

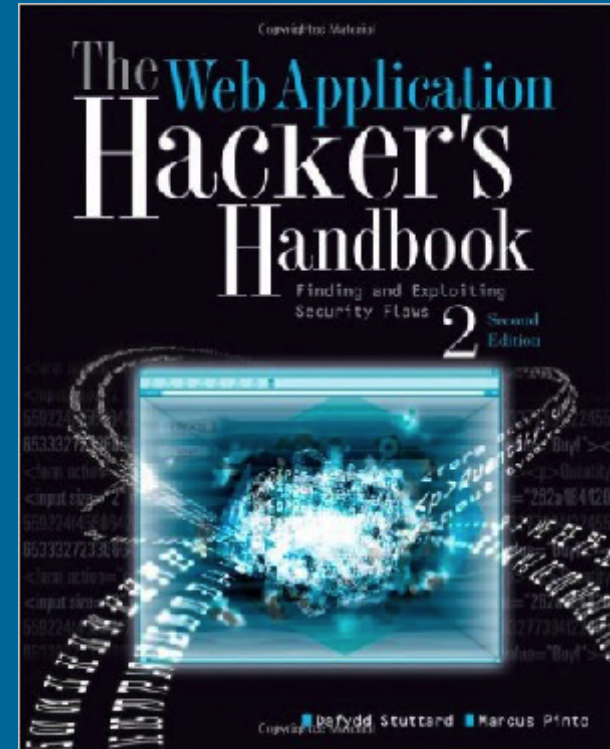
CNIT 129S: Securing Web Applications

39237 501 Mon 6:10-9:00 PM

Moved to SCIE 37

Spring 2019 -- Sam Bowne

[Schedule](#) · [Lecture Notes](#) · [Projects](#) · [Links](#) · [Home Page](#)



Course Justification

Industry advisors have repeatedly asked us to teach this class, because every modern business needs a web presence and there are far too few workers qualified to protect them from hackers. There are many jobs available for students who learn how to protect our healthcare, financial, and other confidential data from criminals, spies, and pranksters.

Catalog Description

Techniques used by attackers to breach Web applications, and how to protect them. How to secure authentication, access, databases, and back-end components. How to protect users from each other. How to find common vulnerabilities in compiled code and source code.

Advisory: CNIT 131 and CNIT 120, or comparable familiarity with websites and security concepts

Major Learning Outcomes

Upon successful completion of this course, the student will be able to:

- A. Explain the current state of Web application security
- B. Analyze basic application functionality
- C. Secure data stores and back-end components
- D. Protect users from other users
- E. Demonstrate common exploits and patch their root causes
- F. Implement servers and firewalls effectively

Textbook

"The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition", by Dafydd Stuttard , Marcus Pinto;
ISBN-10: 1118026470 [Buy from Amazon](#)

Quizzes

The quizzes are multiple-choice, online, and open-book. Study the textbook chapter and take the quiz before that class. Each quiz is due 30 min. before class. Each quiz has 5 questions, you have ten minutes to take it, and you can make two attempts.

To access the quizzes:


- Go to <https://canvas.instructure.com/enroll/KNXMN6>
- If you've taken one of my class previously, you should already have an account on this Canvas server (it's NOT the usual CCSF Canvas system). Otherwise, create a new account.
- You should see the quizzes, as shown below.
- **Questions?** Email CNIT.129S@gmail.com

canvas.instructure.com/courses/1508433

129S-S19 > Assignments


Recent Announcements

Home
Announcements
Assignments
Grades
Quizzes

 **Welcome to the class!**
CNIT 129S: Securing Web Applica... Posted on: Jan 10, 2019 at 1:42pm

SHOW BY DATE SHOW BY TYPE

▼ Upcoming Assignments

 **Quiz Ch 1 and 2**
Due Jan 28 at 5:30pm | -/20 pts

Live Streaming

Live stream at: <https://zoom.us/j/4108472927>

Classes will also be recorded and published on YouTube for later viewing.

