

Forum:[Hack Forums](#)

Thread: [\[Tools\] Penetration testing with Google Chrome Utility](#)

??g???! - June 4, 2012, 7:04 am

Looking around i just found some some interesting and useful extensions that can help anyone of us on a penetration test using Chrome Browser.

Websecurify Scanner

[Websecurify](#) is a powerful cross-platform web security testing technology designed from the ground up with simplicity in mind.

Websecurify is an advanced testing solution built to quickly and accurately identify web application security issues. Websecurify saves you time and money by automating a tiresome and very technical process used by experts to find scary security vulnerabilities.

XSS Rays

[Complete XSS reversing/scanner tool](#). Find how a site is filtering code, check for injections and inspect objects.

XSS Rays is a security tool to help pen test large web sites. It's core features include a XSS scanner, XSS Reverser and object inspection. Need to know how a certain page filters output? Don't have the source? No problem. XSS Rays will blackbox reverse a XSS filter without needing the source code.

Google Hack Data Base

[Google Hack Data Base](#) - application to work with GHDB.

Google Hack Data Base - application to work with GHDB. Choose a category and click on the necessary query. To find description vulnerability, click "Search on [www.exploit-db.com](#)". Application provides possibility to search vulnerabilities on the specified site. Just click on the search button and enter the site name. This application allows a better understanding of the basis web security.

XSS ChEF

[Chrome Extension Exploitation Framework](#)

This is a Chrome Extension Exploitation Framework - think BeEF for Chrome extensions. Whenever you encounter a XSS vulnerability in Chrome extension, ChEF will ease the exploitation.

Site Spider

Website Crawler

Use this extension to [spider a website](#) looking for dead links. One can restrict the spidering to a directory, a domain, or any other regular expression. The spider can also follow one link beyond this restriction, allowing one to find broken external links.

Form Fuzzer

HTML form fuzz tester.

This is a [fuzz testing](#), utility created to assist in populating web forms with some random data.

HPP Finder

Detect potential HPP attack vectors.

[HTTP Parameter Pollution \(HPP\)](#) is a recently discovered web exploitation technique. Please read the NDSS 2010 paper for more details about the technique. HPP Finder is a Chrome extension designed for detecting HPP attempts. HPP Finder can detect URLs and HTML forms that might be susceptible of parameter pollution, but it is not a complete solution against HPP.

This is not my work.

Credits go to Security-Shell

MaXoNe - June 4, 2012, 9:16 am

Really cool collection , I myself am kind of Firefox and Burp Proxy type of guy , but will take a look at these , maybe Chrome with these tools will turn out to be a better option. Thanks

n00b.ca - June 4, 2012, 12:27 pm

Looks really good. I'll be checking these tools out.

iRBAWS - June 4, 2012, 12:52 pm

Nice extensions, but with the Chrome XSS "block", they are kind of useless...