

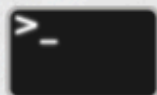
# TESTE DE PENETRAÇÃO

## RELATÓRIO

### WEB APPLICATION



EST. 2024



## TABELA DE CONTEÚDO

<b>1. CONTROLE DE VERSÃO .....</b>	<b>2</b>
<b>2. DISCLAIMER .....</b>	<b>3</b>
<b>3. RELATÓRIO EXECUTIVO .....</b>	<b>4</b>
<b><i>3.1 objetivo e escopo .....</i></b>	<b><i>4</i></b>
<b><i>3.2 estatísticas .....</i></b>	<b><i>5</i></b>
<b><i>3.3 conclusão .....</i></b>	<b><i>6</i></b>
<b><i>3.4 recomendações.....</i></b>	<b><i>7</i></b>
<b>4. RELATÓRIO TÉCNICO .....</b>	<b>8</b>
<b><i>4.1 metasploit .....</i></b>	<b><i>8</i></b>
<b><i>4.2 xss .....</i></b>	<b><i>11</i></b>
<b><i>4.3 nmap .....</i></b>	<b><i>14</i></b>
<b><i>4.4 cyberchef.....</i></b>	<b><i>16</i></b>
<b><i>4.5 falta de cabeçalho de segurança .....</i></b>	<b><i>18</i></b>
<b>5. ANEXOS .....</b>	<b>19</b>
<b><i>5.1 lista de ferramentas .....</i></b>	<b><i>19</i></b>
<b><i>5.2 metodologia .....</i></b>	<b><i>20</i></b>

## 1. CONTROLE DE VERSÃO

VERSÃO	RESPONSÁVEL	DATA
1	PENTEST TEAM	10/11/2023
2	QA TEAM	—
3	GERENTE DE PROJETOS	—

## **2. DISCLAIMER**

Este relatório é fornecido com base nos resultados dos testes de invasão conduzidos nas datas especificadas no escopo e reflete o estado de segurança dos sistemas avaliados naquele momento específico. Devido à natureza evolutiva da tecnologia e do cenário de ameaças, a segurança de qualquer sistema ou aplicação pode mudar ao longo do tempo com a introdução de novos softwares, atualizações, configurações ou ameaças emergentes.

A Giovanna Guedes realizou este teste de invasão com o máximo de diligência e profissionalismo, usando metodologias reconhecidas e ferramentas atualizadas. No entanto, não há garantia de que todas as vulnerabilidades potenciais tenham sido identificadas ou que os sistemas testados sejam imunes a ameaças não detectadas durante o período de avaliação.

As recomendações e conclusões fornecidas neste relatório são baseadas na melhor avaliação e entendimento dos analistas no momento da avaliação. A responsabilidade final pela implementação de qualquer medida corretiva e pela segurança contínua dos sistemas testados pertence à contratante.

Este relatório é confidencial e destinado exclusivamente ao uso da contratante. Qualquer distribuição, reprodução ou divulgação deste documento, no todo ou em parte, sem a permissão expressa da Giovanna Guedes é estritamente proibida.

## 3. RELATÓRIO EXECUTIVO

### 3.1 OBJETIVO E ESCOPO

Neste tópico, detalharemos os ativos específicos que foram incluídos na avaliação sejam eles sistemas, redes, aplicações ou outros componentes tecnológicos. Além disso, esclareceremos quaisquer restrições ou exclusões que foram acordadas previamente, bem como as datas em que a atividade ocorreu.

#### Ativo alvo

- <https://www.testphp.vulnweb.com>

#### Credenciais

- Não provido

Recomenda-se que as contas fornecidas para esse exercício sejam deletadas após a finalização deste projeto.

