Unvalidated Parameters W/WebGoat

You will use the following Virtual Machine (VM) and application in this lab:

- Windows Server 2012 VM
- WebGoat application from OWASP
- Burp Suite Community Edition from PORTSWIGGER
- Web Browser (Firefox)

Before we proceed you will need to download and setup the lab environment on your Windows Server 2012 VM.

Step 1

Log in to your Administrator account on your windows server 2012 VM. Use your administrator account credential from your previous lab. If you followed setup according to previous lab setup the following login credential will work.

User: Administrator

Password: Admin123

Administrator Admini23	
₩ Windows Server 2012	

Minimize Windows Server manager dashboard. we will use it late to disable windows IIS web server. Open internet explorer and follow the steps to download and setup applications.

Download mozilla firefox web browser for convenience. Enter the following URL on your internet explorer and download the setup file and install firefox on your VM.

JRL: https://www.mozilla.org/firefox	
Home × Windows Server 2012 × ome >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>	L_10 0
moz://a Firefox Pocket Internet Health Technology About Us Get Involved	Download Firefox
Desktop Mobile Extensions Support Blog	
5 The new Firefox	 Implies the sector of the address Implies the sector of the address
Meet Firefox Quantum.	C. Search the Web
Fast for good.	
Download now Firefox Privacy Notice	
ther platforms & languages	
Do you want to run or save Firefox Installer.exe (306 KB) from stubdownloader.cdn.r	mozilla.net? Run the firefox installer.exe ×
🕐 This type of file could harm your computer.	Run Save 🔻 Cancel

Open your firefox web browser and download few more applications to setup your lab environment.

Visit WebGoat official web site and download WebGoat-OWASP_Standard-5.2.

URL : <u>https://www.owasp.org/</u>

OWASP	× +		
\leftrightarrow > C $$	① A https://www.owasp.org/index.php/Main_Page		
	Welcome to OWASP		 Proactiv
Home About OWASP Acknowledgements	the free and open software security community	Dependen cy Checkt	e Controls⊉ ZAP Proxy⊉
Advertising AppSec Events Books	Donate		● Cheat Sheets &
Brand Resources Chapters	About · Searching · Editing · New Article · OWASP Categories . CONTACT-US		
Donate to OWASP Click on I	Downoads and follow the Steps		
Funding	Every vibrant technology marketplace needs an unbiased source of information	n on best practi	ces as well as

Category	Discussion			Read	View source	View history	Search	ų	,
Cat	tegory	:OWASP	Download					() Help	
_				 					

The OWASP Download category should be used to mark any page that has a significant download available. The download should be clearly marked and described near the top of the page. Our old download center is located at SourceForge ? Many of our documents and tools are still available there.

Redirect to sourceforge.net. Sourceforge is a centralized web-based service that offers software developer a online platform to control and manage free and open-source software project.

♦ OWASP Source Code Center - 🗄 🗙 +				
← → C f	ceforge.net/projects/owasp/files	/		
SOURCE FORGE	Articles	Cloud Storage	Business VoIP	Intern
Home				
Name 🗢	Modified 🖨	Size 🖨	Downloads / Week 🖨	
ASVS	2013-08-22		9	
WebGoat Select the folder.	2008-07-12		122 🖵	
C Pantera	2008-05-29		176 🛌	
Home / WebGoat				
Name 🖨	Modified 🖨	Size 🖨	Downloads / Week 🖨	•
WebGoat 5.2 Select the Folder	2008-07-12		90 🛋	
WebGoat 5.1	2008-01-19		8	

♦ OWASP Source Code Center - E × +						
← → C û (i) ▲ https://sourceforge	① A https://sourceforge.net/projects/owasp/files/WebGoat/WebGoat 5.2/					
SOURCE FORGE	Articles	Cloud Storage	Business VoIP	Intern		
Home / WebGoat / WebGoat 5.2						
Name 🖨	Modified 🖨	Size 🖨	Downloads / Week	¢		
WebGoat-OWASP_Standard-5.2.zip	e 2008-07-12	87.1 MB	61 🛋	(i)		
WebGoat-5.2.war	2008-07-12	37.3 MB	9	(i)		
WebGoat-OWASP_Developer-5.2.zip	2008-07-12	305.0 MB	18 🔔	(i)		
readme-5.2.txt	2008-07-12	7.8 kB	2	<i>(i)</i>		

Opening WebGoat-OWASP_Standard-5.2.zip			
You have chosen to open:	?source=typ_redirect	~ … ⊠ ☆	IIIY
WebGoat-OWASP_Standard-5.2.zip which is: Compressed (zipped) Folder (83.0 MB) from: https://astuteinternet.dl.sourceforge.net	Browse	WebGoat-OWASP_Standard-5.2.zip	
What should Firefox do with this file? Open with Windows Explorer (default) Save File Do this automatically for files like this from now on. OK	ernet Speed Test	After complete downolad click on folder icon on your Show All Downloads firefox downlaod tab to locate your download directory.	uti

Right click WebGoat-OWASP_Standard-5.2.zip file and click Extract all.

🐌 🕨 Adr	ninistrator 🕨 Downloads 🕨				~ Ç	Sea
	Name	Date modified	Туре	Size		
is aces ts ts Select a Files will be CUSERSA	WebGoat-OWASP Standard-5.2 Open Open in new window Pin to Start Extract All Open with Share with Restore previous versions Send to Cottompressed (Zipped) Folders Destination and Extract Files extracted to this folder: tracted files when complete	4/17/2018 3:37 PM	Compressed (zipp	85,029 KB		
🗼 🕨 Adn	Click Extract C Extract	Cancel				~
-	Name	Date modified 4/17/2018 3:47	Type PM File folder	Size		

By default, the file is extracted inside the same download folder you can make change to your extract directory according to preference.

Extracted location: C:\Users\Administrator\Downloads\WebGoat-OWASP_Standard-5.2\WebGoat-5.2

File Home Share	View			
€ ⊙ - ↑ 🖡 • 4	Administrator + Downloads +			
⊿ 🚖 Favorites	Name	Date modified	Туре	Size
Desktop	UebGoat-OWASP_Standard-5.2	4/17/2018 3:47 PM	File folder	
Downloads Recent places	UebGoat-OWASP_Standard-5.2	4/17/2018 3:37 PM	Compressed (zipp	85,029 KB

The extracted folder contains tomcat webserver, java files and .bat windows executable file.

File Home Share	View				
🗲 🕘 - 🛧 👢 🕨 A	dministrator 🕨 Downloads 🕨 WebG	ioat-OWASP_Standard-5.2 WebGo	pat-5.2 🕨		✓ 🖒 Searc
🚖 Favorites	Name	▼ Date modified	Туре	Size	
Desktop	👢 java	4/17/2018 3:47 PM	File folder		
駨 Downloads	🐌 tomcat	4/17/2018 3:48 PM	File folder		
laces 😓 Recent places	i readme.txt	4/17/2018 3:47 PM	Text Document	8 KB	
	🔍 webgoat.bat	4/17/2018 3:47 PM	Windows Batch File	1 KB	
门 Libraries	webgoat.sh	4/17/2018 3:47 PM	SH File	2 KB	
locuments 🔍	💿 webgoat_8080.bat	4/17/2018 3:47 PM	Windows Batch File	1 KB	
N					

Step 2

We need to download java to run the WebGoat application. You can download java from java official website. Enter the following URL on your web browser and follow the steps to install java on your Windows Server 2012 VM

URL: <u>https://java.com/</u>





Run the java setup file after complete download.

