ISH Tecnologia

Anne Caroline
PENETRATION TESTER

DOCUMENTO CONFIDENCIAL

Classificação: Confidencial
Versão: 1.0
Criado em: 02/10/2023
Revisado em: 06/10/2023

Controle de Versões

Data	Autor	Versão	Descrição
02/10/2023	Anne Caroline	1.0	Versão Inicial
05/10/2023	Anne Caroline	1.1	Revisão Inicial
06/10/2023	Anne Caroline	1.2	Revisão Final
06/10/2023	Anne Caroline	1.3	Versão Final

Classificação: Confidencial
Versão: 1.0
Criado em: 02/10/2023
Revisado em: 06/10/2023

Informações de Contato

Nome	Cargo	Contato
ISH Tecnologia		
ISH Tecnologia	Diretor de Segurança	
Corpo Técnico		
Anne Caroline	Pentester	

Classificação: Confidencial
Versão: 1.0
Criado em: 02/10/2023
Revisado em: 06/10/2023

Índice

Classificação: Confidencial
Versão: 1.0
Criado em: 02/10/2023
Revisado em: 06/10/2023

AVISO LEGAL

O Pentest foi realizado durante o dia **02/10/2023 à 06/10/2023**. As constatações e recomendações refletem as informações coletadas durante a avaliação e estado do ambiente naquele momento e não quaisquer alterações realizadas posteriormente fora deste período.

O trabalho desenvolvido pela **Anne Caroline** NÃO tem como objetivo corrigir as possíveis vulnerabilidades, nem proteger a **ISH Tecnologia** contra ataques internos e externos, nosso objetivo é fazer um levantamento dos riscos e recomendar formas para minimizá-los.

As recomendações sugeridas neste relatório devem ser testadas e validadas pela equipe técnica da empresa **ISH Tecnologia** antes de serem implementadas no ambiente em produção. A **Anne Caroline** não se responsabiliza por essa implementação e possíveis impactos que possam vir a ocorrer em outras aplicações ou serviços.

Classificação: Confidencial
Versão: 1.0
Criado em: 02/10/2023
Revisado em: 06/10/2023

INTRODUÇÃO

A **Anne Caroline** foi contratada para conduzir uma avaliação de segurança (Penetration Testing) no ambiente digital da **ISH Tecnologia.**

A avaliação foi conduzida de maneira a simular um ciberataque à partir da internet com o objetivo de determinar o impacto que possíveis vulnerabilidades de segurança possam ter no que diz respeito à **integridade, disponibilidade e confidencialidade** das informações da empresa contratante.

Os testes foram realizados do dia 02 de outubro de 2023 a 06 de outubro de 2023 e este documento contém todos os resultados.

O método utilizado para a execução do serviço proposto segue rigorosamente as melhores práticas de mercado, garantindo a adequação às normas internacionais de segurança da informação, e os relatórios gerados apontam evidências quanto à segurança do ambiente definido no escopo.

1. METODOLOGIA

Para execução destes trabalhos, a **Anne Caroline** adotou a metodologia OWASP na qual o objetivo é avaliar a segurança de uma aplicação web e identificar vulnerabilidades que podem ser exploradas por atacantes. Essas atividades foram conduzidas através das seguintes etapas:

- Enumeração
- Coleta de Informações
- Varredura
- Exploração
- Documentação

A fase de enumeração permite identificar detalhes sobre os serviços ativos, identificando possíveis versões, fornecedores, usuários e informações que possam ser úteis para o sucesso de um ataque.

A fase de coleta de informações tem como objetivo mapear a superfície de ataque, identificando informações sobre blocos de IP, subdomínios e ambientes digitais de propriedade da **ISH Tecnologia.**

Faixas de IP

Classificação: Confidencial
Versão: 1.0
Criado em: 02/10/2023
Revisado em: 06/10/2023

```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#


NetRange:       66.94.96.0 - 66.94.127.255
CIDR:           66.94.96.0/19
NetName:        CONTA-48
NetHandle:      NET-66-94-96-0-1
Parent:         NET66 (NET-66-0-0-0-0)
NetType:        Direct Allocation
OriginAS:       AS40021
Organization:   Contabo Inc. (CONTA-48)
RegDate:        2021-07-28
Updated:        2023-05-16
Ref:            https://rdap.arin.net/registry/ip/66.94.96.0



OrgName:        Contabo Inc.
OrgId:          CONTA-48
Address:        710 N Tucker Blvd. STE 400A
City:           St. Louis
StateProv:      MO
PostalCode:     63101
Country:        US
RegDate:        2019-12-23
Updated:        2023-04-05
Ref:            https://rdap.arin.net/registry/entity/CONTA-48


OrgTechHandle: CONTA392-ARIN
OrgTechName:   Contabo Tech
OrgTechPhone:  +498921268372
OrgTechEmail:  wilhelm.zwalina@contabo.de
OrgTechRef:    https://rdap.arin.net/registry/entity/CONTA392-ARIN

OrgAbuseHandle: CAD61-ARIN
OrgAbuseName:   Contabo Abuse Department
OrgAbusePhone:  +498921268372
OrgAbuseEmail:  abuse@contabo.de
OrgAbuseRef:    https://rdap.arin.net/registry/entity/CAD61-ARIN
```

