2022 version

GENERIC VULNERABILITY AND PENETRATION TESTING SCOPING QUESTIONNAIRE

hyrrokkin®
WE BUILD BIG BRANDS

Activity Scope

S. No.	Activity	Yes/No/NA	# Of Targets
1	External Web Application Black Box Penetration Testing		
2	External Web Application Grey Box Penetration Testing		
3	Internal Web Application Black Box Penetration Testing		
4	Internal Web Application Grey Box Penetration Testing		
5	External Network Vulnerability Testing		
6	External Network Penetration Testing		
7	Internal Network Vulnerability Testing		
8	Internal Network Penetration Testing		
9	Mobile Application Penetration Testing (iOS & Android)		
10	Webservices/API Penetration Testing		

Generic Questions

S. No.	Questions	Response
1	Briefly describe the objective of conducting this assessment.	
2	Do you want us to re-test after the initial round of bug fixing? If yes, # of targets.	
3	Please specify an approximate timeframe for completing the test.	
4	Will there be any kind of documentation for any of the target applications?	
5	Is the assessment activity conducted as per any compliance requirement? If yes mention which compliance?	

Web Application Vulnerability Assessment / Penetration Testing

S. No.	Questions	Response
1	Any IDS / IPS / WAF in place before the target?	Yes/No/NA
2	Is it possible to configure the IDS / IPS / Firewall /WAF to whitelist our IP addresses?	Yes/No/NA
3	Is it allowed to perform any intrusive or disruptive tests?	Yes/No/NA
4	Is the web application hosted by the client or it is third-party hosting?	Yes/No/NA
5	Is it developed in-house / purchased / custom made through an outsourced partner?	
6	What languages do you use for your web services? (Examples: PHP, Perl, Ruby, ASP, etc.)	
7	What database technologies does your organization use? (Examples – Oracle, Microsoft SQL, IBM DB2, MySQL)	

Grey-box Web Application Penetration Testing

S. No.	Questions	Response
1	The number of roles (users) to be tested.	
2	An approximate number of pages, forms, and input fields.	
3	Do you have WAF (Web Application Firewall) in place?	Yes/No/NA
4	Number of IDS/IPS/Firewalls/WAF	
5	If you have WAF in place, is it possible to configure the WAF to allow scans from our IP addresses? Whitelisting our IP addresses.	Yes/No/NA
6	Is Database intrusive tests are allowed? Like altering database records; etc.	Yes/No/NA
7	Is it allowed to perform any intrusive or disruptive tests? Like denial-of-service test; etc.	Yes/No/NA

8	Are proper database and application backups in place?	Yes/No/NA
9	Does the web application handle sensitive data like a credit card, user personal information, or other PII?	Yes/No/NA

Network Vulnerability Assessment / Penetration Testing

S. No.	Questions	Response
1	Any IDS / IPS in place before the target?	Yes/No/NA
2	Is it possible to configure the IDS / IPS / Firewall to whitelist our IP addresses?	Yes/No/NA
3	Is it allowed to perform any intrusive or disruptive tests?	Yes/No/NA
4	Does any of the targets belong to a part of any public/private cloud?	Yes/No/NA
5	Do any targets belong to DMZ networks?	Yes/No/NA
6	Does your organization use any Remote Access services? (VPN)	Yes/No/NA
7	Are you connected to third-party public cloud services (such as Amazon / Azure / Google)? Mention If yes.	

Mobile Application Vulnerability Assessment / Penetration Testing

S. No.	Questions	Response
1	Which are the platforms used by mobile applications?	
2	Is it possible to configure the IDS / IPS / Firewall to whitelist our IP addresses?	Yes/No/NA
3	Is it allowed to perform any intrusive or disruptive tests?	Yes/No/NA

4	Does the application use Webservice/API as their backend?	Yes/No/NA
5	Do you need to conduct separate comprehensive Webservice/API testing on these backends? If yes, please add it to the Activity Scope table.	Yes/No/NA
6	How many Mobile applications have login/logout functionality?	
7	What type of environment the assessment will be conducted? (Example: production, pre-production, test, development, etc.)	
8	What all platforms were used for the development of the mobile application? (Examples: React, Ionic, Flutter, XCode, etc.)	
9	Will the mobile application work on rooted/jailbroken devices?	Yes/No/NA

Grey-box Mobile Application Penetration Testing

S. No.	Questions	Response
1	The number of roles (users) to be tested.	
2	An approximate number of screens	
3	Do you have WAF (Web Application Firewall) in place?	Yes/No/NA
4	If you have WAF in place, is it possible to configure the WAF to allow scans from our IP addresses? Whitelisting our IP addresses.	Yes/No/NA
5	Are proper database and application backups in place?	Yes/No/NA
6	Does the mobile application handle sensitive data like credit card, user personal information, or other PII?	Yes/No/NA
7	What all platforms were used for development of the mobile application? (Examples: React, Ionic, Flutter, Xcode, etc.)	
8	Will the mobile application work on rooted / jailbroken devices?	Yes/No/NA

Note:

1. Black-box Penetration Testing:

Under this approach, the systems shall be subjected to testing without the credentials given. With the available access towards the target, the vulnerabilities shall be enumerated and exploited. No prior information about the target is given in the approach.

2. Grey-box Penetration Testing:

Under this approach, the systems shall be subjected to testing with the credentials given. In this approach, the credentials shall be used to log into the machine and scan for vulnerabilities. Since the degree of access is greater, the enumeration vulnerabilities shall also be bigger. Also, in this approach, prior information about the server is provided, like database server, firewall device, load balancer; etc.

3. Default Approach:

Wherever there is no mention of the approach of testing, Black-box testing will be conducted as default testing.

4. Whitelisting:

The client will whitelist the IP address provided to them to carry out the assessment. This shall be done prior to the start of the engagement.

5. Application Walkthrough:

For a better quality of assessment during the Grey-box approach, the client shall provide a walkthrough of the application before initiating the assessment.

6. Set of Application Credentials:

For optimum results during a grey box approach, It is recommended to have two sets of user credentials for each user role (user privilege).