6

HACKERS DO BEM_

Módulo 06

Proteção Web e Desenvolvimento Seguro

Aula 01

Ataques e Proteção Web – Parte 1_

Softex SENAI RNP MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO

Introdução

Nesta aula, você conhecerá os seguintes assuntos:

- Os ataques API Attacks e Replay Attacks, sua identificação e prevenção;
- Os ataques Session Hijacking e Clickjacking, sua identificação e prevenção;
- Os ataques Cross-Site Request Forger e SSL Strip, sua identificação e prevenção;
- Análise de URLs suspeitas.

Aula 01

Ataques e Proteção Web – Parte 1

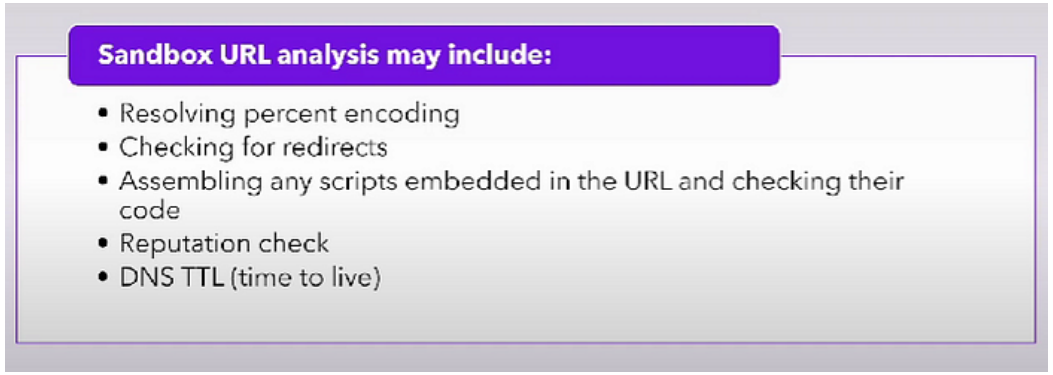
Análise de URL (Uniform Resource Locators)

ESTRUTURA DA URL

- URLs são endereços precisos de recursos web passados para o navegador.
- Componentes:

1. Esquema (Scheme);
2. Domínio (Host);
3. Porta (Port);
4. Caminho (Path);
5. Query String;
6. Âncora (Fragment).

Fonte: Iraqi Academic Scientific Journals.
Disponível em: <https://www.iasj.net/iasj/download/38d686435bc620a5>.
Acesso em: 20 mar. 2024.



Fonte: Medium, 2023.
Disponível em: <https://medium.com/@kumarishefu.4507/malware-analysis-episode-4-phishing-url-attachment-analysis-2af651cb88bf>.
Acesso em: 20 mar. 2024.

IDENTIFICAÇÃO DE URLS MALICIOSAS

Técnicas de Identificação:

1. Verificação do Domínio (Nome do Host);
2. Protocolo Seguro (HTTPS);
3. Examine a Estrutura Geral;
4. Verificação de Ortografia;
5. Evite URLs Encurtadas;
6. Use um Antivírus e Anti-Malware;
7. Reputação de Domínio;
8. Verificação de E-mails e Mensagens.

Aula 6.1

Ataques e Proteção Web – Parte 1

HTTP Percent Encoding (Codificação Percentual no HTTP)

REPRESENTAÇÃO DO HTTP PERCENT ENCODING

- Trata-se de uma técnica para representar caracteres especiais e caracteres não imprimíveis em URLs, parâmetros de consulta (query string) e cabeçalhos.

- Técnicas de representação:

1. Caracteres Reservados;
2. Caracteres Não Imprimíveis;
3. Caracteres Não Seguros.

Character	URL Encoded
;	%3B
?	%3F
/	%2F
:	%3A
#	%23
&	%26
=	%3D
+	%2B
$	%24
,	%2C
<space>	%20 or +
%	%25
<	%3C
>	%3E
~	%7E
%	%25

Fonte: Ambilgratis, 2011.
Disponível em: <https://ambilgratis.com/tag/url-encoding/>.
Acesso em: 20 mar. 2024.

Fonte: Circuits 4 you, 2019.
Disponível em: <https://circuits4you.com/2019/03/21/esp8266-url-encode-decode-example/#google_vignette>.
Acesso em: 20 mar. 2024.

