Team: 10.4

Members – Abhishek, Diti, Dev and Aditi

Report Vulnerabilities

1. Vulnerability Name: Sensitive Data Exposer

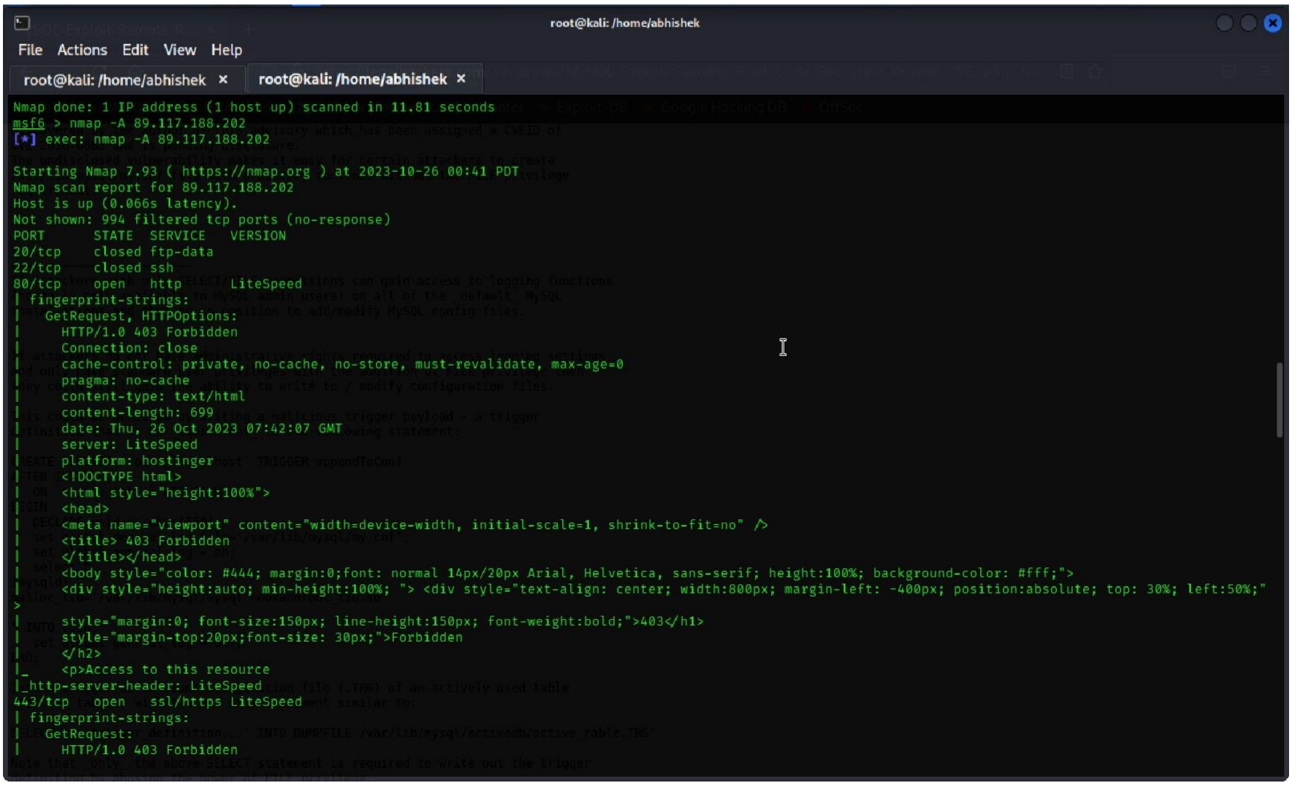
OWASP Category: Inadequate Data Protection

Description: The "Sensitive Data Exposer" vulnerability is a critical security flaw in web applications that puts confidential and personal information at risk. It occurs when sensitive data, such as credit card numbers or personal identification details, is not adequately protected. This can result from weak encryption, poor access controls, or insufficient data storage safeguards. Exploiting this vulnerability can lead to data breaches, financial loss, legal repercussions, and a tarnished reputation for the affected organization. Protecting against this vulnerability requires robust security measures and careful handling of sensitive data to prevent unauthorized access and disclosure.

Business Impact: The impact of a "Sensitive Data Exposer" vulnerability can be severe. It can lead to data breaches, identity theft, financial loss, legal consequences, reputational damage, and loss of customer trust. In addition, organizations may incur costs related to incident response and mitigation.

