EXPRESIA

Pentesting Report

Upconnection Audit

Inhouse translated document

Produced:
December 19th, 2021

Written by:
Upconnection

Translated y by:

Miguel Suárez - Security Officer

Introduction

The performance of Hacking activities on sample infrastructures is an efficient and real way to identify the risks to which our infrastructures and applications are exposed. The idea is to put oneself in the position of an attacker to try to breach a group of systems. This type of testing can have different contexts depending on the position of the ethical hacker and the information available to them to carry out the test.

For the presentation of the test results, ethical hacking uses the Black Box method, where the security tester only has information about the site to generate intrusion from the front of the portal. There is also the Grey Box method, where the security tester performs tests from the backend using two types of credentials with high and low privileges to identify how far an attacker could go if they gained access.

Objective

Presentation of the results of the analysis and identification of security breaches and vulnerabilities in the infrastructure and applications of the Backbone portals through the provision of Ethical Hacking testing services, in which it is possible to:

- Evaluate vulnerabilities and security breaches that may be identified in the external infrastructure on the Front in the following portals: https://finanprimas-development.finesa.com.co and https://vacantvioletwolf.xpr.cloud

- Evaluate vulnerabilities and security breaches that may be identified in the external infrastructure from the Backend with the users provided by the Backbone team.

- Evaluate the effectiveness and correct configuration of the currently implemented security controls and procedures.

- Identify vulnerabilities that allow for the generation of risk or fraud scenarios for the organization.

- Execute the different phases that make up Ethical Hacking, acting in a similar way to how a real attacker would, in order to identify the attack vectors and weaknesses that could be used by malicious actors against the company.

- Generate actions that allow for the eradication of existing vulnerabilities or reduce the associated risk with them.

Risk Definition

The level of risk is based on the international standard CVSS (Common Vulnerability Scoring System) version 3, which allows for a quantitative estimate of the severity and impact associated with each identified vulnerability, as well as a correlation with the real risk that the materialization of such risks represents for the organization.

The risks are classified as follows:

Classification

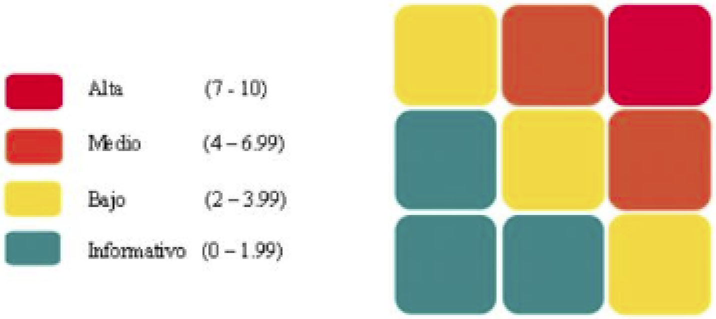
• **Informational:** This type of finding is not a vulnerability itself, but rather characterized as a series of good practices that can be implemented in order to increase the overall digital security posture of an organization.

• **Low:** When the failure is used to collect information associated with the components of the technological infrastructure, such as user enumeration, service identification, and identification of operating systems. Also included are failures that correspond to poor configuration practices of operating systems. These are corrected by making internal configurations to the server. Information related to good practices, which must be taken into account to avoid risks to information assets.

• **Medium:** When the vulnerability allows for unauthorized access or services, but without the possibility of taking on the role of administrator of the access or service. For example, use of insecure protocols and/or weak passwords that compromise the confidentiality of information, access permissions and visualization of internal server structures, poor programming practices such as XSS (Cross Site Scripting) and SQL injections, poor configurations that allow for partial control of an application. Represents a risk to the organization that requires specific conditions to materialize.

• **High:** When the failure allows for some element of the technological infrastructure to become unavailable or to take control over it with administrator privileges. For example, denial of service attacks on the server or arbitrary code execution attacks that allow for obtaining privileges on the server for full or partial control.

These can be fixed by applying patches, fixes, or updating the versions of the services involved in the vulnerability. They should be addressed as a priority because they represent a potential risk to the organization.



Common Vulnerabilities and Exposures (CVE)

This is a security project focused on software and funded by the US National Security Division and maintained by MITRE Corporation. CVE uses the Security Content Automation Protocol (SCAP) to collect information about vulnerabilities and security exposures.

General Results by Risk Level

Vulnerability	Description	Level of Risk
WAF Bypass	It is possible to access the site directly without having to go through the WAF control.	HIGH
Unrestricted File Upload (Web Shell)	The portal allows generating a web shell with any unauthorized file extension loaded onto the server, both in the front-end and back-end, with files such as "php", "html", "exe".	HIGH
Sensitive VPN Connection Information	It is possible to extract information from the VPN connection established between Backbone and Finesa through the Remote shell generated from the Frontend.	HIGH

Brute-Force Attacks	Since there are no anti-robot controls or blocking for failed attempts, it is possible to carry out brute-force attacks without restriction.	HIGH
reCAPTCHA Control Bypass	It is possible to ignore the control in the HTTP request and thus achieve the execution of brute-force attacks to obtain sensitive information and/or flood the database with irrelevant information.	HIGH
Broken Access Control in API	It is possible to impersonate any user without the need to have logged into the administration panel from the "Impersonate" functionality.	HIGH
Validation Failure of Parameters in API	In multiple parameters, adequate validations are not being made when receiving information in the API.	HIGH
Weak Password Policy	It is possible to define weak passwords such as "testtest". The use of weak passwords and the lack of anti-robot controls in the login portal to access the Backend.	HIGH
Session Token Compromise	There is a risk that a hacker will compromise a user's session token in the administration panel and can maintain access for at least 5 days.	MEDIUM
Disabled Session Cookie Flags	It facilitates the compromise of cookies by an unauthorized actor.	MEDIUM

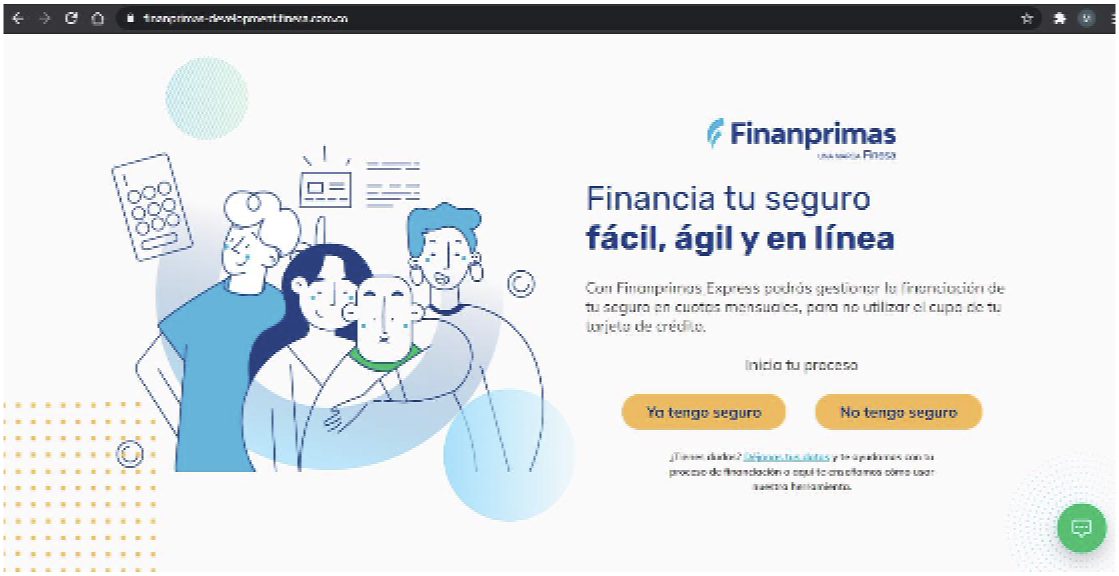
Exposed .htaccess File	A server configuration file is unnecessarily exposed.	LOW
Lack of Security Headers	In the HTTP server responses, it was possible to identify the absence of the following security headers.	LOW
Unrestricted Outbound Traffic on Server	The lack of restrictions on outbound traffic to the internet allowed the execution of a reverse shell on unconventional ports (above port 10000) that makes it possible for a hacker to have more convenience in unauthorized access to the server.	HIGH
Sensible Data Leak through Debug Information	Debug information in the responses allowed for the disclosure of sensitive data.	HIGH

Page Analisis

Web Page Check

URL: https://finanprimas-development.finesa.com.co

Recognisance:



finanprimas-development.finesa.com.co

Finanprimas

una marca Finesa

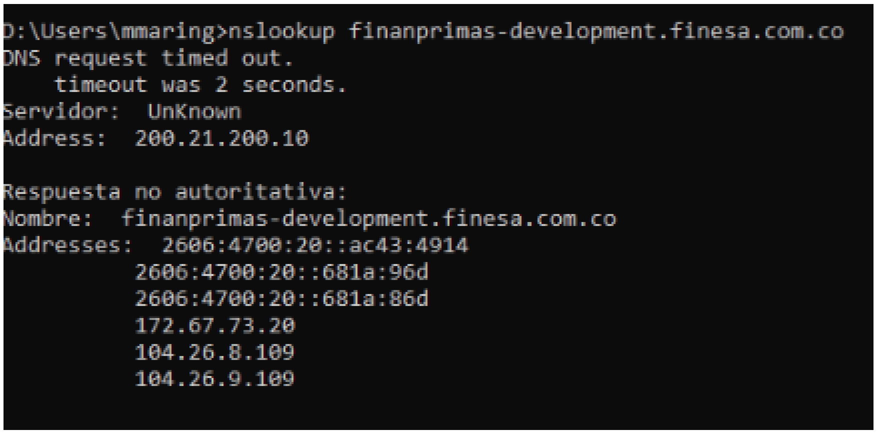
Financia tu seguro
fácil, ágil y en línea

Con Finanprimas Express podrás gestionar la financiación de tu seguro en cuotas mensuales, para no utilizar el cupo de tu tarjeta de crédito.

Inicia tu proceso

¿Tienes dudas? Déjanos tus datos y te ayudamos con tu proceso de financiación o aquí te enseñamos cómo usar nuestra herramienta.

Figura 1. Identificación aplicación web objetivo de la prueba



```
D:\Users\mmaring>nslookup finanprimas-development.finesa.com.co
DNS request timed out.
    timeout was 2 seconds.
Servidor:  UnKnown
Address:  200.21.200.10

Respuesta no autoritativa:
Nombre:  finanprimas-development.finesa.com.co
Addresses:  2606:4700:20::ac43:4914
          2606:4700:20::681a:96d
          2606:4700:20::681a:86d
          172.67.73.20
          104.26.8.109
          104.26.9.109
```

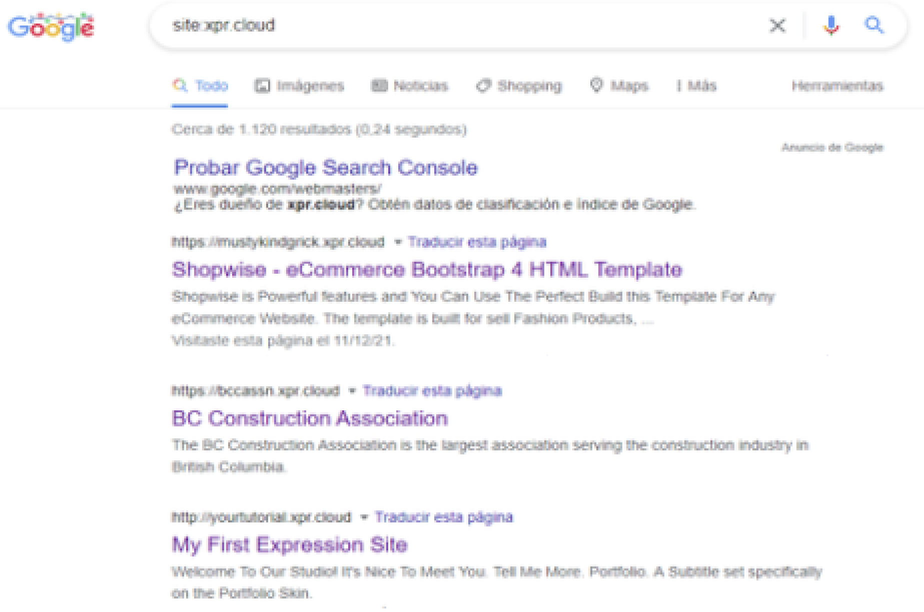
Figura 2. Identificación de dirección IP de aplicación web objetivo de la prueba.

Frontend Findings:

WAF Evasion

Description: Currently, the Finesa website allows connections from any site and not just from CloudFlare, which allows direct access to the site without passing the connection through the WAF control. A hacker can indicate in the hosts file of their operating system that the IP address associated with the domain "finanprimas-development.finesa.com.co" will be that of AWS and not that of CloudFlare, and therefore, evade the WAF control. Currently, Expression's web pages are all hosted on the same public IP address. A hacker can easily identify this IP address by making DNS requests to the websites under the xpr.cloud domain and thus know which IP address to target directly in order to evade CloudFlare's WAF control.