Name	•		Date modified	Туре	Size
👢 WebGoat-OWA	SP_Stand	1. Double Click on .e ard-5.2	exe file to begin the ja 4/17/2018 3:47 PM	<mark>wa setup</mark> File folder	
🖆 jxpiinstall.exe		\Leftrightarrow	4/17/2018 4:07 PM	Application	1,838 KB
🐌 WebGoat-OWA		Open F	ile - Security Warr	ning	Х 15,029 КВ
	Do y	ou want to run this file	e?		
		Name: C:\User Publisher: <u>Oracle</u>	rs\Administrator\Dowr	nloads\jxpiinstall.exe	
		Type: Applic	ation		
		From: C:\Use	rs\Administrator\Dowr	nloads\jxpiinstall.exe	
		2. Click o to execute setup proc	e the Run cess.	Cancel	
	✓ Al	ways ask before openir	ng this file		

Click on Install and it will take a while download and complete the java setup on you Windows Server 2012 VM. Make sure you need to restart your Web Browser after successfully completing a java setup.

Java Setup - Welcome 📃 🗖 🗙
Welcome to Java
Java provides access to a world of amazing content. From business solutions to helpful utilities and entertainment, Java makes your Internet experience come to life.
Note: No personal information is gathered as part of our install process. <u>Click</u> <u>here</u> for more information on what we do collect.
Click Install to accept the <u>license agreement</u> and install Java now.
Change destination folder Cancel Install >

Step 3

We need to install Burp Suite on our windows server 2012 VM. Open your web browser and enter the following URL to download Burp Suite free community edition.

URL: https://portswigger.net/burp/communitydownload



Opening burpsuite_community_v	vindows-x64_v1_7_33.exe	
You have chosen to open:		
burpsuite_community_windows-	x64_v1_7_33.exe	
which is: Binary File (90.0 MB)		
from: https://portswigger.net		
Would you like to save this file?		
Save the setup file	Save File Cancel	
	· ··· ♥ ☆ 1. Click on □> ↓ IIN Download Tab	
burpsuite_commur Completed — 90.0 f	ity_windows-x64_v1_7_33.exe ^{MB} 2. Click on Folder to ℃	
Show All Downloads	view your downloaded file.	
Share View Manage		
Computer Local Disk (C:) User	s • Administrator • Downloads	Search De
Name 1. Double Click on bur	Size	
	psuit community Windows x64-v1 7exe setup	
file and follow the setu WebGoat-OWASP_Standa	pinstruction. rd-5.2	
file and follow the setu WebGoat-OWASP_Standa Is Is	pisuit_community_Wind8ws'*x64**Y_7exe3setup 512e p instruction. 4/17/2018 3:47 PM File folder dows-x64_v1_7_33 4/17/2018 4:30 PM Application 92	,201 KB
file and follow the setu WebGoat-OWASP_Standa Is Is inces jxpiinstall.exe	pinstruction. rd-5.2 4/17/2018 3:47 PM File folder dows-x64_v1_7_33 4/17/2018 4:30 PM Application 92	,201 KB
file and follow the setu WebGoat-OWASP_Standa Is is ices jxpiinstall.exe WebGoat-OWASP_Standa	pistruction. 4/17/2018 3:47 PM File folder dows-x64_v1_7_33 4/17/2018 4:30 PM Application Open File - Security Warning	,201 KB
Is WebGoat-OWASP_Standa	pisuit_community_Wind8ws*x64*4*1_7ex33etup 5126 p instruction. 4/17/2018 3:47 PM File folder dows-x64_v1_7_33 4/17/2018 4:30 PM Application 92 Open File - Security Warning Do you want to run this file?	,201 KB
file and follow the setu WebGoat-OWASP_Standa Is ices jxpiinstall.exe WebGoat-OWASP_Standa WebGoat-OWASP_Standa is	pissuit_community_Wind8ws**x64*4*1_7ex33etup Size pinstruction. 4/17/2018 3:47 PM File folder dows-x64_v1_7_33 4/17/2018 4:30 PM Application 92 Open File - Security Warning Do you want to run this file? Name: s\burpsuite_community_windows-x64_v1_7_33 Publisher: PortSwigger Ltd	,201 KB X
file and follow the setu WebGoat-OWASP_Standa Is ices jxpiinstall.exe WebGoat-OWASP_Standa S	pisuit_community_Wind8ws*x64*4*1_7ex33etup 5126 p instruction. 4/17/2018 3:47 PM File folder dows-x64_v1_7_33 4/17/2018 4:30 PM Application 92 Open File - Security Warning Do you want to run this file? Name: s\burpsuite_community_windows-x64_v1_7_33 Publisher: PortSwigger Ltd Type: Application	,201 KB
Is WebGoat-OWASP_Standa	pissuit_community_Wind8ws*x64*4*1_7ex33etup Size pissruction. 4/17/2018 3:47 PM File folder dows-x64_v1_7_33 4/17/2018 4:30 PM Application 92 Open File - Security Warning Do you want to run this file? Name: s\burpsuite_community_windows-x64_v1_7_33 Publisher: PortSwigger Ltd Type: Application From: C:\Users\Administrator\Downloads\burpsuite_componention	,201 KB X .exe
Is WebGoat-OWASP_Standa Is Signature Standa WebGoat-OWASP_Standa Signature Standa WebGoat-OWASP_Standa Signature Standa Signature St	pissuit_community_Wind8ws*x64*4*1_7ex33etup Size pissruction. 4/17/2018 3:47 PM File folder dows-x64_v1_7_33 4/17/2018 4:30 PM Application 92 Open File - Security Warning Do you want to run this file? Image:s\burpsuite_community_windows-x64_v1_7_33 Publisher: PortSwigger Ltd Type: Application From: C:\Users\Administrator\Downloads\burpsuite_community_Ltd Cancel 2. Select Run to start the setup	,201 KB .exe om

Follow the setup instruction and use the default setting don't make changes. After installation, you can access the application from your windows server startup screen or application shortcut from Desktop.

Exercise 1 Parameter Tampering

In this lab, we will use the WebGoat application form OWASP to do perform some attack on web application. It is good learning environment and allows us to exploit a number of different web application specific vulnerabilities.

Webgoat runs as a webserver. In order to start it up, you must first stop the IIS Webserver. To do so we can access our Server Manager Dashboard from our windows startup screen. Press Windows key real then select Server Manager from the start menu.



Select IIS service tab from you server manager dashboard on you left and scroll down to services list and find world wide web publishing service inside the list. You need to check the status of the service and if it is running you need to stop the service. To do so you need to select the world wide web publishing service, right click on it and select stop services. It might take few minutes wait until the status is updated with stopped sign.

Server Ma	anager + IIS	🕶 遼 🚩 Manage Tools View H
 Dashboard Local Server All Servers DHCP DNS File and Storage Services NS IS 1. Click on IIS NAP 	SERVICES Image: Constraint of the service service inside IIS Tab. All services 3 total Image: Constraint of the service service inside IIS Tab. Filter Image: Constraint of the service service inside insite inside inside inside inside inside inside inside in	_ TASKS ▼ ⊙
	WIN-J98QEP0G2JF World Wide Web Publishing Service WSVC Running WIN-J98QEP0G2JF Application Host Helper Service AppHostSvc Running WIN-J98QEP0G2JF Windows Process Activation Service WAS Running WIN-J98QEP0G2JF Windows Process Activation Service WAS Running Restart Services Restart Services Restart Services Pause Services Resume Services Copy	3. Righ Click on World Wide Web Publising Service and selcet Stop.
SERVICES All services 3 total	 ٩ ٩ ٩ 	TASKS
Server Name Display Nam WIN-J98QEP0G2JF World Wide	me Service Name Status Start Type Web Publishing Service W3SVC Stopped Automatic	

Start up the Webgoat by opening the Webgoat-5.4 extracted folder on your Windows Server 2012 VM. In our case the Webgoat-5.4 is extracted inside our administrator download folder.

Navigate inside the extracted folder and double click on the WebGoat.bat (Don't use the WebGoat_8080.bat file). By default, a file extension is hidden we can enable from folder view menu. Click on the view menu inside the folder and check File Name Extensions on top right menu options.