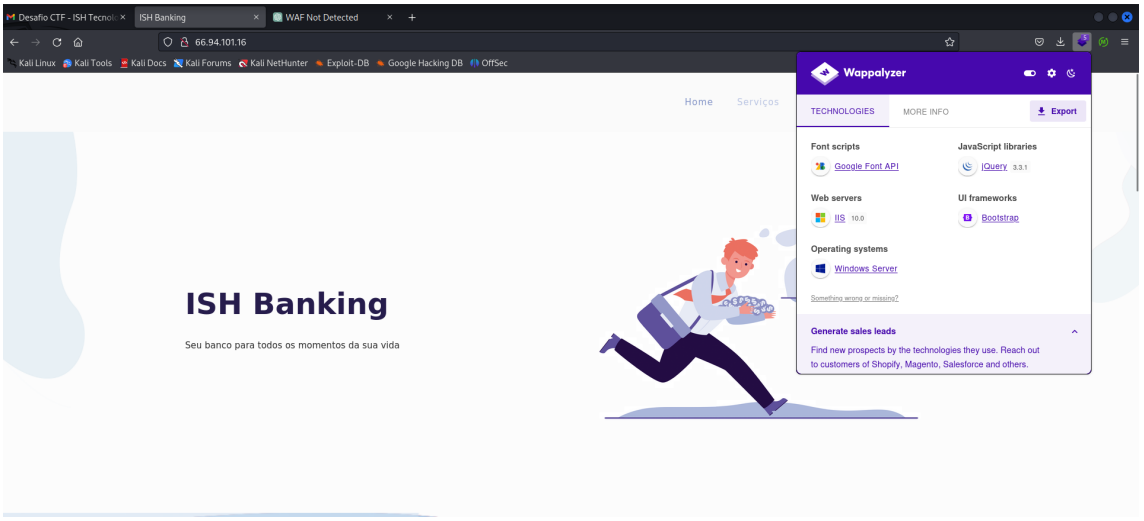
Classificação: Confidencial
Versão: 1.0
Criado em: 02/10/2023
Revisado em: 06/10/2023

```
OrgRoutingHandle: CONTA393-ARIN
OrgRoutingName:   Contabo NOC
OrgRoutingPhone:  +498921268372
OrgRoutingEmail:  sascha.wintz@contabo.com
OrgRoutingRef:    https://rdap.arin.net/registry/entity/CONTA393-ARIN

OrgNOCHandle: CONTA393-ARIN
OrgNOCName:   Contabo NOC
OrgNOCPhone:  +498921268372
OrgNOCEmail:  sascha.wintz@contabo.com
OrgNOCRef:    https://rdap.arin.net/registry/entity/CONTA393-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2023, American Registry for Internet Numbers, Ltd.
#
```

Tecnologias do site




```
┌──# cat whatweb.txt
http://66.94.101.16 [200 OK] Bootstrap, Country[UNITED STATES][US], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[66.94.101.16], JQuery, Microsoft-IIS[10.0], Scr
ipt, Title[ISH Banking]
```

A fase de varredura consiste em identificar portas abertas, serviços ativos e possíveis mecanismos de defesa.