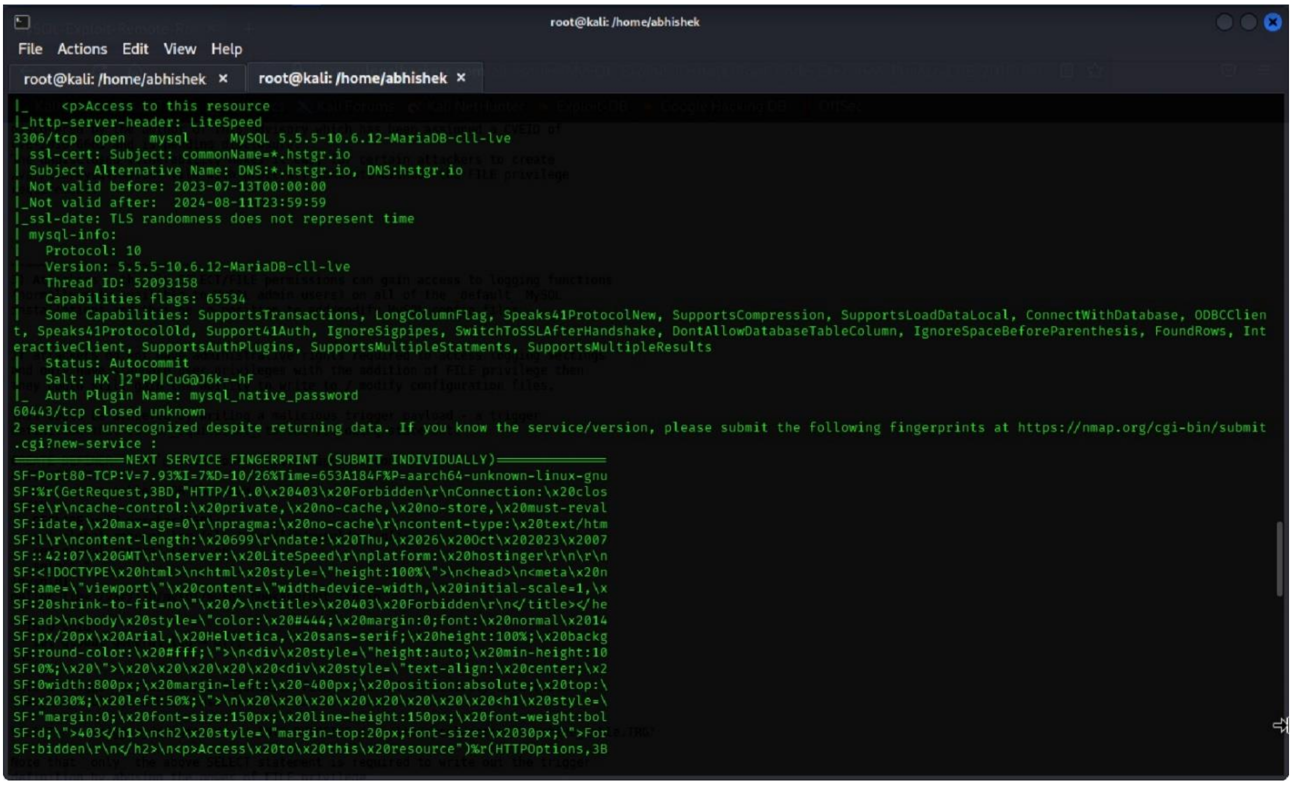
Vulnerability Path: The vulnerability path for a "Sensitive Data Exposer" can vary widely based on the specific implementation and circumstances of the application. It may involve multiple stages, including data collection, data storage, data transmission, and data access.

Vulnerability Parameter: The vulnerability parameter for a "Sensitive Data Exposer" depends on the specific data and context but can include various parameters where sensitive information is handled. These parameters can be things like input fields, database tables, file storage, APIs, and network communication channels.



```
Nmap done: 1 IP address (1 host up) scanned in 11.81 seconds
msf6 > nmap -A 89.117.188.202
[*] exec: nmap -A 89.117.188.202

Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-26 00:41 PDT
Nmap scan report for 89.117.188.202
Host is up (0.066s latency).
Not shown: 994 filtered tcp ports (no-response)
PORT      STATE  SERVICE   VERSION
20/tcp    closed ftp-data
22/tcp    closed ssh
80/tcp    open   http      LiteSpeed
| fingerprint-strings:
|   GetRequest, HTTPOptions:
|     HTTP/1.0 403 Forbidden
|     Connection: close
|     cache-control: private, no-cache, no-store, must-revalidate, max-age=0
|     pragma: no-cache
|     content-type: text/html
|     content-length: 699
|     date: Thu, 26 Oct 2023 07:42:07 GMT
|     server: LiteSpeed
|     platform: hostinger
|     <!DOCTYPE html>
|     <html style="height:100%">
|     <head>
|     <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no" />
|     <title> 403 Forbidden
|     </title></head>
|     <body style="color: #444; margin:0;font: normal 14px/20px Arial, Helvetica, sans-serif; height:100%; background-color: #fff;">
|     <div style="height:auto; min-height:100%; "> <div style="text-align: center; width:800px; margin-left: -400px; position:absolute; top: 30%; left:50%;"
>
|     style="margin:0; font-size:150px; line-height:150px; font-weight:bold;">403</h1>
|     style="margin-top:20px;font-size: 30px;">Forbidden
|     </h2>
|_    <p>Access to this resource
|_http-server-header: LiteSpeed
443/tcp   open   ssl/https LiteSpeed
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.0 403 Forbidden
```



```
|_    <p>Access to this resource
|_http-server-header: LiteSpeed
3306/tcp  open   mysql     MySQL 5.5.5-10.6.12-MariaDB-cll-lve
