Vulnerability Assessment and Penetration Report

August 26th, 2024

Report For: **REDTEAM**

Prepared By: **ABHINAV S**

Sensitive: The information in this document is strictly confidential and is made by ABHINAV S

TABLE OF CONTENTS

Document Control

Client Confidentiality

This document contains Client Confidential information and may not be copied without written permission.

Proprietary Information

The content of this document is considered proprietary information and should not be disclosed outside of the recipient organization’s network.

Pen Test-Hub gives permission to copy this report for the purposes of disseminating information within your organization or any regulatory agency.

EXECUTIVE SUMMARY

I performed a security assessment on four different web applications. The purpose of this assessment was to discover and identify vulnerabilities in the four websites' infrastructure and suggest methods to remediate the vulnerabilities and identified a total of four vulnerabilities within the scope of the engagement which are broken down by severity in the table below.

#	Risk Rating	CVSSv3 Score	Description
1	**CRITICAL**	9.0 - 10	A vulnerability was discovered that has been rated as critical. This requires resolution as quickly as possible.
2	**HIGH**	7.0 – 8.9	A vulnerability was discovered that has been rated as high. This requires resolution in a short term.
3	**MEDIUM**	4.0 – 6.9	A vulnerability was discovered that has been rated as medium. This should be resolved throughout the ongoing maintenance process.
4	**LOW**	1.0 – 3.9	A vulnerability was discovered that has been rated as low. This should be addressed as part of routine maintenance tasks.
5	**INFO**	0 – 0.9	A discovery was made that is reported for information. This should be addressed in order to meet leading practice.

The highest severity vulnerabilities give potential attackers the opportunity in confidential data being deleted, lost or stolen; websites being defaced; unauthorized access to systems or accounts and, ultimately, compromise of individual machines or entire networks. In order to ensure data confidentiality, integrity, and availability, security remediations should be implemented as described in the security assessment findings.

Note that this assessment may not disclose all vulnerabilities that are present on the systems within the scope. Any changes made to the environment during the period of testing may affect the results of the assessment.

SCOPE

Security assessment includes testing for security loopholes in the scope defined below. Apart from the following, no other information was provided. Nothing was assumed at the start of the security assessment. The following was the scope covered under the security audit:

Web Application 1:

http://www.trinity-me.com/AdminLogin.aspx

Web Application 2:

https://ycet.ac.in/.

Web Application 3:

https://www.odishaassembly.nic.in/

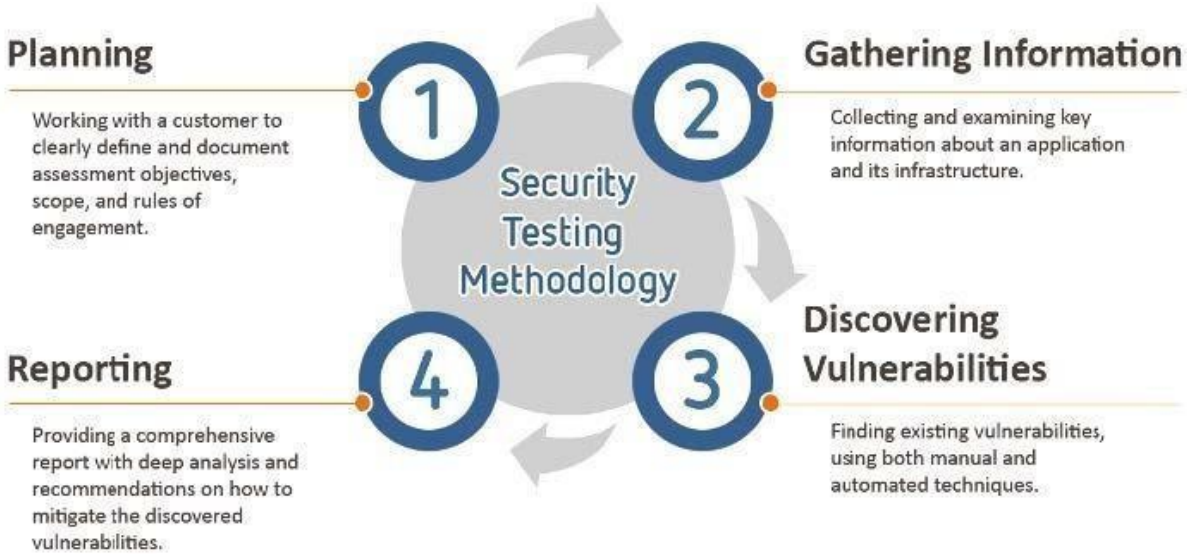
Web Application 4:

http://onlineagaetn.cag.gov.in/Login

TESTING METHODOLOGY

My testing methodology was split into three phases: Reconnaissance, Target Assessment, and Discovering Vulnerabilities. During reconnaissance, we gathered information about the web applications. I gathered evidence of vulnerabilities during this phase of the engagement in a manner that would not disrupt normal business operations.

The following image is a graphical representation of this methodology.


Planning
1
Working with a customer to clearly define and document assessment objectives, scope, and rules of engagement.
Gathering Information
2
Collecting and examining key information about an application and its infrastructure.
Security Testing Methodology
Discovering Vulnerabilities
3
Finding existing vulnerabilities, using both manual and automated techniques.
Reporting
4
Providing a comprehensive report with deep analysis and recommendations on how to mitigate the discovered vulnerabilities.

