RADICALLY OPEN SECURITY B.V.

OFFER

PENETRATION TESTING SERVICES

FOR

SITTING DUCK B.V.

July 8, 2016

INTRODUCTION

Sitting Duck B.V. (hereafter “**Sitting Duck**”), with its registered office at Reed Street 42, Pond City, Amazonia, has requested Radically Open Security B.V. (hereafter “**ROS**”) to perform penetration testing services. Motivation for this request is that Sitting Duck wishes to get a better insight in the security of their webservers and the FishInABarrel Web Application.

This offer sets out the scope of the work and the terms and conditions under which ROS will perform these services.

PROJECT OVERVIEW

ROS will perform penetration testing services for Sitting Duck of the systems described below. The services are intended to gain insight into the security of these systems. To do so, ROS will access these systems, attempt to find vulnerabilities, and gain further access and elevated privileges by exploiting any vulnerabilities found.

ROS will test the following targets (the “**Targets**”):

- target1.sittingduck.com
- target2.sittingduck.com
- FishInABarrel App

ROS will test for the presence of the most common vulnerabilities, using both publicly available vulnerability scanning tools and manual testing. ROS shall perform a 10-day, crystal-box, intrusive test via the internet.

PREREQUISITES

In order to perform this audit, ROS will need access to:

- Test accounts
- Test environment

- Contact information of system administrators, in case of emergencies

DISCLAIMER

It is possible that in the course of the penetration testing, ROS might hinder the operations of the Targets or cause damage to the Targets. Sitting Duck gives permission for this, to the extent that ROS does not act negligent or recklessly. Sitting Duck also warrants it has the authority to give such permission.

It is important to understand the limits of ROS's services. ROS does not (and cannot) give guarantees that something is secure. ROS, instead, has an obligation to make reasonable efforts (in Dutch: "*inspanningsverplichting*") to perform the agreed services.

ROS and Sitting Duck agree to take reasonable measures to maintain the confidentiality of information and personal data they gain access to in the course of performing the penetration test within the Targets. Both parties will use the information and data they receive or access only for the purposes outlined in this agreement. ROS warrants that all core-team members, external freelancers, and volunteers it engages to perform the penetration test have signed a non-disclosure agreement (NDA).

PENTEST METHODOLOGY

During the execution of penetration tests, Radically Open Security B.V. broadly follows the following steps:

1. Requirements Gathering and Scoping;
2. Discovery;
3. Validation;
4. Information Collection;
5. Threat and Vulnerability Analysis;
6. Exploitation;
7. Reporting;

Step 1: Requirements Gathering and Scoping
The expectations of both parties are discussed and agreements are made regarding how to conduct the test(s). For example, contact details and the pentest's scope are documented.

Step 2: Discovery

As much information as possible about the target organization and target objects is collected. This information is passively gathered, primarily from public sources.

Step 3: Validation
All customer-specified systems are cross-referenced with findings from the Discovery step. We do this to ensure that discovered systems are legal property of the customer and to verify the scope with the customer.

Step 4: Information Collection
Information from Step 2 is now used to actively collect information about the system. Activities conducted during this phase may include: Determining which parts of the various components will be investigated; Testing for the presence of known vulnerabilities, using automated tests; Identifying the offered services and fingerprinting the software used for them.

Step 5: Threat and Vulnerability Analysis
Potential threats and vulnerabilities are indexed, based upon the collected information.

Step 6: Exploitation
Attempt to use vulnerabilities of the various components. The diverse applications and components of the client's infrastructure are relentlessly probed for frequently occurring design, configuration, and programming errors.

Note: Radically Open Security B.V. uses open-source scanning tools to get its bearings, but generally performs most of the exploitation by hand.

Step 7: Reporting
After finishing the audit, a report will be delivered where the step-by-step approach, results, and discovered vulnerabilities are described. The report and results will be presented to the responsible project leader or manager at the client's office.

Steps 4-6 may be repeated multiple times per test. For example, access may be acquired in an external system, which serves as a stepping-stone to the internal network. The internal network will then be explored in Steps 4 and 5, and exploited in Step 6.

CODE AUDIT

ROS will perform a code audit to aid pentesting. During a code audit, we manually examine the code of an application to ensure there are no security vulnerabilities and use our understanding of the code to guide our pentesting. If vulnerabilities are found, we document those and suggest ways to fix them. This is done by highly-trained penetration testers who can both review the raw code as well as interpret the findings of the automated scans, putting them into context.