Portas Abertas e Suas Versões

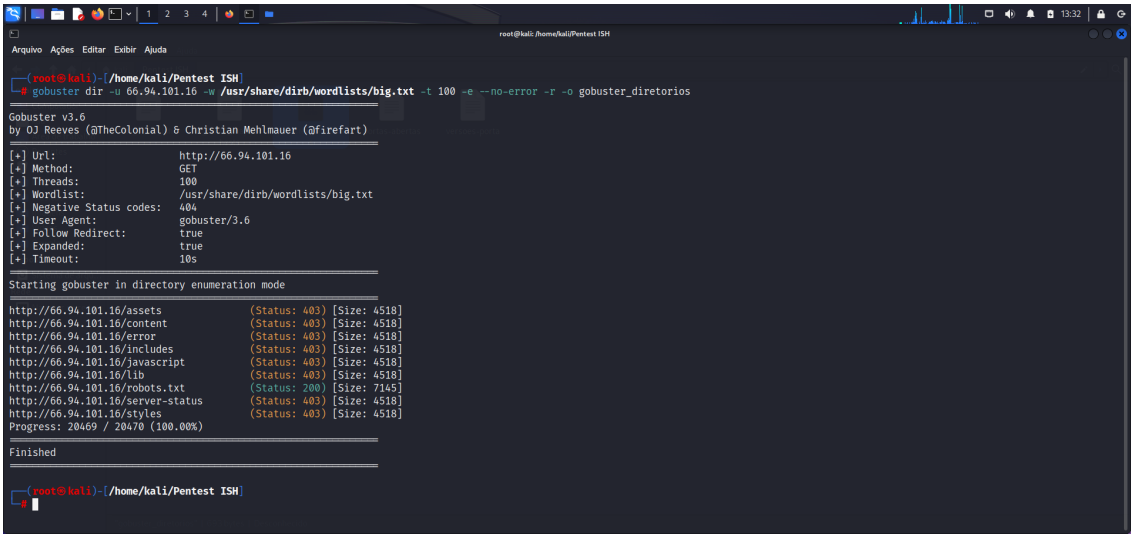
Classificação: Confidencial
Versão: 1.0
Criado em: 02/10/2023
Revisado em: 06/10/2023

```
# Nmap 7.93 scan initiated Tue Oct  3 13:19:05 2023 as: nmap --open -sV -p80,21,554 -oN versoes-porta 66.94.101.16
Nmap scan report for vmi672037.contaboserver.net (66.94.101.16)
Host is up (0.015s latency).

PORT    STATE SERVICE    VERSION
21/tcp  open  tcpwrapped
80/tcp  open  http       Microsoft IIS httpd 10.0
554/tcp open  tcpwrapped
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Oct  3 13:21:16 2023 -- 1 IP address (1 host up) scanned in 131.44 seconds
```

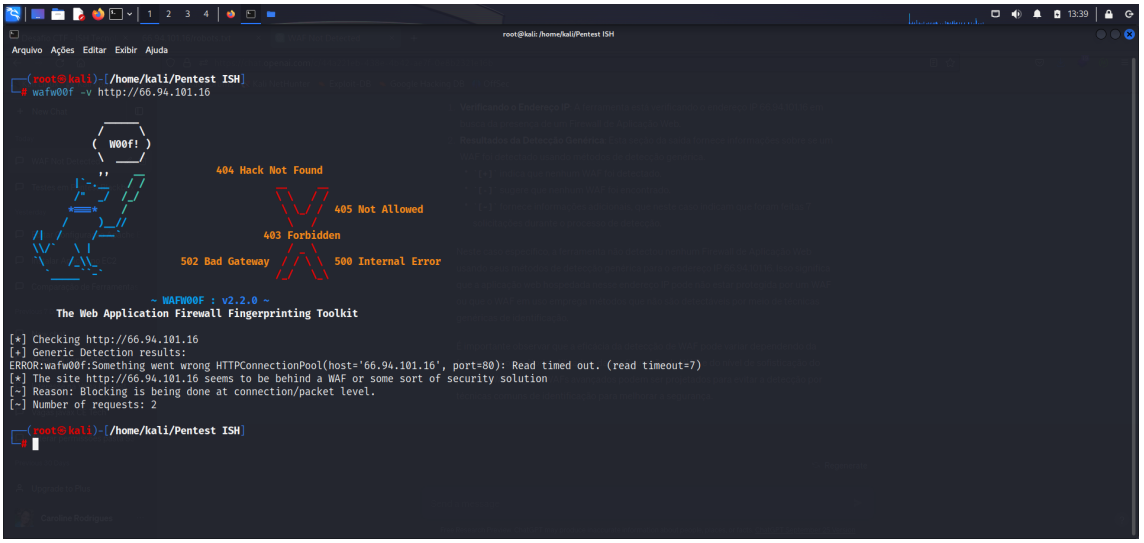
Diretórios Encontrados



Vulnerabilidades Identificadas com Nikto

Varredura de Firewall

Classificação: Confidencial
Versão: 1.0
Criado em: 02/10/2023
Revisado em: 06/10/2023



A fase de exploração tem como objetivo explorar as possíveis vulnerabilidades identificadas nos serviços e sistemas identificados nas fases anteriores e obter acesso ao sistema.

A fase de documentação consiste em relatar todos os resultados obtidos nas fases anteriores.

2. ESCOPO

Tipo de Avaliação	URL
Pentest Black Box Externo	http://66.94.101.16

De acordo com o combinado e acordado entre as partes, a avaliação escolhida foi do tipo **Black Box (sem conhecimento de informações)**, ou seja, a única informação oferecida pela **ISH Tecnologia** foi uma URL.

