República Federativa do Brasil
Ministério da Economia
Instituto Nacional da Propriedade Industrial

(11) BR 112018074497-2 B1

(22) Data do Depósito: 18/04/2017

(45) Data de Concessão: 30/11/2021

(54) Título: MÉTODO PARA PREVENIR QUE UM SERVIDOR SEJA ATACADO E DISPOSITIVO PARA PREVENIR QUE UM SERVIDOR SEJA ATACADO

(51) Int.Cl.: H04L 29/02; H04L 29/06; H04L 9/32.

(52) CPC: H04L 29/02; H04L 63/102; H04L 9/3213.

(30) Prioridade Unionista: 31/05/2016 CN 201610377847.0.

(73) Titular(es): ADVANCED NEW TECHNOLOGIES CO., LTD..

(72) Inventor(es): YARAN LU.

(86) Pedido PCT: PCT CN2017080862 de 18/04/2017

(87) Publicação PCT: WO 2017/206605 de 07/12/2017

(85) Data do Início da Fase Nacional: 27/11/2018

(57) Resumo: A presente invenção divulga um método e um dispositivo para prevenir que um servidor seja atacado e se relaciona com o campo de tecnologias de segurança de rede, para resolver um problema de baixa segurança de servidor. As principais soluções técnicas da presente invenção são as seguintes: alocar dinamicamente e aleatoriamente um script de página correspondendo a uma solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página, ao receber a solicitação da página enviada por um navegador; enviar o script de página alocado dinamicamente e aleatoriamente para o navegador, para que o navegador execute o script de página para obter um parâmetro de execução de script; determinar se uma solicitação de verificação da página está expirada, ao receber a solicitação de verificação da página enviada pelo navegador; e, se estiver espirada, exibir informações de prompt de erro indicando a expiração da página; ou se não estiver expirada, verificar se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido; e se for inválido, rejeitar a solicitação da página. A presente invenção é usada principalmente para prevenir que um servidor seja atacado.

“MÉTODO PARA PREVENIR QUE UM SERVIDOR SEJA ATACADO E DISPOSITIVO PARA PREVENIR QUE UM SERVIDOR SEJA ATACADO”

CAMPO DA INVENÇÃO

[001] A presente invenção refere-se ao campo das tecnologias de segurança de rede e, em particular, a um método e um dispositivo para prevenir que um servidor seja atacado.

ANTECEDENTES DA INVENÇÃO

[002] À medida que as tecnologias da Internet se desenvolvem rapidamente, a garantia de segurança de rede atrai mais atenção. De modo geral, a segurança da rede está relacionada a como prevenir que um servidor na rede seja atacado. Para atacar um servidor, um invasor usa uma solicitação de serviço para ocupar recursos de serviço excessivos do servidor, o que leva à sobrecarga do servidor. Além disso, o servidor não pode responder a outras solicitações e, consequentemente, os recursos do servidor podem se esgotar. Como tal, o invasor faz com que o servidor se recuse a fornecer serviços.

[003] Atualmente, um navegador envia primeiro uma solicitação de serviço ao servidor. A solicitação de serviço inclui um valor de token no cookie (dados armazenados pelo servidor em um dispositivo terminal local de um usuário) criptografado usando o algoritmo de resumo de mensagem 5 (MD5). Depois de receber a solicitação de serviço, o servidor verifica o valor do token criptografado para determinar se a solicitação de serviço enviada pelo navegador é válida para prevenir que um servidor seja atacado. No entanto, o valor do token criptografado é obtido pela execução do código de script estático e o código de script estático é exposto em um texto simples. Portanto, o invasor pode obter diretamente a lógica no código de script estático e analisar o método de criptografia do valor do token. Assim, o invasor pode ignorar um mecanismo de detecção do servidor, simulando a solicitação de serviço do usuário comum e, em seguida, atacando o servidor. Portanto, a proteção de

segurança para o servidor existente é baixa.

DESCRIÇÃO DA INVENÇÃO

[004] Em vista do problema do estado da técnica, a presente invenção é proposta para fornecer um método e um dispositivo para prevenir que um servidor seja atacado, para superar o problema do estado da técnica ou pelo menos resolver parcialmente o problema do estado da técnica.

[005] Para atingir o objetivo anterior, a presente invenção fornece principalmente as soluções técnicas abaixo.

[006] Uma forma de realização da presente invenção fornece um método para prevenir que um servidor seja atacado, e o método inclui o seguinte: alocar dinamicamente e aleatoriamente um script de página correspondendo a uma solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página, ao receber a solicitação da página enviada por um navegador; enviar o script de página alocado dinamicamente e aleatoriamente para o navegador, para que o navegador execute o script de página para obter um parâmetro de execução de script; determinar que a solicitação de verificação da página está expirada, ao receber uma solicitação de verificação da página enviada pelo navegador; e, se estiver espirada, exibir informações de prompt de erro indicando a expiração da página; ou, se não estiver espirada, verificar se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido; e se for inválido, rejeitar a solicitação da página.

[007] Uma outra forma de realização da presente invenção fornece ainda um dispositivo para prevenir que um servidor seja atacado, e o dispositivo inclui uma unidade de alocação, configurada para alocar dinamicamente e aleatoriamente um script de página correspondendo a uma solicitação da página de uma pluralidade de scripts de página correspondendo à solicitação da página, quando a solicitação da página enviada por um

navegador é recebida; uma unidade de envio, configurada para enviar o script de página alocado dinamicamente e aleatoriamente para o navegador, para que o navegador execute o script de página para obter um parâmetro de execução de script; uma unidade de determinação, configurada para determinar se uma solicitação de verificação da página está expirada, quando a solicitação de verificação da página enviada pelo navegador é recebida; uma unidade de saída, configurada para fornecer informações de prompt de erro indicando a expiração da página, se a solicitação de verificação da página estiver espirada; uma unidade de verificação, configurada para verificação se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido, se a solicitação de verificação da página não estiver expirada; e uma unidade de rejeição, configurada para rejeitar a solicitação da página, se o parâmetro de execução de script compreendido na solicitação de verificação da página estiver inválido.

[008] Com base no acima exposto, as soluções técnicas fornecidas nas formas de realização da presente invenção possuem pelo menos as vantagens abaixo.

[009] De acordo com o método e dispositivo para prevenir que um servidor seja atacado, fornecido nas formas de realização da presente invenção, ao receber a solicitação de verificação da página enviada pelo navegador, o servidor primeiro determina se a solicitação de verificação da página está expirada. Se a solicitação de verificação da página não estiver espirada, o servidor verificará se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido. Se o parâmetro de execução de script estiver inválido, o servidor rejeitará a solicitação da página para prevenir que um servidor seja atacado. Atualmente, o servidor verifica um valor de token criptografado para determinar se uma solicitação de serviço enviada pelo navegador é válida para prevenir que um servidor seja

atacado. Comparado com isso, na presente invenção, o servidor verifica o parâmetro de execução de script para evitar que o servidor seja atacado. O parâmetro de execução de script é obtido com base no script de página, alocado dinamicamente e aleatoriamente a partir da pluralidade de scripts de página correspondendo à solicitação da página, e é utilizada uma lógica de aquisição de parâmetros de execução de script diferente nos scripts de página. Portanto, mesmo que um invasor obtenha lógica de script no código dinâmico, o invasor não poderá analisar o método de criptografia do parâmetro de execução de script dentro de um período de tempo predeterminado. Além disso, quando o tempo de solicitação da solicitação de verificação da página excede o período de tempo predeterminado, o servidor rejeita a solicitação da página. O navegador precisa recarregar uma solicitação de verificação da página para enviar novamente a solicitação de verificação da página, e um parâmetro de execução de script na solicitação de verificação da página recarregada é obtido pela execução de um script de página reextraído. Portanto, o invasor não pode atacar o servidor nas formas de realização da presente invenção. Como tal, a segurança do servidor é melhorada nas formas de realização da presente invenção.

BREVE DESCRIÇÃO DOS DESENHOS

[010] Ao ler as descrições detalhadas das seguintes formas de realização preferidas, várias outras vantagens e benefícios podem ser entendidos por um técnico no assunto. Os desenhos em anexo são utilizados apenas para ilustrar as formas de realização preferidas e não são considerados como uma limitação na presente invenção. Além disso, os mesmos símbolos de referência são usados para representar os mesmos componentes ao longo dos desenhos anexos. Nos desenhos anexos:

- A Figura 1 é um fluxograma que ilustra um método para prevenir que um servidor seja atacado, de acordo com uma forma de realização da

presente invenção;

- A Figura 2 é um fluxograma que ilustra outro método para prevenir que um servidor seja atacado, de acordo com uma forma de realização da presente invenção;

- A Figura 3 é um diagrama de blocos de composição que ilustra um dispositivo para prevenir que um servidor seja atacado, de acordo com uma forma de realização da presente invenção;

- A Figura 4 é um diagrama de blocos de composição que ilustra outro dispositivo para prevenir que um servidor seja atacado, de acordo com uma forma de realização da presente invenção; e

- A Figura 5 é um diagrama de blocos que ilustra um sistema para prevenir que um servidor seja atacado, de acordo com uma forma de realização da presente invenção.

