Apresentação das Regras de WAF

Esta apresentação tem como objetivo a complementação da documentação de apresentação da solução de proteção a aplicações web no ambiente do Cloud, contendo assim, parte do conteúdo inicial como forma de contextualização do cenário em questão.

CONCEITOS BÁSICOS DE PROTEÇÃO DAS FERRAMENTAS

Conforme a própria documentação do provedor, as informações oficiais apresentam explanações abstratas de forma que em detalhes, não possam ser utilizadas por atacantes a fim de contorna-las. Portanto, não haverá grandes detalhes sobre como as regras trabalham em nível de julgamento do tráfego para bloqueio.

REGRAS Básicas

AWSManagedRulesCommonRuleSet

Isso fornece proteção contra a exploração de uma ampla gama de vulnerabilidades, incluindo algumas das vulnerabilidades comuns e de alto risco descritas em publicações do OWASP, como OWASP Top 10.[1]

Em nível de regras, é possível flexibilizar componentes dentro da regra, caso ocorra incompatibilidade com algum recurso da solução web, sendo possível, customizar regras complementares em caso de necessidade.

AWSManagedRulesAmazonIpReputationList

O grupo de regras da lista de reputação de IP da Amazon contém regras baseadas na inteligência de ameaças internas da Amazon. Isso é útil se você quiser bloquear endereços IP normalmente associados a bots ou outras ameaças. Bloquear esses endereços IP pode ajudar a diminuir bots e reduzir o risco de um agente mal-intencionado descobrir um aplicativo vulnerável.[2]

AWSManagedRulesAnonymousIpList

Esse grupo de regras da lista de IPs anônimos contém regras para bloquear solicitações de serviços que permitem a ofuscação da identidade do visualizador. Elas incluem solicitações de VPNs, proxies, nós Tor e provedores de hospedagem. Esse grupo de regras é útil se você quiser filtrar visualizadores que podem estar tentando ocultar a identidade do seu aplicativo.

[1] https://docs.aws.amazon.com/pt_br/waf/latest/developerguide/aws-managed-rule-groups-baseline.html

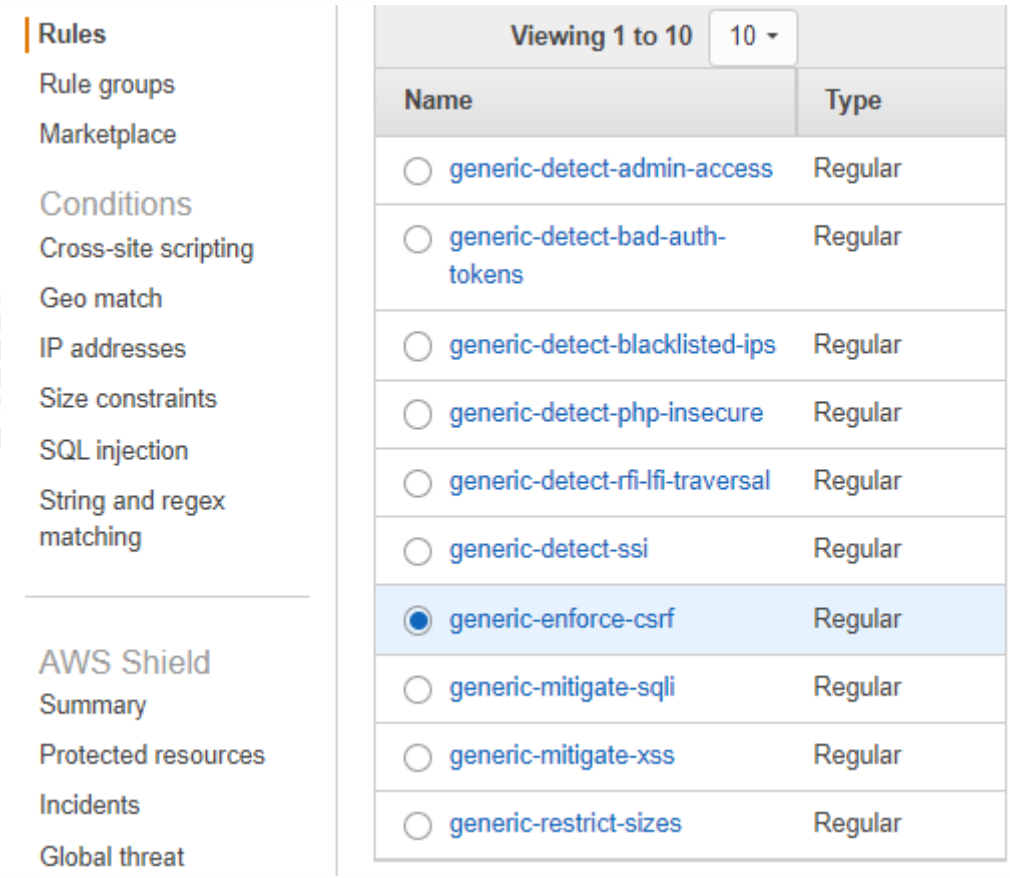
[2] https://docs.aws.amazon.com/pt_br/waf/latest/developerguide/aws-managed-rule-groups-ip-rep.html#aws-managed-rule-groups-ip-rep-amazon

Bloquear os endereços IP desses serviços pode ajudar a mitigar bots e evasão de restrições geográficas.[3]

REGRAS COMPLEMENTARES OU CUSTOMIZÁVEIS

Neste tópico apresento como complemento, informações específicas solicitadas a respeito de um tipo de ataque específico conhecido comumente como CSRF (Cross-site Request Forgery). Importante ressaltar que segundo a OWASP este tipo de ataque não se encontra mais em relatórios TOP 10 desde meados de 2017.[4] O documento referenciado explana tal alteração nas publicações da organização.

A seguir, alguns detalhes sobre a regra relacionada a este ataque presente em nosso ambiente. Observando que estaremos detalhando apenas esta regra por conta dos pré-requisitos solicitados.



No detalhamento a seguir, temos o julgamento do cumprimento do cabeçalho 'x-csrf-token' igual a 36, para métodos post.

[3] https://docs.aws.amazon.com/pt_br/waf/latest/developerguide/aws-managed-rule-groups-ip-rep.html#aws-managed-rule-groups-ip-rep-anonymous
[4] https://github.com/OWASP/Top10/blob/master/2017/OWASP%20Top%2010-2017%20(en).pdf

When a request does not match at least one of the filters in the size constraint condition generic-match-csrf-token
Filters in generic-match-csrf-token
The length of the Header 'x-csrf-token' is equal to 36.

And

When a request matches at least one of the filters in the string match condition generic-match-csrf-method
Filters in generic-match-csrf-method
HTTP method matches exactly to: "post" after converting to lowercase.

Av. Presidente Vargas, 2921
Edifício Sky Towers office
5º Andar - Sala 513 - Vila Homero
Indaiatuba - SP - 13.338-705
(19) 3014-8080
www.datapar.com.br

RELATÓRIO MENSAL DE CYBER SEGURANÇA

11/01/2024

INTRODUÇÃO

Este documento apresenta resultados referentes às políticas e controles de acesso no ambiente no período de 05/12/2023 à 11/01/2024.

A metodologia empregada tem como base a família de normas ISO 27000, bem como adaptações para se enquadrar à legislação vigente: Lei n° 13.709/2018, ou Lei Geral de Proteção de Dados Pessoais.

DESCRIÇÃO

Para facilitar o acompanhamento e compreensão deste documento, são apresentadas as ferramentas utilizadas para manutenção da segurança da informação no ambiente, seguidas de evidências assegurando seu uso.
Em cada um dos tópicos também são detalhadas as finalidades destas mesmas ferramentas, a importância de suas adoções e melhorias que elas trazem.
Por fim, são apresentados os próximos passos para o processo contínuo de melhorias e a conclusão do estado atual do ambiente.

FERRAMENTAS UTILIZADAS NO AMBIENTE

Para assegurar um ambiente que se encaixe nas normas e legislações atuais quanto à segurança da informação, são utilizadas as ferramentas abaixo listadas:

AWS WAF

O AWS WAF é um firewall para aplicações Web que permite monitorar as solicitações HTTP e HTTPS que são encaminhadas ao CloudFront e controlar quem pode acessar seu conteúdo. Com base em condições previamente especificadas, tais como valores de query strings ou endereços IP dos quais as solicitações se originam, o CloudFront responderá às solicitações com o conteúdo solicitado ou com um código de status HTTP 403 (Forbidden). Há também mecanismos que possibilitam o retorno de páginas personalizadas com base em regras de bloqueio.

PFSENSE PLUS

Pfsense Plus é um stateful firewall baseado em rede que rastreia individualmente as sessões de conexões de rede que o atravessam. A inspeção dinâmica de pacotes, também conhecida como filtragem dinâmica de pacotes, é um recurso de segurança usado para invocar políticas de segurança refinadas, elevando os níveis de proteção de uma rede interna, garantindo robustez e segurança nos controles de acesso.

SNORT IDS/IPS

Snort IDS/IPS é um sistema de prevenção a intrusões na rede (intrusion prevention system – IPS) open source, mantido e desenvolvido pela Cisco. A ferramenta se destaca por sua capacidade de analisar tráfegos em tempo real e registrar pacotes de protocolo TCP (Transmission Control Protocol).
Em função dessa versatilidade, o Snort consegue desempenhar o papel de três tipos de aplicações cruciais para monitorar um servidor. Logo, ele pode ser usado como sniffer de pacotes (de modo similar ao tcpdump), como um registrador de pacotes (o que é útil para depuração de tráfego de rede) e / ou um sistema avançado de prevenção à intrusão.

INCIDENTES DE CYBER SEGURANÇA

Sobre os incidentes relacionados a cyber segurança ou infraestrutura do sistema no mês de dezembro, obtivemos uma falha com a solução de CDN.

Executamos os procedimentos para ajuste de acesso e iniciamos o troubleshooting, sendo realizadas correções a nível de aplicação, apenas.

