



Do Know Evil

Web Application Exploits and Defenses

by Bruce Leban in Google Kirkland

<http://jarlsberg.appspot.com>

If you want your application to be as secure as possible, you need to **learn how Evil People think**. And you'll want to use that knowledge to **do penetration testing**: attacking your own application to try to find bugs.

To help you **understand how applications can be attacked** and how to protect them from attack, we've created the **“Web Application Exploits and Defenses” codelab**. The codelab uses Jarlsberg, a small, cheesy, web application that is full of real world bugs.

In the codelab, you'll learn how to:

- Attack a web application to find and exploit common web security vulnerabilities.
- Avoid and fix these common bugs.

Jarlsberg is chock full of cool features, and **the more features** an application has **the larger the attack surface**. Your application probably has features just like these:

Can you match each feature to the vulnerability that it exposes and the exploit it enables?

Feature	Vulnerability	Exploit
New template language	Cross Site Scripting (XSS)	Information disclosure
HTML allowed in snippets	Cross Site Request Forgery (XSRF)	Elevation of privilege
File upload capability	Cross Site Script Inclusion (XSSI)	Denial of Service (DoS)
AJAX	Path traversal	Spoofing
Web-based admin console	Client-state manipulation	Code execution

Ha! Tricked you! Each of these features introduces multiple vulnerabilities. And each vulnerability can be exploited in multiple ways. **The codelab walks you step by step through each vulnerability**, with progressive hints guiding you on how to find them, how to exploit them and how to avoid them.

Here are some **examples of fictitious attacks** against Google applications. Do you recognize them? (answers below)

<code>http://www.gmail.com/?search=in:spam+-%3Cscript%3EselectAll().toInbox()%3C/script%3E</code>
<code>http://www.blogger.com/delete-blog.g</code>
<code>http://www.picasa.com/../../../../../../../../etc/passwd</code>
<code>http://www.youtube.com/control-panel?v=Vr0oK3gMzK&action=rickroll</code>
<code>http://checkout.google.com/update/cart?order=4815162342&total=1.08</code>

Are you sure that your application isn't vulnerable to similar attacks!?

More information, discussion, and archives:

<http://googletesting.blogspot.com>



© 2010 Google Inc. Licensed under a Creative Commons Attribution-Share Alike 3.0 License <http://creativecommons.org/licenses/by-sa/3.0/>

Did you correctly identify the attacks?

Answers: XSS, XSRF, path traversal, configuration vulnerability, and client-state manipulation.

