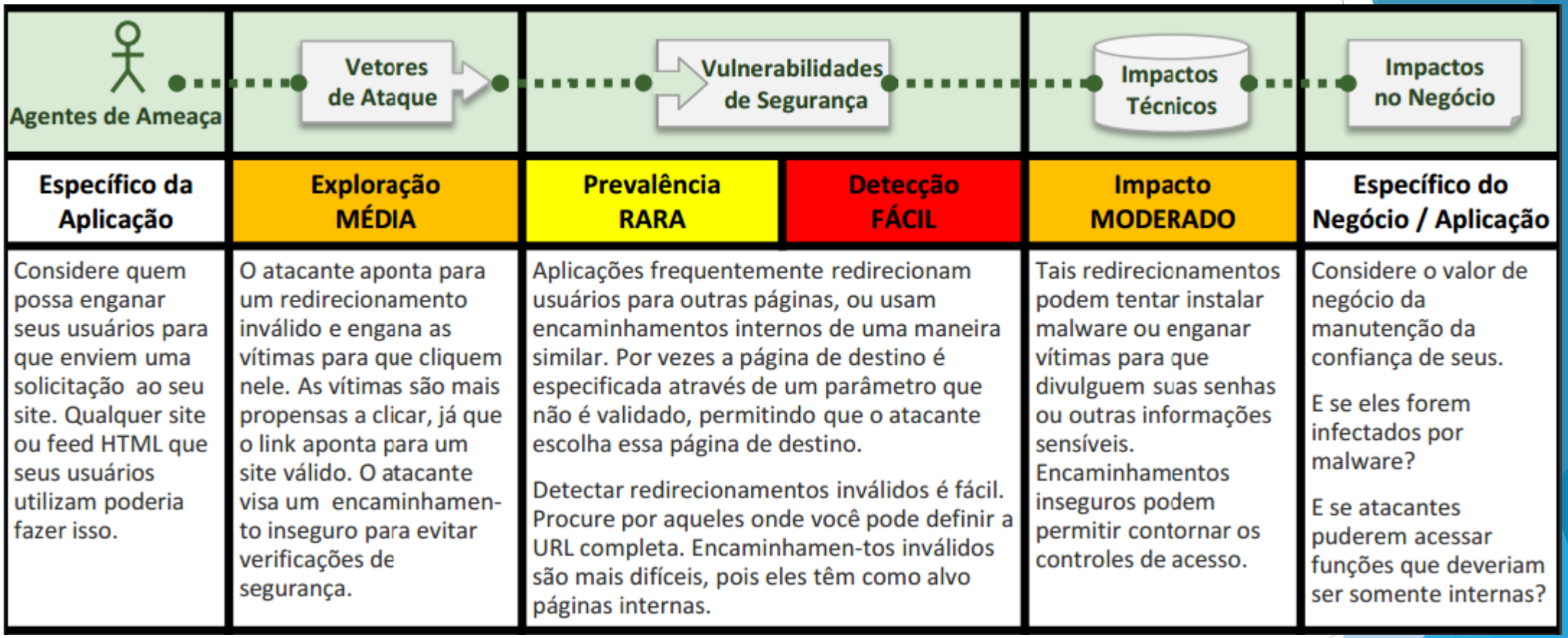
A10 – Redirecionamentos e Encaminhamentos Inválidos

Claudecir da Silva Teixeira

Marylene Guedes Bruno

Ameaça

Aplicações web frequentemente redirecionam e encaminham usuários para outras páginas e sites, e usam dados não confiáveis para determinar as páginas de destino. Sem uma validação adequada, os atacantes podem redirecionar as vítimas para sites de *phishing* ou *malware*, ou usar encaminhamentos para acessar páginas não autorizadas.