REGRAS DE FILTRAGEM DE PACOTES PFSENSE PLUS FIREWALL

Abaixo constam as regras de controle de acessos configuradas e em execução no Pfsense Plus Firewall:

Rules

		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description
☐	✓	WAN3	TCP/UDP	pfB_ AWSCloudFront_ v4	*	10.0.252.97	TSPLUSPORTS	10.0.1.167	TSPLUSPORTS	TSPLUS4
☐	✓	WAN3	TCP/UDP	DHL	*	10.0.252.97	TSPLUSPORTS	10.0.1.167	TSPLUSPORTS	TSPLUS4_DHL

Regras do firewall Pfsense Plus.

LOGS PFSENSE PLUS FIREWALL

Com o objetivo de realizar o controle de acesso via regras de aceitação / negação, o Pfsense Plus Firewall atua como intermediador analisando os cabeçalhos de todos pacotes, principalmente quanto à origem e destino. Contudo, pode-se obter um refinamento ainda maior com uma grande variedade de possibilidades para filtragem.
Abaixo temos registros de log no firewall Pfsense Plus evidenciando a correta aplicação de regras e negação de acessos indevidos:

1445 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-01-11 15:48:12	⚠	2	TCP	Misc Attack	185.196.8.151	48599	10.0.253.83	22	1:2500020	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 11
2024-01-11 15:38:15	⚠	2	TCP	Misc Attack	185.196.8.151	60678	10.0.253.82	22	1:2500020	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 11
2024-01-11 15:37:12	⚠	1	UDP	Attempted Administrator Privilege Gain	91.92.244.147	58682	10.0.253.85	9034	1:2044008	ET EXPLOIT Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35394)
2024-01-11 15:33:34	⚠	2	TCP	Misc Attack	185.196.8.151	36442	10.0.253.83	22	1:2500020	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 11
2024-01-11 15:30:24	⚠	3	TCP	Unknown Traffic	74.82.47.20	59665	10.0.253.85	80	119:24	(http_inspect) MULTIPLE HOST HDRS DETECTED
2024-01-11 15:12:32	⚠	2	TCP	Misc Attack	185.196.8.151	59116	10.0.253.151	22	1:2500020	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 11
2024-01-11 15:12:02	⚠	3	TCP	Unknown Traffic	64.62.197.115	58909	10.0.253.94	80	119:24	(http_inspect) MULTIPLE HOST HDRS DETECTED
2024-01-11 15:09:36	⚠	2	TCP	Misc Attack	45.95.147.236	48216	10.0.253.151	443	1:2500026	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 14
2024-01-11 14:53:51	⚠	2	UDP	Potentially Bad Traffic	192.241.196.120	55826	10.0.253.94	5060	140:18	(spp_sip) Content length mismatch
2024-01-11 14:53:19	⚠	2	TCP	Misc Attack	185.196.8.151	39697	10.0.253.88	22	1:2500020	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 11

Registros de log no firewall Pfsense Plus: acessos negados de acordo com regras especificadas.

SNORT IDS/IPS

Snort IDS/IPS atua na detecção e prevenção de intrusão, realizando bloqueios em casos de pacotes maliciosos enviados ao Pfsense Plus Firewall.
Abaixo temos evidenciada a configuração e execução do Snort em todas as interfaces de rede do Pfsense Plus Firewall:

Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
☐	WAN2 (ena2)	✔ ↻ ◉	AC-BNFA	LEGACY MODE	WAN2	✎ ⧉ 🗑
☐	WAN3 (ena3)	✔ ↻ ◉	AC-BNFA	LEGACY MODE	WAN3	✎ ⧉ 🗑

Status do Snort IDS/IPS: configurado e em execução em ambas interfaces de rede do Pfsense Plus Firewall.

Na sequência temos uma amostragem de pacotes maliciosos bloqueados pela ferramenta Snort nas interfaces de rede do Pfsense Plus Firewall:

Last 10000 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	89.190.156.40	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 9 -- 2024-01-02 23:42:52 ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 10 -- 2024-01-03 23:58:36	✖
2	74.82.47.32	(http_inspect) MULTIPLE HOST HDRS DETECTED -- 2024-01-09 12:14:35	✖
3	216.218.206.80	(http_inspect) MULTIPLE HOST HDRS DETECTED -- 2024-01-03 15:06:23	✖
4	222.186.16.186	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 7 -- 2024-01-02 13:34:11	✖
5	165.22.58.90	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 4 -- 2024-01-02 00:47:31	✖
6	143.198.91.141	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 3 -- 2024-01-02 00:38:55	✖
7	65.49.1.59	(http_inspect) MULTIPLE HOST HDRS DETECTED -- 2024-01-01 11:53:50	✖
8	159.203.45.248	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 3 -- 2024-01-01 11:58:46	✖
9	216.218.206.123	(http_inspect) MULTIPLE HOST HDRS DETECTED -- 2024-01-03 11:47:17	✖
10	222.186.16.162	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 7 -- 2024-01-02 19:06:33	✖

Bloqueios de pacotes maliciosos realizado pela ferramenta Snort IDS/IPS.

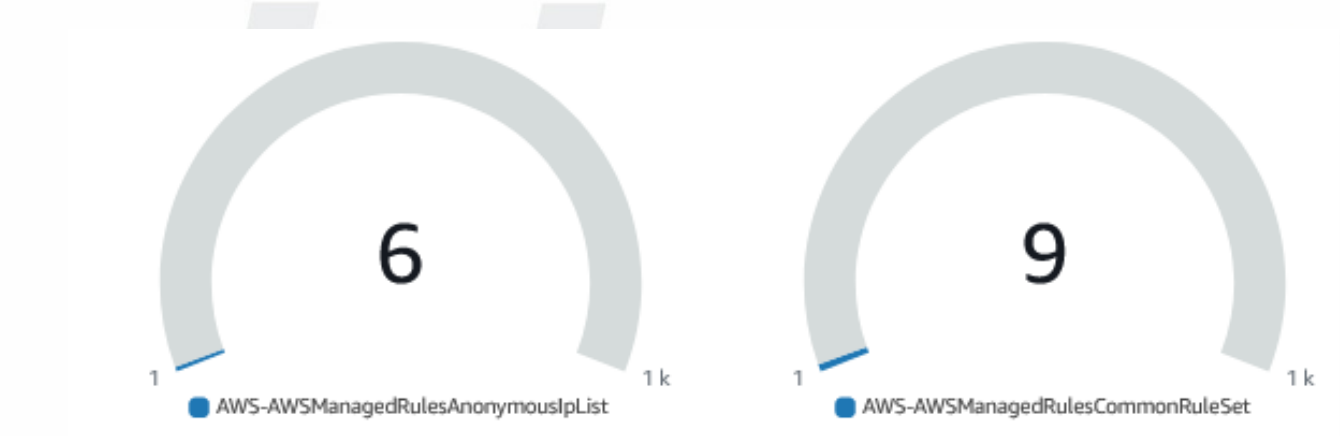
AWS WEB APPLICATION FIREWALL

O WAF, ou firewall de aplicativos web, ajuda a proteger os aplicativos web ao filtrar e o monitorar o tráfego HTTP entre o aplicativo web e a internet. De modo geral, o WAF protege os aplicativos web contra ataques como falsificação de solicitação entre sites, cross-site-scripting (XSS), inclusão de arquivo e injeção de SQL, entre outros. O WAF é uma defesa de protocolo da camada 7 (no modelo OSI). Esse método de mitigação costuma fazer parte de um conjunto de ferramentas que, juntas, criam uma defesa holística contra diversos vetores de ataque.

O AWS Web Application Firewall possui grande robustez e facilidade de implantação e manutenção, assegurando que a aplicação possua níveis adequados e segurança sem impactar no desempenho.

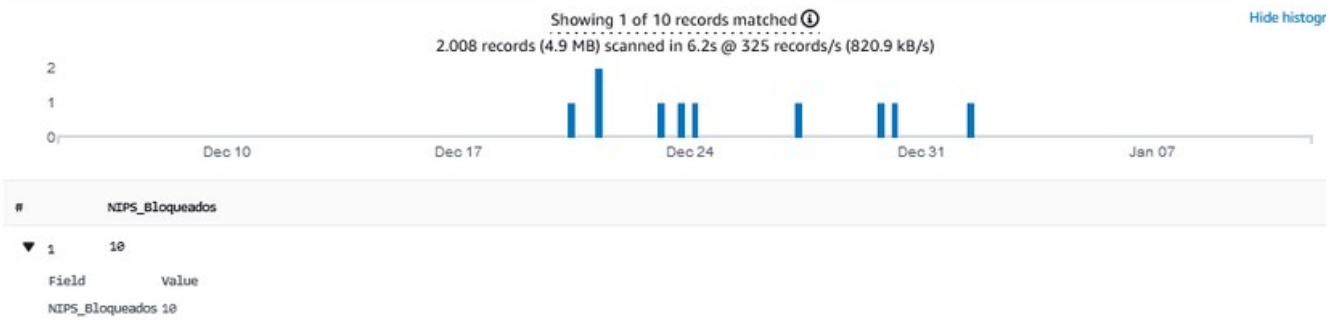
Abaixo podemos observar o conjunto de regras do AWS WAF aplicado ao ambiente DHL:

Abaixo evidências dos eventos tratados e status atual da ferramenta:



Regras do AWS WAF: gráfico contendo quantidade de bloqueios realizados.