DESCRIÇÃO DE REALIZAÇÕES DA INVENÇÃO

[011] O modo seguinte descreve as formas de realização de exemplo da presente invenção com mais detalhe com referência aos desenhos anexos. Embora os desenhos acompanhantes mostrem as formas de realização de exemplo da presente invenção, deve ser entendido que a presente invenção pode ser implementada em várias formas, e não deve ser limitada pelas formas de realização aqui descritas. Em vez disso, estas formas de realização são proporcionadas para proporcionar uma compreensão mais completa da presente invenção e para transmitir completamente o escopo da presente invenção a um técnico no assunto.

[012] Para tornar mais claras as vantagens das soluções técnicas na presente descrição, o que se segue descreve a presente invenção em detalhe com referência aos desenhos anexos e às formas de realização.

[013] Uma forma de realização da presente invenção fornece um método para prevenir que um servidor seja atacado. Como mostrado na Figura

1, o método inclui os passos abaixo.

[014] (101). Alocar dinamicamente e aleatoriamente um script de página correspondendo à solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página, ao receber uma solicitação da página enviada por um navegador.

[015] A solicitação da página inclui uma URL da página e o URL da página é uma página que corresponde ao script de página solicitado pelo navegador. Nesta forma de realização da presente invenção, uma URL da página corresponde a uma pluralidade de scripts de página. Uma lógica de aquisição de parâmetros de execução de script diferente é usada em scripts de página correspondendo à mesma URL da página. Uma pluralidade de parâmetros de execução de script diferentes é obtida quando uma pluralidade de scripts de página correspondendo à mesma URL da página são executados. Resultados de execução da página da pluralidade de scripts de página correspondendo à mesma URL da página são os mesmos, ou seja, páginas geradas depois que o navegador carrega e executa os scripts de página são os mesmos. Vale a pena notar que nesta forma de realização da presente invenção, o script de página correspondendo à solicitação da página pode ser alocado dinamicamente e aleatoriamente a partir da pluralidade de scripts de página correspondendo à solicitação da página, utilizando um número aleatório gerado com base em um tempo atual ou um número aleatório gerado com base em um tempo para enviar a solicitação da página. Nenhuma limitação específica é imposta nesta forma de realização da presente invenção.

[016] Por exemplo, se um usuário inserir uma URL do AMAZON em uma barra de endereços do navegador e pressionar uma tecla Enter, o servidor receberá uma solicitação da página enviada pelo navegador. Uma URL da página na solicitação da página é AMAZON. Em seguida, o servidor aloca dinamicamente e aleatoriamente um script de página correspondendo à

solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página. Ou seja, o servidor aloca dinamicamente e aleatoriamente um script de página correspondendo à solicitação da página a partir de uma pluralidade de scripts de página correspondendo ao AMAZON.

[017] (102). Enviar o script de página alocado dinamicamente e aleatoriamente para o navegador.

[018] Além disso, o navegador carrega e executa o script de página para obter um parâmetro de execução de script. Depois de carregar e executar o script de página, o navegador exibe uma página correspondente e obtém o parâmetro de execução de script. Os parâmetros de execução de script são alguns parâmetros adicionais na página e não afetam a página exibida. Nesta forma de realização da presente invenção, quando são executados scripts de página correspondendo mesma URL da página, diferentes parâmetros de execução de scripts são gerados em resultados de execução de scripts de página diferentes.

[019] Por exemplo, uma determinada URL da página é correspondente a três scripts de página. A lógica de aquisição de parâmetros de execução de script em um script de página é obter um valor de token criptografado em informações de cookie. A lógica de aquisição de parâmetros de execução de script em outro script de página é obter valores criptografados das coordenadas atuais do mouse do usuário. A lógica de aquisição de parâmetros de execução de script no script de página restante é obter um valor criptografado de um tempo atual. Vale a pena notar que nesta forma de realização da presente invenção, a lógica para executar o script de página e o método de encriptação do parâmetro de execução de script não estão limitados, desde que seja utilizada uma lógica de aquisição de parâmetros de execução de scripts diferente nos scripts de página no presente relatório da

invenção para distinguir entre diferentes scripts de página.

[020] (103). Determine se uma solicitação de verificação da página está expirada ao receber a solicitação de verificação da página enviada pelo navegador.

[021] A solicitação de verificação da página pode ser enviada usando a página obtida com base no carregamento e execução na etapa (102). De forma específica, a solicitação pode ser enviada clicando em um determinado link na página, selecionando um determinado botão de comando, inserindo algumas palavras-chave etc. Nenhuma limitação específica é imposta nesta forma de realização da presente invenção. A solicitação de verificação da página inclui o parâmetro de execução de script e o parâmetro de execução de script é um parâmetro criptografado.

[022] Nesta forma de realização da presente invenção, um processo específico de determinar que a solicitação de verificação da página está expirada pode ser o seguinte: Primeiro, o servidor obtém um tempo de solicitação da solicitação de verificação da página e um tempo para o navegador executar o script de página na solicitação de verificação da página. Em seguida, o servidor determina se o tempo de solicitação da solicitação de verificação da página é posterior à soma de um período de tempo predeterminado e o tempo para o navegador executar o script de página. O servidor determina que a solicitação de verificação da página expira, se o tempo de solicitação da solicitação de verificação da página for posterior à soma do período de tempo predeterminado e a hora em que o navegador executará o script de página. O servidor determina que a solicitação de verificação da página não está expirada, se o tempo de solicitação da solicitação de verificação da página não for posterior à soma do período de tempo predeterminado e da hora em que o navegador executará o script de página.

[023] O período de tempo predeterminado pode ser definido com base nos requisitos reais, por exemplo, 10 minutos, 20 minutos ou 40 minutos. Nenhuma limitação é imposta nesta forma de realização da presente invenção. Vale a pena observar que um invasor pode atacar o servidor simulando o comportamento do usuário comum e leva tempo para o invasor simular o comportamento do usuário comum. Por conseguinte, nesta forma de realização da presente invenção, sob a condição de que o usuário possa enviar uma solicitação ao servidor normalmente, quanto menor o período de tempo predeterminado, menos provável o invasor atacar o servidor.

[024] Por exemplo, se o tempo de solicitação da solicitação de verificação da página obtida na solicitação de verificação da página for 13:15, o tempo para o navegador executar o script de página é 12:34 e o período de tempo predeterminado é de um tempo, o servidor determina que o tempo de solicitação da solicitação de verificação da página é anterior à soma do período de tempo predeterminado e do tempo para o navegador executar o script de página, isto é, 13:15 é anterior a 13:34. Portanto, a solicitação de verificação da página não está expirada. Se o tempo de solicitação da solicitação de verificação da página for 14:12, o servidor poderá usar o método de determinação anterior para concluir que a solicitação de verificação da página está expirada.

[025] (104a). Se está expirada, enviar informações de prompt de erro indicando a expiração da página.

[026] Nesta forma de realização da presente invenção, a informação de solicitação de erro indicando a expiração da página será exibida se a solicitação de verificação da página tiver expirado, para solicitar ao usuário o fato de a página corrente ter expirado. Se o usuário ainda quiser executar uma operação na página, o usuário precisará atualizar a página. Atualizar a página é equivalente a enviar uma solicitação da página ao servidor. Depois de

receber a solicitação, o servidor aloca dinamicamente e aleatoriamente um script de página correspondendo à solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página. Isto é, após o passo (104a), se receber uma instrução de atualização do usuário, o servidor salta para o passo (101) para executar novamente o passo (101).

[027] (104b). Se não estiver expirada, verifique se um parâmetro de execução de script compreendido na solicitação de verificação da página é válido.

[028] O passo (104b) é paralelo ao passo (104a). O servidor verifica se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido, se a solicitação de verificação da página não estiver expirada. Nesta forma de realização da presente invenção, o servidor pode verificar, com base no script de página executado para obter o parâmetro de execução de script, se o parâmetro de execução de script é válido. Um processo específico da etapa (104b) pode ser o seguinte: Primeiro, o servidor obtém um parâmetro de script local com base no script de página e, em seguida, determina se o parâmetro de script local é o mesmo que o parâmetro de execução de script compreendido na solicitação de verificação da página; se sim, indica que o parâmetro de execução de script é válido; se não, indica que o parâmetro de execução de script é inválido.

