LiU TopDog Challenge 2017

TSIT01, TSIT02 Computer Security
Linköping University

Jonathan Jogenfors
Information Coding Group
Department of Electrical Engineering, Linköping University

November 13, 2017
About this document

This lab memo is intended for the computer security courses TSIT01 and TSIT02 for Master-level students at Linköping University.

Changelog

2017 Revised for the 2017 course.
2016 Initial version.

Acknowledgements

This lab owes its existence to Anders Mårak Leffler who brought this software to my attention back in 2015. I also want to thank the OWASP Foundation and the OWASP chapter in Gothenburg for help with getting started. Thanks to the LiU IT department who was willing to set up and support a web application server that, contrary to all common sense and in violation of probably a dozen IT policies, contains all kinds of web vulnerabilities. Also thanks to Niklas Johansson for helping me get all the lab details straight and, of course, prof. Jan-Åke Larsson, who gave us the go-ahead to build what is probably going to be a very interesting lab course.

Linköping, November 2016
Jonathan Jogenfors
# Contents

1 Introduction ........................................ 4  
   1.1 Overview ........................................ 4  
   1.2 Lab organization ................................. 4  
   1.3 Deadline ........................................ 5  
   1.4 Disciplinary stuff ............................... 5  
   1.5 Ethics ........................................... 5  
   1.6 Contact information .............................. 5  
      1.6.1 TSIT01 Datasäkerhetsmetoder .......... 5  
      1.6.2 TSIT02 Computer Security ............... 5  

2 Preparing for the lab .............................. 6  
   2.1 Lab group ....................................... 6  
   2.2 User account registration ...................... 6  

3 Performing the Lab .................................. 8  
   3.1 Assignments ..................................... 8  
   3.2 Result keys ..................................... 8  
   3.3 Finishing the lab ................................ 8  
   3.4 Best Practices .................................. 9  
   3.5 Scoreboard ...................................... 9  
   3.6 List of lessons .................................. 12  
   3.7 List of assignments .............................. 12  

4 Frequently Asked Questions (FAQ) ............... 14  
   4.1 There is something wrong with the server! .. 14  
   4.2 How do I create a TopDog account? ............ 14  
   4.3 How can I get bonus points for the exam? ... 14  
   4.4 What happens if I can't go to the coaching session? .................. 14  
   4.5 I finished the lab and want something more challenging! .......... 15  
   4.6 I don't get a result key, only “Key Should be here! Please refresh the home page and try again! If that doesn't work, sign in and out again!” . 15  
   4.7 The result key in insecure crypto challenges isn't working! ....... 15  
   4.8 In the Insecure Direct Object Reference Bank challenge, there's no money left ............................... 15  
   4.9 I found a typo or have a suggestion for this lab PM! .............. 15  
   4.10 I love computer security and I am looking for thesis work! ........ 15
A Tools

A.1 Viewing the source code .................................................. 16
A.2 The Zed Attack proxy (ZAP) ............................................. 16
  A.2.1 Configuring ZAP .................................................. 18
  A.2.2 Intercepting HTTP(S) traffic with ZAP ....................... 19

B Capturing The Flag .......................................................... 24
Chapter 1

Introduction

Have you ever taken a computer security course and wanted to learn more? Tired of just listening to the lecturer going on about hacking computers while you dream about actually breaking into stuff? Now is your chance. In this lab course you will be taking on the role as penetration tester, or pentester for short. This means you’ll be shown a selection of vulnerable web applications with the goal of breaking into them and/or make the application perform tasks that it was not designed for.

1.1 Overview

In the LiU TopDog 2017 challenge you will practice penetration testing. Using a set of increasingly difficult assignments, you will gradually learn the basics of how an adversary might exploit badly designed applications and security systems. The goal is to give you the basics in practical security work and understand some common pitfalls when developing web applications. After the lab you should be well-equipped to avoid these security issues whenever you develop your own web application.

1.2 Lab organization

This lab will run for the entire duration of the course, from the start of the lab to the end of the exam period. The lab system is publicly available and you can work on the assignments in your own time on the lab computers or your personal laptops. The progress will be stored on the server so you can come back at any time.

