



Virginia Information Technologies Agency

# Web Application Vulnerability Scanning

**VITA**  
Commonwealth Security  
& Risk Management

**April 8, 2016**



## Terms

- Threat – A *thing* that can cause harm
- Vulnerability – A flaw that can be exploited to cause bad things
- Exploit – An instance where software or actions take advantage of a vulnerability
- Risk – When a threat and vulnerability have a crossover



## Why do we scan #1?

- We are attempting to identify web application vulnerabilities.
- So we can remediate them and block threats to reduce the risk!



## Who should conduct the scans?

- Someone with knowledge of tools, vulnerabilities, exploits and the rules of engagement.
- We don't have to be developers.
  - We find vulnerabilities and exploit them.
- ***An authorized person!***



## Why is authorization so important?

- Because it's a crime to test without it.
- US Law
  - Title 18 § 1029 + 18 § 1030 and 18 § 1362
    - ...intentionally accesses a computer without authorization or exceeds authorized access...
    - ...20 years & 1 million dollars



# In the Code of Virginia too

law.lis.virginia.gov/vacode/18.2-152.2/

VIRGINIA GENERAL ASSEMBLY / LIS HOME / SIGN IN

Code of Virginia Search

- Code of Virginia
  - Popular Names
  - 2015 Updates
  - SECTION LOOK UP
  - Administrative Code
  - Constitution of Virginia

Code of Virginia  
 Table of Contents » Title 18.2. Crimes and Offenses Generally » Chapter 5. Crimes Against Property » § 18.2-152.2. Definitions; computer crimes

← Section →

§ 18.2-152.2. Definitions; computer crimes.

For purposes of this article:

"Commercial electronic mail" means electronic mail, the primary purpose of which is the advertisement or promotion of a commercial product or service.

A person is "without authority" when he knows or reasonably should know that he has no right, agreement, or permission or acts in a manner knowingly exceeding such right, agreement, or permission.



## Main Take Away

- Practice before you test apps or scan
- Get permission
  - A phone “OK” is not “OK”
  - E-mail approval is questionable
  - Get it in writing, signed by someone with authority.
- Have penetration testing in your EWP – your job description.



## What kind of other scans do we do?

- **OS/Network Vulnerability Scanning**
- Tenable Nesses, Rapid 7 Nexpose, Qualys Guard Vulnerability Management tools produce this information and reports.
  - Service Center - Nesses
  - Full Service partnership agencies do not require additional reporting as this is done internally.
  - Agencies not under the partnership full service infrastructure, please submit evidence of periodic OS/Network scanning to the CISO.

## Penetration testing?

- The terms Penetration Testing and Web Application Scanning are frequently interchanged, but they are different.
  - Penetration testing includes reconnaissance, discovery, enumeration and exploiting. Even client attacks if they are in scope. Sometimes they are total black box.
  - Involves scanning, both OS/Network and Web Application scans.
  - Web App Scans can be used as Web App Pen Tests if we take it one more step further.



# Web application vulnerability scanning

- **Web Application Vulnerability Scanning**
  - Web Application Scanner tools like Acunetix, Burp Suite Pro, Qualys Web Application Security and OWASP ZAP produce these reports. Many Others!
  - Conducted with and without authentication. We know the targets and work with the client to ensure full coverage.
  - Coordinated, with a well defined scope
  - URL Based Scans
  - We can scan public or internal facing



## Web app scans continued

- White or crystal box scanning
- Some crossover with OS/Network Scans & Pen Tests
- It's not a challenge to see if we can break authentication , although we test that.
- Not intelligent, but can do thousands of tests in the time a person can do one.
- Our Primary scanner tests for over 600 flaws and is constantly improving
- Requires a human
- Scans take less than an hour to several days



## What are we required to scan?

- 501-09 Requires this of both public facing AND sensitive. ALL public facing and ALL sensitive, that permit browser interaction, should have these scans.
  - Agencies receiving the web application scanning service from VITA need only to send a notice to the CISO that all public facing sensitive systems have been scanned.
- Every 90 Days



## Do we have to web app scan hosted apps?

- It's primarily about the location and the data.
- If it's public facing, then yes.
- If it hosts sensitive data then yes, if it is a browser accessed application or web service.
- This must be well understood and spelled out carefully in our vendor contacts.
  - Some misunderstanding on this recently



