Let's Hack! Workshop

Let's Hack! Workshop

Stephen Rees-Carter

The majority of security incidents occur as a result of common vulnerabilities and weaknesses that were overlooked or not fully understood by developers. The goal of **Let's Hack!** is to make sure your company's doesn't fall victim to the same fate. By teaching your developers to think like a hacker, they'll be able to spot vulnerabilities and weaknesses within your applications, so they can protect them from the most commonly exploited security vulnerabilities.

Summary

Let's Hack! is an interactive workshop that teaches web developers security concepts in a hands-on and engaging way. Attendees work through a series of challenges, learning about and directly using different hacking techniques to compromise an intentionally vulnerable application.

The hands-on nature of this workshop means that developers will get a really solid understanding of how common security exploits work, which will set them up to write more secure code, and consider about security concepts when building apps.

Throughout the workshop, the attendees will learn how to think like a hacker - how to identify and exploit vulnerabilities - which in turn teaches them how to recognise when their own code (and those of their peers) could be vulnerable, so they can write more secure code and build more secure applications. The goal of the workshop is to train developers to write more secure code, and to identify and fix vulnerable code in the applications they work on - making them more secure and less vulnerable to the common weaknesses hackers go looking for.

Target Audience

The target audience is Laravel / PHP developers, however most of the concepts are applicable to anyone with technical skills and an interest in cyber security. Most of the challenges don't require any coding skills, and those that do are fairly generic. As part of the workshop, I move around the room (or check in with folks digitally) to see how they are going, and help everyone complete the challenges.

For the more competitive teams, solving challenges earns attendees points which goes onto the leader board, indicating the most accomplished hackers on the team.

I can also tailor the content to be more generic depending on your team. I.e. If you don't use Laravel, we'll do generic challenges instead.

Stephen Rees-Carter
Director / Friendly Hacker
stephen@valorinsecurity.com
CompTIA Security+
Certified Ethical Hacker

Valorin Security Pty Ltd
ABN 93 660 758 574

For more information, visit:
https://valorinsecurity.com

Let’s Hack! Workshop

How Does it Work?

The workshop is fully interactive and run with small group of developers, up to around 30 attendees. The workshop is structured in a series of challenges, each featuring a different security vulnerability or risk, with a specific takeaway concept for attendees to learn from each. The concept of each challenge will be discussed as a group and then attendees will need to solve the challenges directly within the application, with direct support given to any attendees who require it. We’ll then work through the challenge as a group, ensuring everyone progresses and learns the different concepts being covered.

As part of the challenges, live progress and attempts will be shown on the screen, with attendees earning points for solving challenges. This adds to the interactive feel and allows attendees to see how their peers are going. Some teams may also enjoy the competitive nature of the point scoring, and complete for bragging rights.

Each attendee will require their own laptop, with access to at least a web browser. Access to a command line and the ability to run other code, such as PHP, is preferred not but required. The workshop uses a custom built, intentionally vulnerable application, which is accessible through a web browser. It is intentionally slow paced, with ample time for questions to be asked, and tangents to be taken.

What Topics Are Covered?

- OWASP Top 10
- Password Enumeration
- Password Reuse
- SQL Injection
- Rate Limiting
- Missing Authorisation
- Incomplete Configuration
- Cryptography Failures
- Mass-Assignment
- Insecure Direct Object References
- Information Leakage
- Local File Inclusion
- Cross-Site Scripting
- Privilege Escalation
- Session Hijack
- Watering Hole Attacks
- Deserialisation Attacks
- Content Security Policies
- Canary Tokens
- Debugging Tools

A subset of these challenges will be included within the workshop, depending on the length of the workshop and your specific needs. If you have specific topics you’d specifically like covered, let me know and they can be enabled or implemented (if suitable).

Stephen Rees-Carter
Director / Friendly Hacker
stephen@valorinsecurity.com
CompTIA Security+
Certified Ethical Hacker

Valorin Security Pty Ltd
ABN 93 660 758 574

For more information, visit:
https://valorinsecurity.com

Let’s Hack! Workshop

Format

Half-Day Workshop (~4 hours)
The half-day workshop focuses mainly on the vulnerabilities themselves through the web browser. The idea is to teach the attendees how the different vulnerabilities work, and the hacker mindset needed to discover and exploit them across a variety of scenarios. Attendees can then take this knowledge and apply it to their own code and the apps they work on, as they’ll recognise vulnerable patterns and weaknesses before it’s deployed to production.

Full-Day Workshop (~8 hours)
The full-day workshop covers everything in the half-day, and adds code reviews by teaching attendees how to find and exploit vulnerable code patterns. These are the more subtle vulnerabilities that aren’t obvious or easily findable from the browser alone, but can be devastating if found by someone with malicious intent.

Sample Outline

12:30pm → Welcome (20 mins)
12:50pm → User Enumeration (20 mins)
1:10pm → Broken Access Control (20 mins)
1:25pm → BREAK (10 mis)
1:35pm → Mass-Assignment (30 mins)
2:05pm → IDOR (15 mins)
2:16pm → BREAK (10 mins)
2:26pm → XSS & Ziggy (30 mins)
3:10pm → BREAK (10 mins)
3:20pm → Local File Inclusion (30 mins)
3:50pm → Telescope & Account Hijack (30 mins)
4:20pm → Questions!

Stephen Rees-Carter
Director / Friendly Hacker
stephen@valorinsecurity.com
CompTIA Security+
Certified Ethical Hacker

Valorin Security Pty Ltd
ABN 93 660 758 574

For more information, visit:
https://valorinsecurity.com

Let’s Hack! Workshop

Feedback

Let’s Hack! was first presented at **Longhorn PHP 2023**, and received a number of 5/5 reviews from attendees: https://joind.in/event/longhorn-php-conference-2023/lets-hack

.“Stephen put together a really insightful, helpful tutorial. He made the hack session interactive, engaging, and educational. He gave time for attendees to poke around, and gave tips to help solve the challenges. Loved it!”

“It was a lot of fun! Hacking an actual website really really drove the items home & was super engaging. The website was also put together really well. And the leaderboard aspect w/ real time stats just added to everything.”

“The challenge was fun and made me rethink some of our security related test procedures.”

“An enjoyable and very informative guide to test sites and really think about security from all levels for a site.”

About Stephen Rees-Carter

Stephen Rees-Carter is a PHP and Laravel specialist with over 20 years experience working with PHP and over 10 years experience specialising on Laravel as a senior developer, technical lead and product manager.

Stephen holds current CompTIA Security+ and Certified Ethical Hacker certifications, and teaches Laravel developers about security through conference talks, workshops, his Practical Laravel Security course, Securing Laravel mailing list, and is an active contributor to the Laravel framework.

Stephen started **Valorin Security Pty Ltd** to provide PHP and Laravel developers with specialised security audits, penetration tests, and consulting, focused on understanding the Laravel and PHP ecosystem and the unique abilities, protections, and weaknesses within it.

Stephen Rees-Carter
Director / Friendly Hacker
stephen@valorinsecurity.com
CompTIA Security+
Certified Ethical Hacker

Valorin Security Pty Ltd
ABN 93 660 758 574

For more information, visit:
https://valorinsecurity.com