| ssl-cert: Subject: commonName=*.hstgr.io
| Subject Alternative Name: DNS:*.hstgr.io, DNS:hstgr.io
| Not valid before: 2023-07-13T00:00:00
|_Not valid after:  2024-08-11T23:59:59
|_ssl-date: TLS randomness does not represent time
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.6.12-MariaDB-cll-lve
|   Thread ID: 52093158
|   Capabilities flags: 65534
|   Some Capabilities: SupportsTransactions, LongColumnFlag, Speaks41ProtocolNew, SupportsCompression, SupportsLoadDataLocal, ConnectWithDatabase, ODBCClien
t, Speaks41ProtocolOld, Support41Auth, IgnoreSigpipes, SwitchToSSLAfterHandshake, DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, FoundRows, Int
eractiveClient, SupportsAuthPlugins, SupportsMultipleStatments, SupportsMultipleResults
|   Status: Autocommit
|   Salt: HX`]2"PP|CuG@J6k=-hF
|_  Auth Plugin Name: mysql_native_password
60443/tcp closed unknown
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi-bin/submit
.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.93%I=7%D=10/26%Time=653A184F%P=aarch64-unknown-linux-gnu
SF:%r(GetRequest,3BD,"HTTP/1\.0\x20403\x20Forbidden\r\nConnection:\x20clos
SF:e\r\ncache-control:\x20private,\x20no-cache,\x20no-store,\x20must-reval
SF:idate,\x20max-age=0\r\npragma:\x20no-cache\r\ncontent-type:\x20text/htm
SF:l\r\ncontent-length:\x20699\r\ndate:\x20Thu,\x2026\x20Oct\x202023\x2007
SF::42:07\x20GMT\r\nserver:\x20LiteSpeed\r\nplatform:\x20hostinger\r\n\r\n
SF:<!DOCTYPE\x20html>\n<html\x20style=\"height:100%\">\n<head>\n<meta\x20n
SF:ame=\"viewport\"\x20content=\"width=device-width,\x20initial-scale=1,\x
SF:20shrink-to-fit=no\"\x20/>\n<title>\x20403\x20Forbidden\r\n</title></he
SF:ad>\n<body\x20style=\"color:\x20#444;\x20margin:0;font:\x20normal\x2014
SF:px/20px\x20Arial,\x20Helvetica,\x20sans-serif;\x20height:100%;\x20backg
SF:round-color:\x20#fff;\">\n<div\x20style=\"height:auto;\x20min-height:10
SF:0%;\x20\">\x20\x20\x20\x20\x20<div\x20style=\"text-align:\x20center;\x2
SF:0width:800px;\x20margin-left:\x20-400px;\x20position:absolute;\x20top:\
SF:x2030%;\x20left:50%;\">\n\x20\x20\x20\x20\x20\x20\x20\x20<h1\x20style=\
SF:"margin:0;\x20font-size:150px;\x20line-height:150px;\x20font-weight:bol
SF:d;\">403</h1>\n<h2\x20style=\"margin-top:20px;font-size:\x2030px;\">For
SF:bidden\r\n</h2>\n<p>Access\x20to\x20this\x20resource")%r(HTTPOptions,3B
```

