

# Web Hacking 101

How to Make Money Hacking Ethically

Peter Yaworski

This book is for sale at <http://leanpub.com/web-hacking-101>

This version was published on 2018-11-30



Leanpub

This is a [Leanpub](#) book. Leanpub empowers authors and publishers with the Lean Publishing process. [Lean Publishing](#) is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

© 2015 - 2018 Peter Yaworski

# Tweet This Book!

Please help Peter Yaworski by spreading the word about this book on [Twitter!](#)

The suggested tweet for this book is:

Can't wait to read [Web Hacking 101: How to Make Money Hacking Ethically](#) by [@yaworsk](#) [#bugbounty](#)

The suggested hashtag for this book is [#bugbounty](#).

Find out what other people are saying about the book by clicking on this link to search for this hashtag on Twitter:

[#bugbounty](#)

To Andrea and Ellie, thank you for supporting my constant roller coaster of motivation and confidence. Not only would I never have finished this book without you, my journey into hacking never would have even begun.

To the HackerOne team, this book wouldn't be what it is if it were not for you, thank you for all the support, feedback and work that you contributed to make this book more than just an analysis of 30 disclosures.

Lastly, while this book sells for a minimum of \$9.99, sales at or above the suggested price of \$19.99 help me to keep the minimum price low, so this book remains accessible to people who can't afford to pay more. Those sales also allow me to take time away from hacking to continually add content and make the book better so we can all learn together.

While I wish I could list everyone who has paid more than the minimum to say thank you, the list would be too long and I don't actually know any contact details of buyers unless they reach out to me. However, there is a small group who paid more than the suggested price when making their purchases, which really goes a long way. I'd like to recognize them here. They include:

1. @Ebrietas0
2. Mystery Buyer
3. Mystery Buyer
4. @nahamsec (Ben Sadeghipour)
5. Mystery Buyer
6. @Spam404Online
7. @Danyl0D (Danylo Matviyiv)
8. Mystery Buyer
9. @arneswinnen (Arne Swinnen)

If you should be on this list, please DM me on Twitter.

To everyone who purchased a copy of this, thank you!

# Contents

- 1. Foreword . . . . . 1**
- 2. Introduction . . . . . 3**
  - How It All Started . . . . . 3
  - Just 30 Examples and My First Sale . . . . . 4
  - Who This Book Is Written For . . . . . 6
  - Chapter Overview . . . . . 7
  - Word of Warning and a Favour . . . . . 9
- 3. Background . . . . . 10**
- 4. Open Redirect Vulnerabilities . . . . . 13**
  - Description . . . . . 13
  - Examples . . . . . 14
    - 1. Shopify Theme Install Open Redirect . . . . . 14
    - 2. Shopify Login Open Redirect . . . . . 14
    - 3. HackerOne Interstitial Redirect . . . . . 16
  - Summary . . . . . 17
- 5. HTTP Parameter Pollution . . . . . 19**
  - Description . . . . . 19
  - Examples . . . . . 22
    - 1. HackerOne Social Sharing Buttons . . . . . 22
    - 2. Twitter Unsubscribe Notifications . . . . . 23
    - 3. Twitter Web Intents . . . . . 24
  - Summary . . . . . 27
- 6. Cross-Site Request Forgery . . . . . 28**
  - Description . . . . . 28
  - Examples . . . . . 32
    - 1. Shopify Twitter Disconnect . . . . . 32
    - 2. Change Users Instacart Zones . . . . . 34
    - 3. Badoo Full Account Takeover . . . . . 35
  - Summary . . . . . 37