Using a Google Dork, multiple sites under the .xpr.cloud domain can be identified. The results of this search are presented below:



site:xpr.cloud

Cerca de 1.120 resultados (0,24 segundos)

Anuncio de Google

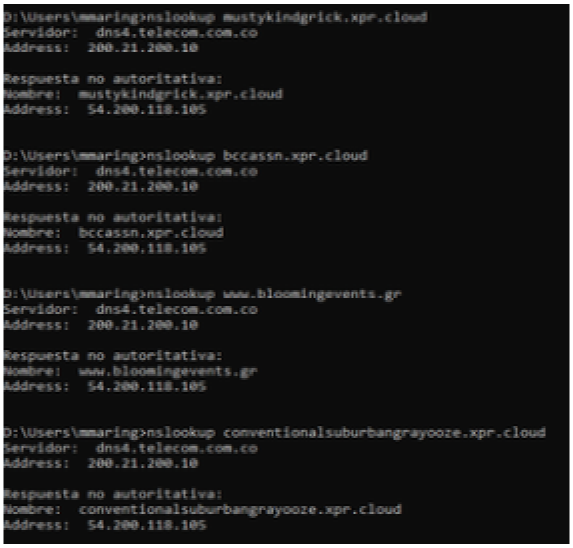
Probar Google Search Console
www.google.com/webmasters/
¿Eres dueño de **xpr.cloud**? Obtén datos de clasificación e índice de Google.

https://mustykindgrick.xpr.cloud ▾ Traducir esta página
Shopwise - eCommerce Bootstrap 4 HTML Template
Shopwise is Powerful features and You Can Use The Perfect Build this Template For Any eCommerce Website. The template is built for sell Fashion Products, ...
Visitaste esta página el 11/12/21.

https://bccassn.xpr.cloud ▾ Traducir esta página
BC Construction Association
The BC Construction Association is the largest association serving the construction industry in British Columbia.

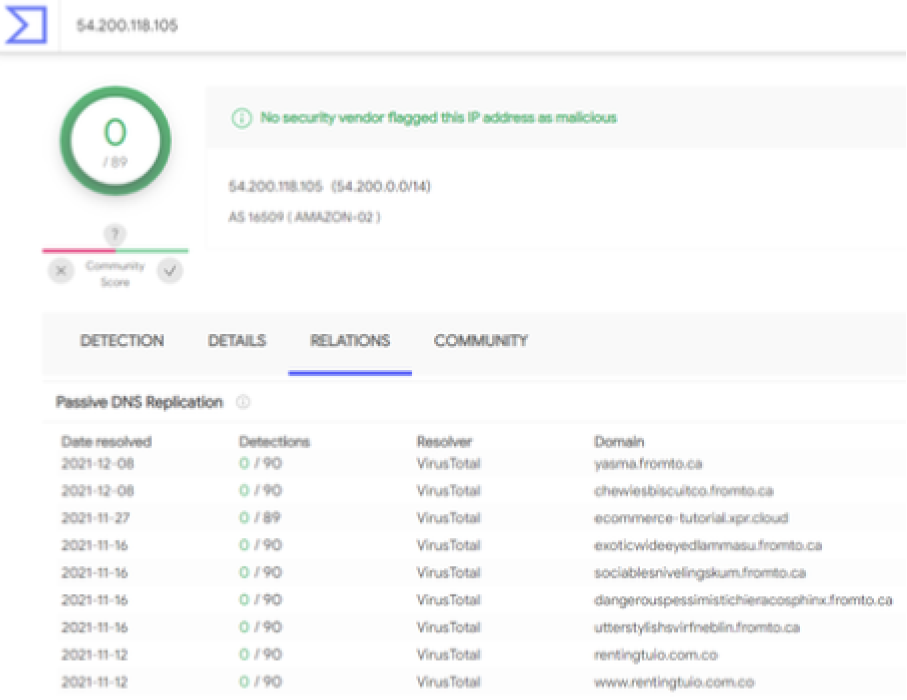
http://yourtutorial.xpr.cloud ▾ Traducir esta página
My First Expression Site
Welcome To Our Studio! It's Nice To Meet You. Tell Me More. Portfolio. A Subtitle set specifically on the Portfolio Skin.

Performing DNS analysis on these web pages, the IP address associated with Expression pages is identified:



```
D:\Users\mmaring>nslookup mustykindgrick.xpr.cloud
Servidor:  dns4.telecom.com.co
Address:  200.21.200.10

Respuesta no autoritativa:
Nombre:  mustykindgrick.xpr.cloud
Address:  54.200.118.105


D:\Users\mmaring>nslookup bccassn.xpr.cloud
Servidor:  dns4.telecom.com.co
Address:  200.21.200.10

Respuesta no autoritativa:
Nombre:  bccassn.xpr.cloud
Address:  54.200.118.105


D:\Users\mmaring>nslookup www.bloomingevents.gr
Servidor:  dns4.telecom.com.co
Address:  200.21.200.10

Respuesta no autoritativa:
Nombre:  www.bloomingevents.gr
Address:  54.200.118.105


D:\Users\mmaring>nslookup conventionalsuburbangrayooze.xpr.cloud
Servidor:  dns4.telecom.com.co
Address:  200.21.200.10

Respuesta no autoritativa:
Nombre:  conventionalsuburbangrayooze.xpr.cloud
Address:  54.200.118.105
```

The IP address for all these web pages is 54.200.118.105. Below is the enumeration of sites that are hosted on that same IP address.



No security vendor flagged this IP address as malicious

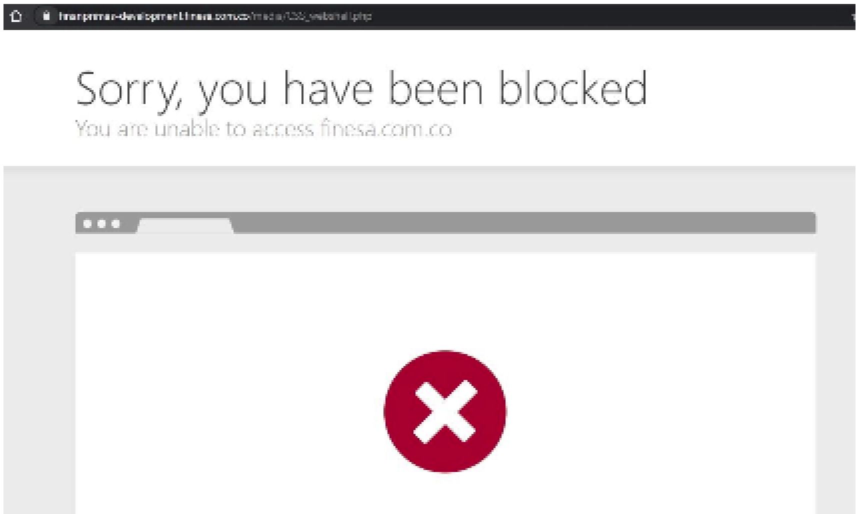
54.200.118.105 (54.200.0.0/14)

AS 16509 (AMAZON-02)

Passive DNS Replication

Date resolved	Detections	Resolver	Domain
2021-12-08	0 / 90	VirusTotal	yasma.fromto.ca
2021-12-08	0 / 90	VirusTotal	chewiesbiscuitco.fromto.ca
2021-11-27	0 / 89	VirusTotal	ecommerce-tutorial.xpr.cloud
2021-11-16	0 / 90	VirusTotal	exoticwideeyedlammasu.fromto.ca
2021-11-16	0 / 90	VirusTotal	sociablesnivelingskum.fromto.ca
2021-11-16	0 / 90	VirusTotal	dangerouspessimistichieracosphinx.fromto.ca
2021-11-16	0 / 90	VirusTotal	utterstylishsvirfneblin.fromto.ca
2021-11-12	0 / 90	VirusTotal	rentingtuio.com.co
2021-11-12	0 / 90	VirusTotal	www.rentingtuio.com.co

When attempting to perform different tests directly on the portal's DNS, it can be identified by Cloudflare.

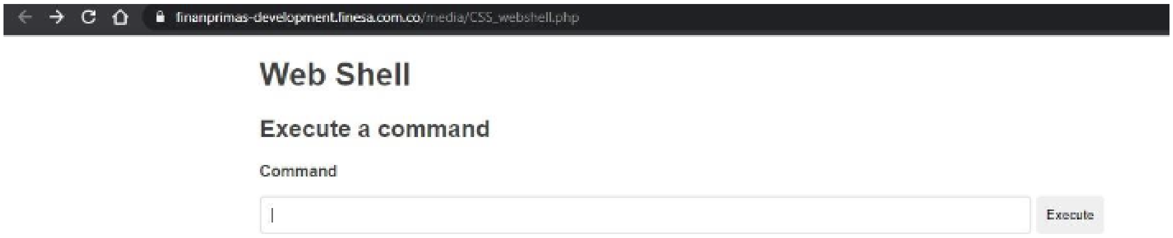


finanprimas-development.finesa.com.co/media/CSS_webshell.php

Sorry, you have been blocked

You are unable to access finesa.com.co

But by editing the host file of the local DNS of the computer where the tests are performed, the public IP address of the server with the XPR.CLOUD domain can be navigated directly on the page without passing through Cloudflare. In this way, the revisions were carried out to avoid Cloudflare blocks, achieving the WAF Bypass.



finanprimas-development.finesa.com.co/media/CSS_webshell.php

Web Shell

Execute a command

Command: |

Figura 7. Evación del Cloudflare y ejecución de la Shell

Level of Risk: 9.0 (High)

Evidence: See video "Finesa_WAF_Evasion.mp4" Affected systems: finanprimas-development.finesa.com.co

Risk: The website is left unprotected and there is a false sense of controlling some cyber attacks with the acquired WAF control. WAF systems can protect websites against multiple web application attacks, such as:

- Cookie protection.

- Protection against information leakage.

- Cross Site Request Forgery.

- Unrestricted file upload.

- Parameter tampering.

- Distributed Denial of Service (DDoS).

- Directory listing (Path Traversal).

- Input data validation (Partially, depending on the application architecture and WAF configuration).

- Buffer Overflow.

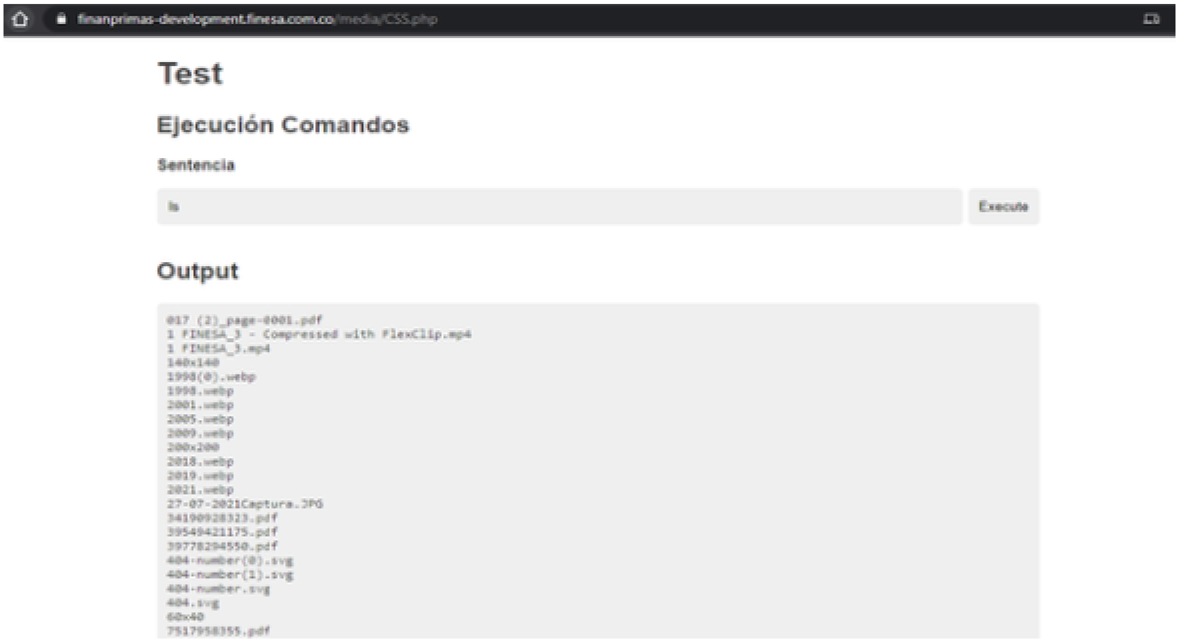
Recommendation: Once the WAF control is implemented, limit the connections on the server so that it can only receive requests coming from CloudFlare. The use of a WAF becomes especially relevant in the case of specific vulnerabilities. For example, some of the vulnerabilities identified through penetration testing or source code reviews can be partially or completely closed using this technology. Even if it were possible to promptly and reasonably fix the vulnerability in the application, the modified version can usually only be implemented in the next maintenance window or application release.

Unrestricted File Upload (Web Shell)

Description: File upload represents a significant risk to web applications. The first step in many attacks is to upload code to the system to be attacked. Then the attacker only needs to find a way to execute the code. The use of file upload helps the attacker to perform the first step.

In the section "Cotiza la financiación de tu seguro" in the section "Adjunta la póliza que quieres financiar", and in the "media" section of the administration panel, proper validation of the type of document (file extension) that the user is uploading is not being performed. On the user-facing site, it was found that there is validation at the javascript level, which can be bypassed by the user tricking the system into thinking that a file is a JPG but is actually a shell, allowing any unauthorized file extension such as "php", "html", "exe", among others to be uploaded to the server.