LIMITAÇÕES DO ESCOPO

As limitações impostas pela **ISH Tecnologia** foram:

- Ataques DoS e DDoS (Negação de Serviço).

3. EXECUTIVO

A **Anne Caroline** avaliou a postura de segurança do item http://66.94.101.16 através de um Pentest Externo no dia 03 de outubro de 2023. Os resultados das avaliações efetuadas no ambiente a partir da internet demonstram que a empresa possui alguns riscos cibernéticos com a presença de vulnerabilidades de níveis CRíTICOS que comprometem a integridade e o sigilo de informações sensíveis.

É altamente recomendável que a **ISH Tecnologia** resolva as vulnerabilidades classificadas como críticas com alta prioridade para que não haja um impacto negativo para os negócios, visto a criticidade das vulnerabilidades encontradas e passíveis de serem exploradas através da internet.

A tabela abaixo resume as principais vulnerabilidades e riscos encontrados durante os testes realizados:

PRINCIPAIS RISCOS				
Alvo	Crítica	Alta	Média	Baixo
http://66.94.101.16	6			

4. NARRATIVA DA ANÁLISE TÉCNICA

Os testes iniciaram no dia 02/10/2023 de posse apenas do endereço do domínio informado pelo cliente. (http://66.94.101.16).

Configuração Incorreta Entre Domínios

Status	Severidade	Score CVSS
Identificada	**Crítica**	**10**
Vetor	http://66.94.101.16	
Vulnerabilidade	Configuração Incorreta Entre Domínios	
CWE ID	CWE-264: Permissions, Privileges, and Access Controls	
CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
Referências	https://vulncat.fortify.com/en/detail?id=desc.config.dotnet.html5_overly_permissive_cors_policy https://chandanbn.github.io/cvss/#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	

Recomendação

- Seguir as melhores práticas de segurança. Essas práticas incluem:
  - Um DNS seguro que utiliza criptografia para proteger o tráfego de rede;
  - Os firewalls devem ser configurados para bloquear o acesso não autorizado a recursos;
  - Uma autenticação forte deve ser usada para verificar a identidade de um usuário.

Descrição

A configuração incorreta entre domínios é uma vulnerabilidade que ocorre quando as configurações de segurança entre dois domínios não são aplicadas corretamente. Isso pode permitir que um atacante acesse dados ou recursos de um domínio que não lhe pertence. Essa vulnerabilidade pode ocorrer devido a uma variedade de fatores, incluindo:

- Falhas na configuração de DNS;
- Falhas na configuração de firewalls;
- Falhas na configuração de autenticação.

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 80 66.94.101.16 --script http-enum
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-06 12:40 -03
Nmap scan report for vmi672037.contaboserver.net (66.94.101.16)
Host is up (0.027s latency).

PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|_  /robots.txt: Robots file