#### Exclusões

Os seguintes recursos tecnológicos foram excluídos do escopo definido:

- Upload de documentos

#### Data

O teste de invasão nos ativos acima mencionados foi realizado entre as seguintes datas: 26.09.2023 até 10.10.2023

### 3.2 ESTATÍSTICAS

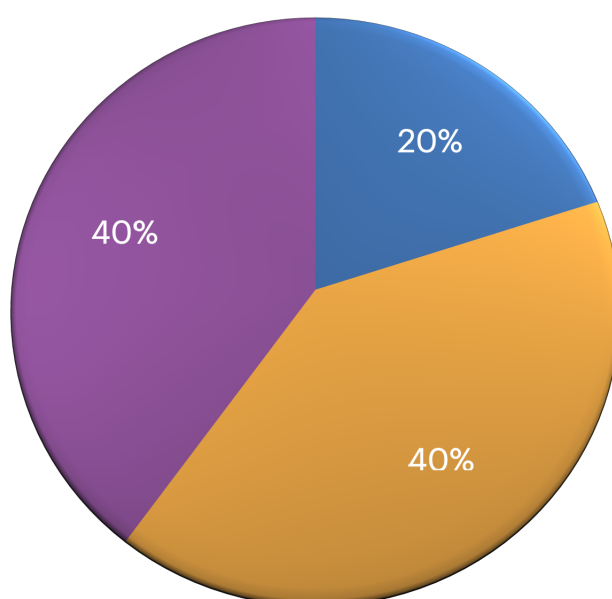
Esta seção do relatório apresenta estatísticas cruciais obtidas a partir de nossa avaliação de teste de invasão, fornecendo aos gestores uma visão quantificada das vulnerabilidades e riscos associados aos sistemas avaliados.

Nesta seção, você encontrará dados agregados que ilustram aspectos como o número total de vulnerabilidades encontradas, sua distribuição por gravidade e categorias, bem como comparações relevantes que podem ajudar a contextualizar a postura atual de segurança da organização. A intenção é fornecer uma ferramenta que auxilie na formulação de estratégias e na tomada de decisões informadas para aprimorar a resiliência cibernética da empresa.

#	DESCRIÇÃO	SEVERIDADE	RESPONSÁVEL	ATIVOS AFETADOS
1	METASPLOIT	Crítico		VEJA TÓPICO 4.1
2	XSS	Crítico		VEJA TÓPICO 4.2
3	NMAP	MÉDIO		VEJA TÓPICO 4.3
4	CYBERCHEF	MÉDIO		VEJA TÓPICO 4.4
5	FALTA DE CABEÇALHO DE SEG.	Informativo		VEJA TÓPICO 4.5

No gráfico abaixo temos a representação da distribuição das vulnerabilidades por nível de severidade.

● INFORMATIVO ● BAIXO ● MÉDIO ● ALTO ● CRÍTICO



### 3.3 CONCLUSÃO

A Giovanna Guedes realizou um teste de invasão nas aplicações definidas no escopo deste relatório e, ao final do projeto, foram identificadas vulnerabilidades: 2 críticas, 2 médias e 1 informativa.

Entre as vulnerabilidades encontradas duas delas poderiam comprometer a integridade, confidencialidade e disponibilidade dos dados dos clients que usam a aplicação, e duas que potencialmente causariam os mesmos impactos.

Durante o período de teste, os analistas conseguiram (simulando um atacante real) copiar os dados pessoais de clientes cadastrados na plataforma. vulnerabilidade que possibilitou tal acesso pode ser resolvida por aprimorar validação dos dados enviados pelos usuários e fazendo uso de técnicas de desenvolvimento que anulam esse tipo de ataque.

Adicionalmente, um item informativo foi colocado no relatório para análise interna do time, mas recomendações foram fornecidas no tópico correspondente.

É importante destacar que embora as correções recomendadas neste relatório sejam cruciais, a segurança é um processo contínuo que exige vigilância, atualizações regulares e revisões periódicas.

Recomendamos que a organização adote as sugestões fornecidas neste relatório como parte de uma estratégia de segurança holística. Além disso, a realização de testes de invasão regulares, acompanhada de treinamento contínuo conscientização sobre segurança para a equipe de desenvolvimento, garantirá que a aplicação permaneça resiliente diante de ameaças futuras.

