Relatorio Pentest

Solicitação: RTR 01

Jul,2022

Índice

1. **Informações**
2. **Uso deste relatório**
3. **Limitações**
4. **Testes Realizados**
5. **Checklist**
6. **Histórico**
7. **Descrição técnica das vulnerabilidades**
   7.1. **Aplicação não valida assinatura JWT**
8. **Matriz Vulnerabilidade**

1. Informações

Contato Técnico	anderson.h.porcel@next.b.br adriano.a.almeida@next.b.br eric.paulo@next.b.br
Data de Início / Fim	05/07/2022 > 07/07/2022
Tipo de Aplicação	Web
Aplicação/Escopo	**Host/Aplicação** : web-security-academy.net
Ambiente Testes	Produção

2. Uso deste relatório

Esse relatório tem a finalidade de informar brechas de segurança encontradas, sem a finalidade de corrigi-las, aplicações testadas e apresentadas pertencem ao CNPJ: 60.746.948.0001-12 | **Banco next** .

Todos os dados apresentados, credenciais utilizadas e vulnerabilidades apresentadas são reais , portanto são dados sensíveis e confidenciais.

3. Limitações

Resultados apresentados neste relatório refletem apenas o momento em que a aplicação foi analisada, sem garantir que todas as vulnerabilidades existentes na aplicação estejam relatadas neste documento.

O trabalho desenvolvido pelo analista **NÃO** tem como objetivo corrigir as possíveis vulnerabilidades, nem proteger a contratante contra ataques internos e externos, tem apenas o objetivo fazer um levantamento dos riscos e recomendar formas para minimizá-los.

As recomendações sugeridas neste relatório devem ser testadas e validadas pela equipe técnica responsável antes de serem implementadas no ambiente de produção. O analista **NÃO** se responsabiliza por essa implementação e possíveis impactos que possam vir a ocorrer em outras aplicações ou serviços.

4. Testes Realizados

Os testes realizados foram feitos manualmente, com uso de ferramentas de segurança a fim de auxiliar na realização dos mesmos. Principais testes realizados seguem a **OWASP Top 10** , **NIST** e **Top 25 SANS** , dentre outras práticas recomendadas pelo mercado de segurança da informação.

5. Checklist

Tópico checklist tem a função de informar quais testes foram ou não realizados referente a aplicação em questão, tendo 3 possíveis respostas:

- " **Realizado** " o qual informa que foram feitos testes referentes ao tópico.
- " **Não realizado** " o qual informa que não foram feitos testes em relação ao tópico, e o mesmo existe na aplicação, porém por questões externas (como limitação de escopo ou tempo) o mesmo não foi realizado.
- " **Não se aplica** " o qual informa que o teste não foi realizado, pois não faz sentido para a aplicação em questão, por conta de funcionalidades as quais estão atreladas ao teste não existirem na mesma, ou estar fora do escopo solicitado de testes.

Teste realizado	Check
Testes de Privilégio (ex: Escalação de Privilégio Horizontal ou Vertical)	Realizado
Testes de Autorização (ex: IDOR)	Não realizado
Testes de Autenticação (ex: Bypass Login, Weak Password, CAPTCHA)	Não se aplica
Testes de Token (ex: JWT, JWE)	?
Testes de Cookie (ex: Flag Secure, Flag HTTPOnly)	?
Testes Lógicos (ex: Alteração do Fluxo lógico)	?
Testes de Input de Dados (ex: Injections, SSRF)	?
Testes de Envio de Arquivos (ex: Bypass File Upload, Envio de N Arquivos)	?
Teste de Carga (ex: Brute Force, Limite Requisição, DOS)	?
Testes HTTP Header (ex: CRLF, Open Redirect)	?
Security Misconfiguration (ex: robots.txt, Information Exposure)	?
Enumeração	?
Componentes Desatualizados	?
Criptografia/Canal de Comunicacao (ex: Uso de SSL/criptografia)	?

6. Histórico

A tabela com histórico mostra a evolução da solicitação ao longo da realização de novos testes/retestes, informando quando vulnerabilidades foram abertas/encontradas e fechadas/corrigidas.

