Jeff Williams Röportajı

OWASP Turkey, Aralık 2010, WGT E-Dergi 7. Sayı

1. How did you end up dealing with web/application security?

The short answer is that I've been making software fail since the early 1980's and finding vulnerabilities always came naturally. But over the last 15 years or so, my "breaker" side is losing out to the "builder" in me. So I've been focused on helping companies get better at building secure applications. (The long answer is here)

2. How do you foresee the evolution of web attacks in the near future?

I think we'll continue to see new technologies emerge that ignore the security lessons of the past. I think we'll continue to see organizations try to react to security problems rather than preventing them from occurring. And I think we'll continue to make very slow progress in application security – much slower than the threat.

Specifically, as applications become more and more connected, I think we'll see a lot of issues related to federated authentication and access control schemes. We'll start to see injection attacks that chain through multiple layers of systems, encoding, and decoding to reach their target interpreters. And I think we'll start to see the same types of problems with rich client communication channels that we see in the typical web application today, but since they're all custom, diagnosing them will be more difficult. I know this is a grim assessment, but we have to do something different if we want to effect a change.

3. What are your recommendations to underground web security community in Turkey to get their hands cleaned and become professionals?

I've found that working to create great security controls like the ESAPI project is very rewarding. In many ways, it's harder to build a control that can withstand any attack than it is to break something. The game has changed for me. Now I'm interested in changing the software ecosystem so that it produces more security. To do this, you have to understand how the ecosystem works, look for opportunities, and do unexpected things. Innovate. If you can focus your hacking skills on finding ways to change culture -- both in organizations and across the world -- it's a great career and a fun way to go through life.