## LAB SESSIONS: TOOLS REQUIRED

The second half of the Friday lectures will be a `lab session' in which some of the security theory is applied by performing some basic security attacks. You can prepare your computer for the lab sessions by installing the required software. Guidelines on where to find the software and how to install it are given below.

## A. MOZILLA FIREFOX

Mozilla Firefox will be the reference browser we will use during the lab sessions. Download and install the latest version that you can find here: <u>http://www.mozilla.org/en-US/firefox/new/</u>

## **B.** MOZILLA ADD-ONS TAMPER DATA

A tampering tool is one of the most important means needed to exploit web application vulnerabilities. For our exercises we need *Tamper Data*, a Firefox Add-Ons you can download at the following address: <u>https://addons.mozilla.org/en-US/firefox/addon/tamper-data/</u>

Be sure to correctly install it and to restart your browser once finished. The tool will allow you to intercept every HTTP request/response that you send or receive during your browsing session. To start *TamperData* click on Firefox Menu Bar, Tools  $\rightarrow$  Tamper Data. This will open a new window where you can observe your HTTP traffic. As shown in Figure 1 *tampering* can be started and stopped according to your needs (e.g. tampering is needed to solve exercises but you can stop it during normal browsing). The *TamperData* plugin does not only allow you to see the content of the requests/responses, but also to modify them. For example you can change the parameters of a request by just typing the new values, as shown in Figure 2.