2. Vulnerability Name: Hidden URL Discovery

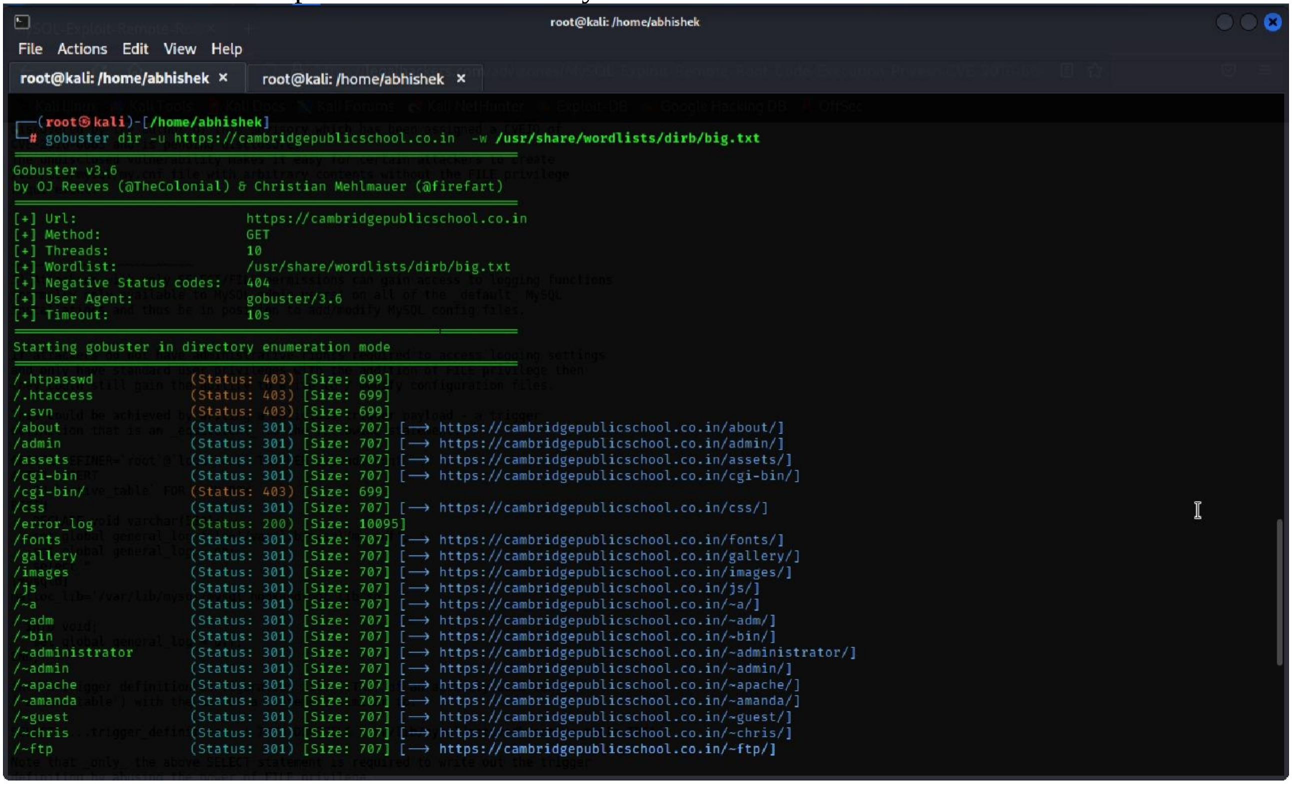
OWASP Category: Unauthorized Access,

Description: This situation involves the discovery of URLs that were not publicly linked or disclosed but can be accessed through directory and file enumeration. It may occur when a web application exposes URLs or files that should be hidden from public access, which could lead to unauthorized access or information disclosure.

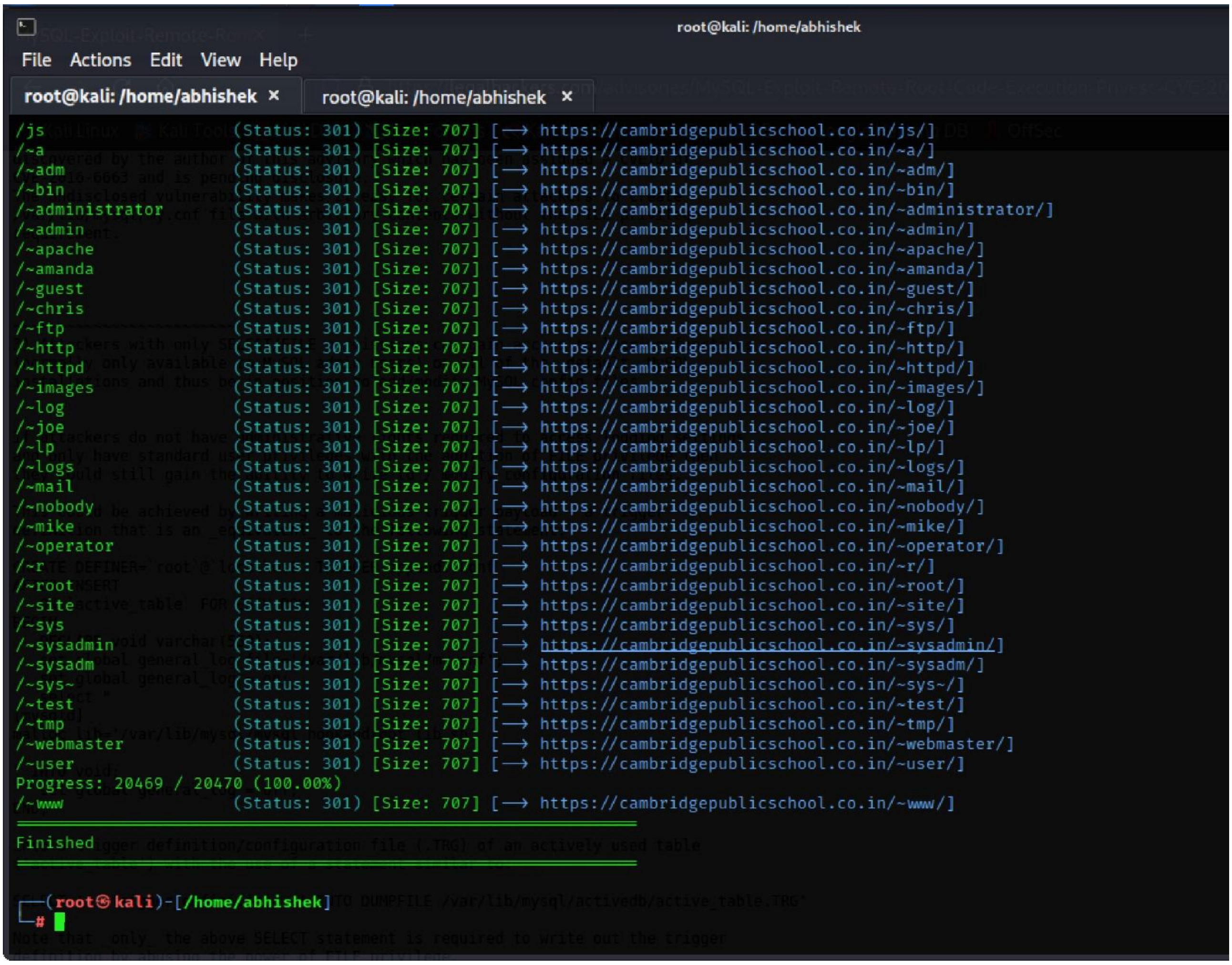
Business Impact: The impact can vary widely depending on what is discovered. It could potentially lead to unauthorized access to sensitive information, data exposure, or other security issues. The impact can range from minimal to severe, depending on what can be accessed and the nature of the web application.

Vulnerability Path: The vulnerability path involves the use of a tool like DirBuster or other directory and file enumeration techniques to discover hidden URLs. The path typically includes running the tool against the web application, analyzing the results, and attempting to access the discovered URLs.