## What about a sensitive non browser app?

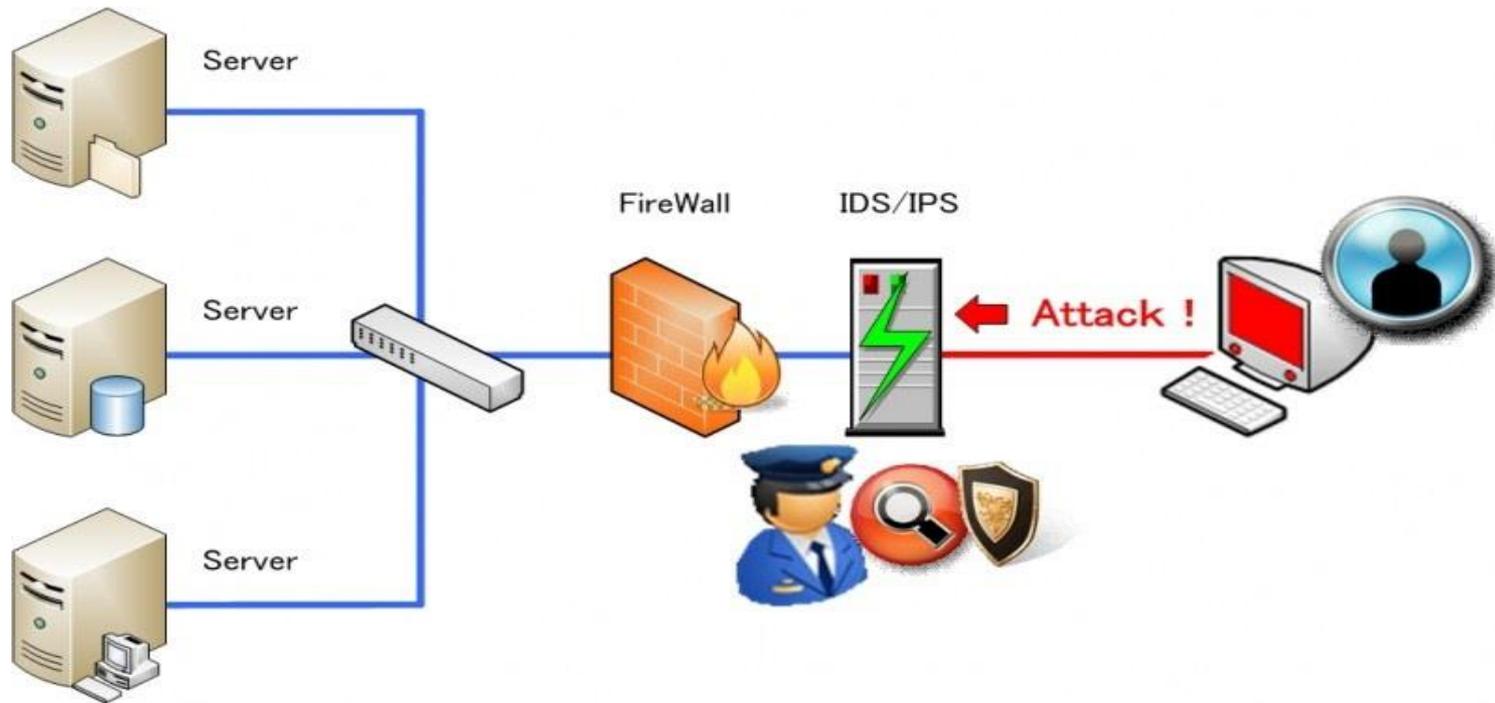
- Client Server
- Proprietary Client
- Emulation
  - In this case we rely on CSRM, vendor and community advisories.
  - And our OS/Network vulnerability scans we can review in the Security Center –Nesses.
  - Stay current on our patching!



## Why do we scan #2?

- Security and Compliance
  - The initial scans and working through the vulnerabilities will be for security first
  - After remediation, the scans will be for compliance first...hopefully.

