|  |  |  |  |
| --- | --- | --- | --- |
| **Teste de aplicativos móveis OWASP** | | | |
|  |  | **0%** | **Porcentagem concluída** |
| **Instruções do questionário:**  **Para cada pergunta, escolha Sim, Não ou N/A no menu suspenso fornecido. Se N/A for escolhido, uma explicação é obrigatória. Use o campo "Additional Information" (Informações adicionais) para a direita da pergunta. Clique na caixa pop-up de instruções e arraste-a, se necessário.** | | | |
| **Número da pergunta** | **Pergunta/solicitação** | **Resposta** | **Informações adicionais** |
| **M.1** | Testes realizados para verificar se o aplicativo não está vulnerável a ataques de engenharia reversa/falta de código | Sim |  |
| **M.2** | Testes realizados para informações confidenciais codificadas no código do aplicativo (incluindo criptografia) | Sim |  |
| **M.3** | Testes realizados para verificar o MSISDN (WAP) | Não |  |
| **M.4** | Teste realizado se o invasor puder ignorar a autenticação de segundo nível | Sim |  |
| **M.5** | teste de instantâneo/background do iOS realizado | Não | Nenhum conteúdo sensível como parte das capturas de tela |
| **M.6** | Teste realizado para verificar se a depuração está definida como TRUE (somente Android) | Sim |  |
| **M.7** | Informações de texto claro no teste de túnel SSL realizado | Sim | Prazo limitado devido à estrutura do flutter |
| **M.8** | Testes realizados para verificar se a validação do lado do cliente não pode ser contornada | Sim |  |
| **M.9** | Testes realizados para informações confidenciais enviadas como texto simples pela rede/falta de dados | Sim |  |
| **M.10** | Testes realizados para implementação inadequada ou NÃO da página Alterar senha | Não | Não há alteração de senha disponível via aplicativo móvel |
| **M.11** | Teste de modificação de URL realizado | Sim |  |
| **M.12** | Informações confidenciais no teste Memory Dump realizado | Sim |  |
| **M.13** | Testes realizados para acessibilidade em dispositivos com root ou com jailbreak | Sim |  |
| **M.14** | Testes de ataque Back-and-Refresh realizados | Sim |  |
| **M.15** | Teste de navegação no diretório realizado | Não |  |
| **M.16** | Teste de redirecionamentos de URL aberto realizado | Não |  |
| **M.17** | Teste de permissões de aplicativos inseguros realizado | Sim |  |
| **M.18** | Teste realizado se a compilação do aplicativo contiver arquivos obsoletos | Não |  |
| **M.19** | Teste de divulgação de IP privado realizado | Sim |  |
| **M.20** | Teste de personificação da interface do usuário por meio da modificação do arquivo RMS (JAVA) realizado | Não |  |
| **M.21** | Teste de personificação da interface do usuário por meio da modificação do arquivo JAR (Android) realizado | Sim |  |
| **M.22** | Operação em um recurso após a expiração ou liberação | Sim |  |
| **M.23** | Teste de ASLR realizado (iOS) | Sim |  |
| **M.24** | Teste de proteção contra quebra de cache realizado (oOS) | Não |  |
| **M.25** | Teste de vulnerabilidade de backup do Android realizado (Android) | Sim |  |
| **M.26** | Teste de permissão global de arquivos em dados de aplicativos realizado (Android) | Sim |  |
| **M.27** | Testes realizados para armazenar a chave de criptografia localmente/armazenar dados confidenciais no ClearText | Sim |  |
| **M.28** | Testes de trânsito de dados de terceiros em canais não criptografados realizados | Não |  |
| **M.29** | Testes realizados por falha na implementação de emissores confiáveis (Android) | Sim |  |
| **M.30** | Teste do verificador de nome de host realizado (Android) | Sim |  |
| **M.31** | Teste do verificador de nome de host personalizado fraco realizado (Android) | Sim |  |
| **M.32** | Teste de vazamento de dados confidenciais de caches de aplicativos/Web realizado | Sim |  |
| **M.33** | Teste do provedor de conteúdo com vazamento realizado | Sim |  |
| **M.34** | Redundância Permissão Concedida teste realizado (Android) | Sim |  |
| **M.35** | Valores passíveis de spoof para testes de autenticação de usuários realizados (IMEI, UDID) | Não | IMEI / UDID não é necessário para o aplicativo |
| **M.36** | Teste de sequestro de atividade realizado (Android) | Sim |  |
| **M.37** | Teste de sequestro de serviço realizado (Android) | Sim |  |
| **M.38** | Teste do Broadcast Thief realizado (Android) | Sim |  |
| **M.39** | Teste de injeção de transmissão maliciosa realizado (Android) | Sim |  |
| **M.40** | Teste de atividade maliciosa/início de serviço realizado (Android) | Sim |  |
| **M.41** | Uso do identificador do dispositivo como teste de sessão realizado | Sim |  |
| **M.42** | Símbolos Testes de remanescentes realizados (iOS) | Não |  |
| **M.43** | Falta de controles de soma de verificação/testes de detecção alterados realizados (Android) | Sim |  |
| **M.44** | Teste de permissões inseguras em soquetes de domínio Unix realizado (Android) | Sim |  |
| **M.45** | Teste de uso inseguro de soquetes de rede realizado (Android) | Sim |  |
| **M.46** | Senha de texto claro no teste Response realizado | Sim |  |
| **M.47** | Referência direta a recursos internos sem a realização de testes de autenticação | Sim |  |
| **M.48** | Teste de que o aplicativo NÃO tem gerenciamento de sessão ou tem um gerenciamento de sessão inadequado/falha para inválido realizado | Sim |  |
| **M.49** | Teste de vulnerabilidade de script entre domínios realizado | Não |  |
| **M.50** | Testes de compartilhamento de recursos entre origens realizados | Sim |  |
| **M.51** | Teste de validação de entrada inadequado realizado - lado do servidor | Sim |  |
| **M.52** | Testes de falsificação de solicitação entre sites (CSRF)/SSRF realizados | Sim |  |
| **M.53** | Teste de respostas HTTPS armazenáveis em cache realizado | Sim |  |
| **M.54** | Atributo de caminho não definido em um teste de cookie realizado | Sim |  |
| **M.55** | Atributo Http Only não definido para um teste de cookie realizado | Sim |  |
| **M.56** | Atributo seguro não definido para um teste de cookie realizado | Sim |  |
| **M.57** | O aplicativo é vulnerável ao teste de ataque de Clickjacking/Tapjacking realizado | Sim |  |
| **M.58** | teste de que é possível realizar a impressão digital do Server/OS | Sim |  |
| **M.59** | Teste de falta de proteção adequada de tempo limite realizado | Sim |  |
| **M.60** | Teste do número de vezes que uma função pode ser usada Limites realizados | Não |  |
| **M.61** | Teste de defesas contra o mau uso do aplicativo realizado | Sim |  |
| **M.62** | Teste de manipulação de recursos no lado do cliente | Sim |  |