Nmap done: 1 IP address (1 host up) scanned in 7.73 seconds
```

Cabeçalho da Política de Segurança de Conteúdo (CSP) Não Definido

Status	Severidade	Score CVSS
Identificada	**Crítica**	**10**
Vetor	http://66.94.101.16	
Vulnerabilidade	Content Security Policy (CSP) Header Not Set	
CWE ID	CWE-693: Protection Mechanism Failure	
CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
Referências	https://owasp.org/Top10/A05_2021-Security_Misconfiguration/ https://cwe.mitre.org/data/definitions/693.html https://owasp.org/www-project-secure-headers/ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)?redirectedfrom=MSDN https://chandanbn.github.io/cvss/#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	

Recomendação

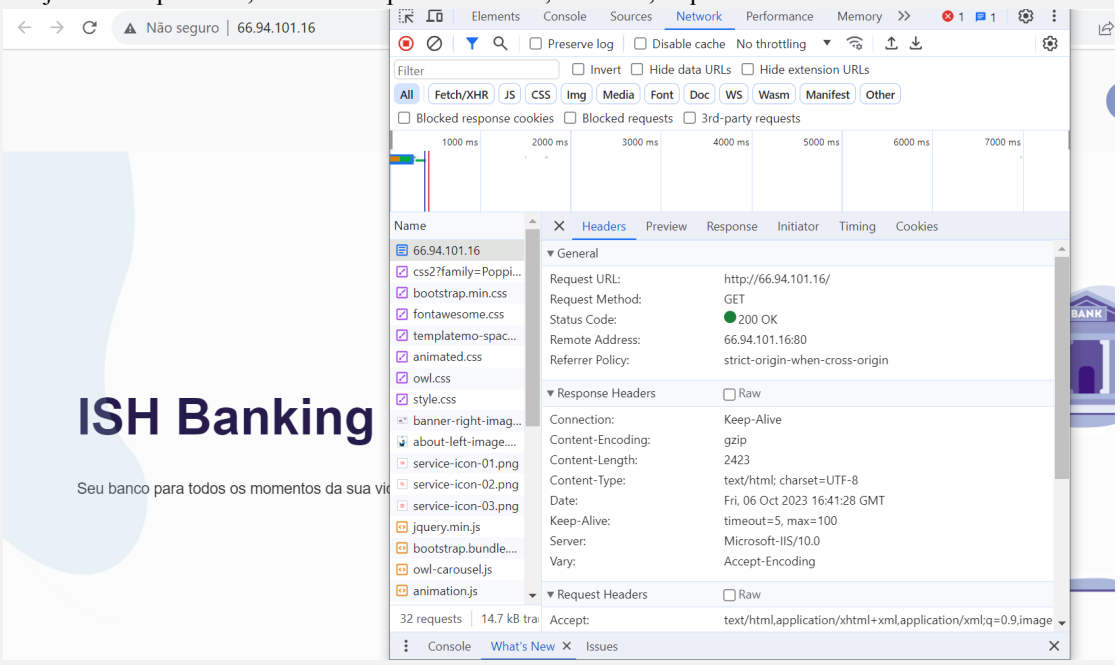
- Certifique-se de que seu servidor web, servidor de aplicativos, balanceador de carga, etc. esteja configurado para definir o cabeçalho Content-Security-Policy. Configurar a Política de Segurança de Conteúdo envolve adicionar o cabeçalho HTTP Content-Security-Policy a uma página da web e fornecer valores para controlar quais recursos o agente do usuário tem permissão para carregar para essa página.

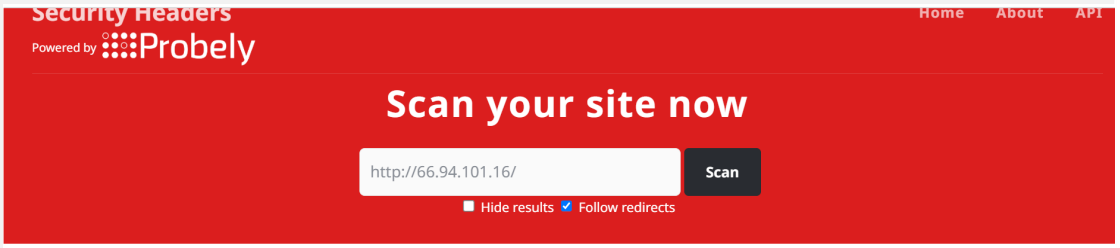
```
<system.webServer>
  <httpProtocol>
    <customHeaders>
      <add name="Content-Security-Policy" value="default-src 'self';" />
    </customHeaders>
  </httpProtocol>
</system.webServer>
```

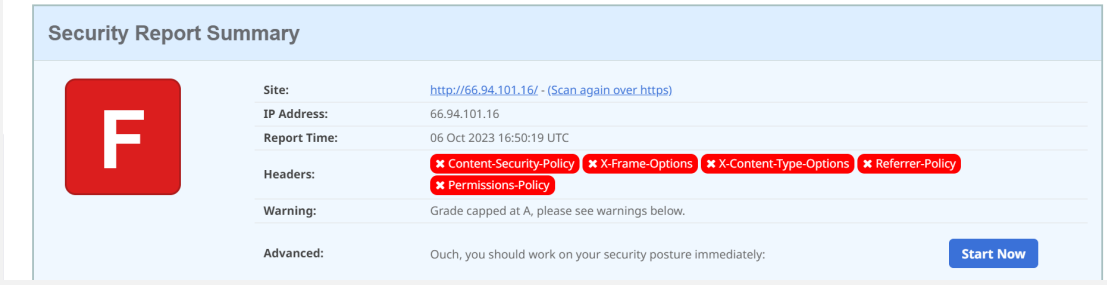
Descrição

Classificação: Confidencial
Versão: 1.0
Criado em: 02/10/2023
Revisado em: 06/10/2023

A Política de Segurança de Conteúdo (CSP) é uma camada adicional de segurança que ajuda a detectar e mitigar certos tipos de ataques, incluindo Cross Site Scripting (XSS) e ataques de injeção de dados. Esses ataques têm uma ampla gama de finalidades, desde roubo de dados até destruição de sites ou distribuição de malware. O CSP fornece um conjunto de cabeçalhos HTTP padrão que permitem aos proprietários de sites declarar fontes aprovadas de conteúdo que os navegadores devem ter permissão para carregar naquela página - os tipos cobertos são JavaScript, CSS, quadros HTML, fontes, imagens e objetos incorporáveis, como miniaplicativos Java, ActiveX, arquivos de áudio e vídeo.







Cabeçalho Anti-Clickjacking Ausente

Status	Severidade	Score CVSS

Identificada	**Crítica**	**10**
Vetor	http://66.94.101.16	
Vulnerabilidade	Missing Anti-clickjacking Header	
CWE ID	CWE-1021: Improper Restriction of Rendered UI Layers or Frames	
CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
Referências	https://cwe.mitre.org/data/definitions/1021.html https://owasp.org/Top10/A05_2021-Security_Misconfiguration/ https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/11-Client-side_Testing/09-Testing_for_Clickjacking https://chandanbn.github.io/cvss/#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	

Recomendação

- Navegadores da Web modernos suportam os cabeçalhos HTTP X-Frame-Options. É importante garantir que eles estejam definidos em todas as páginas da web retornadas pelo site. Se a intenção é permitir que a página seja enquadrada apenas por páginas do servidor (por exemplo, como parte de um FRAMESET), a opção recomendada é usar 'SAMEORIGIN'. Por outro lado, se não se espera que a página seja enquadrada em nenhum contexto, a opção adequada é 'DENY'.

- Recomendo também reforçar a segurança dos cabeçalhos HTTP com as seguintes configurações:
  - X-XSS-Protection: Essa medida visa proteger contra ataques de script entre sites (XSS).
  - Strict-Transport-Security: Esta configuração é fundamental para forçar o uso de HTTPS e proteger contra ataques de interceptação de tráfego.

