Orange
Cyberdefense

Assessment Services

Application Assessments

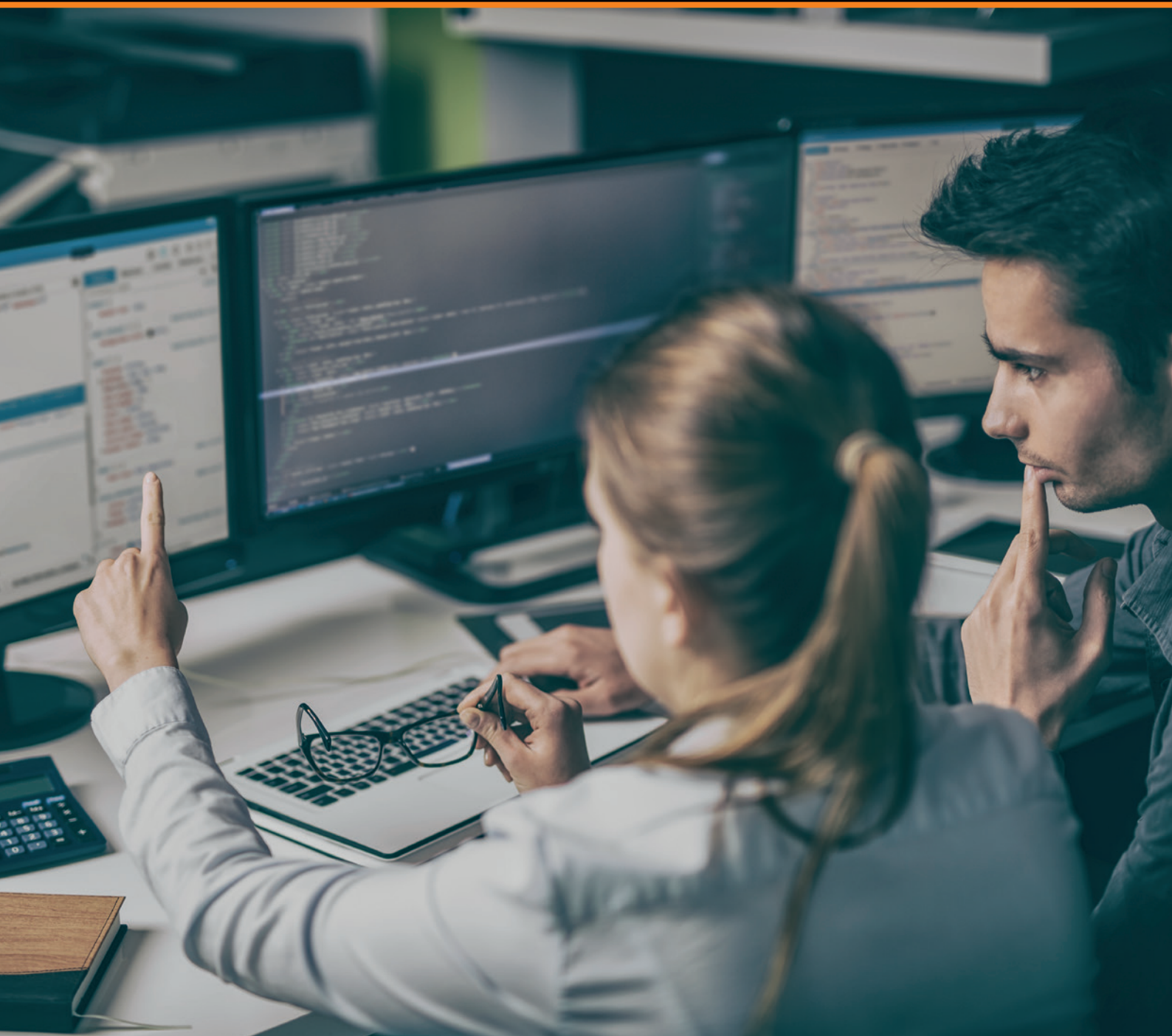


Table of Contents

1. Overview

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 though. 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.