CLASSIFICATION

RISK CLASSIFICATION

LEVEL	SCORE	DESCRIPTION
Critical	10	The vulnerability poses an immediate threat to the organization. Successful exploitation may permanently affect the organization. Remediation should be immediately performed.
High	7-9	The vulnerability poses an urgent threat to the organization, and remediation should be prioritized.
Medium	4-6	Successful exploitation is possible and may result in notable disruption of business functionality. This vulnerability should be remediated when feasible.
Low	1-3	The vulnerability poses a negligible/minimal threat to the organization. The presence of this vulnerability should be noted and remediated if possible.
Information	0	These findings have no clear threat to the organization, but may cause business process to function differently than desired or reveal sensitive information about the company

ASSESSMENT FINDINGS

Number	Findings	CVSS	Severity
1	SQL Injection	9	Critical
2	Cross Site Scripting (XSS)	7	High
3	Secure Flag Missing	4.2	Medium
4	Clickjacking	3.1	Low

VULNERABILITY #1

CRITICAL RISK (9/10)	
Name of Vulnerability	**SQL INJECTION**
Security Impact	**Severe**

Vulnerable URL

http://www.trinity-me.com/AdminLogin.aspx

Security Implications

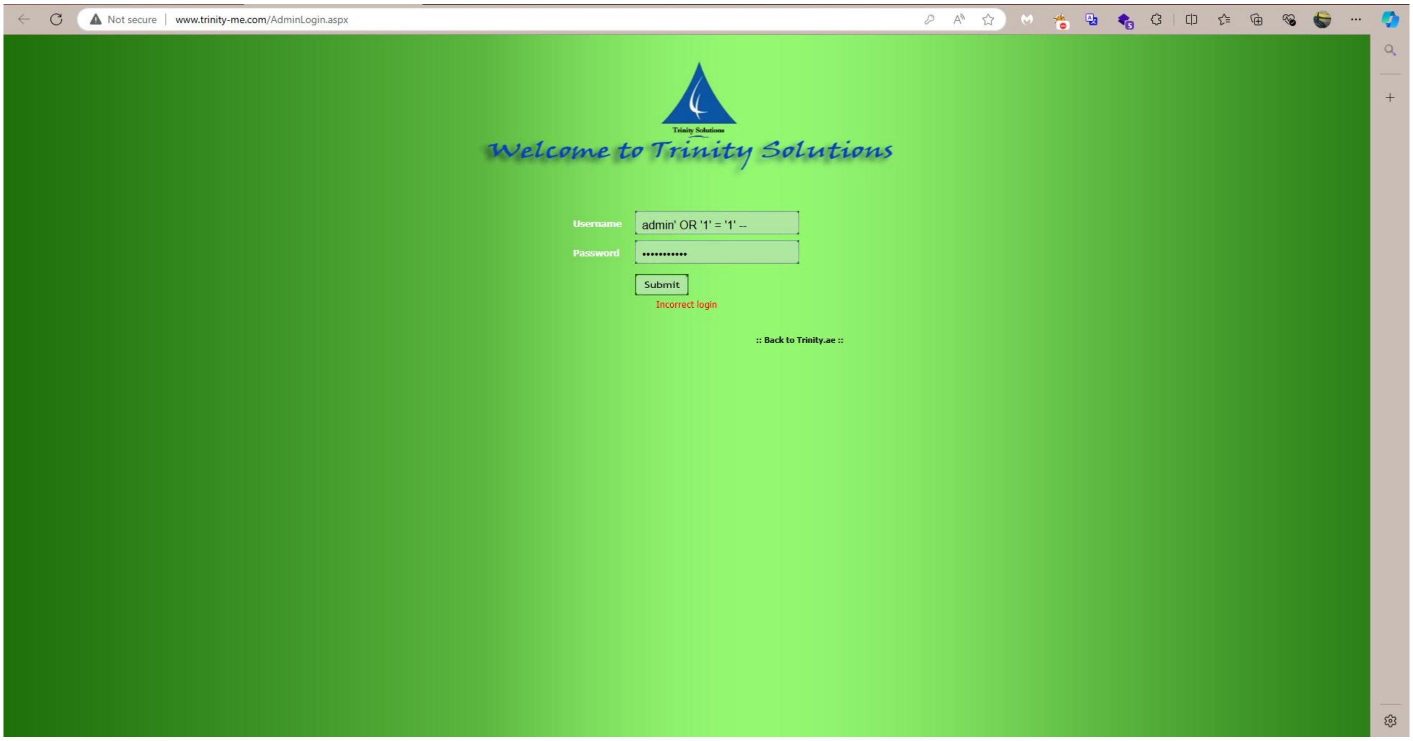
SQL injection vulnerabilities can have severe security implications for web applications. Attackers can exploit these vulnerabilities to bypass authentication, access sensitive data, modify or delete data, and even execute arbitrary commands on the underlying database server. This can lead to data breaches, unauthorized access, and compromise of the entire system.

Steps to Reproduce

1. Identify the target website: The target website is http://www.trinity-me.com/AdminLogin.aspx
2. Inject SQL Error: Append a sql injection payload in the login page ‘ OR ‘1’ = ‘1’ --. For example: admin’ OR ‘1’ = ‘1’ --

3. Observe Error Response: Note any error messages or abnormal behavior returned by the application, indicating a possible SQL injection vulnerability.
4. Confirm Vulnerability: Verify the presence of a SQL injection vulnerability by observing how the application handles the injected SQL error.
5. Exploit : Found that the payload is been worked and we have got the admin access