# Are the IDS/ IPS functions scanning?

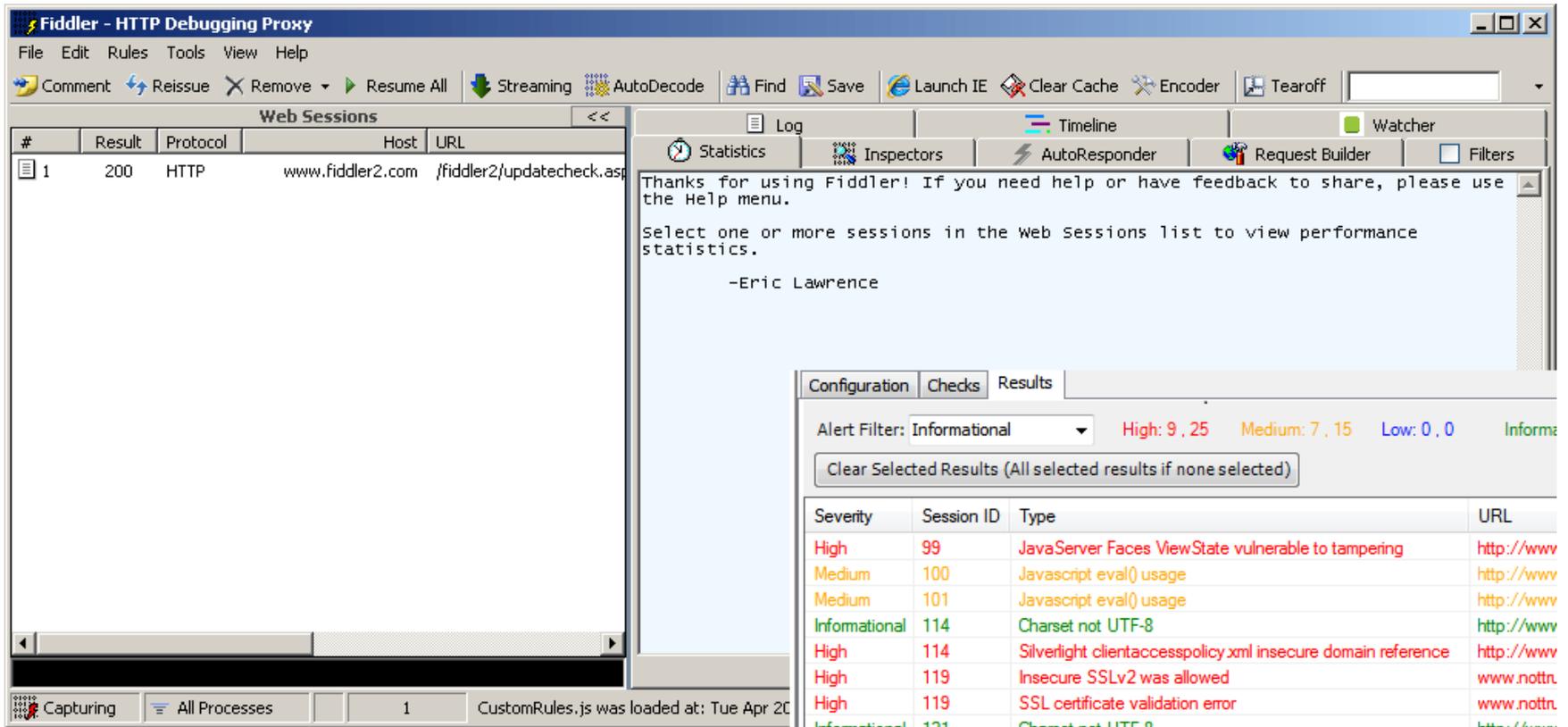


Yes, a form, scanning the traffic. This activity frequently initiates Web App Scans too!

## Examples of common tools

- Fiddler
  - With Watcher
- Burp Suite Pro
- Acunetix
- A weaponized browser
  - In the right hands