Schedule (subject to revision)

Date

Quiz

Topic

Mon
1-14

Ch 1: Web Application (In)security
Ch 2: Core Defense Mechanisms



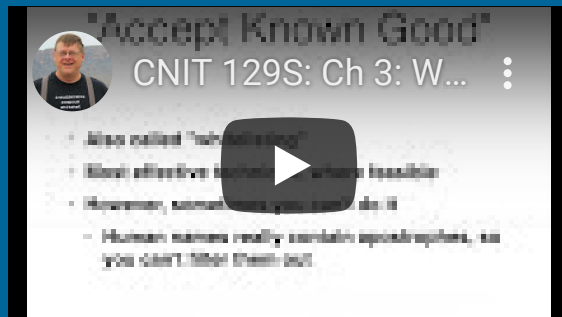
Mon
1-21

Holiday - No Class

Mon
1-28

Quiz Ch 1-2 *
Proj 1 due

Ch 3: Web Application Technologies

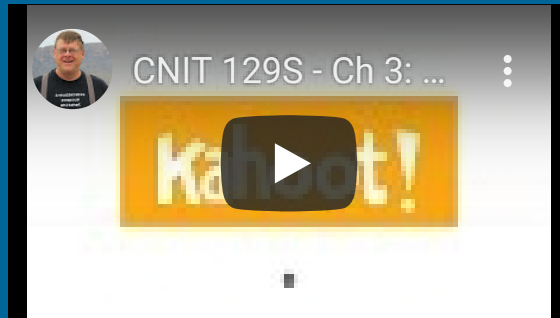


Fri 2-1 *Last Day to Add Classes*

Ch 3: Web Application Technologies (continued)

**Mon
2-4**

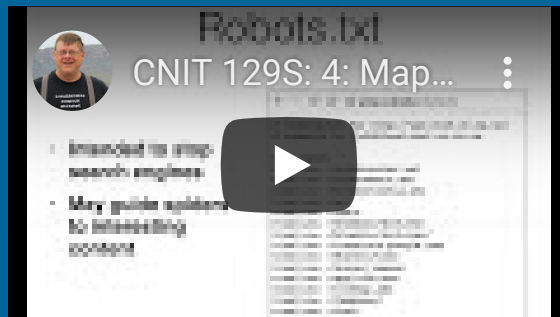
Quiz Ch 3 *
Proj 2 due



Ch 4: Mapping the Application

**Mon
2-11**

Quiz: Ch 4 *

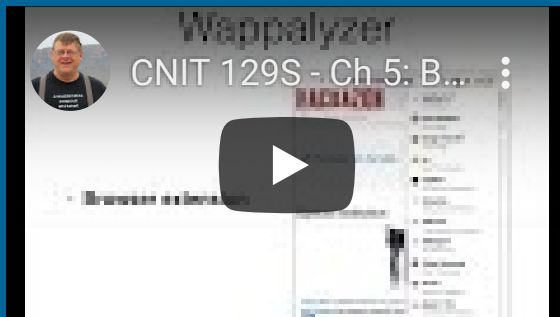


Mon 2-18 *Holiday - No Class*

Ch 5: Bypassing Client-Side Controls

Mon 2-25

Quiz Ch 5 *
Proj 3 & 5 &
6 due



Ch 6: Attacking Authentication

Mon 3-4

Quiz: Ch 6 *



Mon 3-11

Quiz: Ch 7 *
Proj 7 & 8

Ch 7: Attacking Session Management

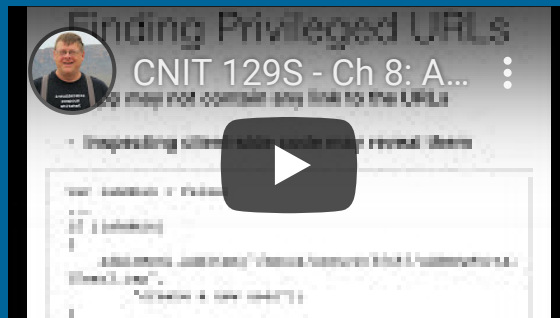
due



Ch 8: Attacking Access Controls
Ch 9: Attacking Data Stores (Part 1)