Fitter web/Goat   Time Duration   10/39-47/322 94 ms   10/39-47/322 96 ms   10/39-47/322 92 ms   10/39-47/323 92 ms   10/39-47/329 96 ms   10/39-47/329 96 ms   10/39-47/329 96 ms   10/39-47/329 92 ms   10/39-47/324 92 ms	Total Duration 84 ms 90 ms 87 ms 92 ms 93 ms 89 ms 91 ms 91 ms 92 ms	Size -1 -1 -1 -1 -1 -1 -1 -1 -1	Method GET GET GET GET GET GET	Status 304 304 304 304 304 304 304	Content Type application/= unkn. application/= unkn. application/= unkn. application/= unkn.	URL http://loc http://loc http://loc http://loc	Show All Load Flags LOAD_NORMAL LOAD_NORMAL LOAD_NORMAL LOAD_NORMAL
Time Duration   10-39-47.322 84 ms   10-39-47.322 90 ms   10-39-47.323 97 ms   10-39-47.323 92 ms   10-39-47.323 92 ms   10-39-47.323 92 ms   10-39-47.324 91 ms	Total Duration 84 ms 90 ms 87 ms 92 ms 93 ms 89 ms 91 ms 92 ms	Size -1 -1 -1 -1 -1 -1 -1	Method GET GET GET GET GET	Status 304 304 304 304 304 304 304	Content Type epplication/x-unkn. epplication/x-unkn. epplication/x-unkn. epplication/x-unkn.	URL http://loc http://loc http://loc http://loc	Load Flags LOAD_NORMAL LOAD_NORMAL LOAD_NORMAL LOAD_NORMAL
20:3947.322 84 ms 10:3947.322 90 ms 10:3947.322 87 ms 10:3947.323 92 ms 10:3947.323 93 ms 10:3947.324 92 ms 10:3947.324 92 ms 10:3947.324 92 ms	84 ms 90 ms 87 ms 92 ms 93 ms 91 ms 91 ms 91 ms	44444	GET GET GET GET	304 304 304 304 304 304	application/s-unkn. application/s-unkn. application/s-unkn. application/s-unkn.	http://loc http://loc http://loc http://loc	LOAD_NORMAL LOAD_NORMAL LOAD_NORMAL
10:3947.322 87 ms 10:3947.323 92 ms 10:3947.323 93 ms 10:3947.323 89 ms 10:3947.324 91 ms 10:3947.324 91 ms	92 ms 92 ms 93 ms 89 ms 91 ms 91 ms	-1 -1 -1 -1	GET GET GET	304 304 304 304	application/s-unkn. application/s-unkn. application/s-unkn.	http://loc http://loc http://loc	LOAD_NORMAL LOAD_NORMAL
10:3947.323 92 ms 10:3947.323 93 ms 10:3947.323 93 ms 10:3947.324 91 ms 10:3947.324 92 ms 10:3947.324 91 ms	92 ms 93 ms 89 ms 91 ms 92 ms	-1 -1 -1	GET GET	304 304 304	application/x-unkn	http://loc	LOAD_NORMAL
10.3947.323 93 ms 10.3947.323 89 ms 10.3947.324 91 ms 10.3947.324 92 ms 10.3947.324 91 ms	93 ms 89 ms 91 ms 92 ms	-1 -1 -1	GET	304	application/x-unkn.	http://loc	Court Jugarda
10:39:47.323 89 ms 10:39:47.324 91 ms 10:39:47.324 92 ms 10:39:47.324 92 ms 10:39:47.324 91 ms	89 ms 91 ms 92 ms	-1 -1	GET	304			LOAD NORMAL
10:39:47.324 91 ms 10:39:47.324 92 ms 10:39:47.324 91 ms	91 ms	-1			application/x-unkn	http://loc	LOAD NORMAL
10-39:47.324 92 ms 10-39:47.324 91 ms	92 ms		GET	304	application/x-unkn	http://loc.	LOAD NORMAL
10-39-47.324 91 ms	2 B 17 18	-1	GET	304	application/x-unkn_	http://loc	LOAD NORMAL
	91 ms	-1	GET	304	application/s-unkn.	http://loc	LOAD_NORMAL
10:39:47.324 92 ms	92 ms	-1	GET	304	application/x-unkn	http://loc	LOAD NORMAL
10:39:47.352 64 ms	64 ms	-1	GET	304	application/wunkn	http://loc	LOAD_NORMAL
10:39:47.433 63 ms	63 ms	1072	GET	404	text/html	http://loc	LOAD, NORMAL
10:39:47.435 73 ms	73 ms	-1	GET	304	application/x-unkn	http://loc	LOAD_NORMAL
10:39:47.436 66 ms	66 ms	-1	GET	304	application/x-unkn	http://loc	LOAD_NORMAL
10:39:47.436 68 ms	68 ms	-1	GET	304	application/x-unkn	http://loc	LOAD_NORMAL
10:39:47.436 75 ms	75 ms	-1	GET	304	application/x-unkn	http://loc	LOAD_NORMAL
10:39:47.437 71 ms	71 ms	-1	GET	304	application/x-unkn_	http://loc	LOAD_NORMAL
10:39:47.437 75 ms	75 ms	-1	GET	304	application/x-unkn	http://loc	LOAD NORMAL
10:39:47.437 65 ms	65 ms	-1	GET	304	application/x-unkn	http://loc	LOAD_NORMAL
10:39:47.438 64 ms	64 ms	-1	GET	304	application/x-unkn	http://loc	LOAD_NORMAL