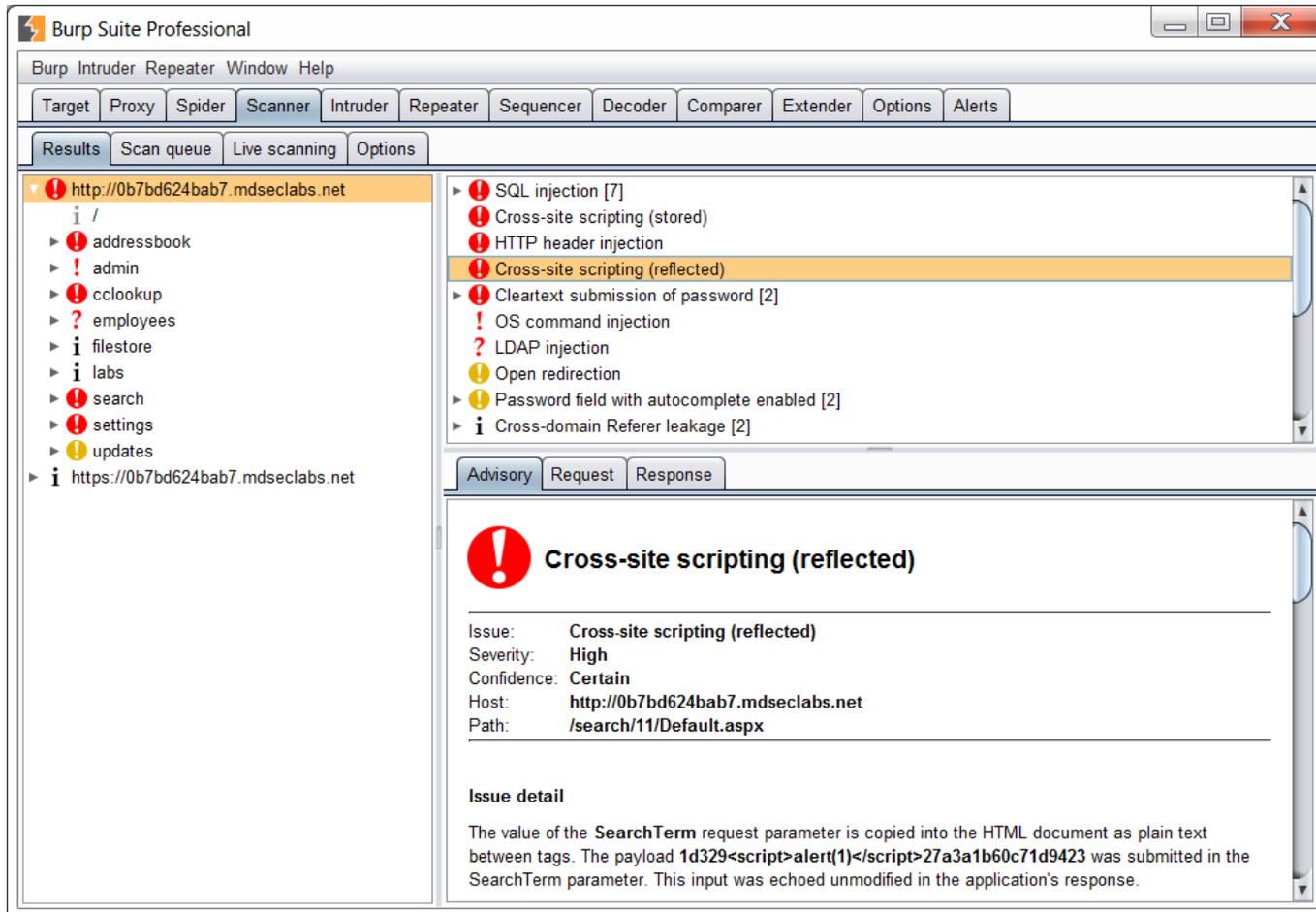
# Fiddler with Watcher



The screenshot shows the Fiddler - HTTP Debugging Proxy interface. The 'Web Sessions' pane on the left shows a single session with a 200 status code over HTTP to www.fiddler2.com. The main pane displays a welcome message from Eric Lawrence. The 'Results' pane at the bottom right shows a table of security alerts.

Severity	Session ID	Type	URL
High	99	JavaServer Faces ViewState vulnerable to tampering	http://www
Medium	100	Javascript eval() usage	http://www
Medium	101	Javascript eval() usage	http://www
Informational	114	Charset not UTF-8	http://www
High	114	Silverlight clientaccesspolicy.xml insecure domain reference	http://www
High	119	Insecure SSLv2 was allowed	www.notrn
High	119	SSL certificate validation error	www.notrn
Informational	121	Charset not UTF-8	http://www

# Burp Suite Pro



The screenshot displays the Burp Suite Professional interface. The main window shows a list of scan results for the target `http://0b7bd624bab7.mdseclabs.net`. The results include:

- SQL injection [7]
- Cross-site scripting (stored)
- HTTP header injection
- Cross-site scripting (reflected)** (highlighted)
- Cleartext submission of password [2]
- OS command injection
- LDAP injection
- Open redirection
- Password field with autocomplete enabled [2]
- Cross-domain Referer leakage [2]

The detailed view for the selected issue, **Cross-site scripting (reflected)**, is shown below:

**Issue:** Cross-site scripting (reflected)  
**Severity:** High  
**Confidence:** Certain  
**Host:** http://0b7bd624bab7.mdseclabs.net  
**Path:** /search/11/Default.aspx

**Issue detail**

The value of the **SearchTerm** request parameter is copied into the HTML document as plain text between tags. The payload `1d329<script>alert(1)</script>27a3a1b60c71d9423` was submitted in the SearchTerm parameter. This input was echoed unmodified in the application's response.

# Acunetix

The screenshot displays the Acunetix Web Vulnerability Scanner (Consultant Edition) interface. The main window shows a list of scan results for a target URL: `http://testphp.vulnweb.com:80/`. The scan is finished, and 122 alerts were generated. A detailed view of an SQL Injection vulnerability is shown on the right.

**SQL Injection (verified)** HIGH

**Vulnerability description**

This script is possibly vulnerable to SQL Injection attacks.

SQL injection is a vulnerability that allows an attacker to alter backend SQL statements by manipulating the user input. An SQL injection occurs when web applications accept user input that is directly placed into a SQL statement and doesn't properly filter out dangerous characters.

This is one of the most common application layer attacks currently being used on the Internet. Despite the fact that it is relatively easy to protect against, there is a large number of web applications vulnerable.

This vulnerability affects `/listproducts.php`.

Discovered by: Scripting (Sql\_injection.script).

**Attack details**

URL encoded GET input `artist` was set to `{select 1 and row(1,1)=(select count(*) concat(concat(CHAR(52),CHAR(67),CHAR(117),CHAR(98),CHAR(52),CHAR(117),CHAR(78),CHAR(77),CHAR(72),CHAR(79),CHAR(55)),floor(rand()*2))x) from (select 1 union select 2)a group by x limit 1)}`

Injected pattern found:

```
4Cub4u0907
```

View HTTP headers  
 View HTML response  
 Launch the attack with HTTP Editor  
 Retest alert(s)  
 Mark this alert as a false positive

**The impact of this vulnerability**

An attacker may execute arbitrary SQL statements on the vulnerable system. This may compromise the integrity of your database and/or expose sensitive information.

Depending on the back-end database in use, SQL injection vulnerabilities lead to varying levels of data/system access for the attacker. It may be possible to not only manipulate existing queries, but to UNION in arbitrary data, use subselects, or append additional queries. In some cases, it may be possible to read in or write out to files, or to execute shell commands on the underlying operating system.

Certain SQL Servers such as Microsoft SQL Server contain stored and extended procedures (database server functions). If an attacker can obtain access to these procedures it may be possible to compromise the entire machine.

**How to fix this vulnerability**

Your script should filter metacharacters from user input.  
 Check detailed information for more information about fixing this vulnerability.

