RELATÓRIO DE PENTEST

Web Application

Wesley SIQUEIRA

wEST enterprise

# Resumo Executivo

* **Objetivo**
  + O objetivo principal deste relatório é a execução de teste de pentest na infraestrutura e web application da empresa Acunetix Ltda, <http://testphp.vulnweb.com>
* **Contexto**
  + Todo teste de pentest foi realizado utilizando metódologia Black Box and WSGT, então não foi fornecido nenhuma credencial ou informação de sistemas
* **Tipo de Pentest**
  + Pentest realizado usando Black Box, sendo um pentest externo, com tecnicas de enumeração e osint, com intuito de testar a privacidade e segurança da web application
* **Escopo**
  + O escopo do teste incluiu a análise de segurança da aplicação web no endereço <http://testphp.vulnweb.com>, com a identificação de vulnerabilidades de alto risco, como XSS e Injeção SQL.Foi excluido bancos de produções e execuções de SQL injection que cause interrupção do sistemas.
* **Comunicação com os Envolvidos**
  + Sera comunicado ao contrate ao encotrar vulnerabilidades de alto risco que demande uma urgente correção, fora isso comunicação sera na etapas finais para alinhamento do que foi econtrado de vulnerabilidade
* **Plano de Teste de Penetração**
  + Sera relizado o teste em 1 mes com 4 semanas de varias etapas,desde a coleta de informação a exploração dessas vulnerabilidades
* **Acordo de Não Divulgação (NDA)**
  + O Acordo de Não Divulgação (NDA) foi firmado para garantir que todas as informações do teste de penetração, incluindo vulnerabilidades e dados técnicos, sejam mantidas em sigilo. Qualquer uso indevido ou divulgação não autorizada das informações pode resultar em danos à segurança da organização.
* **Autorização Formal**
  + A autorização formal foi assinada pela empresa Acunetix LTDA para realizar o teste de penetração na aplicação web, com a devida autorização de exploração de vulnerabilidades, desde que não afete sistemas de produção ou recursos críticos.

# **DISCLAIMER / AVISO DE ISENÇÃO DE RESPONSABILIDADE**

Este relatório de **Teste de Pentest** foi elaborado exclusivamente para a **Acunetix LTDA** com base no escopo, permissões e condições previamente acordadas. As informações contidas neste documento são **estritamente confidenciais** e destinadas apenas ao contratante e à sua empresa.

O objetivo deste relatório é identificar vulnerabilidades de segurança e fornecer recomendações para mitigação. No entanto, **não é garantido que todas as falhas de segurança tenham sido detectadas**, nem que o ambiente esteja completamente seguro contra **possíveis ataques futuros**. A segurança da informação é um **processo contínuo**, e novas ameaças podem surgir a qualquer momento.

A execução dos testes seguiu as **melhores práticas do setor**, respeitando os limites definidos no **Acordo de Não Divulgação (NDA)** e na **Autorização Formal** concedida pelo cliente. **Qualquer uso indevido deste relatório, sua divulgação não autorizada ou ações baseadas em seu conteúdo sem o devido acompanhamento profissional podem representar riscos adicionais à segurança da organização.**

O cliente assume total responsabilidade pela **implementação das recomendações apresentadas** e pelas decisões tomadas com base nos achados deste documento. **Não nos responsabilizamos por quaisquer danos diretos ou indiretos** decorrentes da interpretação ou aplicação das informações aqui contidas.

# **OBJETIVO E ESCOPO**

O objetivo deste relatório é documentar a realização do teste de **pentest** em aplicações web e sua infraestrutura, com foco principal no site [**http://testphp.vulnweb.com**](http://testphp.vulnweb.com). O objetivo principal foi identificar vulnerabilidades de segurança críticas, como XSS e SQL Injection, e fornecer recomendações para mitigação. A autorização para a realização dos testes foi obtida após uma conversa com o cliente, na qual ficou acordada a execução das atividades na empresa **Acunetix LTDA**.

