Cybersecurity Service Proposal for Dr. Shaji MRI

📌 Introduction

Sesame Technologies is proud to have played a key role in developing and supporting the digital infrastructure for **Dr. Shaji MRI Center**, including the patient management platform `desk.drshajimri.com`.

When we built this system, it was developed using **security protocols and technologies that were up to date at the time**. However, cybersecurity threats have significantly evolved since then. Even well-built systems can become vulnerable if not continuously updated, monitored, and hardened.

To proactively address this, our newly established **Cybersecurity Division** conducted a detailed internal audit of the application and discovered a set of **critical security risks** that now need to be resolved to protect your platform, your patients, and your data.

🚨 Key Vulnerabilities Identified

1. Critical: Multi-Vector Information Disclosure

- Admin credentials (username and email) are **exposed through inconsistent error messages**.
- Source code and DNS records expose vendor names, internal projects, and infrastructure details.
- Enables **targeted password attacks** and makes account compromise much easier.

2. High: Use of Outdated Components

- Detected use of **jQuery v1.10.2** and old AngularJS, both with public XSS vulnerabilities.
- These were secure at the time of development but are **no longer safe today**.

3. Medium: Missing Security Headers

- Headers like `Strict-Transport-Security`, `X-Frame-Options`, and `X-Content-Type-Options` are missing.
- These are essential for **protecting against clickjacking, SSL stripping, and MIME attacks**.

4. Medium: Insecure Cookie Configuration

- Session cookie lacks the `Secure` flag, which can allow session theft on unsecured networks.

5. Low: Exposed Sensitive Directories

- Paths like `/console`, `/backend`, and `/uploads` are visible and give insight into internal structure.

🛠️ Proposed 6-Month Cybersecurity Engagement

Service	Description
Initial Remediation	Patch information leaks, update libraries, secure cookies, and headers
Monthly Security Audits	Scheduled scans for emerging threats
Application Hardening	CSP headers, uniform error handling, and metadata cleanup
Real-Time Monitoring Setup	Set up alerting for abnormal logins and attacks
Incident Response	Quick action if a breach or anomaly is detected
Reporting & Compliance	Monthly reports to meet regulatory or internal compliance

---

> “We built this platform with modern security standards. But no system remains secure forever unless it's actively maintained. Today’s cyber threats are automated, targeted, and far more aggressive.”

The risks:

> “We’ve found critical vulnerabilities that attackers could easily exploit to gain admin access or hijack sessions.”

The solution:

> “Rather than fixing it once and forgetting, we suggest a continuous 6-month cybersecurity engagement to harden, monitor, and keep everything secure.”

The impact:

> “This protects not only your systems but also your patients, staff, and brand reputation.”

🙋 Anticipated Questions & Responses

Objection	Suggested Response
Didn’t you build it? Isn’t this your job?	Yes, and we built it securely for its time. But the tech world moves fast. Security today requires continuous attention, not one-time development.
Why now? We’ve never had a breach.	Just like you do preventive health scans, cybersecurity needs prevention. These risks may not be exploited yet, but they are very exploitable.
Why pay for this separately?	Because ongoing cybersecurity was never part of the original dev scope. It’s a new service — just like maintenance after warranty.
Can you just fix the main issue?	We can fix what’s visible now, but new threats come up monthly. A 6-month plan ensures consistent protection.

✅ Why Action is Needed Now

- Admin account compromise risk is **real and active**
- Critical patient data could be exposed in minutes
- Cybersecurity is no longer optional — it’s a **compliance and trust** necessity

---

👥 Let's Secure This Together

We propose onboarding Sesame Technologies as your **Cybersecurity Partner** for the next 6 months. This will ensure:

- Complete remediation of known flaws
- Continuous protection of patient data
- Peace of mind for your team and patient