
Newton
Quem se prepara, não para.

Arquitetura de Aplicações Web

5º período

Professora: Michelle Hanne

Sumário

- Confidencialidade e Integridade
- Vulnerabilidades mais exploradas na Web
- JSON WEB TOKEN (JWT)
- Autenticação e Autorização

Confidencialidade e Integridade

Conforme descrição feita pela norma ISO/IEC 17799, a proteção da informação é vital, sendo caracterizada pela trilogia CID, ou seja, Confidencialidade, Integridade e Disponibilidade.

Fonte: Fernandes, 2014.

Confidencialidade e Integridade

Newton
Quem se prepara, não para.

Confidencialidade

- Garante que somente pessoas autorizadas poderão acessar as informações.
- Trata-se da não permissão da divulgação de uma informação sem prévia autorização.

Disponibilidade

- Garante acesso a uma informação no momento desejado. Isso implica no perfeito funcionamento da rede e do sistema. Imagine você necessitando de umas informações para concluir um relatório e o sistema não está funcionando!

Integridade

- Garante que a exatidão e completeza das informações não sejam alteradas ou violadas. Um exemplo, vamos supor que um gerente de uma empresa determina aumento de salário de 2% aos funcionários, para isso, utilizou seu e-mail para o departamento financeiro. Alguém interceptou e alterou de 2% para 20% o aumento!!!

Fonte: Fernandes, 2014.

Vulnerabilidades

Ataque, *Exploit* e Código Malicioso

Ataque – qualquer tentativa, bem ou mal sucedida, de acesso ou uso não autorizado de um serviço, computador ou rede.

Exploit – programa ou parte de um programa malicioso projetado para explorar uma vulnerabilidade existente em um programa de computador.

Código Malicioso – termo genérico usado para se referir a programas desenvolvidos para executar ações danosas e atividades maliciosas em um computador ou dispositivo móvel.

- Tipos específicos são: vírus, *worm*, *bot*, *spyware*, *backdoor*, cavalo de troia e *rootkit*.

Fonte: https://www.cert.br/docs/palestras/certbr-egi2014.pdf

Vulnerabilidades

Tipos de Ataque

Engenharia social – técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações.

Varredura em redes (*scan*) – consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados.

Negação de serviço distribuída (DDoS) – atividade maliciosa, coordenada e distribuída, pela qual um conjunto de computadores e/ou dispositivos móveis é utilizado para tirar de operação um serviço, um computador ou uma rede conectada à Internet.

Força bruta – consiste em adivinhar, por tentativa e erro, um nome de usuário e senha de um serviço ou sistema.

Invasão ou comprometimento – ataque bem sucedido que resulte no acesso, manipulação ou destruição de informações em um computador.

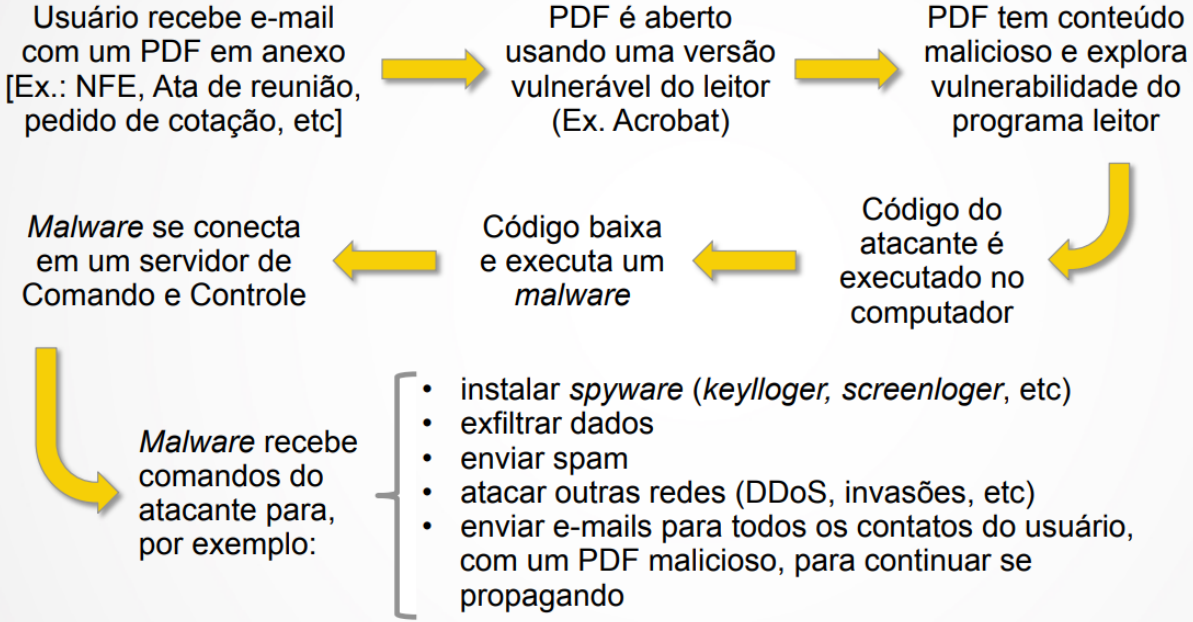
Desfiguração de página (*Defacement*) – consiste em alterar o conteúdo da página *Web* de um *site*.