A seguir, total de IPs bloqueados no período de 05/12/2023 a 11/01/2024:



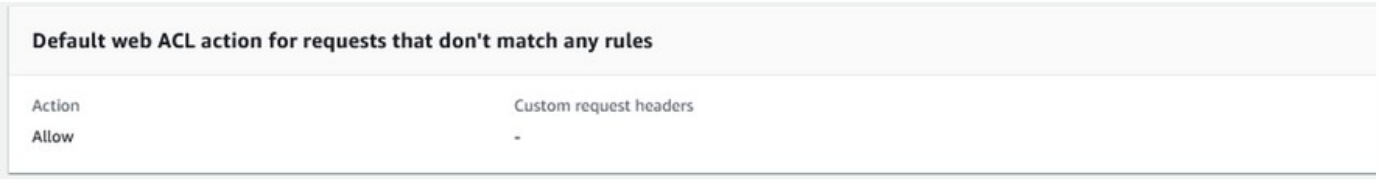
#	NIPS_Bloqueados
▼ 1	10

Field	Value
NIPS_Bloqueados	10

A seguir, evidências de log de bloqueio realizado:

@timestamp	1704116478366
action	BLOCK
formatVersion	1
httpRequest.args	REDACTED
httpRequest.clientIp	198.235.24.11
httpRequest.country	US
httpRequest.headers.0.name	Host
httpRequest.headers.0.value	webcloud4.datapardc.com
httpRequest.httpMethod	REDACTED
httpRequest.httpVersion	HTTP/1.1
httpRequest.requestId	mImH2DfYRI00aBsINQE6CmNQ1esvh1NRA3fQw1HrbIjag1t7o8Q_SQ==
httpRequest.uri	REDACTED
httpSourceId	E19HKCNWGZ9V8V
httpSourceName	CF
ja3Fingerprint	473cd7cb9faa642487833865d516e578
labels.0.name	awswaf:managed:aws:core-rule-set:NoUserAgent_Header
ruleGroupList.0.ruleGroupId	AWS#AWSManagedRulesAmazonIpReputationList
ruleGroupList.1.ruleGroupId	AWS#AWSManagedRulesAnonymousIpList
ruleGroupList.2.ruleGroupId	AWS#AWSManagedRulesCommonRuleSet
ruleGroupList.2.terminatingRule.action	BLOCK
ruleGroupList.2.terminatingRule.ruleId	NoUserAgent_HEADER
terminatingRuleId	AWS-AWSManagedRulesCommonRuleSet
terminatingRuleType	MANAGED_RULE_GROUP
timestamp	1704116478366
webaclId	arn:aws:wafv2:us-east-1: :global/webacl/TSPLUS04/c2b729b1-2d93-4821-bc4d-0d0c15117a0e

Abaixo segue a ACL padrão para requisições que não se enquadrem em nenhuma regra:



Definição da ACL padrão.

INCIDENTES RELACIONADOS A INFRAESTRUTURA

- O ambiente teve direcionados a área de infraestrutura 30 acionamentos no período entre ações de:
  - Aplicação de atualizações em :
    - Sistemas de homologação
    - EDIs.
    - Aplicações integradoras
    - Restart de senha de usuário
- Alteração de configurações em serviços e de uso comum para usuários específicos.

PRÓXIMOS PASSOS

Este relatório será analisado e atualizado de forma mensal, garantindo assim que o ambiente se enquadre às normas e leis vigentes quanto à segurança da informação.
Na necessidade de aplicação de novas ferramentas ou metodologias, este documento permanecerá como documentação de quaisquer alterações realizadas.

CONCLUSÃO

Com a adoção de ferramentas topo de linha para manutenção da segurança do ambiente, garante-se uma proteção de alto nível atendendo às principais normas e legislações vigentes, abrangendo os princípios da confidencialidade, integridade e disponibilidade das informações necessárias ao perfeito funcionamento.
Foram informadas neste relatório as ferramentas utilizadas no ambiente no que tange à busca pela segurança cibernética do ambiente.

Abaixo, listamos estas ferramentas, bem como suas finalidades e status atual:

FERRAMENTA	FINALIDADE	STATUS
Pfsense Firewall	Filtragem de pacotes e controle de acesso	Operacional
Snort IDS/IPS	Detecção e Prevenção de Intrusão	Operacional
AWS Web Application Firewall	Firewall de Aplicação Web	Operacional

WAF – ACESSO WEB VISUAL RODOPAR

MECANISMOS IMPLEMENTADOS PARA PROTEÇÃO DOS RECURSOS WEB

Técnico Responsável: Felipe Neofiti de Carvalho

Para proteção dos recursos expostos à Web foi implantado um **WAF** (*Web Application Firewall*) nativo do provedor de Cloud para melhor integração à infraestrutura e demais mecanismos existentes.

Inicialmente as regras implementadas permitem IPS específicos, julga requisições geradas por "exploits" que abusam do top 10 pontos mais importantes previstos pela OWASP[1] e julgam IPs com más reputações geradas pelo SOC do provedor.

O recurso de direcionamento do tráfego **(CDN** – *Content Delivery Network*), não entrega o conteúdo em regiões geográficas que não sejam Brasil e Estados Unidos. Possui também recursos para mitigação de ataques de "**DDoS"** nativos.

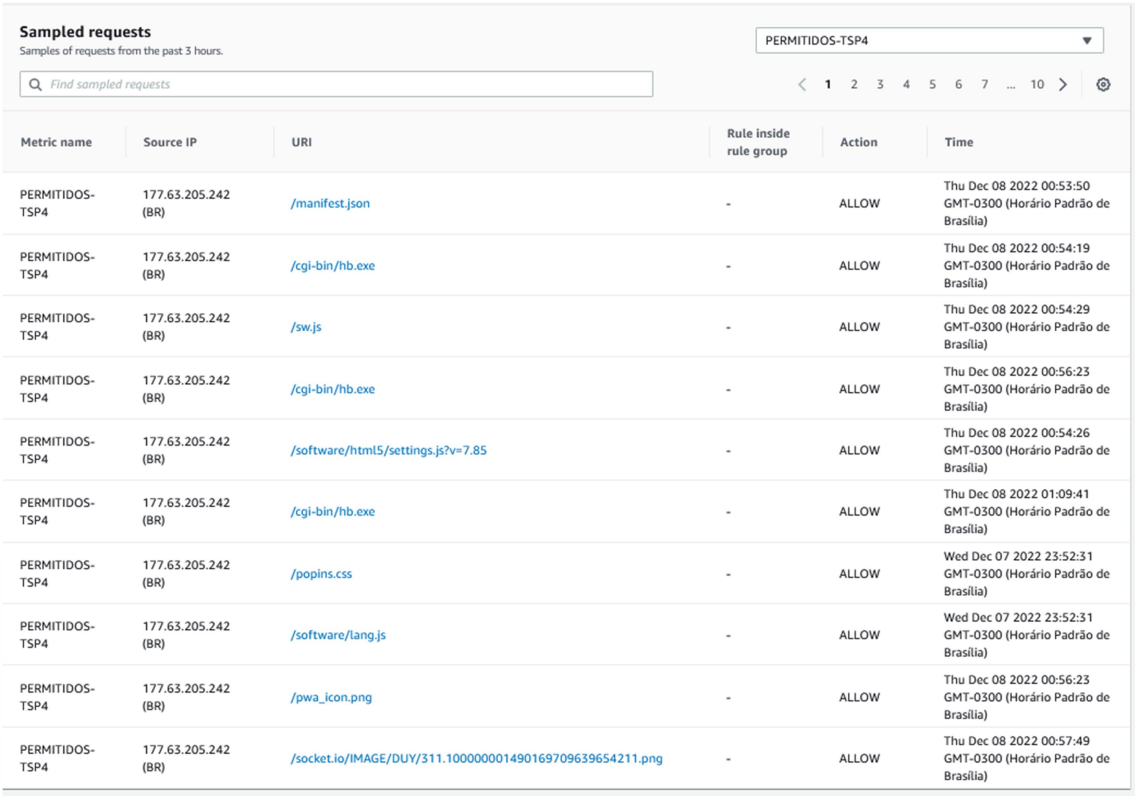
Todo o tráfego de camada web passa também por proteções na borda da rede em camadas mais baixas onde possuímos também a análise de tráfego com mecanismos **IPS / IDS** e filtros geográficos também, porém apenas para o Brasil, com exceções pontuais a IPs fixos comunicados pelo cliente.

A aplicação de acesso ao sistema possui também proteções relacionadas aos pontos da **OWASP TOP 10 Web**, recursos de proteção para utilização de senha e ou se aplicável utilização de **2FA** (*Duplo fator de autenticação*) e certificado digital para a troca de informações pelo protocolo HTTPS.

A seguir, temos evidências de duas regras monitoradas onde no primeiro caso, permitimos um IP pontual pela regra "**PERMITIDOS**"; inicialmente bloqueado pela regra de reputação do provedor a fim de validar a permissão do tráfego. Na coluna, nome da Métrica, temos também o nome da REGRA. Na parte superior direita, temos o filtro aplicado também pelo nome da regra que permitiu a execução das requisições.

[1] https://owasp.org/www-project-top-ten/

12 de Dezembro de 2022



Sampled requests

Samples of requests from the past 3 hours.