Vulnerability Parameter: The vulnerability parameter would be the specific URLs or files discovered during the enumeration process. These URLs or files can be considered the parameters that were identified as part of the vulnerability.


root@kali: /home/abhishek
File
Actions
Edit
View
Help
root@kali: /home/abhishek ×
root@kali: /home/abhishek ×

```
┌──(root㉿kali)-[/home/abhishek]
└─# gobuster dir -u https://cambridgepublicschool.co.in  -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://cambridgepublicschool.co.in
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd            (Status: 403) [Size: 699]
/.htaccess            (Status: 403) [Size: 699]
/.svn                 (Status: 403) [Size: 699]
/about                (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/about/]
/admin                (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/admin/]
/assets               (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/assets/]
/cgi-bin              (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/cgi-bin/]
/cgi-bin/             (Status: 403) [Size: 699]
/css                  (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/css/]
/error_log            (Status: 200) [Size: 10095]
/fonts                (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/fonts/]
/gallery              (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/gallery/]
/images               (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/images/]
/js                   (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/js/]
/~a                   (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/~a/]
/~adm                 (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/~adm/]
/~bin                 (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/~bin/]
/~administrator       (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/~administrator/]
/~admin               (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/~admin/]
/~apache              (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/~apache/]
/~amanda              (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/~amanda/]
/~guest               (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/~guest/]
/~chris               (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/~chris/]
/~ftp                 (Status: 301) [Size: 707] [--> https://cambridgepublicschool.co.in/~ftp/]
```


root@kali: /home/abhishek
File Actions Edit View Help
root@kali: /home/abhishek ×
root@kali: /home/abhishek ×

```
/js                  (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/js/]
/~a                  (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~a/]
/~adm                (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~adm/]
/~bin                (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~bin/]
/~administrator      (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~administrator/]
/~admin              (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~admin/]
/~apache             (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~apache/]
/~amanda             (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~amanda/]
/~guest              (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~guest/]
/~chris              (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~chris/]
/~ftp                (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~ftp/]
/~http               (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~http/]
/~httpd              (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~httpd/]
/~images             (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~images/]
/~log                (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~log/]
/~joe                (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~joe/]
/~lp                 (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~lp/]
/~logs               (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~logs/]
/~mail               (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~mail/]
/~nobody             (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~nobody/]
/~mike               (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~mike/]
/~operator           (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~operator/]
/~r                  (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~r/]
/~root               (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~root/]
/~site               (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~site/]
/~sys                (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~sys/]
/~sysadmin           (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~sysadmin/]
/~sysadm             (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~sysadm/]
/~sys~               (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~sys~/]
/~test               (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~test/]
/~tmp                (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~tmp/]
/~webmaster          (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~webmaster/]
/~user               (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~user/]
Progress: 20469 / 20470 (100.00%)
/~www                (Status: 301) [Size: 707] [⟶ https://cambridgepublicschool.co.in/~www/]
===============================================================
Finished
===============================================================

┌──(root㉿kali)-[/home/abhishek]
└─#
```

3.Vulnerability Name: SQL Admin Vulnerability

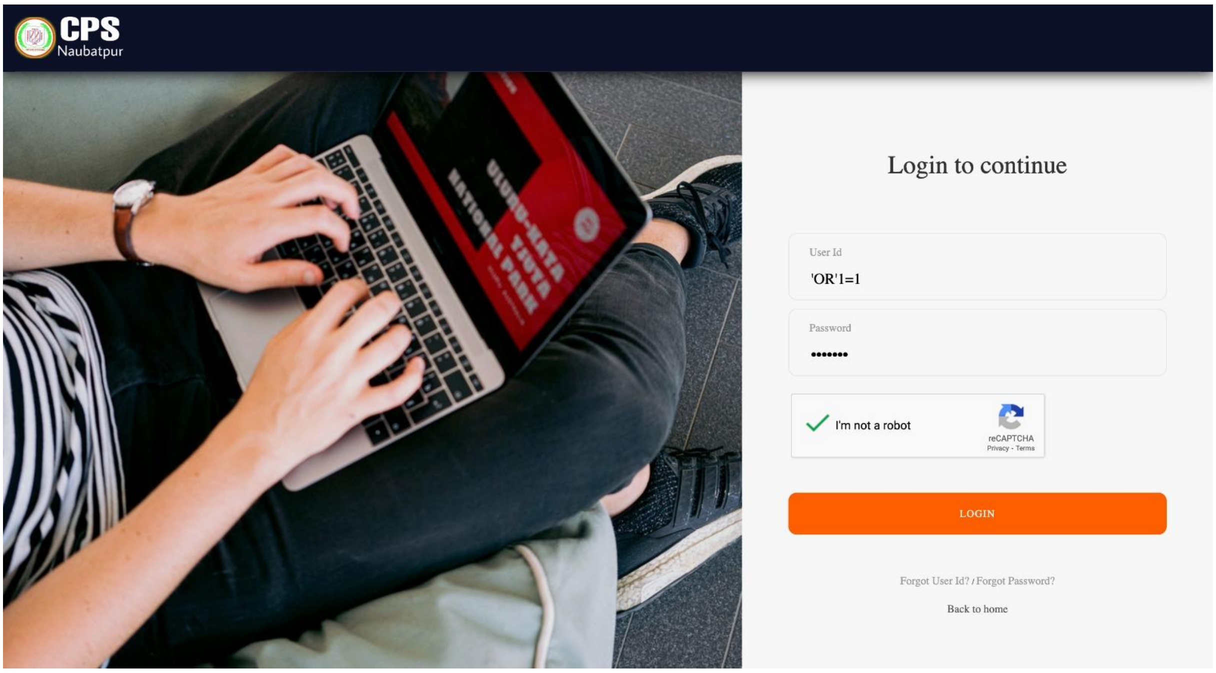
OWASP Category: Inadequate Security Configuration" or "Insecure Access Control

Description: The SQL Admin Vulnerability refers to a situation where the administrative interfaces or configurations of an SQL database are inadequately secured. This may include weak passwords, default credentials, or improper access controls, allowing unauthorized individuals to gain access to the database's administrative features.