Escuta de tráfego – consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos.

Fonte: https://www.cert.br/docs/palestras/certbr-egi2014.pdf

Vulnerabilidades

Cenário:
Ataque Contra Usuários de Internet

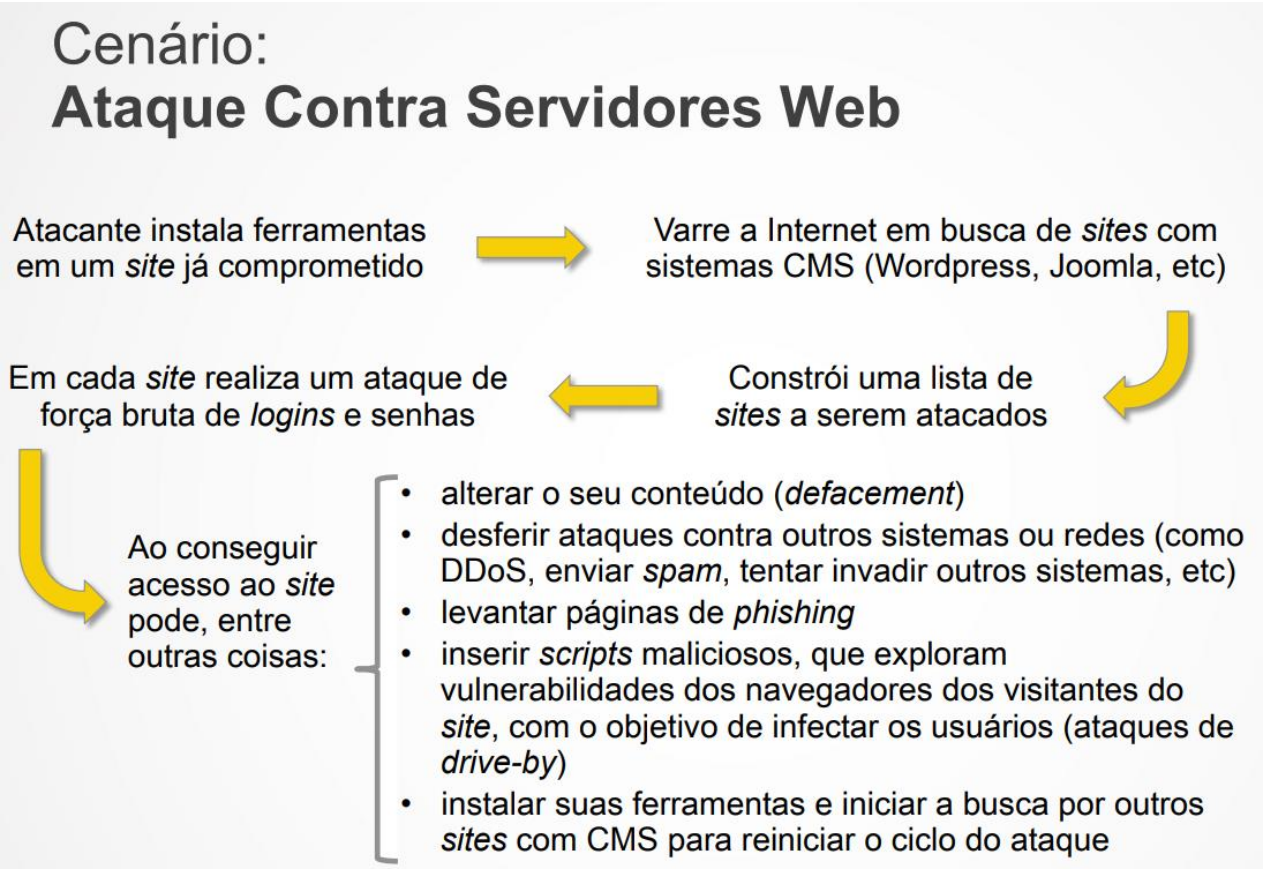


Fonte: https://www.cert.br/docs/palestras/certbr-egi2014.pdf

Vulnerabilidades

Newton
Quem se prepara, não para.

Cenário:
Ataque Contra Servidores Web



Fonte: https://www.cert.br/docs/palestras/certbr-egi2014.pdf

