I.E.S Zaidin Vergeles I Bug Bounty Report

CONFIDENTIAL

Date: Jan 9th, 2022
Project: I Bug Bounty
Version: 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Efren Garcia and IES Zaidin Vergeles (IZV). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Efren and IZV.

Efren may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. I prioritized the assessment to identify the weakest security controls an attacker would exploit. I recommend conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

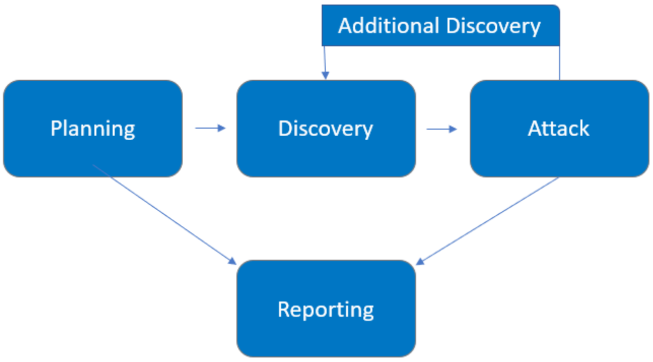
Name	Title	Contact Information
Auditor		
Efren Garcia	Penetration Tester	Email: efrenzaidinvergeles@gmail.com
IES Zaidin Vergeles		
Jose Luis Navarro	Deputy Headmaster	Office: 958 893 850

Assessment Overview

From May 21th, 2019 to June 13th, 2020, I participated in I BUG BOUNTY IES ZAIDIN VERGELES to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test

Phases of penetration testing activities include the following;

- **Planning** – Customer goals are gathered and rules of engagement obtained.
- **Discovery** – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- **Attack** – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- **Reporting** – Document all found vulnerabilities, failed attempts, and company strengths and weaknesses.



Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A penetration tester attempts to gather sensitive information through open-source intelligence (OSINT), including students information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The penetration tester also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

Finding Severity Ratings

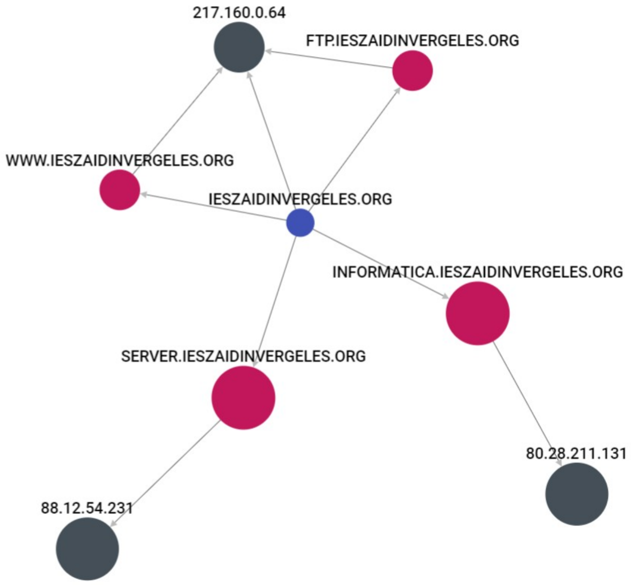
The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization’s attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
External Penetration Test	Any system owned by IZV through internet

During the assessment, the main targets were the following as shown in the image


217.160.0.64
FTP.IESZAIDINVERGELES.ORG
WWW.IESZAIDINVERGELES.ORG
IESZAIDINVERGELES.ORG
INFORMATICA.IESZAIDINVERGELES.ORG
SERVER.IESZAIDINVERGELES.ORG
80.28.211.131
88.12.54.231

Scope Exclusions

- Phishing and credential theft are not allowed in any case
- Bruteforce attacks are limited to low usage periods of time to avoid DOS

Post Assessment Clean-up

Any test accounts which were created for the purpose of this assessment should be disabled or removed, as appropriate, together with any associated content.

Executive Summary

Efren evaluated IZV’s external security posture through an external network penetration test from May 21th, 2019 to June 13th, 2020. By leveraging a series of attacks, Efren found critical level vulnerabilities that allowed full internal access to the IZV’s teachers accounts, impersonation of them and access to sensitive data regarding students and teachers. It is highly recommended that IZV addresses these vulnerabilities as soon as possible to avoid unauthorized access.

Findings Overview

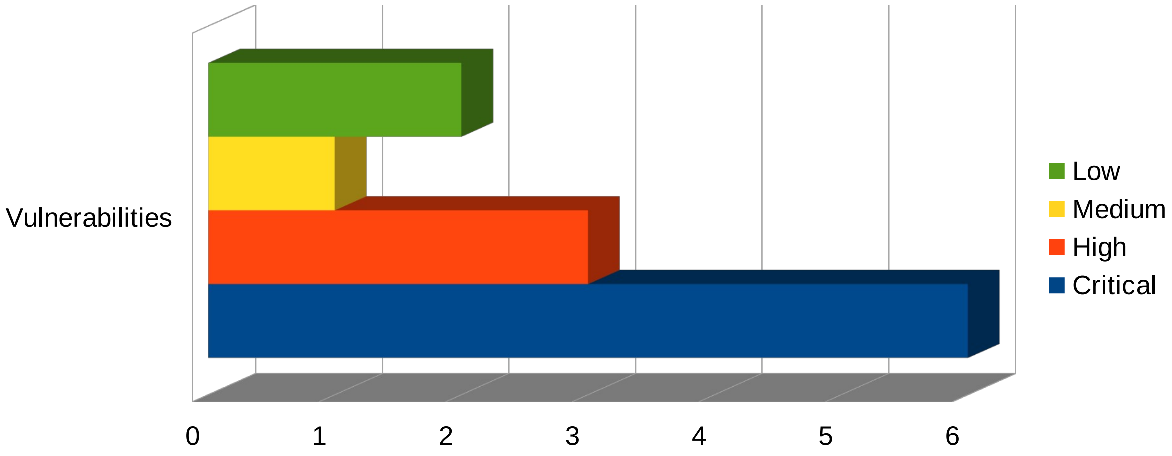
Ref	Description	Mitigation	Risk
1	Full access to teachers Moodle accounts through profile stored XSS	Update Moodle version Set up automatic minor updates	Critical
2	Access to webserver logs & stats through unauthorized AWStats cgi Full webserver path disclosure	Implement authorization	Critical
3	JoobSkee full students IDs guessing	Limit the number of requests to avoid bruteforce attacks Add another required form field to make bruteforcing unviable	Critical
4	Access to confidential documents through open scanner &	Implement authorization & non shared queues	Critical

	printer queue		
5	Multiple Proxmox LXCs root access using default Cloud9 credentials	Avoid using the same default password for every container and posting it in a public directory. Generate secure random default passwords and send them through a secure channel. Enforce the user to set a new one after the first login	Critical
6	Wordpress admin password guessing through XMLRPC bruteforce amplification	Disable XMLRPC	Critical
7	MantisBT unauthorized account creation & access to incidents logs	Restrict account creation to authorized organizational email addresses	High
8	Confidential information through Margavila & PAE files	Implement authorization or remove the file from the webserver	High
9	SlowLoris DOS of multiple hosts	Use NginX	High
10	Usage of webserver as a zombie host in a botnet through XMLRPC	Disable XMLRPC	Moderate
11	Full list of teachers emails and full names through getProfesores open API endpoint	Remove the endpoint in case it's not needed Otherwise, implement authorization	Low
12	Absolute webserver path through FPDF library error	Fix the controller, disable error logs	Low

13	TimThumb version info	The library version is not vulnerable to the popular CVE-2014-4663 Removing version discovery is advised	Informational
14	SQL Server version info	Remove the file from the webserver	Informational

Vulnerabilities By Impact

The following graph shows the number of vulnerabilities found regarding their risk (Note that this summary table does not include the informational items)



Security Strengths

Difficult Staff Impersonation

When trying to impersonate a teacher in the bug tracking service, one of the teachers noticed and found out it was me after checking the user mail address.

Security Weaknesses

Missing Authorization

Most services are missing proper authorization requirements, which allows any user to retrieve potentially sensitive or logging information, skipping the whole discovery process.

