ShopTex

Owner: João Veiga
Reviewer: Rui Barbosa
Contributors: 1211106@isep.ipp.pt, 1211017@isep.ipp.pt
Date Generated: Tue May 20 2025

Executive Summary

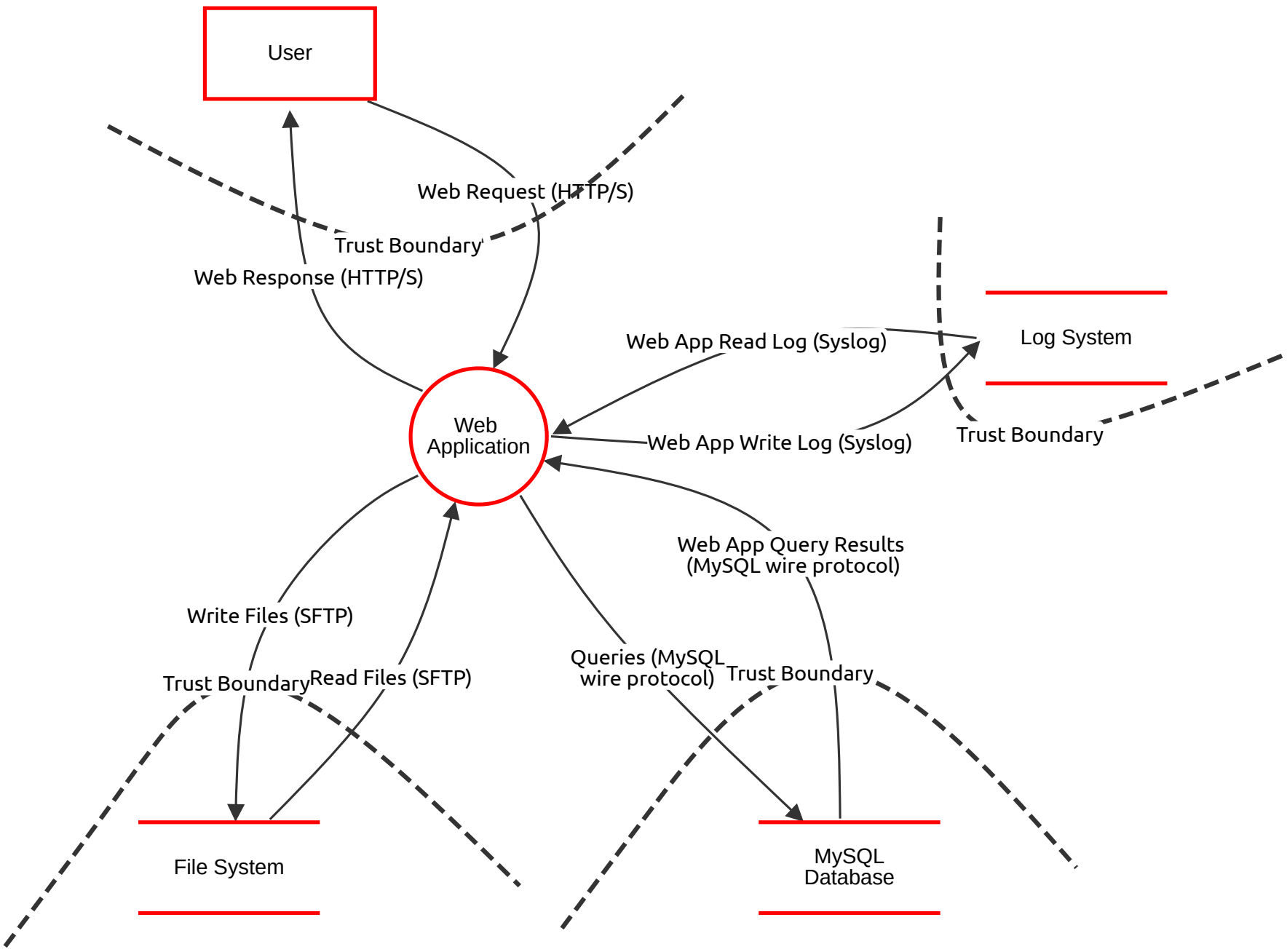
High level system description

Not provided

Summary

Total Threats	75
Total Mitigated	0
Not Mitigated	75
Open / High Priority	35
Open / Medium Priority	34
Open / Low Priority	6
Open / Unknown Priority	0