Vulnerabilidades

Vulnerabilidades

JSON WEB TOKEN (JWT)

Newton
Quem se prepara, não para.

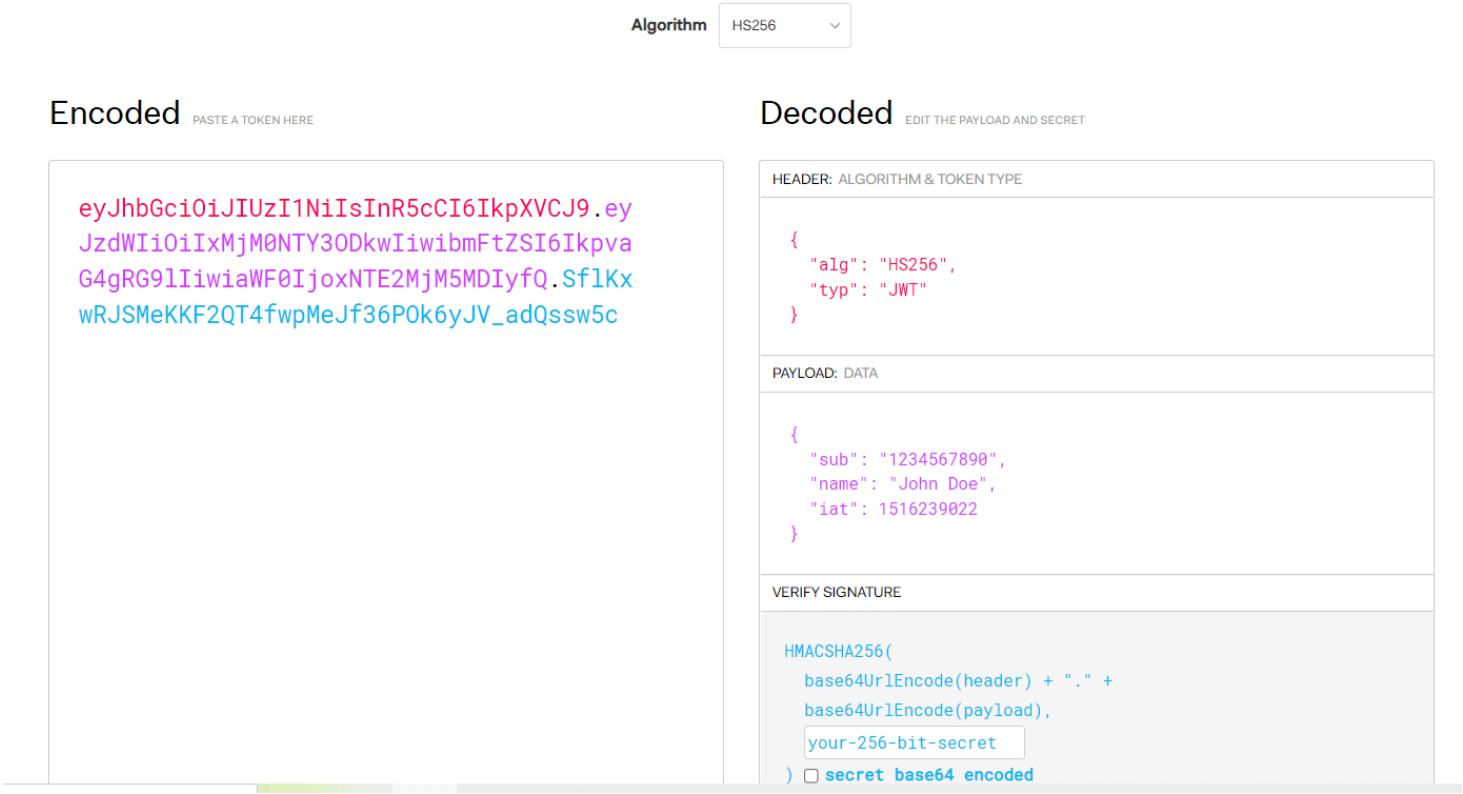
O JSON Web Token (JWT) é um padrão aberto (RFC 7519), que tem por objetivo definir um modo compacto e independente, que pode ser enviado dentro de um cabeçalho HTTP e conter as informações do usuário, para a transmissão segura de informações entre cliente e servidor, através de um objeto JSON.