**Detailed information**

Click here for more detailed information about this vulnerability

**Web references**

- Acunetix SQL Injection Attack
- Advanced SQL Injection
- Security Focus - Penetration Testing for Web Applications (Part Two)
- More Advanced SQL Injection

**Activity Window**

```
04.04.16:40:30, CSRF testing finished.
04.04.16:40:33, Finished scanning.
04.04.16:40:33, Saving scan results to database ...
04.04.16:40:39, Done saving to database.
04.04.16:40:39, Flush file buffers.
```

# Browsers - Firefox



- **HackBar** - Simple security audit / Penetration test tool.
- **Tamper Data** - View and modify HTTP/HTTPS headers and post parameters
- **XSS Me** - Test for reflected Cross-Site Scripting (XSS)
- **Firebug** - Edit, debug, and monitor CSS, HTML, and JavaScript

# Browsers - Chrome



- HTTP Headers
- HTTP Spy
- Live HTTP Headers
  - Each of these display the header in some way.
- Others available
  - Many don't seem to work very well

## We will be the goat!



- Scanning is not the hard part
- We have to understand and defend your findings.
- We have to work with people to help them understand the vulnerability impact and how to resolve vulnerabilities.

## How to be less of a goat

- Understand that the first time you present a report, with a lot of findings, it might be shocking.
- We make more work for people.
- The first line of defense is often denial, then attack, then bewilderment, then hopefully some understanding and success.
- Be gentle and patient and have a thick skin.



## Scan issues and preparation

- Why scans crash sites sometimes
  - Email Flooding
  - SQL and XSS Injections
  - Excessive logging
  - Undersized Resources
  - Configuration Errors
  - DB entries
  - Dangerous Actions executed
  
  - A Backup is a good idea. Be a small goat.



## How to learn more about this

- Books
- Classes
- Web Sites
- Vulnerable Web Builds
- Practice

# Books

Books > Computers & Technology > Networking & Cloud Computing

The Web Application Hacker's Handbook and over one million other books are available for Amazon Kindle. [Learn more](#)

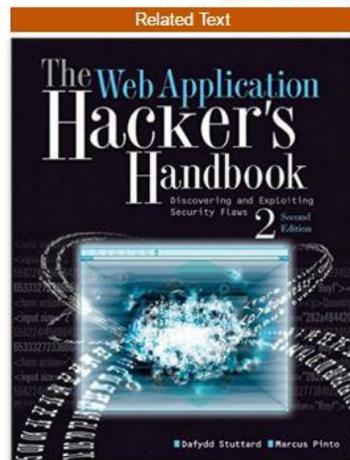
*i* You purchased this item on November 15, 2012.  
[View this order](#)

## The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws 2nd Edition

by Dafydd Stuttard (Author), Marcus Pinto (Author)

★★★★★ 52 customer reviews

[Look inside](#) ↓



ISBN-13: 978-1118026472

ISBN-10: 1118026470

[Why is ISBN important?](#)

Kindle	<b>Paperback</b>	Other Sellers
\$26.39	<b>\$17.49 - \$33.31</b>	from \$23.98
<input type="radio"/> Rent <span style="float: right;">✓Prime \$17.49</span>		
<input type="radio"/> Buy used <span style="float: right;">✓Prime \$29.72</span>		
<input checked="" type="radio"/> <b>Buy new</b> <span style="float: right;">✓Prime <b>\$33.31</b></span>		
<p><b>In Stock.</b>                  Ships from and sold by Amazon.com. Gift-wrap available.</p> <p>✓Prime</p> <p>Want it tomorrow, April 8? Order within <b>3 hrs 38 mins</b> and choose <b>One-Day Shipping</b> at checkout.  <a href="#">Details</a></p>		<p>List Price: <del>\$50.00</del> Save: \$16.69 (33%)                  65 New from \$25.91</p> <p>Qty: 1 ↓</p> <p> <b>Add to Cart</b></p> <p>Turn on 1-Click ordering</p> <p><b>Ship to:</b>                  william p. freda- Midlothian ↓</p>
<p><b>More Buying Choices</b></p>		<p>102 used &amp; new from \$23.98</p>

# More books

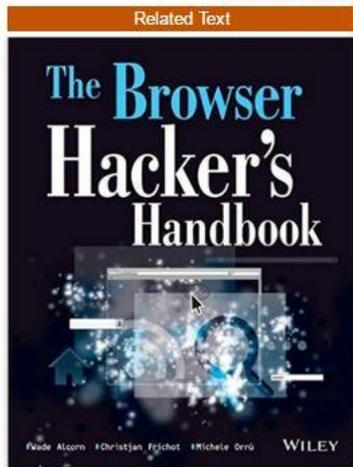
*i* You purchased this item on October 22, 2015.  
View this order

## The Browser Hacker's Handbook 1st Edition

by Wade Alcorn (Author), Christian Fritchot (Author), Michele Orru (Author)

★★★★☆ 13 customer reviews

Look inside ↴



ISBN-13: 978-1118662090  
ISBN-10: 1118662091

Kindle	Paperback	Other Sellers
\$30.99	\$19.52 - \$48.80	from \$24.73
<input type="radio"/> Rent <span style="float: right;">Prime \$19.52</span>		
<input type="radio"/> Buy used <span style="float: right;">\$28.90</span>		
<input checked="" type="radio"/> <b>Buy new</b> <span style="float: right;">Prime \$48.80</span>		
<p><b>In Stock.</b> Ships from and sold by Amazon.com. Gift-wrap available.</p> <p>Prime   FREE One-Day</p> <p>List Price: <del>\$55.00</del> Save: \$6.20 (11%) 30 New from \$24.73</p> <p>Qty: 1</p> <p>Want it tomorrow, April 8? Order within 5 hrs 7 mins and choose One-Day Shipping at checkout. <a href="#">Details</a></p> <p> Add to Cart</p> <p>Turn on 1-Click ordering</p> <p>Ship to: william p. freda- Midlothian</p>		