[029] Por exemplo, depois que a solicitação de verificação da página enviada pelo navegador é recebida, se a lógica de aquisição de parâmetro de execução de script no script de página extraída dinamicamente e aleatoriamente da pluralidade de scripts de página correspondendo à solicitação da página for para obter um valor de token nas informações de cookie é criptografada usando um algoritmo de resumo de mensagem (5) (MD5) e a solicitação de verificação da página está em um período de validade, o servidor determina, com base na lógica de aquisição do parâmetro de

execução de script no script de página, se a verificação no parâmetro de script pode ser bem-sucedida. Ou seja, o servidor determina, com base no valor criptografado MD5 do token nas informações do cookie correspondendo armazenadas no servidor, se a verificação no parâmetro de script enviado pelo navegador pode ser bem-sucedida.

[030] (105b). Se inválido, rejeitar a solicitação da página.

[031] Nesta forma de realização da presente invenção, a solicitação da página é rejeitada se o parâmetro de execução de script estiver inválido após a verificação. Depois, se o usuário ainda quiser executar uma operação na página, o usuário precisará atualizar a página. Atualizar a página é equivalente a enviar uma solicitação da página ao servidor. Depois de receber a solicitação, o servidor aloca dinamicamente e aleatoriamente um script de página correspondendo à solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página. Isto é, após o passo (105b), se receber uma instrução de atualização do usuário, o servidor salta para o passo (101) para executar o passo (101) novamente.

[032] Vale a pena observar que na presente invenção, a solicitação da página pode ser rejeitada usando informações de identidade do usuário na solicitação de verificação da página, e as informações de identidade do usuário são informações de cookie geradas pelo servidor. Depois de receber as informações do cookie enviadas pelo servidor, o navegador armazena uma chave/ valor nas informações do cookie em um arquivo de texto em um determinado diretório. O navegador envia as informações do cookie para o servidor ao solicitar uma página da Web na próxima vez. Se a solicitação de verificação da página enviada pelo navegador está expirada ou o parâmetro de execução de script é inválido após a verificação, o servidor pode definir um serviço correspondendo às informações de cookie na solicitação de verificação da página para “rejeitar” para rejeitar a solicitação da página.

[033] No método para prevenir que um servidor seja atacado, fornecido nesta forma de realização da presente invenção, ao receber a solicitação de verificação da página enviada pelo navegador, o servidor primeiro determina se a solicitação de verificação da página está expirada. Se a solicitação de verificação da página não estiver espirada, o servidor verificará se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido. Se o parâmetro de execução de script estiver inválido, o servidor rejeitará a solicitação da página para prevenir que um servidor seja atacado. Atualmente, o servidor verifica um valor de token criptografado para determinar se uma solicitação de serviço enviada pelo navegador é válida para prevenir que um servidor seja atacado. Comparado com isso, na presente invenção, o servidor verifica o parâmetro de execução de script para evitar que o servidor seja atacado. O parâmetro de execução de script é obtido com base no script de página, alocado dinamicamente e aleatoriamente a partir da pluralidade de scripts de página correspondendo à solicitação da página, e é utilizada uma lógica de aquisição de parâmetros de execução de script diferente nos scripts de página. Portanto, mesmo que um invasor obtenha lógica de script no código dinâmico, o invasor não poderá analisar o método de criptografia do parâmetro de execução de script dentro do período de tempo predeterminado. Além disso, quando o tempo de solicitação da solicitação de verificação da página excede o período de tempo predeterminado, o servidor rejeita a solicitação da página. O navegador precisa recarregar uma solicitação de verificação da página para enviar novamente a solicitação de verificação da página, e um parâmetro de execução de script na solicitação de verificação da página recarregada é obtido pela execução de um script de página reextraído. Portanto, o invasor não pode atacar o servidor nesta forma de realização da presente invenção. Como tal, a segurança do servidor é melhorada nesta forma de realização da presente invenção.

[034] Uma forma de realização da presente invenção fornece outro método para prevenir que um servidor seja atacado. Como mostrado na Figura 2, o método inclui os passos abaixo.

[035] (201). Obtenção de uma URL da página em uma solicitação da página ao receber a solicitação da página enviada por um navegador.

[036] (202). Extração aleatoriamente de um script de página a partir de uma pluralidade de scripts de página que existam em uma biblioteca de scripts predeterminada e correspondam à URL da página.

[037] Lógica de aquisição de parâmetros de execução de script diferente é usada na pluralidade de scripts de página. Nesta forma de realização da presente invenção, antes do passo (202), o método inclui ainda a configuração de scripts de páginas correspondendo a cada URL da página na biblioteca de scripts predeterminada. A biblioteca de scripts predeterminada armazena uma pluralidade de scripts de página, correspondendo respectivamente a URLs das páginas diferentes. Uma lógica de aquisição de parâmetros de script diferente é usada em scripts de página correspondendo a cada URL da página. Nesta forma de realização da presente invenção, o script de página é utilizado para executar e carregar uma página solicitada pelo navegador e obter um parâmetro de execução de script a partir de um resultado de execução. Quando os scripts de página correspondendo à mesma URL da página são executados, diferentes parâmetros de execução de script são gerados a partir da execução de scripts de página diferentes.

[038] Vale a pena observar que, como a única diferença entre os scripts de página é que é usada uma lógica de aquisição de parâmetros de execução de script diferente, as páginas geradas pelo carregamento e execução dos scripts de página são as mesmas. A única diferença da execução dos scripts de página é que os parâmetros de execução de script

gerados são diferentes.

[039] (203). Enviar o script de página alocado dinamicamente e aleatoriamente para o navegador.

[040] Além disso, o navegador executa o script de página para obter um parâmetro de execução de script. Depois de carregar e executar o script de página, o navegador exibe uma página correspondente e obtém o parâmetro de execução de script. Os parâmetros de execução de script são alguns parâmetros adicionais na página e não afetam a página exibida.

[041] (204). Determinar se uma solicitação de verificação da página está expirada ao receber a solicitação de verificação da página enviada pelo navegador.

[042] Nesta forma de realização da presente invenção, o passo (204) inclui determinar se um tempo de solicitação da solicitação de verificação da página é posterior à soma de um período de tempo predeterminado e um tempo para o navegador executar o script de página; e se sim, determinar que a solicitação de verificação da página está expirada; ou, se não, determinar que a solicitação de verificação da página não está expirada. O período de tempo predeterminado é usado para limitar um tempo em que o navegador pode enviar a solicitação da página ao servidor, e o período de tempo predeterminado pode ser definido com base nos requisitos reais.

[043] Vale a pena observar que um invasor pode atacar o servidor simulando o comportamento do usuário comum e leva tempo para o invasor simular o comportamento do usuário comum. Por conseguinte, nesta forma de realização da presente invenção, sob a condição de que o usuário possa enviar uma solicitação ao servidor normalmente, quanto menor o período de tempo predeterminado, menos provável o invasor atacar o servidor.

[044] (205a). Se está expirada, enviar informações de prompt de erro indicando a expiração da página.

[045] (205b). Se não estiver expirada, verifique se um parâmetro de execução de script compreendido na solicitação de verificação da página é válido.

[046] O passo (205b) é paralelo ao passo (205a). Se a solicitação de verificação da página não estiver espirada, o servidor verificará se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido. Nesta forma de realização da presente invenção, a solicitação da página inclui ainda informação do identificador de script de página executado pelo navegador. A etapa (205b) inclui o seguinte: pesquisar na biblioteca de scripts predeterminada um script de página correspondendo à informação do identificador, em que a biblioteca de scripts predeterminada armazena ainda a informação do identificador correspondendo a cada script de página; e verificar, com base no script de página correspondendo à informação do identificador, se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido. O script de página executado pelo navegador é o script de página enviado pelo servidor para o navegador na etapa (203). Ao enviar o script de página para o navegador, o servidor também envia a informação do identificador correspondendo ao script de página para o navegador. Ao enviar a solicitação de verificação da página ao servidor, o navegador também envia a informação do identificador de script de página para o servidor. Em seguida, o servidor obtém um script de página correspondendo da biblioteca de scripts predeterminada com base na informação do identificador de script de página e verifica, com base no script de página obtido, se o parâmetro de execução de script está correto.

[047] Nesta forma de realização da presente invenção, a verificação, com base no script de página correspondendo à informação do identificador, se o parâmetro de execução de script compreendido na

solicitação de verificação da página é válido inclui a obtenção de um parâmetro de script local com base no script de página correspondendo ao identificador em formação; determinar se o parâmetro de script local é o mesmo que o parâmetro de execução de script compreendido na solicitação de verificação da página; e se sim, determinar que o parâmetro de execução de script é válido; ou, se não, determinar que o parâmetro de execução de script é inválido.

[048] (206b). Se inválido, rejeitar a solicitação da página.