There are scheduled sessions, but the idea is that you try to solve as much as possible on your own and if you get stuck you can book yourself up for a sessions. In other words you should think of theses session as time-slots where the assistant is available for questions, and not as sessions where you go and perform the lab from start to finish. In order to get the most out of these coaching sessions, make sure you prepare well for the sessions. The coaching session will be attended by a large number of students, so the lab assistant won’t be able to spend too much time giving individual help. Instead, prepare some questions that you bring, for instance if you are stuck in a module and need a hint.

You register for the coaching session in Lisam. The coaching sessions are not compulsory!
1.3 Deadline

The lab server opens up for registration on November 8th at 17:00. The lab must be finished before the end of the exam period. Shortly after, the TopDog server will be shut down, so you can’t do the lab after this date. If you don’t complete the assignments before the deadline, you will have to do the lab next year.

1.4 Disciplinary stuff

You are expected to do the lab in your own in groups of two. Co-operation between groups is allowed, but remember that pentesting is best learned when you try it for yourselves. You are not allowed to copy answers from other groups, and you are expected to understand and follow the university-wide rules for disciplinary matters. As for any other examination you are not allowed to cheat.

1.5 Ethics

This lab and what you learn is for educational purposes only. Do not attempt to use these techniques without authorization. If you are caught engaging in unauthorized hacking, most companies will take legal action. Claiming that you were doing security research will not protect you.

1.6 Contact information

To get in touch with the lab assistant, please send e-mail to the e-mail address below corresponding to your course. The course homepage always contains the latest version of this document, so be sure to check it out regularly.

1.6.1 TSIT01 Datasäkerhetsmetoder

Course homepage: http://www.icg.isy.liu.se/courses/tsit01/
Lab E-mail: tsit01-lab@isy.liu.se

1.6.2 TSIT02 Computer Security

Course homepage: http://www.icg.isy.liu.se/courses/tsit02/
Lab E-mail: tsit02-lab@isy.liu.se
Chapter 2

Preparing for the lab

Begin by reading through the entire lab PM. Remember to regularly check the course homepage to see if we updated the PM, as we continuously improve the lab.

2.1 Lab group

First, you need to find a partner to work with. All students are expected to work in groups of two. If this is not possible, please contact the lab assistant. When you have somebody to work with you will need to choose a username and password to use on the TopDog server. Each group of two will have an account, so you will need to choose a username and password for the group. Please note the following:

1. Your username (not password) is public and will be shown to the entire university on the scoreboard (which is shown on monitors around the campus).

2. We reserve the right to ban stupid and/or offensive usernames for any reason.

3. Both of you will have the password, so choose a password you don’t use anywhere else.

4. The password storage in TopDog is hashed and salted, however do not use a password that you care about.

Tip: Generate a random password and write it down on a note in your wallet, or use a password manager!

2.2 User account registration

Now go to http://snickerboa.it.liu.se/register.jsp and register an account, see fig. 2.2. Note that the registration link is hidden and must be typed just like that. The registration screen is shown in fig. 2.1. Note that registration requires you to type in the correct passcode, which is found in Lisam. The passcode is to discourage people outside the course to do the lab and appear on the scoreboard. Please do not share the passcode.

Next, return to the login screen and login with your credentials. If you succeeded, you will be greeted with “Let’s get started!”. This means you logged in. If the login fails, please double-check the login username and password before contacting us (see section 1.6).
Figure 2.1: The TopDog registration page.

Figure 2.2: The TopDog login page.
Chapter 3
Performing the Lab

TopDog contains a number of modules that cover different topics in web pentesting. It also offers a number of lessons that give a gentle introduction to the topic on hand.

3.1 Assignments

In order to pass the lab, you are required to finish all 21 assignments. In order to prepare yourself for the assignments, there are also lessons which give a gentle introduction to the topic at hand. You can solve the assignments in any order you want.

There are also challenges which can be performed if you wish to try your luck. Note that the lab assistant will not help you with the challenges, you have to do your own research here.

3.2 Result keys

For each lesson and challenge your goal is to retrieve the so-called “result key”. When you finish a lesson or challenge, TopDog detects that “it has been hacked” and gives you the key. Paste this key into the box on top, shown in fig. 3.1. Depending on the module the format of the result key can vary, but it might look something like the following:

3BSuxx30Rkg3zcq7Y7D0m18a46M23AS978FtaFq4E4HN14NDiafeYaKiDPwUa/xrrDSfHH9E6d5UpPrJA0nAV15bu6uk0U3S5qe5FFEjE=

Whenever you receive a result key, paste it to the “Submit Result Key Here” box on the top of the screen.

