



A Real-World Breach Analysis + OWASP Mapping Report

JUNAID QUADRI

quadrijunaid369258@gmail.com



Contents

1. Executive Summary	3
2. Introduction.....	4
3. Incident Timeline.....	5
4. Technical Root Cause Analysis.....	6
5. OWASP Top 10 Mapping.....	7
6. CIA Triad Impact Mapping.....	8
7. Dark Web Intelligence Findings.....	9
8. Affected Stakeholders.....	10
9. Threat Modeling.....	11
10. Recommended Remediation & Mitigation Strategies.....	17
11. Secure Coding & Web Hardening Practices.....	19
12. Recommended Security Architecture.....	20
13. References and Appendices (Screenshots, Proof, Technical Artifacts)	21
14. Conclusion.....	26



Executive Summary

The Tendermines.com data breach serves as a crucial real-world example of how multiple overlooked web application vulnerabilities can come together to pose a serious risk to security, trust, and operational integrity. The technical and strategic aspects of the breach are examined in this report from the perspective of cybersecurity research, aligning the incident with globally recognized frameworks such as the OWASP Top 10 and the CIA Triad.



Introduction

In the current digital ecosystem, small and medium-sized businesses typically ignore cybersecurity best practices. An illustration of how this way of thinking can result in significant data exposure is the hack of the Indian web service tendermines.com. With an emphasis on technical and strategic analysis of real breaches, this report was produced in Week 3 of the SECT cybersecurity internship program.

Tools and Sources Used

- Passive reconnaissance: Google Dorks, IntelX.io, Sublist3r, BuiltWith, Wayback Machine
- Vulnerability testing: Burp Suite, Firefox Dev Tools, SecurityHeaders.io
- Open-source frameworks: OWASP Top 10, CIA Triad
- Reference reports: Week 1 (Reconnaissance), Week 2 (Vulnerability Report)

Purpose of the Report

- Simulate the role of a cybersecurity analyst investigating an actual breach.
- Identify the technical flaws that led to the event. Align the root causes to OWASP Top 10 categories.
- Evaluate the security implications using the CIA Triad.
- Make recommendations for mitigation techniques based on what is learned in Weeks 1 and 2.



Incident Timeline

Date	Event
2016-12-25	tendermines.com was registered
2023-11-01	tendermines.com.sql database first appeared on dark web
2022-07-07	Passive recon identifies admin/login page exposed via Google Dorks
2020-08-13	SSL Labs and Firefox inspection revealed that the domain did not have HTTPS.
2025-07-10	DNS misconfigurations found (no SPF, DKIM, DMARC)
2025-07-18	SECT Team performed vulnerability scan (Week 2 analysis)
2025-07-10	Reconnaissance report confirms high-risk exposure (Week 1)
2025-07-18	SQL Injection vulnerability confirmed during proof-of-concept testing
2025-07-10	Security headers and error disclosure were discovered through an analysis of HTTP responses.



Technical Root Cause Analysis

Issue	Description	Severity
SQL Injection	Raw SQL errors and schema information can be revealed by manipulating the login form.	Critical
No HTTPS/TLS	All traffic is insecure because the entire website is accessible via unencrypted HTTP.	High
Missing SPF/DKIM/DMARC	No DNS-based email authentication records configured, allowing email spoofing	High
Publicly Indexed Admin Pages	/login and /admin pages accessible and indexed by search engines	High
Verbose Error Message	SQL errors exposed the technology stack, database structures, and internal file paths.	High
Missing Security Headers	HTTP response headers lacking CSP, HSTS, Referrer-Policy, Permissions-Policy, etc.	Medium
Dark-Web Database Exposure	The full database dump (tendermines.com.sql) that was made public contained sensitive user data.	Critical
Unrestricted Directory Access	Email addresses and internal URLs like /uploads and /contact were searchable.	Medium



OWASP Top 10 Mapping

OWASP Category	Vulnerability Found	Description	Affected Component
A01:2021 Broken Access Control	SQL Injection on login endpoint	The login allowed bypassing of authentication through crafted SQL payloads	Admin Panel
A02:2021 Cryptographic Failures	Without a TLS certificate, the entire website is served over HTTP.	data is vulnerable to MiTM attacks when HTTPS is not used.	No HTTPS, exposed backups
A05:2021 Security Misconfiguration	No security headers, exposed pages, and missing SPF, DKIM, and DMARC	Unrestricted admin paths, incorrectly configured web server headers, and no DNS protection	No headers, index exposed
A03:2021 Injection	SQL Injection	Raw SQL queries without input sanitization led to full DB errors and possible data access	SQLi in login
A04:2021 Insecure Design	No CAPTCHA or rate-limiting on login/admin	Lack of protections indicates poor design planning and threat modeling	No CAPTCHA, no auth flow
A06:2021 Vulnerable and Outdated Components	Verbose SQL error shows WAMP stack	Targeted attacks are made easier by error messages that reveal filesystem paths and stack versions.	WAMP stack leak
A07:2021 Identification and Authentication Failures	Google indexes admin/login pages	Authentication interfaces lacked brute-force protection and were openly accessible.	Predictable login, brute-force
A09:2021 Security Logging and Monitoring Failures	Leaked SQL dump undetected, no alerts logged	No evidence of monitoring or incident response for the publicly leaked database	Breach unalerted



CIA Triad Impact Mapping

Confidentiality

Evidence of Compromise:

- As early as November 1, 2023, it was found that the SQL database dump (tendermines.com.sql) containing private user data was openly accessible on the dark web.
- The website lacked HTTPS/TLS, causing all form submissions (login, contact forms) to be transmitted in clear text.
- Internal phone numbers, email addresses, and possibly password hashes were exposed by the database and indexed webpages.