10:39:47.438 65 ms	65 ms	-1	GET	304	application/x-unkn	http://loc	LOAD_NORMAL
11:01:09.462 0 ms	0 ms	unknown	GET	pending	unknown	http://loc	LOAD_NORMAL
Request Header Name	Request Hea	der Value		Response Head	der Name Re	sponse Head	ir Value
	103947332 64 ms 103947433 63 ms 103947433 63 ms 1039474436 65 ms 1039474436 65 ms 1039474438 73 ms 103947438 73 ms 103947437 75 ms 103947437 75 ms 103947438 64 ms 103947438 64 ms	10.3967/232 54 mm 64 mm 10.3967/232 54 mm 64 mm 10.3967/233 57 mm 73 mm 10.3967/235 57 mm 73 mm 10.3967/246 56 mm 64 mm 10.3967/246 56 mm 75 mm 10.3967/246 57 mm 75 mm 10.3967/247 71 mm 73 mm 10.3967/247 75 mm 75 mm 10.3967/247 55 mm 65 mm 10.3967/247 55 mm 65 mm 10.3967/248 57 mm 75 mm 75 mm 75 mm 75 mm 10.3967/248 57 mm 75 mm	10.3967/232 24 fm; 44 m; 10 10.3967/233 25 fm; 57 m; 73 m; 11 10.3967/233 25 77 m; 73 m; 12 10.3967/245 66 m; 66 m; 11 10.3967/246 66 m; 76 m; 11 10.3967/246 75 m; 75 m; 12 10.3967/247 71 m; 74 m; 14 10.3967/247 75 m; 55 m; 14 10.3967/247 55 m; 55 m; 14 10.3967/247 55 m; 55 m; 14 10.3967/248 55 m; 14 10.3977/248 55 m; 14 10.3977/248 55 m; 14 10.3977/248 55 m; 14 10.3977/248 55 m; 14 10.39777/248 55 m; 14 10.39777777777777777	10.396.723 24 4mg 64 mg 10 cT 10.396.7243 25 4mg 64 mg 102 cT 10.396.7243 25 72 mg 23 mg 11 cT 10.396.7243 25 72 mg 23 mg 12 cT 10.396.7245 66 mg 66 mg 11 cT 10.396.7245 73 mg 12 mg 12 cT 10.396.7245 73 mg 12 mg 12 cT 10.396.7247 71 mg 12 mg 12 cT 10.396.7247 71 mg 12 mg 12 cT 10.396.7247 71 mg 12 mg 12 cT 10.396.7243 75 mg 15 mg 12 cT 10.396.7243 75 mg 12 cT 10.396.7248 55 mg 12 cT 10.396.7248 55 mg 12 cT 10.396.7248 55 mg 12 mg 12 cT 10.396.7488 55 mg 12 cT 10.396.748 55 mg 12 cT 10.396.7488 55 mg 12 cT 10.396.748 55 mg 12 cT	10.396.723 24 min 1 CTT 304   10.396.723 24 min 1 CTT 304   10.396.723 25 min 53 min 1 GTT 304   10.396.723 25 min 1 GTT 304   10.396.7243 57 min 1 GTT 304   10.396.7243 56 min 66 min 1 GTT 304   10.396.7243 75 min 75 min 1 GTT 304   10.396.7247 75 min 71 min 1 GTT 304   10.396.7247 75 min 71 min 1 GTT 304   10.396.7247 75 min 75 min 1 GTT 304   10.396.7247 55 min 65 min 1 GTT 304   10.396.7247 55 min 65 min 1 GTT 304   10.396.7248 57 min 67 min 304 304   10.396.7248 57 min 67 min 304 304	10.397.123 G4 mm 4 mm 1 GTT 204 reprintation/v units.   10.397.123 G4 mm G4 mm 1 GTT 204 tep/situation/v units.   10.397.123 G7 mm G7 404 tep/situation/v units.   10.397.123 G7 mm 77 mm -1 GTT 204 tep/situation/v units.   10.397.125 G7 mm 77 mm -1 GTT 204 application/v units.   10.397.126 G6 mm -6 GTT 304 application/v units.   10.397.128 75 mm 75 mm -6 GTT 304 application/v units.   10.397.128 75 mm 75 mm -6 GTT 304 application/v units.   10.397.128 75 mm -6 GTT 304 application/v units.   10.397.128 75 mm -1 GTT 304 application/v units.   10.397.128 65 mm -1 GTT 304 application/v units.   10.397.128 15 m	D3937232 G4 ms G4 ms 1 GTT 504 epplication/wurkn. Http://toc.   D3937232 G4 ms G6 ms 1027 GTT 404 epplication/wurkn. Http://toc.   D3937232 G4 ms 77 ms 77 ms 71 ms 12 GTT 404 explication/wurkn. Http://toc.   D3937233 G4 ms 66 ms 1 GTT 204 epplication/wurkn. Http://toc.   D39374236 G4 ms 66 ms 1 GTT 204 epplication/wurkn. Http://toc.   D39374236 G4 ms 66 ms 1 GTT 204 epplication/wurkn. Http://toc.   D39374236 G4 ms 75 ms 1 GTT 204 epplication/wurkn. Http://toc.   D39374237 75 ms 75 ms 1 GTT 204 epplication/wurkn. Http://toc.   D39374237 75 ms 75 ms 1 GTT 204 epplication/wurkn. Http://toc.   D39374237 75 ms 67 ms 1 GT 204 epplication/wurkn. Http://toc.