3.3 Finishing the lab

You are done with the lab when you have finished the 21 required assignments. When this is done, make sure you have signed the lab attendance list (available at the lectures and the coaching sessions) and then send an email to the Lab E-mail (see section 1.6) with the following information:
• **Subject** should be your **account** name at Snickerbo.

• **LiU-id** for both of you.

• And your **Personal number**.

and we will then check that you have done everything required of you. If you have passed we will reply with an OK. Check section 1.3 for information on when the deadline is. The deadline is strict and the server will be taken offline afterwards!

### 3.4 Best Practices

It is a good idea to keep notes of how you pass each challenge. While your progress on the server is backed up frequently we can never be too sure. Save your notes so you can get back to where you were in case of a catastrophic server failure.

### 3.5 Scoreboard

Whenever you finish a lesson, assignment, or challenge, it will show up on the LiU TopDog scoreboard. The scoreboard is public, and anybody can see the progress of the different groups. In addition, the scoreboard will be displayed on monitors around the campus, so the whole University will see how well you are doing.

The scoreboard is just for fun, and in order to pass you are only required to finish the assignments. If you have finished the assignments and want more points, you are welcome to try the challenges. Again: the scoreboard has nothing to do with your grade! See fig. 3.2 for an example of what the scoreboard looks like. For each completed lesson, assignment, or challenge you will receive points, so the more challenges you finish, the more bragging rights you have. Also, harder challenges give more points.

Your name will not appear on the scoreboard until you have finished your first challenge. There is also a small bonus for being the first student to finish a given lesson or challenge in the form of medals. A gold medal is awarded to a group who finishes a lesson or challenge nobody else has finished yet. A silver medal is given to the second one, and bronze to the third. In the scoreboard there will therefore be users with medals in addition to the normal point score. These medals give extra points to the scoreboard!

But remember, the scoreboard is just for fun. It has nothing to do with actually passing the lab.
Figure 3.1: Example of result key and where to paste it.
Figure 3.2: The TopDog scoreboard from 2016. Note the medals on some of the usernames.
3.6 List of lessons

The following lessons are available:

Broken Session Management
Cross Site Request Forgery (CSRF)
Cross Site Scripting (XSS)
Failure to Restrict URL Access
Insecure Cryptographic Storage
Insecure Direct Object References
Poor Data Validation
Security Misconfiguration
SQL Injection
Unvalidated Redirects and Forwards

3.7 List of assignments

Below are the required assignments (there are hidden hints!):

Session Management Challenge 1

Poor Data Validation 1

Cross Site Scripting 1
Session Management Challenge 2
Session Management Challenge 3
SQL Injection 1
SQL Injection 2

Insecure Cryptographic Storage Challenge 1
Insecure Cryptographic Storage Challenge 2

Insecure Direct Object Reference Challenge 1
Insecure Direct Object Reference Challenge 2

Poor Data Validation 2

Failure to Restrict URL Access 1

CSRF 1

Cross Site Scripting 2

Session Management Challenge 4

Failure to Restrict URL Access 2

Cross Site Scripting 3

Insecure Cryptographic Storage Challenge 3

SQL Injection 3

Insecure Direct Object Reference Bank
Chapter 4

Frequently Asked Questions (FAQ)

This section will be updated with frequently asked questions about the lab.

4.1 There is something wrong with the server!

First check that your Internet connection is working and that your attack proxy isn’t giving you problems. If the TopDog server is unavailable, or if there’s some technical issue with it that has nothing to do with the lab itself, first wait a few minutes. If it doesn’t come back it might be an outage (planned or unplanned). If we are doing some planned work on the server this will be posted on Lisam.

If the server is still down and there’s nothing on Lisam saying it’s a planned outage, the server might be down. Please send an e-mail to the lab assistant, see section 1.6.

4.2 How do I create a TopDog account?

See section 2.2.