Screenshots



Not secure | www.trinity-me.com/AdminLogin.aspx

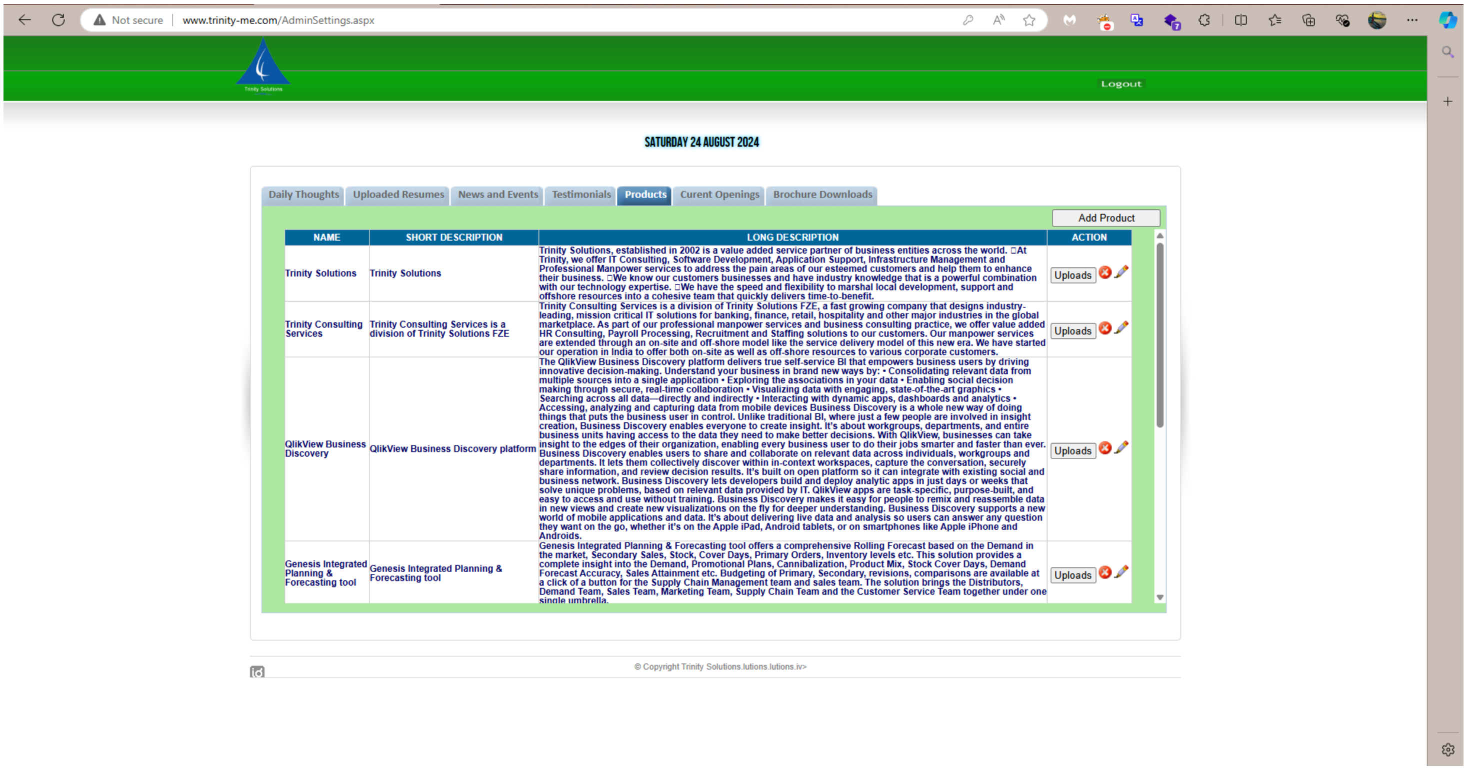
Welcome to Trinity Solutions

Username: admin' OR '1' = '1' --

Password: •••••••••••

Incorrect login

:: Back to Trinity.ae ::



Not secure | www.trinity-me.com/AdminSettings.aspx

SATURDAY 24 AUGUST 2024

NAME	SHORT DESCRIPTION	LONG DESCRIPTION	ACTION
Trinity Solutions	Trinity Solutions	Trinity Solutions, established in 2002 is a value added service partner of business entities across the world. □At Trinity, we offer IT Consulting, Software Development, Application Support, Infrastructure Management and Professional Manpower services to address the pain areas of our esteemed customers and help them to enhance their business. □We know our customers businesses and have industry knowledge that is a powerful combination with our technology expertise. □We have the speed and flexibility to marshal local development, support and offshore resources into a cohesive team that quickly delivers time-to-benefit.	Uploads
Trinity Consulting Services	Trinity Consulting Services is a division of Trinity Solutions FZE	Trinity Consulting Services is a division of Trinity Solutions FZE, a fast growing company that designs industry-leading, mission critical IT solutions for banking, finance, retail, hospitality and other major industries in the global marketplace. As part of our professional manpower services and business consulting practice, we offer value added HR Consulting, Payroll Processing, Recruitment and Staffing solutions to our customers. Our manpower services are extended through an on-site and off-shore model like the service delivery model of this new era. We have started our operation in India to offer both on-site as well as off-shore resources to various corporate customers.	Uploads
QlikView Business Discovery	QlikView Business Discovery platform	The QlikView Business Discovery platform delivers true self-service BI that empowers business users by driving innovative decision-making. Understand your business in brand new ways by: • Consolidating relevant data from multiple sources into a single application • Exploring the associations in your data • Enabling social decision making through secure, real-time collaboration • Visualizing data with engaging, state-of-the-art graphics • Searching across all data—directly and indirectly • Interacting with dynamic apps, dashboards and analytics • Accessing, analyzing and capturing data from mobile devices Business Discovery is a whole new way of doing things that puts the business user in control. Unlike traditional BI, where just a few people are involved in insight creation, Business Discovery enables everyone to create insight. It's about workgroups, departments, and entire business units having access to the data they need to make better decisions. With QlikView, businesses can take insight to the edges of their organization, enabling every business user to do their jobs smarter and faster than ever. Business Discovery enables users to share and collaborate on relevant data across individuals, workgroups and departments. It lets them collectively discover within in-context workspaces, capture the conversation, securely share information, and review decision results. It's built on open platform so it can integrate with existing social and business network. Business Discovery lets developers build and deploy analytic apps in just days or weeks that solve unique problems, based on relevant data provided by IT. QlikView apps are task-specific, purpose-built, and easy to access and use without training. Business Discovery makes it easy for people to remix and reassemble data in new views and create new visualizations on the fly for deeper understanding. Business Discovery supports a new world of mobile applications and data. It's about delivering live data and analysis so users can answer any question they want on the go, whether it's on the Apple iPad, Android tablets, or on smartphones like Apple iPhone and Androids.	Uploads
Genesis Integrated Planning & Forecasting tool	Genesis Integrated Planning & Forecasting tool	Genesis Integrated Planning & Forecasting tool offers a comprehensive Rolling Forecast based on the Demand in the market, Secondary Sales, Stock, Cover Days, Primary Orders, Inventory levels etc. This solution provides a complete insight into the Demand, Promotional Plans, Cannibalization, Product Mix, Stock Cover Days, Demand Forecast Accuracy, Sales Attainment etc. Budgeting of Primary, Secondary, revisions, comparisons are available at a click of a button for the Supply Chain Management team and sales team. The solution brings the Distributors, Demand Team, Sales Team, Marketing Team, Supply Chain Team and the Customer Service Team together under one single umbrella.	Uploads