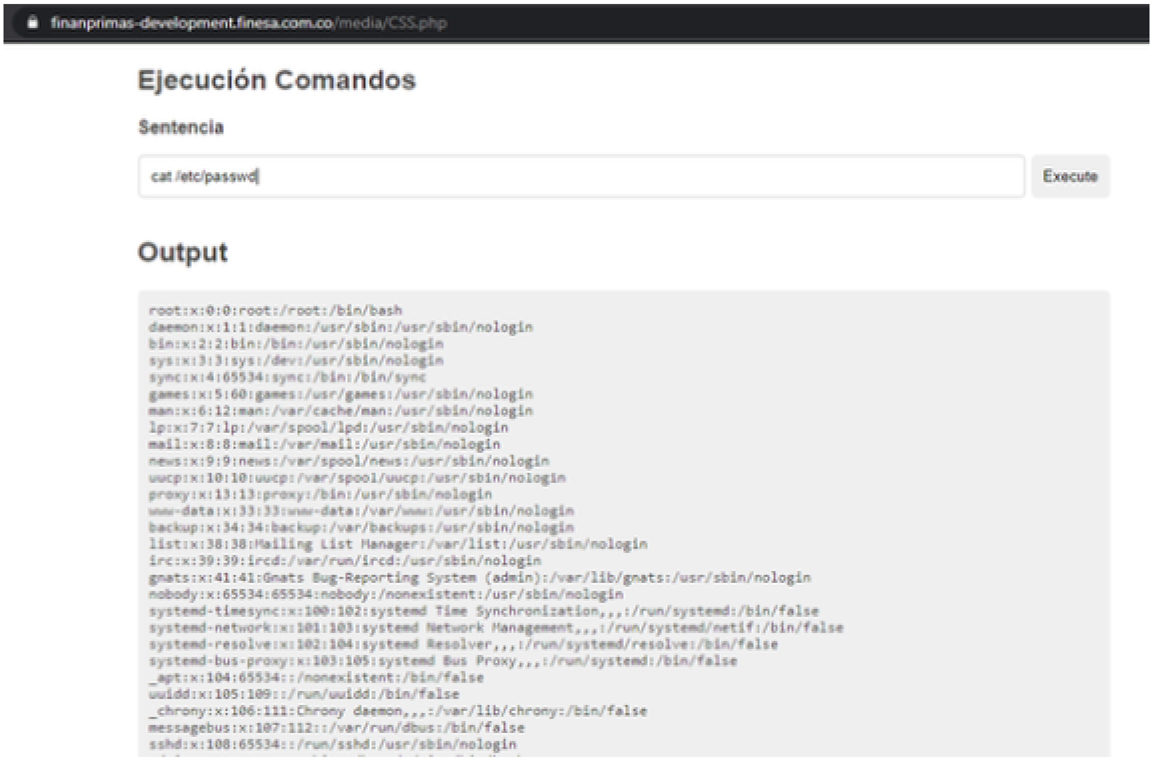
On the Finesa website, a malicious file was uploaded that allows for the execution of commands in the operating system through a web shell. The images below show the execution of commands:



```
ls
```

```
017 (2)_page-0001.pdf
1 FINESA_3 - Compressed with FlexClip.mp4
1 FINESA_3.mp4
140x140
1998(0).webp
1998.webp
2001.webp
2005.webp
2009.webp
200x200
2018.webp
2019.webp
2021.webp
27-07-2021Captura.JPG
34190928323.pdf
39549421175.pdf
39778294550.pdf
404-number(0).svg
404-number(1).svg
404-number.svg
404.svg
60x40
7517958355.pdf
```

Figura 8. Ejecución de comandos a través de Web Shell



```
cat /etc/passwd
```

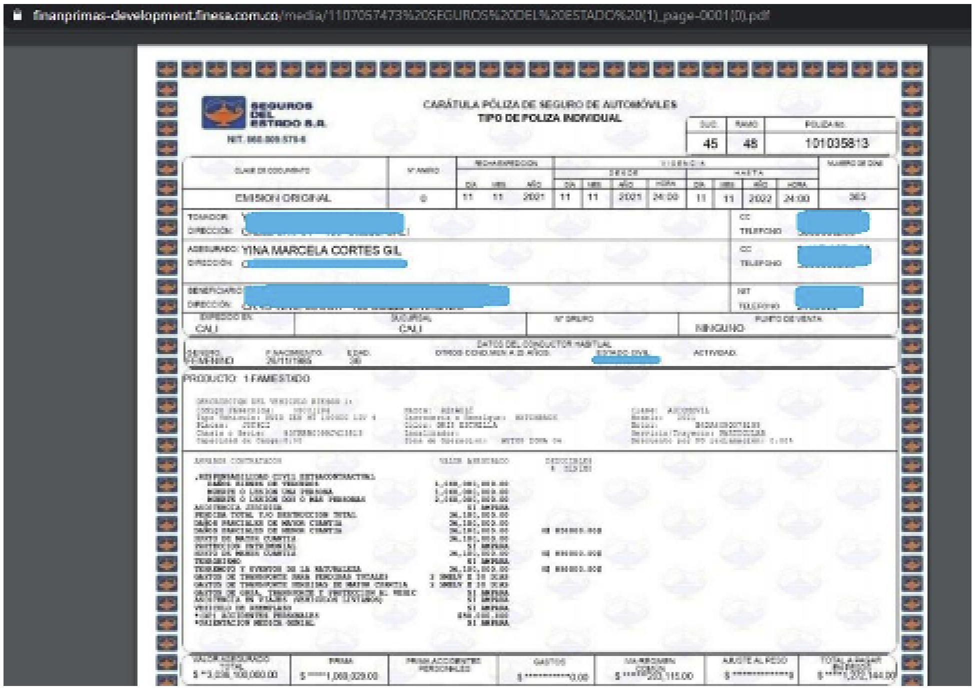
```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
uuidd:x:105:109::/run/uuidd:/bin/false
_chrony:x:106:111:Chrony daemon,,,:/var/lib/chrony:/bin/false
messagebus:x:107:112::/var/run/dbus:/bin/false
sshd:x:108:65534::/run/sshd:/usr/sbin/nologin
```

[illegible]

Unrestricted File Upload (Web Shell)

Route: https://finanprimas-development.finesa.com.co/media/CSS.php

Through this vulnerability, by listing the existing files in the /media folder of the web server, it is possible to identify other files and start browsing and downloading customer information on the website, compromising the confidentiality and availability of the information stored there. Below are some of the images associated with access to files containing sensitive customer information.



finanprimas-development.finesa.com.co/media/1107057473%20SEGUROS%20DEL%20ESTADO%20(1)_page-0001(0).pdf

SEGUROS DEL ESTADO S.A.
NIT. 860.009.578-6

CARÁTULA PÓLIZA DE SEGURO DE AUTOMÓVILES
TIPO DE POLIZA INDIVIDUAL

SUC.	RAMO	POLIZA No.
45	48	101035813

CLASE DE DOCUMENTO	Nº ANEXO	FECHA EXPEDICION DIA	MES	AÑO	VIGENCIA DESDE DIA	MES	AÑO	HORA	HASTA DIA	MES	AÑO	HORA	NUMERO DE DIAS
EMISION ORIGINAL	0	11	11	2021	11	11	2021	24:00	11	11	2022	24:00	365

TOMADOR: [redacted] CC [redacted]
DIRECCIÓN: TELEFONO
ASEGURADO: YINA MARCELA CORTES GIL CC [redacted]
DIRECCIÓN: [redacted] TELEFONO
BENEFICIARIO: [redacted] NIT [redacted]
DIRECCIÓN: TELEFONO

EXPEDIDO EN	SUCURSAL	Nº GRUPO	PUNTO DE VENTA
CALI	CALI		NINGUNO

DATOS DEL CONDUCTOR HABITUAL

GENERO	F.NACIMIENTO	EDAD	OTROS COND.MEN A 25 AÑOS	ESTADO CIVIL	ACTIVIDAD
FEMENINO	20/11/1985	36		[redacted]	

PRODUCTO: 1 FAMESTADO

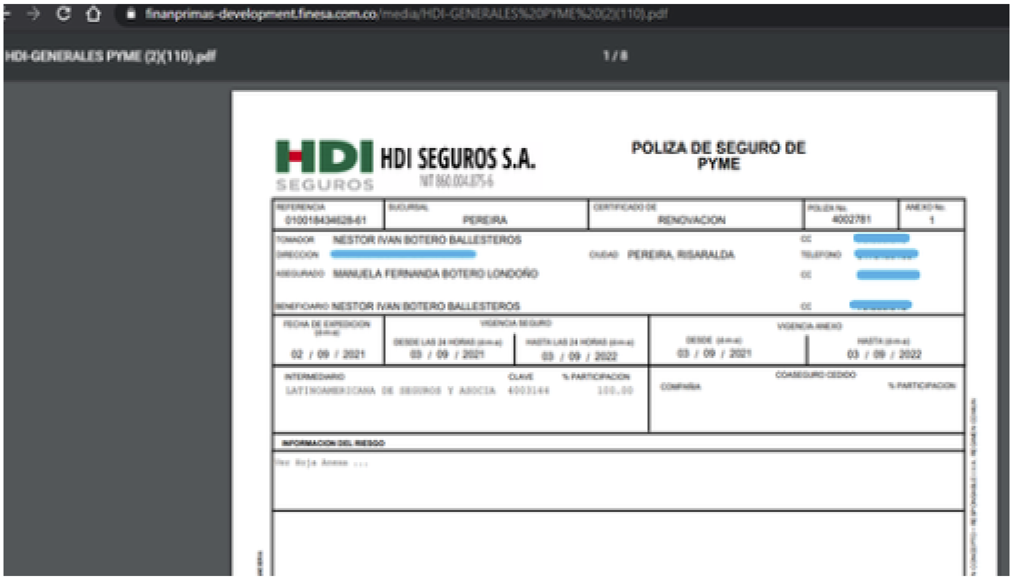
DESCRIPCION DEL VEHICULO RIESGO 1: [illegible]

AMPAROS CONTRATADOS — VALOR ASEGURADO — DEDUCIBLES

RESPONSABILIDAD CIVIL EXTRACONTRACTUAL
DAÑOS BIENES DE TERCEROS
MUERTE O LESION UNA PERSONA
MUERTE O LESION DOS O MAS PERSONAS
ASISTENCIA JURIDICA — SI AMPARA
PERDIDA TOTAL Y/O DESTRUCCION TOTAL
DAÑOS PARCIALES DE MAYOR CUANTIA
DAÑOS PARCIALES DE MENOR CUANTIA
HURTO DE MAYOR CUANTIA
PROTECCION PATRIMONIAL — SI AMPARA
HURTO DE MENOR CUANTIA
TERRORISMO — SI AMPARA
TERREMOTO Y EVENTOS DE LA NATURALEZA
GASTOS DE TRANSPORTE PARA PERDIDAS TOTALES
GASTOS DE TRANSPORTE PERDIDAS DE MAYOR CUANTIA
GASTOS DE GRUA, TRANSPORTE Y PROTECCION AL VEHIC — SI AMPARA
ASISTENCIA EN VIAJES — SI AMPARA
VEHICULO DE REEMPLAZO — SI AMPARA
SPT ACCIDENTES PERSONALES
*ORIENTACION MEDICA GENERAL — SI AMPARA

VALOR ASEGURADO TOTAL	PRIMA	PRIMA ACCIDENTES PERSONALES	GASTOS	IVA REGIMEN COMUN	AJUSTE AL PESO	TOTAL A PAGAR EN PESOS
$ **3,036,100,000.00	$ *****1,069,029.00		$ ***********0.00	$ ******203,115.00	$ *************9	$ *****1,272,144.00

Figura 10. Acceso a archivos sensibles del sistema operativo por medio de web Shell.



finanprimas-development.finesa.com.co/media/HDI-GENERALES%20PYME%20(2)(110).pdf

HDI-GENERALES PYME (2)(110).pdf 1 / 8

HDI SEGUROS
HDI SEGUROS S.A.
NIT 860.004.875-6

POLIZA DE SEGURO DE PYME

REFERENCIA	SUCURSAL	CERTIFICADO DE	POLIZA No.	ANEXO No.
010018434628-61	PEREIRA	RENOVACION	4002781	1

TOMADOR NESTOR IVAN BOTERO BALLESTEROS CC [redacted]
DIRECCION [redacted] CIUDAD PEREIRA, RISARALDA TELEFONO [redacted]
ASEGURADO MANUELA FERNANDA BOTERO LONDOÑO CC [redacted]
BENEFICIARIO NESTOR IVAN BOTERO BALLESTEROS CC [redacted]

FECHA DE EXPEDICION (d-m-a)	VIGENCIA SEGURO DESDE LAS 24 HORAS (d-m-a)	VIGENCIA SEGURO HASTA LAS 24 HORAS (d-m-a)	VIGENCIA ANEXO DESDE (d-m-a)	VIGENCIA ANEXO HASTA (d-m-a)
02 / 09 / 2021	03 / 09 / 2021	03 / 09 / 2022	03 / 09 / 2021	03 / 09 / 2022

INTERMEDIARIO	CLAVE	% PARTICIPACION	COASEGURO CEDIDO COMPAÑIA	% PARTICIPACION
LATINOAMERICANA DE SEGUROS Y ASOCIA	4003144	100.00		

INFORMACION DEL RIESGO

Ver Hoja Anexa ...

Figura 11. Acceso a archivos sensibles del sistema operativo por medio de web Shell.

Risk Level: 10.0 (High)

Evidence: See videos

Finesa_CargaArchivos_NoAutorizado.mp4

Affected Systems:

https://finanprimas-development.finesa.com.co/

https://finanprimas-development.finesa.com.co/media/media.pht
HTTP POST https://finanprimas-development.finesa.com.co/financiar/adjuntar-poliza/{id}

Risk: The successful exploitation of this vulnerability allows for:

- Server-side attacks: The web server was compromised by loading and executing a web shell that allows for command execution, exploration of system files, exploration of local resources, among others. Even more serious was the ability to establish a reverse shell connection to the attackers' computer, allowing for post-exploitation activities in a much more comfortable way, revealing bad practices in the perimeter controls of the AWS instances. An attacker can use these accesses to perform privilege escalation on the local server, install additional tools, and move laterally on Backbone AWS servers to compromise additional assets.
- Client-side attacks: Uploading malicious files can make the website vulnerable to client-side attacks, such as XSS or compromise of sensitive user information browsing the web page, such as session cookies.
- Uploading files with sensitive content (pornographic, material that promotes bad habits and negative values, disturbing resources, among others) that are disseminated on networks under the official domain of Finesa.
- Uploading malware to the server not only to affect the Finesa server but also to use the Finesa domain and disseminate malware to its clients. For example, sharing the URL "https://finanprimas-development.finesa.com.co/media/beneficios.exe" to its clients.