Threat Model



Threat Model

Web Response (HTTP/S) (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web Request (HTTP/S) (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Queries (MySQL wire protocol) (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web App Query Results (MySQL wire protocol) (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Read Files (SFTP) (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web App Write Log (Syslog) (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web App Read Log (Syslog) (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Write Files (SFTP) (Data Flow)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations

Web Application (Process)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
17	Code Injection	Tampering	High	Open	4	Attackers inject malicious code into input fields or URLs	Input validation / escaping; WAF; SAST/DAST
18	Remote Code Execution (RCE)	Elevation of privilege	High	Open	5	Exploiting vulnerabilities that let attackers run arbitrary code on your server.	Rapid patching; container isolation; SAST
19	DDoS	Denial of service	High	Open	4	Botnets exhaust bandwidth/resources.	CDN/Anycast; auto-scaling; rate-limiting
20	DoS	Denial of service	High	Open	3	Single-source resource exhaustion (e.g., slow-loris).	Short timeouts; connection limits
21	Broken Authentication	Spoofing	Medium	Open	4	Poor session management or credential flaws.	MFA; strong hashing (bcrypt); token rotation
22	Directory Traversal	Information disclosure	High	Open	3	Using ../ in URLs to access restricted files.	Path normalization; whitelists; chroot/jail
23	Server-Side Request Forgery (SSRF)	Information disclosure	Medium	Open	4	Exploiting a web server's ability to make HTTP requests on behalf of the attacker.	Destination allow-list; block metadata IPs; WAF
24	Cross-Site Scripting (XSS)	Tampering	High	Open	4	Injecting malicious scripts into web pages served to users.	Output encoding; CSP; input sanitization
25	Misconfigured Security Headers	Information disclosure	High	Open	2	Missing or misconfigured HTTP response headers.	Set headers like Content-Security-Policy, X-Frame-Options, X-XSS-Protection.
26	Information Leakage	Information disclosure	Low	Open	3	Server discloses sensitive info (e.g., stack traces, headers, debug messages).	Disable debug in prod; sanitize error output
27	Open Redirects	Spoofing	Medium	Open	3	Web server accepts unvalidated redirects.	Allow-list destinations; state tokens
28	Cross-Site Request Forgery (CSRF)	Tampering	Medium	Open	3	Trick users into submitting unwanted requests to your server while they’re logged in.	CSRF tokens; SameSite cookies; origin check
29	Broken Access Control / IDOR	Elevation of privilege	High	Open	5	Endpoints allow unauthorized access or modification of resources (Insecure Direct Object Reference).	Enforce server-side authorization checks; least-privilege APIs; rigorous test cases
30	Insecure Deserialization	Elevation of privilege	High	Open	4	Untrusted data is deserialized leading to RCE, data tampering or DOS.	Avoid native serialization of untrusted data; integrity signatures; deserialization firewalls
31	XML External Entity (XXE)	Information disclosure	High	Open	4	XML parsers process external entities allowing file read, SSRF or DOS.	Disable DTDs/external entities; switch to safe parsers; WAF regex filters
32	Server-Side Template Injection (SSTI)	Elevation of privilege	High	Open	4	User input injected into template engine expressions leading to code execution.	Strict template delimiters; sandbox templates; input validation
33	Mass Assignment	Tampering	Medium	Open	3	Automatic binding of HTTP parameters to object fields lets attacker overwrite sensitive properties.	Allow list bindable fields; DTOs; security-focused frameworks

Number	Title	Type	Priority	Status	Score	Description	Mitigations
34	Business Logic Abuse	Tampering	High	Open	4	Legitimate features mis-used in unexpected order/volume to subvert business rules.	Threat modeling; usage rate-limits; server-side invariant checks
35	Insecure Randomness	Spoofing	Medium	Open	3	Predictable tokens, IDs or OTPs allow guessing and takeover.	Use cryptographically secure PRNGs; sufficient entropy; periodic rotation
36	HTTP Request Smuggling (Back-end)	Tampering	Medium	Open	3	Front/back proxy parsing mismatch enabling cache poisoning or credential bypass.	Consistent parser versions; disable conflicting encodings; detailed logging