Várias bibliotecas que implementam o padrão JWT estão disponíveis para as mais variadas linguagens de programação, dentre elas: .NET, Python, NodeJs, Java, JavaScript, Perl, Ruby e PHP

Fonte: Montanheiro, 2017

JSON WEB TOKEN (JWT)

Newton
Quem se prepara, não para.



Fonte: https://jwt.io/#debugger-io

JSON WEB TOKEN (JWT)

Newton
Quem se prepara, não para.

As bibliotecas podem ser usadas tanto para autenticação de usuários, que é o cenário mais comum, **sendo que a cada solicitação de uma rota, serviço ou recurso o usuário envia junto o token**, permitindo seu acesso ou não com base nesse token, quanto para transmitir informações de forma segura, uma vez que com base em sua **assinatura criptografada é possível verificar se o conteúdo não foi adulterado.**

Fonte: Montanheiro, 2017

JSON WEB TOKEN (JWT)

Newton
Quem se prepara, não para.

Um token gerado pela aplicação tem **sua estrutura divida em três partes, cada parte é separada por um ponto final (“.”)** e contém informações de diferentes tipos. A primeira parte é identificada como **header**, que é o **cabeçalho do token e contém informações a respeito da criptografia** usada para assinar o token.

{"alg": "HS256" XIII Encontro Anual de Computação - EnAComp 2017 - UFG 188 3. }

Fonte: Montanheiro, 2017

JSON WEB TOKEN (JWT)

Newton
Quem se prepara, não para.

A segunda parte é conhecida como **payload**, que é a parte onde ficam as informações no token, geralmente **informações do usuário que aquele token pertence e a sua validade**.
No token gerado as informações encontradas foram a **“iat”, que é o momento em que foi gerado, contado em segundos desde às 00:00 de 01/01/1970**. A informação de **“sub” que define do subject do token**, isso é, o número de identificação do sujeito para quem o token pertence. Já a informação de **“iss” é o issue**r que foi definido para identificar o nível de acesso daquele usuário à aplicação. A última informação encontrada nessa parte é a **“exp”** que define o tempo de expiração do token, usando a contagem de tempo da mesma maneira que o anterior.

Quadro 4. *Payload* do *Token* em JSON

```
{
  "iat": 1491609751,
  "sub": "2",
  "iss": "client",
  "exp": 1491717751
}
```

Quadro 5. *Payload* do *Token* em *base64*

```
eyJpYXQiOjE0OTE2MDk3NTEsInN1YiI6IjIiLCJpc3MiOiJjbGllbnQiLCJleHA
iOjE0OTE3MTc3NTF9
```

Fonte: Montanheiro, 2017

JSON WEB TOKEN (JWT)

Newton
Quem se prepara, não para.

A terceira e última parte do token **é a signature** que guarda uma assinatura criptografada com base no algoritmo especificado no cabeçalho. Para criar a assinatura, **o algoritmo usa como base os dados das duas primeiras partes do token**, que são os dados do tipo da criptografia, **os dados de payload**, e uma chave definida ao gerar o token. Essa chave em especial é definida em texto puro e o algoritmo a converte para **base64**, o resultado da assinatura em binário também é convertido para base64

Quadro 6. Assinatura do *Token* criptografado em SHA256 e transformado em *base64*

VnEwyZdBzekCIycPoezPp_Hzi0sD4BmM_KOFnMyMhBo

Fonte: Montanheiro, 2017

Autenticação Usando JWT Web Token

A autenticação do usuário se dará por meio de um **envio de uma requisição HTTP**, do tipo **POST**, ao **servidor de aplicação**, o qual no corpo **da requisição enviará o usuário e senha para login**. Os dados serão **validados pelo banco de dados** e se coincidirem será gerado um **token** para aquele **usuário**. Esse **token** será enviado de **volta para o usuário**, o qual pode armazená-lo em **cookies** ou no armazenamento de sessão do dispositivo.