Vulnerabilidades em Aberto

Solicitação	Analista	Data	n*	Vulnerabilidade	Criticidade
RTR ??	ANALISTA	??/??/????	01	Aplicação não valida assinatura JWT.	Média
RTR ??	ANALISTA	??/??/????	02	Aplicação não valida assinatura JWT.	Média

Vulnerabilidades Corrigidas

Solicitação	Analista	Data	n*	Vulnerabilidade	Criticidade

7. Descrição técnica das vulnerabilidades

Os parâmetros utilizados para classificação de severidade das vulnerabilidades foram baseados na metodologia aplicada pelo CVSS, disponível em: *https://www.first.org/cvss/calculator/3.1*

7.1 Aplicação não valida assinatura JWT

CVSS Score:</br>Criticidade Crítica
CVSS:3.1/
CWE-7:
Aplicação/Rota Afetada /:*
--- ---
Explicação da Vulnerabilidade
Riscos
Recomendação de correção
Referências Casos Reais Relacionados:

CVSS Score:</br>Criticidade Alta

CVSS:3.1/
CWE-7:
Aplicação/Rota Afetada /:*
--- ---
Explicação da Vulnerabilidade
Riscos
Recomendação de correção
Referências Casos Reais Relacionados:

CVSS Score:</br>Criticidade Média

CVSS:3.1/
CWE-7:
Aplicação/Rota Afetada /:*
--- ---
Explicação da Vulnerabilidade
Riscos
Recomendação de correção
Referências Casos Reais Relacionados:

CVSS Score:</br>Criticidade Baixa

CVSS:3.1/
CWE-7:
Aplicação/Rota Afetada /:*
--- ---
Explicação da Vulnerabilidade
Riscos
Recomendação de correção
Referências Casos Reais Relacionados:

CVSS Score: 0.0</br>Criticidade Informativa

CVSS:3.1/
CWE-7:
Aplicação/Rota Afetada /:*
Explicação da Vulnerabilidade
Riscos
Recomendação de correção

Referências Casos Reais Relacionados:

Evidências e informações adicionais :

Figura 1 - Ao logar e acessar a rota my-account, foi verificado que a aplicação usa um token JWT

Evidências de correção: --

8. Matriz Vulnerabilidade

Para o cálculo de criticidade foi utilizado a metodologia utilizada pelo NIST CVSS https://nvd.nist.gov/vuln-metrics/cvss . Abaixo segue um informativo para cada criticidade.

Vulnerabilidade Criticidade Crítica **CVSS: 9.0 > 10.0** **Deadline: 14 dias**	Vulnerabilidades de criticidade “Crítica” são caracterizadas por comprometer completamente a confidencialidade, integridade e avaliabilidade da aplicação, por meio de ataques de baixa complexidade ou da falta de privilégios requeridos para realização do ataque. Exemplo: SQL Injection, RCE (Remote Control Execution).
Vulnerabilidade Criticidade Alta **CVSS: 7.0 > 8.9** **Deadline: 1 mês**	Vulnerabilidades de criticidade “Alta” são caracterizadas por comprometer quase totalmente a confidencialidade, integridade e avaliabilidade da aplicação. Exemplo: SSRF, Broken Authentication.
Vulnerabilidade Criticidade Média **CVSS: 4.0 > 6.9** **Deadline: 4 meses**	Vulnerabilidades de criticidade “Média” são caracterizadas por comprometer parcialmente a confidencialidade, integridade e avaliabilidade da aplicação, por meio de ataques de alta complexidade ou do excesso de privilégios requeridos para realização do ataque. Exemplo: Improper Input Validation, CSRF.
Vulnerabilidade Criticidade Baixa **CVSS: 0.1 > 3.9** **Deadline: 6 meses**	Vulnerabilidades de criticidade “Baixa” são caracterizadas por comprometer parcialmente a confidencialidade, integridade ou avaliabilidade da aplicação, como vazamento de dados sensíveis e falhas de configuração. Exemplo: Uncaught Exception, Clickjacking.
Vulnerabilidade Criticidade Informativa **CVSS: 0.0** **Deadline: Á definir**	Vulnerabilidades de criticidade “Informativa” são caracterizadas por não comprometer a confidencialidade, integridade e avaliabilidade da aplicação, são apenas recomendações de segurança.