## CONTENTS

|  |           |
|--|-----------|
| <b>7. HTML Injection</b> . . . . .               | <b>38</b> |
| Description . . . . .                            | 38        |
| Examples . . . . .                               | 38        |
| 1. Coinbase Comments . . . . .                   | 38        |
| 2. HackerOne Unintended HTML Inclusion . . . . . | 40        |
| 3. Within Security Content Spoofing . . . . .    | 41        |
| Summary . . . . .                                | 43        |
| <b>8. CRLF Injection</b> . . . . .               | <b>44</b> |
| Description . . . . .                            | 44        |
| 1. Twitter HTTP Response Splitting . . . . .     | 45        |
| 2. v.shopify.com Response Splitting . . . . .    | 47        |
| Summary . . . . .                                | 49        |
| <b>9. Cross-Site Scripting</b> . . . . .         | <b>50</b> |
| Description . . . . .                            | 50        |
| Examples . . . . .                               | 55        |
| 1. Shopify Wholesale . . . . .                   | 55        |
| 2. Shopify Giftcard Cart . . . . .               | 57        |
| 3. Shopify Currency Formatting . . . . .         | 59        |
| 4. Yahoo Mail Stored XSS . . . . .               | 60        |
| 5. Google Image Search . . . . .                 | 62        |
| 6. Google Tagmanager Stored XSS . . . . .        | 63        |
| 7. United Airlines XSS . . . . .                 | 64        |
| Summary . . . . .                                | 69        |
| <b>10. Template Injection</b> . . . . .          | <b>70</b> |
| Description . . . . .                            | 70        |
| Server Side Template Injections . . . . .        | 70        |
| Client Side Template Injections . . . . .        | 71        |
| Examples . . . . .                               | 72        |
| 1. Uber Angular Template Injection . . . . .     | 72        |
| 2. Uber Template Injection . . . . .             | 73        |
| 3. Rails Dynamic Render . . . . .                | 76        |
| Summary . . . . .                                | 77        |
| <b>11. SQL Injection</b> . . . . .               | <b>78</b> |
| Description . . . . .                            | 78        |
| SQL Databases . . . . .                          | 78        |
| Countermeasures Against SQLi . . . . .           | 80        |
| Examples . . . . .                               | 80        |
| 1. Drupal SQL Injection . . . . .                | 80        |
| 2. Yahoo Sports Blind SQL . . . . .              | 83        |
| 3. Uber Blind SQLi . . . . .                     | 86        |

## CONTENTS

|  |            |
|--|------------|
| Summary . . . . .                                      | 89         |
| <b>12. Server Side Request Forgery . . . . .</b>       | <b>90</b>  |
| Description . . . . .                                  | 90         |
| HTTP Request Location . . . . .                        | 90         |
| Invoking GET Versus POST Requests . . . . .            | 91         |
| Blind SSRFs . . . . .                                  | 91         |
| Leveraging SSRF . . . . .                              | 92         |
| Examples . . . . .                                     | 93         |
| 1. ESEA SSRF and Querying AWS Metadata . . . . .       | 93         |
| 2. Google Internal DNS SSRF . . . . .                  | 94         |
| 3. Internal Port Scanning . . . . .                    | 98         |
| Summary . . . . .                                      | 100        |
| <b>13. XML External Entity Vulnerability . . . . .</b> | <b>101</b> |
| Description . . . . .                                  | 101        |
| Examples . . . . .                                     | 106        |
| 1. Read Access to Google . . . . .                     | 106        |
| 2. Facebook XXE with Word . . . . .                    | 107        |
| 3. Wikiloc XXE . . . . .                               | 110        |
| Summary . . . . .                                      | 113        |
| <b>14. Remote Code Execution . . . . .</b>             | <b>114</b> |
| Description . . . . .                                  | 114        |
| Examples . . . . .                                     | 114        |
| 1. Polyvore ImageMagick . . . . .                      | 114        |
| 2. Algolia RCE on facebooksearch.algolia.com . . . . . | 116        |
| 3. Foobar Smarty Template Injection RCE . . . . .      | 118        |
| Summary . . . . .                                      | 122        |
| <b>15. Memory . . . . .</b>                            | <b>123</b> |
| Description . . . . .                                  | 123        |
| Buffer Overflow . . . . .                              | 123        |
| Read out of Bounds . . . . .                           | 124        |
| Memory Corruption . . . . .                            | 126        |
| Examples . . . . .                                     | 127        |
| 1. PHP ftp_genlist() . . . . .                         | 127        |
| 2. Python Hotshot Module . . . . .                     | 128        |
| 3. Libcurl Read Out of Bounds . . . . .                | 129        |
| 4. PHP Memory Corruption . . . . .                     | 130        |
| Summary . . . . .                                      | 131        |
| <b>16. Sub Domain Takeover . . . . .</b>               | <b>132</b> |
| Description . . . . .                                  | 132        |