Unrestricted Login Attempts

Most forms submissions allow an unlimited number of retries and don’t implement any kind of security like a captcha. Implementing proper security measures and notifying of unsuccessful login attempts would result in secure formularies

Technical Details

Moodle Profile Stored XSS (CVE-2021-20279)

Moodle is vulnerable to stored XSS through multiple fields in users profile formulary.

Vulnerability Details

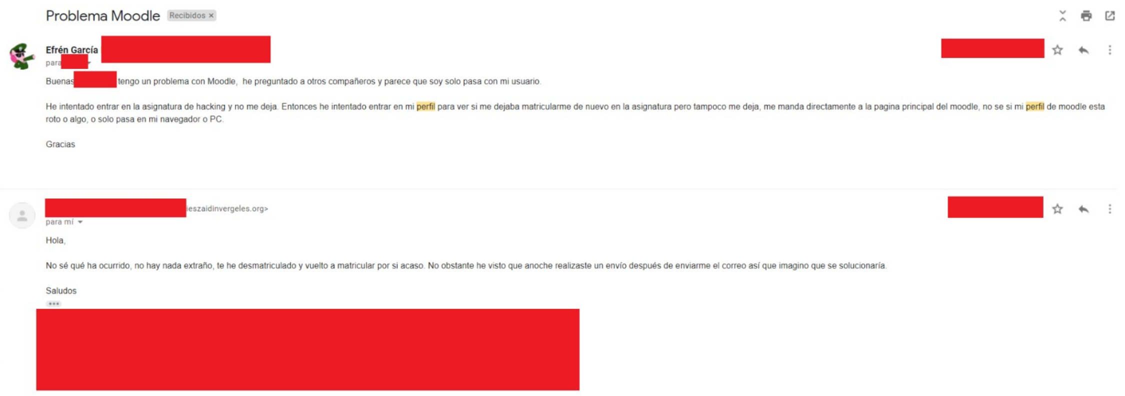
Affects	https://server.ieszaidinvergeles.org/moodle3
Attack Vectors	XSS
References	https://www.cvedetails.com/cve/CVE-2020-25627

I discovered that Moodle was vulnerable to stored XSS through users profile fields. A malicious user can inject arbitrary Javascript code by updating their user profile info. Moodle version was found in the file “upgrade.txt”

To test it I set up a simple cookie farm;

I injected Javascript code that obtains the visiting user cookie, redirects to a server I set up and finally stores the cookie in a file

After setting up the cookie farm I just had to do a simple social engineering attempt to gain access to any account I wanted. In this case I chose the Hacking subject teacher as evidence.



Problema Moodle

Efrén García [redacted] [redacted]
para [redacted]

Buenas [redacted] tengo un problema con Moodle, he preguntado a otros compañeros y parece que soy solo pasa con mi usuario.

He intentado entrar en la asignatura de hacking y no me deja. Entonces he intentado entrar en mi perfil para ver si me dejaba matricularme de nuevo en la asignatura pero tampoco me deja, me manda directamente a la pagina principal del moodle, no se si mi perfil de moodle esta roto o algo, o solo pasa en mi navegador o PC.

Gracias

[redacted] ieszaidinvergeles.org> [redacted]
para mí

Hola,

No sé qué ha ocurrido, no hay nada extraño, te he desmatriculado y vuelto a matricular por si acaso. No obstante he visto que anoche realizaste un envío después de enviarme el correo así que imagino que se solucionaría.

Saludos

[redacted]

After the teacher visited my profile, I was able to log into his account using the cookie

Remediation Guidance

Update Moodle to latest version and schedule automatic minor updates.

AWStats Logs & Absolute Path (CVE-2018-10245)

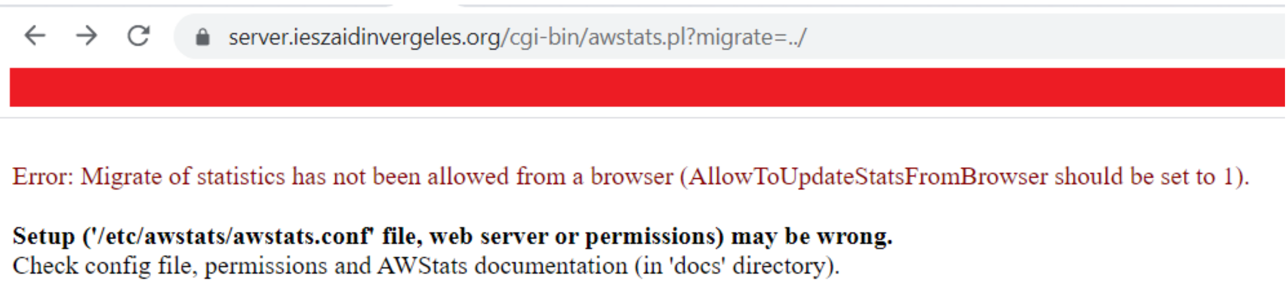
AWStats is accessible without any authentication and absolute webserver path can be discovered

Vulnerability Details

Affects	https://server.ieszaidinvergeles.org/cgi-bin/awstats.pl https://server.ieszaidinvergeles.org/cgi-bin/awstats.pl?migrate=passwd
Attack Vectors	HTTP Request
References	https://www.cvedetails.com/cve/CVE-2018-10245

AWStats is a cgi-bin service which shows multiple server stats, such as access logs, most visited pages, IPs and more. It has a search feature but lacks any kind of bulk export, so I decided to develop a Python program to retrieve all data to later process and search it in bulk.

This allowed me to have all the webserver routes without having to use fuzzing, as well as identifying staff IPs.



server.ieszaidinvergeles.org/cgi-bin/awstats.pl?migrate=../

Error: Migrate of statistics has not been allowed from a browser (AllowToUpdateStatsFromBrowser should be set to 1).

Setup ('/etc/awstats/awstats.conf' file, web server or permissions) may be wrong.
Check config file, permissions and AWStats documentation (in 'docs' directory).

Remediation Guidance

Update AWStats to latest version and implement authorization.

JoobSkee Students IDs Guessing

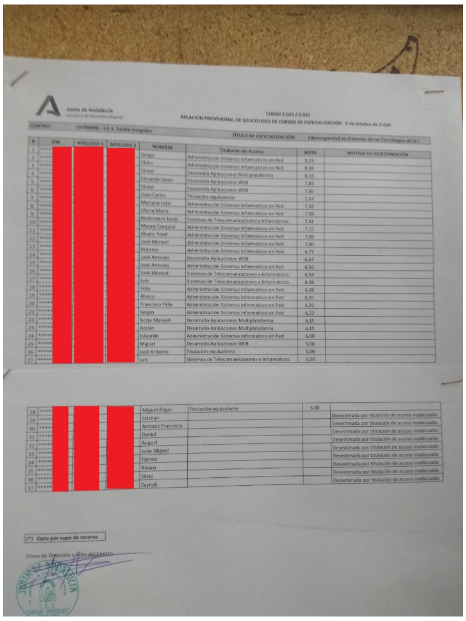
Complete students Ids can be bruteforced through the ID field in JobSkees job bank formulary.

Vulnerability Details

Affects	https://server.ieszaidinvergeles.org/bolsaempleo https://server.ieszaidinvergeles.org/jobskee/jobskee.sql
Attack Vectors	Bruteforce
References	https://capec.mitre.org/data/definitions/112.html

I discovered that JobSkees job bank was vulnerable to bruteforce through the ID fields. A malicious user can bruteforce the ID field to get subscribed as another student, supplant their identity and obtain their complete personal ID.

Since guessing a complete ID would take too much time, I used the join requests paper posted by IZV in a pinboard, which included full names and partial IDs containing the last 3 numbers and letter.



Junta de Andalucía
Consejería de Educación y Deporte

CURSO 2.020 / 2.021
RELACIÓN PROVISIONAL DE SOLICITUDES DE CURSOS DE ESPECIALIZACIÓN - 5 de octubre de 2.020.

