Body1

Website Security-

Our Approach

August, 2017

Confidential

Body1

Top 10 Website Security Vulnerabilities*

1. Injection
2. Broken Authentication & Session Management
3. Cross-Site Scripting (XSS)
4. Broken Access Control
5. Security Misconfiguration
6. Sensitive Data Exposure
7. Insufficient Attack Protection
8. Cross Site Request Forgery (CSRF)
9. Using Components with Known Vulnerabilities
10. Under-protected API's

* Open Web Application Security Project (OWASP) 2017

Body1

Body1 Approach

1. Internal education/awareness
2. Ongoing server-level monitoring
3. Self-audit for major vulnerabilities
4. Code to minimize Injection risks:
   - Limit long query strings
   - Application-level query string validation
   - Javascript form validation
5. Tight authentication controls
   - Internal flagging of attempted abuse
6. Cross-Site Scripting (XSS) scans using specialized tools
   - Fix code vulnerabilities as found
   - Replace vulnerable plug-ins if not patched promptly

Body1

Body1 Approach

7. Physical firewall locked down to only approved IP's
   - Web traffic 1st all routed through a CDN w/ a Web Application layer firewall:
     - Known attack IP's blocked
     - Infected browsers blocked
     - Malicious request patterns blocked
8. Patches & regular malware scanning
9. On-going packet level traffic monitoring (SNORT) for diagnosis in the event of intrusion
10. Pre-deployment malware scanning of all web asset acquisitions
11. Component & API vulnerability reviews
12. On-going event documentation to build our Security KB

Body1

Attacks we blocked on a BioPharma client-

typical 30 day snapshot