Integrity

Possible Impact:

- Although no direct data tampering was reported, the presence of a SQL injection vulnerability raises the possibility that attackers may have changed database records.
- Internal directory listings and verbose error outputs may have provided information for a more thorough access or configuration change.

Availability

No Evidence of Disruption:

- The website continued to function during the period of the breach.
- No signs of system outages, denial-of-service (DoS) attacks, or unavailability were discovered or reported by external sources during the engagement.

CIA Impact Overview

CIA Element	Status	Description
Confidentiality	Compromised	Sensitive user information and emails were made public by a SQL dump.
Integrity	Possibly Compromised	SQLi and lack of monitoring imply potential for data tampering
Availability	Not Impacted	Website remained online and functional; no DoS or ransomware detected



Dark Web Intelligence Findings

A publicly available file called `tendermines.com.sql` was found while conducting passive reconnaissance on IntelX.io, a dark web intelligence and OSINT search engine. Initially, the file was indexed on:

Date: 20:29:57 on November 1, 2023

It was verified that this file was a full SQL dump, and it probably contained private user data like usernames, email addresses, and possibly password hashes.

Breach Impact Based on Dump

The database that is exposed could include:

- Verified user names and email addresses
- Password hashes (SHA/MD5/Plaintext), perhaps
- Details regarding the backend database tables' structure
- Records of possible administrative users

Risk Situations:

- Stuffing credentials against accounts that have been used again
- Targeted phishing with legitimate user emails

Potential Root Causes of Exposure

The following are the most likely technical reasons, depending on the file's nature and timing:

- The SQL injection vulnerability was successfully exploited.
- An unprotected backup directory or an incorrectly configured public path
- Internal assets are not tokenized or encrypted.
- No incident response detection or monitoring



Affected Stakeholders

Internal Stakeholders

1. Employees and Administrative Staff

- The compromised database and indexed contact pages made a number of employee email addresses public.
- Emails that were made public:
pratimaenterprise19@gmail.com, rushilmbhatt@yahoo.com, sales@tendermines.com

2. Web Application Developers / IT Team

- The infrastructure and development teams neglected to use secure coding techniques (such as HTTPS and SQL injection mitigation).

External Stakeholders

1. Registered Users / Customers

- The leaked SQL dump might have contained user data, revealing emails, usernames, and potentially passwords. These users are now vulnerable to:
 - Credential stuffing
 - Phishing attacks
 - Identity theft.

2. Vendors / Business Partners

- Due to missing SPF/DKIM/DMARC records, any partners who interacted with emails from @tendermines.com may also be vulnerable to spoofing attempts.
- Partners might have doubts about the company's capacity to securely handle private communications.

Reputational Stakeholders

- The platform's lack of transparency and visible incident response may cause users and the public to lose faith in it.
- A detrimental effect on traffic and SEO (Google flags HTTP sites as "Not Secure")

Summary Table

Stakeholder Group	Risk Level	Primary Impact
Employees/Admins	High	Email exposure, phishing, impersonation risk
Registered Users	High	Data leakage, credential compromise, identity risk
Vendors/Partners	Medium	Email spoofing, brand risk
Company Executives	High	Reputational, financial, and legal consequences
Public/Customers	Medium	Trust erosion, customer churn



Threat Modelling

Assets at Risk

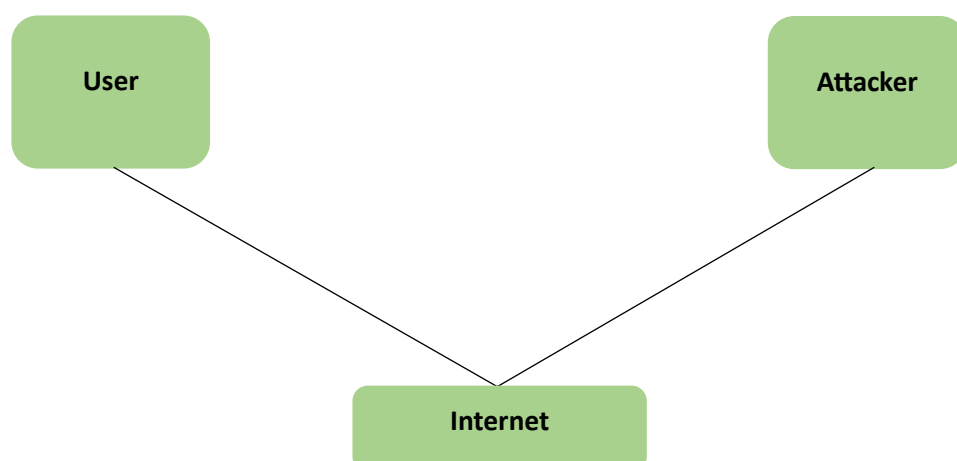
Asset	Description
User Credentials	kept in the SQL database on the backend
Admin Control Panel (/admin)	Sensitive backend operations
Email Infrastructure (@tendermines)	Public email identities used for business ops
Contact Forms and Input Fields	Points of entry for malicious payloads
Database (MySQL)	Core data store (leaked SQL dump)
File System or Error Logs	Verbose error outputs that reveal
Web Server(Apache or WAMP stack)	operates backend services and is fingerprinted publicly.