CENTRO: 18700098 - I.E.S. Zaidín-Vergeles

TÍTULO DE ESPECIALIZACIÓN: Ciberseguridad en Entornos de las Tecnologías de la I

#	DNI	APELLIDO 1	APELLIDO 2	NOMBRE	Titulación de Acceso	NOTA	MOTIVO DE DESESTIMACIÓN
1	***** [redacted]	[redacted]	[redacted]	Sergio	Administración Sistemas Informaticos en Red	9,23	
2	***** [redacted]	[redacted]	[redacted]	Efrén	Administración Sistemas Informaticos en Red	8,38	
3	***** [redacted]	[redacted]	[redacted]	Victor	Desarrollo Aplicaciones Multiplataforma	8,18	
4	***** [redacted]	[redacted]	[redacted]	Eduardo Javier	Desarrollo Aplicaciones WEB	7,83	
5	***** [redacted]	[redacted]	[redacted]	Victor	Desarrollo Aplicaciones WEB	7,60	
6	***** [redacted]	[redacted]	[redacted]	Juan Carlos	Titulación equivalente	7,57	
7	***** [redacted]	[redacted]	[redacted]	Mariano Iván	Administración Sistemas Informaticos en Red	7,54	
8	***** [redacted]	[redacted]	[redacted]	Gloria María	Administración Sistemas Informaticos en Red	7,38	
9	***** [redacted]	[redacted]	[redacted]	Baldomero Jesús	Sistemas de Telecomunicaciones e Informáticos	7,31	
10	***** [redacted]	[redacted]	[redacted]	Mauro Ezequiel	Administración Sistemas Informaticos en Red	7,15	
11	***** [redacted]	[redacted]	[redacted]	Álvaro Yerel	Administración Sistemas Informaticos en Red	7,09	
12	***** [redacted]	[redacted]	[redacted]	José Manuel	Administración Sistemas Informaticos en Red	7,00	
13	***** [redacted]	[redacted]	[redacted]	Antonio	Administración Sistemas Informaticos en Red	6,77	
14	***** [redacted]	[redacted]	[redacted]	José Antonio	Desarrollo Aplicaciones WEB	6,67	
15	***** [redacted]	[redacted]	[redacted]	José Antonio	Administración Sistemas Informaticos en Red	6,56	
16	***** [redacted]	[redacted]	[redacted]	José Manuel	Sistemas de Telecomunicaciones e Informáticos	6,54	
17	***** [redacted]	[redacted]	[redacted]	Luis	Sistemas de Telecomunicaciones e Informáticos	6,38	
18	***** [redacted]	[redacted]	[redacted]	Félix	Administración Sistemas Informaticos en Red	6,38	
19	***** [redacted]	[redacted]	[redacted]	Álvaro	Administración Sistemas Informaticos en Red	6,31	
20	***** [redacted]	[redacted]	[redacted]	Francisco Félix	Administración Sistemas Informaticos en Red	6,31	
21	***** [redacted]	[redacted]	[redacted]	Sergio	Administración Sistemas Informaticos en Red	6,23	
22	***** [redacted]	[redacted]	[redacted]	Borja Manuel	Desarrollo Aplicaciones Multiplataforma	6,15	
23	***** [redacted]	[redacted]	[redacted]	Adrián	Desarrollo Aplicaciones Multiplataforma	6,15	
24	***** [redacted]	[redacted]	[redacted]	Eduardo	Administración Sistemas Informaticos en Red	6,00	
25	***** [redacted]	[redacted]	[redacted]	Miguel	Desarrollo Aplicaciones WEB	5,58	
26	***** [redacted]	[redacted]	[redacted]	José Antonio	Titulación equivalente	5,00	
27	***** [redacted]	[redacted]	[redacted]	Luis	Sistemas de Telecomunicaciones e Informáticos	5,00	
28	***** [redacted]	[redacted]	[redacted]	Miguel Ángel	Titulación equivalente	5,00	
29	***** [redacted]	[redacted]	[redacted]	Cristian			Desestimada por titulación de acceso inadecuada.
30	***** [redacted]	[redacted]	[redacted]	Antonio Francisco			Desestimada por titulación de acceso inadecuada.
31	***** [redacted]	[redacted]	[redacted]	Daniel			Desestimada por titulación de acceso inadecuada.
32	***** [redacted]	[redacted]	[redacted]	August			Desestimada por titulación de acceso inadecuada.
33	***** [redacted]	[redacted]	[redacted]	Juan Miguel			Desestimada por titulación de acceso inadecuada.
34	***** [redacted]	[redacted]	[redacted]	Fátima			Desestimada por titulación de acceso inadecuada.
35	***** [redacted]	[redacted]	[redacted]	Álvaro			Desestimada por titulación de acceso inadecuada.
36	***** [redacted]	[redacted]	[redacted]	Silvia			Desestimada por titulación de acceso inadecuada.
37	***** [redacted]	[redacted]	[redacted]	Zaynab			Desestimada por titulación de acceso inadecuada.

(*) Opta por cupo de reserva

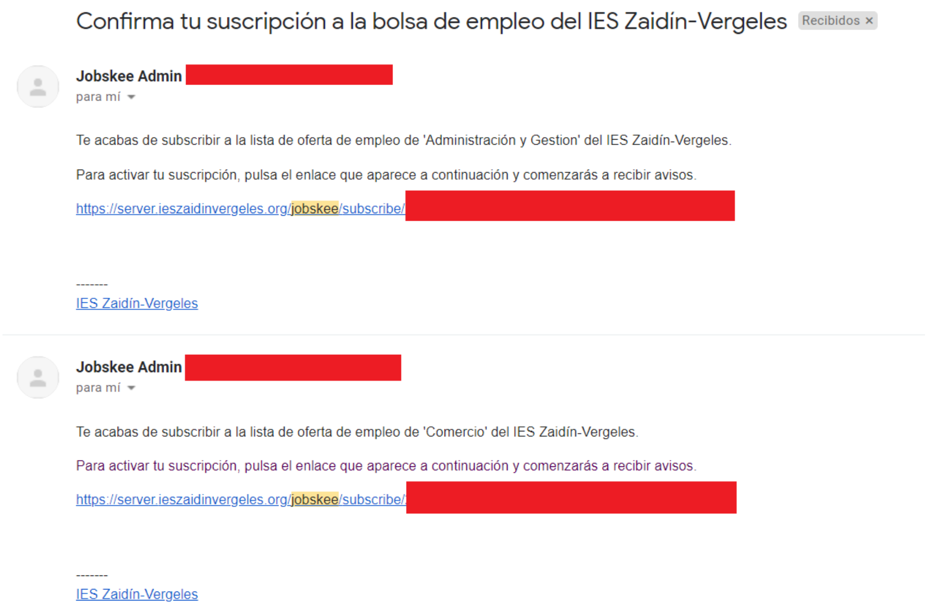
Firma de Dirección y sello del Centro:

JUNTA DE ANDALUCIA
I.E.S. "ZAIDIN VERGELES"

That means I only had to bruteforce the first 5 numbers, using the charset [0-9], which is a total of 10^5 permutations (100k requests) to find all the students IDs.

Due to the birthday attack, I also found IDs from students in different study plans to the one posted in the pinboard.

Here’s some evidence of the subscription to other IZV study plans by supplanting students guessing their ID;



Confirma tu suscripción a la bolsa de empleo del IES Zaidín-Vergeles

Jobskee Admin [redacted]
para mí

Te acabas de subscribir a la lista de oferta de empleo de 'Administración y Gestion' del IES Zaidín-Vergeles.

Para activar tu suscripción, pulsa el enlace que aparece a continuación y comenzarás a recibir avisos.

https://server.ieszaidinvergeles.org/jobskee/subscribe/[redacted]

IES Zaidín-Vergeles

Jobskee Admin [redacted]
para mí

Te acabas de subscribir a la lista de oferta de empleo de 'Comercio' del IES Zaidín-Vergeles.

Para activar tu suscripción, pulsa el enlace que aparece a continuación y comenzarás a recibir avisos.

https://server.ieszaidinvergeles.org/jobskee/subscribe/[redacted]

IES Zaidín-Vergeles

Also, the default JobSkee database was public, but it was useless since the default admin password was changed as it should.

Remediation Guidance

Add authentication and security to the form such a Captcha to avoid bruteforcing.

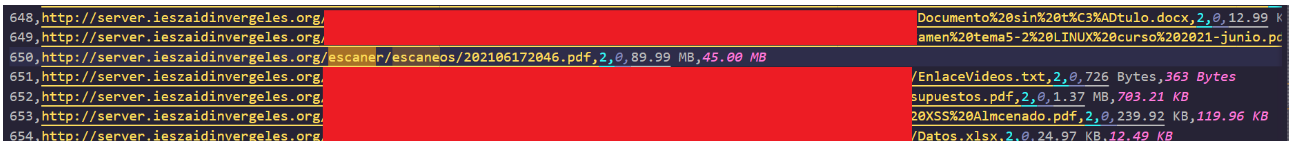
Printer & Scanner Access

IZVs printer and scanner queue can be accessed by unauthorized users to fetch confidential documents.