Due to the need for rapid development and deployment, opportunities for authorisation bypass, passing usernames and passwords in plain text, SQL injection vulnerabilities, input validation failures, buffer overflow vulnerabilities, information leaks and many other flaws get introduced during application development.

2. About Orange Cyberdefense

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group. As Europe's go-to security provider, we strive to protect freedom and *build a safer digital society*.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

With a 25+ year track record in information security, 250+ researchers and analysts and 16 SOCs distributed across the world and sales and services support in 160 countries, we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle

3. Orange Cyberdefense Application Assessments

With increasing attention being paid to applications and the vulnerabilities they introduce, organisation's concerns over the applications they use daily and the risks these may pose are becoming heightened.

With 17-years' experience in deliberately abusing applications during Penetration Tests and Red Team exercises, and having discovered and reported 15 zero-day exploits in some of the world's best known software in the past 12 months, Orange Cyberdefense'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.

Whether via source-code review performed by specialist Security Analysts, dynamic analysis of an application while it is executing or static analysis of the application in a non-runtime environment, Orange Cyberdefense are able to introduce assurance at any point in the software development life cycle (SDLC) testing both the application and the technical security controls that are relied on to protect against vulnerabilities.

4. Scope of Services

4.1 Service Implementation

Orange Cyberdefense service implementation methodology takes advantage of our long-standing industry knowledge using our PRINCE-II certified Project Management Office (PMO) to ensure effective delivery. The Service Implementation includes the following phases:

5.1.1. Scoping meeting with a Security Consultant to identify the requirements and produce a proposal and scope of works.

5.1.2. Project kick-off meeting conducted with the key project stakeholders to introduce the project teams and agree key milestones and escalation paths. This also serves as a formal handover from commercial to project teams who then become the primary point of contact.

5.1.3. The assessment will commence based on the agreed Statement of Works document. The Project Management Office will manage delivery and ensure stakeholders are updated on progress throughout project delivery.

5. Application Assessment service

5.1 Web Application Assessment Components

Our methodology takes into consideration industry-wide statistic projects looking at the most vulnerable areas of application deployments, including the OWASP Top 10 and the SANS Top 25 Most Dangerous Software Errors. Considering our alignment to the OWASP Application Security Verification Project (ASVS), our testing methodology includes six key areas of an application

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

5.2 Mobile Application Assessment Components – Static Analysis

Mobile application assessments, while similar in process to those of application assessments, include several mobile-specific tests. They are broken down into two key areas being static analysis, which analyses raw mobile source code, decompiled or disassembled code, and dynamic analysis which analyses the application as it is running and interacting with remote services.

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

5.3 Mobile Application Assessment Components – Dynamic Analysis

Dynamic analysis, generally conducted against the backend services and APIs, varies depending on mobile application type.

Application Types include: -

a) Native Mobile Applications:

Native mobile applications can be installed on to the device. This type of applications generally stores most of their code on the device. Any information required can be requested to the server using the HTTP/s protocol.

b) Web services for Mobile Applications:

Native mobile application that uses SOAP or REST based web services to communicate between client and Server

c) Mobile Browser Based Applications:

Web browser based applications can be accessed using device's browsers such as Safari or Chrome. Most of the commercial applications are nowadays specifically designed and optimized for mobile browsers. These applications are no different than traditional web application and all the web application vulnerabilities apply to these apps and these should be tested as traditional web apps.

d) Mobile Hybrid Applications:

Applications can leverage web browser functionality within native applications, blending the risks from both classes of applications.

- Generate file system baseline fingerprint (before app installation)
- Install, configure and use the application
- Debugging

5.4 Source Code Assessment Components

Source Code review methodology is subject to the type of code and languages of the application being assessed; however, the basic principles follow several strategies or hybrid approaches that can be used.

