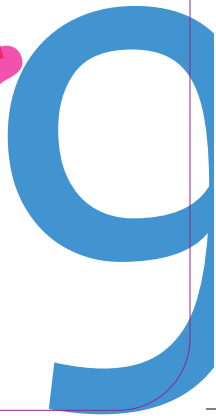



Microsoft
elevation of privilege
of

9 Elevación de Privilegios

No existe una forma razonable para que una persona que llama averigüe qué validación de datos contaminados realiza antes de pasárselos

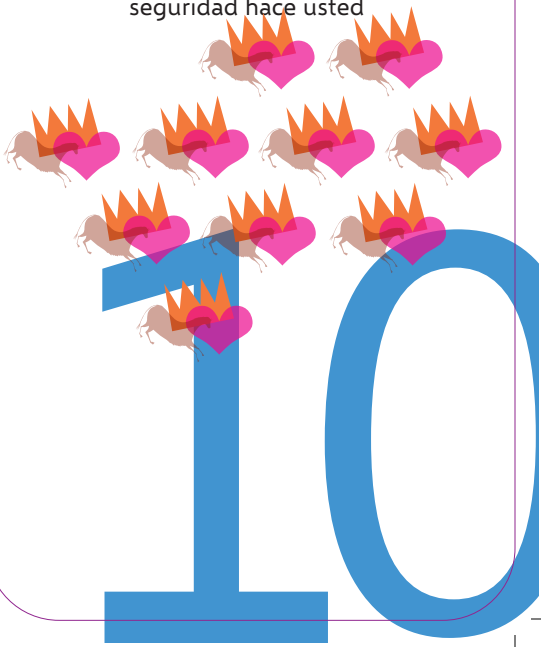





Microsoft
elevation of privilege
of

10 Elevación de Privilegios

No existe una forma razonable para que una persona que llama averigüe qué suposiciones de seguridad hace usted

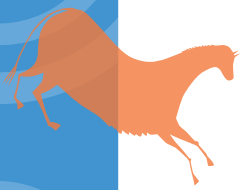



Microsoft
elevation of privilege
of

J

Elevación de Privilegios

Un atacante puede reflejar la entrada a un usuario, como secuencias de comandos entre sitios



J


Microsoft
elevation of privilege
of

Q

Elevación de Privilegios

Incluye contenido generado por el usuario dentro de su página, posiblemente incluyendo el contenido de URL aleatorias


Microsoft
elevation of privilege
of

K

Elevación de Privilegios

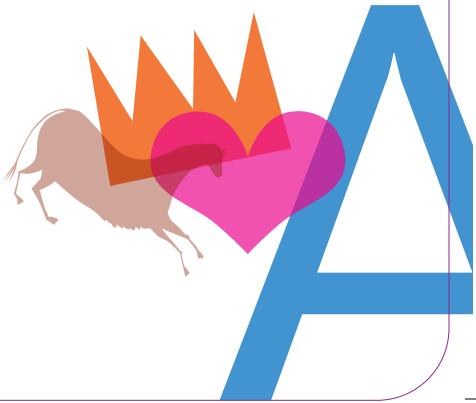
Un atacante puede inyectar un comando que el sistema ejecutará con un nivel de privilegio más alto


Microsoft
elevation of privilege
of

A

Elevación de Privilegios

Has inventado un nuevo ataque de Elevación de Privilegios




Microsoft
elevation of privilege
of

Spoofing

2. Un atacante podría apoderarse del puerto o socket que normalmente utiliza el servidor

3. Un atacante podría probar una credencial tras otra y no hay nada que las ralentice (en línea o fuera de línea)

4. Un atacante puede conectarse de forma anónima porque esperamos que la autenticación se realice en un nivel superior

5. Un atacante puede confundir a un cliente porque hay demasiadas formas de identificar un servidor

6. Un atacante puede falsificar un servidor porque los identificadores no se almacenan en el cliente y no se verifica su coherencia al volver a conectarse (es decir, no hay persistencia de claves)

7. Un atacante puede conectarse a un servidor o a través de un enlace que no está autenticado (ni cifrado)

8. Un atacante podría robar las credenciales almacenadas en el servidor y reutilizarlas (por ejemplo, una clave se almacena en un archivo legible por todo el mundo)

continuó en la parte de atrás

Spoofing

Spoofing cont.