O teste foi realizado utilizando a metodologia de **caixa preta (Black Box)**, em que **nenhuma informação confidencial ou técnica dos sistemas foi fornecida**. Durante os testes, foram empregados os meios descobertos para identificar falhas ou vazamento de informações, respeitando os limites acordados para garantir que **não houvesse interferência ou danos às instalações ou sistemas da empresa**. Além disso, os testes foram realizados **apenas em horários não comerciais**, para evitar impactos nas operações da empresa.

***Ativos explorados:***

* <http://testphp.vulnweb.com>
* Servidor Ubuntu 20.4
* PHP 5.6.40-38

**Credencias:**

O teste foi realizado utilizando o método **Black Box**, ou seja, **não foram fornecidas credenciais** para a realização deste pentest.

**Exclusões:**

Seguintes recursos que foram excluidos do escopo desse relatório e dos testes, para não ocasionar interrupções de sistemas que afetem o trabalho operacional da empresa.

* **Banco de dados (PRODUÇÃO) – MySQL**
* **Execução de Injections SQL e XSS**

**Data de Execução:**

Testes executado na data 01/03/2025 até 31/03/2025, em horarios não comerciais para não atrapalhar as operações corporativas da empresa.

# **Tipo de Pentest**

O teste de penetração descrito neste relatório segue a metodologia **Black Box**, na qual nenhuma informação prévia foi passadaa sobre os sistemas ou infraestrutura da empresa. Esse método foi escolhido por ser o mais adequado para identificar vulnerabilidades que, muitas vezes, não são vistas internamente pela organização.

Durante o teste, será avaliado como a aplicação web responde a diferentes abordagens de ataque, especialmente em relação à **privacidade**,**segurança** e a sua conformidade com os princípios da **Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidaade (CIDAL)** dos dados.

As atividades incluirão:

* **Enumeração de portas para identificar serviços expostos**
* **Varredura de vulnerabilidades para detectar falhas**
* **Fingerprint Web Server**
* **Coleta de informações públicas (OSINT)**

Princiapl objetivo é validar as medidas de segurança já implementadas pela empresa, testando-as sob uma perspectiva externa, com informações limitadas, semelhante à de um atacante real.

# **Comunicação com os Envolvidos**

Neste contrato, são adotados dois tipos de comunicação entre as equipes externas e internas da empresa. O compartilhamento de informações e os resultados das análises de vulnerabilidades seguirão uma abordagem prioritária, na qual **as falhas de alto risco serão imediatamente reportadas ao time de segurança da empresa para uma rápida resolução**.

Vulnerabilidades de menor impacto ou com risco reduzido serão documentadas e compiladas ao longo do processo, sendo entregues **junto ao relatório final**, que abrangerá tanto a infraestrutura quanto a aplicação web testada.

# **Plano de Teste de Penetração**

Será utilizado como metodologia o **Web Security Testing Guide (WSTG)**, um guia criado pela OWASP (Open Web Application Security Project), com o intuito de criar padronizações para testes de aplicações web, garantindo que as aplicações sejam testadas de forma eficaz contra vulnerabilidades. Com isso, realizaremos vários dos testes recomendados em um cronograma que durará cerca de 1 mês, sendo dividido da seguinte forma:

1. **Semana 1 - Coleta de informações**
   1. Será realizada a busca de informações a respeito dos sistemas do contratante, sendo o foco principal, como dito anteriormente, o site <http://testphp.vulnweb.com>.
   2. Testes de enumeração
   3. Testes de fingerprinting
2. **Semana 2 - Análise das vulnerabilidades e informações encontradas**
   1. Caso seja encontrada uma vulnerabilidade de alto risco, será reportada imediatamente.
3. **Semana 3 -Exploração de certas vulnerabilidades encontradas**
   1. Avaliar o impacto das vulnerabilidades e as formas de correção.
4. **Semana 4 – Entrega do Relatorio**
   1. Comunicação e organização de reunião com os times envolvidos na questão de segurança
   2. Entrega do relatório final, com vulnerabilidades encontradas e possíveis soluções.