COMO FUNCIONA O HTTP PERCENT ENCODING

- Consiste em substituir um caractere problemático por um "%" seguido por dois dígitos hexadecimais cujo valor é o byte do caractere na tabela ASCII.
- Por exemplo:

1. O espaço em branco é codificado como "%20".
2. O caractere "/" é substituído por "%2F”.

IDENTIFICAÇÃO DE PERCENT ENCODING EM URLS MALICIOSAS

- Técnicas e ferramentas que podem ajudar na detecção:

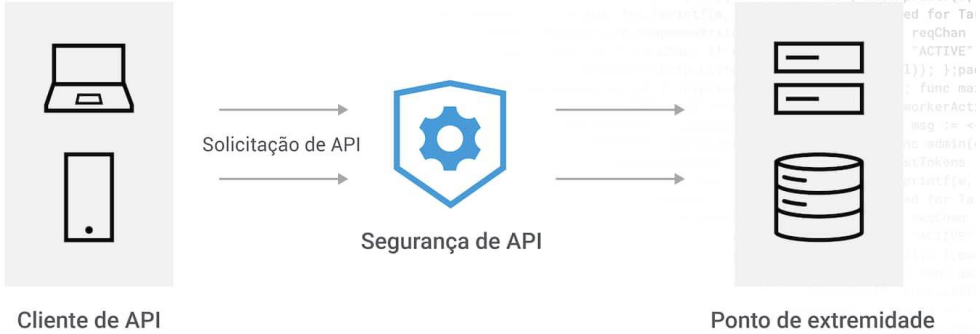
1. Inspeção Visual;
2. Utilização de Ferramentas de Segurança;
3. Análise de Logs;
4. Serviços de Reversão de Percent Encoding;
5. Treinamento de Conscientização.

Fonte: PowerDMARC, 2023.
Disponível em: <https://powerdmarc.com/pt/what-is-url-phishing/>.
Acesso em: 20 mar. 2024.

Aula 6.1

Ataques e Proteção Web – Parte 1

Ataques na Web – Parte 1



Fonte: Akamai.
Disponível em: <https://www.akamai.com/pt/glossary/what-is-api-security>.
Acesso em: 20 mar. 2024.

ATAQUES DE API (APPLICATION PROGRAMMING INTERFACE)

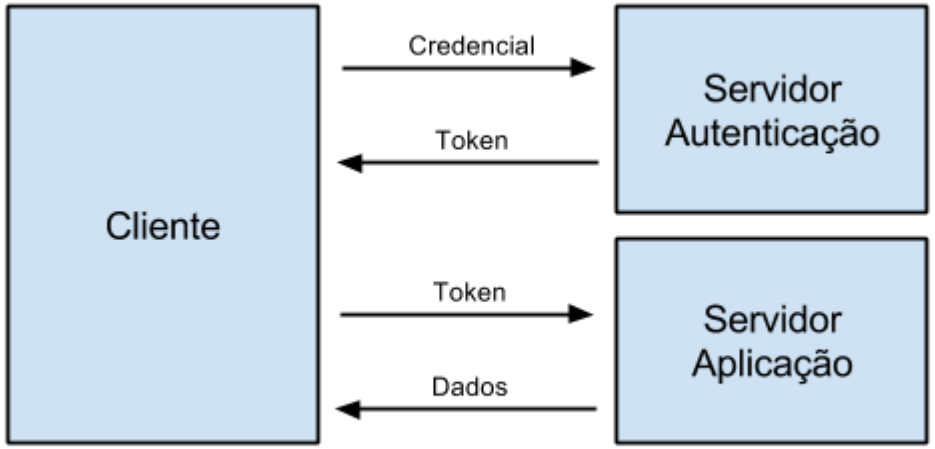
- APIs são conjuntos de regras, ferramentas e protocolos para criação de aplicativos.
- Permite aos desenvolvedores interligarem soluções e serviços sem a necessidade de conhecer como estes foram implementados.
- São tipos comuns de ataques a APIs:

1. Injeção de SQL;
2. Ataques de Força Bruta;
3. Cross-Site Scripting (XSS);
4. Ataques de Dicionário.

AUTENTICAÇÃO EM APIs

- Autenticação é o processo de verificar a identidade de um usuário ou aplicativo que está tentando acessar uma API.
- Maneiras de autenticar usuários em APIs:

1. Autenticação baseada em Token;
2. Autenticação com Credenciais (Usuário/Senha);
3. Autenticação de API Key;
4. Autenticação de Certificado.