### 3.4 RECOMENDAÇÕES

Esta seção visa fornecer uma série de diretrizes e melhores práticas que, embora não ligadas diretamente a uma vulnerabilidade específica, têm o potencial de fortalecer significativamente o ambiente de segurança como um todo.

Estas recomendações buscam abordar não apenas aspectos técnicos, mas também operacionais e organizacionais, considerando uma abordagem geral de segurança.

1. Considere a implementação de uma esteira de desenvolvimento seguro.
2. Considere a implementação da gestão de vulnerabilidades para o ambiente externo.
3. Realize testes de segurança na infraestrutura interna.
4. Apoie o time de desenvolvimento com treinamentos focados em desenvolvimento seguro.
5. Realize testes de segurança com foco na organização ex: Red Team e Campanhas de Phishing.

**Nota:** Reforçamos a importância de avaliar cada recomendação no contexto específico da organização, considerando a viabilidade técnica, os recursos disponíveis e os objetivos estratégicos.



## 4. RELATÓRIO TÉCNICO

### 4.1 METASPLOIT

#### Descrição

O Metasploit é uma framework de código aberto que disponibiliza uma ampla coleção de exploits, desenvolvidos para explorar vulnerabilidades específicas em softwares. Além disso, os exploits podem ser personalizados permitindo uma maior flexibilidade. Quando um invasor consegue explorar uma vulnerabilidade, ele pode:

- Injetar e executar códigos maliciosos no sistema, ganhando controle total ou parcial sobre o ambiente comprometido.
- Instalar backdoors, que são acessos ocultos ao sistema, permitindo o retorno futuro ao ambiente comprometido sem detecção.
- Desabilitar firewalls, antivírus, ou outros mecanismos de proteção para facilitar a manutenção do controle sobre o sistema.
- Usar o sistema comprometido como um ponto de partida para acessar outros sistemas na rede, ampliando o alcance do ataque.

**Severidade:** Crítico

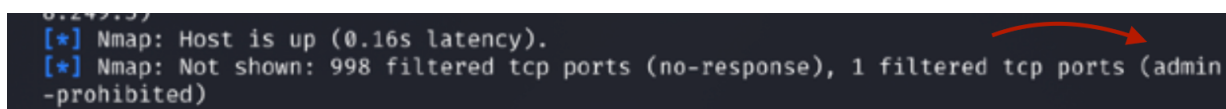
**Base Score:** CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

#### Ativos Afetados:

- <http://testphp.vulnweb.com/admin>
  - Parâmetro: admin

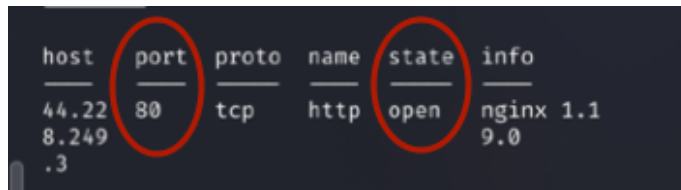
#### Demonstração

Fazendo uso da ferramenta *METASPLOIT* o analista conseguiu explorar a vulnerabilidade no terminal comprometendo o parâmetro ‘admin’, porta aberta, hosts presente na rede, e mantendo uma conexão constante. Segue abaixo ferramenta em execução divulgando o link privado “admin-prohibited”:



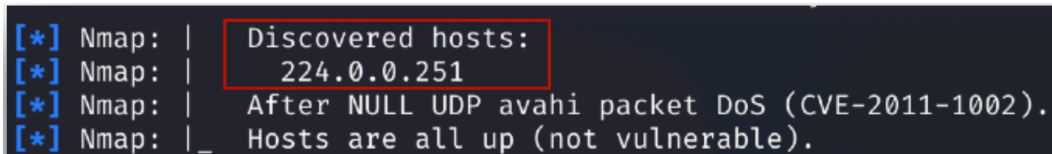
```
0.249.137
[*] Nmap: Host is up (0.16s latency).
[*] Nmap: Not shown: 998 filtered tcp ports (no-response), 1 filtered tcp ports (admin-prohibited)
```