▶ > ▶ = File Home Share	Application Tools Manage View File extension	We menu bar and check	bGoat-5.2 File name Exte	ensions to	- □ × -∷ ?
Preview pane Details pane Navigation pane •	Extra large icons Large icons Small icons List Tiles Content	ons ▲ v Sort by v Siz	oup by • d columns • e all columns to fit	 ☐ Item check boxes ✓ File name extensions Hide nitems 	Options
Panes	Layout	Curr	ent view	Show/hide	
🗼 Downloads	👢 tomcat	4/17/2018 3:48 PM	ile folder		
😹 Recent places	readme.txt	4/17/2018 3:47 PM	Fext Document	8 KB	
	🔍 webgoat.bat	4/17/2018 3:47 PM	Windows Batch File	e 1 KB	
🧱 Libraries	webgoat.sh	4/17/2018 3:47 PM	SH File	2 KB	
locuments 🔍	webgoat_8080.bat	4/17/2018 3:47 PM	Windows Batch File	e 1 KB	
🕹 Music					
le Pictures					

You should see a status windows appear and Apache/Tomcat running:

Now, minimize this window.

Do not close this windows during the lab, as it will stop the Apache service as well as WebGoat!



After it starts, open firefox inside your Windows Server 2012 server, and navigate to.

http://localhost/WebGoat/attack

Make sure the W and G on webgoat is capital.

You will next be prompted with a login. Log in with account:

Username: guest

Password: guest

Home × Windows Server 2012	K Contraction of the second	
• New Tab X	+	_ 🗇 🗙
\leftrightarrow × \bigstar	Q. localhost/WebGoat/attack	\ ⊡ ≡
6	Q. Search the Web → Import Now Import Now Import Now Im	*

Webgoat welcome interface.

→ C' û	i localhost/WebGo	at/attack	≣ … ◙ ☆
	- 7	H Charling	
Stars	and the second s	multiple and the second s	à
OWASP WebG	ant VE 2		
UWASP WebG	oat v5.2		
T he set 1 (1997)		The second se	
I hank you for usin exercises are inte	ng WebGoat! This program is a de inded to provide hands on experie	emonstration of common web application flaws. The ince with application penetration testing techniques.	
		····· ································	
The WebCest and			
WebGoat pro	ject is lead by Bruce Mayhew. Ple	ease send all comments to Bruce at	
WebGoat@owasp	oject is lead by Bruce Mayhew. Ple p.org.	ease send all comments to Bruce at	
Thanks to () O	ject is lead by Bruce Mayhew. Ple p.org. UNCE LABS for supporting B	ease send all comments to Bruce at iruce on the WebGoat Project.	
The WebGoat@owasp WebGoat@owasp	ject is lead by Bruce Mayhew. Ple 5.org. UNCE LABS for supporting B	ease send all comments to Bruce at iruce on the WebGoat Project.	
The WebGoat@owasp	iject is lead by Bruce Mayhew. Ple 5.org. UNCE LABS for supporting B	ASPECT) SECURITY	
Thanks to (1)	iject is lead by Bruce Mayhew. Ple b.org. UNCE LABS for supporting B OWASP The Open Web Application Security Project	ASPECT) SECURITY	
Thanks to (1)	iject is lead by Bruce Mayhew. Ple b.org. UNCE LABS for supporting B OWASP The Open Web Application Security Project WebGoat Design Team	ASPECT) SECURITY ASPECT) Applications Security Specialities Lesson Contributers	
The webGoat @owasp	iject is lead by Bruce Mayhew. Ple b.org. UNCE LABS for supporting B OVASP The Open Web Application Security Project WebGoat Design Team Bruce Mayhew David Anghreson	ASPECT Security Application Security Application Security Applications Security Sherf Konsea	
The webGoat @owasp	iject is lead by Bruce Mayhew. Ple 5.org. UNCE LABS for supporting B OPPORT Not Application Source in Project WebGoat Design Team Bruce Mayhew Dand Anderson Rogan Dawes Larence Clasey (Graphics)	ease send all comments to Bruce at iruce on the WebGoat Project. ASPECT)SECURITY Application Security Security Sherf Koussa Romain Brechet	
The webGoat @owasp	iject is lead by Bruce Mayhew. Ple 5.org. UNCE LABS for supporting B OPPORT Web Application Sourity Project WebGoat Design Team Bruce Mayhew Dand Angheson Rogan Dawes Laurence Casey (Graphics) Concil Theorem for M 0	ASPECT Security Application Security Application Security Application Security Sherff Acrossa Romain Brechet	
The webGoat @owasp	iject is lead by Bruce Mayhew. Ple 5.org. UNCE LABS for supporting B OPEN Web Application Scaring Project WebGoat Design Team Bruce Mayhew David Anderson Rogan Davies Laurence Casey (Sraphics) Special Thanson	ease send all comments to Bruce at iruce on the WebGoat Project. ASPECT)SECURITY Applications Security Specializes Lesson Contributers Aspect Security Sherif Koussa Romain Direchet Sherif Koussa	
Thanks to (1)	oject is lead by Bruce Mayhew. Ple 5. org. UNCE LABS for supporting B OVASP The Open Web Application Security Project WebGoat Design Team Bruce Mayhew David Anderson Rogan Dawes Laurence Casey (Graphics) Special Thanks for V5.2 Reto Lippuner Marcel With	ease send all comments to Bruce at inuce on the WebGoat Project. ASPECT)SECURITY Applications Security Specialists Lesson Contributers Aspect Security Sherif Koussa Romain Brechet Documentation Frechet Sherif Koussa Aung Khant Direction Specialist	
Thanks to (1)	oject is lead by Bruce Mayhew. Ple p.org. UNCE LABS for supporting B WebGoat Design Team Bruce Mayhew David Anderson Rogan Dawes Laurence Casey (Graphics) Special Thanks for V5.2 Ret Lippuner Marcel Wirth To all who have sent comments	Aspect Security Roman Brecket Sherif Koussa Roman Brecket Documentation Contributers Sherif Koussa Roman Brecket Documentation Contributers Sherif Koussa Aung Khart (http://yehg.org) Chrim German Langer	
Thanks to (1)	iject is lead by Bruce Mayhew. Ple 5. org. UNCE LABS for supporting B WebGoat Design Team Bruce Mayhew David Anderson Rogan Dawes Laurence Casey (Graphics) Special Thanks for V5.2 Rea Lippuner Marcel Wirth To all who have sent comments	Aspect Security Aug Koutes Roman Brecket Sherif Koussa Roman Brecket Documentation Contributers Sherif Koussa Roman Brecket Documentation Contributers Sherif Koussa Kong Khant (http://www.zionsecurity.com/)	

Most of these exercises will be done with Burp Suite, a full feature web proxy. Start burp from you windows server 2012 VM desktop or starup screen. The startup screen prompt you with an option to create or open an existing project. We will select a default option and continue with temporary project and select next and click start Burp on next window with the default option. It will take few minutes to load the dashboard.



8	Burp Suite Community Edition v1.7.33							
?	Welcome to Burp Suite Con Note: Disk-based projects a	mmunity Edition. Use t	dition. Use the options below to create or open a project.					
	Temporary project	<⊐ 1. Default O	ption					
	New project on disk	File:			С	hoose file		
		Name:						
	Open existing project							
	• open enising project		Name	File				
		File:			С	hoose file		
			Pause Spider and Scanner		2	. Click Next		
					Cancel	Next		

8		Burp Suite Community Edition v1.7.33	
?	Select the configuration that you would like to lo	ad for this project.	BURPSUITE
	● Use Burp defaults <⊐ 1. Select Defa	ult	
	Use options saved with project		
	Load from configuration file	File	
	File:		Choose file
	Disable extensions		2. Click Start

Burp Suit dashboard.