Fonte: Raphael Cardoso, 2015.
Disponível em: <https://raphaelcardoso.com.br/criando-e-consumindo-web-api-parte-1/>.
Acesso em: 20 mar. 2024.

AUTORIZAÇÃO EM APIs

- É o processo que verifica se o usuário autenticado tem permissão para acessar determinados recursos ou executar ações dentro da API.

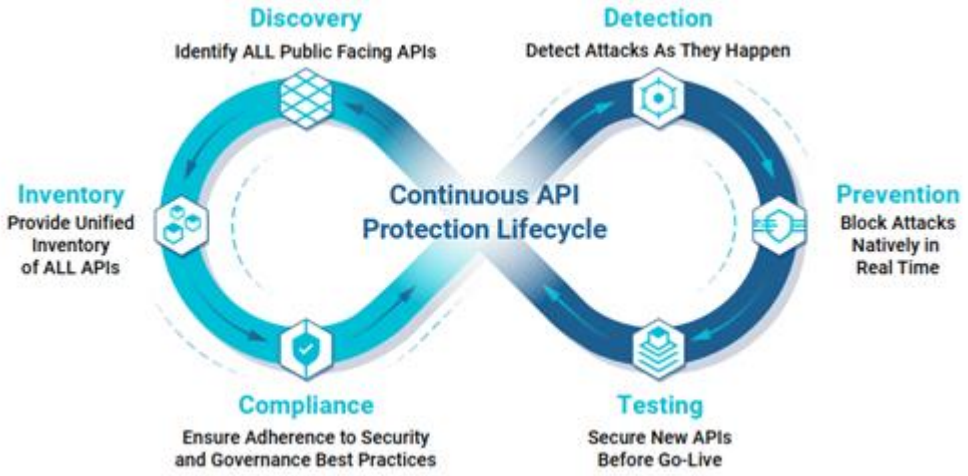
- Formas de implementar a autorização em APIs:

1. Controle de Acesso Baseado em Função (RBAC);
2. Controle de Acesso Baseado em Política (ABAC);
3. OAuth e OAuth2.

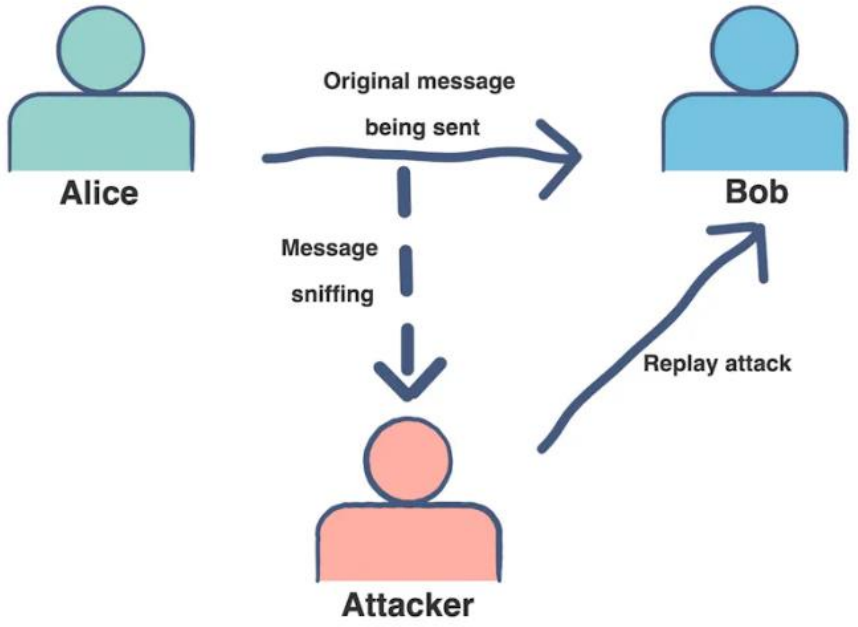
BOAS PRÁTICAS PARA PROTEGER APIS

- Formas de implementar:

1. Validação de Entrada;
2. Limite de Taxa;
3. Controle de Acesso;
4. Monitoramento e Registro;
5. Atualização Regular;
6. Autenticação Forte
7. Documentação Segura.



Fonte: eSafer.
Disponível em: <https://e-safer.com.br/api-protection/>.
Acesso em: 20 mar. 2024.