A segunda evidência mostra o resultado da porta aberta encontrada:



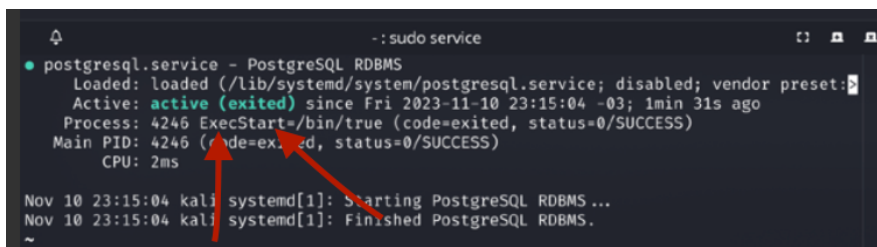
host	port	proto	name	state	info
44.228.249.3	80	tcp	http	open	nginx 1.19.0

A terceira evidência mostra o resultado do escaneamento de hosts:



```
[*] Nmap: | Discovered hosts:
[*] Nmap: | 224.0.0.251
[*] Nmap: | After NULL UDP avahi packet DoS (CVE-2011-1002).
[*] Nmap: |_ Hosts are all up (not vulnerable).
```

A quarta evidência mostra o resultado da conexão constante utilizando um servidor para capturar informações sensíveis:



```
~$ sudo service postgresql.service
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: en
   Active: active (exited) since Fri 2023-11-10 23:15:04 -03; 1min 31s ago
     Process: 4246 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
    Main PID: 4246 (code=exited, status=0/SUCCESS)
       CPU: 2ms

Nov 10 23:15:04 kali systemd[1]: Starting PostgreSQL RDBMS...
Nov 10 23:15:04 kali systemd[1]: Finished PostgreSQL RDBMS.
```

## **Recomendações**

Para defesa mais eficaz contra ataques de metasploit, é importante seguir algumas práticas de segurança:

- Atualizações frequentemente contêm correções de segurança que protegem contra vulnerabilidades exploradas por scripts maliciosos.
- Evitar clicar em links de sites suspeitos ou desconhecidos. Sites maliciosos podem injetar scripts prejudiciais em seu navegador sem que você perceba.
- Em sites que você não confia completamente, limite permissões para cookies e a execução de scripts.

## **Referências**

- <https://owasp.org/www-community/attacks/xss/>
- <https://developer.mozilla.org/en-US/docs/Web/Security>

## 4.2 XSS

### Descrição

XSS é uma ferramenta automatizada que ajuda a identificar, explorar, ou documentar vulnerabilidades em sistemas de computadores ou redes. Ele é desenvolvido para realizar tarefas repetitivas, economizando tempo e garantindo precisão. Quando um invasor consegue explorar uma vulnerabilidade de SCRIPT, ele pode:

- O invasor pode executar comandos no servidor, controlando-o remotamente e obtendo acesso a recursos críticos.
- Pode obter permissões elevadas, ganhando acesso a dados sensíveis e funcionalidades restritas.
- Extrair informações confidenciais, como credenciais de usuário, dados financeiros ou propriedade intelectual.
- Em alguns casos, pode instalar malwares ou backdoors, garantindo acesso contínuo ao sistema para futuras explorações ou ataques.