[049] Nesta forma de realização da presente invenção, se o parâmetro de execução de script estiver inválido após a verificação, a solicitação da página será rejeitada. Depois, se o usuário ainda quiser executar uma operação na página, o usuário precisará atualizar a página. Atualizar a página é equivalente a enviar uma solicitação da página ao servidor. Depois de receber a solicitação, o servidor aloca dinamicamente e aleatoriamente um script de página correspondendo à solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página. Ou seja, após rejeitar a solicitação da página, se receber uma instrução de atualização do usuário, o servidor salta para a etapa (201) para executar a etapa (201) novamente e aleatoriamente extrai um script de página após realizar a etapa (201) novamente. Portanto, o invasor não pode atacar o servidor nesta forma de realização da presente invenção. Como tal, a segurança do servidor é melhorada nesta forma de realização da presente invenção.

[050] Nesta forma de realização da presente invenção, um cenário mostrado na Figura 5 pode ser aplicado, mas não está limitado a isto. O cenário inclui o seguinte: No passo (1) da Figura 5, o navegador primeiro envia a solicitação da página para o servidor. A solicitação da página inclui o URL da página. Depois de receber a solicitação da página, o servidor extrai aleatoriamente o script de página correspondendo à URL da página da

biblioteca de scripts predeterminada e, em seguida, envia o script de página ao navegador. Isto é, o servidor envia o script de página extraído aleatoriamente para o navegador usando o passo (2) na Figura 5. Após receber o script de página enviado pelo servidor, o navegador executa o script de página e obtém o parâmetro de execução de script obtido pela execução de script de página. Em seguida, o navegador envia a solicitação de verificação da página ao servidor. A solicitação de verificação da página inclui o parâmetro de execução de script. Ou seja, o navegador envia a solicitação de verificação da página para o servidor usando o passo (3) na Figura 5.

[051] Depois de receber a solicitação de verificação da página, o servidor primeiro determina se a hora da solicitação de verificação da página é posterior à soma do período de tempo predeterminado e da hora em que o navegador executará o script de página. O servidor verifica se o parâmetro de execução de script é válido, se a hora da solicitação de verificação da página for anterior à soma do período de tempo predeterminado e da hora em que o navegador executará o script de página. Se inválido, o servidor rejeita a solicitação da página. O parâmetro de execução de script na presente invenção é obtido executando o script de página que é correspondendo à URL da página e é extraído aleatoriamente da biblioteca de scripts predeterminada, e é utilizada uma lógica de aquisição de parâmetros de execução de script diferente nos scripts de página. Portanto, mesmo que um invasor obtenha lógica de script no código dinâmico, o invasor não poderá analisar o método de criptografia do parâmetro de execução de script dentro do período de tempo predeterminado. Além disso, quando a solicitação de verificação da página estiver espirada, o navegador precisará recarregar uma solicitação de verificação da página, e um parâmetro de execução de script na solicitação de verificação da página recarregada será obtido pela execução de um script de página reextraído correspondendo à URL da página. Portanto, o invasor não

pode atacar o servidor nesta forma de realização da presente invenção. Como tal, a segurança do servidor é melhorada nesta forma de realização da presente invenção.

[052] Em outro método para prevenir que um servidor seja atacado, fornecido nesta forma de realização da presente invenção, ao receber a solicitação de verificação da página enviada pelo navegador, o servidor primeiro determina se a solicitação de verificação da página está expirada. Se a solicitação de verificação da página não estiver espirada, o servidor verificará se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido. Se o parâmetro de execução de script estiver inválido, o servidor rejeitará a solicitação da página para prevenir que um servidor seja atacado. Atualmente, o servidor verifica um valor de token criptografado para determinar se uma solicitação de serviço enviada pelo navegador é válida para prevenir que um servidor seja atacado. Comparado com isso, na presente invenção, o servidor verifica o parâmetro de execução de script para evitar que o servidor seja atacado. O parâmetro de execução de script é obtido com base no script de página, alocado dinamicamente e aleatoriamente a partir da pluralidade de scripts de página correspondendo à solicitação da página, e é utilizada uma lógica de aquisição de parâmetros de execução de script diferente nos scripts de página. Portanto, mesmo que um invasor obtenha lógica de script no código dinâmico, o invasor não poderá analisar o método de criptografia do parâmetro de execução de script dentro do período de tempo predeterminado. Além disso, quando o tempo de solicitação da solicitação de verificação da página excede o período de tempo predeterminado, o servidor rejeita a solicitação da página. O navegador precisa recarregar uma solicitação de verificação da página para enviar novamente a solicitação de verificação da página, e um parâmetro de execução de script na solicitação de verificação da página recarregada é obtido pela execução de um

script de página reextraído. Portanto, o invasor não pode atacar o servidor nesta forma de realização da presente invenção. Como tal, a segurança do servidor é melhorada nesta forma de realização da presente invenção.

[053] Além disso, uma forma de realização da presente invenção fornece um dispositivo para prevenir que um servidor seja atacado. Como mostrado na Figura 3, o dispositivo inclui uma unidade de alocação (31), uma unidade de envio (32), uma unidade de determinação (33), uma unidade de saída (34), uma unidade de verificação (35) e uma unidade de rejeição (36).

[054] A unidade de alocação (31) é configurada para atribuir dinamicamente e aleatoriamente um script de página correspondendo a uma solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página, quando a solicitação da página enviado por um navegador é recebido.

[055] A unidade de envio (32) é configurada para enviar o script de página alocado dinamicamente e aleatoriamente para o navegador, para que o navegador execute o script de página para obter um parâmetro de execução de script.

[056] A unidade de determinação (33) é configurada para determinar se uma solicitação de verificação da página está expirada, quando a solicitação de verificação da página enviada pelo navegador é recebida.

[057] A unidade de saída (34) é configurada para fornecer informações de prompt de erro, indicando a expiração da página, se expirado.

[058] A unidade de verificação (35) é configurada para verificação se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido, se a solicitação de verificação da página não estiver expirada.

[059] A unidade de rejeição (36) é configurada para rejeitar a solicitação da página se o parâmetro de execução de script compreendido na

solicitação de verificação da página estiver inválido.

[060] Vale a pena notar que, para outras descrições correspondendo das unidades de função no dispositivo para prevenir que um servidor seja atacado nesta forma de realização da presente invenção, pode ser feita referência às descrições correspondendo do método mostrado na Figura 1. Detalhes são omitidos aqui para simplificar. No entanto, deve ficar claro que o dispositivo nesta forma de realização pode, de forma correspondendo, implementar todo o conteúdo na forma de realização do método.

[061] De acordo com o método e dispositivo para prevenir que um servidor seja atacado, fornecido nas formas de realização da presente invenção, ao receber a solicitação de verificação da página enviada pelo navegador, o servidor primeiro determina se a solicitação de verificação da página está expirada. Se a solicitação de verificação da página não estiver espirada, o servidor verificará se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido. Se o parâmetro de execução de script estiver inválido, o servidor rejeitará a solicitação da página para prevenir que um servidor seja atacado. Atualmente, o servidor verifica um valor de token criptografado para determinar se uma solicitação de serviço enviada pelo navegador é válida para prevenir que um servidor seja atacado. Comparado com isso, na presente invenção, o servidor verifica o parâmetro de execução de script para evitar que o servidor seja atacado. O parâmetro de execução de script é obtido com base no script de página, alocado dinamicamente e aleatoriamente a partir da pluralidade de scripts de página correspondendo à solicitação da página, e é utilizada uma lógica de aquisição de parâmetros de execução de script diferente nos scripts de página. Portanto, mesmo que um invasor obtenha lógica de script no código dinâmico, o invasor não poderá analisar o método de criptografia do parâmetro de

execução de script dentro de um período de tempo predeterminado. Além disso, quando um tempo de solicitação da solicitação de verificação da página excede o período de tempo predeterminado, o servidor rejeita a solicitação da página. O navegador precisa recarregar uma solicitação de verificação da página para enviar novamente a solicitação de verificação da página, e um parâmetro de execução de script na solicitação de verificação da página recarregada é obtido pela execução de um script de página reextraído. Portanto, o invasor não pode atacar o servidor nesta forma de realização da presente invenção. Como tal, a segurança do servidor é melhorada nesta forma de realização da presente invenção.

[062] Além disso, uma forma de realização da presente invenção fornece outro dispositivo para prevenir que um servidor seja atacado. Como mostrado na Figura 4, o dispositivo inclui uma unidade de alocação (41), uma unidade de envio (42), uma unidade de determinação (43), uma unidade de saída (44), uma unidade de verificação (45) e uma unidade de rejeição (46).

[063] A unidade de alocação (41) é configurada para alocar dinamicamente e aleatoriamente um script de página correspondendo a uma solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página, quando a solicitação da página enviada por um navegador é recebida.

[064] A unidade de envio (42) é configurada para enviar o script de página alocado dinamicamente e aleatoriamente para o navegador, para que o navegador execute o script de página para obter um parâmetro de execução de script.

[065] A unidade de determinação (43) está configurada para determinar se uma solicitação de verificação da página está expirada, quando a solicitação de verificação da página enviada pelo navegador é recebida.