Vulnerability Details

Affects	https://server.ieszaidinvergeles.org/impresion/borrafich.php https://server.ieszaidinvergeles.org/impresion/ini.php https://server.ieszaidinvergeles.org/impresion/upload.php https://server.ieszaidinvergeles.org/impresion/quedan.php http://server.ieszaidinvergeles.org/impresion/cierre.php
Attack Vectors	HTTP Request
References	https://capec.mitre.org/data/definitions/149.html https://capec.mitre.org/data/definitions/155.html

After pulling access logs from AWStats and analyzing them, multiple paths with names related to a printing functionality were found. Inferring the different printer and scanner paths contents by checking the access logs, multiple scanned files were found and accessed freely.



```
648,http://server.ieszaidinvergeles.org/[redacted]Documento%20sin%20t%C3%ADtulo.docx,2,0,12.99 K
649,http://server.ieszaidinvergeles.org/[redacted]amen%20tema5-2%20LINUX%20curso%202021-junio.pd
650,http://server.ieszaidinvergeles.org/escaner/escaneos/202106172046.pdf,2,0,89.99 MB,45.00 MB
651,http://server.ieszaidinvergeles.org/[redacted]/EnlaceVideos.txt,2,0,726 Bytes,363 Bytes
652,http://server.ieszaidinvergeles.org/[redacted]supuestos.pdf,2,0,1.37 MB,703.21 KB
653,http://server.ieszaidinvergeles.org/[redacted]20XSS%20Almcenado.pdf,2,0,239.92 KB,119.96 KB
654,http://server.ieszaidinvergeles.org/[redacted]/Datos.xlsx,2,0,24.97 KB,12.49 KB
```

All the scanned files follow the format YearMonthDayHourMinute, also expressed as date "+%Y%m%d%H%M".

A malicious user can retrieve files in realtime by simply writing a script that fetches the path with an HTTP request, containing the actual time in the mentioned format, in an endless loop.

Remediation Guidance

Implement authorization in the printer & scanner endpoints to ensure confidentiality and privacy

Proxmox LXCs Root Access

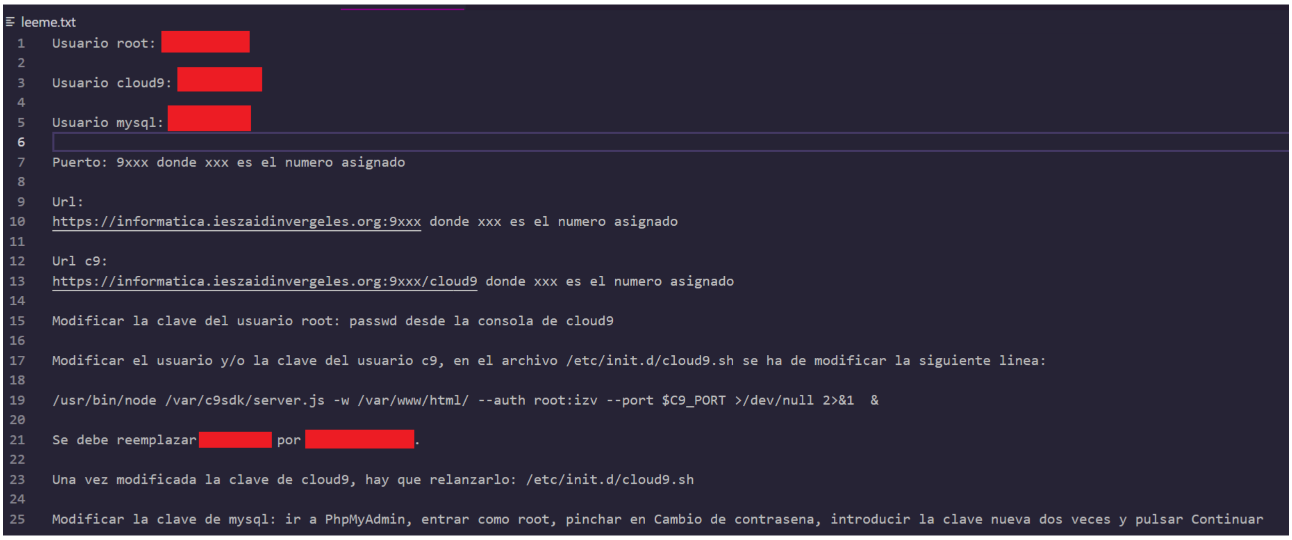
Multiple IZVs Proxmox node LXC containers can be accessed through Cloud9 with default credentials provided by the staff in README files.

Vulnerability Details

Affects	https://informatica.ieszaidinvergeles.org:9xxx https://web.archive.org/web/20210314231124/https://informatica.ieszaidinvergeles.org:9201/index.html
Attack Vectors	Credential Stuffing, Dictionary Attack, POST Request
References	https://capec.mitre.org/data/definitions/600.html https://capec.mitre.org/data/definitions/555.html https://capec.mitre.org/data/definitions/16.html https://cwe.mitre.org/data/definitions/256.html

Using domain discovery and port scanning, multiple LXC hosts were accessible through different ports using the HTTP protocol.

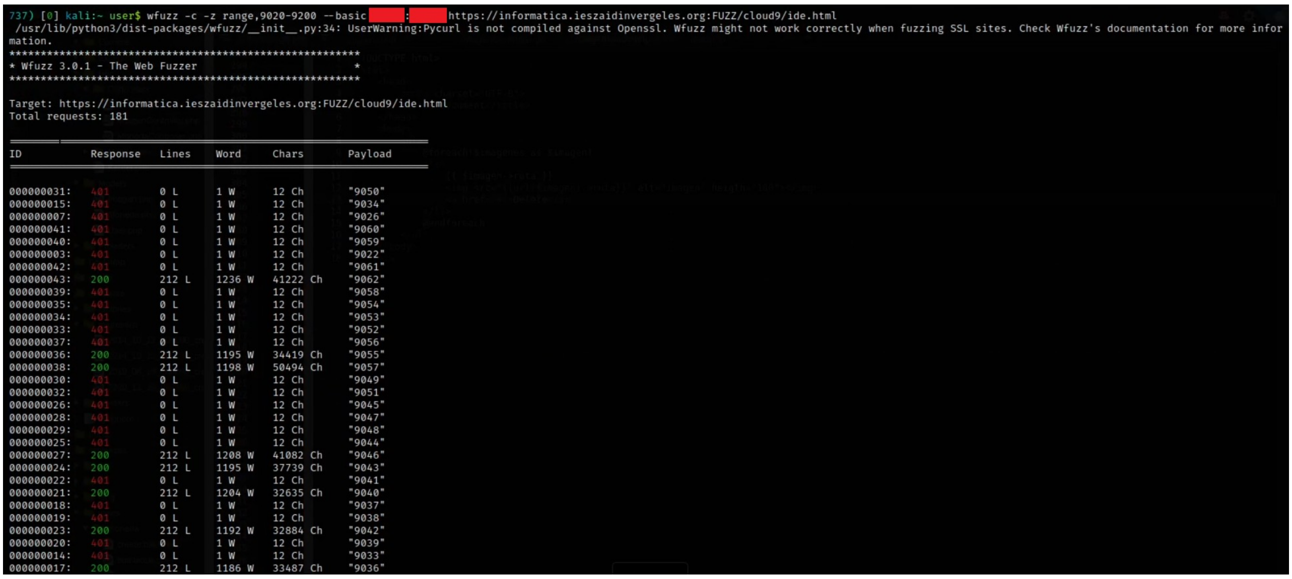
Each of the hosts shared some common files, being the most important the README. This file contained a guide for the users on how to access their LXC container IDE and terminal, and also the assignment of each LXC based on a port pattern.