-				Bu	irp Suite (Commur	nity Edition v1	.7.33 - Te	mporary	Project				-	- 🗆 X
Burp Intruder Repeater Window	lelp														
Target Proxy Spider Scan	er Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User option	ns Alerts						
Site map Scope															
Filter: Hiding not found items; hiding	CSS, image a	nd general bi	nary content;	hiding 4xx re	sponses; hidi	ng empty fo	olders								?
			Host		Method	URL		Params	Status 4	Length	MIME type	Title	Com	ment	Time requ
			4												
			Request	Response)					_					
			Raw He		I										
			Naw me	EA											Ă
															n - 1
															Y
			? <	+	> Type a	a search ter	m								0 matches

We now need to configure Firefox to route all web traffic the Burp suite. This can be done by selecting the menu button on the top right corner of your Firefox browser and select options.



Inside General scroll down to the bottom for Network Proxy options and click on settings.

✿	General	Performance
Q	Search	✓ Use recommended performance settings Learn more
	Privacy & Security	These settings are tailored to your computer's hardware and operating system.
C	Firefox Account	Browsing
		✓ Use <u>a</u> utoscrolling
		✓ Use smooth scrolling
		Show a touch <u>keyboard</u> when necessary
		Always use the <u>c</u> ursor keys to navigate within pages
		Search for text when you start typing
		Network Proxy
?	Firefox Support	Configure how Firefox connects to the Internet Click on Settings

Use the following settings as shown on the screenshot. Select Manual proxy configuration use localhost as HTTP proxy with port number 8080 select Sock $\underline{v}5$ and click ok to apply the setting and close the options tab.

	Connection Settings			
				^
Configure Proxies to Access th	ne Internet			
O No proxy				
 Auto-detect proxy settings for 	this net <u>w</u> ork			
<u>U</u> se system proxy settings				≡
<u>Manual proxy configuration</u>	<□1. Select Manual Proxy Configuation	3. Use	port 8080	
HTTP Proxy localhost	<⊐ 2. use localhost for HTTP proxy	<u>P</u> ort	8080 ÷	
U <u>s</u> e this prox	xy server for all protocols			
SS <u>L</u> Proxy		P <u>o</u> rt	0 -	
<u>F</u> TP Proxy		Po <u>r</u> t	0	
SO <u>C</u> KS Host		Por <u>t</u>	0	
SOC <u>K</u> S v4	● SOCKS v5 <=> 4. Select Socks v5			
<u>N</u> o Proxy for				
				~
5. Click	t on Ok to Apply the settings $rac{>}$ OK	Cancel	<u>H</u> elp	

If you have set this up correctly, you can now click on the **Start WebGoat** button on the page open inside Firefox, and the **POST** request to the webserver form your Firefox browser should be captured by the Burp Suit as show (notice the intercept on button is in use):

1975	- ann	mm Lessarta
OWASP WebGoat	V5.2	
Thank you for using exercises are intende	WebGoat! This program is a de ed to provide hands on experier	monstration of common web application flaws. The nce with application penetration testing techniques.
The WebGoat project WebGoat@owasp.or	t is lead by Bruce Mayhew. Ple rg.	ase send all comments to Bruce at
Thanks to 🕕 OUI	NCE LABS for supporting Bi	ruce on the WebGoat Project.
	OWASP The Open Web Application Security Project	
	WebGoat Design Team	Lesson Contributers
	Bruce Mayhew David Anderson Rogan Dawes Laurence Casey (Graphics)	Aspect Security Sherif Koussa Romain Brechet
	Special Thanks for V5.2	Documentation Contributers
	Reto Lippuner Marcel Wirth	Sherif Koussa Aung Khant (http://yehg.org/)
	To all who have sent comments	Erwin Geirnaert (http://www.zionsecurity.com/)
	Start \	WebGoat <a>Click Start
		WebGoat to POST
		Kequest

Burp Suite Community Edition v1.7.33 - Temporary Project
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Alerts
Intercept HTTP history WebSockets history Options
C Select Intercept Request to http://localhost.80 [127.0.0.1]
Forward Drop Intercept is on Action
Raw Params Headers Hex ¹ 3. Notice the Intercept is selected
POST /WebGoat/attack HTTP/1.1
Host: localhost
User-Agent: Rosilla/S.U (Windows MT 6.2; WUWC4; TV:SS.U) 6e268/2U100101 FireFox/SS.U
h = h = 0, $h = h = 1$, $h = h = 0$.
Accept English, di statistica di sta
Referer: http://localhost/WebGoat/attack
Content-Type: application/x-wwww-form-urlencoded
Content-Length: 19
Cookie: JSESSIONID=FF04A03405CB1491DFDABFC926CDD3F0
Authorisation: Basic Z3V1c3Q6Z3V1c3Q=
Connection: close
Upgrade-Insecure-Requests: 1
start=Start+WebGoat

Click the **Forward** button as shown in the above screenshot to allow the request through the burp suit proxy.

Optionally, you can click on the **Intercept On** button in the Burp Suit to disable the holding of requests. This will allow all requests to flow through the brup suite proxy uninterrupted. After clicking on forward button, switch back to your Firefox and see a Webgoat Home page with different Options on Left panel.



Step 1

Go to the WebGoat application in your browser. Click on the **Parameter Tampering** link on the menu on the left, and select **Exploit Hidden Fields** as shown:



This page simulates a shopping cart feature on a website.

Purchase the TV normally to see how it work (it shows an amount charged to credit card of 2999)



Solution VideosTry to purchase the HDTV for less than the purchase price, if Restart this Lesson you have not done so already.

Shopping Cart

Shopping Cart Items To Buy Now	Price:	Quantity:	Total
56 inch HDTV (model KTV-551)	2999.99	1	\$2999.99
The total charged to your credit card:	\$2999.99	Update Cart	Purchase
		ASPECT	ECURITY plication Security Specialist

OWASP Foundation | Project WebGoat | Report Bug

Targe	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts
Interce	ept HTTI	P history	WebSocke	ts history	Options							
Re Fo	Request to http://localhost:80 [127.0.0.1] Forward Drop Intercept is on Action											
Raw	Raw Params Headers Hex											
GET / Wel	Goat/att	ack?Scree	en=536menv	1500 HTT	P/1.1							
Host: 10	calhost											
User-Age	Jsex-Agent: Mosilla/5.0 (Windows NT 6.2; W0W64; rv:59.0) Gecko/20100101 Firefox/59.0											
Accept:	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8											
Accept-I	Accept-Language: en-US, en;q=0.5											
Accept-H	Accept-Encoding: gsip, deflate											
Aeferer: http://localhost/WebGoat/attack												
:ookie: JSESSIONID=FF04A834052B1491DFDABFC9262DD3F8												
Authoris	uthorisation: Basic Z3V1c3Q6Z3V1c3Q=											
Connect	ion: clos	e										
Upgrade.	grade-Insecure-Requests: 1											

POST request captured on Burp Suite for the request Exploit Hidden Field page.

Now, we want to enable Burp Suite to capture requests. Click the Intercept Off button in burp suite if it is set to Intercept Off. If it already shows Intercept On, do not click it.

Intercept HTTP history WebSockets history Options				
Click on Intercept off to enable Intercept				
Forward Drop Intercept is off Action				
Raw Params Headers Hex				
Intercept HTTP history WebSockets history Options				
Intetercept Mode On				
Forward Drop Intercept is on Action				
Raw Params Headers Hex				

Now, go back to the WebGoat application and click the purchase Button.

Solution VideosTry to purchase the HDTV for less than the purchase price, if Restart this Lesson you have not done so already.

Shopping Cart

Shopping Cart Items To Buy Now	Price:	Quantity:	Total	
56 inch HDTV (model KTV-551)	2999.99	1	\$2999.99	
The total charged to your credit card:	\$2999.99	Update Cart Pu	irchase	<⊐ Click on Purch
		ASPECT	CURI tion Security Speci	T Y ialists

OWASP Foundation | Project WebGoat | Report Bug

Change the contents of the Price field to 5.00 and click Forward to complete the attack



You will see the new price you added. If this were a real application, it would get submitted to the company. If there is no manual checking of the prices, and automated fulfillment, the item would be send out.

Solution VideosTry to purchase the HDTV for less than the purchase price, if Restart this Lesson you have not done so already.

