WEB APPLICATION ASSESSMENTS

KEY SERVICE COMPONENTS

- **Information Gathering**
  - o Determine what the attack surface area is
  - o Determine what technologies are in use
  - o Identify input areas and other application functionality
  - o Understand general application function and data flow
- **Authentication and Authorisation**
  - o Determine what mechanisms are in place to protect user accounts and authorisation schemes
  - o Test for known authentication and authorisation flaws
  - o Test for user enumeration and information leakage
  - o Brute-force user accounts and passwords
  - o Test logout and browser cache management
  - o Test multiple-factor authentication (2FA/Certificate)
  - o Test forgotten password functionality and user-creation functionality
  - o Test for race conditions or privilege escalation
- **Session Management**
  - o Analyse the session management functions implemented
  - o Analyse the session management token generation function for flaws
  - o Test session transport functionality
  - o Test cookie attributes
  - o Test for Cross-Site Request Forgery (CSRF)
  - o Input Validation
  - o Test the application's ability to handle malicious input and malformed requests
  - o Test the input/output encoding functionality present in the application
  - o Test system commands in input fields
  - o Test for Cross-Site Scripting (Reflected/DOM/Stored)
  - o Test for SQL injection
  - o Test for LDAP/ORM/XML/SSI/XPATH/Code injection
  - o Test for HTTP Splitting/Smuggling
  - o Test AJAX functionality
- **Business Logic**
  - o Determine if logic flow can be abused or bypassed
- **Configuration Management**
  - o Determine if any configuration management flaws exist, such as incorrect deployment and system hardening
  - o Test for platform-specific vulnerabilities
  - o Test HTTP methods and Cross-Site Tracing
- **Data Storage and Encryption**
  - o Determine what encryption mechanism is in place and the algorithms in use
  - o Test session cache control mechanisms
  - o Test SSL/TLS (SSL version, Algorithms, Key Length, Validity)

SERVICE DESCRIPTION

Exploiting vulnerabilities within applications, whether an installed executable or supporting library, a web application or smartphone application, is a primary vector for skilled and semi-skilled attackers. With many tools available to reverse engineer applications, the bar to application abuse is lowered continuously.

Once the domain of the elite hacker, but now attainable by hackers with less skill and experience, using application exploits to compromise systems to steal data is core to taking control of a computer or device until the software flaw is found and patched.

Software vendors and publishers aren't the only ones creating exploitable applications. The last few years have seen a massive increase in the development of in-house applications. Bespoke applications created for an organisation's sole use suffer from similar issues to those created by software vendors, most commonly when back-end databases or intranet web applications are used.

With 18 years' experience in deliberately abusing applications during Penetration Tests and Red Team exercises, and having discovered and reported 22 zero-day exploits in some of the world's best known software in the past 12 months, SecureData's team of Ethical Hackers' are the ideal candidates for testing applications. Our analysts are also co-project leaders of the OWASP Application Security Verification Standard (ASVS), the standard used for testing web application technical security controls and providing developers with a list of requirements for secure development practises.

KEY BENEFITS & DELIVERABLES

- **Real-World testing:** Manual supervision of assessments applying 18 years' worth of Ethical Hacker skills and experience in manipulating applications during penetration tests and red-team exercises
- **Secure by Design:** Incorporates security into application design during SDLC
- **Detailed reporting:** A uniquely detailed report containing the results of the review including the following elements:
  - o An executive summary highlighting the risk summary and prioritised recommendations
  - o Detailed technical results
  - o Potential exploit techniques
  - o Ease of exploit
  - o Potential impact
  - o Recommended remediation
  - o Appendixes including the detailed methods used to test and exploit the application.

WHY SECUREDATA

Cybersecurity specialists
SecureData specialises in cybersecurity services and solutions, with a 25-year track record of delivering managed services to some of the largest companies in the world.

Outstanding expertise
Our Managed Firewall service is delivered by our UK-based SOC - delivering immediate, 24x7x365 access to specialists who deal with device health incidents, requested and recommended changes, security optimisation and help ensure continuous availability.

Extensive security insight
SecureData's Threat Intelligence platform processes over 30 billion security events per month, giving us unparalleled access to current and emerging threats. SensePost, our elite consulting arm, is at the forefront of cybersecurity - providing insight into the criminal mind-set. We use this information to ensure our Managed Firewall customers are as secure as they possibly can be.

Vendor insights
Our close partnership with Check Point, Fortinet, Cisco and Palo Alto Networks provides superior access to their technical experts and product roadmaps - keeping our SOC's knowledge ahead of the game.

Complementary services
We offer a broad range of services that complement our Managed Firewall service and strengthen your security posture, including Managed IDS/IPS, Managed Threat Detection, Managed Vulnerability Scanning and Managed Compliance Monitoring.

ABOUT SECUREDATA

SecureData is a leading provider of cybersecurity services and solutions.

SecureData looks beyond point technologies to address cybersecurity as a whole. The company offers a comprehensive set of professional and managed security services across the entire attack continuum.

For over 25 years SecureData has been helping organisations assess risks, detect threats, protect assets and respond to breaches quickly and effectively ensuring essential IT infrastructure always remains secure and available.

SensePost, the consulting arm of SecureData includes some of the world's most preeminent cybersecurity experts. Trusted by both corporate and military organisations across multiple countries, SensePost helps organisations to protect IT infrastructure and stay ahead of evolving cybersecurity threats.

Operating across the UK, South Africa and the USA, SecureData has an enviable track record having delivered cybersecurity services for many business sectors including finance, insurance, retail, property, professional services, technology and government.

@SECUREDATAEUROPE @SECDATAEU WWW.SECDATA.COM

@SENSEPOST @SENSEPOST WWW.SENSEPOST.COM

SENSEPOST

FOR MORE INFORMATION PLEASE CONTACT US
T: +44 (0)1622 723400 | E: info@secdata.com