Agentes de Ameaça
Vetores de Ataque
Vulnerabilidades de Segurança
Impactos Técnicos
Impactos no Negócio
Específico da Aplicação
Exploração MÉDIA
Prevalência RARA
Detecção FÁCIL
Impacto MODERADO
Específico do Negócio / Aplicação
Considere quem possa enganar seus usuários para que enviem uma solicitação ao seu site. Qualquer site ou feed HTML que seus usuários utilizam poderia fazer isso.
O atacante aponta para um redirecionamento inválido e engana as vítimas para que cliquem nele. As vítimas são mais propensas a clicar, já que o link aponta para um site válido. O atacante visa um encaminhamen-to inseguro para evitar verificações de segurança.
Aplicações frequentemente redirecionam usuários para outras páginas, ou usam encaminhamentos internos de uma maneira similar. Por vezes a página de destino é especificada através de um parâmetro que não é validado, permitindo que o atacante escolha essa página de destino.
Detectar redirecionamentos inválidos é fácil. Procure por aqueles onde você pode definir a URL completa. Encaminhamen-tos inválidos são mais difíceis, pois eles têm como alvo páginas internas.
Tais redirecionamentos podem tentar instalar malware ou enganar vítimas para que divulguem suas senhas ou outras informações sensíveis. Encaminhamentos inseguros podem permitir contornar os controles de acesso.
Considere o valor de negócio da manutenção da confiança de seus.
E se eles forem infectados por malware?
E se atacantes puderem acessar funções que deveriam ser somente internas?

Estou vulnerável?

- Existem formas para saber se você está exposto a esse tipo de ataque seguindo os seguintes passos:

- ✓ Testar todos os redirecionamentos existentes na interação com o usuário;
- ✓ Navegar por toda a aplicação para verificar quais são as páginas que retornam códigos de redirecionamento (geralmente código de retorno 301 e 302);
- ✓ Se a aplicação não empregar criptografia ou *hashing* nos parâmetros de redirecionamento enviados você provavelmente está exposto.

Como evitar?

Evite usá-los. Caso necessário, não envolva parâmetros do usuário no cálculo do destino. Se os parâmetros de destino não podem ser evitados, recomenda-se que qualquer parâmetro de destino seja um valor mapeado e que o código do lado do servidor traduza esse mapeamento para a URL de destino.

Aplicações podem usar ESAPI para substituir o método *sendRedirect()* para certificarem-se de que todos os destinos do redirecionamento são seguros.

Exemplo de aplicação vulnerável

- Neste exemplo, a aplicação possui um script(página) chamado *"redireciona.php"* que utiliza apenas um parâmetro denominado "*url_destino*". O script tem como objetivo redirecionar o usuário para determinada página dentro ou fora da aplicação. Vejamos um exemplo no código abaixo:

```php
<?php

$ir_para_url = $_GET['url_destino'];
header("Location: $ir_para_url");

?>
```

Exemplo de aplicação vulnerável

- O atacante, percebendo este detalhe, criará uma URL maliciosa apontando para um site(servidor) que, uma vez acessado, poderá induzir à vitima a realizar operações indesejadas, conforme demonstra o código abaixo:

```
http:/www.appvulneravel.com/redireciona.php?url_destino=www.craker.com
```

URL maliciosa utilizada no redirecionamento inválido

Prevenção

Uma das formas de prevenção é fazer uso da ESAPI conforme código mostrado abaixo:

```php
<?php
$ir_para_url = $_GET['url_destino'];
$ir_para_url = $ESAPI->HTTPUtilities->sendRedirect("response", request.getParameter("$ir_para_url")  );
header("Location: $ir_para_url");
?>
```

Prevenindo redirecionamentos e encaminhamentos inválidos

Referências

- **OWASP** – Disponível em: https://www.owasp.org/images/9/9c/OWASP_Top_10_2013_PT-BR.pdf
- **Análise das principais vulnerabilidades de aplicações web** – Disponível em: https://flaviomicheletti.github.io/tcc-flavio-alexandre-micheletti.pdf
- **Série Ataques: Saiba quais são os efeitos do redirecionamento arbitrário** – Disponível em: http://www.redesegura.com.br/2012/04/serie-ataques-saiba-sobre-redirecionamento-arbitrario/