Recommendation: The best way to protect against web shells is to make it impossible to use them on your system. You can do this by:

• Strengthening your server to detect and locally block such connections.

• Removing all excess permissions.

• Blocking potentially dangerous functions.

• Restricting the execution of scripts in upload directories.

• Analyze malware at the moment files are uploaded and prevent them from being within the system.

• Complement additional security controls to the WAF such as a RASP or with direct protection on the server in case the WAF control security is bypassed, to have direct control within the application or server.

Note: Review the attached document "Remediation and Security Controls.pdf"

Apply proper validation of the file extension that the user wants to upload to the site, not only from the frontend but also from the backend that receives these parameters. Deny all extensions and implement the use of a "positive list" to indicate which are the only allowed file extensions in the upload functionality.

Define a route on the server to upload sensitive files (policies and/or documents) that users upload, so that it cannot be accessed by anyone who goes to the resource "https://finanprimas-development.finesa.com.co/media/". Through the obtained accesses, it was possible to access all the information stored in the path: /var/www/expression/clients/finanprimas_development_finesa_finesa_com_co/web/media, in other web browsers without any authentication. Additionally, it is recommended to store files on the web server named using Digest functions such as md5, not with the plain name with which they were stored in the server web upload folder.

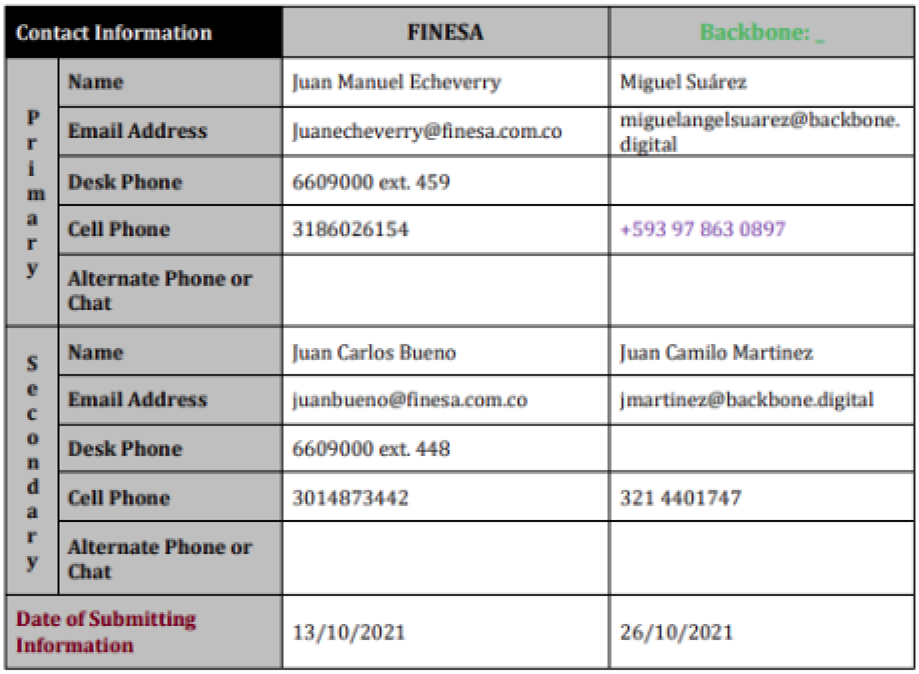
Sensitive VPN Information

Description: Through the remote shell attack, it was possible to extract sensitive information. The obtained information refers to the communication and encryption keys that should be used for point-to-point VPN connection between Finesa and Backbone on the AWS platform.

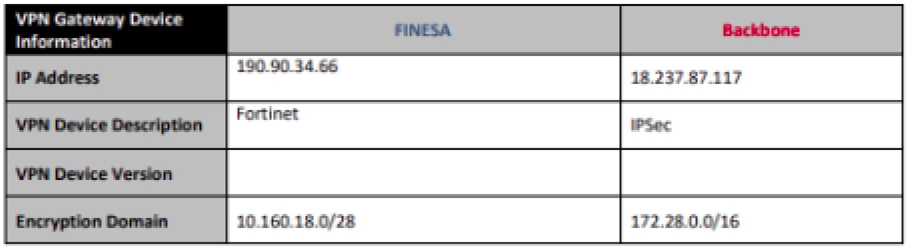
Risk Level: 7.0 (High)
Evidence:

Formato de Configuración VPN Pruebas Finesa – Backbone

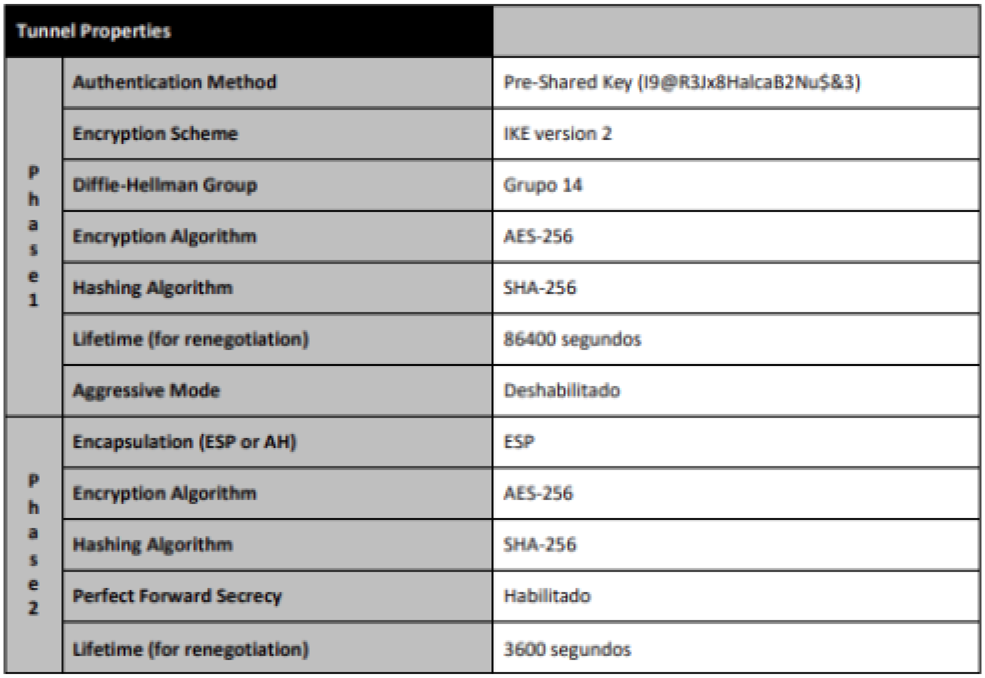
VPN Technical Information:



Contact Information		FINESA	Backbone: _
Primary	Name	Juan Manuel Echeverry	Miguel Suárez
	Email Address	Juanecheverry@finesa.com.co	miguelangelsuarez@backbone.digital
	Desk Phone	6609000 ext. 459	
	Cell Phone	3186026154	+593 97 863 0897
	Alternate Phone or Chat		
Secondary	Name	Juan Carlos Bueno	Juan Camilo Martinez
	Email Address	juanbueno@finesa.com.co	jmartinez@backbone.digital
	Desk Phone	6609000 ext. 448	
	Cell Phone	3014873442	321 4401747
	Alternate Phone or Chat		
Date of Submitting Information		13/10/2021	26/10/2021



VPN Gateway Device Information	FINESA	Backbone
IP Address	190.90.34.66	18.237.87.117
VPN Device Description	Fortinet	IPSec
VPN Device Version		
Encryption Domain	10.160.18.0/28	172.28.0.0/16



Tunnel Properties		
Phase 1	Authentication Method	Pre-Shared Key (I9@R3Jx8HalcaB2Nu$&3)
	Encryption Scheme	IKE version 2
	Diffie-Hellman Group	Grupo 14
	Encryption Algorithm	AES-256
	Hashing Algorithm	SHA-256
	Lifetime (for renegotiation)	86400 segundos
	Aggressive Mode	Deshabilitado
Phase 2	Encapsulation (ESP or AH)	ESP
	Encryption Algorithm	AES-256
	Hashing Algorithm	SHA-256
	Perfect Forward Secrecy	Habilitado
	Lifetime (for renegotiation)	3600 segundos

Figura 13. Figura 1. Extracción Información VPN parte 2

Affected systems: https://finanprimas-development.finesa.com.co/

Risk: From this information, social engineering techniques can be used on the contacts of the responsible persons registered in these documents. Obtaining information about the specifications of the VPN connection, although the channel itself cannot be directly interrupted or compromised, attempts to impersonate access could be made using brute force attacks and having information about the type of connection and platform used. The information found refers to technical specifications of the VPN connection and contact data of responsible persons at both points, both in Backbone and Finesa.

Recommendation: Apply access controls and minimum privileges to prevent access to sensitive information. Avoid placing configuration information and personal information located within the server.

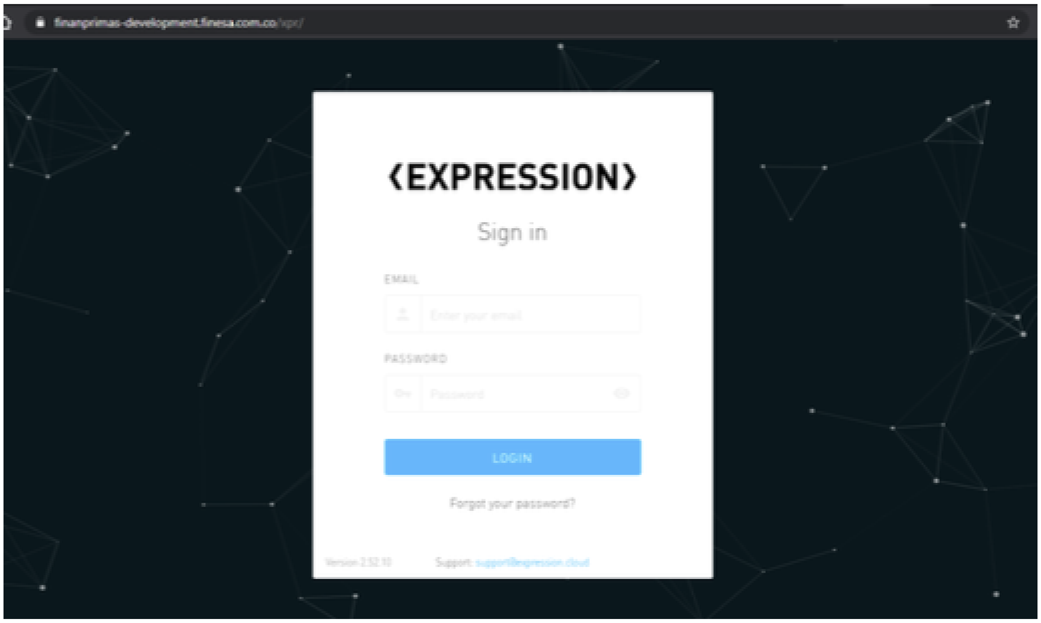
Brute Force Attack

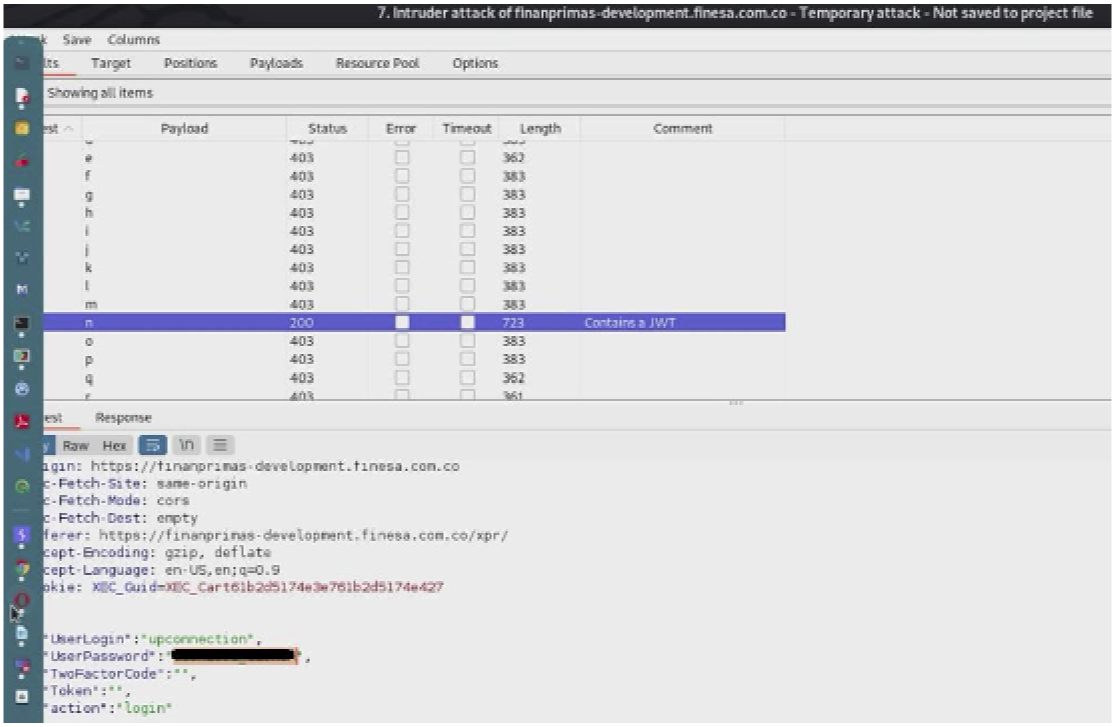
Description: The authentication form for the administration site does not show anti-robot controls, nor rules for blocking failed attempts for the same user. This configuration facilitates the execution of brute force attacks on the form, that is, multiple authentication attempts are made until access (username and password) to the administration panel is identified.

