MERIMETSO

Website / Web Applicaiton Penetration Test

Service Description Introduction

A website / web application penetration test aims to review an entire application. An assessed application will be subjected to a review for vulnerabilities (including those detailed within the OWASP Top Ten located at https://owasp.org/www-project-top-ten/) in order to identify any weaknesses that could allow an attacker to compromise the application, the data it interacts with, its users or the hosting environment. Website / Web application security testing should be part of all organisations risk assessment phase prior to launching live services. Merimetso takes web application security testing to the highest level, ensuring that a customer can release their web app, knowing it has been extensively scrutinised by industry leaders. We can provide scheduled monthly website / web application penetration testing services to our customers to ensure their web presence is secure on an ongoing basis.

The difference between the terms Website and Web Application:

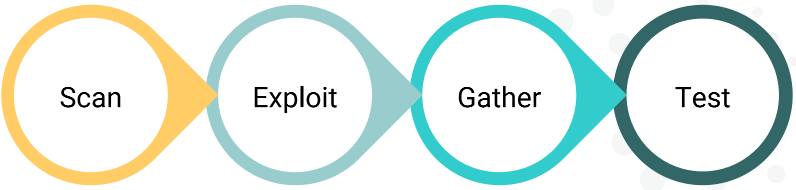
- A website is typically considered a set of web pages viewed within a browser. This may be a static set of pages that provide visitors with information; similar to a brochure, with limited or no way for users to interact with it.
- Web applications are interactive sites or those that rely on and provide interactive elements and are predicated on user engagement.

Engagement Structure

Part 1: Website Pen Test - A full test on the nominated website / application (including OWASP Top Ten most common vulnerabilities) with manual verification of any potential vulnerabilities found. This will be followed by an in-depth analysis and report highlighting risk, effect and effort to fix.

Part 2: Web Application Test – We will employ different software testing techniques to find issues in applications hosted on the Internet.

Our Approach - Website



Methodology - Website

Scan

Remote Scan - To ascertain any potential vulnerabilities that may be identified using automated tools. This will also identify links to other sites that could present a risk to the target site. Those sites that are identified and require examination will be added to the scope once authority to do so is given.

Exploit

A senior security consultant will use the results of automated and manual assessment to identify target areas which may be vulnerable.

These areas will then be scrutinised further with the aim to exploit the issue in order to identify what an malicious actor could achieve.

The testing may be non-destructive, thus protecting the integrity of the website in a live environment where required.

Gather

Information Gathering - Fingerprinting the application using bespoke and COTS tools to identify assets/software/resources in use.

Test

Config Management Test

Review the services presenting the application and that the application interacts with (where possible). This can include database management systems, infrastructure and secure communication protocols.

Business Logic Test

Creating functional tests to understand how the application works and then applying incorrect functional flow to assess how the application reacts.

Authentication Test

Assessing the security of authentication mechanisms in use.

If the application provides user login functionality, then it can be tested from both black- and grey-box approaches:

- **Black-box:** User enumeration and brute force attacks will be attempted on the user login function to gain authenticated access from an unauthorised perspective.
- **Grey-box**: An account with a low-level privilege within the application will be provided to the test team in order to assess the application as a legitimate user.

Where present/required, the assessment will also include the reviewing of functionality including CAPTCHA, multiple-factor authentication, testing the application’s resilience to brute-force testing and identifying the predictability of username and password combinations.

Authorisation Test

Applications which implement access controls/user accounts will be tested for privilege escalation and authorisation bypass issues to help ensure that users are unable to gain access to resources/functionality beyond their requirements/authorisation.

This will be reviewed in two manners:

1. **Horizontal segregation:** The application will be assessed to identify any issues which could allow access to resources belonging to another user account by a similarly privileged user (outside of their required access).
2. **Vertical segregation:** The application will be assessed to identify any issues which could allow a less-privileged user account to access privileged resources (e.g. administrative functionality).

Session Management

Testing for cookie implementation, linear regression testing of cookie value randomness, session management schema, session fixation, session variable theft and exposure and cross-site request forgery.

Data Validation

A thorough series of automated and manual tests will be undertaken to verify that all user-supplied data sent to the application is correctly sanitized. Testing seeks to identify, but is not limited to, cross-site scripting, DOM-based issues, SQL, LDAP, ORM, XML, SSI and Xpath injections, as well as vector-based overflows.