## Classes

Web Application Penetrat x

← → G https://www.sans.org/course/web-app-penetration-testing-ethical-hacking

**Take Cyber Insurance Survey for Chance to Win a \$400 Amazon Gift Card!**

**SANS**

Find Training | Live Training | Online Training | Programs | Resources | Vendor | About

### SEC542: Web App Penetration Testing and Ethical Hacking

<a href="#">Contents</a>   <a href="#">Additional Info</a> <b>Delivery Methods:</b> <a href="#">Live</a>   <a href="#">Online</a>	<a href="#">GWAPT Certification</a> <a href="#">Affiliate Pricing</a> 36 CPEs <a href="#">Laptop Required</a>	<a href="#">Masters Program</a> <a href="#">Cyber Guardian</a>
---	--	---

SEC542 provides rapid exposure to a variety of tools and techniques invaluable to recon on target site.  
 — Gareth Grindie, QA Ltd.

The SEC542 tools and course presentation are top-notch. I will be using this material extensively.  
 — Jeremy Pierson, Academy Mortgage

Web applications play a vital role in every modern organization. But, if your organization does not properly test and secure its web apps, adversaries can compromise these applications, damage business functionality, and steal data. Unfortunately, many organizations operate under the mistaken impression that a web application security scanner will reliably discover flaws in their systems.

**SEC542 helps students move beyond push-button scanning to professional, thorough, high-value web application penetration testing.**

Customers expect web applications to provide significant functionality and data access. Even beyond the importance of customer-facing web applications, internal web applications increasingly represent the most commonly used business tools within any organization. Unfortunately, there is no "patch Tuesday" for custom web applications, so major industry studies find that web application flaws play a major role in significant breaches and intrusions. Adversaries increasingly focus on these high-value targets either by directly abusing public-facing applications or by focusing on web apps as targets after an initial break-in.

Modern cyber defense requires a realistic and thorough understanding of web application security issues. Anyone can learn to sling a few web hacks, but effective web application penetration testing requires something deeper.

**SEC542 enables students to assess a web application's security posture and convincingly demonstrate the impact of inadequate security that plagues most organizations.**



Get Registered

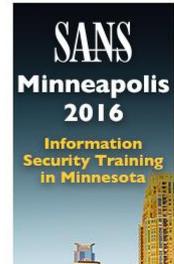
Free Excerpt

Course List

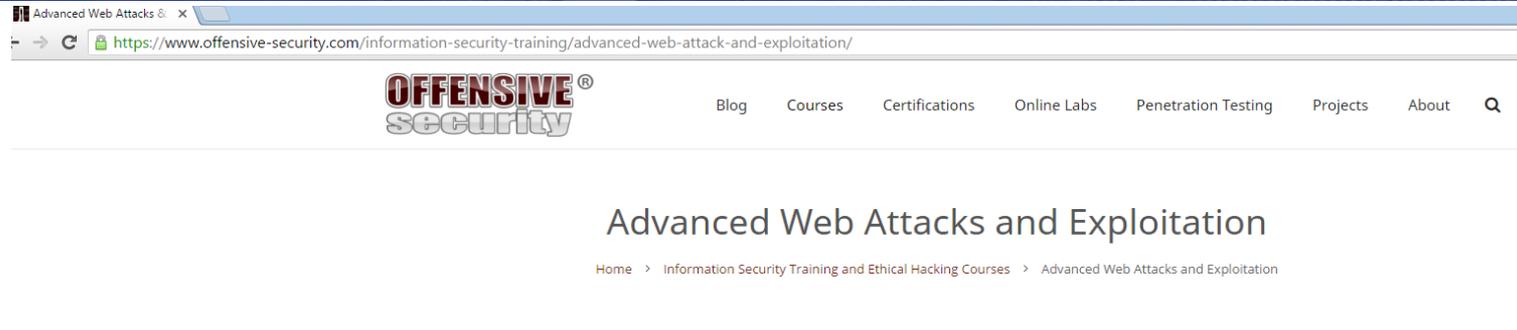
Curricula

Downloads  
 • Course Brochure

Share



## The I wish class



### Web Penetration Testing Live Course

Offensive Security's **Advanced Web Attacks and Exploitation (AWAE)** ethical hacking course was created by taking widely deployed web applications found in many enterprises and actively exploiting them. Web service testing is just one facet to our penetration testing methodology, which will put you at the forefront of **advanced web attacks** today. Finding vulnerabilities in perimeter defenses, web server application attacks, and bypassing internet security to traverse from the web into private networks are just a few examples of exploitation techniques you will learn in this course.

The days of porous network perimeters are fading fast as web services become more resilient and harder to exploit. In order to penetrate today's modern networks, a new approach is required to gain that initial critical foothold into a network. Penetration testers must be fluent in the art of exploitation when using web based attacks. From mind-bending XSS attacks, to exploiting race conditions, this intensive hands-on course will take your skills beyond run-of-the-mill SQL injection and file inclusion attacks while propelling you into a world of brain-melting SQL queries, **advanced web attacks** and more!