## CONTENTS

|   |            |
|---|------------|
| Examples . . . . .                                      | 132        |
| 1. Ubiquiti Sub Domain Takeover . . . . .               | 132        |
| 2. Scan.me Pointing to Zendesk . . . . .                | 133        |
| 3. Shopify Windsor Sub Domain Takeover . . . . .        | 134        |
| 4. Snapchat Fastly Takeover . . . . .                   | 135        |
| 5. api.legalrobot.com . . . . .                         | 137        |
| 6. Uber SendGrid Mail Takeover . . . . .                | 140        |
| Summary . . . . .                                       | 143        |
| <b>17. Race Conditions . . . . .</b>                    | <b>144</b> |
| Description . . . . .                                   | 144        |
| Examples . . . . .                                      | 146        |
| 1. Starbucks Race Conditions . . . . .                  | 146        |
| 2. Accepting HackerOne Invites Multiple Times . . . . . | 147        |
| 3. Exceeding Keybase Invitation Limits . . . . .        | 150        |
| 4. HackerOne Payments . . . . .                         | 151        |
| Summary . . . . .                                       | 153        |
| <b>18. Insecure Direct Object References . . . . .</b>  | <b>154</b> |
| Description . . . . .                                   | 154        |
| Examples . . . . .                                      | 155        |
| 1. Binary.com Privilege Escalation . . . . .            | 155        |
| 2. Moneybird App Creation . . . . .                     | 156        |
| 3. Twitter Mopub API Token Stealing . . . . .           | 158        |
| Summary . . . . .                                       | 160        |
| <b>19. OAuth . . . . .</b>                              | <b>161</b> |
| Description . . . . .                                   | 161        |
| Examples . . . . .                                      | 165        |
| 1. Swiping Facebook Official Access Tokens . . . . .    | 165        |
| 2. Stealing Slack OAuth Tokens . . . . .                | 166        |
| 3. Stealing Google Drive Spreadsheets . . . . .         | 167        |
| Summary . . . . .                                       | 170        |
| <b>20. Application Logic Vulnerabilities . . . . .</b>  | <b>171</b> |
| Description . . . . .                                   | 171        |
| Examples . . . . .                                      | 172        |
| 1. Shopify Administrator Privilege Bypass . . . . .     | 172        |
| 2. HackerOne Signal Manipulation . . . . .              | 173        |
| 3. Shopify S3 Buckets Open . . . . .                    | 174        |
| 4. HackerOne S3 Buckets Open . . . . .                  | 175        |
| 5. Bypassing GitLab Two Factor Authentication . . . . . | 177        |
| 6. Yahoo PHP Info Disclosure . . . . .                  | 179        |
| 7. HackerOne Hactivity Voting . . . . .                 | 180        |

## CONTENTS

|  |            |
|--|------------|
| 8. Accessing PornHub's Memcache Installation . . . . . | 183        |
| 9. Bypassing Twitter Account Protections . . . . .     | 185        |
| Summary . . . . .                                      | 186        |
| <b>21. Getting Started . . . . .</b>                   | <b>188</b> |
| Reconnaissance . . . . .                               | 188        |
| Subdomain Enumeration . . . . .                        | 189        |
| Port Scanning . . . . .                                | 190        |
| Screenshotting . . . . .                               | 190        |
| Content Discovery . . . . .                            | 191        |
| Previous Bugs . . . . .                                | 192        |
| Testing the Application . . . . .                      | 193        |
| The Technology Stack . . . . .                         | 193        |
| Functionality Mapping . . . . .                        | 194        |
| Finding Vulnerabilities . . . . .                      | 195        |
| Going Further . . . . .                                | 196        |
| Summary . . . . .                                      | 198        |
| <b>22. Vulnerability Reports . . . . .</b>             | <b>199</b> |
| Read the disclosure guidelines. . . . .                | 199        |
| Include Details. Then Include More. . . . .            | 199        |
| Confirm the Vulnerability . . . . .                    | 200        |
| Show Respect for the Company . . . . .                 | 200        |
| Bounties . . . . .                                     | 202        |
| Don't Shout Hello Before Crossing the Pond . . . . .   | 202        |
| Parting Words . . . . .                                | 203        |
| <b>23. Tools . . . . .</b>                             | <b>205</b> |
| Burp Suite . . . . .                                   | 205        |
| ZAP Proxy . . . . .                                    | 205        |
| Knockpy . . . . .                                      | 206        |
| HostileSubBruteforcer . . . . .                        | 206        |
| Sublist3r . . . . .                                    | 206        |
| crt.sh . . . . .                                       | 206        |
| IPV4info.com . . . . .                                 | 207        |
| SecLists . . . . .                                     | 207        |
| XSSHunter . . . . .                                    | 207        |
| sqlmap . . . . .                                       | 207        |
| Nmap . . . . .   | 208        |
| Eyewitness . . . . .                                   | 208        |
| Gowitness . . . . .                                    | 209        |
| Gobuster . . . . .                                     | 209        |
| Meg . . . . .  | 209        |
| Shodan . . . . .                                       | 209        |