4.3 How can I get bonus points for the exam?

The scoreboard and its points, bonus points, and medals is for fun only. They have absolutely nothing to do with passing the lab or with the examination of the course. The lab assistant can see how many assignments you have finished, independently of the scoreboard.

4.4 What happens if I can’t go to the coaching session?

The coaching sessions are not a compulsory part of the course. If you can’t attend, there is no penalty. However, the sessions can be valuable as you have the opportunity to get coaching and ask questions about the lab. Also, you must sign the lab attendance list before finishing. This is important as we need to know who is who, otherwise anyone could pretend to be the scoreboard leader!
4.5 I finished the lab and want something more challenging!

Try your skills on the challenges! If this is still not enough, check out appendix B!

4.6 I don’t get a result key, only “Key Should be here! Please refresh the home page and try again! If that doesn’t work, sign in and out again!”

This is a bug that sometimes happens. Contact us (section 1.6) and we’ll help you.

4.7 The result key in insecure crypto challenges isn’t working!

Make sure you check that you’ve got UPPERCASE/lowercase correctly. Some online calculators will mess this up. Also make sure it handles spaces correctly.

4.8 In the Insecure Direct Object Reference Bank challenge, there’s no money left

It can happen that the total amount of money is too small to pass the lab. In this case, contact us at section 1.6 and we’ll fill up bank with some more money to steal :)

4.9 I found a typo or have a suggestion for this lab PM!

We constantly work on getting the lab and this document as good as possible. If you have a suggestion, don’t hesitate to contact us (see section 1.6).

4.10 I love computer security and I am looking for thesis work!

Check out Jonathan’s list of thesis projects¹ or the list at the Information Coding Group². Also, if you like crypto we highly recommend the course TSIT03 Cryptology³ that is given in HT1 every year.

¹http://people.isy.liu.se/icg/jonfo33/supervision/proposals.html
²http://www.icg.isy.liu.se/exjobb/
³http://www.icg.isy.liu.se/courses/tsit03/
Appendix A

Tools

Penetration testing requires you to have a large and diverse toolbox. In this lab, you will mostly use online tools (that you’ll have to find yourself) and one offline tool: ZAP. The online tools can be things such as online calculators, hex-to-dec-converters, decryption tools for cryptographic algorithms etc. Use Google! Also, the slides from the lab preparation lecture will be of use to you.

A.1 Viewing the source code

The first step in most web attacks is usually to look at the source code. This will show you the raw HTML/CSS/JavaScript that builds up the page. For a quick reference on what the HTML tags do, check out the W3 HTML Reference\(^1\). Figure A.1 shows the source code of one of the modules.

There are two main ways to view source code. The “traditional” way is to use the View Source feature found in most web browsers. Right-click the page and select “View Source”. You can also use the “inspect” feature to view the source related to a particular item on a page by right-clicking it and selecting “Inspect” or “Inspect Element”, depending on your web browser.

In the TopDog challenge you must remember that the web modules are located in an iframe in the web page. You must therefore click inside the module itself and select “View Frame Source”, or “This Frame” followed by “View Source” as shown in fig. A.2 (this example assumes you are using Firefox). Otherwise, you will be reading the source code of TopDog itself and not the module.

A.2 The Zed Attack proxy (ZAP)

ZAP is the Zed Attack Proxy by OWASP\(^2\). You will use this tool to modify HTTP packets sent between your web browser and the web server. An attack proxy is the most important tool for pentesting web applications. There are of course other attack proxies for you to use, but ZAP is the tool we can help you with during the coaching sessions. ZAP runs on Windows, Linux and OSX and requires Java 7 or higher.

\(^1\)http://www.w3schools.com/tags/

\(^2\)https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project
Failure To Restrict URL Access Challenge

To recover the result key for this challenge you need to obtain the current server status message from an administrator.

Use this form to view the status of the server - from the point of view of a peasant or guest.

<form id="leForm" action="javascript:;"
  "table"
  <tr id="id"
    <div id="submitButton">
      <input type="submit" value="Get Server Status"/>
    </div>
    <p style="display: none;" id="loadingSign">Loading</p>
    <div style="display: none;" id="hintButton"><input type="button" value="Would you like a hint?" id="theHint"
  </td/>
  </tr>
  </table>
</form>

Figure A.1: An example of a source code of a module.