* Congratulations. You have successfully completed this lesson.

Your total price is: \$5.0

This amount will be charged to your credit card immediately.



OWASP Foundation | Project WebGoat | Report Bug

Exercise 2 Cross Site Scripting (XSS)

In this lab we will be looking at how to perform a Cross Site Scripting attack against a "stored" Cross Site Scripting vulnerability. The general goal of a Cross Site Scripting attack is to have a user other than yourself execute a script/function on your behalf using their permission. One common thing is executing password change, where a user unknowingly changes their password to something picked by the attacker via a script. Another example and probably the most common demonstration is having a user send the attacker his/her session cookies or tokens. This is precisely the attack we'll demonstrate in this exercise.

To begin, go back to the WebGoat start page. Remember if you've still got the *intercept on* enabled in Burp, you'll need to make sure you go there and hit the *forward* button for each browsing action.

Once you're back at the WebGoat start page, Select Cross Site Scripting > Stage 1 Stored XSS.



Just another friendly reminder, make sure you hit the forward button on the Burp Suite proxy if you have it enabled, otherwise it'll appear nothing is happening when you browse from step to step.

The instructions say the following;

As Tom, execute a stored XSS attack against the stree field on the edit profile page. Verify that jerry is affected by the attack.

So, we'll actually be doing this as Tom. But we'll want our script injection to affect Jerry. First step is to login as Tom. As the instructions tell us, each user's password is simply the all lower-case version of the username. To login as Tom, click the drop-down button and select Tom's name form the list.



Enter "tom" as the password for the Tom Cat account, then select the login button. After logged in, select the "View profile" option.

	Request to http://localhost:80 [127.0.0.1]						
3. We need to Forward the POST request to	Forward Drop Intercept is on Action						
	Raw Params Headers Hex 1. Make note of Intercept is enable or off						
successfully login.	POST /WebGoat/attack?Screen=336menu=900 HTTP/1.1						
• •	Host: localhost						
	User-Agent: Mosilla/5.0 (Windows NT 6.2; W0W64; rv:59.0) Gecko/20100101 Firefox/59.0						
	Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8						
	Accept-Language: en-US, en; q=0.5						
	ccept-Encoding: gsip, deflate						
	eferer: http://localhost/WebGoat/attack						
	<pre>content-Type: application/x-www-form-urlencoded</pre>						
	ontent-Length: 41						
	:ookie: JSESSIONID=FF04A834052B1491DFDABFC9262DD3F8						
	Authorisation: Basic Z3V1c3Q6Z3V1c3Q=						
	Connection: close						
	Upgrade-Insecure-Requests: 1						
	employee_id=105&password=tom&action=Login <> 2. View the Post method detail and note the login details.						

Next, you'll want to select the employee form the list and click Edit Profile button.

Solution VideosStage 1: Execute a Stored Cross Site Scripting (XSS) attack. Restart this Lesson As 'Tom', execute a Stored XSS attack against the Street field on the Edit Profile page. Verify that 'Jerry' is affected by the attack. The passwords for the accounts are the prenames.

E.	Goat Hills Financial Human Resources
👬 Welcome	e Back Tom - Staff Listing Page
Select from the	a list below
Tom Cat (er	nployee) $\leq \square$ 1. Select the employee from the list
	SearchStaff
	ViewProfile <= 2. Click on ViewProfile
	Logout
	✓

Next you'll want to select the Edit Profile button.

Solution VideosStage 1: Execute a Stored Cross Site Scripting (XSS) attack. Restart this Lesson As 'Tom', execute a Stored XSS attack against the Street field on the Edit Profile page. Verify that 'Jerry' is affected by the attack. The passwords for the accounts are the prenames.

Goat Hills Financial Human Resources				
🙀 Welcome Ba	ack Tom			
First Name:	Tom	Last Name:	Cat	
Street:	2211 HyperThread Rd.	City/State:	New York, NY	
Phone:	443-599-0762	Start Date:	1011999	
SSN:	792-14-6364	Salary:	80000	
Credit Card:	5481360857968521	Credit Card Limit:	30000	
Comments:	Co-Owner.	Manager:	106	
Disciplinary Explanation:	NA	Disciplinary Action Dates:	0	
	<u> </u>			
Emp	loyee Information			
ListStaff EditProfile				
Listotan	changes o	n Profile Details.	Logout	

Here we'll see all the editable fields for this profile. In the street field we will attempt to add a script that would be executed by any other user viewing Tom's Profile.

	E Cart	Goat Hills F Human Resourc	inancia es	l .
	Welcome	Back Tom		٢
	First Name:	Tom	Last Name:	Cat
1. Add Script Here ∟	Street:	ed by infosec")	City/State:	New York, NY
	Phone:	443-599-0762	Start Date:	1011999
	SSN:	792-14-6364	Salary:	80000
	Credit Card:	5481360857968521	Credit Card Limit:	30000
	Comments:	Co-Owner.	Manager:	Tom Cat ∨
	Disciplinary Explanation:	NA 	Disciplinary Action Dates:	0
	ViewProfile	UpdateProfile a	. Click Upda dd Script.	te to Logout

Next, you'll want to make the street field read exactly as it is shown below. You'll be adding the string.

"><script>alert("Owned by infosec")</script>

To what's already there. So the complete entry in the street field should read as follows.

221 HyperThread Rd. "><script>alert("Owned by infosec")</script>

After making the changes, go ahead and click the "Update Profile" button at the bottom to save these changes. You should immediately see a popup alert that says, "Owned by Infosec". See below.



Click Ok and notice the change on Tom Street address field.

Goat Hills Financial Human Resources				
Welcome	Back Tom		C	
First Name:	Tom	Last Name:	Cat	
Street:	2211 HyperThread Rd. ">	City/State:	New York, NY	
Phone:	443-599-0762	Start Date:	1011999	
SSN:	792-14-6364	Salary:	80000	
Credit Card:	5481360857968521	Credit Card Limit:	30000	
Comments:	Co-Owner.	Manager:	105	
Disciplinary Explanation:	NA	Disciplinary Action Dates:	0	

So the goal is Jerry Should basically see this same popup when he views our (Tom's) profile. If he see the script, then that means Tom has been able to successfully "store" a script on this website that is transparently executed by Jerry upon Jerry viewing Tom's profile. This would essentially mean that anyone viewing Tom's profile would execute his script in their browser. Let's test it out and see. You'll need to hit the **logout** button and the button right. Then login again as Jerry.

Latris	Larry Stooge (employee)	Cross Site Scripting
🔫 Hints 🕨 Show Parai	Moe Stooge (manager)	an Show Java Solution
Solution VideosStage 1: E As 'Tom', e on the Edit Profile page. Ver The passwords for the acco	Curly Stooge (employee) Eric Walker (employee) Tom Cat (employee) Jerry Mouse (hr)	(XSS) attack. Restart this Lesson the Street field ack.
Goa Huma	David Giambi (manager) Bruce McGuirre (employee) Sean Livingston (employee) Joanne McDougal (hr) John Wayne (admin) Neville Bartholomew (admin) Larry Stooge (employee) Password Login	

Remember, Jerry's password is simply Jerry in all lowercase format. Once you're logged in as Jerry, select Tom's account, then select the "View Profile" button on the right.

Goat Hills Financial Human Resources				
Select from the list below Tom Cat (employee) Jerry Mouse (hr) Joanne McDougal (hr)	 Staff Listing Page I. Select Tom Cat Profile. SearchStaff 			
	ViewProfile <_ 2. click ViewProfile. CreateProfile DeleteProfile Logout			

Selecting the ViewProfile button should cause the Owned by Infosec popup to now show up in Jerry's browser session. See below.



At this point you'll also see the "You have completed Stage1: Stored XSS" message at this point as well.

The implications are pretty strong here. What if the script did something like "change my password to hacker" or "send my session id to <u>owned@infosecinstitute.com</u>"? These are all function that are very easily coded using Javascript or even just plain old html for that matter!