During the code audit portion of penetration tests, we take the following criteria into account:

1. Risk Assessment and "Threat Modeling"
   In this step, we analyze the risks of a particular application or system. Threat Modeling is a specific, structured approach to risk analysis that enables us to identify, qualify, and address the security risks, thus dovetailing with the Code Review process. For example, user data is sacred. We focus on encrypted storage, discover if Sitting Duck employees have a backdoor into data, and cut loose stolen devices by wiping them remotely and revoking accounts.
2. Purpose and Context
   Here we focus on risks, especially in the quick and easy sharing of internal documents and itineraries. Account details aren't so secret when we know who will be in meetings, but what's being discussed is secret.
3. Complexity
   The complexity of the system is in the frameworks that support the web application. We'd ignore those and focus only on the custom code and backend code. We would also focus on implementation mistakes and known flaws in the systems. For example, we'd ensure you're using the latest versions of software, but we wouldn't delve into the framework itself. Since we assume the code is written by a team, it should be clearly-written code. If you have several full-release versions, there will undoubtedly be several revisions and audits on that code.

For more information, please refer to this link: https://www.owasp.org/index.php/OWASP_Code_Review_V2_Table_of_Contents

TEAM AND REPORTING

TEAM

ROS may perform the activities with its core-team members, external freelancers, and/or volunteers.

First point of contact for this assignment shall be:

- Melanie Rieback (ROS)
- Sir Knowsalot (Sitting Duck)

Our penetration tests are run a bit like a Capture The Flag (CTF) competition: Radically Open Security B.V. has a geographically distributed team and we use online infrastructure (RocketChat, GitLabs, etc.) to coordinate our work. This enables us to invite the customer to send several technical people from their organization to join our penetration test team on a volunteer basis. Naturally, we extend this invitation to Sitting Duck as well.

Throughout the course of the audit, we intend to actively brainstorm with Sitting Duck about both the penetration test and the process. This is a continuous learning experience for both us and you. Also, in our experience, a tight feedback loop with the customer greatly improves both the quality and focus of the engagement.

REPORTING

ROS will report to Sitting Duck on the penetration test. This report will include the steps it has taken during the test and the vulnerabilities it has found. It will include recommendations but not comprehensive solutions on how to address these vulnerabilities.

A sample Pentest report can be found here

- https://github.com/radicallyopensecurity/templates/blob/master/sample-report/REP_SittingDuck-pentestreport-v10.pdf

One of ROS's Core Principles is the Teach To Fish principle – otherwise known as the 'Peek over our Shoulder' (PooS) principle. We strive to structure our services so they can also serve as a teaching or training opportunity for our customers.

PLANNING AND PAYMENT

ROS will uphold the following dates for the planning of the services:

- ROS performs a penetration test on August 1st, 2016, lasting until August 13th, 2016.
- ROS delivers the final report August 26th, 2016.

Our fixed-fee price quote for the above described penetration testing services is € 1,000,000.- excl. VAT and out-of-pocket expenses. ROS will send an invoice after completion of this assignment. Sitting Duck will pay the agreed amount within 30 days of the invoice date.

Any additional work will be charged separately. An hourly rate for additional work will be agreed upon before starting this work.

ABOUT RADICALLY OPEN SECURITY B.V.

Radically Open Security B.V. is the world's first not-for-profit computer security consultancy. We operate under an innovative new business model whereby we use a Dutch fiscal entity, called a “Fiscaal Fondswervende Instelling” (Fiscal Fund raising Institution), as a commercial front-end to send 90% of our profits, tax-free, to a not-for-profit foundation, Stichting NL net. The NLnet Foundation has supported open-source, digital rights, and Internet research for almost 20 years.

In contrast to other organizations, our profits do not benefit shareholders, investors, or founders. Our profits benefit society. As an organization without a profit-motive, we recruit top-name, ethical security experts and find like-minded customers that want to use their IT security budget as a "vote" to support socially responsible entrepreneurship. The rapid pace of our current growth reflects the positive response the market has to our idealistic philosophy and innovative business model.