Denial of Service

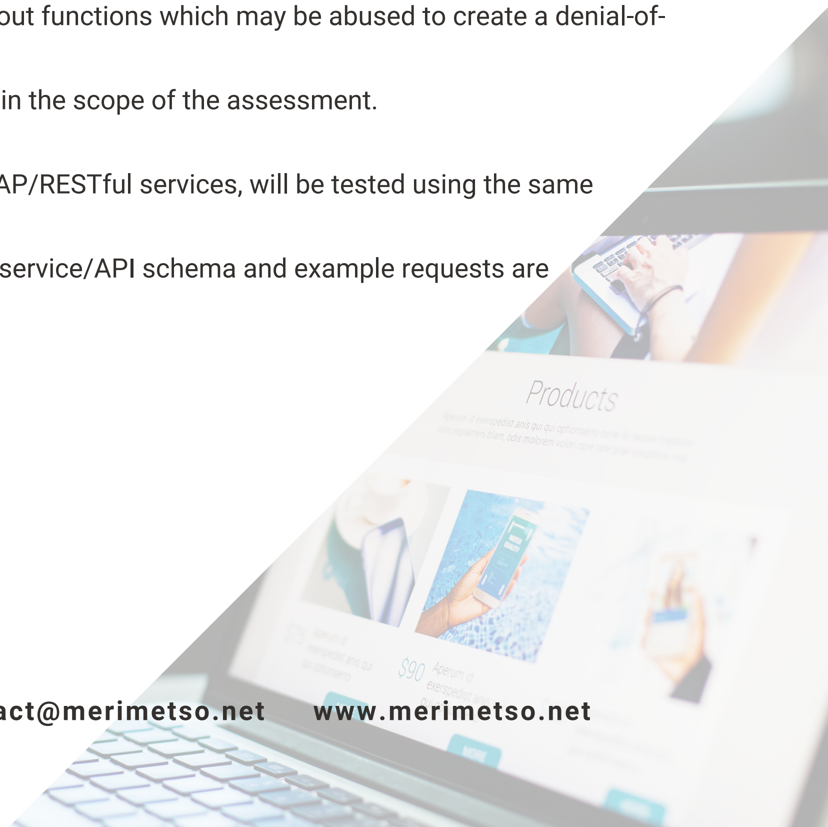
Testing activity will be undertaken to actively seek out functions which may be abused to create a denial-of-service condition within the application.

Such issues will only be leveraged if permitted within the scope of the assessment.

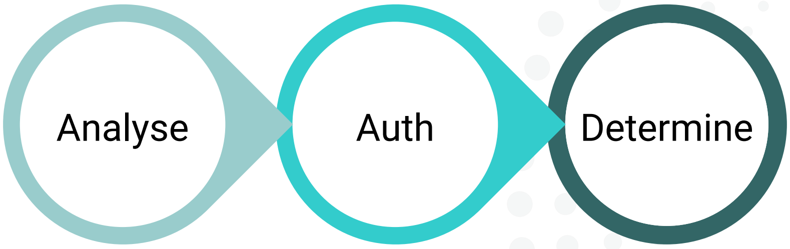
Web Service/ APIs

Where present, web services and APIs, such as SOAP/RESTful services, will be tested using the same methodology detailed above.

For in-depth white-box assessments, a copy of the service/API schema and example requests are requested



Our Approach - Web Applications



Methodology - Web Application

Analyse

Decompose or deconstruct the binary codes, if available.
Determine the protocol specification of the application.
Deduce program logic from the error/debug messages in the application outputs and program behaviours / performance.

Authenticate

- Find possible brute force password guessing access points in the applications
- Find valid login credentials with password grinding, if possible
- Bypass authentication system with spoofed tokens
- Determine the application logic to maintain the authentication sessions - number of (consecutive) failure logins allowed, login timeout, etc.

Determine the limitations of access control in the applications - access permissions, login session duration, idle duration.

Determine

- Determine the session management information - number of concurrent sessions, IP-based authentication, role-based authentication, identity-based authentication, cookie usage, session ID encoding string, session ID in hidden HTML field variables, etc.
- Predict the session ID sequence and format.
- Determine if the session ID is maintained with IP address information; check if the same session information can be retried and reused in another machine.
- Determine the session management limitations - bandwidth usages, file download/upload limitations, transaction limitations, etc.
- Gather excessive information with direct URL, direct instruction, action sequence jumping and/or pages skipping.
- Gather sensitive information with Man-In-the-Middle attacks.
- Inject excess/bogus information with Session-Hijacking techniques.

Replay gathered information to attempt to bypass application restrictions.

Deliverables

In-depth report, broken down into 3 main parts:

1. Management Summary
2. Technical Overview
3. Detailed Technical Findings

Highlighting the vulnerabilities:

1. Type of RISK
2. The EFFECT of that RISK
3. Recommendations on how to address and mitigate vulnerabilities
4. Estimate of effort required to remediate any vulnerabilities identified

Project Management

Project Management resource will be assigned throughout the engagement but will not be allocated full time.

Key roles and responsibilities:

- Run engagement kick off workshop.
- Run engagement closure.
- Maintain and communicate engagement risks and issues log.
- Weekly status meetings and engagement tracker.

