

Easy wins

# Bug Bounty

## Playbook 2

Alex Thomas AKA Ghostlulz

## Exploitation

|                                            |           |
|--------------------------------------------|-----------|
| <b>Introduction</b>                        | <b>8</b>  |
| <b>Basic Hacking Known Vulnerabilities</b> | <b>11</b> |
| Introduction                               | 11        |
| Identifying technologies                   | 13        |
| Introduction                               | 13        |
| Wappalyzer                                 | 13        |
| Powered By                                 | 14        |
| Summary                                    | 15        |
| Identifying the vulnerabilities            | 16        |
| Introduction                               | 16        |
| Google                                     | 16        |
| ExploitDB                                  | 17        |
| CVE                                        | 19        |
| Summary                                    | 19        |
| Finding the POC                            | 20        |
| Introduction                               | 20        |
| Github                                     | 20        |
| ExploitDB                                  | 21        |
| Summary                                    | 21        |
| Exploitation                               | 22        |
| Conclusion                                 | 22        |
| <b>Basic Hacking CMS</b>                   | <b>23</b> |
| Introduction                               | 23        |
| Wordpress                                  | 24        |
| Drupal                                     | 26        |
| Joomla                                     | 26        |
| Adobe AEM                                  | 28        |
| Other                                      | 29        |
| Conclusion                                 | 31        |
| <b>Basic Hacking Github</b>                | <b>31</b> |
| Introduction                               | 31        |
| Finding Sensitive Information              | 32        |
| Conclusion                                 | 34        |
| <b>Basic Hacking Subdomain Takeover</b>    | <b>35</b> |
| Introduction                               | 35        |

|                                    |           |
|------------------------------------|-----------|
| Subdomain Takeover                 | 35        |
| Github Takeover                    | 37        |
| Conclusion                         | 43        |
| <b>Basic Hacking Databases</b>     | <b>44</b> |
| Introduction                       | 44        |
| Google Firebase                    | 45        |
| Introduction                       | 45        |
| Misconfigured Firebase Database    | 45        |
| Summary                            | 46        |
| ElasticSearch DB                   | 46        |
| Introduction                       | 46        |
| ElasticSearch Basics               | 47        |
| Unauthenticated ElasticSearch DB   | 48        |
| Summary                            | 53        |
| Mongo Database                     | 54        |
| Introduction                       | 54        |
| MongoDB                            | 54        |
| Summary                            | 55        |
| Conclusion                         | 55        |
| <b>Basic Hacking Brute Forcing</b> | <b>57</b> |
| Introduction                       | 57        |
| Login Pages                        | 57        |
| Default Credentials                | 58        |
| Brute Forcing                      | 60        |
| Conclusion                         | 60        |
| <b>Basic Hacking Burp Suite</b>    | <b>62</b> |
| Introduction                       | 62        |
| Proxy                              | 63        |
| Target                             | 69        |
| Intruder                           | 72        |
| Repeater                           | 78        |
| Conclusion                         | 79        |
| <b>Basic Hacking OWASP</b>         | <b>81</b> |
| Introduction                       | 81        |
| SQL Injection(SQLI)                | 82        |
| Introduction                       | 82        |

|                           |     |
|---------------------------|-----|
| MySql                     | 82  |
| Union Based Sql Injection | 84  |
| Error Based Sql Injection | 89  |
| Xpath                     | 89  |
| PostgreSql                | 92  |
| Union Based Sql Injection | 93  |
| Oracle                    | 97  |
| Union Based Sql Injection | 98  |
| Summary                   | 101 |
| Cross Site Scripting(XSS) | 102 |
| Introduction              | 102 |
| Reflected XSS             | 103 |
| Basic script alert        | 103 |
| Input Field               | 104 |
| Event Attributes          | 106 |
| Stored XSS                | 108 |
| DOM Based XSS             | 112 |
| Introduction              | 112 |
| Sources                   | 114 |
| Sinks                     | 115 |
| Polyglot                  | 117 |
| Beyond the alert box      | 118 |
| Cookie Stealer            | 118 |
| Summary                   | 120 |
| File Upload               | 120 |
| Introduction              | 121 |
| File Upload               | 121 |
| Content Type Bypass       | 124 |
| File Name Bypass          | 125 |
| Summary                   | 126 |
| Directory Traversal       | 126 |
| Introduction              | 126 |
| Directory Traversal       | 127 |
| Summary                   | 128 |
| Open Redirect             | 129 |
| Introduction              | 129 |
| Open Redirect             | 129 |
| Summary                   | 130 |

|                                           |            |
|-------------------------------------------|------------|
| Insecure Direct Object Reference(IDOR)    | 131        |
| Introduction                              | 131        |
| IDOR                                      | 131        |
| Summary                                   | 134        |
| Conclusion                                | 134        |
| <b>API Testing</b>                        | <b>135</b> |
| Introduction                              | 136        |
| APIs                                      | 137        |
| Rest API                                  | 137        |
| Remote Procedure Call (RPC)               | 142        |
| Simple Object Access Protocol (SOAP)      | 143        |
| GraphQL API                               | 146        |
| Authentication                            | 148        |
| HTTP Basic                                | 148        |
| Json Web Token (JWT)                      | 150        |
| Introduction                              | 150        |
| Deleted Signature                         | 153        |
| None Algorithm                            | 154        |
| Brute Force Secret Key                    | 155        |
| RSA to HMAC                               | 156        |
| Summary                                   | 158        |
| Security Assertion Markup Language (SAML) | 159        |
| Introduction                              | 159        |
| XML Signature Removal                     | 162        |
| XMLComment Injection                      | 166        |
| XML Signature Wrapping (XSW)              | 167        |
| XSW Attack 1                              | 168        |
| XSW Attack 2                              | 169        |
| XSW Attack 3                              | 171        |
| XSW Attack 4                              | 171        |
| XSW Attack 5                              | 172        |
| XSW Attack 6                              | 172        |
| XSW Attack 7                              | 173        |
| XSW Attack 8                              | 174        |
| API Documentation                         | 176        |
| Introduction                              | 176        |
| Swagger API                               | 176        |