Figure 1: Tamper Data Add-On

mper Popup			
http://localhost:8080/WebGoat/	/attack?Screen=34&menu=1700		
Request Header Name	Request Header Value	Post Parameter Name	Post Parameter Value
Host	localhost:8080	QTY	1
User-Agent	Mozilla/5.0 (Windows NT 6.1	SUBMIT	Purchase
Accept	text/html,application/xhtml+	Price	2999.99
Accept-Language	en-us,en;q=0.5		
Accept-Encoding	gzip, deflate		
Accept-Charset	ISO-8859-1,utf-8;q=0.7,*;q=0		
Connection	keep-alive		
Referer	http://localhost:8080/WebGe		
Cookie	JSESSIONID=F6B8B8CB9938E		
	I	1	
			OK Cancel

Figure 2: Modifying Request Parameters by using Tamper Data

## C. WEB GOAT

WebGoat<sup>1</sup> is a deliberately insecure web application, designed to teach web application security lessons. You can download the version 5.4 of WebGoat here: <u>http://code.google.com/p/webgoat/downloads/detail?name=WebGoat-5.4-</u> <u>OWASP\_Standard\_Win32.zip&can=2&q=</u>

This is a stand-alone version, which means you will get all you need to run the web application on your machine. Once you downloaded the .zip file, extract it on the Desktop. At this point you will have a folder structure looking like the one in Figure 3. Run the file *webgoat\_8080.bat* to start you application, and type <u>http://localhost:8080/WebGoat/attack</u> in your address bar.

	_							<b></b>			×
Set the set of the	Goat	t-5.4 ▶					• +•	Search WebGoat-5	.4		Q
Organize 🔻 Inclu	de ir	n library 👻 Share with 💌	Burn New fo	older					:==	•	0
🔆 Favorites	-	Name		Date modified	Туре	Size					
🧮 Desktop		퉬 java		6-6-2012 14:21	File folder						
📃 Recent Places	Ξ	퉬 tomcat		6-6-2012 14:21	File folder						
퉳 Downloads		README.txt		6-6-2012 14:20	Text Document	8 KB					
💝 Dropbox		🚳 webgoat.bat		6-6-2012 14:20	Windows Batch File	1 KB					
		webgoat.sh		6-6-2012 14:20	SH File	2 KB					
词 Libraries		🚳 webgoat_8080.bat		6-6-2012 14:20	Windows Batch File	1 KB					
Documents											
👌 Music											
Pictures											
Subversion	-										
6 items											

**Figure 3: Folder Structure** 

<sup>&</sup>lt;sup>1</sup> <u>https://www.owasp.org/index.php/Category:OWASP\_WebGoat\_Project</u>

If the address <u>http://localhost:8080/WebGoat/attack</u> does not work you might need to start the tomcat service by yourself. To do so start the service **WebGoat-5.4\tomcat\bin\startup.bat** and browse to <u>http://localhost/WebGoat/attack</u>.

If everything went fine you will be asked for your credentials: insert the word *guest* for both username and password, and you will see the page of Figure 4. Press the *Start WebGoat* button: you are ready to begin the lab session.



Thank you for using WebGoat! This program is a demonstration of common web application flaws. The exercises are intended to provide hands on experience with application penetration testing techniques.

OWASP The Open Web Application Security Project	ASPECT SECURITY Application Security Experts		
WebGoat	Authors		
Bruce M	ayhew		
Jeff Wil	liams		
WebGoat Design Team	V5.4 Lesson Contributers		
David Anderson Laurence Casey (Graphics) Rogan Dawes Bruce Mayhew	Sherif Koussa Yiannis Pavlosoglou		
Special Thanks for V5.4	Documentation Contributers		
Brian Ciomei (Multitude of bug fixes) To all who have sent comments	Erwin Geirnaert Aung Khant Sherif Koussa		
Start We	bGoat		

The WebGoat project is led by Bruce Mayhew. Please send all comments to Bruce at WebGoat@owasp.org.

Figure 4: WebGoat Home Page