PERMITIDOS-TSP4

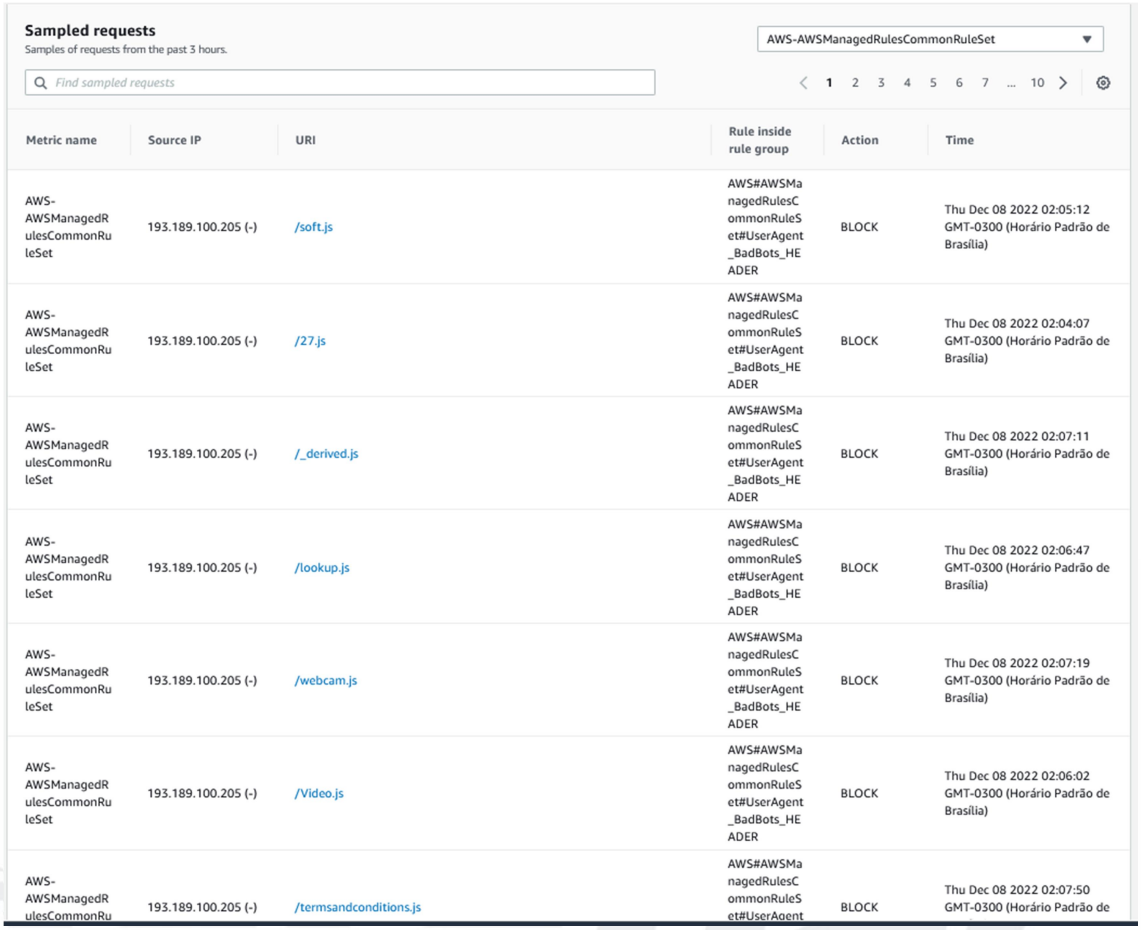
Find sampled requests

1 2 3 4 5 6 7 ... 10

Metric name	Source IP	URI	Rule inside rule group	Action	Time
PERMITIDOS-TSP4	177.63.205.242 (BR)	/manifest.json	-	ALLOW	Thu Dec 08 2022 00:53:50 GMT-0300 (Horário Padrão de Brasília)
PERMITIDOS-TSP4	177.63.205.242 (BR)	/cgi-bin/hb.exe	-	ALLOW	Thu Dec 08 2022 00:54:19 GMT-0300 (Horário Padrão de Brasília)
PERMITIDOS-TSP4	177.63.205.242 (BR)	/sw.js	-	ALLOW	Thu Dec 08 2022 00:54:29 GMT-0300 (Horário Padrão de Brasília)
PERMITIDOS-TSP4	177.63.205.242 (BR)	/cgi-bin/hb.exe	-	ALLOW	Thu Dec 08 2022 00:56:23 GMT-0300 (Horário Padrão de Brasília)
PERMITIDOS-TSP4	177.63.205.242 (BR)	/software/html5/settings.js?v=7.85	-	ALLOW	Thu Dec 08 2022 00:54:26 GMT-0300 (Horário Padrão de Brasília)
PERMITIDOS-TSP4	177.63.205.242 (BR)	/cgi-bin/hb.exe	-	ALLOW	Thu Dec 08 2022 01:09:41 GMT-0300 (Horário Padrão de Brasília)
PERMITIDOS-TSP4	177.63.205.242 (BR)	/popins.css	-	ALLOW	Wed Dec 07 2022 23:52:31 GMT-0300 (Horário Padrão de Brasília)
PERMITIDOS-TSP4	177.63.205.242 (BR)	/software/lang.js	-	ALLOW	Wed Dec 07 2022 23:52:31 GMT-0300 (Horário Padrão de Brasília)
PERMITIDOS-TSP4	177.63.205.242 (BR)	/pwa_icon.png	-	ALLOW	Thu Dec 08 2022 00:56:23 GMT-0300 (Horário Padrão de Brasília)
PERMITIDOS-TSP4	177.63.205.242 (BR)	/socket.io/IMAGE/DUY/311.1000000014901697096396542 11.png	-	ALLOW	Thu Dec 08 2022 00:57:49 GMT-0300 (Horário Padrão de Brasília)

A seguir, temos as evidências de bloqueios sendo realizados por meio de um teste onde atuamos com uma ferramenta de força bruta para enumeração de arquivos e paths da aplicação partindo de um IP dos Estados Unidos, a fim de validar o funcionamento da regra. Na coluna de métrica e na parte superior direita, é possível ver a mudança da regra que gerou os logs.

Av. Presidente Vargas, 2921
Edifício Sky Towers office
5º Andar - Sala 513 - Vila Homero
Indaiatuba - SP - 13.338-705
(19) 3014-8080
www.datapar.com.br



Sampled requests

Samples of requests from the past 3 hours.

AWS-AWSManagedRulesCommonRuleSet

Find sampled requests

1 2 3 4 5 6 7 ... 10

Metric name	Source IP	URI	Rule inside rule group	Action	Time
AWS-AWSManagedRulesCommonRuleSet	193.189.100.205 (-)	/soft.js	AWS#AWSManagedRulesCommonRuleSet#UserAgent_BadBots_HEADER	BLOCK	Thu Dec 08 2022 02:05:12 GMT-0300 (Horário Padrão de Brasília)
AWS-AWSManagedRulesCommonRuleSet	193.189.100.205 (-)	/27.js	AWS#AWSManagedRulesCommonRuleSet#UserAgent_BadBots_HEADER	BLOCK	Thu Dec 08 2022 02:04:07 GMT-0300 (Horário Padrão de Brasília)
AWS-AWSManagedRulesCommonRuleSet	193.189.100.205 (-)	/_derived.js	AWS#AWSManagedRulesCommonRuleSet#UserAgent_BadBots_HEADER	BLOCK	Thu Dec 08 2022 02:07:11 GMT-0300 (Horário Padrão de Brasília)
AWS-AWSManagedRulesCommonRuleSet	193.189.100.205 (-)	/lookup.js	AWS#AWSManagedRulesCommonRuleSet#UserAgent_BadBots_HEADER	BLOCK	Thu Dec 08 2022 02:06:47 GMT-0300 (Horário Padrão de Brasília)
AWS-AWSManagedRulesCommonRuleSet	193.189.100.205 (-)	/webcam.js	AWS#AWSManagedRulesCommonRuleSet#UserAgent_BadBots_HEADER	BLOCK	Thu Dec 08 2022 02:07:19 GMT-0300 (Horário Padrão de Brasília)
AWS-AWSManagedRulesCommonRuleSet	193.189.100.205 (-)	/Video.js	AWS#AWSManagedRulesCommonRuleSet#UserAgent_BadBots_HEADER	BLOCK	Thu Dec 08 2022 02:06:02 GMT-0300 (Horário Padrão de Brasília)
AWS-AWSManagedRulesCommonRu	193.189.100.205 (-)	/termsandconditions.js	AWS#AWSManagedRulesCommonRuleSet#UserAgent	BLOCK	Thu Dec 08 2022 02:07:50 GMT-0300 (Horário Padrão de

Ferramentas

- **Kali Linux** se trata de um sistema operacional linux de código aberto, que possui diversas tarefas de segurança da informação para apoio em pentests, pesquisas de segurança, forense computacional e engenharia reversa.
- **Proton VPN** se trata de um recurso de **VPN** para anonimização de endereço IP.
- **Proxychains** se trata de uma ferramenta de **proxy** também para anonimização de endereço IP.
- **Dirbuster** se trata de uma ferramenta de enumeração de diretórios web baseada em listas predefinidas e por técnicas de força bruta, de acordo com o **top 10 OWASP**.

Av. Presidente Vargas, 2921
Edifício Sky Towers office
5º Andar - Sala 513 - Vila Homero
Indaiatuba - SP - 13.338-705
(19) 3014-8080
www.datapar.com.br

RELATÓRIO MENSAL DE CYBER SEGURANÇA

11/01/2024

INTRODUÇÃO

Este documento apresenta resultados referentes às políticas e controles de acesso no ambiente no período de 05/12/2023 à 11/01/2024.

A metodologia empregada tem como base a família de normas ISO 27000, bem como adaptações para se enquadrar à legislação vigente: Lei n° 13.709/2018, ou Lei Geral de Proteção de Dados Pessoais.

DESCRIÇÃO

Para facilitar o acompanhamento e compreensão deste documento, são apresentadas as ferramentas utilizadas para manutenção da segurança da informação no ambiente, seguidas de evidências assegurando seu uso.
Em cada um dos tópicos também são detalhadas as finalidades destas mesmas ferramentas, a importância de suas adoções e melhorias que elas trazem.
Por fim, são apresentados os próximos passos para o processo contínuo de melhorias e a conclusão do estado atual do ambiente.

FERRAMENTAS UTILIZADAS NO AMBIENTE

Para assegurar um ambiente que se encaixe nas normas e legislações atuais quanto à segurança da informação, são utilizadas as ferramentas abaixo listadas:

AWS WAF

O AWS WAF é um firewall para aplicações Web que permite monitorar as solicitações HTTP e HTTPS que são encaminhadas ao CloudFront e controlar quem pode acessar seu conteúdo. Com base em condições previamente especificadas, tais como valores de query strings ou endereços IP dos quais as solicitações se originam, o CloudFront responderá às solicitações com o conteúdo solicitado ou com um código de status HTTP 403 (Forbidden). Há também mecanismos que possibilitam o retorno de páginas personalizadas com base em regras de bloqueio.

PFSENSE PLUS

Pfsense Plus é um stateful firewall baseado em rede que rastreia individualmente as sessões de conexões de rede que o atravessam. A inspeção dinâmica de pacotes, também conhecida como filtragem dinâmica de pacotes, é um recurso de segurança usado para invocar políticas de segurança refinadas, elevando os níveis de proteção de uma rede interna, garantindo robustez e segurança nos controles de acesso.