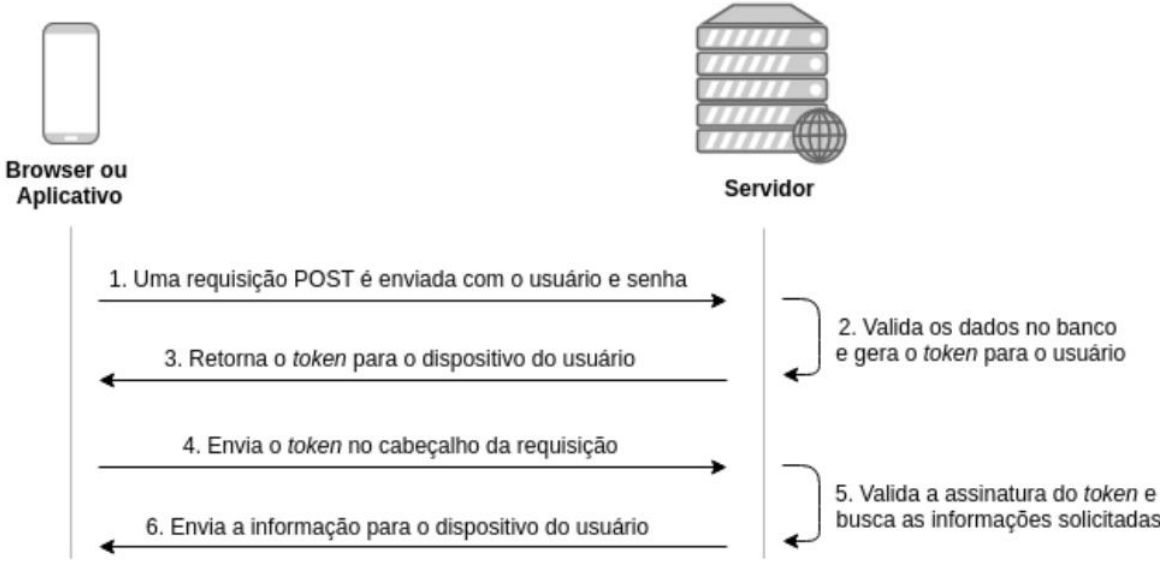


Figura 1. Diagrama de autenticação e validação de *token*

Fonte: Montanheiro, 2017

Autenticação e Autorização

Newton
Quem se prepara, não para.

É possível implementar o **JSON Web Token em uma aplicação através do serviço chamado Auth0**, que implementa o JWT em seu código e libera à seus clientes uma API na qual o cliente se cadastra por meio do serviço, podendo inclusive usar contas de terceiros como Google, Facebook e Twitter, e é enviado para a aplicação apenas as informações do usuário, uma vez que a senha e outros dados são guardados com segurança pelo Auth0.

O serviço é utilizado por grandes empresas, como Nvidia, AMD, Mozilla, Dow Jones, entre outras [Auth0 2017]

Fonte: Montanheiro, 2017

Referências

- FERNANDES, Nélia O. Campo. Segurança da Informação, rede e-Tec Brasil, 2014. Disponível em: <http://proedu.rnp.br/bitstream/handle/123456789/1538/15.6_versao_Finalizada_com_Logo_IFRO-Seguranca_Informacao_04_04_14.pdf?sequence=1&isAllowed=y> . Acesso em: 15 mar. 2022.
- MONTANHEIRO, Lucas Souza, Carvalho, Ana Maria Martins, RODRIGUES, Jackson Alves. Utilização de JSON Web Token na Autenticação de Usuários em APIs REST, XIII Encontro Anual de Computação - EnAComp 2017 – UFG. Disponível em: <https://www.enacomp.com.br/2017/docs/json_web_token_api_rest.pdf>. Acesso em: 15 mar. 2022.