**Severidade:** Crítico

**Base Score:** CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:H/RL:W

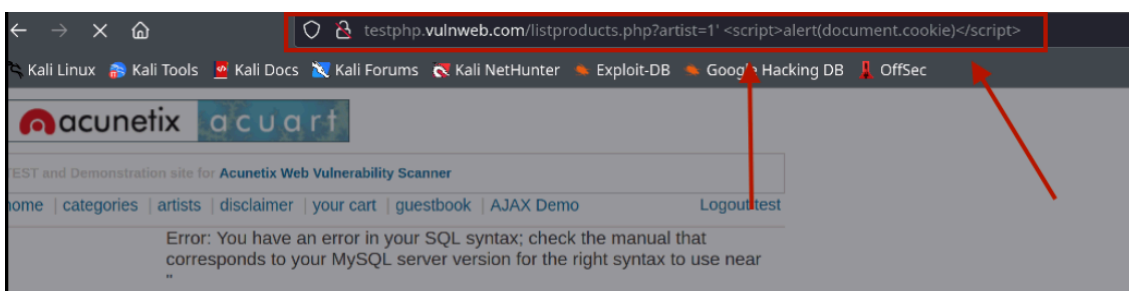
### Ativos Afetados:

- <http://testphp.vulnweb.com/artists>
  - Parâmetro: artists

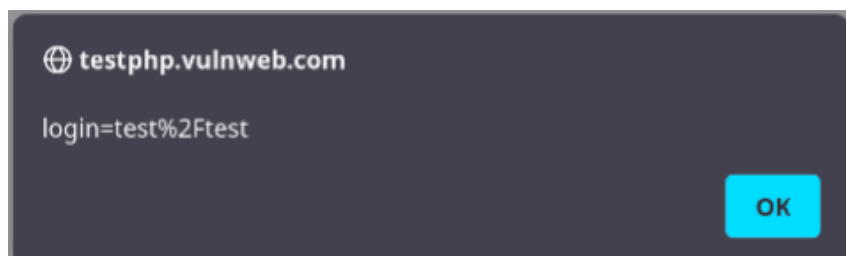
### Demonstração

Fazendo uso da ferramenta XSS o analista conseguiu explorar a vulnerabilidade no parâmetro 'artist' executando a seguinte linha de commando:

```
testphp.vulnweb.com/listproducts.php?artist=1' <script>alert(document.cookie)</script>
```



A segunda evidência mostra o resultado do commando acima onde foi passado um código na URL, retornando o cookie de sessão “login == teste”:



A terceira evidência mostra o resultado do *login* utilizando a credencial encontrada:

If you are already registered please enter your login information below:

Username :	<input type="text" value="test"/>
Password :	<input type="password" value="...."/>
<input type="button" value="login"/>	

A quarta evidência demonstra o resultado de um *login* realizado com sucesso, o que resultou no acesso completo a dados sensíveis, como números de cartões de crédito e endereços. Além disso, foi possível editar essas informações, comprometendo assim a integridade dos dados:

ORIGINAL	MODIFICADO
<b>John Smith (test)</b>	<b>jade Samanta (test)</b>
On this page you can visualize or edit you user information.	
Name: <input type="text" value="John Smith"/>	Name: <input type="text" value="jade Samanta"/>
Credit card number: <input type="text" value="1234-5678-2300-9000"/>	Credit card number: <input type="text" value="1234-5678-2300-9000"/>
E-Mail: <input type="text" value="email@email.com"/>	E-Mail: <input type="text" value="banabuiu@email.com"/>
Phone number: <input type="text" value="2323345"/>	Phone number: <input type="text" value="399992222"/>
Address: <input type="text" value="21 street"/>	Address: <input type="text" value="central park street"/>
<input type="button" value="update"/>	<input type="button" value="update"/>

## **Recomendações**

Para defesa mais eficaz contra ataques de um XSS malicioso, é importante seguir algumas práticas de segurança:

- Atualizações frequentemente contêm correções de segurança que protegem contra vulnerabilidades exploradas por scripts maliciosos.
- Evitar clicar em links de sites suspeitos ou desconhecidos. Sites maliciosos podem injetar scripts prejudiciais em seu navegador sem que você perceba.
- Restringir o acesso e a disponibilidade do site, garantindo que as conexões não sejam mantidas por tempo prolongado, de modo assim, reduzindo a janela de oportunidade para o invasor.