Fonte: Mirror xyz, 2022.
Disponível em: <https://mirror.xyz/zhangfang.eth/sF7aF9fL7t4ax0v93Eosn5xGpoTD4eNj7qQV5vx0Uxg>.
Acesso em: 20 mar. 2024.

REPLAY ATTACKS (ATAQUES DE REPETIÇÃO)

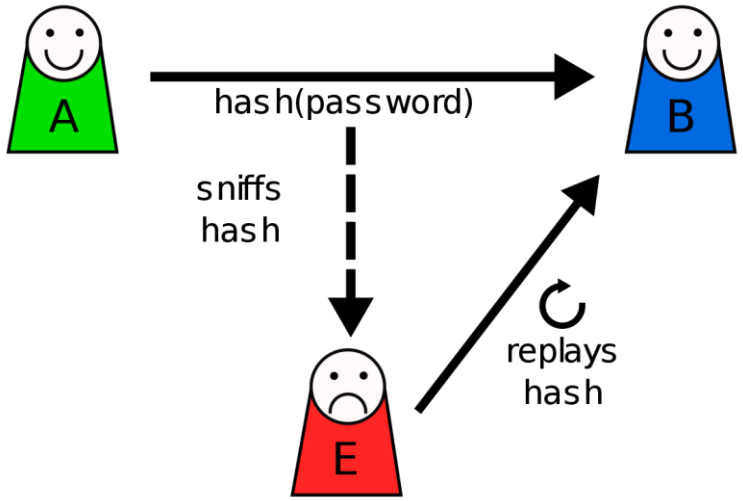
- Um invasor intercepta e depois retransmite dados de comunicação válidos.
- A técnica explora a reutilização de informações legítimas a fim de causar dano.
- Etapas:

1. Interceptação;
2. Armazenamento;
3. Repetição;
4. Exploração ou Acesso Não Autorizado.

MITIGAÇÃO DE ATAQUES DE REPETIÇÃO

- Implementar medidas de segurança:

1. Utilização de Tokens Únicos;
2. Carimbo de Data e Hora;
3. Controle de Sessão;
4. Criptografia;
5. Autenticação Multifator (MFA);
6. Monitoramento de Tráfego;
7. Expiração de Sessão.



Fonte: Gratispng.
Disponível em: <https://www.gratispng.com/png-0y52hb/>.
Acesso em: 20 mar. 2024.

Fonte: Business Process Incubator, 2022.
Disponível em: <https://www.businessprocessincubator.com/content/what-is-session-hijacking/>.
Acesso em: 20 mar. 2024.

SESSION HIJACKING (SEQUESTRO DE SESSÃO)

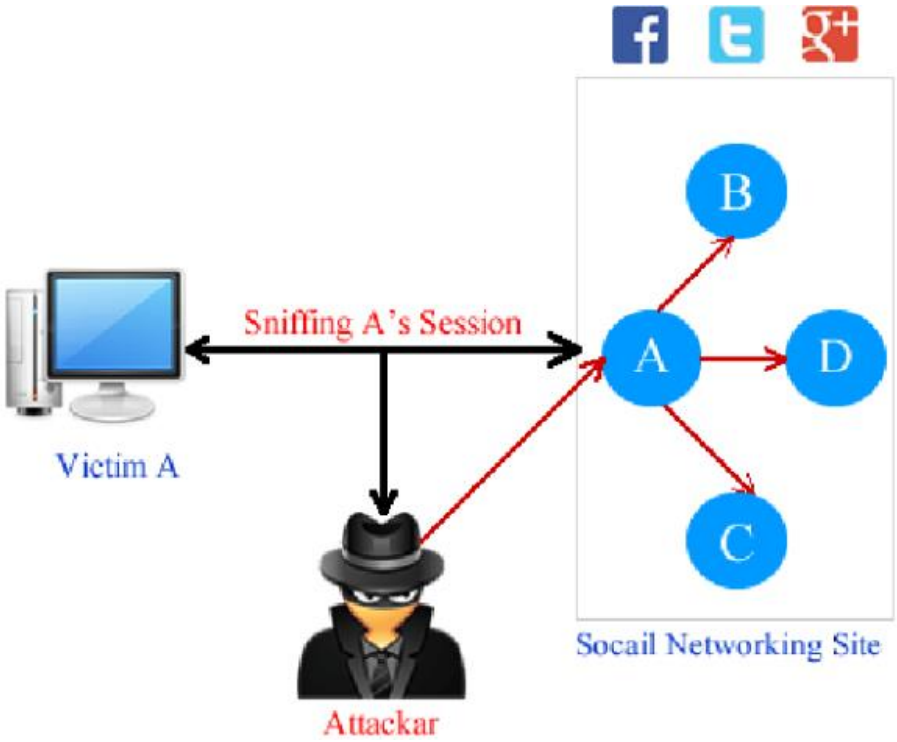
- Trata-se de um ataque cibernético para obter o controle da sessão de um usuário.
- Visa assumir a identidade do usuário legítimo para realizar ações em seu nome.
- Técnicas utilizadas no sequestro de sessão:

1. Captura de Cookies de Sessão;
2. Predição de ID de Sessão;
3. Ataque de Man-in-the-Middle (MitM);
4. Ataque de Session Fixation.

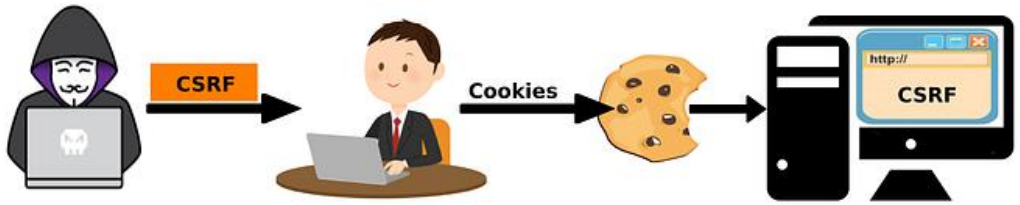
PROTEÇÃO CONTRA SEQUESTRO DE SESSÃO

- Técnicas utilizadas na proteção contra sequestro de sessão:

1. Criptografia;
2. Autenticação Multifator (MFA);
3. IDs de Sessão Aleatórios;
4. Tempo de Expiração de Sessão;
5. Validação de Origem
6. Gerenciamento Seguro de Cookies de Sessão.



Fonte: ResearchGate.
Disponível em: <https://www.researchgate.net/figure/HTTP-Session-Hijacking-of-Social-Network-Users_fig1_297812280>. Acesso em: 20 mar. 2024.



Fonte: Medium, 2021.
Disponível em: <https://medium.com/@efraimmoreira333/csrf-cross-site-request-forgery-conceito-e-pr%C3%A1tica-9f51e091a4a>.
Acesso em: 20 mar. 2024.

CROSS-SITE REQUEST FORGERY (CSRF)

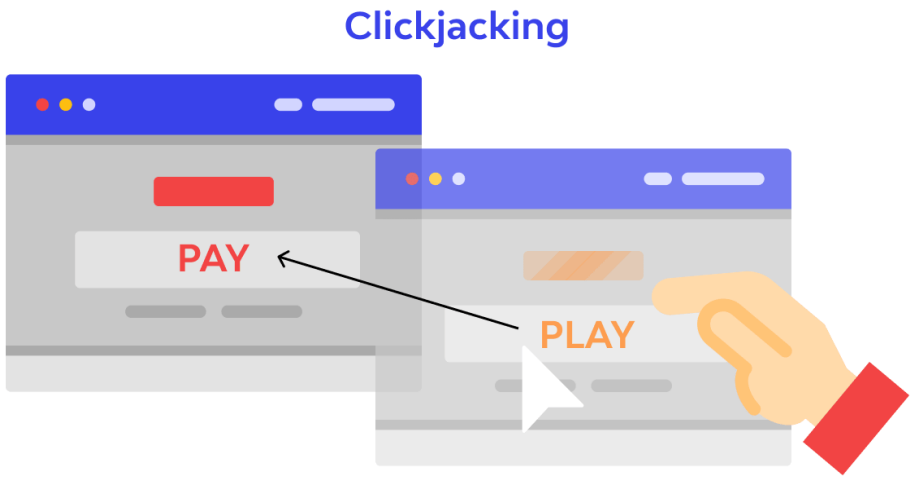
- É um ataque onde um invasor engana um usuário legítimo que já está autenticado.
- Assim, o usuário pode executar ações não intencionais no site ou aplicativo.
- Técnicas utilizadas na prevenção do CSRF:

1. Token Anti-CSRF (CSRF Token);
2. Origens de Referência (Same-Site);
3. Verificação de Origem (Origin);
4. Requerer Confirmação de Ações Críticas;
5. Tempo de Expiração de Sessão.