```html
<!DOCTYPE html>
<html>

<head>
    <!-- Configurando o cabeçalho HTTP X-Frame-Options como DENY -->
    <meta http-equiv="X-Frame-Options" content="DENY">
    <title>Exemplo de CSP</title>
    <!-- Resto do código HTML -->
</head>

<body>
    <!-- Conteúdo da página -->
</body>

</html>
```

Descrição

Clickjacking é um ataque que induz um usuário a clicar em algo que ele não pretendia clicar. Isso pode ser feito sobrepondo uma camada transparente sobre uma página da web, que é invisível para o usuário, mas contém os links ou botões maliciosos.

Biblioteca JS vulnerável

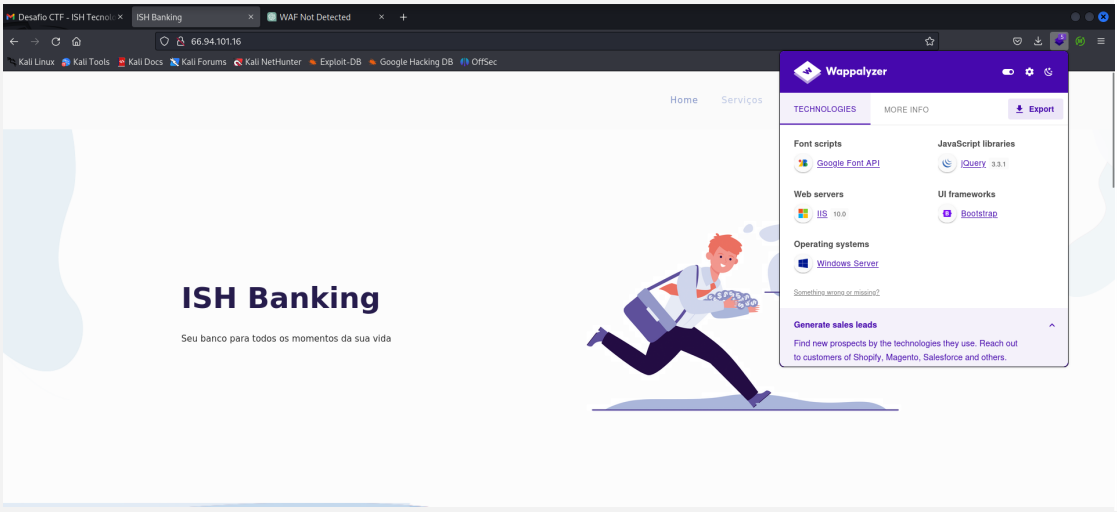
Status	Severidade	Score CVSS
Identificada	**Crítica**	**10**
Vetor	http://66.94.101.16/assets/vendor/jquery/jquery.min.js	
Vulnerabilidade	Vulnerable JS Library	
CWE ID	CWE-829: Inclusion of Functionality from Untrusted Control Sphere	
CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
Referências	https://cwe.mitre.org/data/definitions/829.html https://blog.jquery.com/2023/08/28/jquery-3-7-1-released-reliable-table-row-dimensions/ https://nvd.nist.gov/vuln/detail/CVE-2019-11358 https://chandanbn.github.io/cvss/#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	

Recomendação

- Atualizar a biblioteca para a versão mais recente estável (v3.7.1) - https://code.jquery.com/jquery-3.7.1.min.js

Descrição

O jQuery antes da versão 3.4.0, utilizado no Drupal, Backdrop CMS e outros produtos, lida incorretamente com jQuery.extend(true, {}, ...) devido à poluição do Object.prototype. Se um objeto de origem não sanitizado contivesse uma propriedade __proto__ enumerável, poderia estender o Object.prototype nativo.
A vulnerabilidade JS Library é uma vulnerabilidade de segurança que pode ser explorada para executar código optativo em um sistema que usa uma biblioteca JavaScript vulnerável. A vulnerabilidade ocorre porque a biblioteca JavaScript não trata corretamente os objetos de origem não sanitizada.



Servidor Vaza Informações De Versão Por Meio Do Campo De Cabeçalho De Resposta Http “Server”

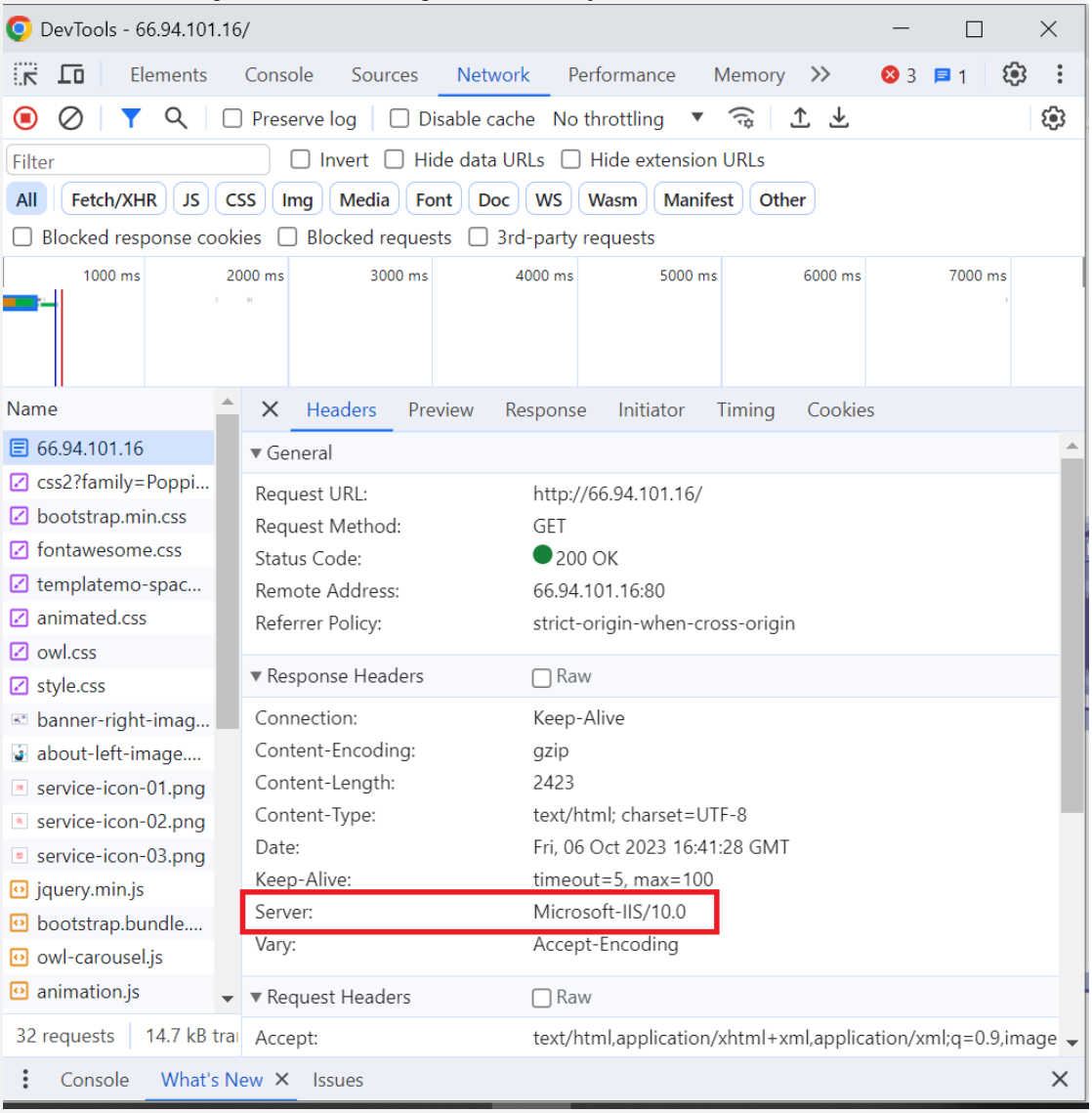
Status	Severidade	Score CVSS
Identificada	**Crítica**	**10**
Vetor	http://66.94.101.16	
Vulnerabilidade	Server Leaks Version Information via "Server" HTTP Response Header Field	
CWE ID	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	
CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L	