A brute force attack can manifest itself in many different ways, but mainly consists of an attacker configuring default values, making requests to a server using those values, and then analyzing the response. In order to increase the efficiency of the attack, a dictionary (with or without mutations) or a traditional brute force attack (with certain classes of characters, for example: alphanumeric, special, case sensitive) can be used. Considering a given method, the number of attempts, the efficiency of the system that carries out the attack, and the estimated efficiency of the system that is being attacked, the attacker can approximately calculate how long it will take to send all the selected default values.

Risk Level: 7.0 (High)

Evidence: Finesa_BruteForceAttacks.mp4




7. Intruder attack of finanprimas-development.finesa.com.co - Temporary attack - Not saved to project file
k Save Columns
lts Target Positions Payloads Resource Pool Options
Showing all items

est	Payload	Status	Error	Timeout	Length	Comment
	e	403	□	□	362	
	f	403	□	□	383	
	g	403	□	□	383	
	h	403	□	□	383	
	i	403	□	□	383	
	j	403	□	□	383	
	k	403	□	□	383	
	l	403	□	□	383	
	m	403	□	□	383	
	n	200	□	□	723	Contains a JWT
	o	403	□	□	383	
	p	403	□	□	383	
	q	403	□	□	362	
	r	403	□	□	361	

est Response
y Raw Hex \n

```
igin: https://finanprimas-development.finesa.com.co
c-Fetch-Site: same-origin
c-Fetch-Mode: cors
c-Fetch-Dest: empty
ferer: https://finanprimas-development.finesa.com.co/xpr/
cept-Encoding: gzip, deflate
cept-Language: en-US,en;q=0.9
okie: XEC_Guid=XEC_Cart61b2d5174e3e761b2d5174e427


"UserLogin":"upconnection",
"UserPassword":"[redacted]",
"TwoFactorCode":"",
"Token":"",
"action":"login"
```

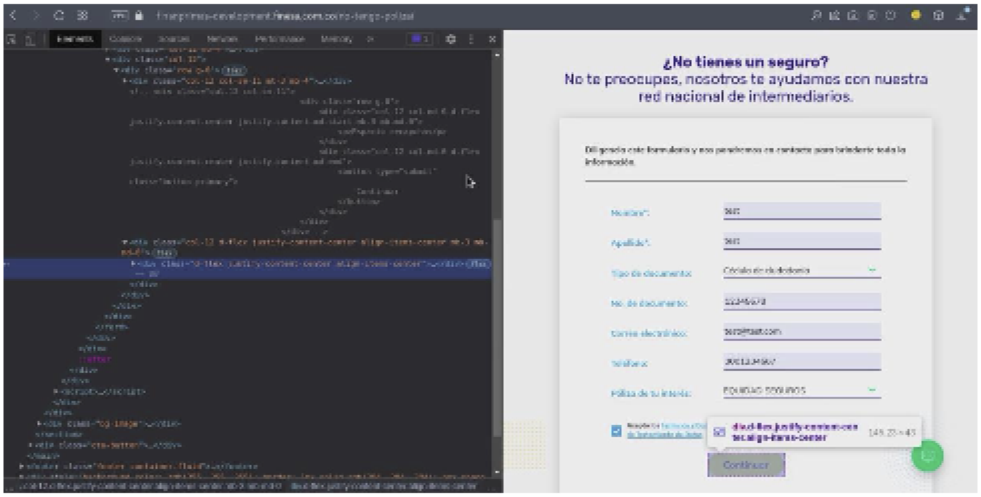
Affected systems: https://finanprimas-development.finesa.com.co/xpr

Risk: Brute force attacks are often used to attack authentication and discover hidden content/pages within a web application. These attacks are usually sent through GET and POST requests to the server. With regard to authentication, brute force attacks are often mounted when there is no account lockout policy, as is the case in the analyzed application. Successful exploitation of this vulnerability allows an external attacker to gain unauthorized access to the administration panel.

Recommendation: Implement anti-robot controls and rules for blocking users or sessions/IPs for failed authentication attempts. Additionally, filters can be implemented based on malicious IP addresses that have been previously identified as performing brute force attacks.

Recaptcha Evasion

Description: The reCAPTCHA control implemented on some forms of the site presents a critical flaw in that it is not being properly validated. The user can ignore it in the HTTP request, thus achieving the execution of brute force attacks to obtain sensitive information and/or to flood the database with irrelevant information.



finanprimas-development.finesa.com.co/no-tengo-poliza

¿No tienes un seguro?
No te preocupes, nosotros te ayudamos con nuestra red nacional de intermediarios.

Diligencia este formulario y nos pondremos en contacto para brindarte toda la información.

Nombre*:	[illegible]
Apellido*:	[illegible]
Tipo de documento:	Cédula de ciudadanía
No. de documento:	[illegible]
Correo electrónico:	[illegible]
Teléfono:	[illegible]
Póliza de tu interés:	EQUIDAD SEGUROS

Risk level: 7.0 (High)

Evidence: Finesa_Evasion-reCaptcha.mp4

Affected systems: https://finanprimas-development.finesa.com.co/no-tengo-poliza/

Risk: Database flooding with false information can occur, hindering operations such as "contact us" (no tengo poliza).

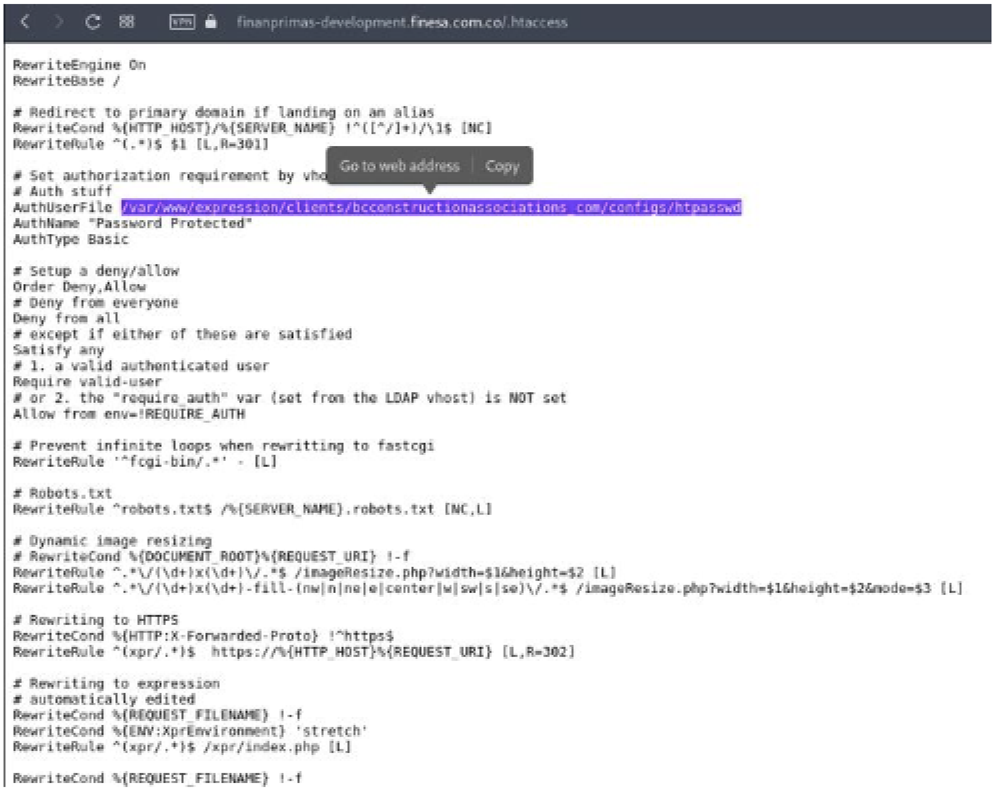
Recommendation: Properly validate reCAPTCHA before processing the HTTP request made by the user. Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) is used to distinguish normal users from bots. Automation is used in an attempt to analyze and determine the response to visual and/or auditory CAPTCHA tests. Apart from the conventional visual and auditory CAPTCHA, sometimes puzzle-solving mini-games or arithmetic exercises are used. Some of these may include context-specific challenges. The process that determines the response may use tools to perform optical character recognition, compare them to a prepared database of previously generated images, or use another form of machine reading or human farms.

Visible .htaccess file

Description: The .htaccess resource is currently exposed on the website, presenting a leakage of information regarding the web service configuration contained in the file.

Risk Level: 3.0 (Low)

Evidence: Exposicion_HTACCESS.png



```
RewriteEngine On
RewriteBase /

# Redirect to primary domain if landing on an alias
RewriteCond %{HTTP_HOST}/%{SERVER_NAME} !^([^/]+)/\1$ [NC]
RewriteRule ^(.*)$ $1 [L,R=301]

# Set authorization requirement by vho
# Auth stuff
AuthUserFile /var/www/expression/clients/bcconstructionassociations_com/configs/htpasswd
AuthName "Password Protected"
AuthType Basic

# Setup a deny/allow
Order Deny,Allow
# Deny from everyone
Deny from all
# except if either of these are satisfied
Satisfy any
# 1. a valid authenticated user
Require valid-user
# or 2. the "require_auth" var (set from the LDAP vhost) is NOT set
Allow from env=!REQUIRE_AUTH

# Prevent infinite loops when rewritting to fastcgi
RewriteRule '^fcgi-bin/.*' - [L]

# Robots.txt
RewriteRule ^robots.txt$ /%{SERVER_NAME}.robots.txt [NC,L]

# Dynamic image resizing
# RewriteCond %{DOCUMENT_ROOT}%{REQUEST_URI} !-f
RewriteRule ^.*\/(\d+)x(\d+)\/.*$ /imageResize.php?width=$1&height=$2 [L]
RewriteRule ^.*\/(\d+)x(\d+)-fill-(nw|n|ne|e|center|w|sw|s|se)\/.*$ /imageResize.php?width=$1&height=$2&mode=$3 [L]

# Rewriting to HTTPS
RewriteCond %{HTTP:X-Forwarded-Proto} !^https$
RewriteRule ^(xpr/.*)$  https://%{HTTP_HOST}%{REQUEST_URI} [L,R=302]

# Rewriting to expression
# automatically edited
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{ENV:XprEnvironment} 'stretch'
RewriteRule ^(xpr/.*)$ /xpr/index.php [L]

RewriteCond %{REQUEST_FILENAME} !-f
```

Systems affected: https://finanprimas-development.finesa.com.co/.htaccess

Risk: A server configuration file is being unnecessarily exposed.

Recommendation: Ensure that the .htaccess file cannot be accessed from the website by users.

Security Header Missing From Response

The following security headers are missing in the HTTP responses of the main web page:

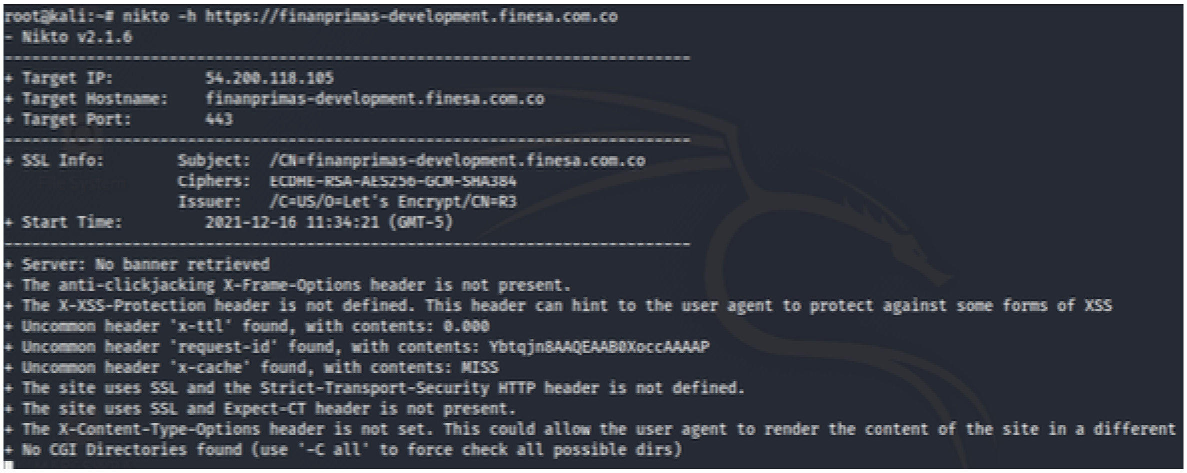
● Strict-Transport-Security (The website is implemented over HTTP)

● Content-Security-Policy

- X-Frame-Options
- X-XSS-Protection
- X-Content-Type-Options
- Referrer-Policy
- Feature-Policy

Risk Level: 3.0 (Low)