Business Impact: The impact of this vulnerability can be significant. Unauthorized access to the SQL database's administrative functions can lead to data breaches, data manipulation, or even complete database compromise. This can result in data loss, financial loss, reputational damage, and legal consequences.

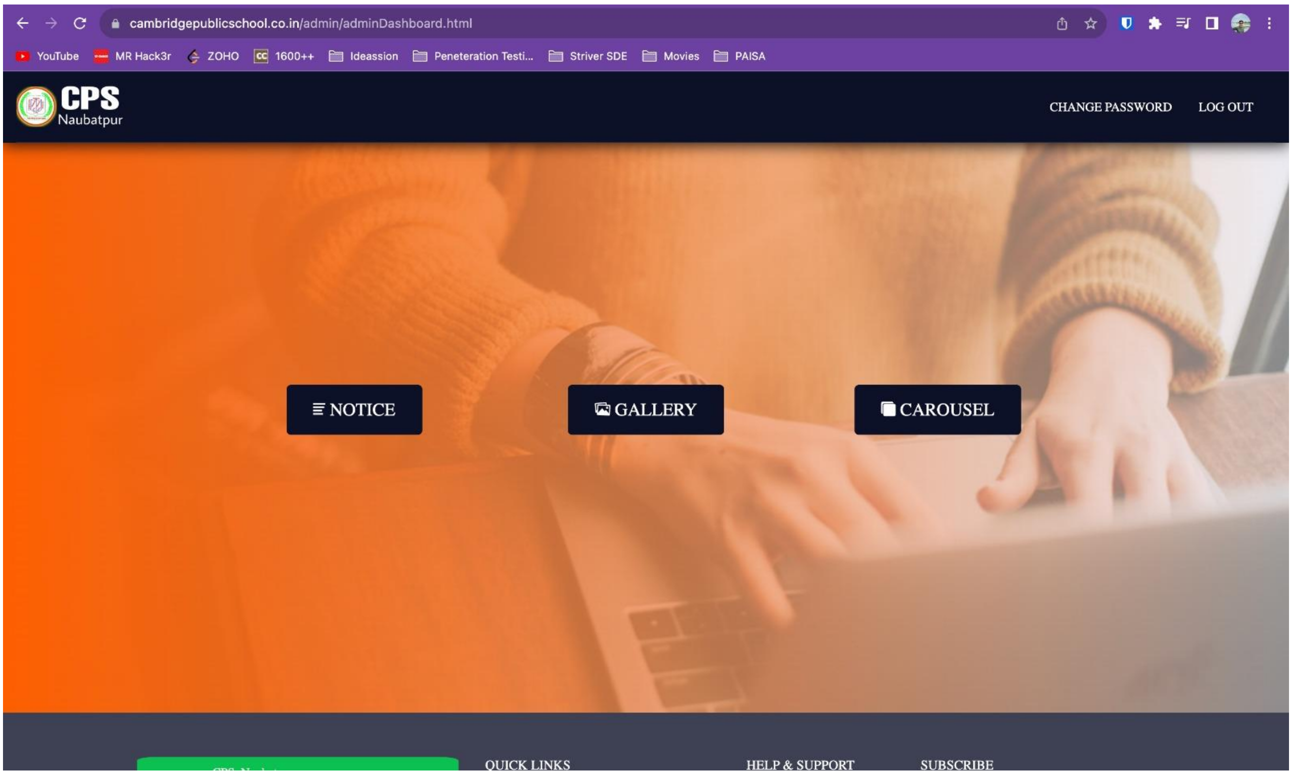
Vulnerability Path: The vulnerability path involves the identification and exploitation of weak or misconfigured administrative access points. Attackers may attempt to guess passwords, exploit known vulnerabilities, or leverage misconfigurations to gain unauthorized access to the SQL database's admin interfaces.

Vulnerability Parameter: The vulnerability parameters would be the specific administrative interfaces, settings, or configurations that are found to be improperly secured. These could include login pages, authentication settings, password policies, and access control lists related to SQL administration.



User Id: 'OR'1=1

Password: •••••••



cambridgepublicschool.co.in/admin/adminDashboard.html

4.Vulnerability Name: SWEET32

OWASP Category: In the OWASP Top Ten, SWEET32 would not have a specific category since it's primarily a cryptographic vulnerability related to outdated encryption algorithms and SSL/TLS.