© Copyright Trinity Solutions.lutions.lutions.iv>

Impacts

The exploitation of SQL injection vulnerabilities can result in significant impacts, including:

- Data Exposure: Attackers can extract sensitive information from the database, such as user credentials, personal data, or proprietary information.
- Data Modification or Deletion: Malicious actors can modify or delete data within the database, leading to data corruption or loss.
- Account Takeover: By extracting user credentials, attackers can gain unauthorized access to user accounts or administrative privileges.
- System Compromise: In severe cases, exploitation of SQL injection vulnerabilities can lead to the compromise of the entire system, allowing attackers to execute arbitrary commands on the underlying server.

Reference

OWASP. (n.d.). SQL Injection. Retrieved from https://owasp.org/www-community/attacks/SQL_Injection

VULNERABILITY #2

HIGH RISK (7/10)	
Name of Vulnerability	**Cross Site Scripting**
Security Impact	**High**

Vulnerable URL

https://www.fenixlight.com/product/index.php?id=37

Security Implications

Cross-Site Scripting (XSS) attacks are a type of injection, in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in the form of a browser side script, to a different end user. Flaws that allow these attacks to succeed are quite widespread and occur anywhere a web application uses input from a user within the output it generates without validating or encoding it.

An attacker can use XSS to send a malicious script to an unsuspecting user. The end user's browser has no way to know that the script should not be trusted, and will execute the script. Because it thinks the script came from a trusted source, the malicious script can access any cookies, session tokens, or other sensitive information retained by the browser and used with that site. These scripts can even rewrite the content of the HTML page.

Cross-Site Scripting (XSS) attacks occur when:

1. Data enters a Web application through an untrusted source, most frequently a web request.
2. The data is included in dynamic content that is sent to a web user without being validated for malicious content.

The malicious content sent to the web browser often takes the form of a segment of JavaScript, but may also include HTML, Flash, or any other type of code that the browser may execute. The variety of attacks based on XSS is almost limitless, but they commonly include transmitting private data, like cookies or other session information, to the attacker, redirecting the victim to web content controlled by the attacker, or performing other malicious operations on the user's machine under the guise of the vulnerable site.

Reflected XSS Attacks

Reflected attacks are those where the injected script is reflected off the web server, such as in an error message, search result, or any other response that includes some or all of the input sent to the server as part of the request. Reflected attacks are delivered to victims via another route, such as in an e-mail message, or on some other website. Reflected XSS is also sometimes referred to as Non-Persistent or Type-I XSS (the attack is carried out through a single request / response cycle).

Stored XSS Attacks

Stored attacks are those where the injected script is permanently stored on the target servers, such as in a database, in a message forum, visitor log, comment field, etc. The victim then retrieves the malicious script from the server when it requests the stored information. Stored XSS is also sometimes referred to as Persistent or Type-II XSS.

Blind Cross-site Scripting

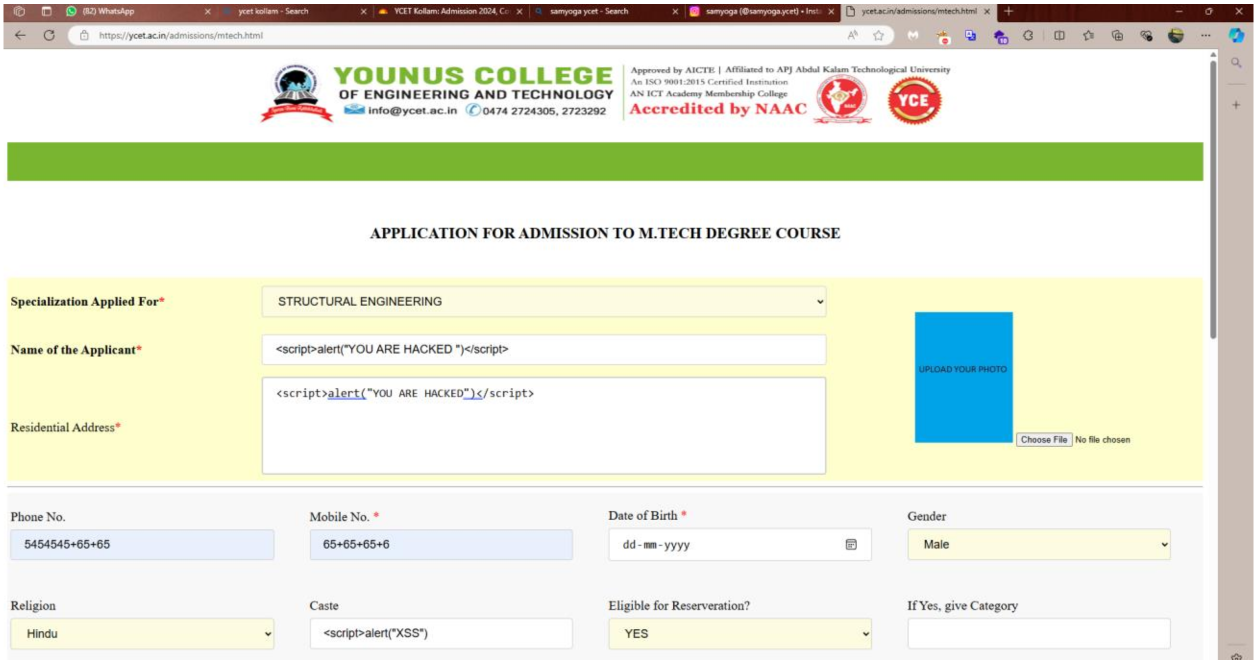
Blind Cross-site Scripting is a form of persistent XSS. It generally occurs when the attacker's payload is saved on the server and reflected back to the victim from the backend application. For example, in feedback forms, an attacker can submit the malicious payload using the form, and once the backend user/admin of the application will open the attacker's submitted form via the backend application, the attacker's payload will get executed.