**Mon
3-18**

Quiz: Ch 8 *
Proj 9 & 10
due



**Mon
3-25**

Holiday - No Class

**Mon
4-1**

Quiz Ch 9 *
Proj 11 due

Ch 9: Attacking Data Stores



Ch 10: Attacking Back-End Components



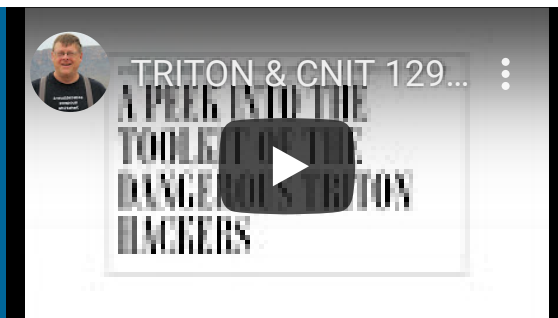
Mon
4-8

Quiz: Ch 10 *

Mon
4-15

Quiz: Ch 11 *
Proj 12 due

Ch 11: Attacking Application Logic



Ch 12: Attacking Users: Cross-Site Scripting

Mon
4-22

Quiz Ch 12 *
Proj 13 & 14
due

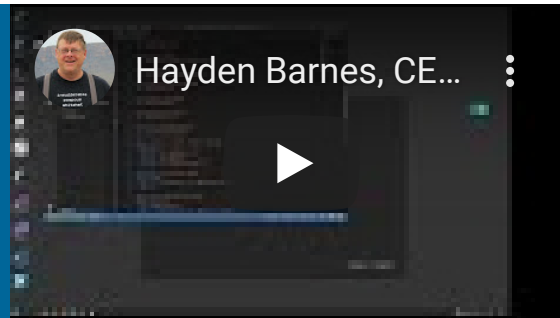


Mon
4-29

No Quiz
Proj 15 Due

Hayden Barnes
CEO, [Whitewater Foundry](#)

Presenting [Penguin](#)
Linux optimized for Windows



Ch 13: Attacking Users: Other Techniques (Part 1)

Mon
5-6

Quiz Ch 13 *
Proj 16 & 17
due

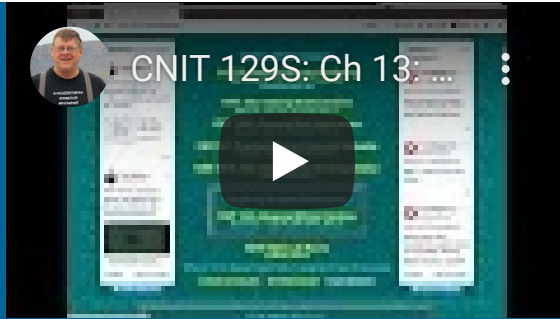


Mon
5-13

No Quiz
All Extra

Last Class
Ch 13: Attacking Users: Other Techniques (Part 2)

Credit Proj
Due



Wed
5-15 - Final Exam available online throughout the week.
Wed
5-22 You can only take it once.

* Quizzes due 30 min. before class; nothing considered late until after 2-4

Lectures

[Grading Policy](#) · [First Day Handout](#)

[Ch 1: Web Application \(In\)security &](#)

[Ch 2: Core Defense Mechanisms](#) · [KEY](#) · [PDF](#)

[Ch 3: Web Application Technologies](#) · [KEY](#) · [PDF](#)
[How to Burp \(PDF\)](#)

[Ch 4: Mapping the Application](#) · [KEY](#) · [PDF](#)

[Ch 5: Bypassing Client-Side Controls](#) · [KEY](#) · [PDF](#)

[Ch 6: Attacking Authentication](#) · [KEY](#) · [PDF](#)

[Ch 7: Attacking Session Management](#) · [KEY](#) · [PDF](#)

[Ch 8: Attacking Access Controls](#) · [KEY](#) · [PDF](#)

[Ch 9: Attacking Data Stores \(Part 1 of 2\)](#) · [KEY](#) · [PDF](#)

[Ch 9: Attacking Data Stores \(Part 2 of 2\)](#) · [KEY](#) · [PDF](#)
[Ch 10: Attacking Back-End Components](#) · [KEY](#) · [PDF](#)
[Ch 11: Attacking Application Logic](#) · [KEY](#) · [PDF](#)
[Ch 12: Attacking Users: Cross-Site Scripting \(Part 1 of 3\)](#) · [KEY](#) · [PDF](#)
[Ch 12: Attacking Users: Cross-Site Scripting \(Part 2 of 3\)](#) · [KEY](#) · [PDF](#)
[Ch 13: Attacking Users: Other Techniques \(Part 1 of 2\)](#) · [KEY](#) · [PDF](#)
[Ch 13: Attacking Users: Other Techniques \(Part 2 of 2\)](#) · [KEY](#) · [PDF](#)
[Ch 14: Automating Customized Attacks](#)
[Ch 15: Exploiting Information Disclosure](#)

To get PPT files, use [Cloud Convert](#).