SNORT IDS/IPS

Snort IDS/IPS é um sistema de prevenção a intrusões na rede (intrusion prevention system – IPS) open source, mantido e desenvolvido pela Cisco. A ferramenta se destaca por sua capacidade de analisar tráfegos em tempo real e registrar pacotes de protocolo TCP (Transmission Control Protocol).
Em função dessa versatilidade, o Snort consegue desempenhar o papel de três tipos de aplicações cruciais para monitorar um servidor. Logo, ele pode ser usado como sniffer de pacotes (de modo similar ao tcpdump), como um registrador de pacotes (o que é útil para depuração de tráfego de rede) e / ou um sistema avançado de prevenção à intrusão.

INCIDENTES DE CYBER SEGURANÇA

Sobre os incidentes relacionados a cyber segurança ou infraestrutura do sistema no mês de dezembro, obtivemos uma falha com a solução de CDN.

Executamos os procedimentos para ajuste de acesso e iniciamos o troubleshooting, sendo realizadas correções a nível de aplicação, apenas.

REGRAS DE FILTRAGEM DE PACOTES PFSENSE PLUS FIREWALL

Abaixo constam as regras de controle de acessos configuradas e em execução no Pfsense Plus Firewall:

Rules

		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description
☐	✓	WAN3	TCP/UDP	pfB_ AWSCloudFront_ v4	*	10.0.252.97	TSPLUSPORTS	10.0.1.167	TSPLUSPORTS	TSPLUS4
☐	✓	WAN3	TCP/UDP	DHL	*	10.0.252.97	TSPLUSPORTS	10.0.1.167	TSPLUSPORTS	TSPLUS4_DHL

Regras do firewall Pfsense Plus.

LOGS PFSENSE PLUS FIREWALL

Com o objetivo de realizar o controle de acesso via regras de aceitação / negação, o Pfsense Plus Firewall atua como intermediador analisando os cabeçalhos de todos pacotes, principalmente quanto à origem e destino. Contudo, pode-se obter um refinamento ainda maior com uma grande variedade de possibilidades para filtragem.
Abaixo temos registros de log no firewall Pfsense Plus evidenciando a correta aplicação de regras e negação de acessos indevidos:

1445 Entries in Active Log

Date	Action	Pri	Proto	Class	Source IP	SPort	Destination IP	DPort	GID:SID	Description
2024-01-11 15:48:12	⚠	2	TCP	Misc Attack	185.196.8.151	48599	10.0.253.83	22	1:2500020	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 11
2024-01-11 15:38:15	⚠	2	TCP	Misc Attack	185.196.8.151	60678	10.0.253.82	22	1:2500020	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 11
2024-01-11 15:37:12	⚠	1	UDP	Attempted Administrator Privilege Gain	91.92.244.147	58682	10.0.253.85	9034	1:2044008	ET EXPLOIT Realtek SDK - Command Execution/Backdoor Access Inbound (CVE-2021-35394)
2024-01-11 15:33:34	⚠	2	TCP	Misc Attack	185.196.8.151	36442	10.0.253.83	22	1:2500020	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 11
2024-01-11 15:30:24	⚠	3	TCP	Unknown Traffic	74.82.47.20	59665	10.0.253.85	80	119:24	(http_inspect) MULTIPLE HOST HDRS DETECTED
2024-01-11 15:12:32	⚠	2	TCP	Misc Attack	185.196.8.151	59116	10.0.253.151	22	1:2500020	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 11
2024-01-11 15:12:02	⚠	3	TCP	Unknown Traffic	64.62.197.115	58909	10.0.253.94	80	119:24	(http_inspect) MULTIPLE HOST HDRS DETECTED
2024-01-11 15:09:36	⚠	2	TCP	Misc Attack	45.95.147.236	48216	10.0.253.151	443	1:2500026	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 14
2024-01-11 14:53:51	⚠	2	UDP	Potentially Bad Traffic	192.241.196.120	55826	10.0.253.94	5060	140:18	(spp_sip) Content length mismatch
2024-01-11 14:53:19	⚠	2	TCP	Misc Attack	185.196.8.151	39697	10.0.253.88	22	1:2500020	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 11

Registros de log no firewall Pfsense Plus: acessos negados de acordo com regras especificadas.

SNORT IDS/IPS

Snort IDS/IPS atua na detecção e prevenção de intrusão, realizando bloqueios em casos de pacotes maliciosos enviados ao Pfsense Plus Firewall.
Abaixo temos evidenciada a configuração e execução do Snort em todas as interfaces de rede do Pfsense Plus Firewall:

Interface Settings Overview

	Interface	Snort Status	Pattern Match	Blocking Mode	Description	Actions
☐	WAN2 (ena2)	✔ ↻ ◉	AC-BNFA	LEGACY MODE	WAN2	✎ ⧉ 🗑
☐	WAN3 (ena3)	✔ ↻ ◉	AC-BNFA	LEGACY MODE	WAN3	✎ ⧉ 🗑

Status do Snort IDS/IPS: configurado e em execução em ambas interfaces de rede do Pfsense Plus Firewall.

Na sequência temos uma amostragem de pacotes maliciosos bloqueados pela ferramenta Snort nas interfaces de rede do Pfsense Plus Firewall:

Last 10000 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	89.190.156.40	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 9 -- 2024-01-02 23:42:52 ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 10 -- 2024-01-03 23:58:36	✖
2	74.82.47.32	(http_inspect) MULTIPLE HOST HDRS DETECTED -- 2024-01-09 12:14:35	✖
3	216.218.206.80	(http_inspect) MULTIPLE HOST HDRS DETECTED -- 2024-01-03 15:06:23	✖
4	222.186.16.186	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 7 -- 2024-01-02 13:34:11	✖
5	165.22.58.90	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 4 -- 2024-01-02 00:47:31	✖
6	143.198.91.141	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 3 -- 2024-01-02 00:38:55	✖
7	65.49.1.59	(http_inspect) MULTIPLE HOST HDRS DETECTED -- 2024-01-01 11:53:50	✖
8	159.203.45.248	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 3 -- 2024-01-01 11:58:46	✖
9	216.218.206.123	(http_inspect) MULTIPLE HOST HDRS DETECTED -- 2024-01-03 11:47:17	✖
10	222.186.16.162	ET COMPROMISED Known Compromised or Hostile Host Traffic TCP group 7 -- 2024-01-02 19:06:33	✖

Bloqueios de pacotes maliciosos realizado pela ferramenta Snort IDS/IPS.

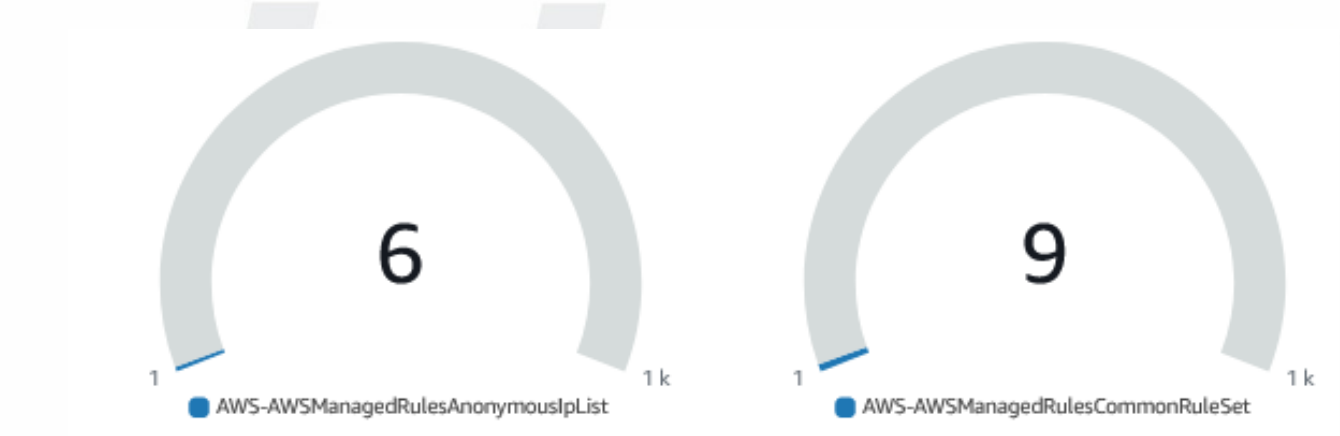
AWS WEB APPLICATION FIREWALL

O WAF, ou firewall de aplicativos web, ajuda a proteger os aplicativos web ao filtrar e o monitorar o tráfego HTTP entre o aplicativo web e a internet. De modo geral, o WAF protege os aplicativos web contra ataques como falsificação de solicitação entre sites, cross-site-scripting (XSS), inclusão de arquivo e injeção de SQL, entre outros. O WAF é uma defesa de protocolo da camada 7 (no modelo OSI). Esse método de mitigação costuma fazer parte de um conjunto de ferramentas que, juntas, criam uma defesa holística contra diversos vetores de ataque.

O AWS Web Application Firewall possui grande robustez e facilidade de implantação e manutenção, assegurando que a aplicação possua níveis adequados e segurança sem impactar no desempenho.