## **Referências**

- <https://owasp.org/www-community/attacks/xss/>
- <https://developer.mozilla.org/en-US/docs/Web/Security>

## 4.3 NMAP

### Descrição

NMAP é uma ferramenta de código aberto que mapeia as redes, dentro de um terminal, identificando dispositivos, serviços e vulnerabilidades. Ele realiza varreduras para mapear a topologia da rede, identificar portas abertas e verificar a presença de possíveis ameaças. Quando um invasor consegue reconhecer uma vulnerabilidade de NMAP, ele pode:

- Identificar serviços e sistemas em execução, o que pode revelar detalhes sobre a infraestrutura e possíveis pontos fracos.
- Usar as informações obtidas para planejar e executar ataques direcionados, como exploração de vulnerabilidades específicas.
- Com informações detalhadas sobre a rede, pode comprometer sistemas e serviços, causando danos ou interrupções.
- Utilizar as informações para se mover lateralmente na rede e comprometer outros sistemas ou serviços.

**Severidade:** Médio

**Base Score:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:H/RL:T/RC:C

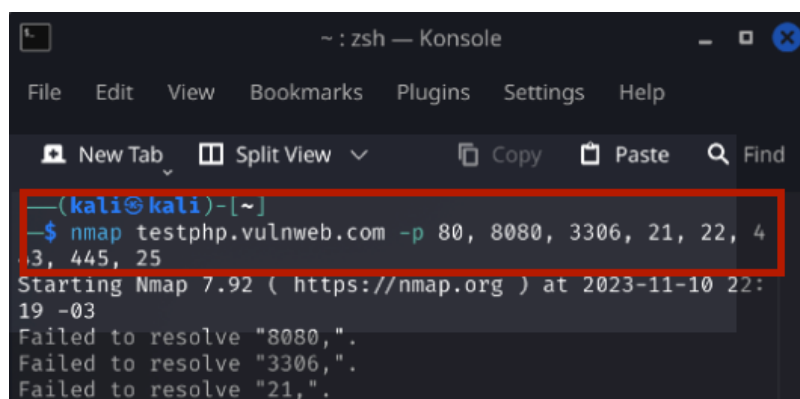
### Ativos Afetados:

- <http://testphp.vulnweb.com>

### Demonstração

Fazendo uso da ferramenta *NMAP* o analista conseguiu explorar a vulnerabilidade de no terminal executando a seguinte linha de comando:

```
nmap http://testphp.vulnweb.com -p 80, 8080, 3306, 21, 22, 443, 445, 25
```



The screenshot shows a terminal window titled '~ : zsh — Konsole'. The command prompt is '(kali@kali)~[~]'. The command entered is '\$ nmap testphp.vulnweb.com -p 80, 8080, 3306, 21, 22, 443, 445, 25'. The output shows 'Starting Nmap 7.92 ( https://nmap.org ) at 2023-11-10 22:19 -03' followed by three lines of error messages: 'Failed to resolve "8080,".', 'Failed to resolve "3306,".', and 'Failed to resolve "21,".'.

A próxima evidência mostra o resultado do commando acima executado, verificando o estado das portas, retornando uma porta http aberta “PORT STATE SERVICE 80/TCP OPEN HTTP”:



```
Failed to resolve 443, .
Nmap scan report for testphp.vulnweb.com (44.228.249.3)
Host is up (0.19s latency).
rDNS record for 44.228.249.3: ec2-44-228-249-3.us-west-2.
compute.amazonaws.com
PORT      STATE SERVICE
80/tcp    open  http
Nmap done: 2 IP addresses (1 host up) scanned in 3.64 seconds
```

## Recomendações

Para proteger de forma mais eficaz o site de mediamentos maliciosos, é importante seguir algumas práticas de segurança:

- Considere usar firewalls e regras de filtragem para limitar o acesso às portas e serviços expostos, permitindo apenas tráfego necessário.
- Monitore logs de rede e eventos de segurança para identificar e responder a atividades de varredura e tentativas de intrusão.
- Técnicas para dificultar a identificação de serviços e sistemas, como camuflar banners e informações de versão.

