WebApp Penetration Test

Scope

Deliver a penetration test for internet-facing application and a test report highlighting the findings in a priority and risk focus with recommended remediation actions.

Maximum Numbers:

1x Internet-Facing application

Small: Several webpages with fill-in forms.

Medium: Several webpages with user authentication.

Large: Many pages front-end with user authentication and administrative backend.

Either Black Box (unauthenticated) or White Box (authenticated).

Backend database servers will be tested through the application itself, not the database server directly so there are no maximum numbers of database servers.

Benefits/Outcomes

Awareness for strengths and weaknesses of the application, understanding of how the web application behaves under testing, risk rated vulnerabilities and recommendations on how to resolve the vulnerabilities.

The testing is aligned to the CIA triad (Confidentiality, Integrity and Availability).

Assumptions

- Customer will not make any changes to the WebApp content or configuration during the testing window
- All delivery will be remote
- Any remediation work is out of scope of this engagement however we can help via a follow-on engagement.

Deliverables

- Testing workshop with the customer to identify the testing approach per the scope
- Perform the penetration test

  Discovery - The tester will attempt to obtain information about the web application. This information will be used in the next steps

  Enumeration - The tester will examine how to obtain the information from the found systems in the best way possible and what the best attack method is to compromise the systems. It is checked whether there are vulnerabilities that can be exploited.

  Testing - The tester will look at specific application vulnerabilities. For example: injection or cross-side scripting techniques.

  Exploitation - The tester proceeds to attack systems with the aim of compromising the system, extracting or modifying data or (theoretically) making the service unavailable.

- Produce a report containing:
  - Timeframe of testing
  - Source IP addresses used for executing the tests
  - The test results in priority and risk ordering
  - Recommended remediations
- Deliver a review workshop to review the test findings and recommended remediations

Cost

Small – Black-box:	£2,315
Medium – Black-box:	£3,830
Medium – White-box:	£4,595
Large – Black-box:	£6,130
Large – White-box:	£7,660

*Hours/Prices might vary in mutual agreement after the intake to ensure we can deliver a quality test.

Optional Items

- Re-test after remediation of findings: 10% of test price
- Onsite testing: Depending on duration of test

Get an email quote

If you are interested in our Web Application Penetration Test service, please don't hesitate to let us know. You can either request an email quote that is personalised to what you need, or you can arrange a call with a member of our team. Please choose an option below:

Email quote

Arrange call

About Tesrex

We're a team of Cisco specialised IT consultants and solution providers based in London. Our goal is to accelerate the adoption of next-generation technologies in the organisations we work with. Everything we do at Tesrex comes down to our ethos; Design. Deliver. Nurture. This core ethos shapes every experience our clients have while working with us.

As a company, our roots first sprouted in San Francisco, USA before we started working in the UK in 2016. Since then we have built a highly-skilled team with diverse knowledge so we can efficiently solve any challenge a customer presents to us and exceed expectations.

Want to talk? Reach out!

Tesrex Ltd.
27A Church Street,
Rickmansworth,
Hertfordshire,
WD3 1DE

☎ 01923 77 66 44

✉ solutions@tesrex.com