

ინტერესის გამოხატვა ფინკა ბანკი საქართველოს IT სისტემებზე შეღწევადობის (PENETRATION TEST) ტესტირების ჩატარების თაობაზე

სს „ფინკა ბანკი საქართველო“ საერთაშორისო საფინანსო ჰოლდინგის ნაწილია. ჰოლდინგში ფინკას პარტნიორები არიან საერთაშორისო საფინანსო კორპორაცია (IFC, World Bank Group), KfW Bankengruppe, FMO, გერმანიის განვითარების ბანკი, ნიდერლანდების განვითარების ბანკი, responsAbility GLobal Microfinance Fund, Triple Jump და სხვა საერთაშორისო საფინანსო ორგანიზაციები.  ფინკა ბანკის სერვისცენტრების ქსელი საქართველოს თითქმის ყველა რეგიონს მოიცავს.

სს ფინკა ბანკი საქართველო ახორციელებს საქმიანობას უმაღლესი ეთიკური და პროფესიული სტანდარტების მიხედვით და ბანკის შიდა წესების მიხედვით, ბანკის თანამშრომელს და/ან მასთან დაკავშირებულ პირს არ შეიძლება ჰქონდეს პირდაპირი ან არაპირდაპირი ფინანსური ინტერესი ბანკის რომელიმე კონტრაჰენტთან (ინტერესთა კონფლიქტი). აღნიშნულის გათვალისწინებით, ტენდერში მონაწილე კომპანიასა და ბანკის თანამშრომელს და/ან მათთან დაკავშირებულ პირებს შორის არ უნდა არსებობდეს ინტერესთა კონფლიქტი.

## მიზანი

* #1: ბანკის საინფორმაციო ტექნოლოგიების გარემოში უსაფრთხოების ტიპის სისუსტეების აღმოჩენა
* #2: ეროვნული ბანკის მოთხოვნის/რეგულაციის შესრულება

## პროექტის საზღვრები

პროექტის ფარგლებში მოხდება IT გარემოს სკანირება და სისუსტეების იდენტიფიცირება. ინფრასტრუქტურის არქიტექტურის/დიზაინის შესწავლა და უსაფრთხოების მიღებული პრაქტიკების შემოთავაზება. აღმოჩენილი დაუცველობის (vulnerability) კრიტიკულობის შეფასება და რისკის დონის განსაზღვრა, იმის მიხედვით თუ რა გავლენა აქვს ბიზნესზე.

* გამოყენებული მეთოდოლოგიის აღწერა;
* ტესტირება უნდა მოხდეს გარე პერიმეტრზე არსებული სისტემებისთვის (External Penetration Test);
* არსებული დაუცველობების იდენტიფიცირება და მათი გამოყენების შესაძლებლობის ანალიზი;
* დაუცველობის გამოყენების შესაძლებლობის დასაბუთება;
* რისკების შეფასება ტესტირებად აპლიკაციებთან მიმართებაში;
* რეკომენდაციების წარმოდგენა დაფიქსირებული რისკების აღმოსაფხვრელად.
* ექსპერტული შეფასება და კონსულტაცია ინფრასტრუქტურის დიზაინის და მისი კომპონენტების უსაფრთხოებაზე.

შესაფასებელი კომპონენტები:

* ინტერნეტნ ბანკი
* Mobile bank
* Microsoft Exchange - OWA
* Corporate website
* ქსელური მოწყობილობები:
  + Remote VPN
  + Internet Router
  + Internet Firewall

ოფციის სახით და ცალკე განფასებით ველით შემოთავაზებას:

* Social Engineering (Mail Phishing);
* ოფისის უსადენო ქსელური ინფრასტრუქტურის შეფასება და სისუსტეების აღმოჩენა.

შენიშვნა:

* ინტერნეტ ბანკი და მობაილ ბანკი ასევე დაიტესტება მომხმარებლის პანელიდან;
* გამოყებულ იქნება მხოლოდ Black / Gray box ტიპის ტესტირება.

# შეღწევადობის ტესტირება

ბანკის შესაბამისი პასუხისმგებელი თანამშრომლები წინასწარ უნდა იყვნენ გაფრთხილებულნი ტესტირების დაწყებამდე მათ მიერ შესასრულებელი მოსამზადებელი სამუშაოების შესახებ.