CLICKJACKING

- Um invasor oculta ou mascara itens de uma página web real utilizando uma outra página maliciosa por trás.
- O usuário clica e pode estar executando uma ação maliciosa e indesejada.
- Técnicas utilizadas na prevenção do Clickjacking:

1. Uso de Cabeçalhos HTTP como X-Frame-Options;
2. Frame-Busting JavaScript;
3. Políticas de Segurança de Conteúdo;
4. Validação Visual.



Fonte: Wallarm.
Disponível em: < https://www.wallarm.com/what/what-is-clickjacking >.
Acesso em: 20 mar. 2024.

Fonte: Infilock, 2023.
Disponível em: <https://infilock.io/blog/how-blockchain-can-prevent-ssl-tls-attacks/>.
Acesso em: 20 mar. 2024.

SSL STRIP (REMOÇÃO DE SSL)

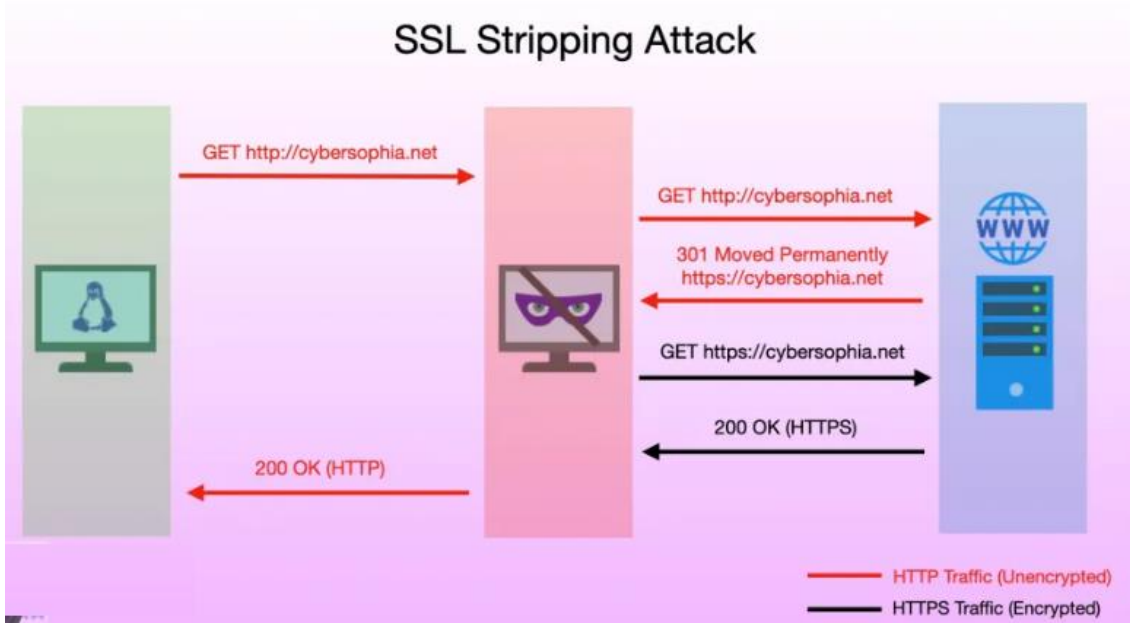
- É um ataque direcionado a conexões SSL/TLS.
- Visa interceptar o tráfego criptografado entre um usuário e um servidor.
- O tráfego é descriptografado e redirecionado para um servidor malicioso.
- Funcionamento:

1. Interceptação;
2. Redirecionamento;
3. Descriptografia;
4. Encaminhamento.

SSL STRIP (REMOÇÃO DE SSL)

- Técnicas utilizadas na prevenção do SSL Strip:

1. Implementação de HTTPS Estrito (Strict HTTPS);
2. HSTS (HTTP Strict Transport Security);
3. Certificados de Segurança e Validação do Usuário;
4. Rede Segura;
5. Segurança do Dispositivo.



HACKERS DO BEM_

Você chegou ao final da Aula 01

Ataques e Proteção Web – Parte 1

Softex SENAI RNP MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÃO GOVERNO FEDERAL BRASIL UNIÃO E RECONSTRUÇÃO