OnDefend
CYBER SECURITY REALIZED

Application Testing Services Info Guide

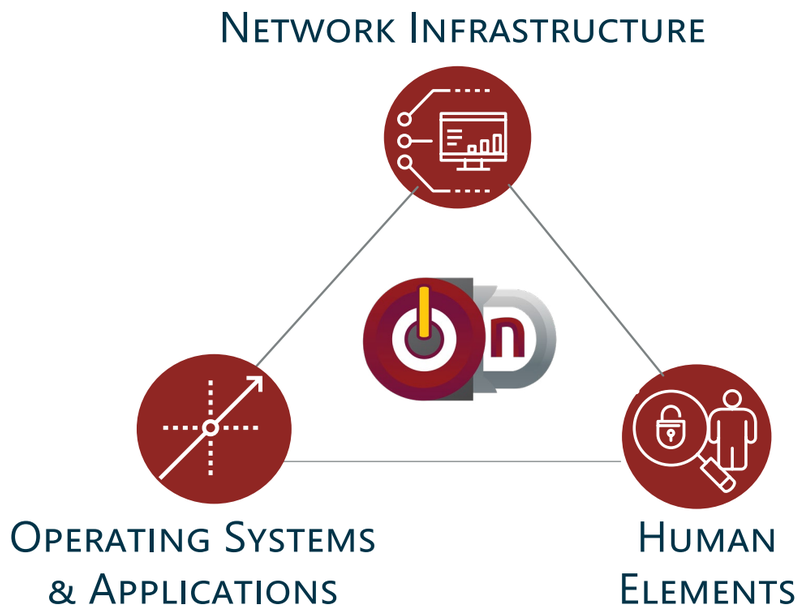
ONDEFEND.COM

WELCOME TO ONDEFEND'S TESTING SERVICES

Our testing services are built from the ground up to provide industry leading assessments based on best practices and mature frameworks. The value of any security assessment is in the actionable information to fix the problems identified in the report of findings. OnDefend's mission is to help organizations of all sizes, budgets and other factors that impact their security decisions.

Our Holistic Approach

Each service offering provides different perspectives into the security posture of an organization, with a focus on testing all layers of the technology (and people) stack in an understandable way that focuses on the true risks facing your organization.



A Snapshot In Time

Security tests are a snapshot which provide detailed information on what an attacker can do once they take advantage of that first vulnerability. Enterprises are like living things, always changing as new systems come online, upgrades to applications are made, infrastructure changes are made to accommodate business needs, and patches are released. New vulnerabilities are announced every day, meaning that a system that is fully patched and secure today may not be tomorrow. As such, security testing needs to be a continuous process, not just a single effort completed every once in a while.

OnDefend works with your organization to understand your maturity in the security testing space and builds a testing plan that meets a cadence your organization can support. This ensures you receive a frequency of testing to provide valuable data while providing enough time for remediation activities in between testing engagements.

APPLICATION SERCURITY TESTING

Overview

Modern web applications have transformed the way we companies deliver their services to their customer. Dozens of languages and frameworks exist that enable desktop-class experiences on virtually any device with a web browser, scalable to meet the demands of any enterprise. These web applications often provide access to extremely sensitive data and are accessible to anyone on the Internet. The sheer complexity of these web applications provides a vast attack surface, one which requires constant attention and testing to correctly secure.

Attackers take full advantage of these complexities leading to vulnerabilities in web applications. The only way to know the state of security for a web application is to test it. Testing that covers not only classic attacks like SQL injection or Cross Site Scripting, but goes in depth to understand the logic of the application, what is important to protect, and can those controls be bypassed. Effective web application requires a combination of automated testing and manual review by a person.