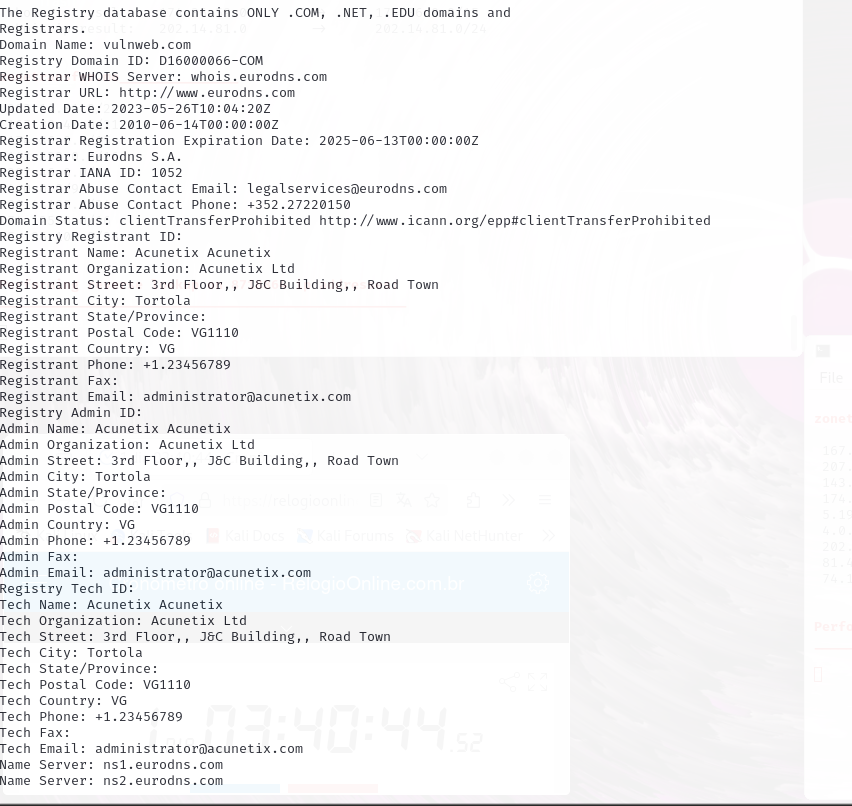
**Ferramentas a serem utilizadas:**

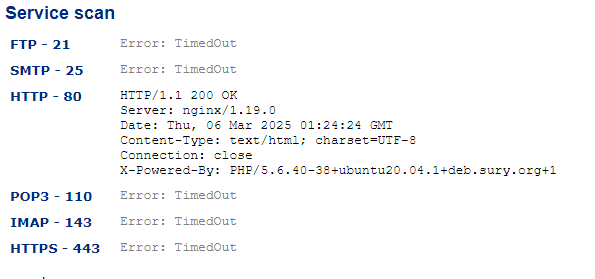
1. **OSINT Framework**: <https://osintframework.com>  
   Utilizado para coletar informações abertas (OSINT)
2. **OWASP ZAP:**  
   Ferramenta de segurança que auxilia na realização de testes de pentest em aplicações web, permitindo a detecção de vulnerabilidades como XSS, injeção de SQL, entre outras.
3. **WHOIS**:  
   Utilizado para obter informações sobre o registro de domínios, como dados de proprietário, servidores de nomes e datas de expiração do domínio. Usadi para coleta de informações sobre a infraestrutura de rede.

