Web Application Penetration Testing Primer

Penetration testing is regularly used by organisations as part of their ongoing security strategy/programme.

Web Application Penetration Testing is a security exercise that involves an ethical hacking team scaling planned attacks against your web application and web server, this can be performed from either an internal and/or an external threat perspective. At the end the exercise you should expect a comprehensive report back on the findings and how to remediate any identified vulnerabilities, this will allow you to better understand the security gaps, current security risk profile and practical steps for improvement of the web application.

Objective

Web application penetration testing actively seeks out any vulnerabilities in your web application and associated web services, essentially simulating a real attack under carefully controlled conditions.

It can also help you in determining exactly how effective your existing defence mechanisms are, and evaluating whether or not your organisation is following security best practise including secure coding.

Types of testing

Penetration testing is generally categorized into 3 primary testing approaches. In order to deliver the outcome, you wish for it is recommend discussing the key objectives of the testing, your budget and time frame in order to identify the most suitable testing approach.

- **White Box Penetration Testing (Authenticated):** Testing is carried out from a position of full knowledge of the application to be tested, including source code. Different levels of authentication are tested during the exercise. White Box testing is very helpful in carrying out extensive penetration testing.
- **Grey Box Penetration testing (Authenticated):** Testing is carried out from a position of limited knowledge of the application to be tested. This allows a tester(s) to focus on areas they think may be of more risk to you and value to a hacker.
- **Black Box Penetration Testing:** Testing is carried out from a position of no knowledge of the application to be tested. By being unaware of the application a tester(s) is dependent on their own reconnaissance, using OSINT and assessment or investigative techniques. While this approach is generally perceived to be a more truthful simulation of a real life hacking campaign, it is carried out under pre-defined time and budget constraints (unlike a real-life malicious attacker) and therefore testing is likely to be less conclusive. This approach is typical suited to static and informational websites with no user login or file upload functionality.

When to Test?

Penetration testing exercises should be conducted regularly, while the frequency will depend on the type of test being done and the reason for the testing, it is recommended testing should be carried out when:

- An existing web application is moved to the cloud.
- An existing web application is moved to an external hosting or development provider.
- New web application, web server or web services are introduced.
- Any significant upgrades or modifications are implemented.
- After web server or CMS security patches are applied.
- After modifications have been made to end user policies.
- After a security breach or incident response is completed.
- In the event of sale or acquisition of the organisation.

Prerequisites

Prior to testing, it is recommended you obtain the following approvals, information, and confirmations.

Sign

- An authority to perform the Web Application Penetration test (this should be signed by the business owner or delegated authority).
- Non-Disclosure Agreement (NDA).

Share

- Target details in accordance with the type of testing.
- Where appropriate - testing authority provided by 3rd party hosting or service provider(s).
- Contact details for a primary and secondary technical point of contact for this activity.
- Contact details for a primary and secondary business point of contact for this activity.
- The escalation or reporting process.
- Test or dummy credentials and dataset to use during this activity.

Confirm

- Ability to perform a full back up the night before the activity.
- Ability to schedule an hourly incremental backup during activity.
- The Incident Response or Disaster Recovery plan that is in place for any unforeseen events.
- The get-out-of-jail-free confirmation to not hold the testing provider or their employees liable for:
    - Any service disruption resulting from this activity.
    - Any attacks, intrusions, breach, or malware outbreaks during this activity, where the testing providers test machine or IP addresses are not the identified source(s).

Approach

A testing provider should be able to demonstrate they have wide ranging experience with complex architecture designs, latest attack techniques, exploits and security flaws. This will allow them to combine complex penetration testing attacks with exclusive forensic techniques to achieve better outcomes. Testing should follow a methodology based on industry standards such as Penetration Testing Execution Standards (PTES) and Open Web Application Security Project (OWASP).