Description: SWEET32 is a vulnerability that arises from the continued use of outdated cryptographic protocols like 3DES in SSL/TLS encryption. It stands for "Security of Web

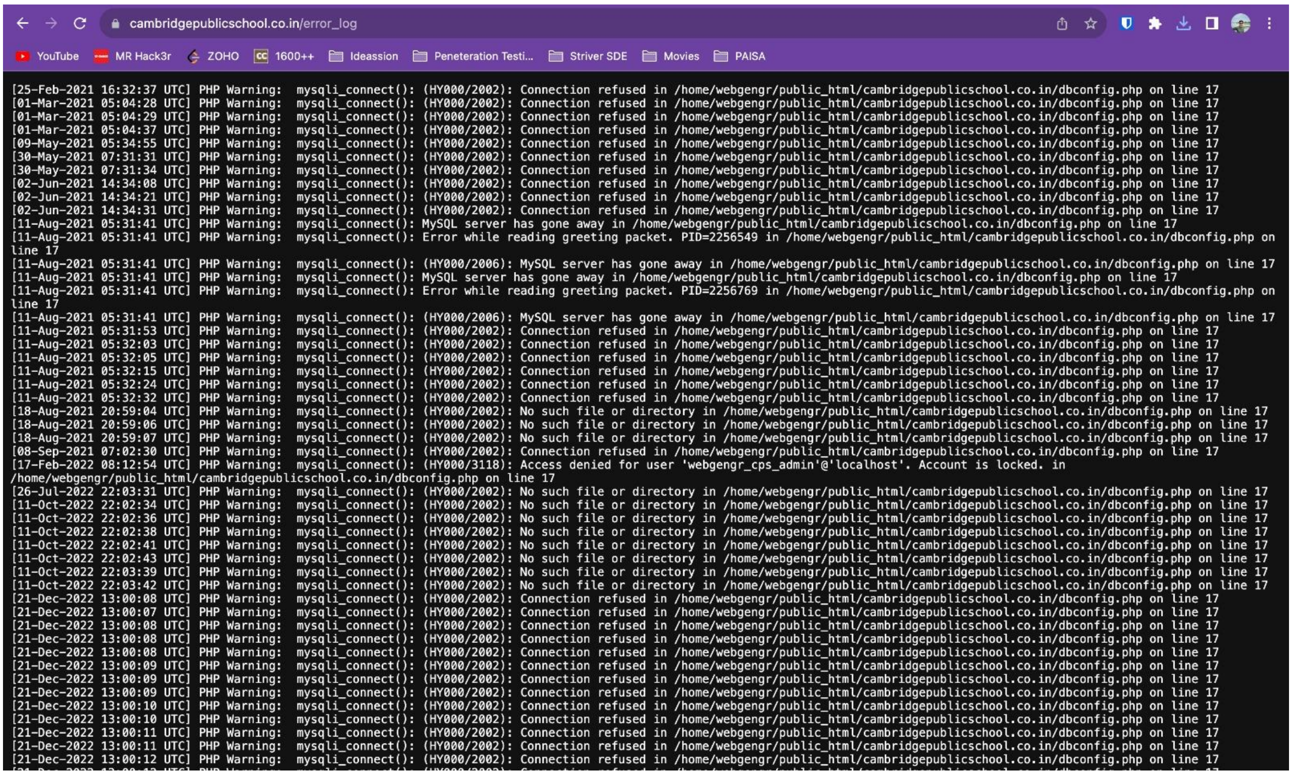
Encryption using Encryption over Triple-DES" and highlights the security implications of maintaining support for these weak encryption algorithms, which can be exploited by attackers.

Business Impact: The impact of SWEET32 is the potential for attackers to carry out a "birthday attack" and decrypt SSL/TLS-encrypted data, potentially exposing sensitive information. This can lead to data breaches, data exposure, and a loss of confidentiality and privacy.

Vulnerability Path: The vulnerability path typically involves attackers exploiting the continued use of 3DES in SSL/TLS to initiate a birthday attack. This may involve eavesdropping on encrypted communication and collecting a sufficient amount of data to carry out the attack.

Vulnerability Parameter: The vulnerability parameters in the context of SQL administration might involve the configuration of the SQL database server, including how it communicates with clients and the encryption protocols it supports. If the SQL database uses SSL/TLS encryption and supports outdated ciphers like 3DES, it could be vulnerable to SWEET32.