- Candidate Point Approach
  - Creation of a list of potential issues
  - Examine source code to determine the relevance of these issues
- Design Generalising
  - Analysis of potential medium- to high-level logic and design flaws
- Code Comprehensive
  - Analyse the source code directly to discover vulnerabilities and improve the auditor's understanding of the application
  - Perform automated code scans using appropriate software toolset
  - Manual verification of the automated analysis
- Desk Check
  - Creation of a table of all variables in a code fragment, populate variables with random initial values for incorrect handling, manual updating of values according to the resultant code
- Subsystem and Dependency Analysis
  - String parser, system API replacements (such as file manipulation APIs and network APIs), custom memory allocators identification

5.5 Service Deliverables

Deliverable	Description	Frequency
Reporting	A uniquely detailed report containing the results of the review including the following elements: • An executive summary highlighting the risk summary and prioritised recommendations • Detailed technical results • Potential exploit techniques • Ease of exploit • Potential impact • Recommended remediation • Appendixes including the detailed methods used to test and exploit the application.	On assessment completion

6. Complementary Services

6.1 Phishing-as-a-Service

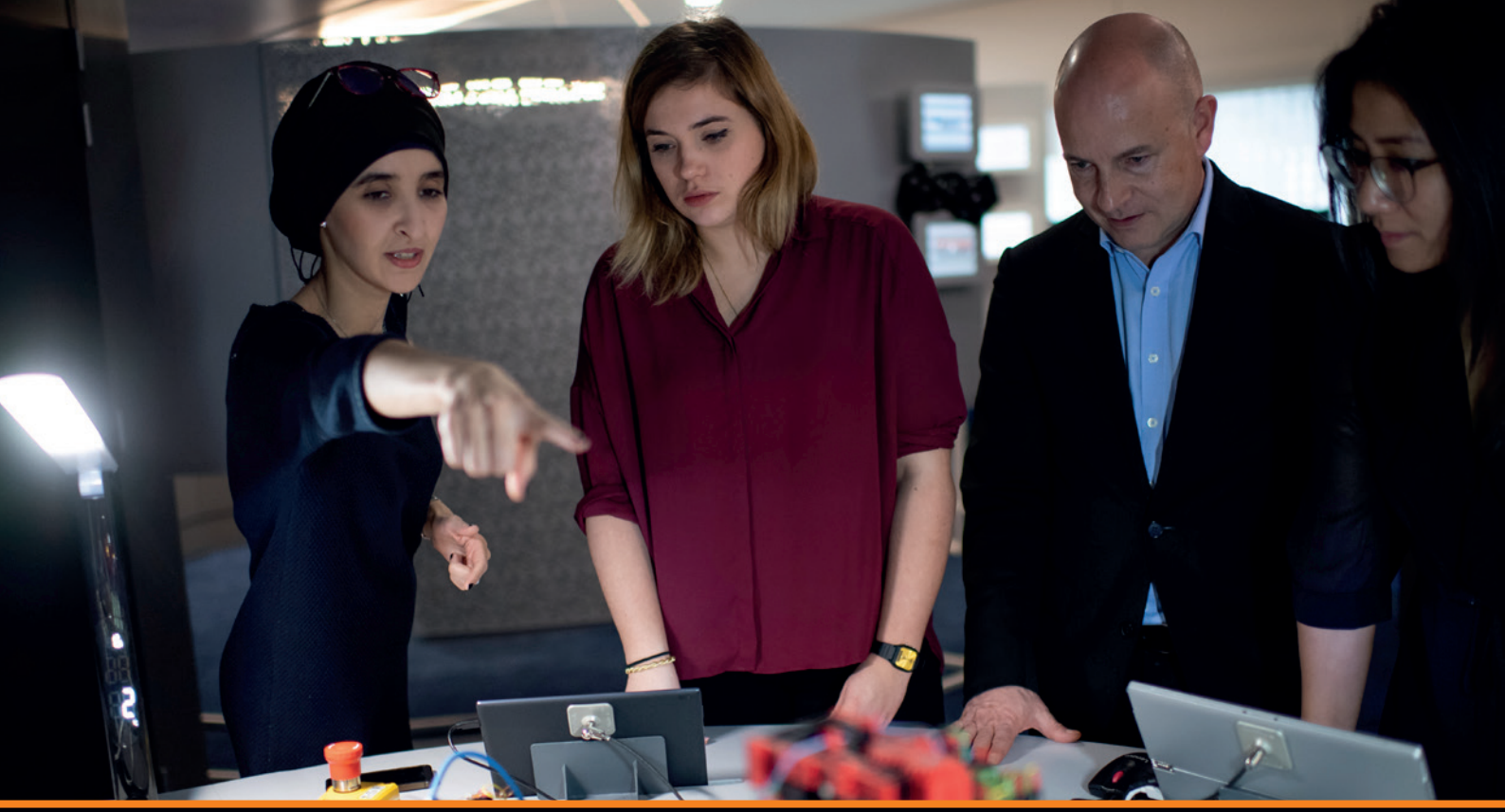
Orange Cyberdefense's Phishing-as-a-Service is designed for organisations concerned about their users' security awareness, seeking assurance that their employees are able to identify and report suspicious communications. Using techniques and methods identical to those employed by malicious actors, either as a limited test where usernames and email addresses are supplied by the client or as an unlimited test against any email addresses discovered from publicly accessible sources, Orange Cyberdefense will provide quarterly assessments of an organisation's employee's susceptibility to social engineering via email.