Projects

[Project 1: Command Injection \(15 pts.\) \(Updated 1-24-18\)](#)
[Project 2: SQL Injection \(10 pts.\)](#)
[Project 3: Intro to Burp \(15 pts.\)](#)
[Project 4: Zed Attack Proxy \(20 pts.\)](#) (treated as extra credit; feel free to skip it)
[Project 5: Mapping an Application with Burp \(15 pts.\)](#)
[Project 6: Making a Linux Virtual Machine \(15 pts.\) \(rev. 2-14-18\)](#)
[Project 7: Using Tripwire for Intrusion Detection \(15 pts.\)](#)
[Project 8: Defeating Client-Side Validation with Burp \(15 pts.\)](#)
[Project 9: reCAPTCHA \(15 pts.\) \(rev. 2-21-18\)](#)
[Project 10: Exploiting ECB-Encrypted Tokens with Burp \(15 pts.\)](#)
[Project 11: SQL Injection 2 \(10 pts.\)](#)
[Project 12: PHP Insecurities \(10 pts.\)](#)
[Project 13: Automating Web Requests with Python \(15 pts. + 30 Extra Credit\)](#)
[Project 14: Logic Flaws \(15 pts. + 20 pts. Extra Credit\)](#)
[Project 15: XSS \(15 pts.\)](#)

[Project 16: SAML \(15 pts.\)](#)
[Project 17: MITM with Evilginx2 \(15 pts.\)](#)

More projects will be added

Extra Credit

[Binary Games \(Up to 25 pts.\) *](#)
[Project 1x: Command Injection Challenges \(25 pts.\) \(Updated 1-17-18\)](#)
[Project 2x: SQL Injection Challenges \(20 pts.\) \(updated 2-7-18\)](#)

[Project 3x: DNSCrypt on Windows \(NEW VERSION\) \(15 pts.\)](#)

[Project 3x: DNSCrypt on Windows OLD VERSION, MORE ANNOYING](#)

[Project 4x: Encrypting Text in ECB and CBC Modes \(15 pts.\)](#)
[Project 5x: Exploiting ECB Encryption \(35 pts.\)](#)
[Project 6x: Protecting SSH with Fail2Ban \(15 pts.\)](#)
[Project 7x: Protecting a Server with iptables and iptstate \(10 pts.\) \(Updated 11-8-16\)](#)
[Project 8x: Exploit Hackazon \(20 pts.\)](#)
[Project 9x: XSS Extra Credit \(25 pts.\) \(Rev. 4-2-18\)](#)
[Proj 11x: Stealing Cookies with XSS \(10 pts.\) \(New 4-23-18\)](#)

* Scores automatically entered in Canvas

Links

Links for Chapter Lectures

[Ch 1a: Highly Secure Dogfood](#)

[Ch 1b: Online Voting - Follow My Vote - 100% Secure](#)

[Ch 1c: Android Apps Vulnerable to Code Modification](#)

[Ch 1d: Security Problems at Colleges](#)

[Ch 1e: CMS Vulnerabilities are Decreasing](#)

[Ch 1f: Attention SinVR users | Continuous Cyber Security | UK | Digital Interruption \(Jan 17, 2018\)](#)

[Ch 2a: SOAP Examples](#)

[Ch 3a: RESTful Resource Naming](#)

[Ch 3b: SOAP Examples](#)

[Ch 3c: HTML form enctype Attribute](#)

[Ch 3d: Microsoft Edge Browser won't support ActiveX, VBScript, other Internet Explorer features](#)

[Ch 3e: VBScript is no longer supported in IE11 edge mode \(Windows\)](#)

[Ch 3f: JavaScript HTML DOM](#)

[Ch 3g: DOM example](#)

[Ch 3h: Map; example of Ajax](#)

[Ch 3i: Simple Google Maps API Example - Jayway](#)

[Ch 3k: XMLHttpRequest - Wikipedia](#)

[Ch 3l: HTTP Status Dogs](#)

[Ch 4a: Using Burp Spider](#)

[Ch 4b: How To Burp -- Slides from David Brown](#)

[Ch 4c: Web Common Directories and Filenames - Word Lists Collection](#)

[Ch 4d: GitHub - spinkham/skipfish: Web application security scanner created by lcamtuf for google - Unofficial Mirror](#)

[Ch 4e: Skipfish project instructions](#)

[Ch 4f: OWASP DirBuster Project](#)