Exercise 3 Preventing Cross Site Scripting with HTTPOnly flag

Microsoft implemented cookie property, HttpOnly, that can help mitigate Cross-Site Scripting attacks that could lead to stolen tokens, credentials and other malicious attacks. When an **HttpOnly** cookie is passed by any browser able to understand it, it become inaccessible to client-side scripts. This is one way of preventing Cross Site Scripting. Internet Explorer 6.0 and earlier does not support HttpOnly.

In this WebGoat exercise, we'll be looking at the differences between when the HttpOnly flag is set and when it's not.

Click on the "HttpOnly Test" portion on the WebGoat home page under Cross Site Scripting. See below:

Introduction General Access Control Flaws	Solution VideosTo help mitigate the cross site scripting threat, Microsoft has new cookie attribute entitled 'HttpOnly.' If this					
AJAX Security Authentication Flaws Buffer Overflows	flag is set, then the browser should not allow client-side script to access the cookie. Since the attribute is relatively new, several browsers neglect to handle the new attribute properly.					
Code Quality	For a list of supported browsers see: OWASP HTTPOnly Support					
Cross-Site Scripting (XSS)	General Goal(s): ect Cross-Site Scripting					
<u>Phishing with XSS</u> LAB: Cross Site Scripting	The purpose of this lesson is to test whether your browser supports the HTTPOnly cookie flag. Note the value of the unique2u cookie. If your browser supports HTTPOnly, and you enable it for a					
•	cookie, client side code should NOT be able to read OR write to that cookie, but the browser can still send its value to the server. Some browsers only prevent client side read access, but don't prevent					
Stage 1: Stored XSS	write access.					
Stage 2: Block Stored XSS using Input Validation	With the HTTPOnly attribute turned on, type "javascript:alert(document.cookie)" in the browser address bar. Notice all cookies are displayed except the unique2u cookie.					
Stage 3: Stored XSS Revisited						
Stage 4: Block Stored XSS using Output Encoding	Your browser appears to be: firefox/59.0					
Stage 5: Reflected XSS	Do you wish to turn HTTPOnly on? Yes No					
Stage 6: Block Reflected XSS	Read Cookie Write Cookie					
Stored XSS Attacks						
<u>Cross Site Request Forgery</u> (CSRF)						
Reflected XSS Attacks	TTEOply Test Make Sure HTTPOnly is turn On before / Application Security Specialists					
	OWASP Foundation Project WebSoat Report Bug					
<u>Cross Site Tracing (XST)</u> <u>Attacks</u>	BurpSuite.					

You'll want to make sure you've enabled intercept in the Burpsuite proxy.

Request to http:	://detectportal.firefox	com:80 [unknown ho	st]	
Forward	Drop	Intercept is on	Action)
		企		

Turn Intercept Mode back On

Once you've made sure intercept is on, you'll want to go back to the WebGoat page and select the radio button turn off HTTPOnly. See below.

With the HTTPOnly attribute turned on, type "javascript:alert(document.cookie)" in the browser address bar. Notice all cookies are displayed except the unique2u cookie.

Your browser appears to be: firefox/59.0		Tu	m Off HTTPOnly	Ī
Do you wish to turn HTTPOnly on?	Yes	0	No 🔘	
Read Cookie Write Cookie				
	ASPE	ст	SECURITY Application Security Specialist	

OWASP Foundation | Project WebGoat | Report Bug

Once you make this change you should see your Burpsuite icon at the bottom of the screen flashing to let you know it's intercepted some data. Go ahead and switch to the Burpsuite screen. Notice the HttpOnly variable is set to false.



Go ahead and hit the Forward button to pass the change.

Next, we're going to see if we can read a cookie while the HttpOnly flag is turned off. Click the Read Cookie button. You should see the following cookie pop up.

≺ Hints ト			Lesson Plan		Solution		
Solution Video	- - - + +			Chilan Dav			
Attribute is rela	unique2u=D	G2NyNtp9/3pqRrHB	kPaCL8PeNE=; JS	ESSIONID=35	891E0B2DA17A0E	DE5D33366197D1C4D	
General Goal(The purpose of the value of the cookie, client si send its value t write access.	o the server. So	me prowsers only pr	event client side t	eau access, pu	at don't prevent	ОК	
With the HTTPC address bar. No	only attribute tur tice all cookies a	rned on, type "javas are displayed except	cript:alert(docum the unique2u coc	ent.cookie)" in kie.	the browser		
Your browser a	opears to be: fir	efox/59.0					
Do you wish to	turn HTTPOnly	on?	Y	es 🔿 No			
Read Cookie	e Write Coo	kie					
			AS	PECT	ECURITY ation Security Specialists		
OWASP Found	dation Project	WebGoat Report E	lug				

Go ahead and click Ok to the popup. You should now see Burpsuite intercept more traffic.

We can see that the httponly flag is set to false. So therefore the script that's being executed to read the cookie is able to run. This exercise is simply doing the script for you that we did in the earlier XSS lab where caused the Infosec popup. Go ahead and hit the Forward button and return to WebGoat. You should see the following message in red.

Intercept HTTP history WebSockets history Options				
Request to http://localhost:80 [127.0.0.1] Forward Drop Intercept is on				
Raw Params Headers Hex				
POST /WebGoat/attack?Screen=1:64menu=900 HTTP/1.1				
Host: localhost				
User-Agent: Mosilla/5.0 (Windows NT 6.2; W0W64; rv:59.0) Gecko/20100101 Firefox/59.0				
$eq:linearized_linearized$				
Accept-Language: en-US,en;q=0.5				
Accept=Encoding: gmip, deflate				
Referer: http://localhost/WebGoat/attack?Screen=126menu=900				
Content-Type: application/x-www-form-urlencoded				
Content-Length: 138				
Cookie: wrique2u=D62HyHtp5/3pqRrHBkPaCL8PeHE=; JSESSIONID=35891E0B2DA17A0DE5D33366197D1C4D				
Authorisation: Basic Z3V1c3Q6Z3V1c3Q=				
Connection: close				
Upgrade-Insecure-Requests: 1				
httponly=Talse&read_result=uniqueSu\$3DD62HyHtpS\$2F3pqRrHBkPaCL6PeHE\$3D\$3B+JSESSI0HID\$3D35851E0B2DA17A0DE5D33366157D1C4D&action=Read+Cookie				

With the HTTPOnly attribute turned on, type "javascript:alert(document.cookie)" in the browser address bar. Notice all cookies are displayed except the unique2u cookie.

* Since HTTPOnly was not enabled, the 'unique2u' cookie was displayed in the alert dialog.



Next Select the Write Cookie button. Again you'll see a cookie popup and upon hitting OK. You should see traffic in Burpsuite again. This time you'll see the Burpsuite has intercepted a "write cookie" action.

Solution VideosTo help mitig introduced a flag is set, then the browser attribute is relatively new, se For a list of supported browse	unique2u=HACKED; JSESSIONID=35891E0B2DA17A0DE5D33366197D1C4D
The purpose of this lesson is the value of the unique2u of cookie, client side code shoul send its value to the server. So write access.	OK
With the HTTPOnly attribute tur address bar. Notice all cookies a	rned on, type "javascript:alert(document.cookie)" in the browser are displayed except the unique2u cookie.
* Since HTTPOnly was not en	abled, the 'unique2u' cookie was displayed in the alert dialog.
Your browser appears to be: fir	refox/59.0
Do you wish to turn HTTPOnly	on? Yes 🔿 No 💿
Read Cookie Write Coo)kie

Intercept HTTP history WebSockets history Options
Request to http://localhost:80 [127.0.0.1]
Raw Params Headers Hex
POST /WebGoat/attack?Screen=126menu=900 HTTP/1.1
Host: localhost
User-Agent: Momilla/5.0 (Windows NT 6.2; W0W64; rv:55.0) Gecko/20100101 Firefox/55.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US, en; q=0.5
Accept-Encoding: gsip, deflate
Referer: http://localhost/WebGoat/attack?Screen=12&menu=900
Content-Type: application/x-www-form-urlencoded
Content-Length: 47
Cookie: unique2u=HACKED; JSESSIONID=35891E0B2DA17A0DE5D33366197D1C4D
Authorisation: Basic Z3V1c3Q6Z3V1c3Q=
Connection: close
Upgrade-Insecure-Requests: 1
httponly=False&read_result=&action <mark>=Write+Cookie</mark>

Click forward to allow the request back to web browser.