The evidence of this finding is presented below:



```
root@kali:~# nikto -h https://finanprimas-development.finesa.com.co
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          54.200.118.105
+ Target Hostname:    finanprimas-development.finesa.com.co
+ Target Port:        443
---------------------------------------------------------------------------
+ SSL Info:        Subject:  /CN=finanprimas-development.finesa.com.co
                   Ciphers:  ECDHE-RSA-AES256-GCM-SHA384
                   Issuer:   /C=US/O=Let's Encrypt/CN=R3
+ Start Time:         2021-12-16 11:34:21 (GMT-5)
---------------------------------------------------------------------------
+ Server: No banner retrieved
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ Uncommon header 'x-ttl' found, with contents: 0.000
+ Uncommon header 'request-id' found, with contents: Ybtqjn8AAQEAAB0XoccAAAAP
+ Uncommon header 'x-cache' found, with contents: MISS
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

- **Missing X-Frame Options header:** The remote web server does not set an X-Frame-Options response header. This could expose the website to a clickjacking attack, where an attacker can trick a visiting user of the page to click on a vulnerable area of the page that is different from what the user perceives the page to be. This can lead to a user performing fraudulent or malicious transactions. This header is supported by major web browsers.

- **Lack of Content Security Policy header:** This header is an effective measure to protect the website from Cross Site Scripting (XSS) attacks. By including a whitelist of approved content sources, it can prevent the browser from loading malicious assets. For detailed information on the use and implementation of this security header, please refer to the following source:

https://developers.google.com/web/fundamentals/security/csp?hl=es

- **Lack of HSTS (Strict Transport Security) header:** It is a feature that allows strengthening security in the implementation of TLS by making the User Agent enforce the use of HTTPS. The most important security vulnerability that HSTS can prevent is SSL-stripping in Man in the Middle (MiTM) attacks. The website of the Vial Túnel Aburrá Oriente concession is implemented over the HTTP protocol, which is why all communications are in plain text. Implementation of the HTTPS protocol with a digital certificate signed by a valid certification authority is recommended in order to implement the HSTS security policy.

Recommended value "Strict-Transport-Security: max-age = 31536000; includeSubDomains".

- **Cookies without HttpOnly flag:** The remote web application sets cookies on both unauthenticated and authenticated user sessions. However, these cookies are not marked as 'HttpOnly', which means that a malicious client-side script, such as JavaScript, could read them. The HttpOnly flag is a security mechanism to protect against Cross Site Scripting (XSS) attacks that was proposed by Microsoft and initially implemented in Internet Explorer. All modern browsers now support it.

Recommendation: Implementation of the security headers and features mentioned above is recommended.

- Strict-Transport-Security
- Content-Security-Policy
- X-Frame-Options
- X-XSS-Protection
- X-Content-Type-Options
- Referrer-Policy
- Feature-Policy

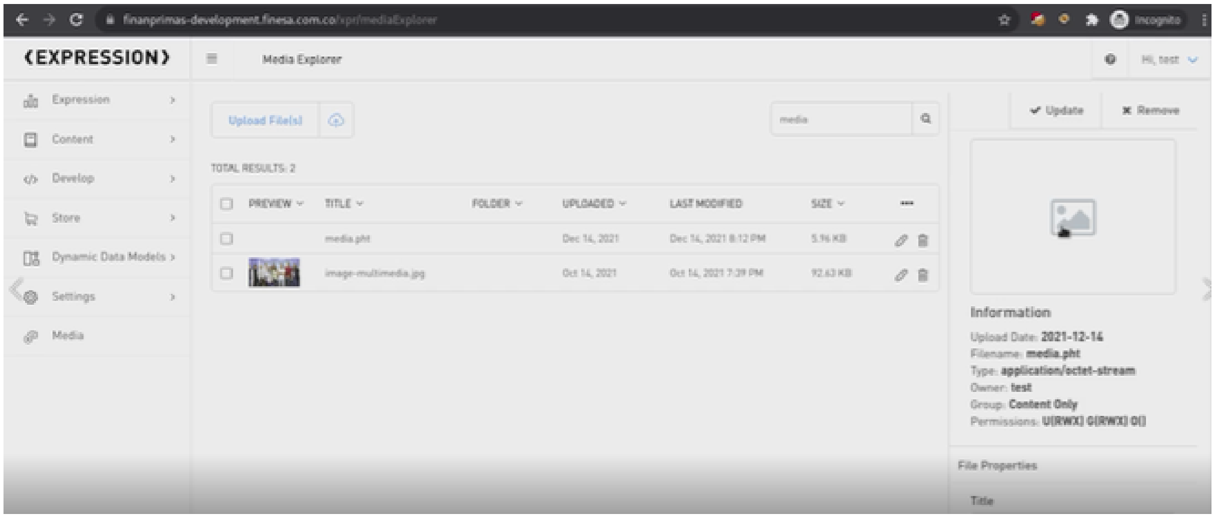
Backend Findings

File Upload Without Restrictions

Description: File upload represents a significant risk for web applications. The first step in many attacks is to upload code to the system to be attacked. Then, the attacker only needs to find a way to execute the code. The use of file upload helps the attacker to perform the first step.

In the site's administration panel, although it is validated in the backend that files such as those mentioned above are not uploaded, others such as "pht", "phtml", among others, are allowed.

From the backend of the Finesa website, a malicious file was successfully uploaded that allows the execution of commands in the operating system through a web shell. The following images show the execution of commands:



finanprimas-development.finesa.com.co/xpr/mediaExplorer

media

TOTAL RESULTS: 2

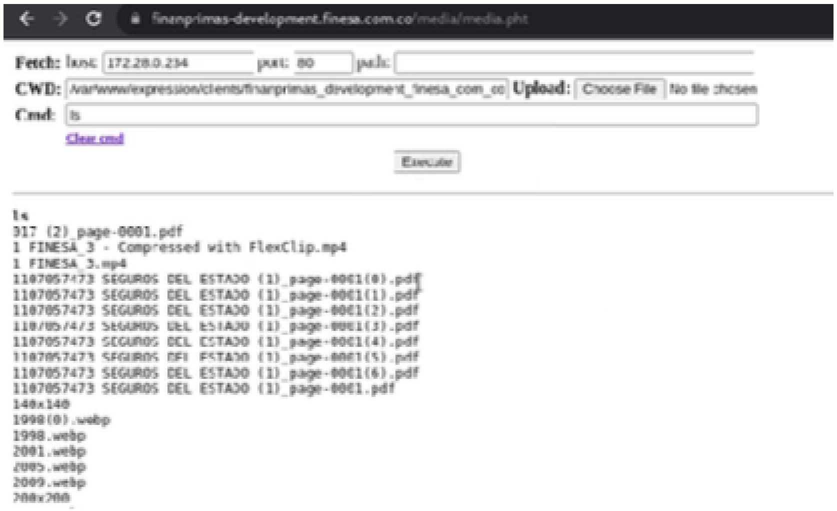
□	PREVIEW	TITLE	FOLDER	UPLOADED	LAST MODIFIED	SIZE
□		media.pht		Dec 14, 2021	Dec 14, 2021 8:12 PM	5.96 KB
□		image-multimedia.jpg		Oct 14, 2021	Oct 14, 2021 7:39 PM	92.63 KB

Information

Upload Date: 2021-12-14
Filename: media.pht
Type: application/octet-stream
Owner: test
Group: Content Only
Permissions: U[RWX] G[RWX] O[]

File Properties

Title



finanprimas-development.finesa.com.co/media/media.pht

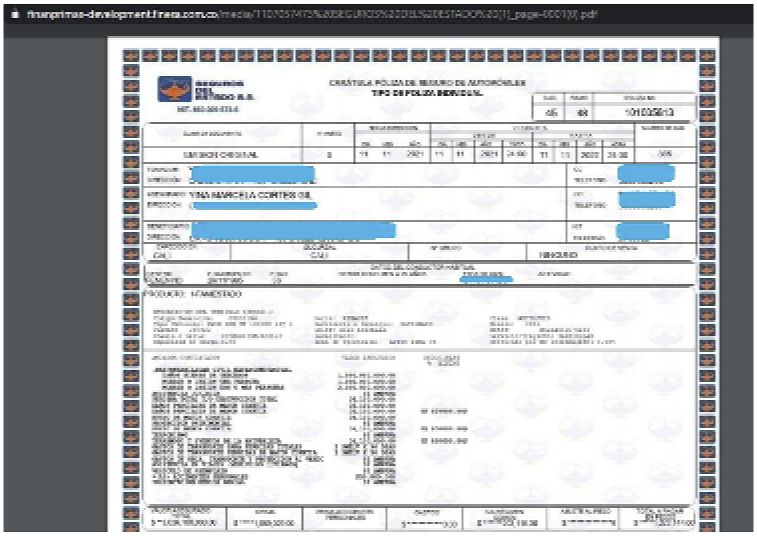
Fetch: host: 172.28.0.234 port: 80 path:
CWD: /var/www/expression/clients/finanprimas_development_finesa_com_co Upload: Choose File No file chosen
Cmd: ls