Figure A.2: How to view only the source of the iframe containing the module.
A.2.1 Configuring ZAP

Installing ZAP is easy. If you don’t have Java, the installer will help you download and install it. If you have any trouble, check the ZAP Quick Start Guide\(^3\) or the ZAP Wiki\(^4\). Upon first startup, ZAP will ask you if you want to persist the session. It’s safe to say yes. After starting up, you will see the ZAP interface as shown in fig. A.3.

In order to use the attack proxy, you will need to configure your web browser to connect through it. Here, it is recommended that you download and install a secondary web browser to your computer, so that you have one normal browser (for googling and general browsing) and one “attack browser” for use with TopDog. Otherwise, ZAP will intercept all your HTTPS sessions (i.e. also your general web browsing), which is very

\(^3\)https://github.com/zaproxy/zaproxy/releases/download/2.5.0/ZAPGetting_started_guide_2.5.pdf

\(^4\)https://github.com/zaproxy/zaproxy/wiki/Introduction
By default, ZAP listens to connections on port 8080. Therefore, configure the attack browser (the one you use for TopDog) to use localhost:8080 as the proxy configuration for HTTP and HTTPS protocols.

For instance, the configuration\(^5\) for Firefox is shown in fig. A.5. Instructions for configuring proxy settings for Chrome can be found here: https://support.google.com/chrome/answer/96815.

Now, using the attack browser, go to the TopDog page: https://snickerboa.it.liu.se. It might be that your browser gives a warning about your connection being insecure since ZAP decrypts and re-encrypts HTTPS traffic (see fig. A.6). Remember that we talked about this in the lecture. You will have to accept the ZAP certificate and add it as an exception to the attack browser.

### A.2.2 Intercepting HTTP(S) traffic with ZAP

Now you can browse around in TopDog and see that the traffic appears in ZAP. In the left-hand pane you see Sites. Expand it and you see the site https://snickerboa.it.liu.se. Inside, you see the different requests (mainly GET and POST) that were made to the server.

On the main pane (the window that says “Welcome to OWASP...”) there are three tabs on top: Quick Start, Request, and Response. The Request tab shows the request sent by the web browser and the Response tab shows the response by the web server. See fig. A.7 for an example of a request package. Figure A.8 is an example of a response package.

Now we want to capture a HTTP response for ourselves. Begin by pressing the green circle (see fig. A.9) so that it turns red. ZAP will now capture all requests that pass through it. Then, in your attack browser, perform some action that sends a HTTP request, like clicking a link or a button. ZAP will then pop up, showing you the packet it captured (just like in fig. A.7). You can now modify the packet before sending it on, or just forward it without modification. Either way, press the step button to pass the request on to the server and capture the next packet.

The web server will then process the request and reply with a HTTP response. Since you clicked step, ZAP will capture this request as well and show it to you, just like in

\(^5\)http://www.wikihow.com/Enter-Proxy-Settings-in-Firefox
Figure A.5: Firefox proxy configuration (Preferences -> Advanced -> Network -> Settings)

Figure A.6: Schematic diagram of ZAP when dealing with HTTPS traffic
Figure A.7: Screenshot of ZAP showing a HTTP request package sent from the web browser to the web server. The request belongs to the lesson module for cross-site scripting. In the lower right side you can see user-data=99, which means that the request contains POST data from a form with the variable user-data set to the value 99.
Figure A.8: ZAP showing a response packet from the web server to the web browser. The body of the response shows a HTML-encoded text saying that “the number 99 is a valid number”.
Now, click the play button which will deactivate the break point entirely and send the response back to the attack browser.

ZAP has many more features, but for this lab you only need to concern yourself with the break/step/play features. Note that the web browser will be stuck on “loading” until ZAP has sent both the request and response to their destinations.
Appendix B
Capturing The Flag

TopDog is what the hacking community calls a CTF, or Capture The Flag. CTF:s are a good way of practicing one’s skills in order to become better at pentesting, reverse-engineering, cracking, etc. It is common for security conferences to have CTF competitions where teams try to solve a number of challenges set up by the organizers. Prizes are usually awarded for the teams who finish first.

If you found this lab course interesting and want more CTF challenges, check out this list: https://captf.com/practice-ctf/.