|  |  |  |
| --- | --- | --- |
| **Nome** | **Nível de Risco** | **Número de Instâncias** |
| Cross Site Scripting (Refletido) | Alto | 19 |
| Cross Site Scripting (baseado em DOM) | Alto | 11 |
| Injeção SQL - MySQL | Alto | 19 |
| Ausência de tokens Anti-CSRF | Médio | 4 |
| Content Security Policy (CSP) Header Not Set | Médio | 54 |
| Injeção XSLT | Médio | 2 |
| Missing Anti-clickjacking Header | Médio | 46 |
| O servidor vaza informações por meio dos campos de cabeçalho de resposta HTTP "X-Powered-By" | Baixo | 79 |
| Server Leaks Version Information via "Server" HTTP Response Header Field | Baixo | 92 |
| X-Content-Type-Options Header Missing | Baixo | 82 |
| Authentication Request Identified | Informativo | 2 |
| Divulgação de Informações - Comentários Suspeitos | Informativo | 1 |
| GET for POST | Informativo | 3 |
| Modern Web Application | Informativo | 9 |
| Má Combinação de Charset (Cabeçalho versus Meta Content-Type Charset) | Informativo | 32 |
| User Agent Fuzzer | Informativo | 223 |
| User Controllable HTML Element Attribute (Potential XSS) | Informativo | 4 |

# Análise de Vulnerabilidades e Informações Coletadas

Vulnerabilidades encotradas ao fazer scan no <http://testphp.vulnweb.com> usando OWASP Zap.

**Estatisca do nivel de riscos encotrados.Informações coletadas usando Osint – no site** [**https://centralops.net/co/DomainDossier.aspx**](https://centralops.net/co/DomainDossier.aspx) **onde fazemos a busca usando a url do para**

**Fazendo Banner Grabrig foi descoberto a versao do servidor que tem a web application**

# Acordo de Não Divulgação (NDA)

**Este Acordo de Não Divulgação (NDA) é celebrado entre:**

**Parte Contratante**

|  |  |
| --- | --- |
| **Empresa/Cliente** |  |
| **CNPJ/CPF** |  |
| **Endereço** |  |

**Parte Receptora**

|  |  |
| --- | --- |
| **Nome/Empresa** |  |
| **CNPJ/CPF** |  |
| **Endereço** |  |

**Data de Início: [Data de início]  
Data de Término: [Data de término]**

**1. OBJETO DO ACORDO**

**Este Acordo de Não Divulgação tem como objetivo garantir que a Parte Receptora mantenha em sigilo todas as informações relacionadas ao Teste de Penetração realizado pela Parte Contratante, incluindo, mas não se limitando a, vulnerabilidades descobertas, dados técnicos, relatórios de segurança, métodos de ataque, entre outros materiais confidenciais.**

**2. DEFINIÇÃO DE INFORMAÇÕES CONFIDENCIAIS**

**Informações Confidenciais incluem todas as informações relacionadas ao teste de penetração, tais como vulnerabilidades de segurança, recomendações, análises técnicas e quaisquer outros dados fornecidos pela Parte Reveladora, por qualquer meio, escrito, eletrônico ou verbal, durante a execução dos testes.**

**3. OBRIGAÇÕES DA PARTE RECEPTORA**

**A Parte Receptora concorda em:**

**a) Manter a confidencialidade de todas as Informações Confidenciais e não divulgá-las a terceiros sem a permissão prévia por escrito da Parte Contratante.**

**b) Usar as Informações Confidenciais exclusivamente para os fins estabelecidos neste Acordo.**

**c) Tomar todas as medidas razoáveis para proteger as Informações Confidenciais de divulgação não autorizada ou uso indevido.**

**4. EXCEÇÕES À CONFIDENCIALIDADE**

**As obrigações de confidencialidade não se aplicam a informações que:**

**a) Já eram de domínio público ou que se tornaram públicas sem violação deste Acordo.**

**b) Foram divulgadas por terceiros sem violação de uma obrigação de confidencialidade.**

**c) Foram exigidas por lei, regulamentação ou ordem judicial, desde que a Parte Receptora informe a Parte Contratante de forma apropriada.**

**5. RESPONSABILIDADE E DANOS**

**A Parte Receptora será responsável por qualquer uso indevido das Informações Confidenciais e por danos diretos ou indiretos resultantes da violação deste Acordo.**