[066] A unidade de saída (44) é configurada para fornecer

informações de prompt de erro, indicando a expiração da página, se a solicitação de verificação da página estiver espirada.

[067] A unidade de verificação (45) é configurada para verificação se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido, se a solicitação de verificação da página não estiver expirada.

[068] A unidade de rejeição (46) é configurada para rejeitar a solicitação da página se o parâmetro de execução de script compreendido na solicitação de verificação da página estiver inválido.

[069] Além disso, a unidade de alocação (41) inclui um módulo de obtenção (411), configurado para obtenção de uma URL da página na solicitação da página; e um módulo de extração (412), configurado para extrair aleatoriamente um script de página a partir de uma pluralidade de scripts de página que existem em uma biblioteca de scripts predeterminada e são correspondentes à URL da página, onde é usada uma lógica de aquisição de parâmetros de execução de script diferente na pluralidade de scripts de página.

[070] Além disso, a unidade de determinação (43) inclui um módulo de determinação (431), configurado para determinar se um tempo de solicitação da solicitação de verificação da página é posterior à soma de um período de tempo predeterminado e um tempo para o navegador executar o script de página; e um módulo de determinação (432), configurado para determinar que a solicitação de verificação da página está expirada, se o tempo de solicitação da solicitação de verificação da página for posterior à soma do período de tempo predeterminado e o tempo para o navegador executar o script de página; ou um módulo de determinação (432), configurado para determinar que a solicitação de verificação da página não está expirada, se o tempo de solicitação da solicitação de verificação da página não for posterior à soma do período de tempo predeterminado e o tempo para o navegador

executar o script de página.

[071] Nesta forma de realização da presente invenção, a solicitação da página inclui ainda informação do identificador de script de página executado pelo navegador, e a unidade de verificação (45) inclui um módulo de pesquisa (451), configurado para procurar na biblioteca de scripts predeterminada para um script de página correspondendo a informação de identificador, em que a biblioteca de scripts predeterminada armazena ainda informação do identificador correspondendo a cada script de página; e um módulo de verificação (452), configurado para verificar, com base no script de página correspondendo à informação do identificador, se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido.

[072] Nesta forma de realização da presente invenção, o módulo de verificação (452) é configurado para obter um parâmetro de script local com base no script de página correspondendo à informação do identificador.

[073] O módulo de verificação (452) é configurado para determinar se o parâmetro de script local é o mesmo que o parâmetro de execução de script compreendido na solicitação de verificação da página.

[074] O módulo de verificação (452) é configurado para determinar que o parâmetro de execução de script é válido, se o parâmetro de script local é o mesmo que o parâmetro de execução de script compreendido na solicitação de verificação da página.

[075] O módulo de verificação (452) é configurado para determinar que o parâmetro de execução de script é inválido, se o parâmetro de script local é diferente do parâmetro de execução de script compreendido na solicitação de verificação da página.

[076] O dispositivo inclui ainda uma unidade de configuração (47), configurada para configurar scripts de página correspondendo a cada

URL da página na biblioteca de scripts predeterminada.

[077] Vale a pena notar que, para outras descrições correspondendo das unidades de função em outro dispositivo para prevenir que um servidor seja atacado nesta forma de realização da presente invenção, pode ser feita referência às descrições correspondendo do método mostrado na Figura 2. Detalhes são omitidos aqui para simplificar. No entanto, deve ficar claro que o dispositivo nesta forma de realização pode, de forma correspondendo, implementar todo o conteúdo na forma de realização do método.

[078] De acordo com o método e dispositivo para prevenir que um servidor seja atacado, fornecido nas formas de realização da presente invenção, ao receber a solicitação de verificação da página enviada pelo navegador, o servidor primeiro determina se a solicitação de verificação da página está expirada. Se a solicitação de verificação da página não estiver espirada, o servidor verificará se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido. Se o parâmetro de execução de script estiver inválido, o servidor rejeitará a solicitação da página para prevenir que um servidor seja atacado. Atualmente, o servidor verifica um valor de token criptografado para determinar se uma solicitação de serviço enviada pelo navegador é válida para prevenir que um servidor seja atacado. Comparado com isso, na presente invenção, o servidor verifica o parâmetro de execução de script para evitar que o servidor seja atacado. O parâmetro de execução de script é obtido com base no script de página, alocado dinamicamente e aleatoriamente a partir da pluralidade de scripts de página correspondendo à solicitação da página, e é utilizada uma lógica de aquisição de parâmetros de execução de script diferente nos scripts de página. Portanto, mesmo que um invasor obtenha lógica de script no código dinâmico, o invasor não poderá analisar o método de criptografia do parâmetro de

execução de script dentro do período de tempo predeterminado. Além disso, quando o tempo de solicitação da solicitação de verificação da página excede o período de tempo predeterminado, o servidor rejeita a solicitação da página. O navegador precisa recarregar uma solicitação de verificação da página para enviar novamente a solicitação de verificação da página, e um parâmetro de execução de script na solicitação de verificação da página recarregada é obtido pela execução de um script de página reextraído. Portanto, o invasor não pode atacar o servidor nesta forma de realização da presente invenção. Como tal, a segurança do servidor é melhorada nesta forma de realização da presente invenção.

[079] O dispositivo para prevenir que um servidor seja atacado inclui um processador e uma memória. A unidade de alocação, a unidade de envio, a unidade de determinação, a unidade de saída, a unidade de verificação, a unidade de rejeição e a unidade de configuração são armazenadas na memória como unidades de programa. O processador executa as unidades de programa armazenadas na memória para implementar as funções correspondendo.

[080] O processador inclui o kernel, e o kernel invoca uma unidade de programa correspondendo da memória. Pode haver um ou mais kernels para melhorar a segurança do servidor ajustando um parâmetro do kernel.

[081] A memória pode incluir um armazenamento não persistente, uma memória de acesso aleatório (RAM) e/ ou uma memória não volátil em um meio legível por computador, por exemplo, uma memória somente leitura (ROM) ou uma memória flash (memória RAM flash). A memória inclui pelo menos um chip de armazenamento.

[082] A presente invenção proporciona ainda um produto de programa de computador e, quando executado em um aparelho de

processamento de dados, o produto aplicável para inicializar o código de programa que inclui os seguintes passos: quando receber uma solicitação da página enviado por um navegador, alocação dinamicamente e aleatoriamente do script de página correspondendo à solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página; enviar o script de página alocado dinamicamente e aleatoriamente para o navegador, para que o navegador execute o script de página para obter um parâmetro de execução de script; ao receber uma solicitação de verificação da página enviada pelo navegador, determinando se a solicitação de verificação da página está expirada; e, se estiver espirada, exibir informações de prompt de erro indicando a expiração da página; ou se não estiver expirada, verificar se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido; e se for inválido, rejeitar a solicitação da página.

[083] Um técnico no assunto deve entender que as formas de realização da presente invenção podem ser fornecidas como um método, um sistema ou um produto de programa de computador. Portanto, a presente invenção pode usar uma forma de formas de realização somente de hardware, formas de realização somente de software ou formas de realização com uma combinação de software e hardware. Além disso, a presente invenção pode usar uma forma de produto de programa de computador que é implementado em um ou mais meios de armazenamento utilizáveis por computador (incluindo, mas não limitado a um armazenamento em disco magnético, um CD-ROM, uma memória ótica, etc.) que incluem código de programa utilizável por computador.

[084] A presente invenção é descrita com referência aos fluxogramas e/ ou diagramas de blocos do método e dispositivo para prevenir que um servidor seja atacado e ao produto de programa de computador, de acordo com as formas de realização da presente invenção. Deve ser entendido

que as instruções de programa de computador podem ser usadas para implementar cada processo e/ ou cada bloco nos fluxogramas e/ ou diagramas de bloco e uma combinação de um processo e/ ou um bloco nos fluxogramas e/ ou nos diagramas de bloco. Estas instruções de programas de computador podem ser fornecidas para um computador de uso geral, um computador dedicado, um processador incorporado ou um processador de outro dispositivo de processamento de dados programável para gerar uma máquina, de modo que as instruções executadas pelo computador ou pelo processador da outra dispositivo de processamento de dados programável gera um aparelho para implementar uma função específica em um ou mais processos nos fluxogramas e/ ou em um ou mais blocos nos diagramas de bloco.

[085] Estas instruções de programas de computador podem ser armazenadas em uma memória legível por computador que pode instruir o computador ou outro dispositivo de processamento de dados programável a funcionar de um modo específico, para que as instruções armazenadas na memória legível por computador gerem um artefato que inclui um aparelho de instruo. O aparelho de instrução implementa uma função específica em um ou mais processos nos fluxogramas e/ ou em um ou mais blocos nos diagramas de bloco.