File System (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
56	Web Shell Uploads	Tampering	Medium	Open	4	Attackers upload malicious files (like PHP, JSP, or Python scripts) that give remote shell access via the browser.	- Strict file validation (type, size, extension). - Block script execution in upload directories via .htaccess, Nginx rules, etc"
57	Directory Traversal	Information disclosure	High	Open	3	Attackers manipulate paths like ../../etc/passwd to access sensitive files.	"- Normalize paths, whitelist directories, never rely on user input for file paths. - Disable directory listings in web server config."
58	Unauthorized File Downloads	Information disclosure	Medium	Open	3	Improper access controls allow direct file downloads (e.g., logs, configs, private PDFs).	- Enforce access controls on all files. - Move sensitive files outside the web root."
59	Insecure Permissions	Tampering	Medium	Open	3	Files or folders have overly permissive access (chmod 777, or owner is www-data for everything).	- Use chown, chmod, and group ownership properly. - Enforce least privilege for web server users"
60	Symbolic Link Abuse	Tampering	Medium	Open	3	Malicious symlinks point from a web-accessible folder to sensitive areas (like /etc/ or /home/).	- Scan for unexpected symlinks. - Use chroot or container isolation."
61	Exposed Backup Files	Information disclosure	Medium	Open	3	Developers leave .bak, .zip, .tar, .sql, or .old files in the web root.	- Never store backup or development artifacts in web-accessible folders. - Automate cleanup with scripts or CI/CD checks."
62	Tampered Static Assets	Tampering	Medium	Open	3	JavaScript, CSS, or images modified to inject malware or tracking (supply chain attacks).	- Use Subresource Integrity (SRI). - Monitor file hashes for changes (integrity scanning)."
63	Log Injection / Poisoning	Tampering	Medium	Open	2	Attacker injects malicious data into logs (e.g., via headers, user agents).	- Sanitize all user-controlled log inputs. - Store logs in write-only or append-only formats."
64	Insecure File Inclusion (LFI/RFI)	Repudiation	Low	Open	4	Web apps dynamically include files using user input (e.g., include($_GET['page'])).	Sanitize/validate all paths before inclusion.
65	Sensitive Config Files in Web Root	Information disclosure	High	Open	4	Files like .env, config.php, wp-config.php, or .htaccess are exposed.	- Move configs outside web root. - Deny access via web server rules (e.g., location ~ /\.(env|htaccess)$ in Nginx)."
66	Ransomware Encryption	Denial of service	High	Open	5	Malware encrypts application data and demands ransom.	Offline backups; SELinux/AppArmor; real-time AV; incident playbooks
67	World-Readable Temp Files	Information disclosure	Medium	Open	3	Temporary files created with insecure permissions leak sensitive data.	umask hardening; secure tmp dirs; periodic scans
68	Hard Link Abuse	Tampering	Medium	Open	3	Attackers create hard links to sensitive files to bypass ACL changes.	fs.protected_hardlinks; disallow links in upload dirs; integrity scans
69	Residual Data in Deleted Files	Information disclosure	Low	Open	2	Deleted files remain recoverable on disk snapshots or backups.	Secure wipe; encrypted filesystems; snapshot lifecycle management
70	Credential Leakage via OS Crash Dumps	Information disclosure	Medium	Open	3	Core dumps containing secrets stored in accessible locations.	Disable core dumps or restrict path; scrub sensitive data; limit ulimit -c

Number	Title	Type	Priority	Status	Score	Description	Mitigations
71	Insecure File Metadata Exposure	Information disclosure	Low	Open	2	File metadata (EXIF, document properties) leaks sensitive info to users.	Strip metadata on upload; content scanning; user education
72	Mounting External Volumes Insecurely	Tampering	High	Open	3	External drives or mounted folders are readable/writable by the web server without proper security.	- Mount with noexec, nosuid, nodev where applicable. - Use access control lists (ACLs) to restrict users."