This web application security training will broaden your knowledge of the web services architecture in order to help you identify and circumvent various protection mechanisms in use on the web today. Don't be left behind! Go beyond the basics and dive deep into the realm of **advanced web application penetration testing**.



*"..119 applications over the next 365 days means a new web application is deployed on an enterprise web property every 3 days."* – Veracode



# Web Site - OWASP

The screenshot shows the OWASP website homepage. The browser address bar displays [https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page). The page features a navigation menu on the left, a search bar at the top right, and a main content area with a welcome message and various resource links.

**Welcome to OWASP**  
the free and open software security community

- Dependency Check
- ZAP Proxy
- Cheat Sheets
- Top 10
- OWTF
- ASVS
- SMM
- Development Guide
- AppSensor
- Testing Guide
- ModSecurity Ruleset
- More...

Home  
About OWASP  
Acknowledgements  
Advertising  
AppSec Events  
Books  
Brand Resources  
Chapters  
Donate to OWASP  
Downloads  
Funding  
Governance  
Initiatives  
Mailing Lists  
Membership  
Merchandise  
News  
Community portal  
Presentations  
Press  
Projects  
Video  
Volunteer

Reference  
Activities  
Attacks  
Code Snippets  
Controls  
Glossary  
How To...  
Java Project  
NET Project

The Open Web Application Security Project (OWASP) is a 501(c)(3) worldwide not-for-profit charitable organization focused on improving the security of software. Our mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about true software security risks.

Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. You'll find everything about OWASP here or linked from our wiki and current information on our OWASP Blog. OWASP does not endorse or recommend commercial products or services, allowing our community to remain vendor neutral with the collective wisdom of the best minds in software security worldwide. We ask that the community look out for inappropriate uses of the OWASP brand including use of our name, logos, project names and other trademark issues.

There are thousands of active wiki users around the globe who review the changes to the site to help ensure quality. If you're new, you may want to check out our getting started page. As a global group of volunteers with over 42,000 participants, questions or comments should be sent to one of our many mailing lists or directed to the OWASP Contact Us Form.

Pick a OWASP Project - Find Your Local OWASP Chapter

Who Trusts OWASP?  
Citations of National & International Legislation, Standards, Guidelines, Committees and Industry Codes of Practice - Click Here

How can OWASP help your org?  
Government Bodies  
Educational Institutions  
Standards Groups  
Trade Organizations  
Certifying Bodies  
Development Organizations

Security101  
Ask a software security question - open to all, especially beginners

Security Conferences, Training  
Global, Regional and Local - Click Here

Upcoming Events

hanka 謝謝 ngiyabonga  
tesekkiur ederim



# OWASP Top 10 -2013

Category:OWASP Top Ten Project | https://www.owasp.org/index.php/Category:OWASP\_Top\_Ten\_Project

Log in Request account



Category Discussion

Read View source View history Search

## Category:OWASP Top Ten Project

Main OWASP Top 10 for 2013 OWASP Top 10 for 2010 Translation Efforts Project Details Some Commercial & OWASP Uses of the Top 10



### OWASP Top 10

The OWASP Top Ten is a powerful awareness document for web application security. The OWASP Top Ten represents a broad consensus about what the most critical web application security flaws are. Project members include a variety of security experts from around the world who have shared their expertise to produce this list.

We urge all companies to adopt this awareness document within their organization and start the process of ensuring that their web applications do not contain these flaws. Adopting the OWASP Top Ten is perhaps the most effective first step towards changing the software development culture within your organization into one that produces secure code.

### Translation Efforts

The OWASP Top 10 has been translated to many different languages by numerous volunteers. These translations are available as follows:

- All versions of the OWASP Top 10 - 2013
- All versions of the OWASP Top 10 - 2010
- Information about the various translation teams

### Licensing

The OWASP Top 10 is free to use. It is licensed under the http://creativecommons.org/licenses/by-sa/3.0/ Creative Commons Attribution-ShareAlike 3.0 license, so you can copy, distribute and transmit the work, and you can adapt it, and use it commercially, but all provided that you attribute the work and if you alter, transform, or build upon this work, you may distribute the resulting work only under the same or similar license to this one.

Share this: [social media icons]

### What is the OWASP Top 10?

The OWASP Top 10 provides:

- A list of the 10 Most Critical Web Application Security Risks

And for each Risk it provides:

- A description
- Example vulnerabilities
- Example attacks
- Guidance on how to avoid
- References to OWASP and other related resources

### Project Leader

- Dave Wichers

### Related Projects

- OWASP Mobile Top 10 Risks
- OWASP Top 10 Cheat Sheet
- Top 10 Proactive Controls
- OWASP Top 10 Mapped to the

### Quick Download

- OWASP Top 10 2013 - PDF
- OWASP Top 10 2013 - wiki
- OWASP Top 10 2013 Presentation - Covering Each Item in the Top 10 (PPTX)

### Email List

Project Email List

### News and Events

- [12 Jun 2013] OWASP Top 10 - 2013 Final Released
- [Feb 2013] Draft OWASP Top 10 - 2013 - Released for Public Comment

### Classifications



- Home
- About OWASP
- Acknowledgements
- Advertising
- AppSec Events
- Books
- Brand Resources
- Chapters
- Donate to OWASP
- Downloads
- Funding
- Governance
- Initiatives
- Mailing Lists
- Membership
- Merchandise
- News
- Community portal
- Presentations
- Press
- Projects
- Video
- Volunteer
- Reference
- Activities
- Attacks
- Code Snippets
- Controls
- Glossary
- How To...
- Java Project
- .NET Project
- Principles
- Technologies
- Threat Agents

# Vulnerable builds - Webgoat



How to work with WebGoat - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://192.168.0.5/WebGoat/attack

Logout ?