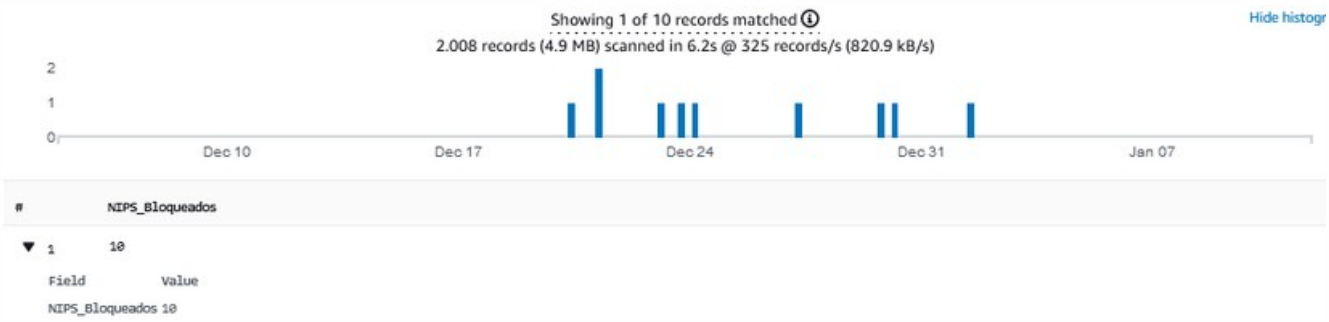
Abaixo podemos observar o conjunto de regras do AWS WAF aplicado ao ambiente DHL:

Abaixo evidências dos eventos tratados e status atual da ferramenta:



Regras do AWS WAF: gráfico contendo quantidade de bloqueios realizados.

A seguir, total de IPs bloqueados no período de 05/12/2023 a 11/01/2024:



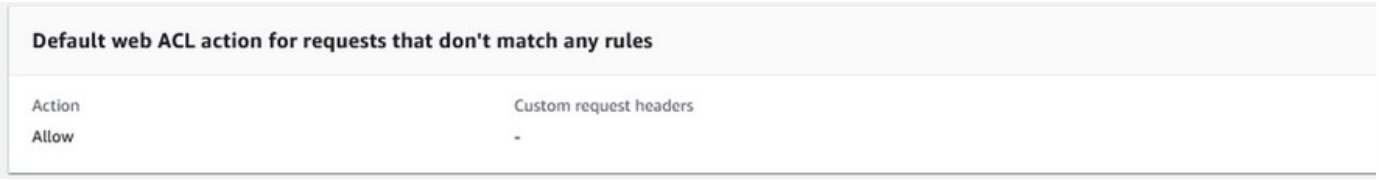
#	NIPS_Bloqueados
▼ 1	10

Field	Value
NIPS_Bloqueados	10

A seguir, evidências de log de bloqueio realizado:

@timestamp	1704116478366
action	BLOCK
formatVersion	1
httpRequest.args	REDACTED
httpRequest.clientIp	198.235.24.11
httpRequest.country	US
httpRequest.headers.0.name	Host
httpRequest.headers.0.value	webcloud4.datapardc.com
httpRequest.httpMethod	REDACTED
httpRequest.httpVersion	HTTP/1.1
httpRequest.requestId	mImH2DfYRI00aBsINQE6CmNQ1esvh1NRA3fQw1HrbIjag1t7o8Q_SQ==
httpRequest.uri	REDACTED
httpSourceId	E19HKCNWGZ9V8V
httpSourceName	CF
ja3Fingerprint	473cd7cb9faa642487833865d516e578
labels.0.name	awswaf:managed:aws:core-rule-set:NoUserAgent_Header
ruleGroupList.0.ruleGroupId	AWS#AWSManagedRulesAmazonIpReputationList
ruleGroupList.1.ruleGroupId	AWS#AWSManagedRulesAnonymousIpList
ruleGroupList.2.ruleGroupId	AWS#AWSManagedRulesCommonRuleSet
ruleGroupList.2.terminatingRule.action	BLOCK
ruleGroupList.2.terminatingRule.ruleId	NoUserAgent_HEADER
terminatingRuleId	AWS-AWSManagedRulesCommonRuleSet
terminatingRuleType	MANAGED_RULE_GROUP
timestamp	1704116478366
webaclId	arn:aws:wafv2:us-east-1: :global/webacl/TSPLUS04/c2b729b1-2d93-4821-bc4d-0d0c15117a0e

Abaixo segue a ACL padrão para requisições que não se enquadrem em nenhuma regra:



Definição da ACL padrão.

INCIDENTES RELACIONADOS A INFRAESTRUTURA

- O ambiente teve direcionados a área de infraestrutura 30 acionamentos no período entre ações de:
  - Aplicação de atualizações em :
    - Sistemas de homologação
    - EDIs.
    - Aplicações integradoras
    - Restart de senha de usuário
- Alteração de configurações em serviços e de uso comum para usuários específicos.

PRÓXIMOS PASSOS

Este relatório será analisado e atualizado de forma mensal, garantindo assim que o ambiente se enquadre às normas e leis vigentes quanto à segurança da informação.
Na necessidade de aplicação de novas ferramentas ou metodologias, este documento permanecerá como documentação de quaisquer alterações realizadas.

CONCLUSÃO

Com a adoção de ferramentas topo de linha para manutenção da segurança do ambiente, garante-se uma proteção de alto nível atendendo às principais normas e legislações vigentes, abrangendo os princípios da confidencialidade, integridade e disponibilidade das informações necessárias ao perfeito funcionamento.
Foram informadas neste relatório as ferramentas utilizadas no ambiente no que tange à busca pela segurança cibernética do ambiente.

Abaixo, listamos estas ferramentas, bem como suas finalidades e status atual:

FERRAMENTA	FINALIDADE	STATUS
Pfsense Firewall	Filtragem de pacotes e controle de acesso	Operacional
Snort IDS/IPS	Detecção e Prevenção de Intrusão	Operacional
AWS Web Application Firewall	Firewall de Aplicação Web	Operacional

RRIE

Análise de Vulnerabilidade Técnica

RELATÓRIO DE **R**ETESTE DE **I**NVASÃO **E**XTERNO

CÓDIGO 20221215

Informação Confidencial
Este relatório contém informação confidencial e **não deve ser enviado por e-mail, fax ou qualquer outro meio eletrônico a menos que este seja previamente aprovado** pelas políticas de segurança da contratante. Todas as cópias eletrônicas ou em papel do presente documento devem ser guardadas em um local protegido. Não compartilhe as informações contidas neste documento, a menos que seja expressamente autorizado.
Somente para uso da Empresa **DORPA**

São Paulo, Quinta-Feira, 15 de Dezembro de 2022.

Atenciosamente a:

DORPA,

Considerações Iniciais:

Através deste presente documento apresentamos o **Relatório de Reteste de Invasão Externo baseado nas Metodologias NIST 800-115** e **OWASP TOP 10 – 2021** sobre infraestrutura, serviços e aplicações disponíveis por meio de uma análise de **1 (uma)** aplicação visíveis em ambiente Externo.

Desde já agradecemos a oportunidade em oferecermos nossos serviços profissionais e estamos a sua disposição para qualquer dúvida que considerem pertinentes.

Prof. MSc. Marcelo Lau

https://www.datasecurity.com.br/

Sumário

Lista de Tabelas

Lista de Figuras

1. Introdução

1.1. Objetivo

Este relatório tem a finalidade de apresentar os resultados da atividade de **Reteste de Invasão Externo** realizada sobre os ativos definidos e acordados entre a **DATA SECURITY** e a **DORPA**, com o propósito de identificar as vulnerabilidades que se encontram expostas nas redes e serviços segundo o objetivo e escopo deste trabalho, onde são apresentadas descrição e recomendações e para a mitigação dos riscos.

Considera-se como valor agregado neste trabalho a inclusão da **visão global de segurança**, que não se limita apenas à indicação do estado de segurança no momento da realização do teste de intrusão, pois inclui questões que permitem a correção de problemas em curto, médio e longo prazo possibilitando um alto nível de excelência de segurança em sua rede.

1.2. Escopo

O escopo deste trabalho consistiu na avaliação do risco de segurança, baseado nas vulnerabilidades listadas no **OWASP TOP 10 (2021)** e seu grau de exposição de ativos através de técnicas de intrusão, com o conhecimento prévio de **1 (um) endereço URL** fornecidos pela empresa **DORPA.**

Este trabalho foi realizado através do uso de ferramentas de segurança, analisadores de vulnerabilidades, códigos de exploração de vulnerabilidades disponíveis na Internet, além de metodologias típicas para realização da coleta e reconhecimento do ambiente em geral utilizado pelos atacantes.

Com o objetivo de atender à atual necessidade do cliente, foi realizada uma análise do ambiente Externo de TI a fim de verificar os controles e riscos existentes em sua aplicação e canais de acesso à Internet, atentando para os seguintes aspectos do ambiente de TI em que os respectivos sistemas alvos desta proposta estão sendo processados:

- Identificação dos controles existentes e sua suficiência para prevenir a ocorrência de ataques externos, provenientes da Internet, bem como a execução de ações não autorizadas e vulnerabilidades decorrentes das configurações;

- Análise da aplicação, levantando os controles existentes e a lógica de transação utilizada, visando verificar a robustez contra fraudes e a revelação de informações sigilosas dos clientes da empresa; e

- Mapeamento e identificação de sistema de acesso remoto, validação dos controles praticados para conter ataques externos, validando a abrangência de uma eventual invasão a redes ou aplicação da empresa **DORPA**.

As atividades realizadas sobre o ambiente avaliado incluíram o reconhecimento ativo dos sistemas, identificação de sistemas ativos encontrados e reconhecimento de portas sobre os sistemas ativos detectados, com a finalidade de determinar sua função, seu serviço, e também a avaliação de sua necessidade, tal como os riscos potenciais dos mesmos.

O complemento deste trabalho foi realizado por meio de uma análise de vulnerabilidades sobre os sistemas ativos detectados com o propósito de apontar as potenciais vulnerabilidades que podem afetar estes sistemas com tentativas de intrusão associados à exploração destas vulnerabilidades.

1.3. Análise de Ativos - IP

As aplicações a seguir foram analisadas mediante solicitação da empresa **DORPA**, totalizando **1 (uma) aplicação**, esta que, no momento dos testes de invasão localizava-se no endereço IP:

Endereço URL
webcloud4.datapardc.com

Tabela 1 – Aplicação Administrador Web

Os resultados aqui apresentados estão relacionados a uma análise realizada no dia **12/12/2022** à **14/12/2022**, portanto, qualquer alteração do ambiente posterior a esta data pode não refletir o resultado apresentado neste relatório.