## Referências

- <https://encr.pw/owasp-org-nmap>
- [https://nmap.org/man/pt\\_BR/index.html](https://nmap.org/man/pt_BR/index.html)



## 4.4 CYBERCHEF

### Descrição

CyberChef é uma ferramenta online que permite realizar diversas operações de manipulação de dados, como encriptação, descriptografia, conversão de dados, e análise de URL. Oferecendo uma ampla gama de funcionalidades para a cibersegurança e forense digital. Quando um invasor consegue explorar a vulnerabilidade, ele pode:

- Ganhar acesso não autorizado.
- Causar danos ao sistema, passando de um usuário comum para um administrador.
- Alterar, corromper, ou apagar dados importantes para causar prejuízos ao sistema ou à organização.
- Compartilhar ou vender as informações sobre a vulnerabilidade e os métodos de exploração em mercados clandestinos.

**Severidade:** Médio

**Base Score:** CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L/IR:H

### Ativos Afetados:

- <http://testphp.vulnweb.com/>

### Demonstração

Fazendo uso da ferramenta *CYBERCHEF* o analista conseguiu reconhecer a vulnerabilidade na plataforma online. O sistema foi configurado de forma inadequada ou incorreta, resultando em possíveis vulnerabilidades como mau funcionamento ou falha de segurança. Isso pode incluir comprometimento da integridade dos pacotes na rede, congestionamento, falta de atualizações. Segue abaixo a operação utilizada em execução:

Parse ipv4 header

```
Protocol14, EMCON (EMCON)
Header checksumd0e (incorrect, should be cae6)
Source IP address14[.]10[.]14[.]14
Destination IP address10[.]14[.]14[.]12options0a 0c
```

A próxima evidência mostra o resultado de congestionamento na rede que pode afetar o desempenho de diversas atividades realizadas na empresa:

Defang ip adress

```
Differentiated Services Code Point (DSCP)3
Explicit Congestion Notification (ECN)2
Total length2574 bytes
```

## Recomendações

Para defesa mais eficaz contra ataques de operações *Parse ipv4 header* e *Defang ip adress*, é importante seguir algumas práticas de segurança:

- Configurar firewalls para inspecionar e filtrar pacotes com cabeçalhos IPv4 mal formados ou suspeitos.
- Validar e sanitizar as entradas e pacotes recebidos.
- Restringir as contas do servidor web, processo e serviço aos menores privilégios possíveis.
- Remova informações desnecessárias dos cabeçalhos de resposta HTTP relacionadas ao sistema operacional, versão do servidor web e estruturas de aplicativos.

## Referências

- <https://owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/02-checklist/05-checklist>
- <https://blog.bughunt.com.br/o-que-e-checksum/>

## 4.5 FALTA DE CABEÇALHO DE SEGURANÇA

### Descrição

A falta de cabeçalho de segurança em uma página web pode criar vulnerabilidades que podem ser exploradas por atacantes. Quando um invasor consegue explorar uma vulnerabilidade, ele pode:

- Injetar códigos maliciosos no sistema.
- Acessar banco de dados.

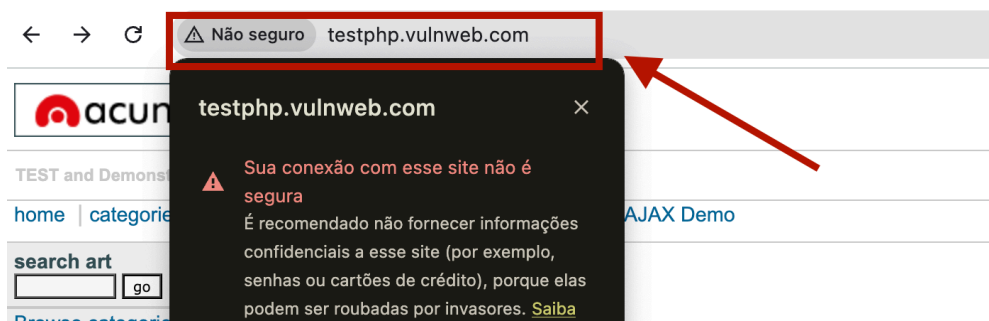
**Severidade:** Informativo

### Ativos Afetados:

- <http://testphp.vulnweb.com/>

### Demonstração

O analista conseguiu reconhecer a vulnerabilidade na URL do site. Segue abaixo a evidência:



### Recomendações

Para defesa mais eficaz contra possíveis ataques na URL, é importante Implementar e configurar corretamente esses cabeçalhos utilizando o HTTPS, essa configuração pode ajudar a proteger uma aplicação web contra várias ameaças comuns.

### Referências

- <https://encr.pw/https-cheatsheetseries-owasp>
- [https://owasp.org/www-community/vulnerabilities/Insecure\\_Transport](https://owasp.org/www-community/vulnerabilities/Insecure_Transport)

## 5. ANEXOS

### 5.1 LISTA DE FERRAMENTAS

Este anexo oferece uma visão detalhada das ferramentas que foram empregadas ao longo do teste de invasão. O propósito deste detalhamento é proporcionar transparência sobre os métodos e técnicas utilizados, permitindo uma melhor compreensão das descobertas apresentadas no relatório principal. Além disso, listar as ferramentas utilizadas pode servir como referência para futuras avaliações, treinamentos internos ou para esclarecimento de dúvidas relacionadas as técnicas aplicadas.

A seguir, apresentamos o catálogo das ferramentas utilizadas, juntamente com uma breve descrição de seu propósito e aplicação no contexto da avaliação.

#	FERRAMENTA	UTILIDADE
1	METASPLOIT	Framework de reconhecimento de vulnerabilidade
2	XSS	Injetar scripts maliciosos em páginas web
3	NMAP	Enumeração de portas expostas
4	CYBERCHEF	Análise e manipulação de dados

**Nota:** É importante ressaltar que, embora essas ferramentas sejam poderosas em mãos experientes, elas são apenas um aspecto do teste. A habilidade, experiência e intuição do avaliador são cruciais para interpretar os resultados e conduzir o teste de maneira ética e responsável.

## 5.2 METODOLOGIA

Ao conduzir um teste de invasão é crucial adotar uma abordagem sistemática e baseada em padrões reconhecidos pela indústria. Para garantir a consistência, eficácia e abrangência de nossa avaliação, baseamos nossa metodologia no **OWASP (Open Web Application Security Project)**, uma entidade renomada que se dedica a melhorar a segurança de software.

Em particular, focamos nossa atenção no **OWASP TOP 10**, uma lista de ameaças e vulnerabilidades mais comuns e críticas em aplicações web. Esta lista, atualizada regularmente com base nas tendências e dados da indústria, serve como um barômetro para a saúde e robustez da segurança de uma aplicação. Ao aderir ao OWASP TOP 10, asseguramos que as vulnerabilidades mais prevalentes e impactantes foram meticulosamente examinadas durante o teste.

Durante nossa avaliação, todos os itens da lista TOP 10 foram verificados. Isso inclui, entre outros, a injeção de SQL, exposição de dados sensíveis, configurações de segurança incorretas e problemas de autenticação e sessão. Esta abordagem abrangente garante que os riscos mais comuns e potencialmente prejudiciais sejam identificados e abordados, proporcionando uma visão completa da postura de segurança da aplicação.

A adoção da metodologia OWASP TOP 10 não apenas alinha nossas práticas com padrões de segurança globalmente reconhecidos, mas também garante que nossos clientes recebam informações e recomendações relevantes e atualizadas, auxiliando na tomada de decisões informadas sobre a mitigação de riscos.

**OWASP:** <https://owasp.org>

**OWASP TOP 10:** <https://owasp.org/Top10/>

# CybersecurityScenario- Webapp-v1.0\_pt