MySQL Database (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
37	SQL Injection (SQLi)	Tampering	Medium	Open	5	Unsanitized input is used to inject malicious SQL queries.	Prepared statements; ORM; WAF
38	File Upload Vulnerabilities	Tampering	High	Open	4	Web apps allow file uploads but fail to properly validate the files.	Strict MIME/extension checks; disable execution
39	Weak or Default Credentials	Tampering	High	Open	4	Using usernames like root with weak passwords (or none at all).	Enforce strong passwords, disable remote root login, and use least privilege.
40	Exposed MySQL Port (3306)	Information disclosure	High	Open	3	MySQL server is publicly accessible.	"- Bind MySQL to localhost (or use a private network). - Use a firewall to restrict access to trusted IPs."
41	Privilege Escalation	Repudiation	Medium	Open	4	Overprivileged accounts can modify or execute harmful queries.	Apply principle of least privilege for all accounts.
42	Data Exfiltration via SELECT / INTO OUTFILE	Information disclosure	High	Open	4	If attackers gain access, they can dump data to a file and retrieve it.	Disable INTO OUTFILE and restrict write permissions to MySQL user.
43	Unencrypted Connections (No TLS)	Information disclosure	High	Open	3	Data, including credentials, flows in cleartext over the network.	Enable SSL/TLS for MySQL connections.
44	Local File Inclusion via LOAD DATA INFILE	Information disclosure	Medium	Open	4	If not disabled, attackers can use this command to read sensitive files.	Disable LOAD DATA LOCAL INFILE unless absolutely required.
45	Unpatched Vulnerabilities	Tampering	High	Open	4	Running outdated versions of MySQL can expose you to known exploits.	Regularly patch and monitor security advisories.
46	Information Disclosure via Errors	Information disclosure	High	Open	3	MySQL error messages reveal schema names, structure, or even partial queries.	Sanitize errors before sending them to clients; disable verbose errors in production.
47	Backup Theft or Exposure	Information disclosure	Medium	Open	4	Backups stored insecurely (e.g., in /tmp, public S3 buckets).	Encrypt and store backups securely, and restrict access.
48	Denial of Service via Heavy Queries	Denial of service	High	Open	3	Resource-intensive queries lock tables or spike CPU/IO.	Rate-limit users, enforce query timeouts, and monitor for unusual activity.
49	Brute Force Attack on User Accounts	Repudiation	Medium	Open	3	Attackers try lots of passwords on known users (root, admin, etc.).	Use fail2ban or other login attempt monitoring tools.
50	Unsafe Stored Procedures / Functions	Repudiation	High	Open	4	Procedures created with SQL SECURITY DEFINER run with elevated privileges and can be abused.	Review DEFINER privileges; limit CREATE ROUTINE; code review
51	Binary Log Poisoning	Tampering	High	Open	4	Malicious statements inserted into replication binlogs compromise replicas.	Encrypt/validate binlogs; restricted REPLICATE privilege; checksum enforcement
52	Federated Table Abuse	Information disclosure	Medium	Open	3	FEDERATED engine queries remote servers, allowing SSRF or data leak if misconfigured.	Disable FEDERATED unless needed; validate hostnames; network ACLs
53	Malicious Triggers for Persistence	Tampering	Medium	Open	3	Triggers added to run malicious code or leak data whenever rows change.	Audit triggers; least-privilege on TRIGGER; metadata integrity checks
54	Unencrypted Data at Rest	Information disclosure	High	Open	4	Data files and backups stored unencrypted, exposing data if disk stolen.	TDE (InnoDB encryption); disk/LUKS encryption; secure backup keys

Number	Title	Type	Priority	Status	Score	Description	Mitigations
55	General Query Log Exposure	Information disclosure	Medium	Open	3	General query log left enabled and world-readable, leaking credentials and queries.	Disable in production; secure file permissions; rotate logs