[Ch 4g: GitHub - sensepost/wikto](#)

[Ch 4h: httprecon project - advanced http fingerprinting](#)

[Ch 4i: Electronic & Transactional Content Management | OpenText, Vignette](#)

[Ch 4j: httpprint download \(from 2005\)](#)

[Ch 4k: Web Application Fingerprint \(OWASP-IG-004\)](#)

[Ch 4l: How to use Httpprint on Kali Linux](#)

[Ch 4m: Using HTTP Methods \(GET, POST, PUT, etc.\) in Web API](#)

[Ch 4n: OWASP DirBuster -- Replaced by Zed Attack Proxy](#)

[Ch 4o: OWASP Zed Attack Proxy](#)

[Ch 5a: HTTP ETag - Wikipedia](#)

[Ch 5b: JavaScript Form Validation](#)

[Ch 5c: Serialization - Wikipedia](#)

[Ch 5d: JAVA De-serialization: It can't get any simpler than this !!](#)

[Ch 5e: WCF Binary Soap Plug-In for Burp \(for Silverlight\)](#)

[Ch 5f: JAD Java Decompiler Download Mirror](#)

[Ch 5g: Flasm Flash decompiler](#)

[Ch 5h: Flare Flash decompiler](#)

[Ch 5i: WebInspect: Dynamic Analysis, DAST, Penetration Testing Tools | Hewlett Packard Enterprise](#)

[Ch 5j: .NET Decompiler: Decompile Any .NET Code | .NET Reflector](#)

[Ch 5k: Code refactoring - Wikipedia](#)

[Ch 5l: Java Optimize and Decompile Environment \(JODE\)](#)

[Ch 5m: JavaSnoop Download](#)

[Ch 5n: Hacking Java Applications using JavaSnoop - InfoSec Resources](#)

[Ch 6a: Microsoft Passport and Windows Hello](#)

[Ch 6b: Obama's Internet Plan Sounds an Awful Lot Like a National Internet ID \(from 2011\)](#)

[Ch 6c: How Weev's prosecutors are making up the rules \(2013\)](#)

[Ch 6d: Errata Security: AT&T provides free user information yet again](#)

[Ch 6e: Secret Microsoft policy limited Hotmail passwords to 16 characters \(2012\)](#)

[Ch 6f: Basic access authentication - Wikipedia](#)

[Ch 6g: Digest access authentication - Wikipedia](#)

[Ch 7a: ASP.NET View State Overview](#)

[Ch 7b: Samy Kamkar - phpwn: Attack on PHP Sessions and Random Numbers](#)

[Ch 7c: How to fix a website with blocked mixed content](#)

[Ch 7d: HttpOnly - OWASP](#)

[Ch 7e: PHP: setcookie - Manual](#)

[Ch 7f: \[WEB SECURITY\] Technical Note by Amit Klein: "Path Insecurity"](#)

[Ch 7g: HTTP Strict Transport Security Cheat Sheet - OWASP](#)

[Ch 7h: Usage Statistics of HTTP Strict Transport Security for Websites](#)

[Ch 7i: Bypassing HSTS or HPKP in Chrome is a badidea](#)

[Ch 7l: X-XSS-Protection - HTTP | MDN](#)

[Ch 7j: Hack Yourself First: FREE COURSE -- HIGHLY RECOMMENDED](#)

[Ch 7k: I figured out a way to hack any of Facebook's 2 billion accounts, and they paid me a \\$15,000 bounty](#)

[Ch 8a: IBM Knowledge Center - HTTP session manager troubleshooting tips](#)

[Ch 8b: Vulnerable USA Colleges](#)

[Ch 9a: escaping - How to escape apostrophe \('\) in MySQL?](#)

[Ch 9b: javascript - Which Logic Operator Takes Precedence](#)

[Ch 10a: Microsoft retires Filemon and Regmon from Sysinternals](#)

[Ch 12w: Memory Forensics: Mandiant Redline](#)

[Ch 12x: Forensic Investigation with Redline](#)

[Ch 12a: apache.org incident report for 04/09/2010](#)

[Ch 12b: MySpace Worm Explanation](#)

[Ch 12c: StrongWebmail CEO's mail account hacked via XSS](#)

[Ch 12d: Two XSS Worms Slam Twitter](#)

[Ch 12e: Null Byte Injection in PHP](#)

[Ch 12f: Window atob\(\) Method](#)