1.4. Metodologia

O trabalho foi realizado aplicando a metodologia de avaliação de segurança por níveis de criticidade de acordo com a pontuação **CVSS** objetivando detectar, avaliar e pontuar as vulnerabilidades de acesso lógico ao ambiente externo da **DORPA**.

A pontuação de **CVSS** se baseia nesses **principais** aspectos para definir uma pontuação relativa a vulnerabilidade:

- Vetor de Acesso;
- Complexidade de Acesso;
- Autenticação;
- Impacto a Confidencialidade;
- Impacto a Integridade; e
- Impacto a Disponibilidade.

Essa metodologia visa analisar os diferentes níveis de proteção dos sistemas definidos pela **DORPA**, avaliando os pontos de acessos externos. Os trabalhos de detecção de vulnerabilidades foram realizados conforme os seguintes passos:

- Verificação dos endereços ativos;
- Identificação dos sistemas relacionados;
- Identificação dos serviços ativos; e
- Identificação das vulnerabilidades.

A atividade contemplou a análise segundo o **OWASP TOP 10 de 2021**, metodologia de testes que contempla as seguintes vulnerabilidades:

1. *Violação do Controle de Acesso;*
2. *Falhas Criptográficas;*
3. *Injeção de Código;*
4. *Design Inseguro;*
5. *Erros de Configurações de Segurança;*
6. *Componentes Vulneráveis e Desatualizados;*
7. *Quebra de Identificação e Autenticação;*
8. *Falhas de Software e Integridade de Dados;*

9. *Falhas de Registro e Monitoramento de Segurança; e*
10. *Server-Side Request Forgery.*

Durante a elaboração da análise não foram realizados testes de estresse, também conhecidos como *stress testing,* ou mesmo testes de capacidade e alto desempenho, para aferição de métricas do tempo de respostas da aplicação e recursos computacionais utilizados pela **DORPA** ou impactos que o uso destes possam acarretar a sua aplicação corporativa.

1.5. Limitações de Escopo e Responsabilidades

O escopo de nosso trabalho foi limitado a analisar os controles de acesso lógico e as funcionalidades de segurança utilizadas nos sistemas alvo descritos anteriormente, tendo em vista apontar fragilidades que possam expor sistemas que potencialmente podem vir a apresentar dados sensíveis externos da empresa.

Nosso trabalho não teve como objetivo corrigir as possíveis vulnerabilidades do ambiente de tecnologia da informação da **DORPA**. Também não foi escopo desta fase a criação de mecanismos para proteção de sistemas identificados contra ataques externos e internos.

As recomendações sugeridas neste relatório devem ser testadas e validadas pela equipe técnica da **DORPA** antes de serem praticadas nos servidores de produção. A **DATA SECURITY** não tem responsabilidade sobre sua utilização e possíveis impactos sobre outras aplicações, serviços ou servidores de dados não analisados por este relatório.

1.6. Ferramentas Adotadas Durante o Teste de Invasão Externo

Durante a condução do Teste de Invasão de Externo foram utilizadas diversas ferramentas técnicas para a viabilização deste trabalho, dentre estas destacam-se:

1.6.1. THC Hydra

O THC Hydra é uma ferramenta clássica usada para quebrar senhas. Resumidamente, é um programa para *crackear* senhas de login na rede através de um método de *brute force* com dicionários

1.6.2. Kali Linux

Kali Linux é um sistema operacional destinado a testes avançados de penetração e auditoria de segurança. Por meio deste é possível realizar ação e exploração de vulnerabilidades.

1.6.3. Nessus

Nessus é um programa que executa a verificação de falhas/vulnerabilidades de segurança. Ele realiza uma varredura de portas, detectando servidores ativos e simulando invasões para detectar vulnerabilidades. Uma característica importante é que o Nessus procura por servidores ativos não apenas nas portas padrão, mas em todas as portas TCP.

1.6.4. Nmap

Nmap é uma ferramenta muito utilizada para avaliar a segurança dos computados, descobrindo serviços ou serviços em uma rede. Em nosso teste, utilizamos esta ferramenta para identificar potenciais portas abertas e versões de serviços utilizados pela **DORPA**.

1.7. Considerações Gerais

Aplicam-se ao presente trabalho e aos resultados alcançados as seguintes considerações:

- Na presente análise foram consideradas - e assumem-se como corretas - as informações, arquivos, subsídios e demais informações fornecidas pela empresa solicitante; e
- Fica estabelecido entre as partes que não cabe à **DATA SECURITY** qualquer responsabilidade por eventuais perdas que possam ser ocasionadas ao solicitante, aos seus acionistas, diretores, credores ou a outras partes como consequência da utilização dos dados e informações constantes neste parecer.

1.8. Revisor Final deste Relatório

O profissional responsável pelo presente parecer é:

Prof. Msc. Marcelo Lau – Diretor executivo da Data Security

- ✓ Atuou por mais de 12 anos em instituições financeiras em áreas de segurança da informação e prevenção a fraude. Engenheiro pela EEM, pós-graduado em administração pela FGV e **mestre em ciência forense pela POLI/USP**.

- ✓ Atuou por mais de 3 anos como pesquisador da POLI/USP.

- ✓ Atual professor nos cursos de Pós-Graduação em Computação Forense na Universidade Presbiteriana Mackenzie e na FIAP. Instrutor da FEBRABAN em cursos na área de *Compliance* e Segurança da Informação, além de diversos centros de ensino no Brasil e no Exterior.

- ✓ Conta com dezenas de Entrevistas em Rádio, TV, Mídia Impressa e publicações online nos mais diversos canais de comunicação de cobertura regional e nacional no Brasil e Argentina como TV Globo, SBT, Valor Econômico, Estado de São Paulo, entre outros.

2. Resultado do trabalho – Sumário Executivo

2.1. Visão Global de Segurança

Esta seção traz um resumo das vulnerabilidades encontradas, seu nível de classificação, o impacto da exploração da vulnerabilidade identificada e recomendações para a diminuição do grau de risco identificado podendo chegar à eliminação do risco mapeado.

2.2. Análise dos Ativos via Rede Externa:

Este escopo abrange análise de vulnerabilidade realizada em sistema externo da **DORPA** e não contempla demais testes internos como análise de segurança física e lógica em outros ambientes que podem permitir acesso de conectividade aos sistemas informados pela empresa, como testes de resposta em ramais telefônicos e demais endereços URL não contemplados ou informados pela **DORPA**.

A análise externa apresentou **1 grupo** de **melhoria**, totalizando cerca de **1 (um) ponto** vulnerável individualmente.

2.3. Classificação do Risco

Foram estabelecidos três níveis de risco para classificação das vulnerabilidades:

Risco	CVSS	Descrição
Baixo	**0.0 – 3.9**	Pode acarretar acesso a informações não relevantes.
Médio	**4.0 – 6.9**	Pode acarretar acesso a informações relevantes, as quais podem ser utilizadas para se descobrir vulnerabilidades de nível alto.
Alto	**7.0 – 10**	Pode acarretar acesso não autorizado a informações relevantes, negação de serviço e prejuízos (tanto financeiros quanto à imagem da Empresa).

Tabela 2 - Tabela de Classificação de Risco

2.4. Classificação OWASP

Em relação à referência adotada, seguem as classes de vulnerabilidades segundo o padrão OWASP TOP 10 presentes na análise.

Classificação OWASP		Descrição
	A5 – Erros de Configurações de Segurança	A fragilidade na configuração de segurança de sistemas é o problema mais comum. Isto ocorre por conta de configurações padrões inseguras, configurações incompletas, armazenamento em nuvem aberta, cabeçalhos HTTP mal configurados e mensagens de erro contendo informações sensíveis. Não só todos os sistemas operacionais, frameworks, bibliotecas e aplicativos devem ser configurados de forma segura, mas também dever ser corrigidos/atualizados em tempo hábil.

Tabela 3 - Classes de Vulnerabilidades Encontradas na Análise da Aplicação

Identifica-se um resumo de vulnerabilidades contabilizadas pelo OWASP como:

A7) Quebra de Identificação e Autenticação:

- ✓ **1 ponto de melhoria.**

2.5. Resultados de Reteste

Segue o sumário das vulnerabilidades encontradas durante o primeiro teste e o atual estado destas, sendo categorizadas como **Corrigida**, **Não Corrigida** ou **Nova**.

Ref.	Vulnerabilidade Encontrada	Status
3.1	Cookies sem Sinalização de Segurança	Corrigida
3.2	Páginas de Erro Padrão	Não Corrigida

Tabela 4 - Resultados do Reteste

2.6. Contabilização das Vulnerabilidades Externas

A totalização de vulnerabilidades permite gerar um resumo de falhas de segurança obtidas por endereço URL em função dos pontos identificados no relatório.

Ref.	Vulnerabilidade	Risco	Aplicação	Status
3.1	**Cookies sem Sinalização de Segurança**	**Médio**	webcloud4.datapardc.com	CORRIGIDA
3.2	**Páginas de Erro Padrão**	**Melhoria**	webcloud4.datapardc.com	NÃO CORRIGIDA

Tabela 5 - Contabilização das Vulnerabilidades Identificadas

2.7. Resumo das Vulnerabilidades, Impactos e Recomendações

Segue o sumário das vulnerabilidades **novas** ou **não corrigidas** nos ativos, sua classificação OWASP, seus impactos e recomendações resumidas para a correção e/ou mitigação dos riscos aos quais os ativos estão expostos.

Ref.	OWASP	Vulnerabilidade	Risco	Impacto	Recomendações
3.2	**A5**	**Página de Erro Padrão**	**Melhoria**	A aplicação testada não possui páginas de erro personalizadas, utilizando as páginas de erro padrão do servidor web.	Recomenda-se a criação de páginas de erros personalizadas ou o redirecionamento para a página principal.

Tabela 6 - Resumo das Vulnerabilidades Identificadas

2.8. Sumário Executivo de Reteste

Em função do item 3 deste relatório podemos resumir as vulnerabilidades encontradas nos subcapítulos a seguir.