Methodology

OnDefend provides comprehensive static and dynamic reviews of targeted web and mobile applications which follow the approach in the Penetration Testing Execution Standard (PTES). Our web and mobile application assessments use the following phases to deliver this service:

Application Security Testing Phases

1. Intelligence Gathering
2. Vulnerability Identification
3. Exploitation
4. Post Exploitation
5. Analysis & Reporting

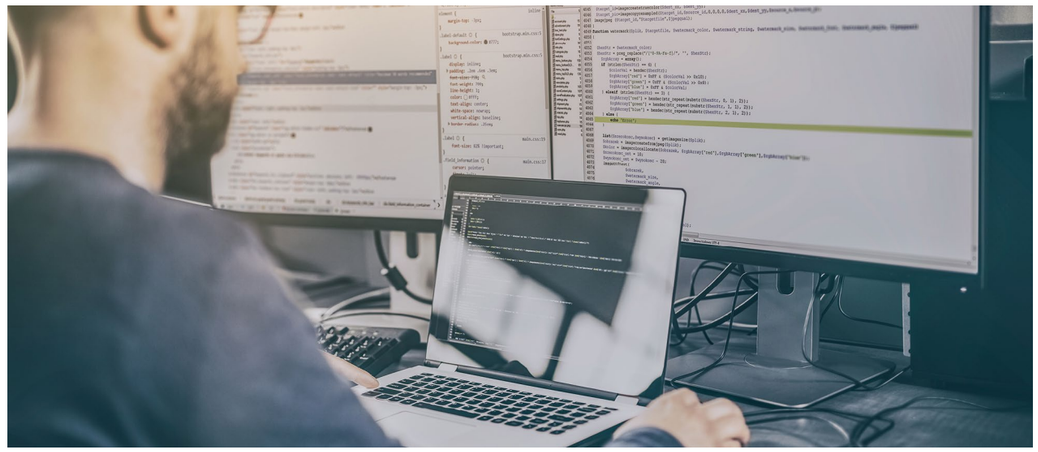
OnDefend uses the Open Web Application Security Project (OWASP) Testing Guide to build a complete checklist of all items tested during the course of the engagement. This enables us to provide easy to understand artifacts after the assessment for validation and retesting as required.

APPLICATION SERCURITY TESTING

Deliverables from this service include a detailed report of all findings, a summary of controls that worked correctly and prevented successful exploitation and an easy-to-import output of findings, ready to import into a ticketing system or GRC tool.

1. Intelligence Gathering

OnDefend starts by building a profile of the application being tested that provides the testing team the boundaries of what can be tested, what can be exploited and how far to go, the services offered by the application that will be tested, and the underlying framework and infrastructure of the application. We'll also map out the business logic of the application, to understand the purpose of the functionality and what actions would be considered unauthorized within that business logic.



2. Vulnerability Identification

Leveraging the profile of the application derived in the Scoping and Information Gathering phase, the testing team begins systematically walking through the application and testing each parameter and function on every module within the application. Every surface of the application, from the web server to the framework the application is built on is tested for weaknesses or additional information that could lead to a vulnerability finding. Both manual and automated tests are used in this stage, to ensure complete coverage and speedy identification of vulnerabilities.

During this phase there is no intrusive testing occurring, and the testing team is still moving through testing checklists to ensure all scenarios and cases are considered, including:

- Unauthorized access to data
- Unauthorized user rights
- Unintended function side effects
- Cross-site scripting
- Buffer overflow encryption
- Identifying mis-implemented encryption
- Denial of service
- Man-in-the middle attacks
- And more...

APPLICATION SERCURITY TESTING

3. Exploitation

In the Exploitation phase the team begins acting on the findings from the Vulnerability Analysis phase. This validates the vulnerability finding and enables the testing team to better rank the risk related to this finding. Testing teams will leverage these vulnerabilities to attempt to bypass security controls, gain access to additional rights or user accounts, and access data not authorized to the supplied testing accounts.

OnDefend testing teams are sensitive to the day-to-day demands of operational teams and will coordinate with the customer before beginning testing activities that may cause the system to become unresponsive or over-write data stored within the application. OnDefend testing teams will always respect the scope of the test and the Rules of Engagement agreed upon before the assessment began.