leeme.txt

```
Usuario root: [redacted]

Usuario cloud9: [redacted]

Usuario mysql: [redacted]

Puerto: 9xxx donde xxx es el numero asignado

Url:
https://informatica.ieszaidinvergeles.org:9xxx donde xxx es el numero asignado

Url c9:
https://informatica.ieszaidinvergeles.org:9xxx/cloud9 donde xxx es el numero asignado

Modificar la clave del usuario root: passwd desde la consola de cloud9

Modificar el usuario y/o la clave del usuario c9, en el archivo /etc/init.d/cloud9.sh se ha de modificar la siguiente linea:

/usr/bin/node /var/c9sdk/server.js -w /var/www/html/ --auth root:izv --port $C9_PORT >/dev/null 2>&1  &

Se debe reemplazar [redacted] por [redacted].

Una vez modificada la clave de cloud9, hay que relanzarlo: /etc/init.d/cloud9.sh

Modificar la clave de mysql: ir a PhpMyAdmin, entrar como root, pinchar en Cambio de contrasena, introducir la clave nueva dos veces y pulsar Continuar
```

Having the default user and password, I created a dictionary with the target ports. Using the birthday attack and credential stuffing through a fuzzing attack I was able to spot around 20 hosts using the default credentials.



```
737) [0] kali:~ user$ wfuzz -c -z range,9020-9200 --basic [redacted]:[redacted]https://informatica.ieszaidinvergeles.org:FUZZ/cloud9/ide.html
 /usr/lib/python3/dist-packages/wfuzz/__init__.py:34: UserWarning:Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sites. Check Wfuzz's documentation for more infor
mation.
********************************************************
* Wfuzz 3.0.1 - The Web Fuzzer                         *
********************************************************

Target: https://informatica.ieszaidinvergeles.org:FUZZ/cloud9/ide.html
Total requests: 181

=====================================================================
ID           Response   Lines    Word     Chars       Payload
=====================================================================

000000031:   401        0 L      1 W      12 Ch       "9050"
000000015:   401        0 L      1 W      12 Ch       "9034"
000000007:   401        0 L      1 W      12 Ch       "9026"
000000041:   401        0 L      1 W      12 Ch       "9060"
000000040:   401        0 L      1 W      12 Ch       "9059"
000000003:   401        0 L      1 W      12 Ch       "9022"
000000042:   401        0 L      1 W      12 Ch       "9061"
000000043:   200        212 L    1236 W   41222 Ch    "9062"
000000039:   401        0 L      1 W      12 Ch       "9058"
000000035:   401        0 L      1 W      12 Ch       "9054"
000000034:   401        0 L      1 W      12 Ch       "9053"
000000033:   401        0 L      1 W      12 Ch       "9052"
000000037:   401        0 L      1 W      12 Ch       "9056"
000000036:   200        212 L    1195 W   34419 Ch    "9055"
000000038:   200        212 L    1198 W   50494 Ch    "9057"
000000030:   401        0 L      1 W      12 Ch       "9049"
000000032:   401        0 L      1 W      12 Ch       "9051"
000000026:   401        0 L      1 W      12 Ch       "9045"
000000028:   401        0 L      1 W      12 Ch       "9047"
000000029:   401        0 L      1 W      12 Ch       "9048"
000000025:   401        0 L      1 W      12 Ch       "9044"
000000027:   200        212 L    1208 W   41082 Ch    "9046"
000000024:   200        212 L    1195 W   37739 Ch    "9043"
000000022:   401        0 L      1 W      12 Ch       "9041"
000000021:   200        212 L    1204 W   32635 Ch    "9040"
000000018:   401        0 L      1 W      12 Ch       "9037"
000000019:   401        0 L      1 W      12 Ch       "9038"
000000023:   200        212 L    1192 W   32884 Ch    "9042"
000000020:   401        0 L      1 W      12 Ch       "9039"
000000014:   401        0 L      1 W      12 Ch       "9033"
000000017:   200        212 L    1186 W   33487 Ch    "9036"
```

Finally, logging in Cloud9 using the default credentials allowed me to spawn a CLI in the IDE. Since the user had root privileges, privilege scalation was not needed.

As evidence, I decided to deface one of the teachers app and upload some random memes and pictures.

Remediation Guidance

Implement secure random default passwords for each user, send them through a secure private channel to the final user (e.g. mail) and require setting a new password after the first login. Never store credentials in a public text file in plaintext.

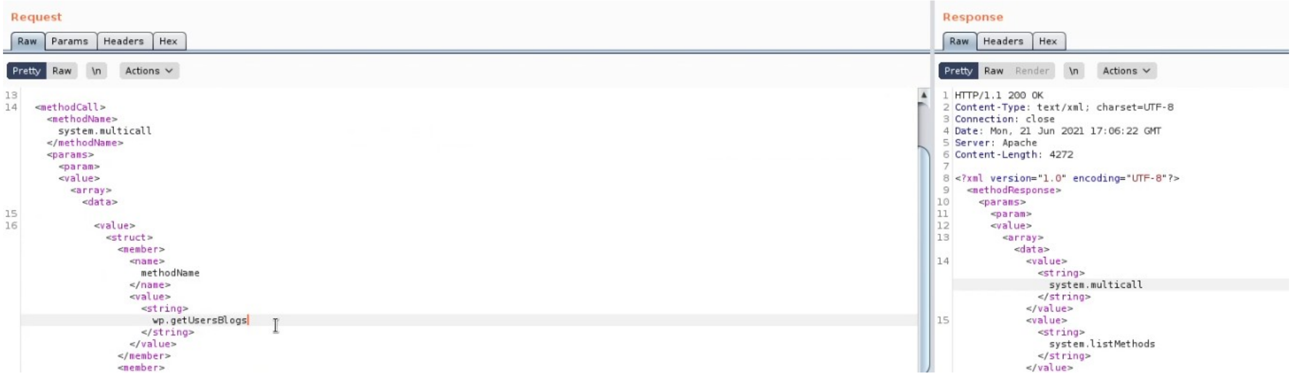
Wordpress XMLRPC Bruteforce Amplification

IZVs Wordpress login can be bruteforced using the XMLRPC protocol to obtain admin access to the content manager interface.

Vulnerability Details

Affects	https://www.ieszaidinvergeles.org
Attack Vectors	Brute Force Amplification
References	https://www.acunetix.com/vulnerabilities/web/wordpress-xml-rpc-authentication-brute-force https://github.com/1N3/Wordpress-XMLRPC-Brute-Force-Exploit

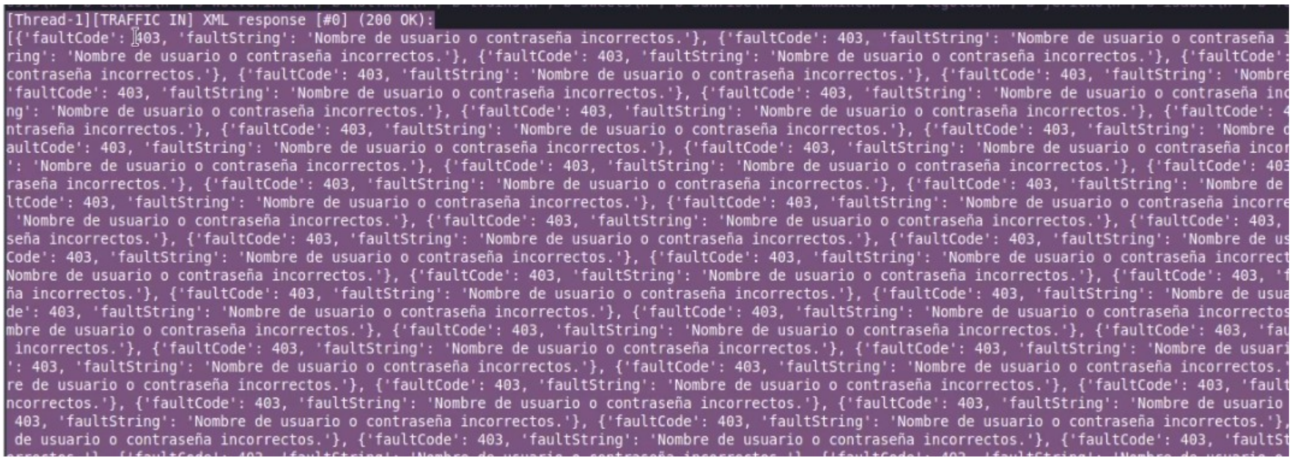
Fuzzing IZVs main webpage showed that Wordpress XMLRPC was found. Crafting arbitrary XML requests showed that the multicall procedure was available.



```
<methodCall>
  <methodName>
    system.multicall
  </methodName>
  <params>
    <param>
    <value>
      <array>
        <data>

          <value>
            <struct>
              <member>
                <name>
                  methodName
                </name>
                <value>
                  <string>
                    wp.getUsersBlogs
                  </string>
                </value>
              </member>
              <member>
```

```
HTTP/1.1 200 OK
Content-Type: text/xml; charset=UTF-8
Connection: close
Date: Mon, 21 Jun 2021 17:06:22 GMT
Server: Apache
Content-Length: 4272

<?xml version="1.0" encoding="UTF-8"?>
  <methodResponse>
    <params>
      <param>
      <value>
        <array>
          <data>
            <value>
              <string>
                system.multicall
              </string>
            </value>
            <value>
              <string>
                system.listMethods
              </string>
            </value>
```

