# Risk mitigation for low-risk web systems

Summary of measures that can help inform risk assessments for public-facing web sites

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **1. OWASP review** | **2. Patching strategy and confirmation** | **3. Monitoring tools** | **4. Encryption** | **5. Authentication mechanisms** | **6. Password policy**(if not using RealMe) | **7. Hosting Agreements** | **8. Procedures & documentation** |
| **What** it is – example risk mitigations | Vulnerability assessment required prior to release of new functionality.Automated testing annuallyArchitecture and code review prior to release of new functionality | All available updates applied at least 3-monthly; Version upgrades assessed annually.Critical patches applied within 2 days.NIST1 Vulnerability database reviewed 6 monthly, & any recommendations acted on.  | *Recommended*: Web Application Firewall (WAF) in place, or cloud-based WAF service deployed.Cloud-based scanning and monitoring tools deployed.E.g. combinations of Pingdom, Qualys, Sucuri, Incapsula, etc. | Admin login pages are SSL encrypted.*Recommended*: SSL Certificates applied to entire site. Certificates must be renewed periodically – a renewal register should be maintained. | Admin accounts managed by RealMe, OR two-factor authentication or IP whitelist controls in place.**IN CONFIDENCE:**Non-pseudonymous public user accounts managed by RealMe. | Strong passwords system-enforced. Measures in place to limit & log failed login attempts. Admin passwords kept to a minimum and whitelisted, and unneeded accounts deleted. Password management policy for all admin staff. *Recommended*: 2FA for admin accounts. | SLAs include vendor security responsibilities. Should include logging and audit, monitoring, Incident Mgt, network security, server and stack maintenance, and environment hardening. Should consider Intrusion Detection / Protection, application whitelisting. | a) Standard Operating  Proceduresb) System Security Plan & Risk Management Plansc) Incident Response  Proceduresd) Hosting Agreement. e) Business Continuity planDocumentation is reviewed and updated annually. |
| **Benefits** – of having themeasure in place | Provides a minimum level of assurance that the system is protected from most forms of attack.Vulnerability assessment and code review validate that defensive measures are properly implemented. | Provides a measure of confidence that systems are protected from recently identified vulnerabilities.Minimises risk of exposure to critical security vulnerabilities.  | Provides ongoing monitoring and scanning, and alerts to site managers as necessary. Enables site managers to take proactive defensive measures. Most scanning tools are continuously updated to notify of vulnerability to evolving threats. | Prevents manipulation of data in transit, makes it much harder to impersonate a govt site, prevents interception (man-in-the-middle) attacks, and prevents exploitation of other potential vulnerabilities. | RealMe provides significantly higher levels of confidence in security of logon & authentication process.RealMe user authentication eliminates risk of weaknesses in product or bespoke authentication systems | Provides defence against unauthorised access through password-related attacks, which are often the weakest point in a web site. | Provides assurance of the level of security provided by vendor. Assurance that monitoring procedures are in place.Assurance that procedures are in place in advance of a security incident. | System operating knowledge is captured and available to relevant parties. Security strategy is available for review. Incident response is available in advance and necessary parties are coordinated when necessary. Clear statement of provider responsibilities. |
| **How much** – the cost of implementation | **MODERATE**. Vulnerability assessment for low-risk sites can be in the order of $6-10k.Architecture and code review depends on complexity of the system. | **LOW**. Cost of patching is minimal if not already specified in provider SLAs.**MODERATE**. Version upgrades depend on the system. | **LOW** for hosted services. Hosted scanning / monitoring and WAF tools are hundreds of dollars per year per site.**HIGH** for dedicated in-house WAFs. | **LOW-NIL.** SSL encryption must be applied to admin logon pages (for sites not using RealMe), so effective cost of applying certificate to entire site is nil.SSL Certificates are a few hundred dollars per year. | **MODERATE - HIGH.** RealMe integration processes can add cost and time to development projects. NOTE that some vendors provide integration services which may reduce cost. | **LOW-MODERATE.** Cost of implementing system-enforced strong passwords can be trivial but depends on the system. All other measures are BAU. | **LOW-NIL.** Standard requirements specified in provider SLAs.Note that Intrusion Detection / Prevention may be an expensive option, and need may be mitigated by other monitoring and scanning tools (Column 3). | **LOW.** Production and maintenance of standard suite of documents is BAU. |
| **Risk** – of not implementing | **HIGH**. Untested systems may contain serious vulnerabilities with unknown consequences.Business owners are exposed to unknown risks.Code review provides extra assurance beyond penetration testing. | **HIGH.** Unpatched systems become vulnerable to unauthorised access, which may result in defacement, data loss, hijacking or malware insertion. | **MODERATE.** Without real-time monitoring and alerting of events on the web server, proactive defensive response is not possible.Hosted monitoring tools are continuously updated which allows proactive response to emerging threats. | **MODERATE.** Somewhat escalated risk profile across the site. However, SSL encryption is required for admin logon (for sites not using Realme authentication) so effort of treating this risk is minimal. | **MODERATE.** Bespoke or product authentication facilities may contain unidentified vulnerabilities. A need to manage multiple password systems may result in unsafe practices by users and duplicate investment across agencies. | **HIGH.** Password attacks can be common and easy to carry out. A successful attack results in unauthorised access which can result in defacement, data loss, or hijacking, or malware insertion. | **MODERATE.** No assurance of security profile of site, or division of responsibilities in regard to maintenance and security. No Incident Event Management processes. | **MODERATE.** No assurance of management and maintenance procedures, responsibilities in regard to maintenance and security are unclear. No Incident Event Management processes. |
| **Likelihood** - of compromise ifnot implemented | **HIGH.** A range of tools and hosted services are available with which unidentified users can scan sites for vulnerabilities which can be exploited. | **HIGH.** Vulnerabilities can be expected to be found over time in most software, unless security updates are regularly applied. | **MODERATE.** Potential attackers may discover a recently identified vulnerability before it is detected in a future security review. | **MODERATE.** Provides assurance of authenticity of information, prevents some common forms of attack (e.g. man-in-the-middle). | **MODERATE.** Systems may be exposed through defects in authentication processes, weak passwords, or interception or disclosure of credentials. | **HIGH.** Weak password policies are a significant attack vector exploitable by dictionary or brute-force attacks. Tools for this purpose are freely available on the web. | Risk cannot be quantified. | Risk cannot be quantified. |
| Notes | Hosted services such as Qualys can be used to provide continuous OWASP monitoring. | 1 <http://nvd.nist.gov/> | *Example services:**Pingdom*: Availability*Qualys*: OWASP monitoring*Sucuri*: Malware scanning*Incapsula*, WAF, DoS protection |  |  |  |  |  |