[086] Estas instruções de programas de computador podem ser carregadas no computador ou outro dispositivo de processamento de dados programável, de modo que uma série de operações e etapas sejam realizadas no computador ou no outro dispositivo programável, gerando assim processamento implementado por computador. Portanto, as instruções executadas no computador ou em outro dispositivo programável fornecem etapas para implementar uma função específica em um ou mais processos nos fluxogramas e/ ou em um ou mais blocos nos diagramas de bloco.

[087] Em uma configuração típica, um dispositivo de computação

inclui um ou mais processadores (CPU), uma interface de entrada/ saída, uma interface de rede e uma memória.

[088] A memória pode incluir um armazenamento não persistente, uma memória de acesso aleatório (RAM) e/ ou uma memória não volátil em um meio legível por computador, por exemplo, uma memória somente leitura (ROM) ou uma memória flash (memória RAM flash). A memória é um exemplo do meio legível por computador.

[089] O meio legível por computador inclui mídia persistente, não persistente, móvel e imóvel que pode armazenar informações usando qualquer método ou tecnologia. A informação pode ser uma instrução legível por computador, uma estrutura de dados, um módulo de programa ou outros dados. Um meio de armazenamento de computador inclui, mas não se limita a memória de acesso aleatório de mudança de fase (PRAM), memória de acesso aleatório estática (SRAM), memória de acesso aleatório dinâmica (DRAM), outro tipo de memória de acesso aleatório (RAM), Memória só de leitura (ROM), uma memória só de leitura programável e apagável eletricamente (EEPROM), uma memória flash ou outra tecnologia de memória, uma memória de leitura em disco compacto (CD-ROM), um disco versátil digital (DVD) ou outro armazenamento óptico, uma cassete magnética, uma fita magnética, um armazenamento em disco magnético, outro dispositivo de armazenamento magnético ou qualquer outro meio não transitório. O meio de armazenamento do computador pode ser usado para armazenar informações acessíveis pelo dispositivo de computação. Com base na definição da presente especificação, o meio legível por computador não inclui meios transitórios legíveis por computador (meios transitórios), por exemplo, um sinal de dados modulado e portadora.

[090] As descrições anteriores são apenas formas de realização da presente invenção e não se destinam a limitar a presente invenção. Um

técnico no assunto pode fazer várias modificações e variações para a presente invenção. Quaisquer modificações, substituições equivalentes ou melhorias feitas sem afastamento do escopo da presente invenção caberá no escopo das reivindicações da presente invenção.

REIVINDICAÇÕES

1. MÉTODO PARA PREVENIR QUE UM SERVIDOR SEJA ATACADO, caracterizado por compreender:

- alocar (101) dinamicamente e aleatoriamente um script de página correspondendo a uma solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página, ao receber a solicitação da página enviada por um navegador;

- enviar (102) o script de página alocado dinamicamente e aleatoriamente para o navegador, para que o navegador execute o script de página para obter um parâmetro de execução de script;

- determinar (103) se uma solicitação de verificação da página está expirada, ao receber a solicitação de verificação da página enviada pelo navegador; e

- se a solicitação de verificação da página está expirada, gerar (104a) informações de prompt de erro indicando a expiração da página; ou

- se a solicitação de verificação da página não estiver espirada, verificar (104b) se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido; e

- se o parâmetro de execução de script for inválido (105), rejeitar a solicitação da página.

2. MÉTODO, de acordo com a reivindicação 1, caracterizado por alocar (101) dinamicamente e aleatoriamente um script de página correspondendo à solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página compreende:

- obtenção (201) de uma URL da página na solicitação da página; e

- extrair (202) aleatoriamente um script de página a partir de

uma pluralidade de scripts de página que existem em uma biblioteca de scripts predeterminada e são correspondentes à URL da página, em que é usada uma lógica de aquisição de parâmetros de execução de script diferente na pluralidade de scripts de página.

3. MÉTODO, de acordo com a reivindicação 1, caracterizado por determinar (204) se uma solicitação de verificação da página está expirada compreende:

- determinar se um tempo de solicitação da solicitação de verificação da página é posterior à soma de um período de tempo predeterminado e um tempo para o navegador executar o script de página; e

- se o resultado for sim, determinar que a solicitação de verificação da página está expirada; ou

- se o resultado for não, determinar que a solicitação de verificação da página não está expirada.

4. MÉTODO, de acordo com qualquer uma das reivindicações 1 a 3, caracterizado pela solicitação da página compreender ainda informação do identificador de script de página executada pelo navegador, e a verificação (205b) se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido compreende:

- pesquisar a biblioteca de scripts predeterminada para um script de página correspondendo à informação do identificador, em que a biblioteca de scripts predeterminada armazena ainda informação do identificador correspondendo a cada script de página da pluralidade de scripts de página correspondendo à URL da página; e

- verificar, com base no script de página correspondendo à informação do identificador, se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido.

5. MÉTODO, de acordo com a reivindicação 4, caracterizado

pela verificação (205b), com base no script de página correspondendo à informação do identificador, se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido compreende:

- obter um parâmetro de script local com base no script de página correspondendo à informação do identificador;
- determinar se o parâmetro de script local é o mesmo que o parâmetro de execução de script compreendido na solicitação de verificação da página; e
- se o resultado for sim, determinar que o parâmetro de execução de script é válido; ou
- se o resultado for não, determinar que o parâmetro de execução de script é inválido.

6. MÉTODO, de acordo com a reivindicação 2, caracterizado por ainda compreender: antes de extrair aleatoriamente um script de página a partir de uma pluralidade de scripts de página que existem em uma biblioteca de scripts predeterminada e são correspondentes à URL da página, o método compreender ainda:

- configurar um script de página correspondendo a cada URL da página na biblioteca de scripts predeterminada e informação do identificador correspondendo aos scripts de página.

7. DISPOSITIVO PARA PREVENIR QUE UM SERVIDOR SEJA ATACADO, caracterizado por compreender:

- uma unidade de alocação (31), configurada para: alocar (101) dinamicamente e aleatoriamente um script de página correspondendo a uma solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página, quando a solicitação da página enviada por um navegador é recebida;
- uma unidade de envio (32), configurada para enviar (102) o

script de página alocado dinamicamente e aleatoriamente para o navegador, para que o navegador execute o script de página para obter um parâmetro de execução de script;

- uma unidade de determinação (33), configurada para determinar (103) se uma solicitação de verificação da página está expirada, quando a solicitação de verificação da página enviada pelo navegador é recebida;

- uma unidade de saída (34), configurada para fornecer (104a) informações de prompt de erro indicando a expiração da página, se a solicitação de verificação da página estiver espirada;

- uma unidade de verificação (35), configurada para verificação (104b) se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido, se a solicitação de verificação da página não estiver expirada; e

- uma unidade de rejeição (36), configurada para rejeitar (105b) a solicitação da página, se o parâmetro de execução de script compreendido na solicitação de verificação da página estiver inválido.

8. DISPOSITIVO, de acordo com a reivindicação 7, caracterizado pela unidade de alocação (31, 41) compreender:

- um módulo de obtenção (411), configurado para obtenção (201) de uma URL da página na solicitação da página; e

- um módulo de extração (412), configurado para extrair (202) aleatoriamente um script de página a partir de uma pluralidade de scripts de página que existem em uma biblioteca de scripts predeterminada e são correspondentes à URL da página, em que é usada uma lógica de aquisição de parâmetros de execução de script diferente na pluralidade de scripts de página.

9. DISPOSITIVO, de acordo com a reivindicação 7, caracterizado pela unidade de determinação (33, 43) compreender:

- um módulo de determinação (431), configurado para determinar se um tempo de solicitação da solicitação de verificação da página é posterior à soma de um período de tempo predeterminado e um tempo para o navegador executar o script de página; e

- um módulo de determinação (432), configurado para determinar (204) que a solicitação de verificação da página está expirada, se o tempo de solicitação da solicitação de verificação da página for posterior à soma do período de tempo predeterminado e o tempo para o navegador executar o script de página; ou

- um módulo de determinação (432), configurado para determinar (204) que a solicitação de verificação da página não está expirada, se o tempo de solicitação da solicitação de verificação da página não for posterior à soma do período de tempo predeterminado e o tempo para o navegador executar o script de página.

10. DISPOSITIVO, de acordo com qualquer uma das reivindicações 7 a 9, caracterizado pela solicitação da página compreender ainda informação do identificador de script de página executada pelo navegador, e a unidade de verificação (35, 45) compreender:

- um módulo de pesquisa (451), configurado para pesquisar a biblioteca de scripts predeterminada para um script de página correspondendo à informação do identificador, em que a biblioteca de scripts predeterminada armazena ainda a informação do identificador correspondendo a cada script de página da pluralidade de scripts de página correspondendo à URL da página; e

- um módulo de verificação (452), configurado para verificar, com base no script de página correspondendo à informação do identificador, se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido.