STRIDE based Threat Classification

STRIDE Threat	Example from Tendermines.com
S – Spoofing	Attackers can impersonate emails from @tendermines.com since there is no SPF, DKIM, or DMARC.
T – Tampering	SQLi vulnerability → Attackers could modify DB content
R – Repudiation	No logging/monitoring → Attackers' actions may go undetected or untraceable
I – Information Disclosure	SQL dump on dark web, verbose error messages with server file paths
D – Denial of Service	/admin endpoint exposed → Subject to brute-force or automated login attacks
E – Elevation of Privilege	SQL Injection on login → May allow attackers to gain admin or privileged access

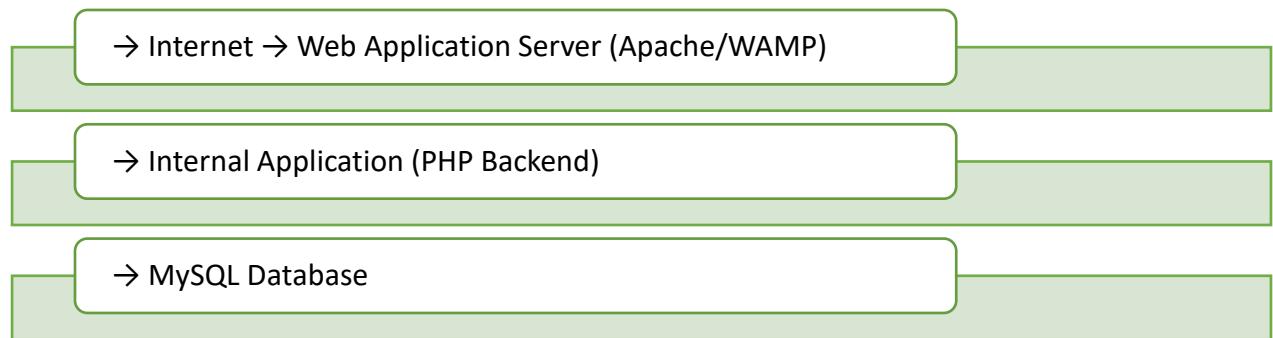
Threat Mapping Diagram

External Entities





Trust Boundaries



Processes

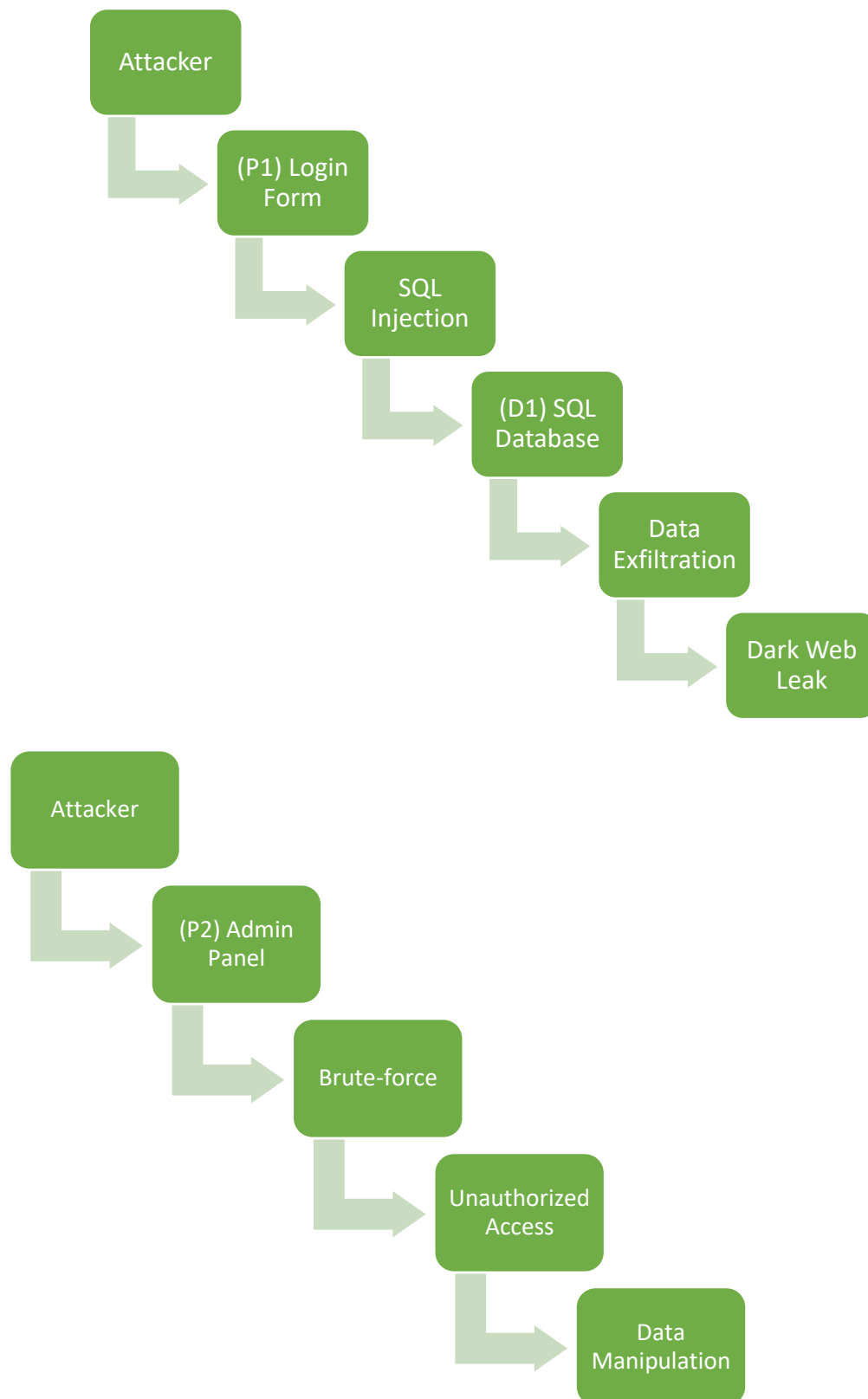
P1	Login Form	/login
P2	Admin Panel	/admin
P3	Contact Form	/contact
P4	Email System	@tendermines.com
P5	DNS Server	DNS & TXT Records
P6	Error Handler	Server stack traces