With the HTTPOnly attribute turned on, type "javascript:alert(document.cookie)" in the browser address bar. Notice all cookies are displayed except the unique2u cookie.

* Since HTTPOnly was not enabled, the browser allowed the 'unique2u' cookie to be modified on the client side.

Your browser appears to be: firefox/59.0				
Do you wish to turn HTTPOnly on?	Yes	0	No	\odot
Read Cookie Write Cookie				
	ASPE	ст	SE	CURITY
		/	Applicatio	on Security Specialists

Now go back to WebGoat and this time we're going to turn on the HTTPOnly functionality. Do this by selecting the "Yes" radio button to the right. See below.

	ASPECT
Read Cookie Write Cookie	
Do you wish to turn HTTPOnly on?	Yes 💿 N
Your browser appears to be: firefox/59.0	



Of course, after making this change, you will see alert flashes from Burpsuite yet again. This is because selecting the "Yes" radio button has dynamically changed what's displayed and changed the functionality of the html to an extent. Go ahead and switch to Burpsuite and hit the forward Button.

```
POST /WebGoat/attack?Screen=12&menu=900 HTTP/1.1
Host: localhost
User-Agent: Mosilla/5.0 (Windows NT 6.2; W0W64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gsip, deflate
Referer: http://localhost/WebGoat/attack?Screen=12&menu=900
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Cookie: unique2u=Gp+XB+uaIPg2dD0s/ZHyR962RMc=; JSESSIONID=35051E0B2DA17A0DE5D33366197D1C4D
Authorisation: Basic 23V1c3Q623V1c3Q=
Connection: close
Upgrade=Insecure=Requests: 1
httponly=True&read_result=
```

Now select the Read Cookie button as we did previously. You should see that the popup contains only JSESSIONID.



Go ahead and hit the Ok button. As was before, this will cause another alert in Burpsuite.

Switch the Burpsuite and notice that even though the cookie is there the script was not able to read all the information like unique2u information on cookie in the popup.



Hit the forward button and return to WebGoat. You should see that it tells you you've successfully prevented the script form reading the cookie because HttpOnly was enabled.

 * SUCCESS: Your browser enforced the HTTPONy preventing direct client side read access to this * Now try to see if your browser protects write a 	y flag properly for the 'unique2u' cookie by cookie. Iccess to this cookie.
Your browser appears to be: firefox/59.0	Yes No
Read Cookie Write Cookie	
	ASPECT SECURITY Application Security Specialists

OWASP Foundation | Project WebGoat | Report Bug

Repeat these steps by hitting the "write Cookie" button. Once you get back to Burpsuite, the results should look like the following.

Raw Params Headers Hex	
POST /WebGoat/attack?Screen=126menu=900 HTTP/1.1	
Host: localhost	
User-Agent: Momilla/5.0 (Windows NT 6.2; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0	
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8	
Accept-Language: en-US, en; q=0.5	
Accept-Encoding: gmip, deflate	
Referer: http://localhost/WebGoat/attack?Screen=12&menu=900	
Content-Type: application/x-www-form-urlencoded	
Content-Length: 46	
Cookie: unique2u=Gp+XB+uaIPg2dD0m/ZHyR96ZRMc=; JSESSIONID=35891E0B2DA17A0DE5D33366197D1C4D	
Authorisation: Basic Z3V1c3Q6Z3V1c3Q=	
Connection: close	
Upgrade-Insecure-Requests: 1	
httponly=True&read_result=&action=Write+Cookie	

Go ahead and hit the "Forward" button.

Now return to WebGoat to see that you're completed the lesson.

General Goal(s):

The purpose of this lesson is to test whether your browser supports the HTTPOnly cookie flag. Note the value of the **unique2u** cookie. If your browser supports HTTPOnly, and you enable it for a cookie, client side code should NOT be able to read OR write to that cookie, but the browser can still send its value to the server. Some browsers only prevent client side read access, but don't prevent write access.

With the HTTPOnly attribute turned on, type "javascript:alert(document.cookie)" in the browser address bar. Notice all cookies are displayed except the unique2u cookie.

* SUCCESS: Your browser enforced the write protection property of the HTTPOnly flag for the 'unique2u' cookie by preventing client side modification. * Congratulations. You have successfully completed this lesson.

Your browser appears to be: firefox/59.0

Do you wish to turn HTTPOnly on?

Yes

No

Read Cookie Write Cookie

Exercise 4 Basic SQL Injection

In this WebGoat exercise, we'll be looking at how to perform basic SQL Injection. We'll first do the string injection exercise, then later follow that up with doing a "blind" injection attack. Here's a short definition of what SQL injection is;

"A SQL injection attack consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data form the database, modify database data (Insert/Update/Delete), execute administration operation on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system". -Source OWSP

Let's take a username and login field on a web form for example. Typically when you enter a username and password to login to a database via a web form (such as an online bank login), the username and password are combined to form par of a sql query that basically says "If the username and password I enter match what's in the database (or form a true statement), then do some action on this users behalf." As it turns out there are many ways to make the username and password part of the query equal "true". This is precisely what we'll be doing in this exercise.

Go back to your WebGoat start page and click on Injection Flaws> LAB: Sql Injection> Stage 1: String SQL Injection.



After clicking each link, remember you'll have to go to Burpsuite and hit the "Forward" button to pass the request through the Burpsuite proxy.

The instructions say that we are to try and use the Neville account which has admin privileges to get to the point that we're able perform and admin function. We'll go to that, but first let's look at some basic way to see what's being sent to the application, how it's being sent, and whether or not there are any apparent client-side control pushed to the browser.

First, we'll use the first account in the list to try and see what we can get passed to the Post request that goes to the application.

You should see activity in the Burpsuite proxy. Locate the where the username and password strings are being passed in the proxy. See below.



Notice we can see the infosec string we entered. It's also important to note that the username has been converted to a numeric value and it's being passed using a field identified as employee_id. If we were doing more advanced injection attack such as using SQL functions like INSERT, UNION, etc. We would have to tell SQL to perform the action to a specific field in the database. We now know there's field named "password" and one named "employee_id".

Let's try some basic tests to begin with. In the request that we have paused, let's change the password string of infosec to a single quote ('). See the change below.

Raw	Params	Headers	Hex	
POST /We	bGoat/at	tack?Scre	en=546	menu=1200 HTTP/1.1
Host: 10	calhost			
User-Age	nt: Mosi	11a/5.0 (Window	s NT 6.2; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept:	text/htm	l, applica	tion/x	html+xml, application/xml; q=0.9, */*; q=0.8
Accept-L	anguage :	en-US, en	;q=0.5	
Accept-E	ncoding:	gzip, de	flate	
Referer:	http://	localhost	/WebGo	at/attack?Screen=54&menu=1200&stage=1
Content	Туре: ар	plication	/ 3c = www	-form-urlencoded
Content	Length:	45		
Cookie:	JSESSION	ID=35891E	OB2DA1	7 AODE 5D 3 3 3 5 6 1 9 7D 1C 4D
Authoris	ation: B	asic Z3V1	c3Q6Z3	V1 c 3 Q =
Connecti	ion: clos	e		
Upgrade	Insecure	-Requests	: 1	
employee	id=1016	password=	'Sacti	on=Login

After making the change, go ahead and hit the "Forward" button. If you go back to the WebGoat page, you should see that the login simply failed.

e pe	Goat Hills Financial
1	Human Resources
άŘ.	
	Please Login
	Larry Stooge (employee) V
	Password
	Login

You should be back at the login field. Now click the drop down and change the login name to the Neville admin account. Repeat the process, using the password of infosec. After you've captured the request in Burpsuite. Make the following change;

After the password identifier, enter the following 'OR 1=1--

That is single quote, OR space, one. Equal sign, one, dash dash. See below.