Prerequisites

The following pre-requisites are required from the client:

- Physical access to the device or exported configuration files
- Make and Model of the Firewalls
- Written permission from the client to test
- Login credentials and digital certificates (if applicable)
- Point of Contact details

Deliverable Acceptance Criteria

Merimetso may present interim deliverables to the customer for review throughout the engagement. Should Merimetso present an interim deliverable, the customer will review, and either accept, or document specific corrective items in writing within three (3) business days. In the absence of any comments, deliverables produced by Merimetso will be deemed accepted after three (3) business days.

Limitations & Exclusions

- This engagement covers only the activities detailed in this document. Additional Merimetso offerings may be purchased as add-ons, otherwise additional consulting work not contained in this engagement is deemed out of scope.
- Working time is defined as Monday to Friday (excluding local bank/statutory holidays), 9am-5pm, with a 60-minute break for lunch.
- Merimetso is not responsible for the installation, configuration, or validation of any third-party software, tools, or utilities.
- Only third-party software and infrastructure identified during the pre-sales phase will be in scope for the engagement. There will be no change of scope where third-party software or infrastructure has been changed by the customer during the course of the engagement, or this will incur additional cost.

Customer Responsibilities

1. The customer must provide appropriate resources during the engagement from commencement date.
2. The customer must provide Merimetso representatives with information and resources to ensure Merimetso is able to successfully execute the engagement. This can include, without limitation, providing access and credentials to systems, completing installation prerequisites, providing resources, and attendance in planning, execution, or training meetings.
3. Customer will ensure resources are available in a timely manner to undertake tasks such as change control and documentation review.
4. Customer must ensure it has the necessary escalation and communication channels to resolve any blockers in a timely manner, including dependencies on third parties customer vendors, suppliers, and consultants.
5. If the consultant should travel to a customer location for the delivery of this engagement, there will be additional travel and expense costs. These travel and expense costs can be paid for prior to the engagement, or at actuals, at engagement completion.
6. The customer shall provide at least seventy-two (72) hours' notice for the cancellation or postponement of any work already scheduled as part of the engagement. In such scenario of a cancellation or postponement Merimetso reserves the right at its sole discretion to charge the customer for additional resources at Merimetso's then current daily rate for the delay period.
7. Customer must have a right to use the software and licenses. This requires that the customer must have purchased, or have converted, the appropriate license rights to the target environment.
8. Hardware requirements are the responsibility of the customer, and it is the customer's responsibility to ensure the hardware requirements are met prior to the engagement.

Merimetso may subcontract all or a portion of the services and/or have the services performed by one of its affiliates.

Note: The services described in this Service Description are subject to the terms and conditions by Merimetso Terms

Our Senior Testing Team

Dr Andrew Blyth - Founder and Director of R&D

Dr Blyth received his PhD in Computer Science in 1995 from Newcastle University, UK. Dr Blyth held the position of Professor of Computer Forensics at the University of South Wales, UK, throughout his illustrious career. Co-authored a textbook on Information Assurance, supervised 15 successful PhD candidates, created several BSc and MSc Computer Forensics and Cybersecurity Programmes. He was instrumental in the University of South Wales being the first University in the UK to behave an MSc in Computer Forensics accredited by the UK Government's National Technical Authority (GCHQ/NCSC).

He was the Cybersecurity Technical Lead at the UK Ministry of Defence's (MOD), Defence Science and Technology Laboratory (DSTL). During that time, he created and ran the Computer Network Defence Technical Demonstrator programme and defined various other research programmes within DSTL. He has over 50 peer-review publications and managed millions of dollars of research funding.

Campbell Murray - Founder and COO

Campbell is an established global leader in the field of information security. With over 25 years of experience ranging from offensive security assessments and security engineering in a vast range of environments providing Campbell with rare detail and insight into the field of cybersecurity. Campbell established himself as a penetration testing consultant in 2000. A firm believer in knowledge transfer, Campbell was a founding director of the TigerScheme in 2007 and the Cyber Scheme in 2013.

The Cyber Scheme is the recognised course used by NCSC to affirm CHECK status on any penetration tester who wishes to work on Government infrastructure in the UK. Campbell is now the chair of the technical panel for the Cyber Scheme and is one of only a handful of GCHQ appointed CHECK Team Leader assessors.

David Mound - Founder and CTO

David is a highly experienced Cyber Security Researcher with a demonstrated history of working in the Computer & Network Security industry and threat intelligence. Skilled in Penetration Testing, Reverse Engineering, Computer Forensics, Red Teaming and Threat Intelligence, he has worked with numerous global agencies within the 5 Eyes community, including GCHQ and the NSA delivering, advising on Red Team methods and engagements to assess Blue Team capabilities.

David's current speciality and focus are cloud-based technologies, and he holds multiple cloud certifications such as AWS Certified Security Specialist. David is an ex-Naval officer and is currently a member of the Army Reserves, where he coordinates threat hunting and assists network defence within the UK MOD and Gov estates. David brings his extensive technical capability to design the innovation to the Merimetso Cyber Technical Training platform.