User (Actor)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
8	Eavesdropping	Spoofing	High	Open	4	Attacker captures clear-text traffic between client and server.	Enforce HTTPS (HSTS) • TLS 1.2+ • Disable plain HTTP
9	Replay Attack	Repudiation	High	Open	3	Re-sending captured legitimate requests (e.g., payments).	Nonces/time-stamps Unique session tokens TLS
10	SSL/TLS stripping or downgrade attack	Spoofing	Medium	Open	4	The attacker downgrades an HTTPS connection to HTTP, allowing them to read the unencrypted data being exchanged.	Redirect HTTP access attempts to HTTPS, among others
11	Weak Encryption Standard	Repudiation	High	Open	3	Using weak or deprecated encryption standards such as SSL	Disable weak suites; TLS 1.2/1.3-only; modern ciphers
12	Transparent Proxy Interception	Spoofing	Medium	Open	3	he attacker sits between the user and server (e.g., via a rogue router or compromised ISP), acting as a silent proxy.	Certificate pinning; DNSSEC / DoH; TLS
13	Session Hijacking (Cookie Theft / Sidejacking)	Spoofing	High	Open	4	Compromising session cookies via network sniffing or injection to impersonate a user.	Secure & HttpOnly cookies; SameSite; TLS; re-authentication; token rotation
14	DNS Spoofing / Cache Poisoning	Repudiation	High	Open	4	Attacker poisons DNS responses to redirect user traffic to a malicious host.	DNSSEC; DoH/DoT; short TTLs; monitor for DNS anomalies
15	HTTP Request Smuggling	Repudiation	Medium	Open	3	Abusing inconsistencies between front-end and back-end HTTP parsing to smuggle requests.	Align proxy/server parsing; disable legacy transfer encodings; WAF rules
16	TLS Interception (with Forged Certificates)	Spoofing	Medium	Open	4	Attacker presents a forged TLS certificate to the client while communicating with the server using the real certificate.	Certificate pinning; trusted public CAs; OCSP stapling

Log System (Store)

Description:

Number	Title	Type	Priority	Status	Score	Description	Mitigations
73	Log Injection / Forgery	Tampering	Medium	Open	3	Attacker crafts inputs (headers, user-agents, etc.) to write fake or malicious entries that mislead analysts.	Sanitize all log fields Use structured logging (JSON) Escape control characters
74	Log Tampering After Write	Tampering	High	Open	4	Insider or attacker with access modifies or deletes existing log files to cover tracks.	Write-once / append-only storage (WORM, immutability) Cryptographic signing / hash-chaining RBAC on logs
75	Unencrypted Log Transport	Information disclosure	Medium	Open	3	Logs shipped over the network (Syslog, Fluentd, Beats) without TLS can be sniffed or altered.	TLS/Mutual-TLS for log shippers VPN or private network links
76	Sensitive Data in Logs (PII / Secrets)	Information disclosure	High	Open	4	Application logs inadvertently capture credentials, tokens, or personal data.	Log scrubbing / redaction middleware Classification & DLP scans Developer guidelines
78	Excessive Log Retention	Information disclosure	Low	Open	2	Logs kept indefinitely increase breach impact and cost.	Retention policy (e.g., 90 days) Lifecycle rules / automatic deletion
79	Insufficient Log Retention	Repudiation	Low	Open	2	Logs rolled-over too quickly, hampering investigations / compliance.	Align retention with regulatory & forensic needs Capacity planning

Number	Title	Type	Priority	Status	Score	Description	Mitigations
80	Log Overflow / Disk Exhaustion	Denial of service	Medium	Open	3	Massive log volume fills disk, crashing services (DoS).	Log rotation & compression Dedicated partition Alert on utilisation
81	Unsecured Central Log Repository	Information disclosure	High	Open	4	Central log directory or network share is world-readable or lacks encryption/ACLs, exposing all logs to any user on the network.	Tight filesystem / share permissions (read-only for SIEM, no public “others” access) Encrypt logs at rest Network segmentation / VPN for log collectors Regular audits of share permissions
82	Missing Integrity Monitoring	Tampering	Medium	Open	3	No mechanism to verify logs weren’t altered in transit or at rest.	HMAC / digital signatures Chain-of-custody audit trails SIEM alerts on hash mismatch
83	Lack of Real-Time Alerting	Repudiation	Medium	Open	3	Critical events are logged but no alert is raised, delaying response.	Define alert rules / thresholds Regular rule testing