Other Types of XSS Vulnerabilities

In addition to Stored and Reflected XSS, another type of XSS, DOM Based XSS was identified by Amit Klein in 2005.

Steps to Reproduce

1. Begin by navigating to the target website https://ycet.ac.in/
2. Inject the payload <script>alert("YOU ARE HACKED")</script> into the forms provided in the website.
3. Upon injecting the payload, the site will popup with an alert msg “YOU ARE HACKED”. Thisindicates that the injected script has been executed successfully.


(82) WhatsApp
ycet kollam - Search
YCET Kollam: Admission 2024, Co
samyoga ycet - Search
samyoga (@samyoga.ycet) • Insta
ycet.ac.in/admissions/mtech.html
https://ycet.ac.in/admissions/mtech.html
YOUNUS COLLEGE
OF ENGINEERING AND TECHNOLOGY
info@ycet.ac.in 0474 2724305, 2723292
Approved by AICTE | Affiliated to APJ Abdul Kalam Technological University
An ISO 9001:2015 Certified Institution
AN ICT Academy Membership College
Accredited by NAAC
YCE
UPLOAD YOUR PHOTO
Choose File
No file chosen

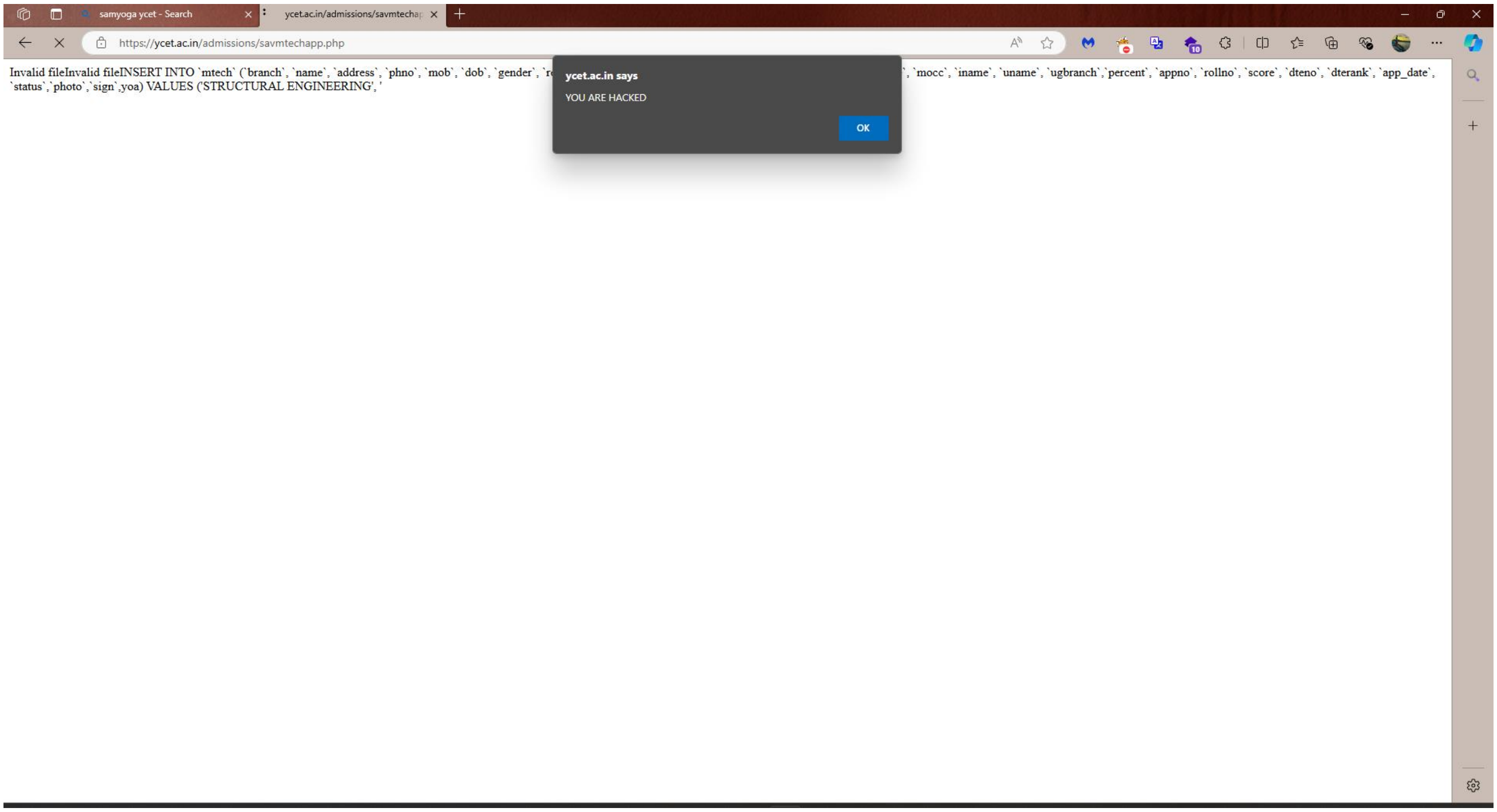
APPLICATION FOR ADMISSION TO M.TECH DEGREE COURSE

Specialization Applied For*: STRUCTURAL ENGINEERING

Name of the Applicant*: <script>alert("YOU ARE HACKED ")</script>

Residential Address*: <script>alert("YOU ARE HACKED")</script>

Phone No.	Mobile No. *	Date of Birth *	Gender
5454545+65+65	65+65+65+6	dd-mm-yyyy	Male
Religion	**Caste**	**Eligible for Reserveration?**	**If Yes, give Category**
Hindu	<script>alert("XSS")	YES	



