Real-World Bug Hunting

A Field Guide to Web Hacking

by Peter Yaworski

errata updated to print 3

Page	Error	Correction	Print corrected
83	We need to eliminate the `password` parameter, which we can do by adding `;--, test' OR `**`1='1;--`**`.	We need to eliminate the `password` parameter, which we can do by adding `;--, test' OR `**`1=1;--`**`.	Print 3
93	You should also look for places where you can pass data to a site in unexpected ways, such as where you can substitute array parameters in request data, as in the **Uber** bug.	You should also look for places where you can pass data to a site in unexpected ways, such as where you can substitute array parameters in request data, as in the **Drupal** bug.	Print 3
109	The default value of **`Responsibility`** is defined as 0 ❼.	The default value of **`fundamental`** is defined as 0 ❼.	Print 3
116	(the */etc/issue* file **will will** return the operating system used):	(the */etc/issue* file **will** return the operating system used):	Print 3
172	Cable submitted the vulnerability, and Yahoo! fixed it **with within** five hours of receiving his report.	Cable submitted the vulnerability, and Yahoo! fixed it **within** five hours of receiving his report.	Print 3
195	When using Burp Intruder, on the other hand, I'll **send send** a request for the domain . . .	When using Burp Intruder, on the other hand, I'll **send** a request for the domain . . .	Print 3
219	As of this writing, HackerOne is the only platform that allows hackers to publicly disclose bugs **on on** their platform,	As of this writing, HackerOne is the only platform that allows hackers to publicly disclose bugs **on** their platform,	Print 3
223	Bryant is the author of some great hacking tools, perhaps most notably XSSHunter, which **you can use you can use** to discover blind XSS vulnerabilities.	Bryant is the author of some great hacking tools, perhaps most notably XSSHunter, which **you can use** to discover blind XSS vulnerabilities.	Print 3