[Ch 12g: Saying goodbye to ActiveX, VBScript, attachEvent-- | Microsoft Edge Dev Blog](#)

[Ch 12h: Javascript Packer](#)

[Ch 12i: Why were Javascript `atob\(\)` and `btoa\(\)` named like that? - Stack Overflow](#)

[Ch 13a: About IFRAME and clickjacking](#)

[Ch 13b: AJAX Introduction](#)

[Ch 13C: XMLHttpRequest Demo](#)

[Ch 13d: HTTP Response Splitting - OWASP](#)

[Ch 13e: Report: Microsoft Edge leaks private browsing data locally](#)

[Ch 13f: Privacy and the :visited selector](#)

[Ch 13g: The power of DNS rebinding: stealing WiFi passwords with a website](#)

[Ch 13h: GitHub - taviso/rbndr: Simple DNS Rebinding Service](#)

[Ch 13i: rbndr.us dns rebinding service](#)

[Ch 13j: Dear developers, beware of DNS Rebinding](#)

Miscellaneous Links

[Xtreme Vulnerable Web Application \(XVWA\) -- GOOD FOR PROJECTS](#)
[SQL Injection Videos - YouTube](#)
[DVWA - Damn Vulnerable Web Application](#)
[XVWA Reddit explaining why it exists](#)
[rapid7/hackazon · GitHub](#)
[OWASP Broken Web Applications Project](#)
[hackazon Installation Guide.pdf](#)
[OWASP Vulnerable Web Applications Directory Project](#)
[Hackazon -- Public hosted server!](#)
[Hackazon: Stop hacking like its 1999 - Dan Kuykendall - OWASP AppSec California 2015 - YouTube](#)
[Hackazon Test Site Review - CyberSecology](#)
[Wikto](#)
[XVWA - Xtreme Vulnerable Web Application -- SERVER TO HACK](#)
[Hackazon -- SERVER TO HACK](#)
[HTML "text-indent: -9999px" and holding the line](#)
[Incident Response for an SEO Spammed Website](#)
[Website Security: How Do Websites Get Hacked?](#)
[7 Security Measures to Protect Your Servers | DigitalOcean](#)
[Stop Forum Spam -- Useful for WordPress Sites](#)
[WS-Attacker · SOAP and XML attacks for web app pentesting -- USEFUL FOR PROJECTS](#)
[securityheaders.io -- USEFUL INFO](#)
[Security Archive - Case Study: phpbb.com Compromised \(from 2009\)](#)
[phpBB.com Hacked in Dec. 2014](#)
[dsnextgen.com iframe hack](#)
[Sfisaca.org ISACA San Francisco -- Domain is 46 years old?](#)
[Google Flagged My Site as Malware](#)
[Best Open Source Web Application Vulnerability Scanners - InfoSec Resources](#)
[WPScan -- Vuln Scanner for Wordpress Sites](#)
[How To: Use Thug Honeyclient to Investigate a Malicious Website](#)
[Thug - Python low-interaction honeyclient](#)
[Welcome to Thug's documentation!](#)
[Removing a PHP Redirector](#)
[Security Engineering - VERY USEFUL VULNERABILITY FIXES](#)
[LifeSize Room Exploits: \"skiplogin\" parameter FTW](#)
[OWASP VBScan is a Black Box vBulletin Vulnerability Scanner](#)
[GitHub's CSP journey](#)
[Victor Santoyo: How To Know If You've Been Hacked | WordPress.tv](#)