samyoga ycet - Search
ycet.ac.in/admissions/savmtechap
https://ycet.ac.in/admissions/savmtechapp.php

```
Invalid fileInvalid fileINSERT INTO `mtech` (`branch`, `name`, `address`, `phno`, `mob`, `dob`, `gender`, `r         `, `mocc`, `iname`, `uname`, `ugbranch`,`percent`, `appno`, `rollno`, `score`, `dteno`, `dterank`, `app_date`,
`status`,`photo`,`sign`,yoa) VALUES ('STRUCTURAL ENGINEERING', '
```

ycet.ac.in says

YOU ARE HACKED

Impact

An attacker could steal credentials. An attacker could exfiltrate sensitive data. An attacker can steal cookies and Sessions. An attacker can quickly obtain access to your other client's computers.
In a DOM-based attack, the HTTP response on the server side does not change. Rather, a malicious change in the DOM environment causes client code to run unexpectedly.

References

- https://owasp.org/www-community/attacks/xss/
- https://portswigger.net/web-security/cross-site-scripting

VULNERABILITY #3

MEDIUM RISK (4.2/10)	
Name of Vulnerability	**Secure Flag Missing**
Security Impact	**Medium**

Vulnerable URL

https://www.odishaassembly.nic.in/

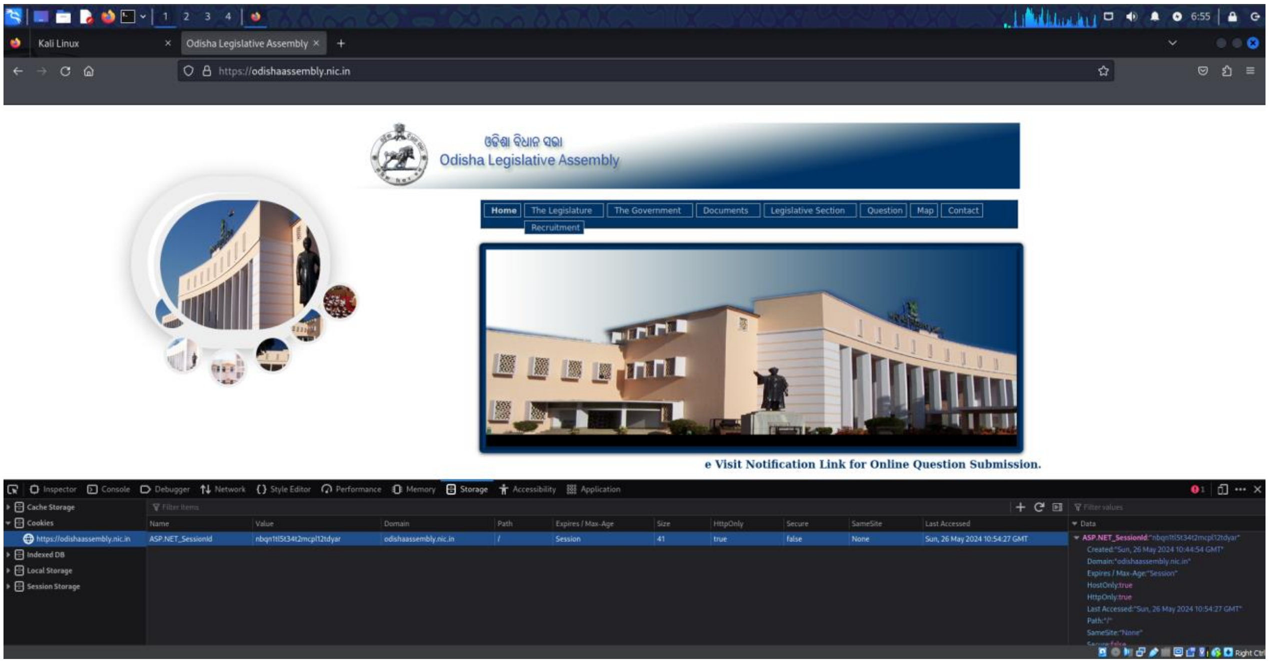
Security Implications

If the secure flag is set on a cookie, then browsers will not submit the cookie in any requests that use an unencrypted HTTP connection, thereby preventing the cookie from being trivially intercepted by an attacker monitoring network traffic. If the secure flag is not set, then the cookie will be transmitted in clear-text if the user visits any HTTP URLs within the cookie's scope. An attacker may be able to induce this event by feeding a user suitable links, either directly or via another web site. Even if the domain that issued the cookie does not host any content that is accessed over HTTP, an attacker may be able to use links of the form http:/ example.com:443/ to perform the same attack.

Steps to Reproduce

1. Go to the URL https://www.odishaassembly.nic.in/
2. In the webpage, right click and then inspecting the webpage, we can see there isan "ASP.NET_SessionId" cookie and the site consist of http only and secure flag is missing;

Screenshots



https://odishaassembly.nic.in

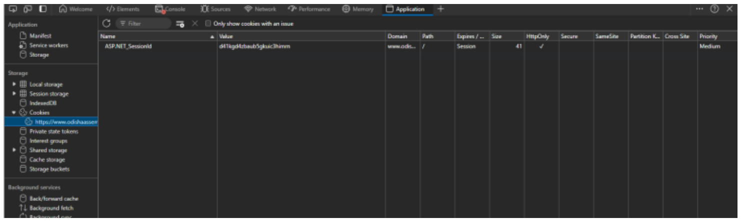
ଓଡ଼ିଶା ବିଧାନ ସଭା
Odisha Legislative Assembly

Home | The Legislature | The Government | Documents | Legislative Section | Question | Map | Contact | Recruitment

e Visit Notification Link for Online Question Submission.

Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite	Last Accessed
ASP.NET_SessionId	nbqn1tl5t34t2mcpl12tdyar	odishaassembly.nic.in	/	Session	41	true	false	None	Sun, 26 May 2024 10:54:27 GMT

```
ASP.NET_SessionId:"nbqn1tl5t34t2mcpl12tdyar"
  Created:"Sun, 26 May 2024 10:44:54 GMT"
  Domain:"odishaassembly.nic.in"
  Expires / Max-Age:"Session"
  HostOnly:true
  HttpOnly:true
  Last Accessed:"Sun, 26 May 2024 10:54:27 GMT"
  Path:"/"
  SameSite:"None"
  Secure:false
```



☐ Only show cookies with an issue

Name	Value	Domain	Path	Expires / ...	Size	HttpOnly	Secure	SameSite	Partition K...	Cross Site	Priority
ASP.NET_SessionId	d41kgd4zbaub5gkuic3himm	www.odis...	/	Session	41	✓					Medium

Impact

When a cookie does not have the Secure-flag set, it will be sent in every request over both HTTP and HTTPS. Even if the web application itself is sent over HTTPS an attacker could still steal the session in use by forcing the user to make an HTTP request and then stealing the session cookie there.

References

- https://portswigger.net/kb/issues/00500200_tls-cookie-without-secure-flag-set#:~:text=If%20the%20secure%20f lag%20is%20not%20set%2C%20then%20the%20cookie,or%20via%20another%20web%20site.
- https://support.detectify.com/support/solutions/articles/48001048982-cookie-lack-secure-flag#:~:text=When%20 a%20cookie%20does%20not,stealing%20the%20session%20cookie%20there.

VULNERABILITY #4

LOW RISK (3.1/10)	
Name of Vulnerability	**Clickjacking**
Security Impact	**Low**

Vulnerable URL

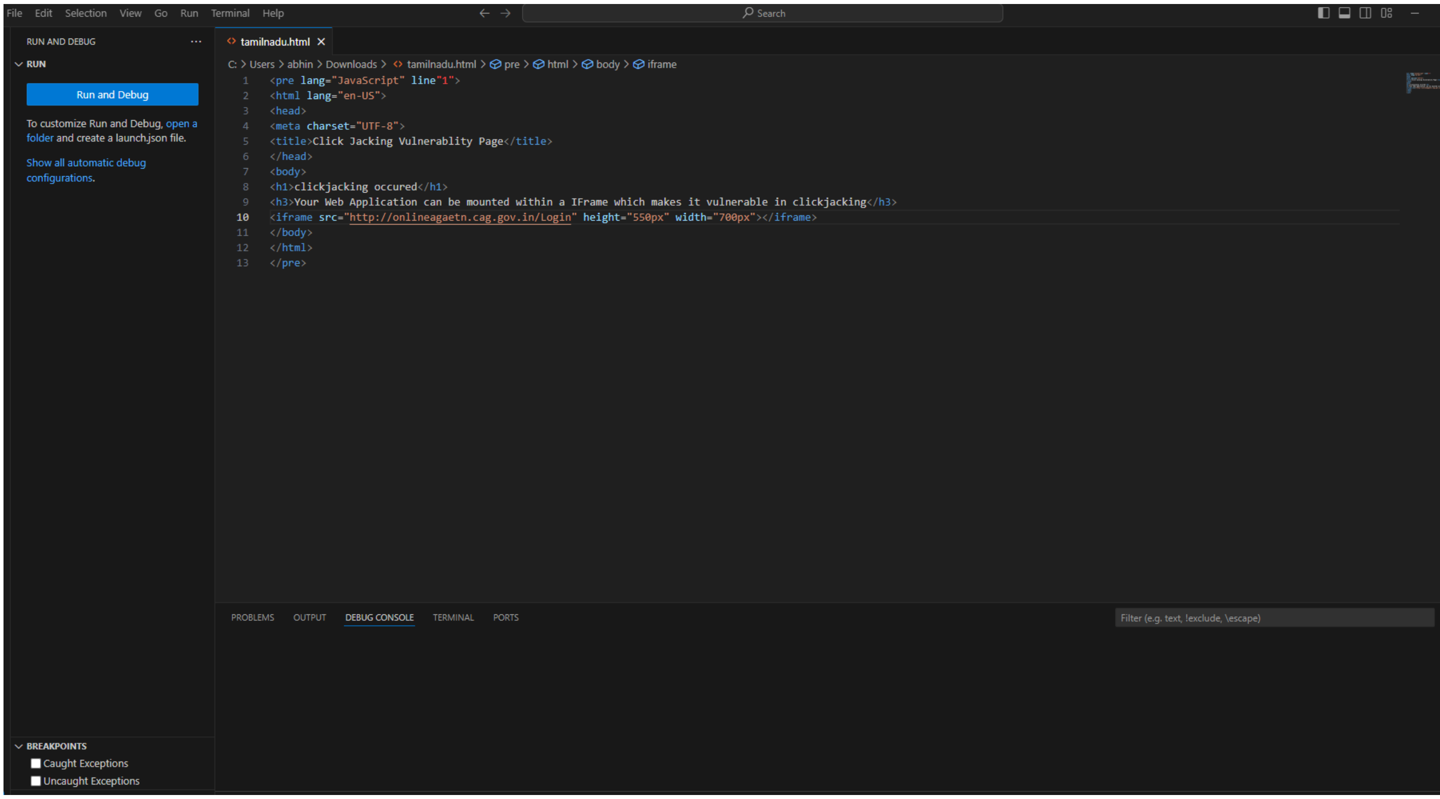
http://onlineagaetn.cag.gov.in/Login

Security Implications

Clickjacking, also known as a “UI redress attack”, is when an attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the top-level page. Thus, the attacker is “hijacking” clicks meant for their page and routing them to another page, most likely owned by another application, domain, or both.

