nccgroup
freedom from doubt

Web Application Penetration Test Prerequisites

A quick reference guide

Before a web application penetration test is scheduled to start, the company performing the test will contact the client with a set of prerequisites; that is, a list of considerations and configurations that are required before the test can begin. Sadly, the importance of these can be lost in amongst the frenzy of ensuring the system is ready on time, or perhaps because the items listed don't seem necessary.

This document aims to provide you with a quick reference guide to what these considerations and requirements are. Hopefully they will help you in preparing for your web application penetration test and be better equipped to answer any questions that come your way.

Download the full whitepaper on our website which goes into more detail behind the reasons for the prerequisites.

‘The Why Behind Web Application Penetration Test Prerequisites – how you can help us help you secure your web apps‘

at, **www.nccgroup.trust/webapppentestguide**

Security Consulting

The below table aims to lay out the considerations and requirements clearly against the high-level areas your web application penetration test may cover.

High-level Area	Considerations	Requirements
Accounts	Which user levels are in scope?	Two accounts per user level. Spare capacity is recommended.
	Does the application support concurrent logins?	Extra accounts may be required depending on the number of consultants.
	Does the application logic tolerate multiple sessions from the same account?	
	Is there an account lockout policy?	Provide the policy up front.
	Does the application support a wide client base made up of several organisations?	Create a second test organisation, within which one additional account per user level should be configured.
	How are accounts at the various levels created normally?	Follow any processes in place to create the test accounts.
	Does a user log in with anything more than a username and password?	Configure and notify in advance.
Non-account details	Can email addresses and phone numbers be changed by the user?	If not, set up accounts with the consultant's details.
	Is there other information the consultant will need in order to make full use of the site but which would be unreasonable or impossible to know?	Provide in advance.
	Does the site involve taking payment?	If possible, consider how this can be tested without the need for real financial transactions.
Application data	What data is required for the application to work normally? Would any of this be impossible or onerous for the consultant to create?	Configure in advance, preferably with differences between accounts where appropriate.
End-user requirements	Does the application require specific software on the user's machine?	Raise any requirements in advance.
Environment	Are third parties involved?	Ensure authorisation is in place.
Workflows	Does the application demand specialist knowledge to use? Are only specific features in scope?	Create and test workflows to assist the consultant with site navigation and use.
Active defence software	Is a web application firewall (WAF), intrusion detection or prevention system (IDS/IPS) or similar software in use?	Add an exception for the consultant's IP address ranges for the duration of the test.
On-site testing	Is the test on-site?	Consider the logistics of the consultant coming on-site and connecting to the office network.
Contacts	Who could be required to assist?	Brief relevant staff, e.g. those involved in system administration of the site, its business area, or security. Consider how issues should be raised by the consultant and, if necessary, escalated.

For more information from NCC Group, please contact:

NCC Group
Manchester Technology Centre
Oxford Road Manchester M1 7EF

+44 (0) 161 209 5111
response@nccgroup.trust
www.nccgroup.trust