**6. PRAZO E VIGÊNCIA**

**Este Acordo entra em vigor na Data de Início e permanecerá em vigor até a Data de Término, com a obrigação de confidencialidade se estendendo por [inserir período] após o término.**

**7. ISENÇÃO DE RESPONSABILIDADE**

**A Parte Contratante não se responsabiliza por quaisquer danos diretos ou indiretos resultantes do uso indevido das Informações Confidenciais pela Parte Receptora. A Parte Receptora reconhece que, ao acessar e usar as Informações Confidenciais, ela o faz por sua própria conta e risco, assumindo total responsabilidade pela aplicação ou interpretação das informações. A Parte Contratante não garante que todas as vulnerabilidades ou falhas de segurança serão identificadas ou corrigidas, sendo este processo sujeito a limitações naturais de qualquer teste de penetração.**

**8. LEGISLAÇÃO APLICÁVEL E JURISDIÇÃO**

**Este Acordo será regido pelas leis da [jurisdição] e as partes elegem o foro da comarca de [local] para a resolução de quaisquer disputas.**

**Assinado por:**

**Parte Contratante: Parte Receptora:**

|  |  |  |
| --- | --- | --- |
| **Nome:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | **Nome: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **Assinatura: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | **Assinatura: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | **Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

# AUTORIZAÇÃO FORMAL DE TESTE DE PENETRAÇÃO

Eu, [Nome do responsável], representante legal da empresa **Acunetix LTDA**, CNPJ [Número do CNPJ], autorizo a realização do Teste de Penetração na infraestrutura de TI e aplicação web da nossa empresa, conforme os termos e condições previamente acordados.

O teste será conduzido pela [Nome da empresa ou consultor responsável] de acordo com a metodologia **Web Security Testing Guide (WSTG)**, da OWASP, e será executado no site [**http://testphp.vulnweb.com**](http://testphp.vulnweb.com).

**1. OBJETIVO DA AUTORIZAÇÃO**

Esta autorização permite que a empresa **[Nome da empresa de pentest]** realize os testes de penetração descritos no relatório com o objetivo de identificar vulnerabilidades de segurança e fornecer recomendações para mitigação.

**2. DEFINIÇÕES**

Os testes incluem, mas não se limitam a, atividades de:

* Enumeração de serviços e portas
* Análise de vulnerabilidades e falhas de segurança
* Exploração controlada de vulnerabilidades identificadas

**3. ESCOPOS E LIMITAÇÕES**

Os testes serão realizados com base no escopo acordado, sendo:

* O teste se concentrará no site [**http://testphp.vulnweb.com**](http://testphp.vulnweb.com) e em seus componentes.
* Não será realizado qualquer teste que possa impactar negativamente a operação da empresa, especialmente em sistemas de produção ou recursos críticos.

**4. SEGURANÇA E CONFIDENCIALIDADE**

O contrato está condicionado à assinatura do **Acordo de Não Divulgação (NDA)**, garantindo que todas as informações obtidas durante o teste sejam mantidas em sigilo.

**6. ISENÇÃO DE RESPONSABILIDADE**  
A empresa contratante entende que a responsabilidade pela implementação das medidas de segurança recomendadas, como a mitigação das vulnerabilidades identificadas, é da própria organização. O relatório fornecido terá como objetivo informar as vulnerabilidades encontradas e sugerir formas de mitigação, mas a implementação das correções fica a cargo da empresa Acunetix LTDA.

**5. PRAZO DE EXECUÇÃO**

O teste será executado entre os dias **01/03/2025 e 31/03/2025**, exclusivamente em horários não comerciais, conforme acordo mútuo.

|  |  |  |
| --- | --- | --- |
| **Nome:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | **Nome: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **Assinatura: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | **Assinatura: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |
| **Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |  | **Data: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_** |

**Parte Contratante: Parte Receptora:**