Raw Params Headers Hex
POST /WebGoat/attack?Screen=54&menu=1200 HTTP/1.1
Host: localhost
User-Agent: Momilla/5.0 (Windows NT 6.2; WOW64; rv:59.0) Gecko/20100101 Firefox/59.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US, en; q=0.5
Accept-Encoding: gsip, deflate
Referer: http://localhost/WebGoat/attack?Screen=54&menu=1200
Content-Type: application/x-www-form-urlencoded
Content-Length: 45
Cookie: JSESSIONID=35891E0B2DA17A0DE5D33366197D1C4D
Authorisation: Basic Z3V1c3Q6Z3V1c3Q=
Connection: close
Upgrade-Insecure-Requests: 1

employee_id=1124<mark>password=infosec</mark>&action=Login



Next go ahead and hit the "Forward" button to pass the request. If you typed everything exactly right. You should notice now that on the WebGoat page, you're informed that you've completed this lesson.

Solution VideosStage 2: Block SQL Injection using a Parameterized Query. Restart this Lesson Implement a fix to block SQL injection into the fields in question on the Login page. Repeat stage 1. Verify that the attack is no longer effective.

* You have completed String SQL Injection.

* Welcome to Parameterized Query #1

Goat Hil Human Res	Is Financial ources
Welcome Back Neville - Stat	ff Listing Page
Select from the list below Larry Stooge (employee) Moe Stooge (manager) Curly Stooge (employee) Eric Walker (employee) Tom Cat (employee) Jerry Mouse (hr) David Giambi (manager) Bruce McGuirre (employee) Sean Livingston (employee) Joanne McDougal (hr) John Wayne (admin)	 ∧ SearchStaff ViewProfile CreateProfile DeleteProfile Logout

At this point, if we wanted to, we could delete profiles, view profiles and do other functions under the privilege of the admin Neville admin account. Let's move on to the next exercise and do Blind SQL Injection using numeric values and operators.

Exercise 5 Blind SQL Injection

NOTE: You need to have WebGoat Version 5.4 to complete Blind SQL Injection. You can download the zip file like the earlier version, but you need to make sure you must only run one WebGoat version at a time. WebGoat version 5.4.zip will be provide by the instructor along with the lab contents.

In this exercise we're going to work on the premise that we've got a stolen credit card or at least, we know the credit card number. We're then going to try and do Blind SQL Injection to a credit card database and extract the card's PIN. Basically, we'll use a comparison operator to try and get SQL to tell us when we've gotten close to the correct PIN, then eventually narrow it down to

the extract PIN associated with the given credit card number. We're given a few of the table names, which are generally created using standard naming conventions.

Start by going back to the WebGoat start page and selecting Injection Flaws > Lab:SQL Injection > Blind Numeric SQL Injection.

See Below.



Based on the instructions, we are to find the value in the field *field* **pin** which is part of the *table* **pins** for the *row* with the **cc_number** of **1111222233334444**.

So behind this form there is a database with a table named pins, which has a field name pin, which also has a row named cc_number. And we have a known credit card number. The form we're presented with is basically created to check a number to see if it's a valid account number. There is probably a field in the database named "account_number" or something like that. But we don't know that for sure, and right now it's not required that we know it, as wer're simply using this part of the form to create a query to try and access other parts of the database.

You'll want to make sure you turn the intercept function off in the Burpsuite proxy before starting this exercise.

First let's do a simple test and find out if we can quickly discern the approximate number of valid accounts. Change the 101 in the field to 102 and hit the Go button.

The goal is to find the value of the field **pin** in table **pins** for the row with the **cc_number** of **1111222233334444**. The field is of type int, which is an integer.

Put the discovered pin value in the form to pass the lesson.

Enter your Account Number: 102	Go!
Account number is valid.	
	INTELLIGENT INFORMATION SECURITY

OWASP Foundation	Project WebGoat	Report Bug
------------------	-----------------	------------

It should have returned the message to inform you that 102 is a valid account. Repeat this with 103, 104, etc.

Notice how will the 104 number being entered the message changes to say the account number is not valid. Now got down from 101. Try 100, then 99 and continue down until you get the invalid account number message again. What you should have figured out is that the valid account number appear to range from 101 to 103. Now for the blind part. Since we know some valid account numbers, we can try to use them to pass other commands to the database on the backend.

Enter the following query in the form field;

101 AND ((SELECT pin FROM pins WHERE cc_number='1111222233334444') > 100);

Now go ahead and hit the Go button. Immediately you should see that the message that confirms a valid account number returns again. This means that what we've just said is "TRUE" as far as SQL is concerned.



So, what we know no is that pin for the given credit card number is greater than 100. Awesome! That really narrows it, down right?

Now let's repeat that with a higher number. Change the number at the end of your query from 100 to 1000. Then hit enter again.



When you hit the Go button, the "Account number is valid" response remains. So that means we now know the credit card PIN is more than 1000.

Now change the value to 10000. Hit Go again.

Put the discovered pin value in the form to pass the lesson.
Enter your Account Number: 233334444') > 10000; Go!
Invalid account number.

OWASP Foundation | Project WebGoat | Report Bug

Whoa! We got a different response. This means that we just said something to SQL that's not true. Essentially, the PIN we're looking for is not greater than 10000, but it is more than 100.

Let's try to narrow it down some more. Try changing the value to 5000. What response do you get?

Response should have been Invalid account number. Which means the PIN we're searching for is not greater than 5000.

Let's cut that in half. Change the value to 2500. Hit Go. The response we get back is still Invalid account. So we know it's less than (or equal to) 2500.

Next try the value of 2200. You should see that it now say Valid Account number again.



OWASP Foundation | Project WebGoat | Report Bug

Before looking below at the answer. Go ahead and keep incrementing and decrementing the value until you find out what the PIN is. If you can't figure it out after a few minutes, keep following this lab.

Now change the value to 2250. Hit Go again. You should that we get a valid account number response again. Now try 2260. It should return valid again. Next try 2265. This brings us another valid account response. Try 2275.

Ok. I think you get the point here! Let me help you speed up the process. Just understand that you might have to spend hours doing this in the real world to eventually find what you're looking for. Try the value of 2363. It should return that it's a valid account number.

Put the discovered pin value in the form to pass the lesson. Enter your Account Number: (2233334444') > 2363); Go! Account number is valid. Created by Chuck ANDIA Willis OWASP Foundation | Project WebGoat | Report Bug Now try 2364 We get an invalid account number response. Put the discovered pin value in the form to pass the lesson. Enter your Account Number: (2233334444') > 2364); Go! Invalid account number. Created by Chuck IZANDIAI Willis INTELLIGENT INFORMATION SE

OWASP Foundation | Project WebGoat | Report Bug

So if the PIN for the credit card number is greater than 2363, but not greater than 2364, then we can assume the actual pin is 2364. Since we know that pins are not typically used in decimal notation, it has to be a whole number that is more than 2363 but not than 2364. There's only one whole number that meets that criteria. 2364! Problem Solved. Blind Injection accomplished.

Go ahead and claim your prize by entering the string 2364 into the form field. See below.

The form below allows a user to enter an account number and determine if it is valid or not. Use this form to develop a true / false test check other entries in the database.

The goal is to find the value of the field **pin** in table **pins** for the row with the **cc_number** of **1111222233334444**. The field is of type int, which is an integer.

Put the discovered pin value in the form to pass the lesson.

* Congratulations. You have successfully completed this lesson.

Enter your Account Number: 2364 Go! Created by Chuck Created by Chuck Willis

OWASP Foundation | Project WebGoat | Report Bug