4. Post Exploitation

Leverage additional access or information gathered during Exploitation phase to find additional vulnerabilities or ability to further access the systems or data. In this phase tester will determine if it is possible to access other systems on the network or access the operating system of the web or database servers hosting the application.

NETWORK PENETRATION TESTING

5. Analysis & Reporting

In this phase a complete report of all testing activities and findings is compiled. Every finding will include actionable remediation options that can prevent or reduce the risk of the finding significantly.

Test reports include:

- Details on how each finding was identified and confirmed
- Severity rankings
- Effective remediation recommendations
- Full narrative of the engagement
- Detailed recommendations of additional detection strategies
- Identifying the effective controls that prevented various attacks from working

Client may request results in alternative formats to facilitate importing into GRC tool or ticketing system as necessary. See Sample Test Report to view our test results deliverable.

Tools and Techniques

OnDefend testers focus on the fundamentals of the systems and applications that are being tested, rather than focusing on specific software testing tools. This adaptive approach enables OnDefend testers to leverage commercial products, open source tools, and custom developed scripts and applications to conduct testing. OnDefend consultants are constantly learning and teaching new skills and techniques and contribute to open source projects in the information security ecosystem.

OnDefend
CYBER SECURITY REALIZED

BLUE TEAM WORKSHOPS

Overview

OnDefend also provides optional Blue Team workshops as part of these engagements. In these workshops, OnDefend security testers conduct in-depth technical training, based on feedback from the customer after the report draft is delivered. OnDefend consultants tailor the workshop based on customer feedback.

The Workshop

Sometimes these courses are focused on teaching the methods used during an engagement to enable a customer's team to reproduce the findings in the report. Other sessions are built to teach tactical and strategic actions to reduce the exposure of those specific findings, or help with other security related concerns, such as incident response planning and reviews. This workshop is typically a one-day course, usually 3-4 hours of content, for up to 10 members of the customer's team.

OnDefend
CYBER SECURITY REALIZED

THE ONDEFEND TESTING TEAM

OnDefend's testing services are only as good as the talented testers we utilize to provide these services. As such, we spend significant time and resources ensuring our testers meet our standard and are constantly improving their skills and expanding their knowledge.

Qualification Program

PRACTICE ASSESSMENT

This real-world work sample method lets us see what a tester will be able to provide for our customer, not just what trivia questions he or she could answer in an interview.

PEER REVIEW

A successful outcome in the practice assessment moves the candidate along to the final interview with some of the senior team members.

EXTENSIVE BACKGROUND CHECK

OnDefend testers must pass an extensive background check in order to be hired.

SHADOW AND RECERTIFICATION

Once hired, the tester shadows other senior testers for a few engagements. All testers undergo annual recertification reviewed by our Principal Consultants.

Testing Team Credentials

OnDefend's typical tester candidate requirements:

- At least 7 years of direct security assessment experience
- A bachelor's degree in Computer Science or Software Development or comparable work experience
- Hold certifications like the EC-Council Certified Ethical Hacker (CEH) and Offensive Security Certified Professional (OSCP)
- Active members of their local information security community
- Present at various conferences and events on security related topics
- Participate in vulnerability research contests and bug bounty programs, to further develop their skills and broaden their experiences

OnDefend provides advanced training for all testers, and such training is an integral component of the employee review process. We host internal training sessions where team members share knowledge and techniques, and also sponsor "hackathons" where testers get the opportunity to work exclusively on solving a problem to make them more effective, whether building a new tool, integrating new methods into the process, or extending the platform to improve the effectiveness of our services. These events often generate ideas that we bring into production as part of the formal process, and ensure our processes and tools are driven by the quality of the testing they enable.

OnDefend
CYBER SECURITY REALIZED

OnDefend
CYBER SECURITY REALIZED

Contact Us Today

Industry Leading Professionals are here to answer any questions you may have regarding our cyber security services & solutions.

Visit us at:

OnDefend.com

Or contact us via:

Email: contact@ondefend.com

Call: 800.214.2107