Radically Open Security B.V. has a number of values that we describe as our “Core Principles.” These are:

- **No sketchy stuff**
  We don't build surveillance systems, hack activists, sell exploits to intelligence agencies, or anything of the sort. If a job is even remotely morally questionable, we simply won't do it.
- **Open-Source**
  Releasing ALL tools and frameworks, we build as open-source on our website.
- **Teach to fish**
  During engagements, we will not only share our results with your company, but also provide a step-by-step description of how to perform the same audit or procedure without us. We want to demystify what we're doing. It's not rocket science, and we genuinely want to help your company improve its security posture, even if it costs us repeat business.
- **IoCs for free**
  Releasing ALL collected threat intelligence (Indicators of Compromise) into an open-source database that everyone can freely use. (Sanitized in agreement with customers.)
- **Zero days**
  We don't sell zero-days - we responsibly disclose them!

For more information about Radically Open Security B.V., we refer you to our website: www.radicallyopensecurity.com.

TERMS AND CONDITIONS

ROS will only perform the penetration test if it has obtained the permission from Sitting Duck B.V. and HotshotDevs Inc. as set out in the penetration testing waiver, attached as **Annex 2**, or provided in a separate document.

ROS performs this assignment on the basis of its general terms and conditions, which are attached to this offer as Annex 1. ROS rejects any general terms and conditions used by Sitting Duck.

In order to agree to this offer, please sign this letter in duplicate and return it to:

Melanie Rieback
Radically Open Security B.V.
Overdiemerweg 28
1111 PP Diemen
melanie@radicallyopensecurity.com

SIGNED IN DUPLICATE

July 8, 2016 Pond City I.M. Portant **Sitting Duck B.V.**	July 8, 2016 Amsterdam Melanie Rieback **Radically Open Security B.V.**

ANNEX 1
GENERAL TERMS AND CONDITIONS

What is this document?

These are the general terms and conditions (in Dutch: “*algemene voorwaarden*”) of Radically Open Security B.V. (ROS). This version of the general terms and conditions is dated 15 July 2014.

In the spirit of ROS's philosophy, ROS wants these general terms and conditions to be as understandable as possible. If you have any questions, feel free to ask for clarification.

What is Radically Open Security B.V.?

ROS is a private limited liability company under Dutch law located in Amsterdam, The Netherlands. It is registered at the Dutch Chamber of Commerce under no. 60628081.

To what do these terms and conditions apply?

These general terms and conditions apply to all agreements between ROS and the customer. ROS rejects any terms and conditions used by the customer. The parties can only deviate from these general terms and conditions in writing. These general terms and conditions are also intended to benefit any person employed or engaged by ROS during the performance of an assignment.

How does ROS agree on an assignment?

ROS wants both parties to have a clear picture of an assignment before it starts. This means there only is an agreement between ROS and the customer after ROS sends a written offer containing the key terms of the agreement and the customer subsequently accepts the offer. Communications other than the written offer do not form part of the agreement. ROS can rescind an offer until it is accepted by the customer.

What can the customer expect from ROS?

It is important to understand the limits of ROS's services. ROS does not (and cannot) give guarantees that something is secure. ROS instead has an obligation to make reasonable efforts (in Dutch: “*inspanningsverplichting*”) to perform the agreed services.

ROS will make reasonable efforts to perform the assignment in accordance with the plan set out in the offer (if any). If ROS expects it will not fulfill the plan as documented, it will let the customer know without delay. ROS is not automatically deemed to be in default if it doesn't meet the plan.

ROS will make reasonable efforts to avoid disruption of the customer's operations and damage to its owned or operated systems, but it cannot guarantee that this will be avoided. The customer agrees to this. ROS is not obliged to restore the systems or recover any data deleted or amended in the course of the assignment.

What can ROS expect from the customer?

The customer will provide ROS with all means necessary to allow ROS to perform the agreed services. If ROS needs explicit permission from the customer to perform its services (for example, when doing penetration tests) the customer gives this permission. The customer also warrants that it has the legal authority to give this permission.

How do the parties handle confidential information?

ROS and the customer will not disclose to others confidential information and personal data they receive from each other or gain access to in the course of an assignment. ROS has the right to disclose this information and data to persons engaged by ROS, but only if these persons have a similar confidentiality obligation vis-á-vis ROS. Any person will only use the information and data it receives or gains access to for the purposes following from the agreement. Both parties will take reasonable measures to maintain the confidentiality of the information and data they received or gained access to, and will ensure that persons engaged by them do the same.

What does ROS do with vulnerabilities it finds in the course of an assignment?

If ROS in the course of an assignment finds a vulnerability which might affect the customer, it will report this to the customer. If a vulnerability might affect third parties as well, ROS retains the right to disclose this vulnerability also to others than the customer. It will only do so after having given the customer a reasonable period to take measures minimising the impact of the vulnerability, in line with responsible disclosure best practices.