Endereço IP	Não Corrigida	Corrigida	Nova	Total
webcloud4.datapardc.com	01	01	00	01
Total	01	01	00	01

Tabela 7 - Sumário Quantitativo de Reteste

Endereço IP	Não Corrigida	Corrigida	Nova	Total
webcloud4.datapardc.com	50,0%	50,0%	0,0%	100,0%
Total	50,0%	50,0%	0,0%	100,0%

Tabela 8 - Sumário Qualitativo de Reteste

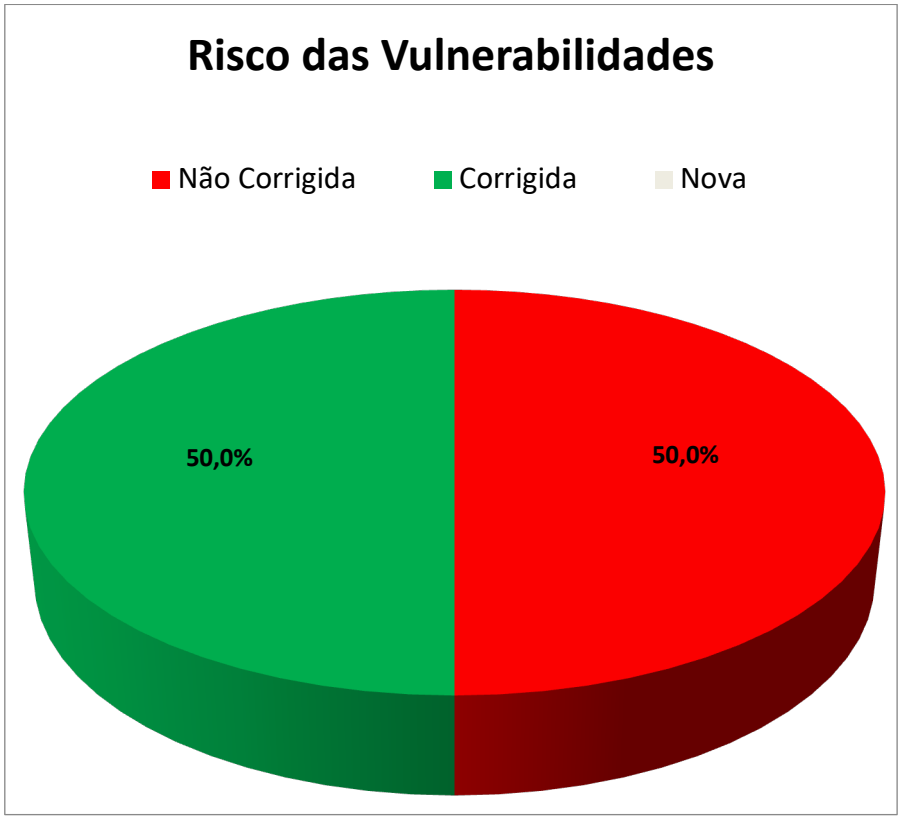


Figura 1 - Risco das Vulnerabilidades Encontradas na Análise

3. Resultado do trabalho – Análise Externa

Detalharemos neste item todos os pontos vulneráveis identificados nas aplicações fornecidas pelo **DORPA** descrevendo as vulnerabilidades e recomendações, visando a melhoria no atual cenário.

Referência	OWASP	CVSS	Vulnerabilidade	Status
3.1	A7	6.4 Médio	Cookies sem Sinalização de Segurança	Corrigida
Pontos Vulneráveis			webcloud4.datapardc.com	

Descrição da Vulnerabilidade

Durante a realização dos testes de forma autenticada, foi possível identificar que a aplicação não utiliza sinalizadores de segurança definidos em alguns de seu *cookie* de sessão. A figura a seguir evidencia a página *WEB* localizada sem as devidas sinalizações de segurança.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure
server	-1	webcloud4.datapardc.com	/	2023-11-25T17:0...	8		
	HttpOnly	webcloud4.datapardc.com	/	Session	8		✓

Figura 2 - Cookie sem sinalização de segurança

A ausência dos sinalizadores de segurança permite que uma pessoa mal-intencionada possa ter acesso ao valor do *cookie*, permitindo caso haja um *cookie* de sessão, que a sessão de um usuário conectado seja clonada, possibilitando ter acesso a aplicação (se passando por um usuário com acesso válido à aplicação) sem ao menos ter acesso direto as suas credenciais de autenticação.

Durante o reteste foi possível atestar que a vulnerabilidade reportada foi corrigida onde, no momento, os sinalizadores de segurança estão presentes.

set-cookie	HttpOnly; Secure; SameSite=None

Figura 3 - Cookie sem sinalização de segurança (corrigido)

Referência	OWASP	Ponto Identificado	Status
3.2	A5 Melhoria	Páginas de Erro Padrão	Não Corrigida
Endereço URL		webcloud4.datapardc.com	

Descrição da Vulnerabilidade

Durante os testes, foi possível identificar que a aplicação testada não possui páginas de erros personalizadas, utilizando as páginas de erro fornecidas pelo servidor web. Na figura abaixo, é possível visualizar a página de erro:

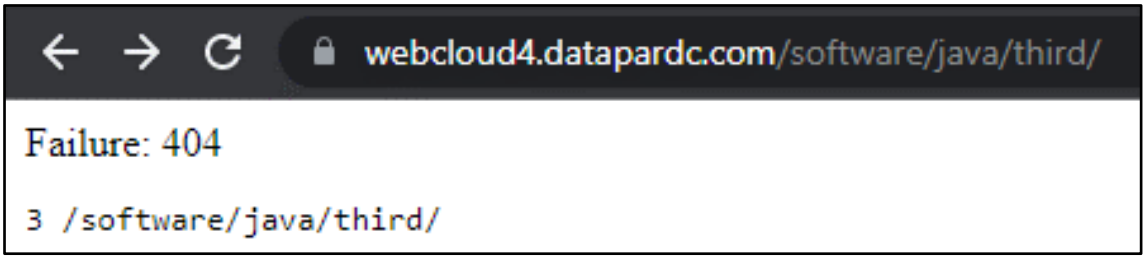


Figura 4 - Página Padrão

Recomendações

Recomenda-se a criação de páginas de erros personalizadas ou o redirecionamento para a página principal. Implementar uma página de erro personalizada no lugar do redirecionamento se torna uma opção mais interessante pois o usuário pode saber o que de fato ocorreu com sua requisição à aplicação.

4. Revisão

Registro de Mudança

Data	Versão	Referência da Alteração
Dezembro / 2022	1.0	Relatório Final

Aceite

Empresa	Versão
DORPA	1.0
DATA SECURITY	1.0

ANEXO I – ACORDO DE CONFIDENCIALIDADE

DATA SECURITY – DORPA

A **CONTRATANTE** (**DORPA**) e a **CONTRATADA** (**DATA SECURITY**) acordam entre si:

1. A **CONTRATANTE** entrega a **CONTRATADA** informação de sua propriedade relativa às políticas, procedimentos, diagramas, configurações de segurança sujeitos ao objeto da atividade contratada (**Teste de Invasão Externo – DORPA**).

2. A informação entregue pela **CONTRATANTE** à **CONTRATADA** e vice-versa, relacionado ao objeto ou mesmo produto da atividade contratada se constitui Informação Confidencial.

3. A **CONTRATADA** se obriga a:
   a. Manter em caráter sigiloso a Informação Confidencial e não disponibilizá-la a terceiros sem o consentimento da **CONTRATANTE**.
   b. Utilizar a Informação Confidencial exclusivamente para a atividade contratada e tarefas definidas no escopo deste trabalho.
   c. Restituir toda a Informação Confidencial toda vez que esta for solicitada pela **CONTRATANTE**.
   d. Destruir toda Informação Confidencial com solicitação e consentimento da **CONTRATANTE**, a qual a **CONTRATADA** deverá provar tal destruição.
   e. Revelar a Informação Confidencial somente às pessoas cujo conhecimento é indispensável para atender a finalidade da atividade contratada. Estas pessoas devem manter as obrigações aqui previstas e a **CONTRATADA** responderá somente a elas.
   f. Eliminar toda cópia eletrônica e/ou impressa da Informação Confidencial de qualquer equipamento informático ou outros equipamentos de apoio, salvo autorização expressa da **CONTRATANTE**, uma vez que o trabalho seja finalizado.

4. A **CONTRATADA** está liberada de sua obrigação em guardar segredo da Informação Confidencial caso:
   a. As evidências fornecidas pela **CONTRANTE** sejam de prévio conhecimento da **CONTRATADA** em período anterior à atividade contratada.
   b. As informações sejam publicamente conhecidas sem que resultem no descumprimento da **CONTRATADA** ou de um terceiro sujeito a uma obrigação de confidencialidade.
   c. Exista uma obrigação jurídica de fornecimento da informação. Neste caso a **CONTRATADA**, poderá revelar somente o mínimo de Informação Confidencial necessário para o cumprimento da exigência legal. Neste caso, a informação apenas será fornecida depois da notificação formal a ambas as partes. Este direito também poderá ser exercido pela **CONTRATADA** no dia do vencimento do prazo para provimento desta informação, descrito no requerimento jurídico.

5. A **CONTRATADA** está ciente que:
   a. A **CONTRATANTE**, não outorga nenhuma garantia a respeito da Informação Confidencial, salvo que este conteúdo é de sua propriedade e tem todo direito em revelá-la.
   b. A Informação Confidencial pode conter erros, ser inexata, não ser aplicável ou não se destinar à questão da atividade contratada.
   c. A **CONTRATADA** é exclusivamente responsável pela atualização da Informação Confidencial, o uso que ela outorgue e os efeitos que esta atualização resulte.
   d. A Informação Confidencial tem um valor estratégico para a **CONTRATANTE.**

6. A **CONTRATANTE** está ciente que:
   a. Os documentos entregues (impressos ou eletrônicos) serão de acesso exclusivo aos responsáveis pela empresa contratante e/ou área contratante.