Using the XMLRPC bruteforce amplification attack, the admin user password could be found



```
[Thread-1][TRAFFIC IN] XML response [#0] (200 OK):
[{'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña i
ring': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode':
contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre
'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña inc
ng': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 4
ntraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre d
aultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incor
': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403
raseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de
ltCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorre
 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403,
seña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de us
Code': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrect
Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'f
ña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usua
de': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos
mbre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'fau
 incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuari
': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'
re de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'fault
ncorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario
 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'},
 de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultString': 'Nombre de usuario o contraseña incorrectos.'}, {'faultCode': 403, 'faultSt
```

Remediation Guidance

Disable the XMLRPC feature in Wordpress

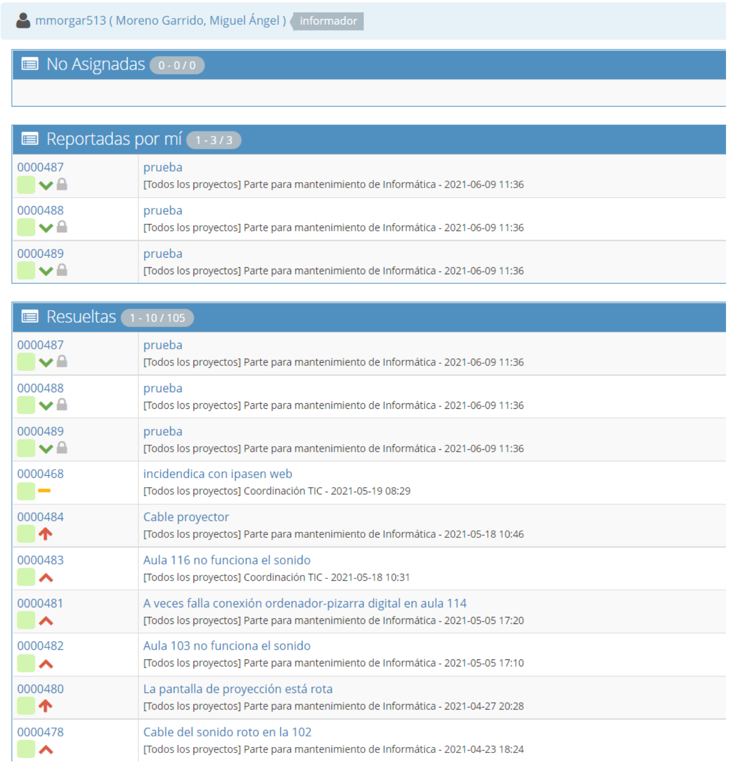
MantisBT Unauthorized Access

IZVs MantisBT service allows unauthorized accounts creation by any user.

Vulnerability Details

Affects	https://server.ieszaidinvergeles.org/mantisbt/admin/install.php https://server.ieszaidinvergeles.org/mantisbt
Attack Vectors	Improper Access Control
References	https://cwe.mitre.org/data/definitions/284.html

Checking AWStats access logs showed MantisBT was running in one of the hosts. Playing around with the app I noticed signing up was not restricted, so I created a user, using one of the teachers data in order to impersonate him, and got access to every bug or incident report and the permission to create new ones.



mmorgar513 (Moreno Garrido, Miguel Ángel) informador

No Asignadas 0 - 0 / 0

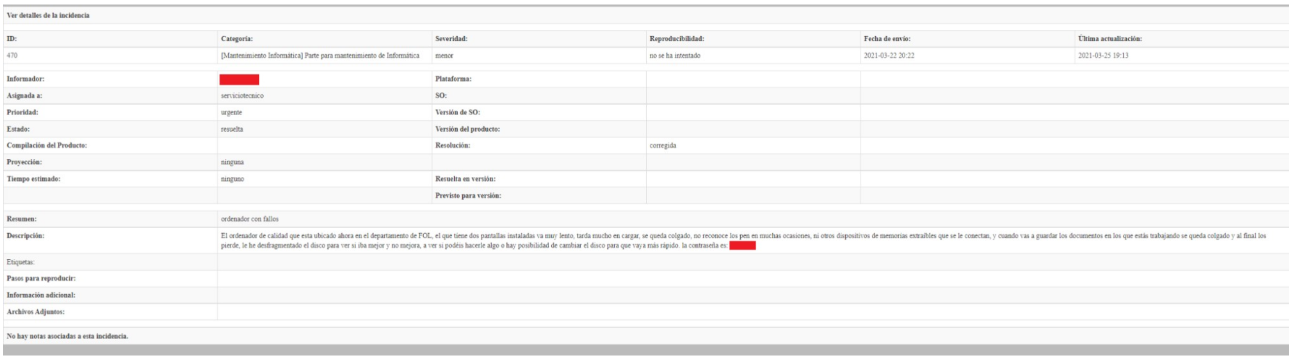
Reportadas por mí 1 - 3 / 3

0000487	prueba [Todos los proyectos] Parte para mantenimiento de Informática - 2021-06-09 11:36
0000488	prueba [Todos los proyectos] Parte para mantenimiento de Informática - 2021-06-09 11:36
0000489	prueba [Todos los proyectos] Parte para mantenimiento de Informática - 2021-06-09 11:36

Resueltas 1 - 10 / 105

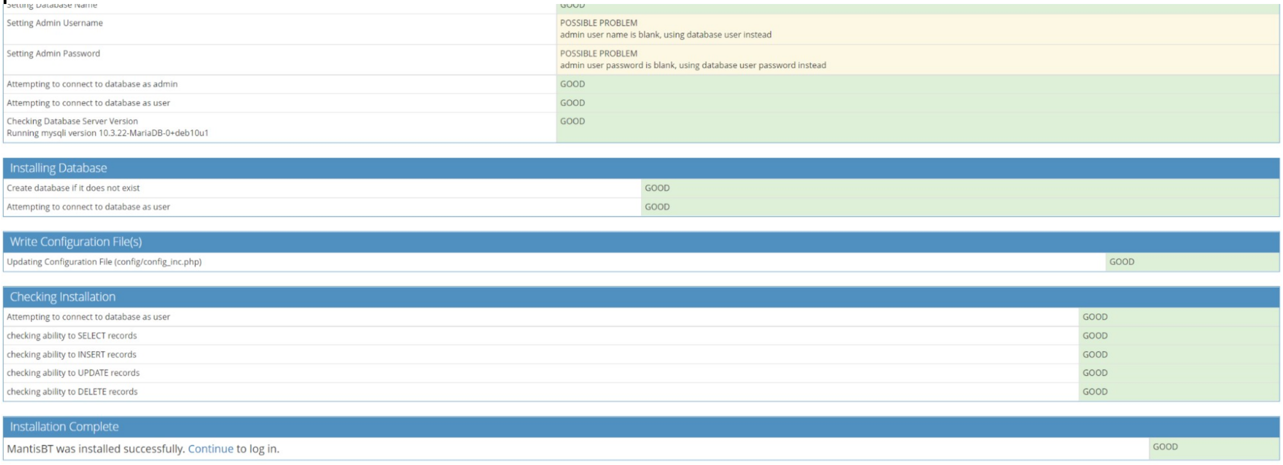
0000487	prueba [Todos los proyectos] Parte para mantenimiento de Informática - 2021-06-09 11:36
0000488	prueba [Todos los proyectos] Parte para mantenimiento de Informática - 2021-06-09 11:36
0000489	prueba [Todos los proyectos] Parte para mantenimiento de Informática - 2021-06-09 11:36
0000468	incidendica con ipasen web [Todos los proyectos] Coordinación TIC - 2021-05-19 08:29
0000484	Cable proyector [Todos los proyectos] Parte para mantenimiento de Informática - 2021-05-18 10:46
0000483	Aula 116 no funciona el sonido [Todos los proyectos] Coordinación TIC - 2021-05-18 10:31
0000481	A veces falla conexión ordenador-pizarra digital en aula 114 [Todos los proyectos] Parte para mantenimiento de Informática - 2021-05-05 17:20
0000482	Aula 103 no funciona el sonido [Todos los proyectos] Parte para mantenimiento de Informática - 2021-05-05 17:10
0000480	La pantalla de proyección está rota [Todos los proyectos] Parte para mantenimiento de Informática - 2021-04-27 20:28
0000478	Cable del sonido roto en la 102 [Todos los proyectos] Parte para mantenimiento de Informática - 2021-04-23 18:24