9. Un atacante que obtiene una contraseña puede reutilizarla (use autenticadores más seguros)

10. Un atacante puede optar por utilizar una autenticación más débil o nula

J. Un atacante podría robar las credenciales almacenadas en el cliente y reutilizarlas

Q. Un atacante podría atacar la forma en que se actualizan o recuperan las credenciales (la recuperación de la cuenta no requiere revelar la contraseña anterior)

K. Su sistema viene con una contraseña de administrador predeterminada y no fuerza ningún cambio

A. Has inventado un nuevo ataque de Spoofing

Manipulación

2. Un atacante puede aprovechar su intercambio de claves personalizado o el control de integridad que usted creó en lugar de usar criptografía estándar

3. Un atacante puede modificar su sistema de compilación y producir compilaciones firmadas de su software

4. Su código toma decisiones de control de acceso en todas partes, en lugar de hacerlo con un núcleo de seguridad

5. Un atacante puede reproducir datos sin ser detectado porque su código no proporciona marcas de tiempo ni números de secuencia

6. Un atacante puede escribir en un almacén de datos en el que se basa su código

7. Un atacante puede eludir los permisos porque no convierte los nombres en canónicos antes de verificar los permisos de acceso

8. Un atacante puede manipular datos porque no existe protección de integridad para los datos en la red

continuó en la parte de atrás

Manipulación

Manipulación cont.

9. Un atacante puede proporcionar o controlar información de estado

10. Un atacante puede alterar la información en un almacén de datos porque tiene permisos débiles/abiertos o incluye un grupo que es equivalente a todos ("cualquier persona con una cuenta de Facebook")

J. Un atacante puede escribir en algún recurso porque se otorgan permisos al mundo o no hay ACL

Q. Un atacante puede cambiar los parámetros más allá de un límite de confianza y después de la validación (por ejemplo, parámetros importantes en un campo oculto en HTML o pasar un puntero a una memoria crítica)

K. Un atacante puede cargar código dentro de su proceso a través de un punto de extensión

A. Has inventado un nuevo ataque de manipulación

Manipulación

R

Repudio

2. Un atacante puede pasar datos a través del registro para atacar a un lector de registros, y no hay documentación sobre qué tipo de validación se realiza

3. Un atacante con privilegios bajos puede leer información de seguridad interesante en los registros

4. Un atacante puede alterar las firmas digitales porque el sistema de firma digital que está implementando es débil o usa MAC donde debería usar una firma

5. Un atacante puede alterar los mensajes de registro en una red porque carecen de controles de integridad sólidos

6. Un atacante puede crear una entrada de registro sin una marca de tiempo (o ninguna entrada de registro tiene una marca de tiempo)

7. Un atacante puede hacer que los registros se retuerzan y pierdan datos

8. Un atacante puede hacer que un registro se pierda o confunda información de seguridad

continuó en la parte de atrás

Repudio

R

Repudio cont.

9. Un atacante puede utilizar una clave compartida para autenticarse como principales diferentes, confundiendo la información en los registros

10. Un atacante puede obtener datos arbitrarios a registros de personas externas no autenticadas (o débilmente autenticadas) sin validación

J. Un atacante puede editar registros y no hay forma de saberlo (quizás porque no hay una opción de latido para el sistema de registro)

Q. Un atacante puede decir "Yo no hice eso" y no habría forma de demostrar que está equivocado

K. El sistema no tiene registros

A. Has inventado un nuevo ataque de repudio

Divulgación de Información

2. Un atacante puede cifrar archivos con fuerza bruta porque no existe ninguna defensa (defensa por ejemplo, extensión de contraseña)

3. Un atacante puede ver mensajes de error con contenido sensible a la seguridad

4. Un atacante puede leer contenido porque los mensajes (por ejemplo, un correo electrónico o una cookie HTTP) no está encriptado incluso si el canal está encriptado

5. Un atacante puede ser capaz de leer un documento o datos porque están encriptados con un algoritmo no estándar

6. Un atacante puede leer datos porque están ocultos u ocluidos (para deshacer o cambiar el seguimiento) y el usuario puede olvidar que está ahí

7. Un atacante puede actuar como un "intermediario" porque no autentica los puntos finales de una conexión de red

continuó en la parte de atrás

Divulgación de Información

Divulgación de Información cont.