6.2 Managed Threat Detection

Orange Cyberdefense's Managed Threat Detection service uses a combination of technologies to provide a comprehensive 24x7x365 cloud based managed threat detection service. The service ingests, aggregates and correlates log and event data using our proprietary Greater Intelligence platform. Our platform adds intelligence and context to the data prior to the examination of suspicious traffic by a team of expert security analysts. Any potential security incidents are communicated to the customer and dealt with as required.

6.3 Footprinting-as-a-Service

Orange Cyberdefense's Managed Advanced Footprinting Service is designed to provide an up to date view of an organisation's publicly exposed infrastructure and resources, especially those which are not obvious or are well hidden. Using techniques and methods identical to those employed by malicious actors, either as a limited test where domain names and/or IP addresses are supplied by the client, or as an unlimited test against any domain names and/or IP addresses discovered from publicly accessible sources, Orange Cyberdefense follows a formal methodology to mine information about DNS domains, Host Names, IP Addresses and Email Addresses from various Open Source data sources.



Why Orange Cyberdefense?

Orange Cyberdefense is the expert cybersecurity business unit of the Orange Group, providing managed security, managed threat detection & response services to organizations around the globe. As Europe's go-to security provider, we strive to build a safer digital society.

We are a threat research and intelligence-driven security provider offering unparalleled access to current and emerging threats.

Our organization retains a 25+ year track record in information security, 250+ researchers and analysts 17 SOCs, 11 CyberSOCs and 4 CERTs distributed across the world and sales and services support in 160 countries. We are proud to say we can offer global protection with local expertise and support our customers throughout the entire threat lifecycle.

Orange Cyberdefense has built close partnerships with numerous industry-leading technology vendors.

We wrap elite cybersecurity talent, unique technologies and robust processes into an easy-to-consume, end-to-end managed services portfolio.

At Orange Cyberdefense we embed security into Orange Business Services solutions for multinationals worldwide. We believe strongly that technology alone is not a solution. It is the expertise and experience of our people that enable our deep understanding of the landscape in which we operate. Their competence, passion and motivation to progress and develop in an industry that is evolving so rapidly.

We are proud of our in-house research team and proprietary threat intelligence thanks to which we enable our customers to focus on what matters most, and actively contribute to the cybersecurity community. Our experts regularly publish white papers, articles and tools on cybersecurity which are widely recognized and used throughout the industry and featured at global conferences, including Infosec, RSA, 44Con, BlackHat and DefCon.

www.orangecyberdefense.com
Twitter: @OrangeCyberDef