Routine Security Checks

FileGenius sites and all Applied Answers domains and servers are routinely subjected to, among other tests, each of the following security checks

- All external e-mails (optional)
- All external links not classified otherwise (optional)
- All external URL redirectors (optional)
- Assorted file POIs (server-side sources, configs, etc)
- Attacker-supplied embedded content (stored and reflected)
- Attacker-supplied script and CSS inclusion vectors (stored and reflected)
- Bad caching directives on cookie setting responses
- Bad caching directives on less sensitive content
- Broken links
- Changing Server, Via, or X-... headers
- Conflicting MIME / charset info on renderables
- Conflicting MIME / charset information on less significant content
- Directory listing bypass vectors
- Directory traversal (including constrained vectors)
- Exceeded crawl limits
- Expired or not-yet-valid SSL certificates
- Explicit SQL-like syntax in GET or POST parameters
- External untrusted embedded content
- External untrusted script and CSS inclusion vectors
- Failed 404 behavior checks
- Failed resource fetch attempts
- File upload forms
- Form fields that could not be autocompleted
- General SSL certificate information
- Generic MIME type on less significant content
- Generic MIME types on renderables
- HTML forms with no XSRF protection
- HTTP credentials in URLs
- Incorrect or missing charset on less significant content
- Incorrect or missing charsets on renderables
- Incorrect or missing MIME type on less significant content

- Incorrect or missing MIME types on renderables
- Integer overflow vulnerabilities
- IPS filtering detected
- Links to unknown protocols
- Locations accepting HTTP PUT
- Mixed content on non-scriptable sub-resources (optional)
- Mixed content problems on script and CSS resources (optional)
- New 404 signatures
- Numerical file names (for external brute-force)
- OGNL-like parameter passing conventions
- Other HTML forms (not classified otherwise)
- Password entry forms (for external brute-force)
- Redirection to attacker-supplied URLs (stored and reflected)
- Resources requiring HTTP authentication
- Resources that cannot be accessed
- Seemingly misclassified crawl nodes
- Self-signed SSL certificates
- Server errors
- Server-side shell command injection (including blind vectors)
- Server-side SQL injection (including blind vectors, numerical parameters)
- Server-side XML / XPath injection (including blind vectors)
- Significantly changing HTTP cookies
- SSL certificate host name mismatches
- Stored and reflected XSS vectors in document body (minimal JS XSS support present)
- Stored and reflected XSS vectors via HTTP header splitting
- Stored and reflected XSS vectors via HTTP redirects
- Unexpected response variations
- User-supplied links otherwise rendered on a page
- Format string vulnerabilities.