Depending on whether the project entails conducting internal or external testing, the methodology ideally should cover -

- Internal and External - Vulnerability Assessment – using a variety of scanning techniques, and combination of leading open source and commercial tools, a tester should be able to accurately map and assess your web application and web service(s).
- Internal and External - Version Enumeration – Version information is gathered about technologies used by your web application and web service(s).
- Internal and External - Information Exposure – Information leaked form your web application and web service(s) are used to tune attacks so they have a higher success rate.
- Internal and External - Brute Force Attacks – various login form fields are identified. Customised login attempts are automated to compromise accounts with weak or common passwords. This can provide access to user/admin web accounts or even provide full control over your web application or web server.
- Internal and External - Misconfiguration Attacks – Misconfigured widgets, CMS, addon, and APIs are identified and exploited to show how real world attacks are run against your web application and web service(s) to attack your organisation through your own systems.
- Internal and External - Exploitation Planning– Using all the information gathered, vulnerabilities are identified to determine the possible attack vectors to remotely compromise your systems.
- Internal and External - Exploitation – These vulnerabilities are exploited in controlled fashion using a combination of leading exploitation frameworks (including open source and custom made commercial exploit packages) to compromise your systems.
- External - Open Source INTelligence (OSINT) collection – the use of OSINT tools and social media investigation techniques to perform real life reconnaissance mimicking hacking campaigns.

Exploits:

The table below is an example of commercially developed and industry sourced exploits that can be combined for use during each penetration testing exercise. Commercially developed exploits are specially designed to provide a real life Proof of Concept. The best exploits used for ICS / SCADA / Utility targets are often custom developed and not always available to all penetration test providers.

Platform	Exploits (Commercial/Other)	Unique Targets
Windows Server 2016		
Windows 10		
Windows Server 2012 R2		
Windows 8.1		
Windows Server 2012 R2		
Windows 8		
Windows Server 2008 R2		
Windows 7		
Windows Server 2008		
Windows Vista		
Widows Server 2003		
Windows XP		
Widows 2000		
Windows NT 4		
Linux		
Mac OS X		
OpenBSD		
FreeBSD		
Utility/SCADA/ICS		
Metaspolit modules		
Exploit DB-exploits		
Total	**Over 42,000**	**Over 16,000**

The success of any penetration testing exercise depends on a few factors:

1. Experience and skills
2. Type of tools used
3. Level of exploitation capability
4. Level of automated exploitation

Benefits

The benefits of Web Application Penetration Testing:

- Identify your information and vulnerability exposure, these are the details that hackers will use against you and to fine tune their attack techniques for greater impact.
- Better understanding of how the identified issues can be exploited and the practical steps you can take to remediate.
- Assist in saving on remediation costs and reduce application downtime.
- Provides an evidence based demonstration of how an attacker could compromise your web application or web service(s) and the associated business risks.
- Comprehensive reporting for decision makers outlines the security exposures of your web application, web service(s), and web server including high impact recommendations and root causes.
- Allows you to create a tactical action plan detailing how to resolve issues.
- Improve the protection of your business intelligence, data, IT systems, brand and reputation by implementing the remediations and recommendations.
- Build towards compliance with security regulations.

Risks

Web Application Penetration Testing is a simulation of a real life hacking campaign. Therefore, this activity comes with its own set of unique risks and opportunities.

Some of the key risks involved are:

- Disruption or destruction of a target or service due to technical aspects outside of the testing providers reasonable ability to control.
- Disruption or destruction of a target or service due to various test activities conducted by the testing provider. Although this is unlikely due to the type of tests and exploits that we use, it is still a possibility.

Despite the risks, performing penetration testing in a production environment using live systems is recommended and provides the following opportunities:

- Test the target in its actual live environment. This presents an opportunity for you to monitor any service disruption and the effectiveness of perimeter security controls.
- Test your Incident Response plan and Disaster Recovery procedures. This activity is performed in a controlled simulation pattern which provides the unique opportunity for you to test your IR/DR effectiveness and the ability to stop the attack.

Precautions: It is essential that you perform a full backup of the target(s) prior to the test activity, additionally it is strongly recommended that you schedule an incremental hourly backup during the activity. In the unfortunate event of target destruction or disruption, this would allow you to recover from any unintentional outage or system loss with minimal downtime or data loss.

Why Kaon Security?

Kaon Security is a highly specialised information technology security consultancy. Kaon Security team members have a wealth of in-depth technical knowledge and skill sets that allows them to undertake ethical and planned attacks against an organisation's web applications and web servers. Kaon Security employs leading security consultants, and invests in them, through ongoing global training and certification.

The highly experienced Kaon Security penetration test team go beyond the point of initial access or security gap discovery, allowing us to locate additional hidden risks or threats.