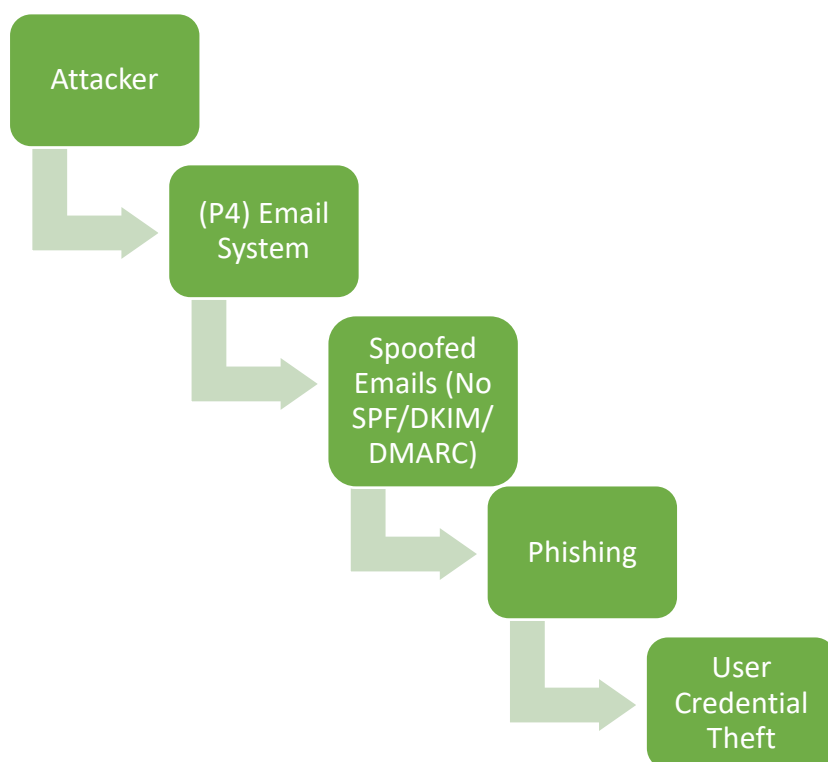
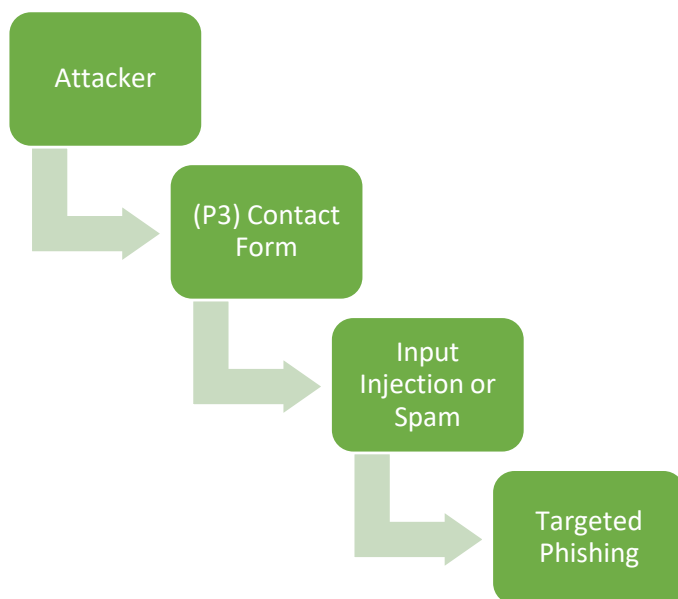
Data Stores