**OWASP WebGoat V5.2**

← Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Restart this Lesson

**How To Work With WebGoat**

Welcome to a short introduction to WebGoat. Here you will learn how to use WebGoat and additional tools for the lessons.

**Environment Information**

WebGoat uses Apache Tomcat as server. It is setup to run on localhost. This configuration is for single user. If you want to use WebGoat in a laboratory or in class you might need to change the setup. Please refer to the Tomcat Configuration in the Introduction section.

**The Interface Of WebGoat**

Logout ?

**2 3 4 5 6 Http Basics 7 8**

**OWASP WebGoat V5.2**

← Hints ▶ Show Params Show Cookies Lesson Plan Show Java Solution

Restart this Lesson

Enter your name in the input field below and press "go" to submit. The server will accept the request, reverse the input, and display it back to the user, illustrating the basics of handling an HTTP request.

Transferring data from 192.168.0.5...



# Vulnerable builds – Vul. by Design

The screenshot shows a web browser window at <https://www.vulnhub.com/>. The page displays a navigation menu with links for HOME, SEARCH, HELP, RESOURCES, BLOG, and ABOUT. The main content area features a card for the virtual machine "SmashTheTux: 1.0.1" by canyoupwn.me, dated 1 Apr 2016. The card includes a thumbnail image of the VM's logo, the title "SmashTheTux v1.0.1", and the author "by canyoupwn.me". Below the title is the text "Introduction to Application Vulnerabilities" and "For Educational Purposes". A paragraph describes the VM as a new VM made by canyoupwn.me for those who want to take a step into the world of binary exploitation, consisting of 9 challenges, each introducing a different type of vulnerability. A list of weaknesses is provided:

- Stack Overflow Vulnerability
- Off-by-One Vulnerability
- Integer Overflow
- Format String Vulnerability
- Denial of Service

Below the list is the SHA1 hash: 01DCB1AB85B139A386AD97B41190731509612F59. A "Download" button is visible in the bottom right corner of the card. Below this card, the beginning of another card for "Kevgir: 1" by canyoupwn.me, dated 15 Feb 2016, is visible.

# Ed's Challenges

Browser: http://www.counterhack.net/Counter\_Hack/Challenges.html | Hacker Challenges

[Welcome](#) | **Challenges** | [Enigma Pr0n](#) | [Articles](#) | [WMIC](#) | [Presentations](#)  
[0x10 Third Place](#) | [Humor](#) | [About Me](#) | [Just Your Typical Office](#)

## Hacker Challenges

**The Hacker Challenge Collection Written By Me:**

- Miracle on Thirty-Hack Street**  
 by Ed Skoudis & Kevin Johnson, Dec 2009  
[\(Answers\)](#)
- Santa Claus is Hacking to Town**  
 Dec 2008 [\(Answers\)](#)
- It Happened One Friday**  
 March 2008 [\(Answers\)](#)
- Frosty the Snow Crash**  
 Dec 2007 [\(Answers\)](#)
- Charlotte's Web Site**  
 Feb 2007 [\(Answers\)](#)
- A Christmas (Hacking) Story**  
 Dec 2006 [\(Answers\)](#)
- Star Hacks, Episode V: The Empire Hacks Back**  
 April 2006 [\(Answers\)](#)
- 0x10 Candles**  
 Nov 2004 [\(Answers\)](#)
- Hackers of the Lost Ark**  
 June 2004 [\(Answers\)](#)
- Lord of the Ring Zero**  
 March 2004 [\(Answers\)](#)

**SEC 504**

Access to World Class Pen Testing Training

**Mentor**

Only \$2500

Click here for details

**SEC 560**

**The Latest Hacker Challenge**

I'm excited to announce that my friend Yori Kvitchko and I have written a new challenge at Ethical Hacker dot Net titled "The Nightmare Before Charlie Brown's Christmas". We hope you'll enjoy it!

**The Nightmare Before Charlie Brown's Christmas**  
 Dec 2010  
 (by Ed Skoudis and Yori Kvitchko)

**Challenges Written By My Friends:**

- SSHiders**



## Need More?

- Set up a lab
- VMWare Player
- Oracle VM Virtualbox
- Plenty of VM images available



## Final words

- Enjoy yourself
- Web vulnerability work is challenging, interesting and fun
- Remember, be a tiny goat



# Questions?



Be a Tiny Goat

**Bill Freda**

CISSP, CRISC, GPEN, GSEC, GWAPT

[bill.freda@vita.virginia.gov](mailto:bill.freda@vita.virginia.gov)

804-416-6031