Using the bulk export feature I examined each report in order to find confidential information. Some MAC addresses and admin passwords for some PCs were leaked in plaintext on some of the reports



Ver detalles de la incidencia					
ID:	**Categoría:**	**Severidad:**	**Reproducibilidad:**	**Fecha de envío:**	**Última actualización:**
470	[Mantenimiento Informática] Parte para mantenimiento de Informática	menor	no se ha intentado	2021-03-22 20:22	2021-03-25 19:13
Informador:	[redacted]	**Plataforma:**			
Asignada a:	serviciotecnico	**SO:**			
Prioridad:	urgente	**Versión de SO:**			
Estado:	resuelta	**Versión del producto:**			
Compilación del Producto:		**Resolución:**	corregida		
Proyección:	ninguna				
Tiempo estimado:	ninguno	**Resuelta en versión:**			
		Previsto para versión:			
Resumen:	ordenador con fallos				
Descripción:	El ordenador de calidad que esta ubicado ahora en el departamento de FOL, el que tiene dos pantallas instaladas va muy lento, tarda mucho en cargar, se queda colgado, no reconoce los pen en muchas ocasiones, ni otros dispositivos de memorias extraíbles que se le conectan, y cuando vas a guardar los documentos en los que estás trabajando se queda colgado y al final los pierde, le he desfragmentado el disco para ver si iba mejor y no mejora, a ver si podéis hacerle algo o hay posibilidad de cambiar el disco para que vaya más rápido. la contraseña es: [redacted]				
Etiquetas:					
Pasos para reproducir:					
Información adicional:					
Archivos Adjuntos:					
No hay notas asociadas a esta incidencia.					

Also, the admin page is advised to be deleted after setting up the service by the own app. It wasn't deleted and I was able to drop the database even without the admin username or password



Setting Database Name	GOOD
Setting Admin Username	POSSIBLE PROBLEM admin user name is blank, using database user instead
Setting Admin Password	POSSIBLE PROBLEM admin user password is blank, using database user password instead
Attempting to connect to database as admin	GOOD
Attempting to connect to database as user	GOOD
Checking Database Server Version Running mysqli version 10.3.22-MariaDB-0+deb10u1	GOOD

Installing Database	
Create database if it does not exist	GOOD
Attempting to connect to database as user	GOOD

Write Configuration File(s)	
Updating Configuration File (config/config_inc.php)	GOOD

Checking Installation	
Attempting to connect to database as user	GOOD
checking ability to SELECT records	GOOD
checking ability to INSERT records	GOOD
checking ability to UPDATE records	GOOD
checking ability to DELETE records	GOOD

Installation Complete	
MantisBT was installed successfully. Continue to log in.	GOOD

Remediation Guidance

Limit the list of allowed mails to sign up in MantisBT, update to latest version and remove the public admin page.

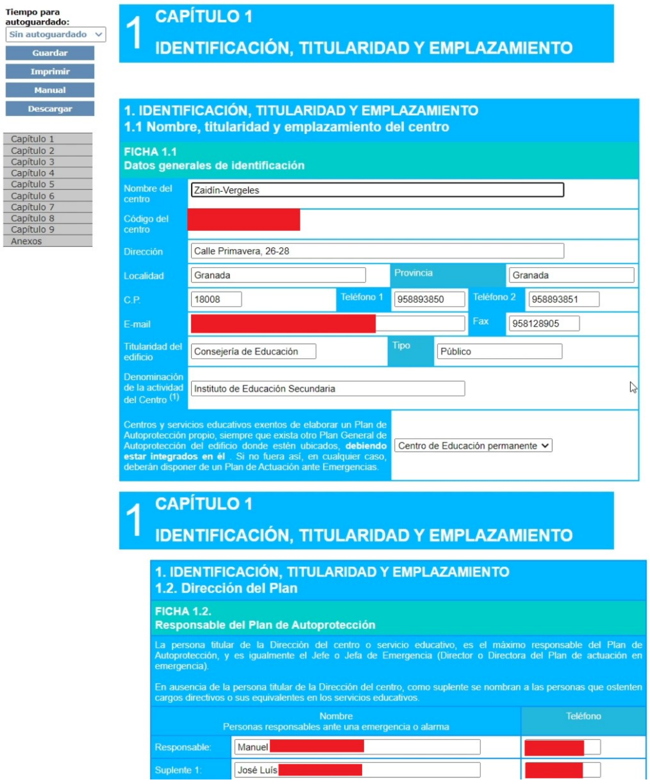
Margavila & PAE

IZVs Margavila & PAE documents can be accessed by unauthorized users to obtain confidential organizational and staff information.

Vulnerability Details

Affects	https://server.ieszaidinvergeles.org/margavila https://server.ieszaidinvergeles.org/PAE
Attack Vectors	HTTP Request
References	https://cwe.mitre.org/data/definitions/284.html

Using fuzzing some confidential documents were found. They contained private info such as a government email and private staff phone numbers



1 CAPÍTULO 1

IDENTIFICACIÓN, TITULARIDAD Y EMPLAZAMIENTO

1. IDENTIFICACIÓN, TITULARIDAD Y EMPLAZAMIENTO
1.1 Nombre, titularidad y emplazamiento del centro

FICHA 1.1
Datos generales de identificación

Nombre del centro	Zaidín-Vergeles		
Código del centro	[redacted]		
Dirección	Calle Primavera, 26-28		
Localidad	Granada	Provincia	Granada
C.P.	18008	Teléfono 1	958893850
		Teléfono 2	958893851
E-mail	[redacted]	Fax	958128905
Titularidad del edificio	Consejería de Educación	Tipo	Público
Denominación de la actividad del Centro (1)	Instituto de Educación Secundaria		

Centros y servicios educativos exentos de elaborar un Plan de Autoprotección propio, siempre que exista otro Plan General de Autoprotección del edificio donde estén ubicados, **debiendo estar integrados en él** . Si no fuera así, en cualquier caso, deberán disponer de un Plan de Actuación ante Emergencias.: Centro de Educación permanente

1 CAPÍTULO 1

IDENTIFICACIÓN, TITULARIDAD Y EMPLAZAMIENTO

1. IDENTIFICACIÓN, TITULARIDAD Y EMPLAZAMIENTO
1.2. Dirección del Plan

FICHA 1.2.
Responsable del Plan de Autoprotección

La persona titular de la Dirección del centro o servicio educativo, es el máximo responsable del Plan de Autoprotección, y es igualmente el Jefe o Jefa de Emergencia (Director o Directora del Plan de actuación en emergencia).

En ausencia de la persona titular de la Dirección del centro, como suplente se nombran a las personas que ostenten cargos directivos o sus equivalentes en los servicios educativos.