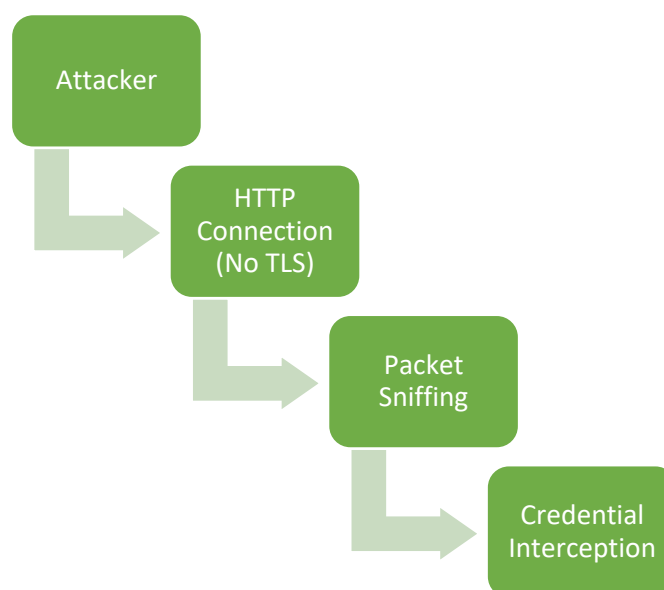
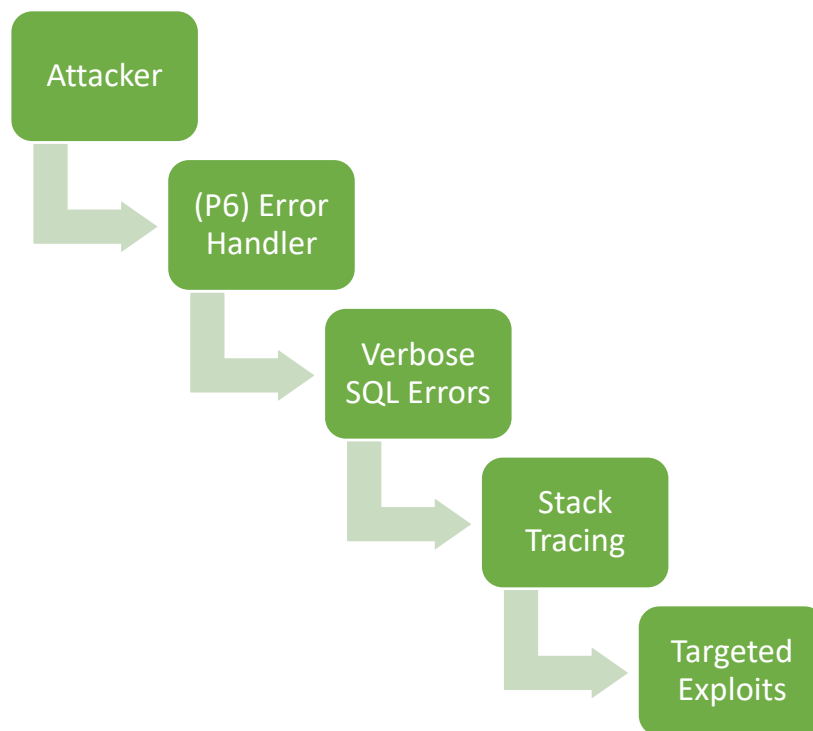
D1	SQL Database	User credentials, emails
D2	Web Server Logs	Verbose errors, IP logs
D3	Public Files	Indexable directories, .sql files

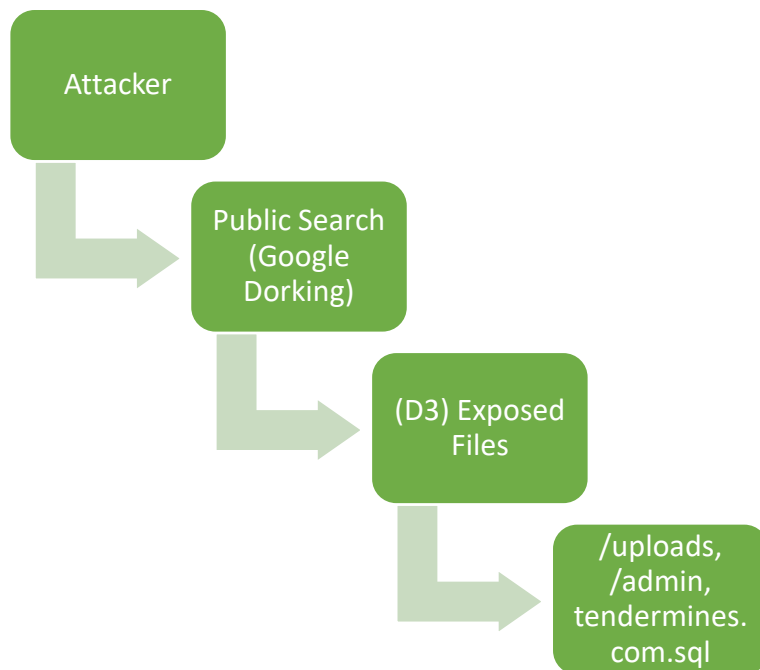


Threat Flows (Shows the possibilities of how the Data may had affected)