## ტესტირების სცენარები

შეღწევადობის ტესტირება უნდა მოიცავდეს მინიმუმ შემდეგ ნაბიჯებს:

1. მოკვლევა და აღწერა
2. ქსელის კომპონენტების შეფასება და სერვისების იდენტიფიცირება
3. ქსელის შეღწევადობის ტესტირება
4. პაროლების მოპოვება
5. ტესტირება ხელით / OWASP მეთოდოლოგია
   1. წვდომის კონტროლი
   2. აუტენტიფიკაცია
   3. სესიის მართვა
   4. კონფიგურაციები / ვებ-აპლიკაციების არქიტექტურის გადახედვა
   5. შეცდომების დამუშავება
   6. მონაცემების დაცვა

## პრეტენდენტის შეფასება და შერჩევა

კონკურსში მონაწილეობაზე დაინტერესებულმა ყველა ორგანიზაციამ საკუთარი წინადადებები და პრეზენტაციები უნდა წარმოადგინონ დალუქული კონვერტით ფინკა ბანკის სათავო ოფისში. ვაჟა -ფშაველას 71, ბლოკი 1, სართული 3, ოფისი 12; **არაუგვიანეს 2017 წლის 19 აპრილისა, მაქსიმუმ 18:00 საათამდე.** შემოსული წინადადებების განხილვის შემდგომ ჩატარდება გასაუბრება შერჩეულ პრეტენდენტებთან და გამოვლინდება გამარჯვებული.

ყველა პრეტენდენტ კომპანიას გაეგზავნება შეტყობინება კონკურსის საბოლოო შედეგების შესახებ (მითითებულ ელ.ფოსტაზე).

**პრეტენდენტებმა უნდა წარმოადგინონ შემდეგი სახის დოკუმენტაცია რაც წარმოადგენს საბოლოო შერჩევის ძირითად კრიტერიუმებს:**

* გამოცდილება აღნიშნული მომსახურების სფეროში:
  + შემსრულებელ ორგანიზიციას უნდა გააჩნდეს ინფორმაციული უსაფრთხოების სფეროში მოღვაწეობის მინიმუმ 5 წლიანი გამოცდილება და წარმოადგინოს შესრულებული პროექტების რაოდენობა, მასშტაბი და კატეგორია.
  + მინიმუმ 1 სარეკომენდაციო წერილი, მსგავსი პროექტის წარმატებით შესრულების შესახებ.
* სამუშაოს შესრულების ვადები;
* შესრულების ღირებულება დეტალურად. (Social Engineering და WIFI ტესტირების საფასური უნდა გამოყოფილი იყოს ცალკე);
* შემსრულებელს მუდმივ შტატში უნდა ყავდეს შესაბამისი სერტიფიცირებული სპეციალსტები(OSCP,CCIE/CCNP Security,CPTE, ა.შ.). შემსრულებელმა უნდა წარმოადგინოს სერტიფიკატების ჩამონათვალი და შტატში მყოფი სერტიფიცირებული სპეციალისტების რაოდენობა.

## ანგარიშგება

საბოლოო ანგარიში წარდგენილი უნდა იყოს ინგლისურ ენაზე და მოიცავდეს მინიმუმ შემდეგ ნაწილესბს:

* შეჯამება (Executive Summary);
* რისკების ანალიზი;
* რეკომენდაციები;
* ჩატარებული სამუშაოების დეტალური აღწერა;

შემსრულებელმა ასევე უნდა ჩაუტაროს ბანკის წარმომადგენლებს პრეზენტაცია აღმოჩენილი სისუსტეების და მათი აღმოფხვრის გზების შესახებ, ფინკა ბანკის სათავო ოფისში.

შემსრულებელი ვალდებულია ტესტირების პერიოდში კრიტიკული რისკის, სისუსტის აღმოჩენის შესახებ დაუყოვნებლივ აცნობოს დამკვეთს და არ დაელოდოს პროექტის დასრულებას.

დამატებითი შეკითხვების არსებობის შემთხვევაში მოგვწერეთ ელექტრონულ ფოსტაზე: [procurement@finca.ge](mailto:procurement@finca.ge)