	Nombre Personas responsables ante una emergencia o alarma	Teléfono
Responsable:	Manuel [redacted]	[redacted]
Suplente 1:	José Luís [redacted]	[redacted]

Remediation Guidance

Remove the documents from the webserver or implement authorization

SlowLoris DOS

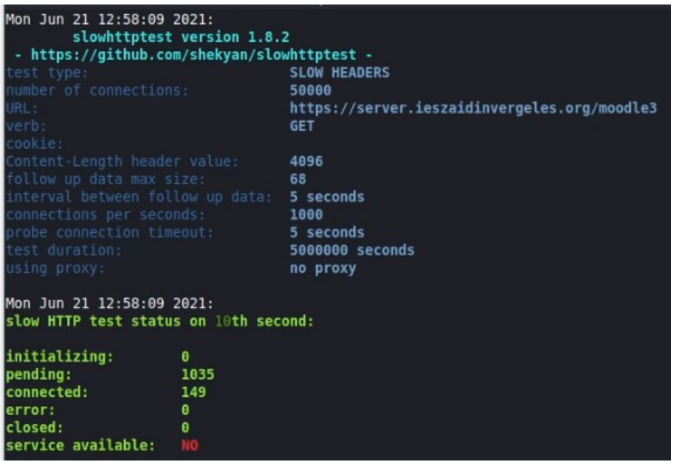
Multiple IZVs webservers are vulnerable to Apache SlowLoris vulnerability.

Vulnerability Details

Affects	https://server.ieszaidinvergeles.org/moodle3 https://informatica.ieszaidinvergeles.org
Attack Vectors	DOS
References	https://www.cvedetails.com/cve/CVE-2007-6750 https://capec.mitre.org/data/definitions/227.html

While testing for simple DOS attacks, SlowLoris was effective agains multiple IZV hosts. This is a kind of low-and-slow attack which keeps connections open to exhaust the web server.

This results in timed out responses for the rest of the users trying to access the web content



```
Mon Jun 21 12:58:09 2021:
        slowhttptest version 1.8.2
 - https://github.com/shekyan/slowhttptest -
test type:                        SLOW HEADERS
number of connections:            50000
URL:                              https://server.ieszaidinvergeles.org/moodle3
verb:                             GET
cookie:
Content-Length header value:      4096
follow up data max size:          68
interval between follow up data:  5 seconds
connections per seconds:          1000
probe connection timeout:         5 seconds
test duration:                    5000000 seconds
using proxy:                      no proxy

Mon Jun 21 12:58:09 2021:
slow HTTP test status on 10th second:

initializing:        0
pending:             1035
connected:           149
error:               0
closed:              0
service available:   NO
```

Remediation Guidance

Migrate to NginX

Wordpress Pingback DDOS

IZVs Wordpress can be used to participate in a DDOS botnet by using the XMLRPC pingback method.

Vulnerability Details

Affects	https://www.ieszaidinvergeles.org
Attack Vectors	DOS
References	https://capec.mitre.org/data/definitions/469.html https://managewp.com/blog/pingback-vulnerability-protect-wordpress

While testing XMLRPC protocol, it was found that the pingback procedure is allowed and can be exploited to join the host in a DDOS botnet.

Remediation Guidance

Disable the XMLRPC feature in Wordpress

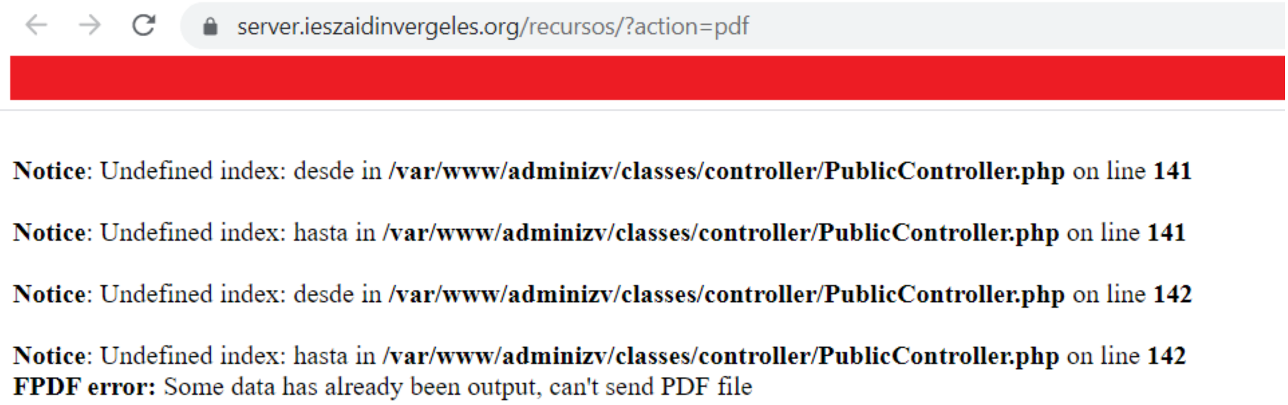
FPDF Error Absolute Path Disclosure

An error of the FPDF library usage shows the webserver absolute path.

Vulnerability Details

Affects	https://server.ieszaidinvergeles.org/recursos/?action=pdf
Attack Vectors	Fuzzing
References	https://capec.mitre.org/data/definitions/215.html

Fuzzing with random GET parameters showed an app error. It disclosed the absolute path and the usage of the FPDF library



```
Notice: Undefined index: desde in /var/www/adminizv/classes/controller/PublicController.php on line 141

Notice: Undefined index: hasta in /var/www/adminizv/classes/controller/PublicController.php on line 141

Notice: Undefined index: desde in /var/www/adminizv/classes/controller/PublicController.php on line 142

Notice: Undefined index: hasta in /var/www/adminizv/classes/controller/PublicController.php on line 142
FPDF error: Some data has already been output, can't send PDF file
```

Remediation Guidance

Fix the controller and disable error logs.

GetProfesores Open API Endpoint

An open API endpoint containing teachers info was found in the webserver.

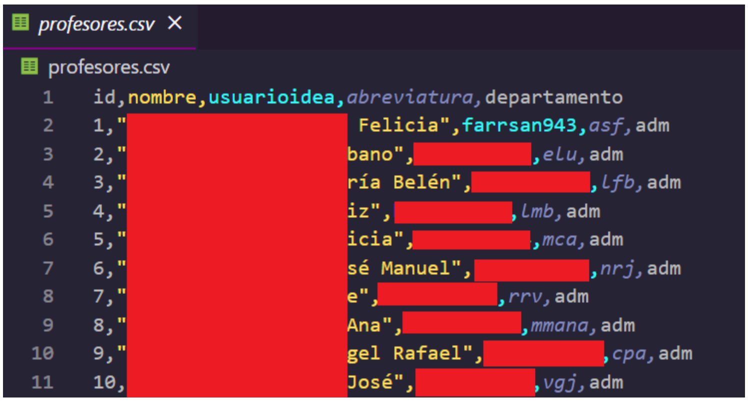
Vulnerability Details

Affects	https://www.ieszaidinvergeles.org
Attack Vectors	DOS
References	https://capec.mitre.org/data/definitions/469.html https://managewp.com/blog/pingback-vulnerability-protect-wordpress

The endpoint retrieved the following teachers data;

ID, full name, username and department.

Using this data we could find teachers mail addresses and check for breaches.



```
id,nombre,usuarioidea,abreviatura,departamento
1,"[redacted] Felicia",farrsan943,asf,adm
2,"[redacted]bano",[redacted],elu,adm
3,"[redacted]ría Belén",[redacted],lfb,adm
4,"[redacted]iz",[redacted],lmb,adm
5,"[redacted]icia",[redacted],mca,adm
6,"[redacted]sé Manuel",[redacted],nrj,adm
7,"[redacted]e",[redacted],rrv,adm
8,"[redacted]Ana",[redacted],mmana,adm
9,"[redacted]gel Rafael",[redacted],cpa,adm
10,[redacted]José",[redacted],vgj,adm
```

Remediation Guidance

Remove the endpoint or implement authorization

TimThumb Version Exposure

TimThumb version can be retrieved from the webserver.

Vulnerability Details

Affects	https://server.ieszaidinvergeles.org/puertasabiertas2021/img.php
Attack Vectors	None
References	https://www.dragonjar.org/vulnerabilidad-en-timthumb-php-afecta-millones-de-blogs-con-wordpress.xhtml

The used version was patched from the RCE, also webshots were disabled.

Remediation Guidance

It’s advised to use a non deprecated library since TimThumb is unmaintained.

SQLServer Version Exposure

SQLServer version can be retrieved from the webserver.

Vulnerability Details

Affects	https://server.ieszaidinvergeles.org/mssql/index2.php
Attack Vectors	None
References	

Remediation Guidance

Remove the file from the webserver to avoid version discovery.