

Web Application Penetration Testing >>



Web Application Penetration Testing

Let **Pentest People** assess your critical **Web Applications** for Security Vulnerabilities with a thorough **Web Application Penetration Test**.

The Web Technologies and applications we use daily have advanced in recent years. This advancement and reliance upon such services has exposed users to a variety of new security risks.

Their complexity and availability have made them an ideal target for attackers, demonstrated by the many publicised major data breaches.

Web Application Penetration Testing is now a critical part of your security strategy to ensure your public facing applications are free from security risks.



What Are the Risks

External facing **Web Applications** used by businesses are by nature available to all via the public Internet. Their complexity and availability have made them an ideal target for attackers and there have been many publicised data breaches that have been caused by insecure web applications.

Protecting these applications from new threats is a constant challenge, especially for developers who may not be security aware and typically working toward a performance deadline.



How Can We Help?

Pentest People will use industry-leading techniques to assess the security of your remote working solution following a defence in depth approach, identifying the available public facing attack surface, authentication control weaknesses, segmentation issues, and any configuration vulnerabilities that could allow a user to escalate privileges.

Pentest People have a wealth of knowledge in the area of application security testing, and their testers have created and contributed to many open source web application security projects.

The results of the assessment are uploaded to your **SecurePortal** account, as part of the **Penetration Testing as a Service (PTaaS)** offering.

All Services Use Our Innovative SecurePortal

SecurePortal is a live security platform designed to improve the way you view and manage your Penetration Test results.

Introducing SecurePortal

SecurePortal is a key component of Penetration Testing as a Service and provides customers of Pentest People with a live platform of engagement and also managing the current security posture of your organisation based on the information gathered from our penetration testing services.

- ✓ Eases the administrative burden of planning a Penetration Testing engagement
- ✓ Provides digital access to your report
- ✓ Tracks the state of your vulnerabilities automatically
- ✓ Alerts you when new threats are relevant
- ✓ Provides a simple way to filter your report data



The SecurePortal offers our clients a multitude of features



Live Vulnerability Dashboard

SecurePortal provides a single dashboard view of all of the identified vulnerabilities across your infrastructure. Data from different assessment types is combined to help you see the full security posture of your organisation.

Receive overview and trend data of all of the current security issues you face in your organisation. Receive useful trend information such as the top vulnerable hosts, and the most common vulnerabilities within your infrastructure.



Helping You Engage With Pentest People

Customers are introduced to **SecurePortal** early in the sales process and all sales proposals are accessed and downloaded securely through the **SecurePortal**.

Once the agreement to proceed has been made, all of the project management tasks associated with our various **Penetration Testing** services are performed on the **SecurePortal** using various secure web-based forms rather than relying on the unsecured emailing of various documents.



Helping You Manage Your Vulnerabilities

Until now, the traditional deliverable from a **Penetration Test** engagement has been a lengthy report. This is usually provided in a PDF file format and can run into the hundreds of pages.

Pentest People have developed a solution to this issue where you interact with your vulnerabilities within the **SecurePortal**. This allows you to quickly search for vulnerabilities rather than scanning through a lengthy document.