



## THE 90'S CALLED

They want their seat-based research back

[www.DropaSeat.com](http://www.DropaSeat.com)

LEARN MORE!

### Immunity Unleashes Automatic Exploit Tool

August 6, 2007

By Lisa Vaas

LAS VEGAS—[Immunity](#), a company already well-known for making pen testing easy, has released a new tool to make writing exploits near-automatic.

Immunity released the tool, called [Debugger](#), here at the Defcon hackers convention on Aug. 3. Debugger is free for download, with its revenue being driven by paid ads from companies looking to hire the pen testers who use such a tool. One of the first help-wanted ads taken out by such companies includes [Application Security](#).

ADVERTISEMENT

**Not Feeling the Love**  
from Your IT Research Provider?

Get the love you deserve — [www.DropaSeat.com](http://www.DropaSeat.com)

Debugger comes with what Immunity says is the industry's first heap analysis tool built specifically for heap creation. It also sports a large Python API for easy extensibility and has function graphing as part of its user interface.

#### RELATED LINKS

- [Undercover 'Dateline' Reporter Outed, Flees from Defcon](#)
- [Websense to Unveil Web 2.0 Threat Detection at Defcon](#)
- [Time to Take Your Blue Pill](#)
- [iPhone Update Erases User Modifications](#)
- [States Seek Funding Help for Real ID Technology](#)

Immunity is claiming that Debugger will cut exploit development time by 50 percent.

Not everybody's happy to hear that.

"They've got a good development community," said Dave Marcus, security research and communications manager at McAfee's Avert Labs, in an interview with eWEEK at Defcon. "But I look at it from the other side of house: What does this mean to the computing public?"

What it means is more zero days, Marcus said. "And that's certainly not a good thing. I think you'll see a spike in zero days, and contributions to the zero-day initiative, because it makes it easier to find vulnerabilities. You're making the job easier.

Immunity CEO Dave Aitel doesn't see any problem with helping customers find zero days. As a matter of fact, Immunity trains people to find zero days.

"That's something we think all companies should do," he told eWEEK. "Otherwise you'll be sticking your head in the sand."

Marcus said he doesn't think that "the bug exists already" argument is a good one. "Yes, we know that," he said. "We know the bugs are in the code. But making more and more tools" to make it easier to find those bugs, that, he said, is not going to make his customers happy.

"They'll all do this," he said, rolling his eyes to the ceiling. "'Great!'"

Of course, there are already fuzzers that track down vulnerabilities that can lead to exploitation. However, until now, writing exploits has been the manual part of it, done in the "tweaking" process, Marcus said.

Read [here](#) about a new application and network security tool from startup Breaking Point Systems.

Now, the security industry doesn't have to write its own programs to automate the translation of a vulnerability to an exploit.

"You don't have to learn the Canvas API [another Immunity tool] or how to build exploits," Aitel promised, as much of the functionality of these tools are built into Debugger.

Debugger's interfaces include a GUI and a command line that's always available at the bottom of the GUI. This allows users to type shortcuts as if they were in a typical text-based debugger. Immunity has also implemented aliases so that users of its other tools don't have to be retrained and can just leap into using the debugger interface.

Check out eWEEK.com's Security Center for the latest security news, reviews and analysis. And for insights on security coverage around the Web, take a look at [eWEEK's Security Watch blog](#).

Copyright (c) 2007 Ziff Davis Media Inc. All Rights Reserved.