Referências	https://cwe.mitre.org/data/definitions/200.html https://owasp.org/Top10/A05_2021-Security_Misconfiguration/ https://owasp.org/www-project-web-security-testing-guide/v42/4-Web_Application_Security_Testing/01-Information_Gathering/02-Fingerprint_Web_Server https://chandanbn.github.io/cvss/#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:L	

Recomendação

- Certifique-se de que a configuração do servidor web, servidor de aplicativos, balanceador de carga, etc., esteja definida para ocultar o cabeçalho 'Server' ou para fornecer informações genéricas.
- A configuração para controlar a divulgação de informações de versão no cabeçalho "Server" de um servidor web pode variar de acordo com o software do servidor que está sendo utilizado, como o Apache ou o Nginx. Essas configurações são específicas para cada servidor e devem ser ajustadas diretamente nas configurações do servidor web escolhido.

Descrição

O servidor web/aplicativo está vazando informações de versão por meio do cabeçalho de resposta HTTP "Server". O acesso a essas informações pode facilitar que invasores identifiquem outras vulnerabilidades às quais servidor web/aplicativo está sujeito.



Cabeçalho X-Content-Type-Options Ausente

Status	Severidade	Score CVSS
Identificada	**Crítica**	**10**
Vetor	http://66.94.101.16	
Vulnerabilidade	X-Content-Type-Options Header Missing	
CWE ID	CWE-693: Protection Mechanism Failure	
CVSS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
Referências	https://cwe.mitre.org/data/definitions/693.html https://owasp.org/Top10/A05_2021-Security_Misconfiguration/	

	https://owasp.org/www-project-secure-headers/ https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85)?redirectedfrom=MSDN https://chandanbn.github.io/cvss/#CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Recomendação

- Certifique-se de que o cabeçalho X-Content-Type-Options com o valor "nosniff" esteja sendo enviado para todas as páginas do site. Essa medida pode ser implementada através da configuração no servidor web ou no aplicativo da web.

Descrição

A vulnerabilidade X-Content-Type-Options Header Missing é uma vulnerabilidade de segurança que ocorre quando um site não envia o cabeçalho HTTP X-Content-Type-Options com o valor nosniff. Este cabeçalho é usado para informar ao navegador que ele deve confiar no tipo de conteúdo especificado no cabeçalho Content-Type em vez de tentar deduzir o tipo de conteúdo com base no próprio conteúdo do arquivo.