What does ROS do with indicators of compromise it finds?

If ROS in the course of an assignment finds indicators of compromise, such as malware signatures and IP-addresses, it will report this to the customer. ROS retains the right to also publish this information in a publicly accessible database. It will only do so after it has given the customer the opportunity to object to the publication of data which would negatively impact the customer.

Who owns the products developed in the course of the assignment?

ROS retains any intellectual property rights in products developed for an assignment, such as software and reports. ROS, however, wants to teach as many customers as possible 'how to fish'.

For software it developed, this means that ROS gives the customer a permanent, non-exclusive, transferable, sub-licensable, worldwide license to distribute and use the software in source and binary forms, with or without modification (very similar to the BSD-license). If ROS's software is based on other software which is provided under a license which restricts ROS's ability to license its own software (such as the GPLv3 license), the more restrictive license will apply.

For other products it developed, such as reports and analyses, ROS gives the customer the same license, but this license is exclusive to the customer and does not contain the right to modification. The latter condition is intended to ensure that the customer will not change ROS's products, such as reports and analyses. ROS retains the right to reuse these products, for example for training and marketing purposes. ROS will remove any confidential information from these products before publication.

ROS retains title to any property transferred to the customer until all outstanding payments by the customer have been done in full (in Dutch: "*eigendomsvoorbehoud*"). ROS also only gives a license after all outstanding payments have been done in full.

Who will perform the assignment?

ROS has the right to appoint the persons who will perform the assignment. It has the right to replace a person with someone with at least the same expertise, but only after having consulted with the customer. This means that section 7:404 Dutch Civil Code (in Dutch: "*Burgerlijk Wetboek*") is excluded.

Due to the nature of ROS's business, ROS regularly works with freelancers for the performance of its assignments. ROS has the right to engage third parties, including freelancers, in the course of the performance of an assignment.

ROS wants to be able to use the expertise of its entire team to help with an assignment. This means that in the course of an assignment, it is possible that the persons performing the assignment will consult with and be advised by others in ROS's team. These others will of course be bound by the same confidentiality obligations as the persons performing the assignment.

What happens when the scope of the assignment is bigger than agreed?

ROS and the customer will attempt to precisely define the scope of the assignment before ROS starts. If during the course of the assignment, the scope turns out to be bigger than expected, ROS will report this to the customer and make a written offer for the additional work.

How is payment arranged?

All amounts in ROS's offers are in Euros, excluding VAT and other applicable taxes, unless agreed otherwise.

For assignments where the parties agreed to an hourly fee, ROS will send an invoice after each month. For other assignments, ROS will send an invoice after completion of the assignment, and at moments set out in the offer (if any). The customer must pay an invoice within 30 days of the invoice date.

ROS may, prior to an assignment, agree on the payment of a deposit by the customer. ROS will settle deposits with interim payments or the final invoice for the assignment.

If the payment is not received before the agreed term, the client will be deemed to be in default without prior notice. ROS will then have the right to charge the statutory interest (in Dutch: "*wettelijke rente*") and any judicial and extrajudicial (collection) costs (in Dutch: "*gerechtelijke- en buitengerechtelijke (incasso)kosten*").

If the customer cancels or delays the assignment two weeks before it starts, ROS is entitled to charge the customer 50% of the agreed price. If the customer cancels or delays the assignment after it already started, ROS is entitled to charge the customer 100% of the agreed price. ROS is entitled to charge a pro rata percentage in the case of cancellation or delay shorter than two weeks before the start of the assignment (i.e. a cancellation one week before the assignment would entitle ROS to charge 75% of the agreed price).

For what can ROS be held liable?

Any liability of ROS resulting from or related to the performance of an assignment, shall be limited to the amount that is paid out in that specific case under an applicable indemnity insurance of ROS, if any, increased by the amount of the applicable deductible (in Dutch: "*eigen risico*") which under that insurance shall be borne by ROS. If no amount is paid out under an insurance, these damages are limited to the amount already paid for the assignment, with a maximum of EUR 10.000. Each claim for damages shall expire after a period of one month from the day following the day on which the customer became aware or could reasonably be aware of the existence of the damages.

To make things clear, ROS is not liable if a person associated with ROS acts contrary to any confidentiality or non-compete obligation vis-á-vis the customer or a third party, this person might have agreed to in another engagement.

What happens when third parties lodge a claim or initiate criminal proceedings against ROS?