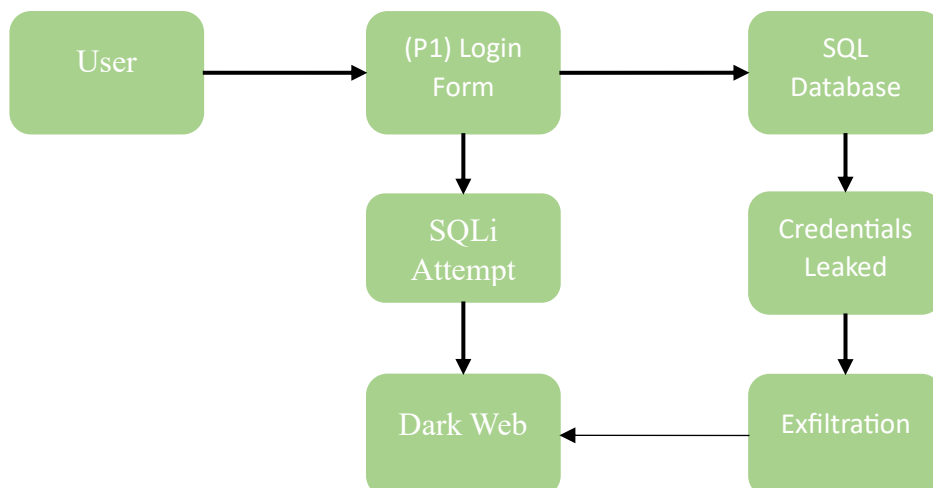








Visual Flow





Recommended Remediation & Mitigation Strategies

Category	Control Area	Recommended Action	Priority
Application Security	SQL Injection remedy	For all SQL operations, use prepared statements or parameterized queries.	Critical
Application Security	Input Validation	Use reliable validation libraries to implement server-side input sanitization.	Critical
Application Security	Authentication	Enforce 2FA, strong password policies, and CAPTCHA on login forms	Critical
Application Security	Admin Panel Access	Restrict /admin via IP whitelist, obfuscate path, and add multi-factor login	Critical
Application Security	Error Disclosure	Eliminate verbose errors, create personalized error pages, and log server-side information.	High
Internal Server and Transport	HTTPS / TLS Enforcement	Set up a working SSL certificate, change HTTP to HTTPS, and activate HSTS.	Critical
Internal Server and Transport	HTTP Security Headers	Include the following headers: Referrer-Policy, X-Frame-Options, X-Content-Type-Options, and CSP.	Medium
Network Defense	Web Application Firewall	Use WAF (such as ModSecurity or Cloudflare) to prevent OWASP, XSS, and SQLi attacks.	High
File or Backup Protection	Directory & Dump Access	Eliminate any.sql or.bak files, and use web configurations, robots.txt, and.htaccess to prevent listing.	Medium



DNS and Email Security	SPF Record	Publish SPF TXT: v=spf1 include:_spf.google.com ~all	High
DNS and Email Security	DKIM Sign	Add the public key to the DNS and enable DKIM on email servers.	High
DNS and Email Security	DMARC Policy	Add monitoring addresses (ruf) that have p=reject or p=quarantine.	High
Monitoring and Logging	Centralized Log Collection	Combine logs using a logging pipeline such as Graylog or ELK Stack.	Medium
Monitoring and Logging	SIEM Integration	To find irregularities and create alerts, use Wazuh, Splunk, or OSSIM.	Medium
Threat Intel	Dark Web Monitoring	Use HaveIBeenPwned, IntelX, and keyword monitors to detect data leaks	Medium
Policy	Incident Response Planning	Create and test an incident response plan that includes legal contacts, roles, and a clear flow.	Ongoing
Policy	Vulnerability Management	Conduct quarterly pen-testing and monthly Nessus/OpenVAS scans.	Ongoing
Policy	Secure SDLC	Incorporate DevSecOps, secure code reviews, and threat modeling into CI/CD.	Ongoing
Data Security	Retention & Encryption	Encrypt backups, reduce retention period, and limit access to sensitive fields	Medium
User Communication	Breach Notification	Notify affected users, enforce password reset, and advise on security best practices	Medium

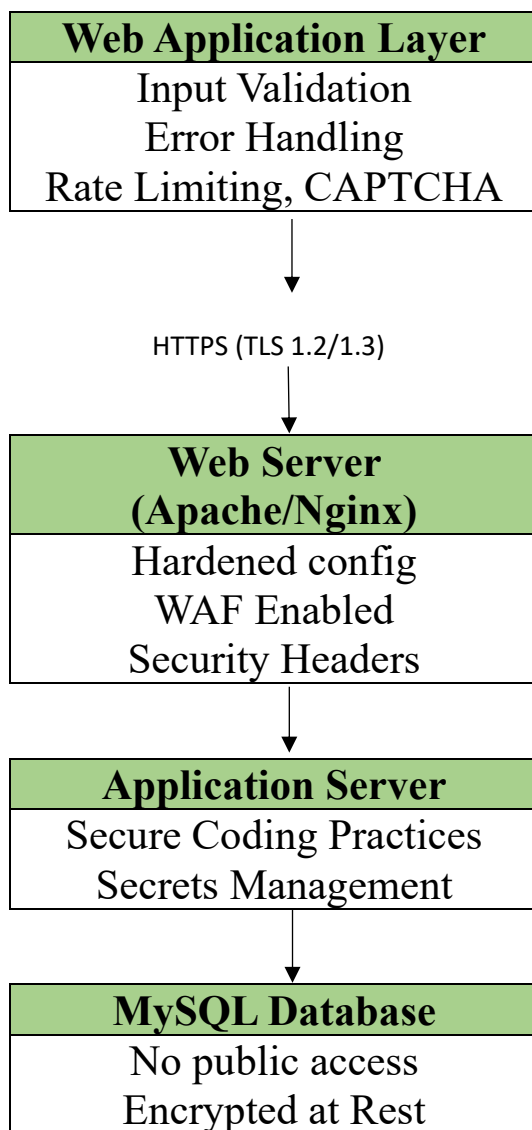


Secure Coding & Web Hardening Practices

Area	Fix
Input Validation	Validate all user inputs on the server side using a positive (allow-list) validation approach.
Output Encoding	Encode output for HTML, JavaScript, and SQL contexts
Authentication	Use secure password hashing algorithms. Enforce 2FA.
Session Management	Use secure session tokens. Enable HttpOnly, Secure, and SameSite flags.
Error Handling	Implement custom error pages.
Access Control	Implement RBAC (Role-Based Access Control).
Database Security	Avoid dynamic SQL queries at all costs.
File Uploads	Restrict file types and extensions. Use MIME type checking.
Apache/Nginx Settings	Disable directory listing and server signature.
Security Headers	Add headers like Content-Security-Policy, Strict-Transport-Security, X-Frame-Options, etc.
HTTPS Enforcement	Redirect all traffic to HTTPS.
File Permissions	Use least privilege on files.
Hidden Admin Panels	Move /admin to non-standard paths, and restrict access.
Logs	Keep logs off-site or in a secure location with restricted access.
Backup Security	Do not store .sql or .bak files in public web roots.