```
ls
317 (2)_page-0001.pdf
1 FINESA_3 - Compressed with FlexClip.mp4
1 FINESA_3.mp4
1107057473 SEGUROS DEL ESTADO (1)_page-0001(0).pdf
1107057473 SEGUROS DEL ESTADO (1)_page-0001(1).pdf
1107057473 SEGUROS DEL ESTADO (1)_page-0001(2).pdf
1107057473 SEGUROS DEL ESTADO (1)_page-0001(3).pdf
1107057473 SEGUROS DEL ESTADO (1)_page-0001(4).pdf
1107057473 SEGUROS DEL ESTADO (1)_page-0001(5).pdf
1107057473 SEGUROS DEL ESTADO (1)_page-0001(6).pdf
1107057473 SEGUROS DEL ESTADO (1)_page-0001.pdf
140x140
1998(0).webp
1998.webp
2001.webp
2005.webp
2009.webp
200x200
```

Path: https://finanprimas-development.finesa.com.co/media/media.pht

Through this vulnerability, by listing the existing files in the /media folder of the web server, it is possible to identify other files and begin to navigate and download customer information on the website, compromising the confidentiality and availability of the information stored there.

Below are some of the images associated with access to files containing sensitive client information and paths of the operating system that can be stolen:



finanprimas-development.finesa.com.co/media/1101057473%20SEGUROS%20DEL%20ESTADO%20(1)_page-0001(1).pdf

SEGUROS DEL ESTADO S.A.

CARÁTULA PÓLIZA DE SEGURO DE AUTOMÓVILES
TIPO DE PÓLIZA INDIVIDUAL

45 | 48 | 101025813

EMISION ORIGINAL | 0 | 11 | 11 | 2021 | 11 | 11 | 2021 | 24:00 | 11 | 11 | 2022 | 24:00 | 365

TOMADOR [redacted] CC [redacted]

ASEGURADO YINA MARCELA CORTES GIL DIRECCION [redacted] CC [redacted]

BENEFICIARIO [redacted] NIT [redacted]

CALI | CALI | NINGUNO

[redacted]

PRODUCTO: [illegible]

Risk Level: 10.0 (High)

Evidence: See videos: Finesa_MaliciousFileUploadBackend.mp4

Affected Systems:

https://finanprimas-development.finesa.com.co/
https://finanprimas-development.finesa.com.co/media/media.pht

HTTP POST https://finanprimas-development.finesa.com.co/financiar/adjuntar-poliza/{id}
Risk: Successful exploitation of this vulnerability allows:

- **Server-side attacks:** The web server was compromised by uploading and executing a web shell that allows command execution, system file exploration, local resource exploration, among others. Even more serious, it was possible to establish a reverse shell connection to the attackers' machine, allowing post-exploitation activities to be carried out much more comfortably, demonstrating poor perimeter controls in the AWS instances. An attacker can use these accesses to carry out privilege escalation on the local server, install additional tools and move laterally on the Backbone AWS servers to compromise additional assets.

Uploading of malware to the server not only to affect Finesa's server, but also to use Finesa's domain and distribute malware to its clients. For example, sharing the URL "https://finanprimas-development.finesa.com.co/media/beneficios.exe" with its clients.

Recommendation: Apply proper validation of the file extension that the user wants to upload to the site. Deny all extensions and implement the use of a "positive list" to indicate which file extensions are the only ones allowed in the upload functionality. Additionally, define a path on the server to upload sensitive files (policies and/or documents) that users upload, so that it cannot be accessed by anyone who goes to the resource "https://finanprimas-development.finesa.com.co/media/". Through the obtained accesses, it was possible to access all the information stored in the path:

/var/www/expression/clients/finanprimas_development_finesa_finesa_com_co/web/media

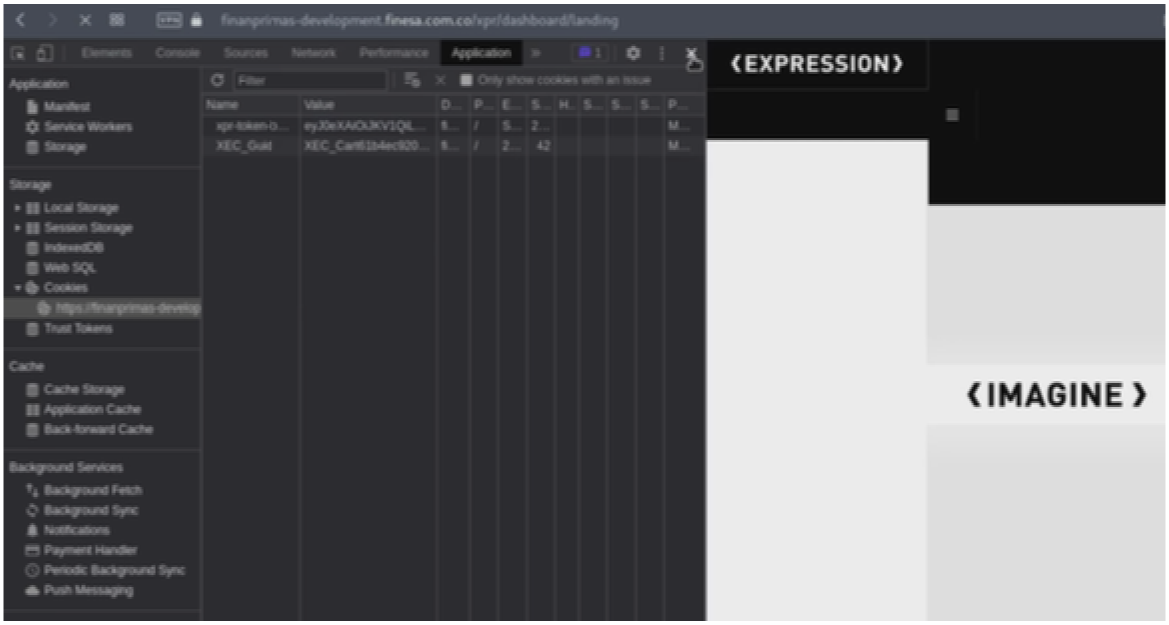
- in other web browsers without any authentication. It is recommended to save files on the web server named using Digest functions such as md5, not with the plain name with which they were stored in the server's upload folder.

Broken Access Control To the API

Description: Broken access control vulnerability occurs when a user can access a resource or perform an action that they are not supposed to access. This occurs in several endpoints of the API in which it is possible to gain access to restricted information without even having a valid session or minimal privileged user.

From the "Impersonate" functionality, it is possible to impersonate any user without the need to have "logged in" to the administration panel, meaning that anyone external can access without authorization by impersonating a user with a "Site Developer" profile.

It was also observed that from a low privilege account such as a user with a content editor role, it is possible to access the information of other users, and even create new users, thus allowing for privilege escalation in the administration panel.



Name	Value	D...	P...	E...	S...	H...	S...	S...	S...	P...
xpr-token-o...	eyJ0eXAiOiJKV1QiL...	fi...	/	S...	2...					M...
XEC_Guid	XEC_Cart61b4ec920...	fi...	/	2...	42					M...

Risk level: 10.0 (High)

Evidence:

Finesa_UnauthorizedImpersonation.mp4 Finesa_BrokenAccessControl.mp4

Affected Systems:

https://finanprimas-development.finesa.com.co/api/
https://finanprimas-development.finesa.com.co/api/auth/admin/impersonate
https://finanprimas-development.finesa.com.co/api/users/

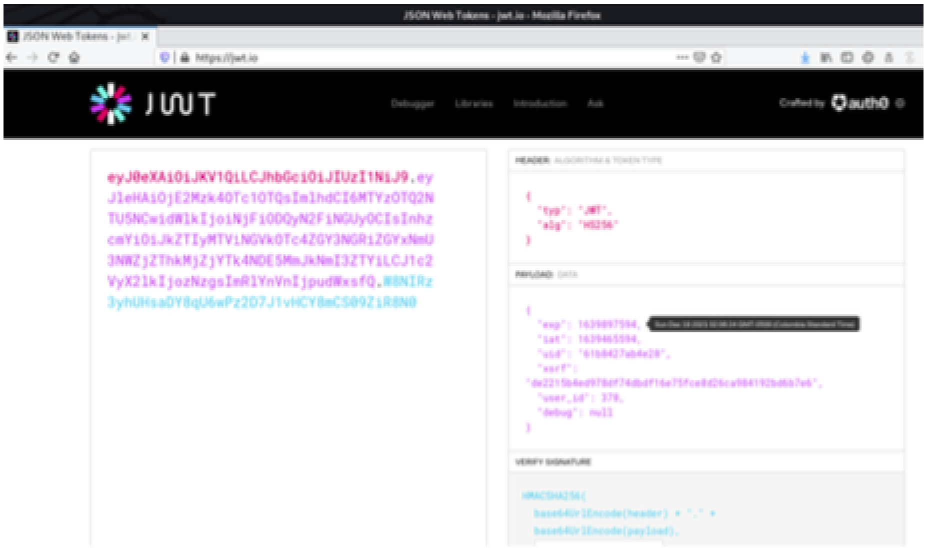
Risk: An unauthorized user could take control of the site, delete and/or modify content, and carry out unwanted actions without the consent of the organization and site administrators. Additionally, broken access control allows low-privileged users to access restricted information.

Recommendation: Apply code statements in the API to perform session validation that the user presents in the HTTP request. Before carrying out any action, it must be verified that the session is valid and that the user session does have the necessary permissions to access the resource requested. Access control is only effective when applied on the server side or serverless API, where the attacker cannot modify access control validation or metadata. Below are the main guidelines to consider when implementing effective access controls.

- Except for public resources, deny by default.
- Implement access control mechanisms once and reuse them throughout the application.
- Access controls should validate the ownership of records and user accesses before allowing the user to take actions such as create, read, update, or delete any record.
- Disable web server directory listing and ensure that file metadata (e.g., .git) and backup files are not present within root web directories.
- Limit access to the API and the controller to minimize damage from automated attack tools.
- Stateful session identifiers should be invalidated on the server after logging out. Stateless JWT tokens should be short-lived to minimize the window of opportunity for an attacker. For longer-lived JWTs, it is recommended to follow OAuth standards to revoke access.

Compromised Session Token

Description: The session token that is generated after user authentication has a fairly long expiration time (5 days) and additionally, when the user presses the sign out button, the session remains valid, that is, it does not expire.



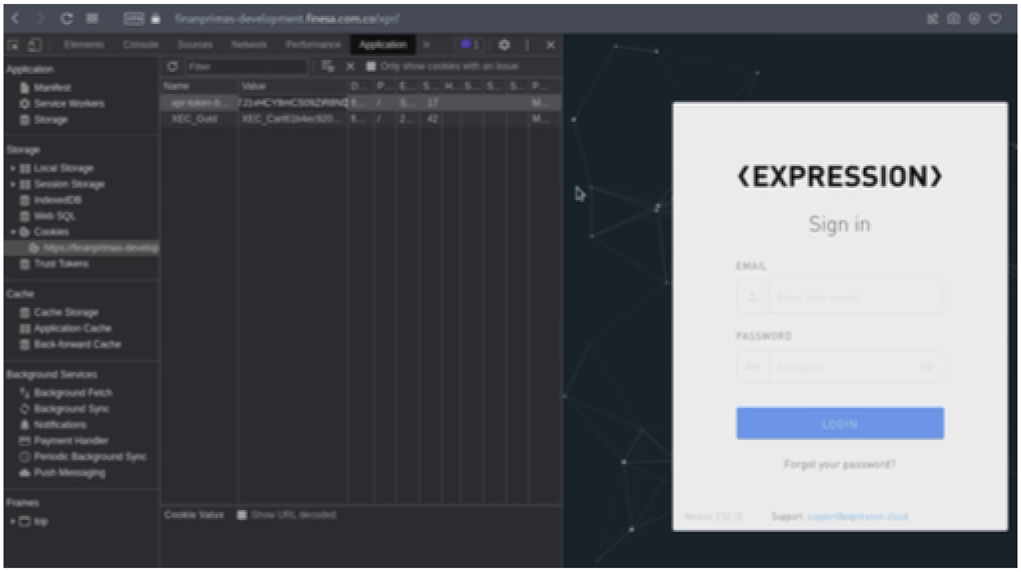
```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.ey
JleHAiOjE2Mzk4OTc1OTQsImlhdCI6MTYzOTQ2N
TU5NCwidWlkIjoiNjFiODQyN2FiNGUyOCIsInhz
cmYiOiJkZTIyMTViNGVkOTc4ZGY3NGRiZGYxNmU
3NWZjZThkMjZjYTk4NDE5MmJkNmI3ZTYiLCJ1c2
VyX2lkIjozNzgsImRlYnVnIjpudWxsfQ.W8NIRz
3yhUHsaDY8qU6wPz2D7J1vHCY8mCS09ZiR8N0
```

```
{
  "typ": "JWT",
  "alg": "HS256"
}
```

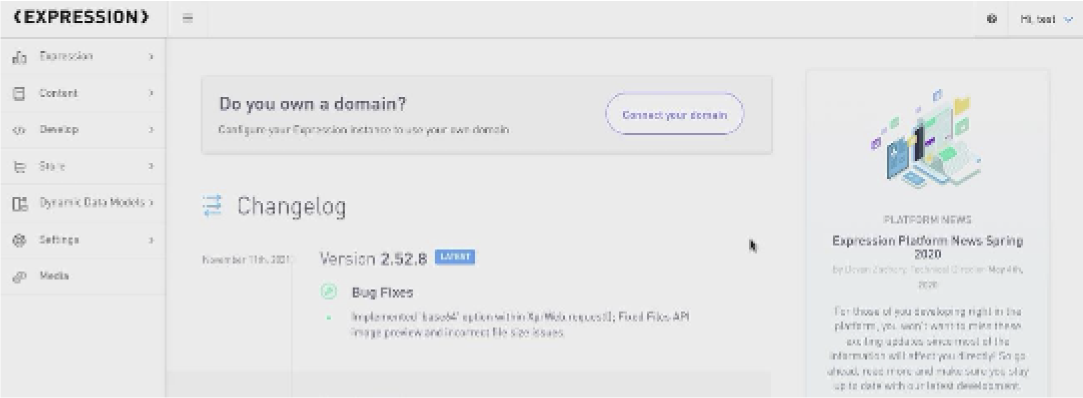
```
{
  "exp": 1639897594,
  "iat": 1639465594,
  "uid": "61b8427ab4e28",
  "xsrf":
"de2215b4ed978df74dbdf16e75fce8d26ca984192bd6b7e6",
  "user_id": 378,
  "debug": null
}
```

```
HMACSHA256(
  base64UrlEncode(header) + "." +
  base64UrlEncode(payload),
```

Figura 23. Exposición Token



Name	Value	D...	P...	E...	S...	H...	S...	S...	S...	P...
xpr-token-b...	7J1vHCY8mCS09ZiR8N0	fi...	/	S...	37					M...
XEC_Guid	XEC_Caf61b4ec920...	fi...	/	2...	42					M...



Do you own a domain?

Configure your Expression instance to use your own domain

Changelog

November 11th, 2021

Version 2.52.8

Bug Fixes

- Implemented 'base64' option within XpWeb.request(); Fixed Files API image preview and incorrect file size issues

PLATFORM NEWS

Expression Platform News Spring 2020

by Devon Zachary, Technical Director May 4th, 2020

For those of you developing right in the platform, you won't want to miss these exciting updates since most of the information will affect you directly! So go ahead, read more and make sure you stay up to date with our latest development.

Risk Level: 5.0 (Medium)

Evidence: Figure 24. Authentication token compromise Finesa_TiempoExpAltoTokenJWT.png Finesa_NoCierreDeSesion.mp4

Affected systems: Session management mechanism of https://finanprimas-development.finesa.com.co/api/

Risk: There is a risk of a hacker compromising a user's session token in the administration panel and being able to maintain access for at least 5 days due to poor practices in the generation and management of the JWT token.

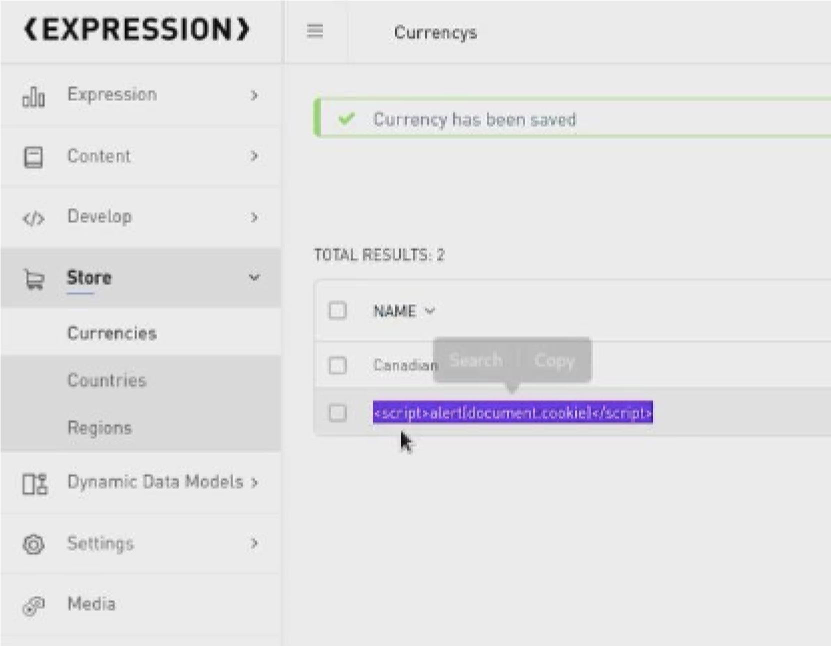
Recommendation: Define a much lower expiration time for the token once the session is created and properly build the sign out endpoint so that it can disable the token once the user presses the "Sign Out" button.

Stateful session identifiers should be invalidated on the server after the session is closed. Stateless JWT tokens should have a short duration to minimize the window of opportunity for an attacker. For longer-lasting JWT tokens, it is recommended to follow OAuth standards to revoke access.

Missing Validation in API Parameters

Description: Input data validation is performed to ensure that only correctly formatted data enters the workflow in a web application, preventing malformed data from reaching systems such as databases or API endpoints, which can cause malfunctioning of several downstream components. Input validation should occur as early as possible in the data flow, preferably as soon as the data is received from an external user. Data from all potentially untrusted sources should be subject to input validation, including not only web clients connected to the Internet, but also connections to the backend through extranets, providers, partners, vendors, or support teams, each of which can be compromised on its own and start sending incorrectly formatted data.

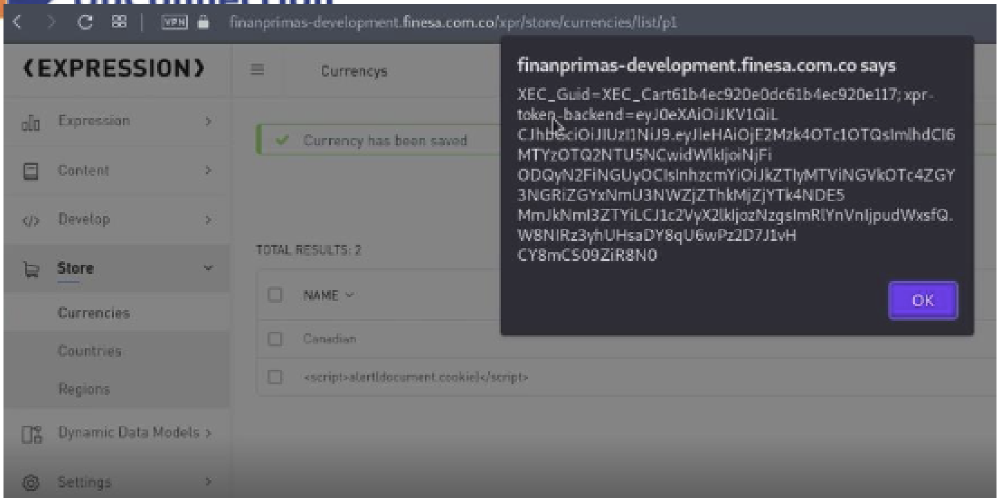
It was observed in multiple parameters that adequate validations are not being performed when receiving information in the API, for example: if a user ID number is required, the API receives any character that is sent and generates a token with that information. Likewise, in a Title field in the administration panel, it was possible to inject javascript code (XSS) due to the lack of user input validation.



Currency has been saved

TOTAL RESULTS: 2

NAME
Canadian
<script>alert(document.cookie)</script>



Currency has been saved

TOTAL RESULTS: 2

NAME
Canadian
<script>alert(document.cookie)</script>