[wordpress-exploit-framework](#)
[Vulnerable Web Application - bWAPP](#)
[Weaponized WordPress](#)
[How Google helps 600,000 webmasters re-secure their hacked sites every year](#)
[Online CSRF PoC Generator: A web alternative to the Burp Suite Pro and ZAP CSRF PoC generators](#)
[urlquery.net - Free URL scanner](#)
[CMSmap automates the process of detecting security flaws of the most popular CMSs](#)
[In Q1/2016 the most hacked platforms were #WordPress, #Joomla and #Magento. Get our full report here](#)
[SQLmap POST request injection](#)
[Joomla : Products and vulnerabilities -- 178 RCE vulns!](#)
[Wordpress : Products and vulnerabilities -- 53 RCE Vulns](#)
[Top 10 content management systems](#)
[CMS Vulnerabilities -- Security is Improving in Recent Years](#)
[Joomla 1.5 \(3.4.5 - Object Injection RCE X-Forwarded-For Header \(CVE-2015-8562\) -- USE FOR PROJECT](#)
[UNIX / Linux Tutorial for Beginners](#)
[RingZer0 CTF -- GOOD FOR PRACTICE](#)
[Javascript without letters or numbers](#)
[JavaScript written only with brackets?](#)
[Tripwire Open Source vs. OSSEC : Which Is Right For You?](#)
[Downloads -- OSSEC](#)
[Intricately -- fingerprints sites](#)
[A Beginner's Guide to HTTP/2 and its Importance](#)
[Practical Website Hacking CTF](#)
[Practical Web Hacking CTF by InfoSecInstitute Write-up -- Ibrahim M. El-Sayed \(the_storm\)](#)
[Hack I-Bank Pro -- Burp defeating authentication](#)
[Google CTF -- Web Write-Ups \(11/15\) | Brett Buerhaus](#)
[Web Application Pen-testing Tutorials With Mutillidae \(Hacking Illustrated Series InfoSec Tutorial Videos\)](#)
[PHP Security: SUHOSIN](#)
[Over 78% of All PHP Installs Are Insecure \(from 2014\)](#)
[How to write insecure code - OWASP](#)
[PHP Tips, Resources and Best Practices for 2015](#)
[10 Most Common Mistakes That PHP Developers Make](#)
[7 More Mistakes Commonly Made by PHP Developers](#)
[18 Critical Oversights in Web Development](#)
[BApp Store: Burp Plugins](#)
[PHP-CGI Exploitation by Example](#)
[Remote code execution via PHP \[Unserialize\]](#)

[PHP Object Injection - OWASP](#)
[GitHub Pull Request Tutorial](#)
[Wiley: Evaluation Copies and Desk Copies](#)
[Secret, forbidden, black-hat technique of obtaining the textbook \(DO NOT CLICK THIS LINK\)](#)
[My Python Mirai Honeypot Script](#)
[WAHH Methodology desktop background for Web Application hackers](#)
[How to Prevent Windows 10 From Automatically Downloading Updates](#)
[Rails SQL Injection Examples](#)
[Common Rails Security Pitfalls and Their Solutions](#)
[UXSS on Microsoft Edge -- Adventures in a Domainless World](#)
[Netgear starts patching routers affected by a critical flaw](#)
[US-CERT: Stop using your remotely exploitable Netgear routers](#)
[Attacking WordPress](#)
[SQL Injection in Rails: Live Demonstrations](#)
[How To Scan And Check A WordPress Website Security Using WPScan, Nmap, And Nikto | Unixmen](#)
[Penetration Testing Your WordPress Site - WordPress Security](#)
[Complete Set Of CGI-BIN Exploits and what they do Article | Hellbound Hackers](#)
[INFOSEC INSTITUTE CTF - capture the flag hacking exercises](#)
[Hacker101 -- Free Web App Security Class -- GOOD FOR PROJECTS](#)
[Using the Requests Library in Python](#)
[Amazon Cookie Re-Use](#)
[Convert cURL command syntax to Python requests](#)
[Reverse Engineering APIs: Coffee Meets Bagel -- Nik Patel -- Medium](#)
[Attacking SSO: Common SAML Vulnerabilities and Ways to Find Them](#)
[Bypassing SAML 2.0 SSO with XML Signature Attacks](#)
[JavaSerialKiller: Burp extension to perform Java Deserialization Attacks](#)
[Java Deserialization Attacks with Burp](#)
[Marshalling Pickles by frohoff](#)
[Marshalling Pickles - Chris Frohoff & Gabriel Lawrence - OWASP AppSec California 2015 - YouTube](#)
[On Breaking SAML: Be Whoever You Want to Be](#)
[Using XMLDecoder to execute server-side Java Code on an Restlet application \(i.e. Remote Command Execution\)](#)
[Serialization Must Die: Act 2: XStream \(Jenkins CVE-2016-0792\)](#)

New Unsorted Links

[The New zANTI: Mobile Penetration & Security Analysis Toolkit -- USE FOR PROJECTS](#)
[Burp Hacks for Bounty Hunters - YouTube](#)
[Web Application Firewalls Reviews](#)
[Ch 3m: Client-side validation](#)
[Better API Penetration Testing with Postman](#)
[Using OWASP ZAP GUI to scan your Applications for security](#)

Last updated: 5-13-19 8:20 pm