Recommended Security Architecture





References and Appendices (Screenshots, Proof, Technical Artifacts)

[IntelX.io](#) – Confirmation of breach artifacts and dark web intelligence

[OWASP Top 10 - 2021](#) – Vulnerability mapping

[MXToolbox](#) – DNS and SPF/DKIM/DMARC lookup

[SecurityHeaders.com](#) – HTTP response header analysis

[Shodan.io](#) – Verification of HTTP responses and service exposure

My own reports: Week 1 (Reconnaissance), Week 2 (Vulnerability Assessment)

Logs and PoC testing results (from tools like Nikto, curl, SQLmap, etc.)

IntelX search result showing tendermines.com.sql leak

[← Back to results](#) [↗](#)

tendermines.com.sql [Part 3 of 9]
2023-11-01 20:29:57

Upgrade your License to view redacted documents. The "Leaks" category is only available to paid users.

Document Metadata Selectors Actions

Title	tendermines.com.sql [Part 3 of 9]
Date	2023-11-01 20:29:57
Media	Database File
Category	Leaks » Restricted » General

[Show Expert Information](#)

Data is provided by our cache and subject to our policies.

SQLi PoC result (screenshot of payload response + DB error)

A Database Error Occurred

Error Number: 1054

Unknown column 'mentorname' in 'field list'

SELECT 'user_id', 'user_name', 'password', 'role_id', 'first_name', 'mentorname', 'ismentor' FROM 'user_master' WHERE 'user_name' = '' OR '1'='1 --' AND 'isActive' = 1

Filename: C:/WAMP/Apache24/htdocs/tendermines/system/database/DB_driver.php


Line Number: 691



HTTP response showing missing headers

```
PS C:\> curl -I http://tendermines.com
HTTP/1.1 200 OK
Date: Thu, 24 Jul 2025 17:12:35 GMT
Server: Apache
x-frame-options: SAMEORIGIN
Set-Cookie: ci_session=8aanrp58c7tc4o6ue20suda3cr8chog3; expires=Thu, 24-Jul-2025 19:12:35 GMT; Max-Age=7200; path=/; HttpOnly
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Content-Type: text/html; charset=UTF-8
```

DNS scan showing absence of SPF, DKIM, and DMARC records

 **MX TOOLBOX**
SUPERTOOL

PricingToolsDelivery CenterMonitor

SuperToolMX LookupBlacklistsDMARCDiagnosticsEmail HealthDNS LookupAnalyze Headers

SuperTool Beta9

tendermines.comDMARC Lookup


dmARC:tendermines.comFind ProblemsSolve Email Delivery ProblemsdmARC

Microsoft Outlook.com now requires DMARC - Get SPF, DKIM and DMARC setup and maintain compliance with Delivery Center

v=DMARC1; p=none; pct=100; rua=mailto:re+azpschemvlgv@dmARC.postmarkapp.com,mailto:dmARC@manishnaik.services; ruf=mailto:dmARC@manishnaik.services; sp=none; aspf=r;

Tag	TagValue	Name	Description
v	DMARC1	Version	Identifies the record retrieved as a DMARC record. It must be the first tag in the list.
p	none	Policy	Policy to apply to email that fails the DMARC test. Valid values can be 'none', 'quarantine', or 'reject'.
pct	100	Percentage	Percentage of messages from the Domain Owner's mail stream to which the DMARC policy is to be applied. Valid value is an integer between 0 to 100.
rua	mailto:re+azpschemvlgv@dmARC.postmarkapp.com,mailto:dmARC@manishnaik.serv ices	Receivers	Addresses to which aggregate feedback is to be sent. Comma separated plain-text list of DMARC URIs.
ruf	mailto:dmARC@manishnaik.services	Forensic Receivers	Addresses to which message-specific failure information is to be reported. Comma separated plain-text list of DMARC URIs.
sp	none	Sub-domain Policy	Requested Mail Receiver policy for all subdomains. Valid values can be 'none', 'quarantine', or 'reject'.
aspf	r	Alignment Mode SPF	Indicates whether strict or relaxed SPF Identifier Alignment mode is required by the Domain Owner. Valid values can be 'r' (relaxed) or 's' (strict mode).

Test	Result
✖ DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled More Info
⚠ DMARC External Validation	External Domains in your DMARC are not giving permission for your reports to be sent to them. More Info
✔ DMARC Record Published	DMARC Record found
✔ DMARC Syntax Check	The record is valid

 **MX TOOLBOX**
SUPERTOOL

PricingToolsDelivery CenterMonitor

SuperToolMX LookupBlacklistsDMARCDiagnosticsEmail HealthDNS LookupAnalyze Headers

SuperTool Beta9

tendermines.com.dnsDKIM Lookup

dkim:tendermines.com:dnsFind Problemsdkim

Test	Result
✖ DKIM Record Published	No DKIM Record found More Info
✖ DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled More Info
✔ DMARC Record Published	DMARC Record found

Your DNS hosting provider is "CloudDNS" [Need Bulk Dns Provider Data?](#)

dns lookupdns checkmx lookupdmARC lookupdns propagation

Reported by dns2.cloudns.net on 7/24/2025 at 12:03:34 PM (UTC -5) [Just for you](#) [Transcript](#)



MX

TOOLBOX

SUPER TOOL

Pricing

Tools

Delivery Center

Monitor

SuperTool

MX Lookup

Blacklists

DMARC

Diagnostics

Email Health

DNS Lookup

Analyze Headers

SuperTool Beta

spf.tendermines.com

SPF Record Lookup

Find Problems

Error

v=spf1 mx ip4:13.235.235.28 include:marshalkk.services ~all

Prefix	Type	Value	PrefixDesc	Description
	v	spf1		The SPF record version
+	mx		Pass	Match if IP is one of the MX hosts for given domain name.
+	ip4	13.235.195.20	Pass	Match if IP is in the given range.
+	include	marshalkk.services	Pass	The specified domain is searched for an 'allow'.
~	all		SoftFail	Always matches. It goes at the end of your record.