To mitigate SWEET32, it's essential to disable the use of weak encryption algorithms like 3DES and ensure that strong, modern encryption protocols are in place for all encrypted communications, including those involving SQL database connections. This vulnerability is not specific to SQL admin vulnerabilities, but securing the underlying infrastructure, including cryptographic protocols, is crucial to overall web application security.



```
[25-Feb-2021 16:32:37 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[01-Mar-2021 05:04:28 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[01-Mar-2021 05:04:29 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[01-Mar-2021 05:04:37 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[09-May-2021 05:34:55 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[30-May-2021 07:31:31 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[30-May-2021 07:31:34 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[02-Jun-2021 14:34:08 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[02-Jun-2021 14:34:21 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[02-Jun-2021 14:34:31 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Aug-2021 05:31:41 UTC] PHP Warning:  mysqli_connect(): MySQL server has gone away in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Aug-2021 05:31:41 UTC] PHP Warning:  mysqli_connect(): Error while reading greeting packet. PID=2256549 in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on
line 17
[11-Aug-2021 05:31:41 UTC] PHP Warning:  mysqli_connect(): (HY000/2006): MySQL server has gone away in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Aug-2021 05:31:41 UTC] PHP Warning:  mysqli_connect(): MySQL server has gone away in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Aug-2021 05:31:41 UTC] PHP Warning:  mysqli_connect(): Error while reading greeting packet. PID=2256769 in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on
line 17
[11-Aug-2021 05:31:41 UTC] PHP Warning:  mysqli_connect(): (HY000/2006): MySQL server has gone away in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Aug-2021 05:31:53 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Aug-2021 05:32:03 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Aug-2021 05:32:05 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Aug-2021 05:32:15 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Aug-2021 05:32:24 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Aug-2021 05:32:32 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[18-Aug-2021 20:59:04 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[18-Aug-2021 20:59:06 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[18-Aug-2021 20:59:07 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[08-Sep-2021 07:02:30 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[17-Feb-2022 08:12:54 UTC] PHP Warning:  mysqli_connect(): (HY000/3118): Access denied for user 'webgengr_cps_admin'@'localhost'. Account is locked. in
/home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[26-Jul-2022 22:03:31 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Oct-2022 22:02:34 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Oct-2022 22:02:36 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Oct-2022 22:02:38 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Oct-2022 22:02:41 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Oct-2022 22:02:43 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Oct-2022 22:03:39 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[11-Oct-2022 22:03:42 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): No such file or directory in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:08 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:07 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:08 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:08 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:08 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:09 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:09 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:09 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:10 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:10 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:11 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:11 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
[21-Dec-2022 13:00:12 UTC] PHP Warning:  mysqli_connect(): (HY000/2002): Connection refused in /home/webgengr/public_html/cambridgepublicschool.co.in/dbconfig.php on line 17
```

5. Vulnerability Name: Unauthorized Access to Admin URL

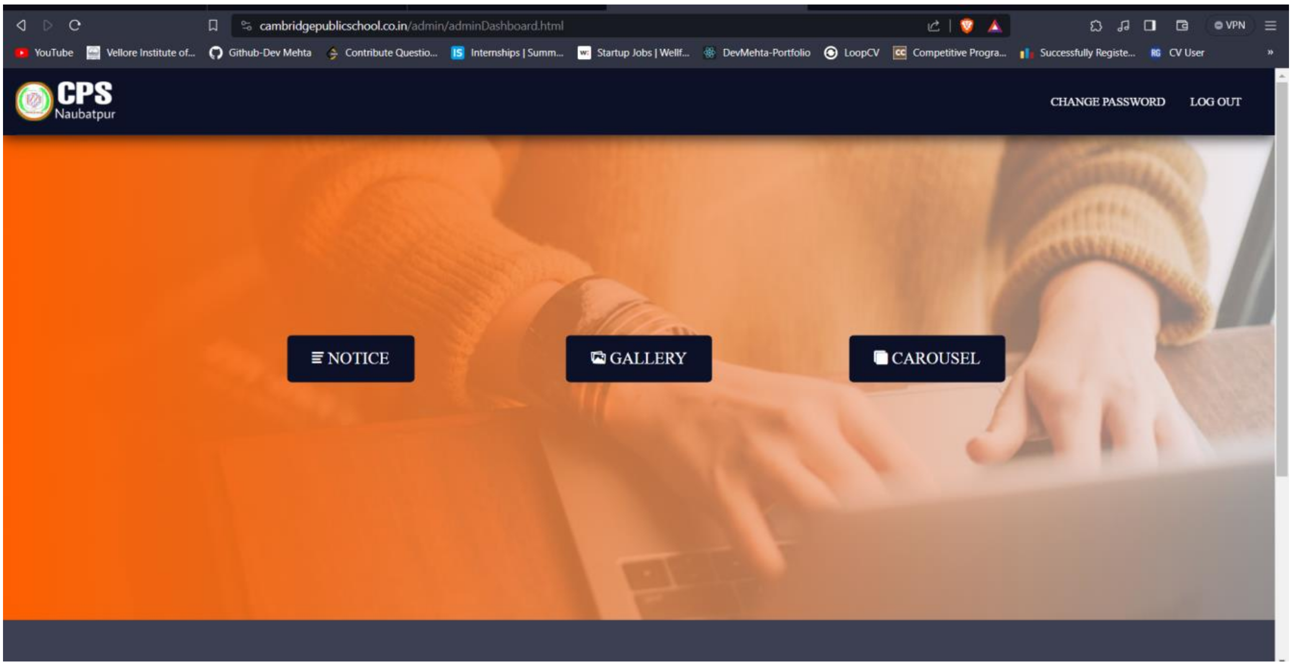
OWASP Category: A5 - Security Misconfiguration

Description: This vulnerability allows an attacker to access the admin URL of a website without the need for proper authentication. Attackers can exploit misconfigured access controls or weak authentication mechanisms to directly access sensitive administrative functionalities or pages reserved for authorized personnel.

Business Impact: Unauthorized access to admin functionalities can lead to unauthorized data manipulation, theft, or deletion. Attackers could potentially disrupt the normal functioning of the website, compromise user data, or deface the site, leading to reputational damage and loss of customer trust.

Vulnerability Path: The vulnerability occurs due to misconfigured access controls or weak authentication mechanisms. It can also result from improper URL handling or lack of proper authorization checks on the server side.

Vulnerability Parameter: The vulnerable parameter in this case is the lack of proper authentication and authorization checks for accessing the admin URL.



On searching this *URL*, it directly opens admin settings without asking for login details.