## CONTENTS

|                                       |            |
|---------------------------------------|------------|
| Censys                                | 210        |
| What CMS                              | 210        |
| BuiltWith                             | 210        |
| Nikto                                 | 210        |
| Recon-ng                              | 211        |
| GitRob                                | 211        |
| CyberChef                             | 211        |
| OnlineHashCrack.com                   | 212        |
| idb                                   | 212        |
| Wireshark                             | 212        |
| Bucket Finder                         | 212        |
| Race the Web                          | 212        |
| Google Dorks                          | 213        |
| JD GUI                                | 213        |
| Mobile Security Framework             | 213        |
| Ysoserial                             | 213        |
| Firefox Plugins                       | 214        |
| FoxyProxy                             | 214        |
| User Agent Switcher                   | 214        |
| Firebug                               | 214        |
| Hackbar                               | 214        |
| Websecurify                           | 214        |
| Cookie Manager+                       | 215        |
| XSS Me                                | 215        |
| Offsec Exploit-db Search              | 215        |
| Wappalyzer                            | 215        |
| <b>24. Resources</b>                  | <b>216</b> |
| Online Training                       | 216        |
| Web Application Exploits and Defenses | 216        |
| The Exploit Database                  | 216        |
| Udacity                               | 216        |
| Bug Bounty Platforms                  | 216        |
| Hackerone.com                         | 216        |
| Bugcrowd.com                          | 217        |
| Synack.com                            | 217        |
| Cobalt.io                             | 217        |
| Video Tutorials                       | 217        |
| youtube.com/yaworsk1                  | 217        |
| Seccasts.com                          | 217        |
| How to Shot Web                       | 217        |
| Further Reading                       | 218        |
| OWASP.com                             | 218        |

## CONTENTS

|  |            |
|--|------------|
| Hackerone.com/hacktivity . . . . .                                 | 218        |
| https://bugzilla.mozilla.org . . . . .                             | 218        |
| Twitter #infosec and #bugbounty . . . . .                          | 218        |
| Twitter @disclosedh1 . . . . .                                     | 218        |
| Web Application Hackers Handbook . . . . .                         | 218        |
| Bug Hunters Methodology . . . . .                                  | 219        |
| Recommended Blogs . . . . .  | 219        |
| philippeharewood.com . . . . .                                     | 219        |
| Philippe's Facebook Page - www.facebook.com/phwd-113702895386410 . | 219        |
| fin1te.net . . . . .   | 219        |
| NahamSec.com . . . . .   | 219        |
| blog.it-securityguard.com . . . . .                                | 220        |
| blog.innerht.ml . . . . .  | 220        |
| blog.orange.tw . . . . .   | 220        |
| Portswigger Blog . . . . .   | 220        |
| Nvisium Blog . . . . .   | 220        |
| blog.zsec.uk . . . . .   | 220        |
| brutellogic.com.br . . . . .                                       | 220        |
| lcamtuf.blogspot.ca . . . . .                                      | 221        |
| Bug Crowd Blog . . . . .   | 221        |
| HackerOne Blog . . . . .   | 221        |
| Cheatsheets . . . . .  | 221        |
| <b>25. Glossary . . . . .</b>                                      | <b>222</b> |
| Black Hat Hacker . . . . .   | 222        |
| Buffer Overflow . . . . .  | 222        |
| Bug Bounty Program . . . . .                                       | 222        |
| Bug Report . . . . .   | 222        |
| CRLF Injection . . . . .   | 222        |
| Cross Site Request Forgery . . . . .                               | 223        |
| Cross Site Scripting . . . . .                                     | 223        |
| HTML Injection . . . . .   | 223        |
| HTTP Parameter Pollution . . . . .                                 | 223        |
| HTTP Response Splitting . . . . .                                  | 223        |
| Memory Corruption . . . . .  | 223        |
| Open Redirect . . . . .  | 224        |
| Penetration Testing . . . . .                                      | 224        |
| Researchers . . . . .  | 224        |
| Response Team . . . . .  | 224        |
| Responsible Disclosure . . . . .                                   | 224        |
| Vulnerability . . . . .  | 224        |
| Vulnerability Coordination . . . . .                               | 225        |
| Vulnerability Disclosure . . . . .                                 | 225        |

## CONTENTS

|   |            |
|---|------------|
| White Hat Hacker . . . . .                                  | 225        |
| <b>26. Appendix A - Take Aways . . . . .</b>                | <b>226</b> |
| Open Redirects . . . . .                                    | 226        |
| HTTP Parameter Pollution . . . . .                          | 227        |
| Cross Site Request Forgery . . . . .                        | 227        |
| HTML Injection . . . . .                                    | 228        |
| CRLF Injections . . . . .                                   | 229        |
| Cross-Site Scripting . . . . .                              | 229        |
| SSTI . . . . .  | 231        |
| SQL Injection . . . . .                                     | 232        |
| Server Side Request Forgery . . . . .                       | 232        |
| XML External Entity Vulnerability . . . . .                 | 233        |
| Remote Code Execution . . . . .                             | 234        |
| Memory . . . . .  | 235        |
| Sub Domain Takeover . . . . .                               | 236        |
| Race Conditions . . . . .                                   | 237        |
| Insecure Direct Object References . . . . .                 | 238        |
| OAuth . . . . .   | 239        |
| Application Logic Vulnerabilities . . . . .                 | 240        |
| <b>27. Appendix B - Web Hacking 101 Changelog . . . . .</b> | <b>242</b> |