Test	Result	
<div>✖</div> SPF Record Null Value	A null DNS lookup was found for include (marshalkk.services)	<div>More Info</div>
<div>✖</div> DMARC Policy Not Enabled	DMARC Quarantine/Reject policy not enabled	<div>More Info</div>
<div>✔</div> SPF Record Published	SPF Record found	
<div>✔</div> SPF Record Deprecated	No deprecated records found	
<div>✔</div> SPF Multiple Records	Less than two records found	
<div>✔</div> SPF Contains characters after ALL	No items after 'ALL'.	
<div>✔</div> SPF Syntax Check	The record is valid	
<div>✔</div> SPF Included Lookups	Number of included lookups is OK	
<div>✔</div> SPF Recursive Loop	No Recursive Loops on Includes	
<div>✔</div> SPF Duplicate Include	No Duplicate Includes Found	
<div>✔</div> SPF Type PTR Check	No type PTR found	
<div>✔</div> SPF Void Lookups	Number of void lookups is OK	
<div>✔</div> SPF MX Resource Records	Number of MX Resource Records is OK	
<div>✔</div> DMARC Record Published	DMARC Record found	

Exposed /admin panel in browser

Not secure tendermines.com/login

TenderMines

Sign In

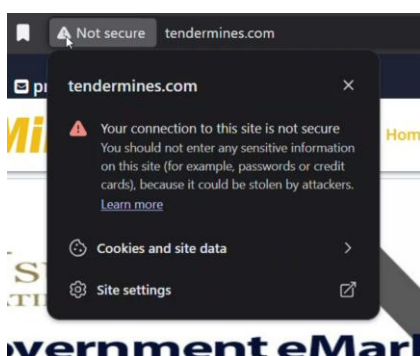
Email

Password

Sign In


Forgot Password

Lack of HTTPS (HTTP padlock warning in browser)





SecurityHeaders.com scan result



Site:

<http://tendermines.com/> - [\(Scan again over https\)](#)

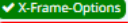
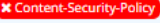
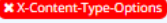
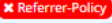
IP Address:

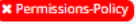
122.176.221.13

Report Time:

24 Jul 2025 16:55:49 UTC

Headers:



Warning:

Grade capped at A, please see warnings below.

Advanced:

Your site could be at risk, let's perform a deeper security analysis of your site and APIs:

Start Now

Missing Headers

Content-Security-Policy

[Content Security Policy](#) is an effective measure to protect your site from XSS attacks. By whitelisting sources of approved content, you can prevent the browser from loading malicious assets.

X-Content-Type-Options

[X-Content-Type-Options](#) stops a browser from trying to MIME-sniff the content type and forces it to stick with the declared content-type. The only valid value for this header is "X-Content-Type-Options: nosniff".

Referrer-Policy

[Referrer Policy](#) is a new header that allows a site to control how much information the browser includes with navigations away from a document and should be set by all sites.

Permissions-Policy

[Permissions Policy](#) is a new header that allows a site to control which features and APIs can be used in the browser.

Warnings

Site is using HTTP

This site was served over HTTP and did not redirect to HTTPS.

Raw Headers

HTTP/1.1

200 OK

Date

Thu, 24 Jul 2025 16:56:37 GMT

Server

Apache

x-frame-options

SAMEORIGIN

Set-Cookie

ci_session=g42hev061nej8gav9717bih9tk7ofak2; expires=Thu, 24-Jul-2025 18:56:38 GMT; Max-Age=7200; path=/; HttpOnly

Expires

Thu, 19 Nov 1981 08:52:00 GMT

Cache-Control

no-store, no-cache, must-revalidate

Pragma

no-cache

Transfer-Encoding

chunked

Content-Type

text/html; charset=UTF-8



Shodan search of IP with server headers or open ports

The image shows a Shodan search result for the IP address 122.176.221.13. The interface includes a map of Ahmedabad, India, and a table of general information. The general information table lists the following details:

General Information	
Hostnames	abts-north-dynamic-013.221.176.122.airtelbroadband.in
Domains	airtelbroadband.in
Country	India
City	Ahmedabad
Organization	BHARTI TELENET LTD. NEW DELHI
ISP	Bharti Airtel Ltd., Telemedia Services
ASN	AS24560
Operating System	Windows Server 2012 R2

On the right side, there is a section for Open Ports showing 3389 / TCP. Below this, the Remote Desktop Protocol (RDP) configuration is displayed, including the Remote Desktop Protocol version, the Remote Desktop Protocol MTU, the OS build (6.3.9600), the target name (TMW2), the NetBIOS domain name (TMW2), the NetBIOS computer name (TMW2), the DNS domain name (TMW2), the FQDN (TMW2), and the administrator name (am Windows Server 2012R2).

The image shows a Windows Server 2012 R2 login screen. The background is dark blue. At the top, the text "Administrator" and "am Windows Server 2012R2" is displayed. Below this, there are three user icons with the following names and status:

- Administrator: Signed in
- apache
- parth

At the bottom, the Windows logo and "Windows Server 2012 R2" are visible.



Conclusion

The analysis of the Tendermines.com breach revealed critical vulnerabilities including SQL injection, misconfigured security headers, and lack of email protection, which led to unauthorized data exposure. Through systematic assessment and remediation planning, we outlined technical root causes, mapped OWASP and CIA impacts, and proposed practical defense strategies. Implementing these controls is essential to restore security, ensure compliance, and prevent future incidents.