```
finanprimas-development.finesa.com.co says
XEC_Guid=XEC_Cart61b4ec920e0dc61b4ec920e117; xpr-
token-backend=eyJ0eXAiOiJKV1QiL
CJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2Mzk4OTc1OTQsImlhdCI6
MTYzOTQ2NTU5NCwidWlkIjoiNjFi
ODQyN2FiNGUyOCIsInhzcmYiOiJkZTlyMTViNGVkOTc4ZGY
3NGRiZGYxNmU3NWZjZThkMjZjYTk4NDE5
MmJkNmI3ZTYiLCJ1c2VyX2lkIjozNzgsImRlYnVnIjpudWxsfQ.
W8NIRz3yhUHsaDY8qU6wPz2D7J1vH
CY8mCS09ZiR8N0
```

Level of Risk: 7.0 (High)

Evidence:

Figure 26. XSS Javascript Injection

Finesa_InputValidationXSS.mp4 Finesa_InputValidation_UnexpectedCharacters.mp4

Affected Systems: https://finanprimas-development.finesa.com.co/

Risk: The lack of user input validation in each of the parameters can generate different types of injections depending on the destination established for the information sent by the user. These injections seek to steal, manipulate, delete or even affect systems through command statements.

Recommendation: It is recommended to implement an adequate input validation and/or sanitization for each parameter that receives information in the API. For example, if a telephone number is requested, the API must validate that the input consists only of numerical data and has a specific length. Input validation must be applied at both the syntactic and semantic levels. Syntactic validation must enforce the correct syntax of structured fields (e.g., SSN, date, currency symbol, among others). Semantic validation must impose the accuracy of its values in the specific business context (e.g., the start date is before the end date, the price is within the expected range). It is always recommended to prevent attacks as early as possible in the user's request processing (attacker). Input validation can be used to detect unauthorized inputs before they are processed by the application.

Weak Password Policy

Description: At the moment when setting the password for a new user in the administration panel, it is evident that it is possible to define weak passwords such as "testtest". The use of weak passwords and the lack of anti-robot controls in the login portal to access the Expression backend increase the likelihood of compromise of administrative credentials over the web application control panel.

Risk Level: 7.0 (High)

Evidence: Finesa_Politica_Contrasenas.mp4

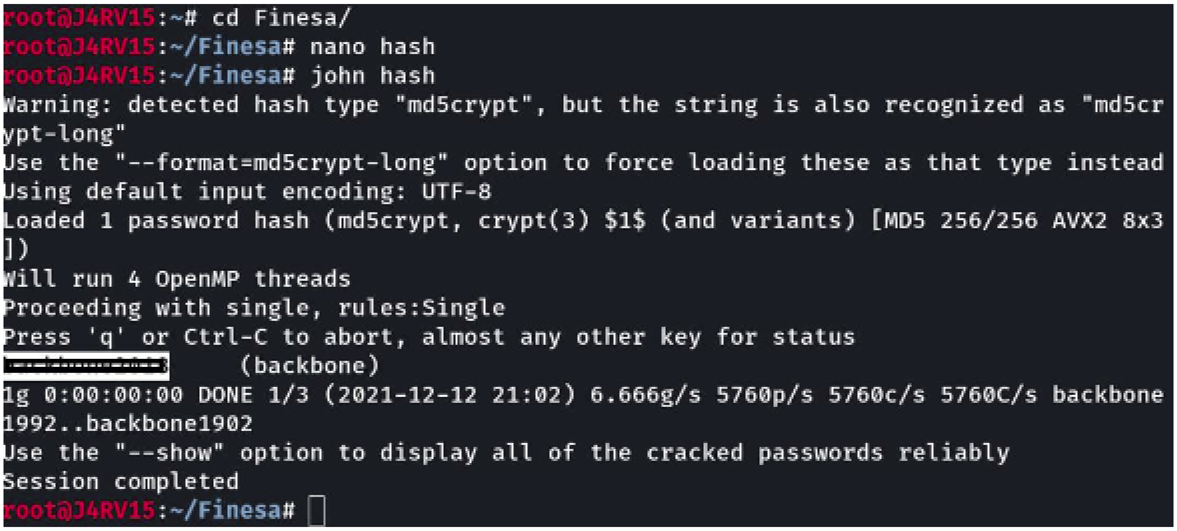
Affected Systems: https://finanprimas-development.finesa.com.co/xpr/

Risk: This vulnerability facilitates unauthorized users to identify passwords of other users, and in combination with vulnerabilities that allow brute force attacks, the risk of compromising passwords in an unauthorized manner increases. Due to the combination of these poor password policies with other vulnerabilities identified on the website, which allow privilege escalation and identity spoofing, the impact of this finding becomes greater as it can compromise the integrity, availability, and confidentiality of Expression's clients in its entirety.
Recommendation: If possible, mandatory multifactor authentication should be established and additionally, a more robust password policy should be defined, including:

- At least 12 characters.
- The use of uppercase letters, lowercase letters, numbers, and special characters.
- The username associated with the password should not be used as the password or included in it.
- Avoid the use of basic keyboard sequences (e.g., "qwerty", "asdf", or typical numbering sequences such as "1234" or "98765").
- Avoid the use of common words related to the organization and/or social context (e.g., "finesa", "backbone", "shakira", "colombia", among others).

Non-restriction server traffic

Description: The operating system supporting the web service of the analyzed site presents unrestricted internet browsing. This outgoing traffic can sometimes be generated by malicious files that are loaded onto the server, and to minimize the impact of these malicious activities, Firewall rules for outgoing traffic are necessary.



```
root@J4RV15:~# cd Finesa/
root@J4RV15:~/Finesa# nano hash
root@J4RV15:~/Finesa# john hash
Warning: detected hash type "md5crypt", but the string is also recognized as "md5cr
ypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8x3
])
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
[redacted]     (backbone)
1g 0:00:00:00 DONE 1/3 (2021-12-12 21:02) 6.666g/s 5760p/s 5760c/s 5760C/s backbone
1992..backbone1902
Use the "--show" option to display all of the cracked passwords reliably
Session completed
root@J4RV15:~/Finesa# 
```

Risk Level: 5.0 (Medium)

Evidence: See Exfiltration folder

Affected Systems: https://finanprimas-development.finesa.com.co/

Risk: The lack of restrictions on outgoing traffic to the internet allowed the execution of a reverse shell on non-conventional ports (above port 10000), which enables a hacker to have more comfort in unauthorized server access.

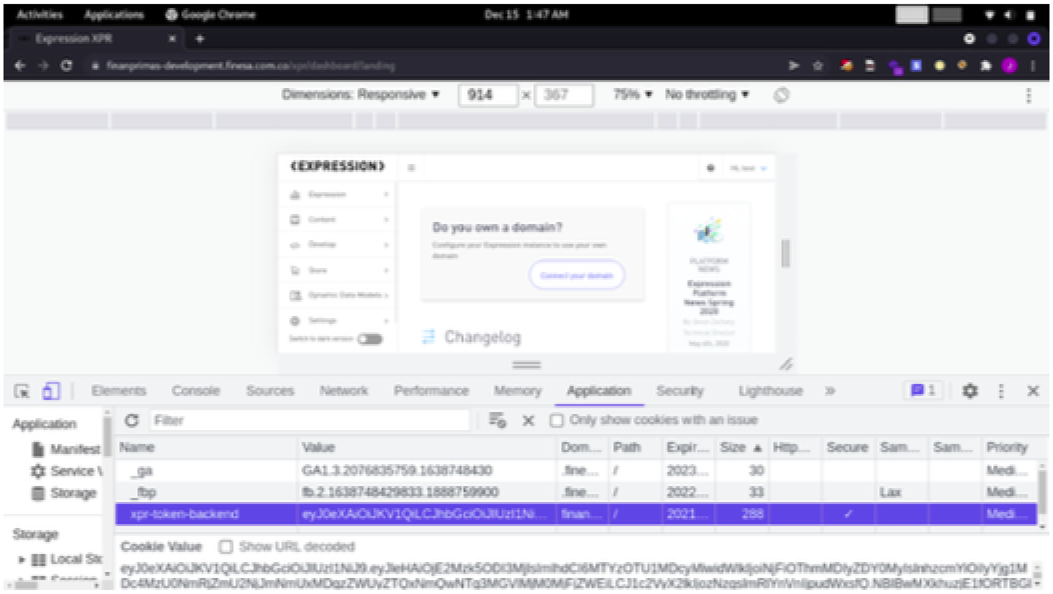
Recommendation: Implement firewall rules for outgoing traffic to the internet, so that only necessary connections for the proper functioning of the server are allowed, i.e., only to required resources and ports.

Cookie Flags not present

Description: The use of security flags in cookies helps prevent their theft to avoid user impersonation. The absence of these flags makes cookie theft easier through attacks such as Cross Site Scripting (XSS).

Risk Level: 4.0 (Medium)

Evidence: Ausencia_Cookie_flags.png



Name	Value	Dom...	Path	Expir...	Size ▲	Http...	Secure	Sam...	Sam...	Priority
_ga	GA1.3.2076835759.1638748430	.fine...	/	2023...	30					Medi...
_fbp	fb.2.1638748429833.1888759900	.fine...	/	2022...	33			Lax		Medi...
xpr-token-backend	eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1Ni...	finan...	/	2021...	288		✓			Medi...

Cookie Value ☐ Show URL decoded

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJleHAiOjE2Mzk5ODI3MjIsImlhdCI6MTYzOTU1MDcyMiwidWlkIjoiNjFiOThmMDIyZDY0MyIsInhzcmYiOiIyYjg1M
Dc4MzU0NmRjZmU2NjJmNmUxMDgzZWUyZTQxNmQwNTg3MGVlMjM0MjFiZWEiLCJ1c2VyX2lkIjoiNzgsImRlYnVnIjpudWxsfQ.NBlBwMXkhuzjE1fORTBGI
```

Systems affected: https://finanprimas-development.finesa.com.co/xpr

Risk: Facilitates the compromise of cookies by an unauthorized actor.

Recommendation: Since the "Secure" attribute is already enabled, configure the security attributes "HttpOnly" and "SameSite" for the session cookie.

Conclusion and Recommendations

• Based on the security analysis conducted, we can conclude that the current security level of the analyzed Finesa web application (https://finanprimasdevelopment.finesa.com.co) is low, since it has several critical vulnerabilities that can allow a remote attacker, not authenticated on the platform, to upload malicious files that can lead to command execution and even a reverse shell that can be used for malicious purposes.

• During the tests carried out, the confidentiality, integrity, and availability of both the Frontend and Backend were compromised. Since the Backend is the same for all applications under the Expression infrastructure, all websites would be affected, as identified during the initial analysis of the demo portal: https://vacantvioletwolf.xpr.cloud.

• The necessary controls must be applied immediately to limit the upload of unauthorized (malicious) files to both the Front and Back of the web application. The Back finding affects all sites built with Expression.

• It is recommended to implement anti-robot controls (reCaptcha technology) on the login page of the Expression Back. Additionally, it is essential to implement user lockout controls after a reasonable number of failed login attempts, as well as a rigorous password policy in order to increase the security level of the web applications.

• The effective implementation of the Web Application Firewall Security control can allow closing several vulnerabilities identified in the tests immediately. Therefore, it is highly important to follow the recommendations indicated in order to allow only connections to the web application from CloudFlare and prevent WAF control evasion.

• It is recommended to implement adequate input validation and/or sanitization for each parameter that receives information in the API. For example, if a phone number is requested, the API must validate that the input is only numerical data and has a specific length.

• Input validation should be applied both at a syntactic and semantic level. Syntactic validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol, among others).

• Semantic validation should enforce accuracy of their values in the specific business context (e.g. start date is before end date, price is within expected range). It is always recommended to prevent attacks as early as possible in the processing of the user (attacker) request. Input validation can be used to detect unauthorized inputs before they are processed by the application.

• Recommendations for the following tests to be performed:

o For the next portal, we request to obtain test data if there is a quoting or payment flow and thus perform the complete flow simulation. This would test simulation of the entire payment flow, regardless of whether it is related to another page endpoint. It would be reviewed to see what can be achieved from the analysis page and how far it can go to generate impersonation or fraud that may affect the end customer and users visiting the page.

o For the next analysis, we recommend conducting the tests before publishing the portal and allowing access through a Security Group from AWS where only the public IP address from where the tests are being performed can access the portal. This will help avoid publishing the portal and having it completely open to the internet where it may have vulnerabilities and exposures that can be corrected before becoming completely public.