The customer shall indemnify ROS and any person employed or engaged by ROS for any claims of third parties which are in any way related to the activities of ROS and any person employed or engaged by ROS for the customer.

Should a third party lodge a claim against ROS or any of the consultants it engaged or employed as a result of the performance of the assignment for the customer, then the customer will co-operate fully with ROS in defending against this claim, including by providing to ROS any evidence it has which relates to this claim. Should the public prosecutor initiate an investigation or criminal proceedings against ROS or any of the consultants it engaged or employed as a result of the performance of the assignment for the customer, then the customer will also co-operate fully with ROS in defending against this investigation or proceedings, including by providing any evidence it has which relates to this investigation or these proceedings.

The customer shall reimburse ROS and any person employed or engaged by ROS all costs of legal defence and all damages in relation to these claims, investigations or proceedings. This provision does not apply to the extent a claim, investigation, or proceeding is the result of the intent or recklessness (in Dutch: “*opzet of bewuste roekeloosheid*”) of ROS or a person employed or engaged by ROS.

When is this agreement terminated and what happens then?

Each of the parties may terminate the agreement wholly or partly without prior notice if the other party is declared bankrupt or is being wound up or if the other party's affairs are being administered by the court (in Dutch: “surséance van betaling”).

When can ROS not be expected to perform the assignment?

In the case of force majeure (in Dutch: “*overmacht*”) as a result of which ROS cannot reasonably be expected to perform the assignment, the performance will be suspended. Situations of force majeure include cases where means, such as soft- and hardware, which are prescribed by the customer do not function well. The agreement may be terminated by either party if a situation of force majeure has continued longer than 90 days. The customer will then have to pay the amount for the work already performed pro rata.

Which law applies and which court is competent?

Dutch law applies to the legal relationship between ROS and its customers. Any dispute between ROS and a customer will be resolved in the first instance exclusively by the District Court (in Dutch: “*rechtbank*”) of Amsterdam, the Netherlands.

ANNEX 2

PENETRATION TEST - WAIVER

***Sitting Duck B.V.* (*Sitting Duck*)**, with its registered office at Reed Street 42, Pond City, Amazonia and duly represented by **B.I.G. Wig**

WHEREAS:

A. Sitting Duck wants some of its systems to be tested, Radically Open Security B.V. ("ROS") has offered to perform such testing for Sitting Duck and Sitting Duck has accepted this offer. The assignment will be performed by ROS' core-team members, external freelancers, and/or volunteers (the "Consultants").

B. Some of the activities performed by ROS and the Consultants during the course of this assignment could be considered illegal, unless Sitting Duck has given permission for these activities. ROS and the Consultant will only perform such activities if they have received the required permission.

C. Sitting Duck is willing to give such permission to ROS, the Consultants and any other person ROS might employ or engage for the assignment.

DECLARES AS FOLLOWS:

1. Sitting Duck is aware that ROS will perform penetration testing services of the following systems of Sitting Duck, as described below. The services are intended to gain insight in the security of these systems. To do so, ROS will access these systems, attempt to find vulnerabilities and gain further access and elevated privileges by exploiting any vulnerabilities found. ROS will test the following targets (the "**Targets**"):

- target1.sittingduck.com
- target2.sittingduck.com
- FishInABarrel App

2. Sitting Duck hereby grants ROS and the Consultants on a date to be confirmed by email the broadest permission possible to perform the assignment, including the permission to:

a. enter and use the Targets;

b. circumvent, breach, remove and turn off any security measures protecting the Targets;

c. copy, intercept, record, amend, delete, render unusable or inaccessible any data stored on, processed by or transferred via the Targets; and

d. hinder the access or use of the Targets,

but Sitting Duck only grants the permission for these activities to the extent that (i) such activities are necessary to perform the assignment and (ii) such activities do not disrupt the normal business operations of Sitting Duck.

3. The permission under Article 1 extends to all systems on which the Targets run, or which ROS or the Consultant might encounter while performing the assignment, regardless of whether these systems are owned by third parties.

4. Sitting Duck warrants that it has the legal authority to give the permission set out under Articles 1 and 2. It also warrants it has obtained the necessary permissions from any third parties referred to under Article 3.

5. Should the public prosecutor initiate an investigation or criminal proceedings against ROS or any of the consultants it engaged or employed as a result of the performance of the assignment for the customer, then Sitting Duck will co-operate fully with ROS in defending against this investigation or proceedings, including by providing any evidence it has which relates to this investigation or these proceedings.