8. Un atacante puede acceder a la información a través de un indexador de búsqueda, un registrador u otro mecanismo similar

9. Un atacante puede leer información confidencial en un archivo con permisos permisivos

10. Un atacante puede leer información en archivos o bases de datos sin controles de acceso

J. Un atacante puede descubrir la clave fija que se utiliza para cifrar

Q. Un atacante puede leer el canal completo porque el canal (por ejemplo, HTTP o SMTP) no está encriptado.

K. Un atacante puede leer información de la red porque no se utiliza criptografía

A. Has inventado un nuevo ataque de divulgación de información

Divulgación de Información

Denegación de Servicio

2. Un atacante puede inutilizar o dejar de estar disponible su sistema de autenticación

3. Un atacante puede agotar nuestra batería fácilmente reemplazable **(batería, temporal)**

4. Un atacante puede agotar una batería que es difícil de reemplazar (sellada en un teléfono, en un dispositivo médico implantado o en un lugar de difícil acceso) **(batería, persistir)**

5. Un atacante puede gastar nuestro presupuesto en la nube **(presupuesto, persistir)**

6. Un atacante puede hacer que un servidor no esté disponible o sea inutilizable sin siquiera autenticarse, pero el problema desaparece cuando el atacante se detiene **(servidor, anónimo, temporal)**

7. An attacker can make a client unavailable or unusable and the problem persists after the attacker goes away **(cliente, autenticación, persistir)**

8. Un atacante puede hacer que un servidor no esté disponible o sea inutilizable y el problema persista después de que el atacante desaparezca **(servidor, autenticación, persistir)**

continuó en la parte de atrás

Denegación de Servicio

Denegación de Servicio cont.

9. Un atacante puede hacer que un cliente no esté disponible o sea inutilizable sin siquiera autenticarse y el problema persiste después de que el atacante desaparece **(servidor, autenticación, persistir)**

10. An attacker can make a server unavailable or unusable without ever authenticating and the problem persists after the attacker goes away **(servidor, anónimo, persistir)**

J. Un atacante puede hacer que el subsistema de registro deje de funcionar

Q. Un atacante puede amplificar un ataque de denegación de servicio a través de este componente con una amplificación del orden de 10 a 1

K. Un atacante puede amplificar un ataque de denegación de servicio a través de este componente con una amplificación del orden de 100 a 1

A. Has inventado un nuevo ataque de denegación de servicio

Denegación de Servicio

Elevación de Privilegios

2. Un atacante ha comprometido a un proveedor de tecnología clave

3. Un atacante puede acceder al servicio en la nube que gestiona sus dispositivos

4. Un atacante puede escapar de un contenedor u otra zona de pruebas

5. Un atacante puede forzar los datos a través de diferentes rutas de validación que dan resultados diferentes

6. Un atacante podría aprovechar los permisos que usted establece, pero no utiliza

7. Un atacante puede proporcionar un indicador a través de un límite de confianza, en lugar de datos que puedan validarse

8. Un atacante puede ingresar datos que se verifican mientras aún están bajo su control y se usan más tarde al otro lado de un límite de confianza

continuó en la parte de atrás

Elevación de Privilegios

Elevación de Privilegios cont.

9. No existe una forma razonable para que una persona que llama averigüe qué validación de datos contaminados realiza antes de pasárselos

10. No existe una forma razonable para que una persona que llama averigüe qué suposiciones de seguridad hace usted

J. Un atacante puede reflejar la entrada a un usuario, como secuencias de comandos entre sitios

Q. Incluye contenido generado por el usuario dentro de su página, posiblemente incluyendo el contenido de URL aleatorias

K. Un atacante puede inyectar un comando que el sistema ejecutará con un nivel de privilegio más alto

A. Has inventado un nuevo ataque de Elevación de Privilegios

Elevación de Privilegios

Acerca de

Modelado de amenazas

El juego Elevación de Privilegio está diseñado para ser la forma más sencilla de empezar a analizar su diseño desde una perspectiva de seguridad. Es una forma de modelar amenazas, destinada a ser recogida y utilizada por cualquier grupo de desarrollo. Debido a que el juego utiliza amenazas STRIDE, te brinda un marco para pensar y ejemplos prácticos específicos de esas amenazas.

STRIDE significa:
Spoofing: Hacerse pasar por algo o alguien más.

Tampering: Modificar datos o código.

Repudiation: Afirmar no haber realizado una acción.

Information Disclosure: Exponer información a alguien no autorizado para verla.

Denial of Service: Denegar o degradar el servicio a las usuarias.

Elevation of Privilege: Obtener capacidades sin la autorización adecuada.

En **www.microsoft.com/security/sdl/eop** tenemos vídeos, hojas de puntuación y consejos y trucos para jugar.

Acerca de

SDL

El juego "Elevation of Privilege" es una manera fácil y divertida de comenzar a comprender la seguridad de sus sistemas mediante el modelado de amenazas. A medida que descubre y corrige problemas de seguridad a nivel de diseño, vale la pena pensar en otras formas en que los problemas de seguridad pueden infiltrarse en su código. Microsoft tiene una gran colección de recursos gratuitos disponibles para ayudarle a comenzar con el ciclo de vida de desarrollo de seguridad (SDL).

Para obtener más información sobre el modelado de

Microsoft

el ciclo de vida de desarrollo de seguridad