

|  |
| --- |
| PENETRATION TESTING REPORT  TING REPORT  TING REPORT  TING REPORT  Pentest – White Box  Pentest – BlackBox  Pentest – BlackBox  Pentest – BlackBox  BlackBox  Pentest – BlackBox  Pentest – BlackBox |
| Nome da Empresa RedSecOpsRedSecOpsRedSecOpsRedSecOpsRedSecOpsRedSecOps **DATA:**  **DATA:** 06/03/2022  **DATA:** 06/03/2022  **DATA:** 06/03/2022  **DATA:** 06/03/2022  **DATA:** 06/03/2022  **DATA:** 06/03/2022  **DATA:** 06/03/2022 |

Texto, Logotipo

Descrição gerada automaticamente

# Controle de Versão

|  |  |  |
| --- | --- | --- |
| Versão 1.0 | 00/00/2022 | Fulano X |
| Versão 2.0 |  |  |

# Confidencialidade

Este documento é propriedade exclusiva da [Nome Da Empresa], contém propriedades e informações confidenciais. A duplicação, redistribuição ou uso, no todo ou em parte, de qualquer forma, requer o consentimento da [Nome da Empresa]

A [Nome da Empresa] pode compartilhar este documento com auditores sob acordos de confidencialidade para demonstrar conformidade com os requisitos dos PenTest

# Informações de contato

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Nome | Cargo | Telefone | E-mail | Endereço |
| Andre Silva | PenTester Sr. | 1111111111 | andresilva@hackersec.com | Av paulista 123 |
|  |  |  |  |
|  |  |  |  |

# Aviso Legal

As conclusões e recomendações refletem de informações coletadas durante a avaliação e também sobre outros tipos de testes, não houve quaisquer modificações feitas fora desse período do dia [Data início] a [Data término]. Os compromissos por tempo limitado não permitem uma avaliação completa de todos os controles de segurança. [Nome da Empresa], priorizou a avaliação para identificar os controles de segurança mais fracos que um invasor exploraria.

# Sumario Executivo

A postura de segurança externa e interna foi testada por meio de um PenTest de aplicação web e de Rede em [Data de início] a [Data de término]. Foi descoberta uma vulnerabilidade crítica do eternalblue, e vulnerabilidades em alguns componentes da aplicação web que podem ser usados como vetor de ataque para causar impacto considerável na aplicação. E caso um invasor malicioso explore, permite que ele execute um ransomware na rede ou se ele explorar a aplicação web, ele pode efetuar o sequestro de sessão de um respectivo usuário ou a execução de código malicioso. Isto é altamente recomendável que a vulnerabilidade seja resolvida o mais rápido possível usando guias de correções. Além disso, algumas vulnerabilidades de nível médio e baixo foram encontradas que podem ser impactantes e que são facilmente corrigidos implementando as melhores práticas para desenvolvimento.

# Metodologia

Todos os testes realizados são baseados no Guia Técnico NIST SP 800-115 para

Teste e avaliação de segurança da informação em redes. E o guia de teste OWASP (v4) para tests em aplicações web. As fases das atividades do PenTest incluem o seguinte:

• Planejamento – Objetivos do cliente são levantados e regras de engajamento são obtidas.

• Descoberta – Execute varredura e enumeração para identificar vulnerabilidades potenciais, fracas áreas e explorações.

• Ataque – Confirme possíveis vulnerabilidades por meio da exploração e execute ações adicionais descoberta mediante novo acesso.

• Relatórios – Documente todas as vulnerabilidades e explorações encontradas, tentativas fracassadas e forças e fraquezas

Foi utilizado o OWASP-TOP 10 para realizar os testes nas aplicações web e a metodologia NIST ou PTES para o resto do ambiente.

Diagrama

Descrição gerada automaticamente

# SeveridadeTabela Descrição gerada automaticamente

# Sumario de vulnerabilidade

|  |  |  |  |
| --- | --- | --- | --- |
| Host | Vulnerabilidade | Risco | Impacto |
| 10.1.0.11 | Eternalblue | Crítico | Alto |
| 10.1.0.12 | Xss Refletido | Alto | Alto |
| 10.1.0.12 | XSS Armazenado | Alto | Alto |
| 10.1.0.12 | XSS DOM | Alto | Alto |
| 10.1.0.12 | ROBOTS.TXT | Informativo | N/A |
|  |  |  |  |
|  |  |  |  |

# Detalhes das vulnerabilidades

# Alvo 1

### **Eternalblue**

|  |
| --- |
| IP: 10.1.0.11 / Vulnerabilidade: MS17-010 – Eternalblue |

## Sobre a vulnerabilidade

## EternalBlue é um exploit desenvolvido pela Agência Nacional de Segurança dos Estados Unidos.Esse código é elemento de um conjunto de programas secretos revelados pelo grupo Shadow Brokers em 14 de abril de 2017 e foi utilizado no ciberataque mundial que utilizava o ransomware WannaCry e pelo malware Adylkuzz.

## Prova de Conceito

## Exploração utilizando o MSFCONSOLE/MetasploitTexto Descrição gerada automaticamente

## Recomendação

<https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010>

# Alvo 2

### **Xss Refletido**

|  |
| --- |
| IP: 10.1.0.12 / Vulnerabilidade: XSS Refletido |

## Sobre a vulnerabilidade

Cross-site scripting refletido também conhecido como XSS refletido, XSS não persistente ou XSS tipo 1, é uma das vulnerabilidades mais encontrada atualmente. Essa falha se manifesta quando a aplicação web vulnerável reflete um valor qualquer, sem antes validá-lo de forma correta.

## Prova de Conceito

Adicionei um <script>alert("Vulneravel")</script> no campo “name”  
  
Interface gráfica do usuário, Aplicativo, Site

Descrição gerada automaticamente

## Recomendação

[**https://cheatsheetseries.owasp.org/cheatsheets/Cross\_Site\_Scripting\_Prevention\_Cheat\_Sheet.html**](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)

### **Xss Armazenado**

|  |
| --- |
| IP: 10.1.0.12 / Vulnerabilidade: XSS Armazenado |

## Sobre a vulnerabilidade

O **XSS armazenado** é quando os dados não seguros são **armazenados** em algum meio para que posteriormente seja recuperado.

## Prova de Conceito

Adicionei um <script>alert(1)</script> no campo “name” e manipulei o parâmetro max-lenght do html  
  
Interface gráfica do usuário, Texto, Aplicativo, Site

Descrição gerada automaticamente

## Recomendação

[**https://cheatsheetseries.owasp.org/cheatsheets/Cross\_Site\_Scripting\_Prevention\_Cheat\_Sheet.html**](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)

### **Xss DOM**

|  |
| --- |
| IP: 10.1.0.12 / Vulnerabilidade: XSS DOM |

## Sobre a vulnerabilidade

Um ataque XSS baseado em DOM é possível se o aplicativo web escrever dados para o Modelo de Objeto de Documento sem higienização adequada. O invasor pode manipular esses dados para incluir conteúdo XSS na página da Web, por exemplo, código JavaScript malicioso.

## Prova de Conceito

Adicionei um <script>alert('vulneravel')</script> no final do parâmetro English  
  
Interface gráfica do usuário, Aplicativo, Site

Descrição gerada automaticamente

## Recomendação

[**https://cheatsheetseries.owasp.org/cheatsheets/Cross\_Site\_Scripting\_Prevention\_Cheat\_Sheet.html**](https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html)