```html
<!DOCTYPE html>
<html>

<head>
    <!-- Configurando o cabeçalho HTTP X-Content-Type-Options como nosniff -->
    <meta http-equiv="X-Content-Type-Options" content="nosniff">
    <title>Exemplo de CSP</title>
    <!-- Resto do código HTML -->
</head>

<body>
    <!-- Conteúdo da página -->
</body>

</html>
```

```
<httpProtocol>
  <customHeaders>
    <add name="X-Content-Type-Options" value="nosniff" />
  </customHeaders>
</httpProtocol>
```

5. CONCLUSÃO

Conforme definido no escopo, os testes deveriam encerrar até a data limite definida pelo **ISH Tecnologia.**

Limpeza de Rastros

Após a coleta das informações e evidências acima demonstradas, restauramos os sistemas exatamente conforme encontramos.

6. CONSIDERAÇÕES FINAIS

A realização deste teste de segurança permitiu identificar vulnerabilidades e problemas de segurança que poderiam causar um impacto negativo aos negócios do cliente. Com isso podemos concluir que o teste atingiu o objetivo proposto.

Podemos concluir que a avaliação de segurança como o teste de invasão apresentado neste relatório é fundamental para identificar vulnerabilidades, testar e melhorar controles e mecanismos de defesa a fim de garantir um bom grau de segurança da informação em seu ambiente digital.

Desde já agradeço a ISH Tecnologia pela oportunidade em oferecer meus serviços de segurança ofensiva.

ANEXOS

- 2023-10-03-ZAP-Report-.pdf
- robots.txt
- Evidencias ISH