11. DISPOSITIVO, de acordo com a reivindicação 10, caracterizado por:

- o módulo de verificação (35, 45) ser configurado para obter um parâmetro de script local com base no script de página correspondendo à informação do identificador;

- o módulo de verificação (35, 45) ser configurado para determinar se o parâmetro de script local é o mesmo que o parâmetro de execução de script compreendido na solicitação de verificação da página; e

- o módulo de verificação (35, 45) ser configurado para determinar se o parâmetro de execução de script é válido, se o parâmetro de script local é o mesmo que o parâmetro de execução de script compreendido na solicitação de verificação da página; ou

- o módulo de verificação (35, 45) ser configurado para determinar se o parâmetro de execução de script é inválido, se o parâmetro de script local é diferente do parâmetro de execução de script compreendido na solicitação de verificação da página.

12. DISPOSITIVO, de acordo com a reivindicação 8, caracterizado pelo dispositivo compreender ainda:

- uma unidade de configuração (47), configurada para configurar scripts de página correspondendo a cada URL da página na biblioteca de scripts predeterminada e informação do identificador correspondendo aos scripts de página.

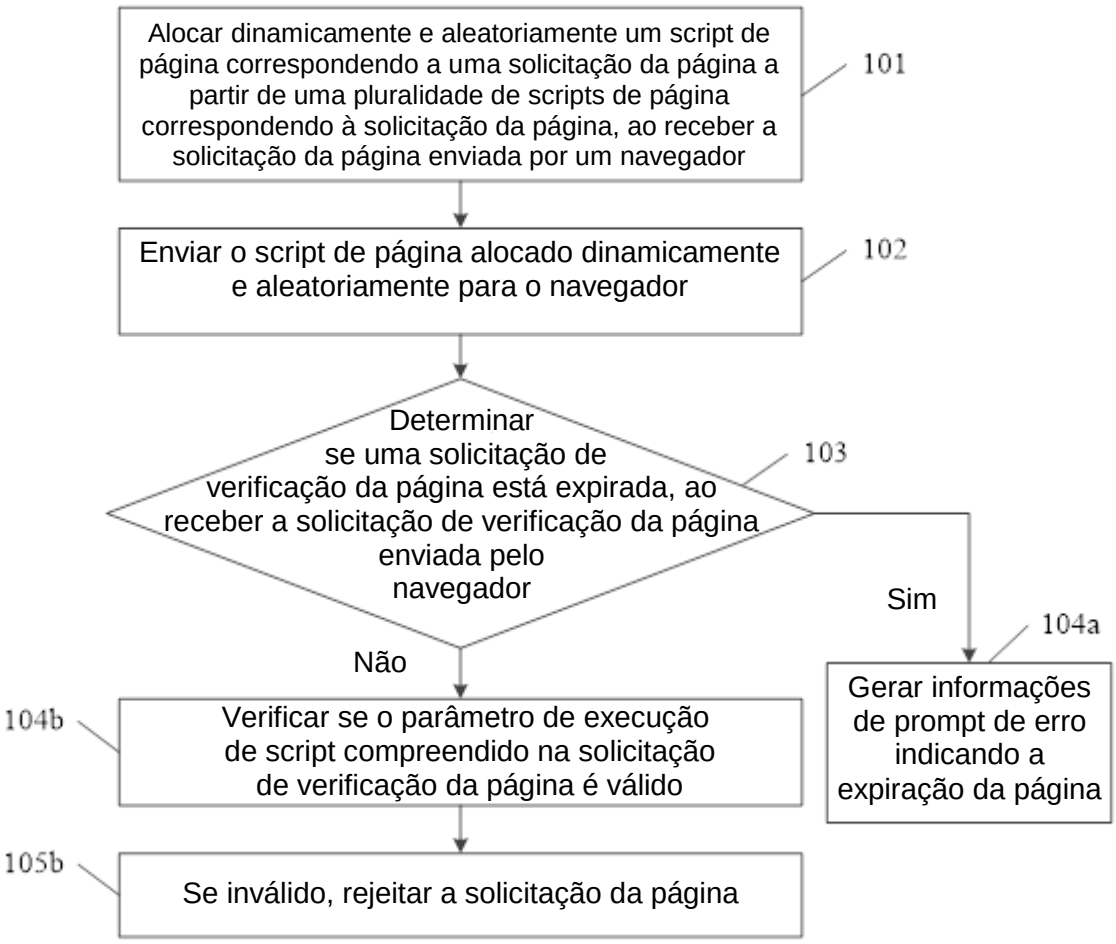
Alocar dinamicamente e aleatoriamente um script de página correspondendo a uma solicitação da página a partir de uma pluralidade de scripts de página correspondendo à solicitação da página, ao receber a solicitação da página enviada por um navegador
101
Enviar o script de página alocado dinamicamente e aleatoriamente para o navegador
102
Determinar se uma solicitação de verificação da página está expirada, ao receber a solicitação de verificação da página enviada pelo navegador
103
Sim
104a
Gerar informações de prompt de erro indicando a expiração da página
Não
104b
Verificar se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido
105b
Se inválido, rejeitar a solicitação da página

Figura 1

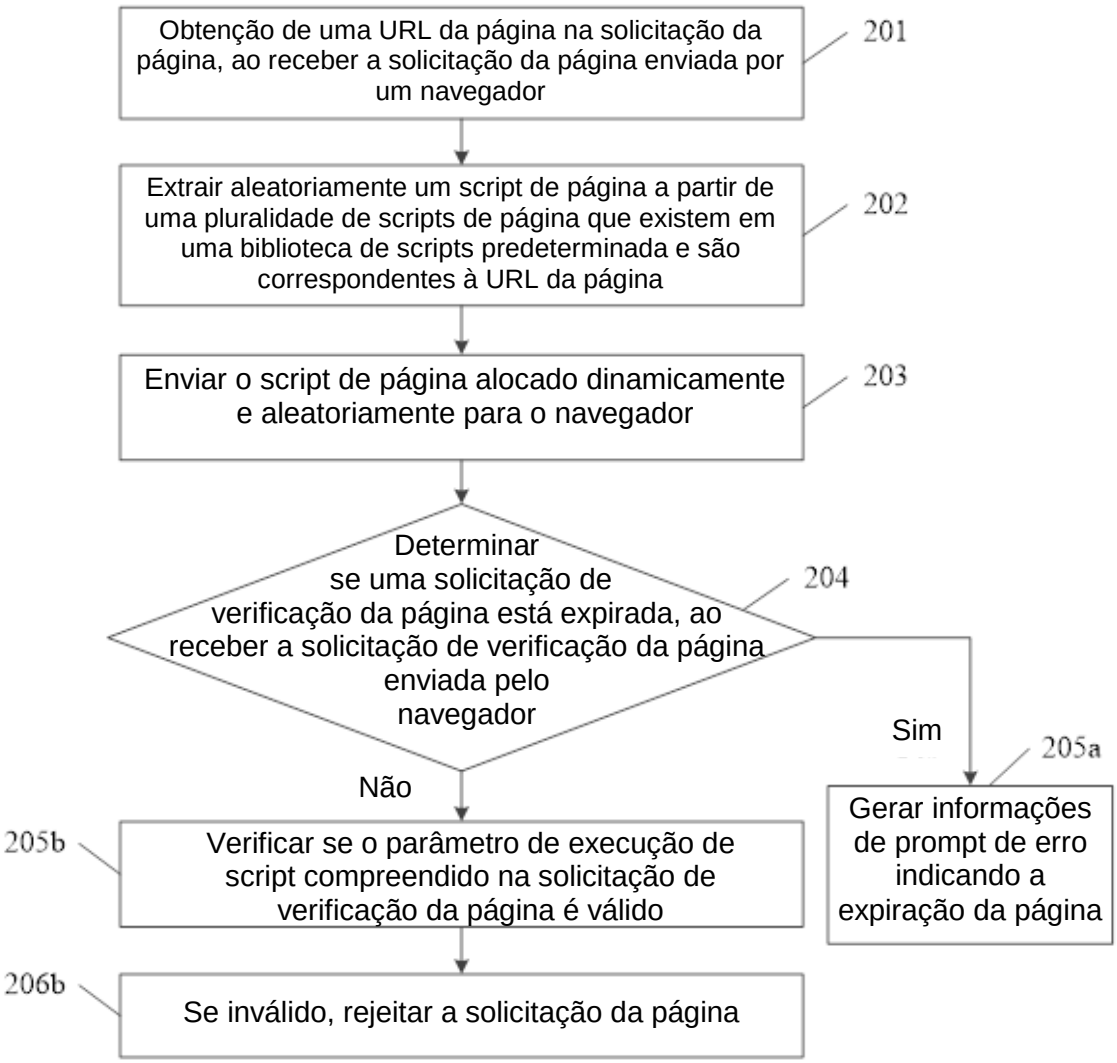
Obtenção de uma URL da página na solicitação da página, ao receber a solicitação da página enviada por um navegador
201
Extrair aleatoriamente um script de página a partir de uma pluralidade de scripts de página que existem em uma biblioteca de scripts predeterminada e são correspondentes à URL da página
202
Enviar o script de página alocado dinamicamente e aleatoriamente para o navegador
203
Determinar se uma solicitação de verificação da página está expirada, ao receber a solicitação de verificação da página enviada pelo navegador
204
Sim
205a
Gerar informações de prompt de erro indicando a expiração da página
Não
205b
Verificar se o parâmetro de execução de script compreendido na solicitação de verificação da página é válido
206b
Se inválido, rejeitar a solicitação da página