Steps to Reproduce

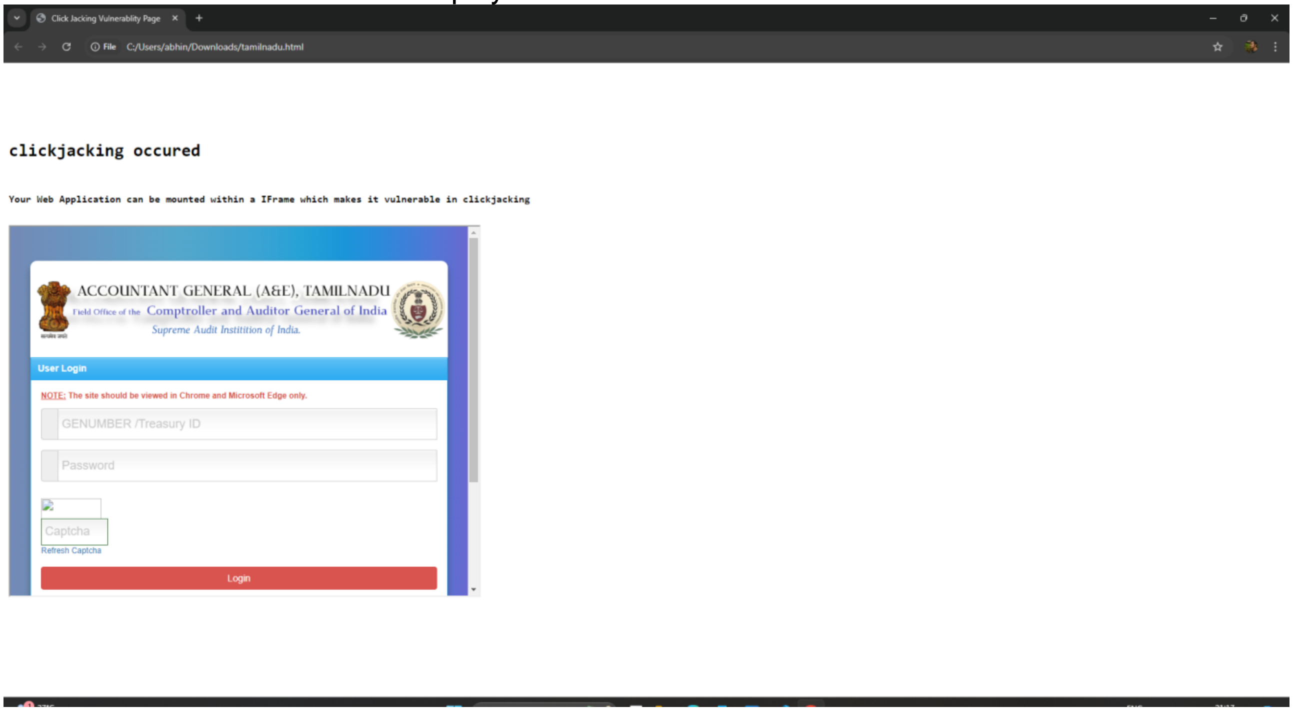
1. Get the URL of the site that needs to be tested for clickjacking vulnerability. Here it is : http://onlineagaetn.cag.gov.in/Login
2. Now paste the URL as the ‘src’ on the clickjacking html code as below:


File Edit Selection View Go Run Terminal Help
Search
RUN AND DEBUG
RUN
Run and Debug
Show all automatic debug configurations.
BREAKPOINTS
□ Caught Exceptions
□ Uncaught Exceptions
tamilnadu.html
C: > Users > abhin > Downloads > tamilnadu.html > pre > html > body > iframe
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS
Filter (e.g. text, !exclude, \escape)

To customize Run and Debug, open a folder and create a launch.json file.

```html
<pre lang="JavaScript" line"1">
<html lang="en-US">
<head>
<meta charset="UTF-8">
<title>Click Jacking Vulnerablity Page</title>
</head>
<body>
<h1>clickjacking occured</h1>
<h3>Your Web Application can be mounted within a IFrame which makes it vulnerable in clickjacking</h3>
<iframe src="http://onlineagaetn.cag.gov.in/Login" height="550px" width="700px"></iframe>
</body>
</html>
</pre>
```

3. Now open this html file and we can see that the resolution of the webpage is changed.
4. Thus, it is vulnerable to clickjacking
5. The result will display as:


Click Jacking Vulnerablity Page
File C:/Users/abhin/Downloads/tamilnadu.html
ACCOUNTANT GENERAL (A&E), TAMILNADU
Field Office of the Comptroller and Auditor General of India
Supreme Audit Institution of India
User Login
GENUMBER /Treasury ID
Password
Captcha
Refresh Captcha
Login

clickjacking occured

Your Web Application can be mounted within a IFrame which makes it vulnerable in clickjacking

NOTE: The site should be viewed in Chrome and Microsoft Edge only.

Impact

- Keystrokes can also be hijacked.
- With a carefully crafted combination of stylesheets, iframes, and text boxes, a user can be led to believe they are typing in the password to their email or bank account, but are instead typing into an invisible frame controlled by the attacker.

References

- https:/owasp.org/www-community/attacks/Clickjacking
- https:/ www.imperva.com/learn/application-security/clickjacking/

APPENDIX A - TOOLS USED

TOOL	DESCRIPTION
Burp Suite Professional	Used for Web Application Penetration Testing

TableA.1: Tools used during assessment

APPENDIX B - ENGAGEMENT INFORMATION

CONTACT INFORMATION

Name	ABHINAV S
Phone	+917306655228
Email	abhinavsajiv89@gmail.com

CONCLUSION

The primary goal is the identification of specific, documented vulnerabilities and their timely remediation. It's important to an organization with an Internet presence because attackers are able to take advantage of any loophole or flaw that may be present.

Vulnerability assessments also provide an organization with the necessary knowledge, awareness and risk backgrounds to understand and react to threats to its environment. A vulnerability assessment process is intended to identify threats and the risks they pose.