Figura 2

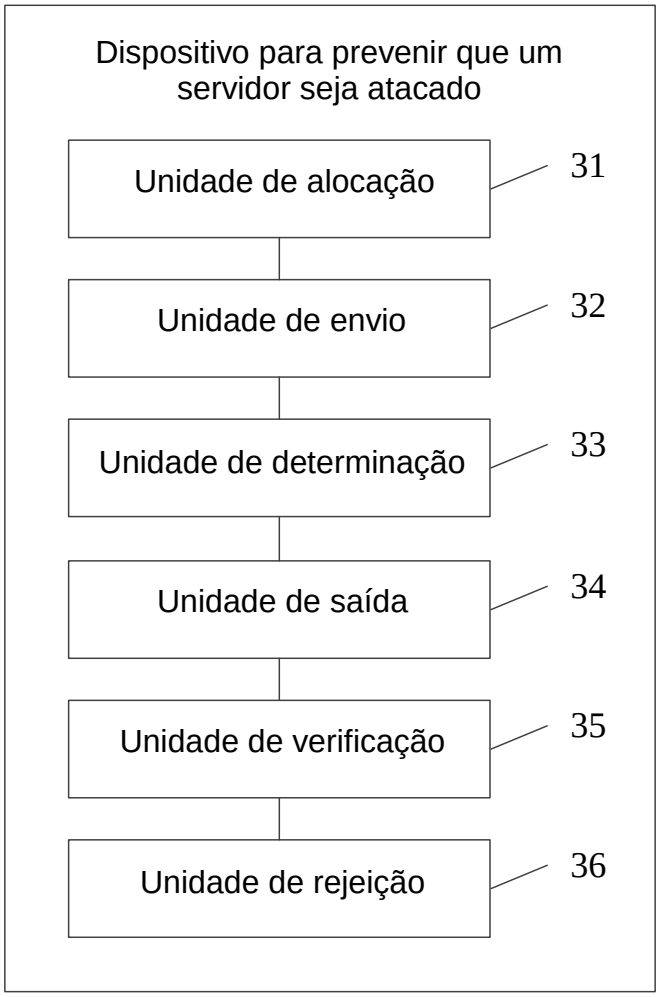
Dispositivo para prevenir que um servidor seja atacado
Unidade de alocação
31
Unidade de envio
32
Unidade de determinação
33
Unidade de saída
34
Unidade de verificação
35
Unidade de rejeição
36

Figura 3

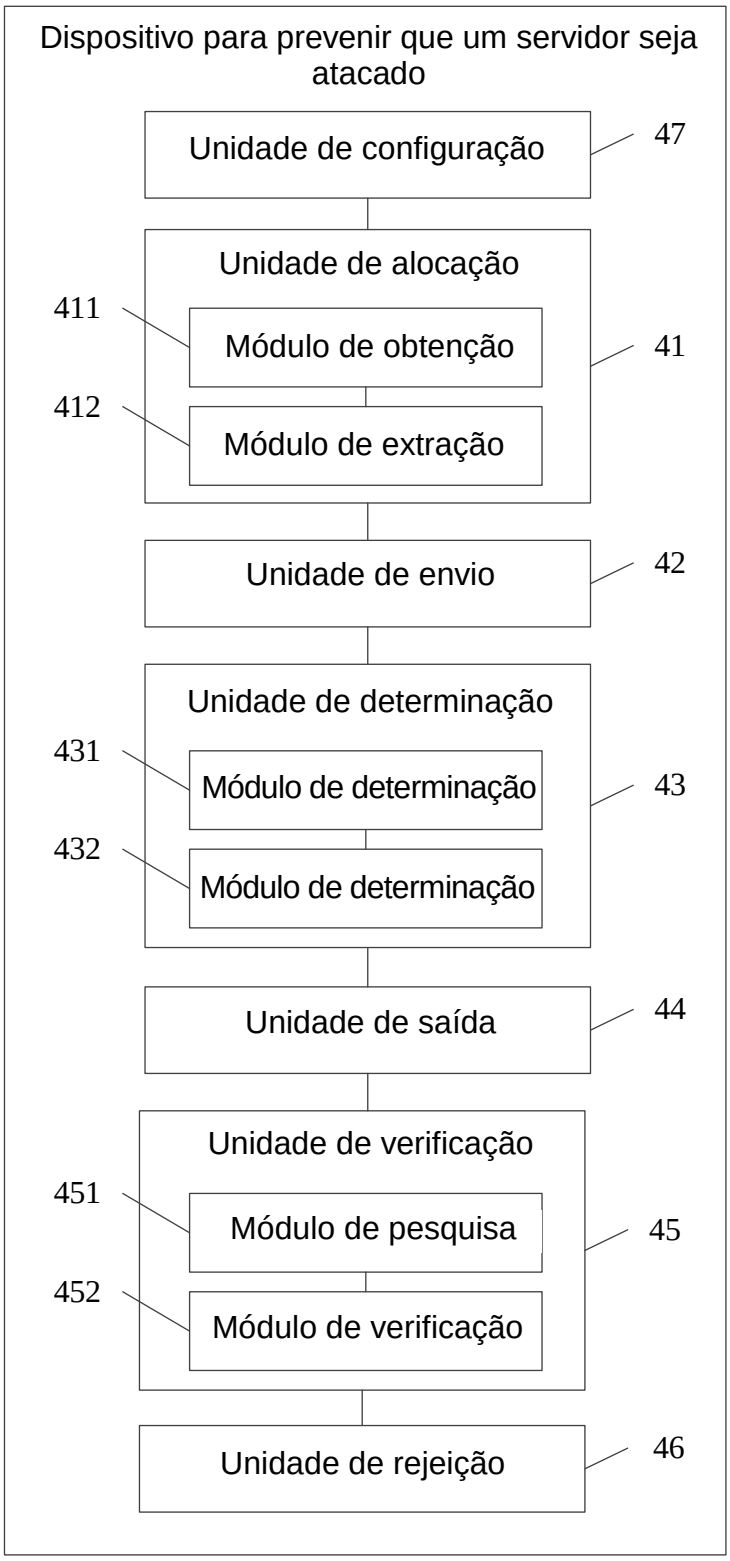
Dispositivo para prevenir que um servidor seja atacado
Unidade de configuração
47
Unidade de alocação
411
Módulo de obtenção
41
412
Módulo de extração
Unidade de envio
42
Unidade de determinação
431
Módulo de determinação
43
432
Módulo de determinação
Unidade de saída
44
Unidade de verificação
451
Módulo de pesquisa
45
452
Módulo de verificação
Unidade de rejeição
46

Figura 4

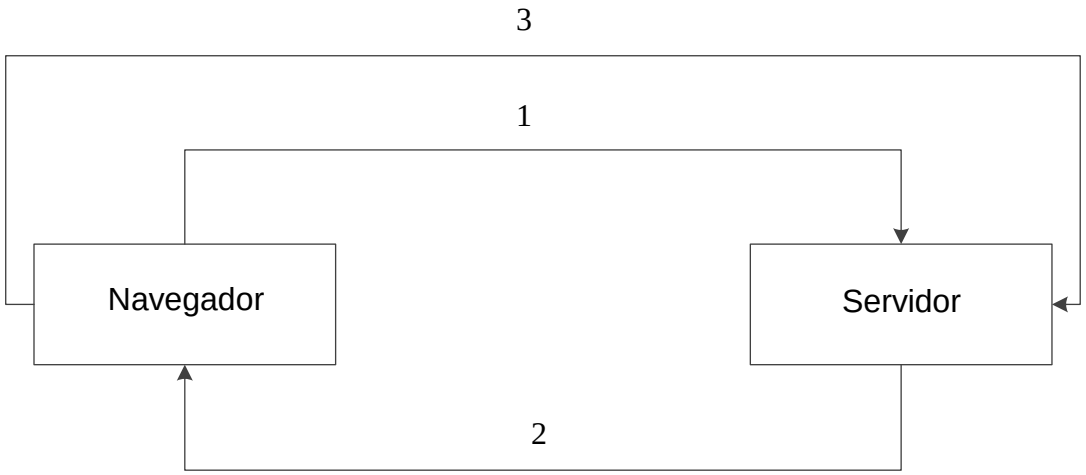

Figura 5