



Contents

General Information	5
WHOIS Information.....	6
Domain Profiler	7
Same domains in other TLD zones (6).....	10
A Records (1).....	10
MX Records (2).....	10
NS Records (3).....	10
TXT Records (5)	11
SOA Records (1)	11
Map Domain/IP/Netblock Owner/Tech Apps & OS.....	11
Related Domains	14
Mail.XXXX.com mapping	17
Associated domains to mail.XXXX.com (21).....	17
Account on external sites – some are of “concerns” (6)	18
DNS entries concernerns (ALL except XXXX.com)	18
Public Code Repository (1).....	19
Spiderfoot Global mapping	19
Malicious IP on Same Subnet (3)	20
Cloud Storage Bucket (1).....	20
Malicious Affiliate IP Address (5)	20
DeHashed (1.226 results).....	20
Nmap Scan Report	21
OpenVAS (3 Medium – 1 Low)	25
OWASP (1 Medium / 10 Low / 6 Informational).....	106
Summary of Alerts.....	106
Alert Detail.....	106
NIKTO	150
Site Mgt Tech Info	150
Drupal Analysis (1 Issue)).....	150
Blacklists & Threat Intel	151
Drupal Modules.....	151
Drupal Theme.....	152
User Enumeration	152

Directory Indexing.....	152
PATH STATUS	153
Linked Sites	153
Linked Javascript	153
Pub IP	154
Page links extraction (40).....	154
Mail header analysis	155
Address Details 01.....	155
Message Details	155
Message Transfer Agent (MTA) - Transfer Details.....	155
Daily hit counter = 0 of 50.....	155
Spam Scoring Details.....	155
Hop Details.....	156
X-Header	158
Mail Header Details 02.....	161
Mail Header.....	173
URLcrazy (89 entries)	177
DNS Entries (88)	180
Email Addresses found (7 Breaches – 51 Domains – 42 Nodes).....	183
Hashes (5).....	207
Past Hashes (29).....	207
Certificates (100).....	208
Resolution (3).....	213
Subdomains (58) - RisqIQ.....	214
Tarckers (7)	216
Components (35)	217
HostPairs (23).....	218
OSINT search Engine (10).....	219
DNS (21)	220
Cookies (9).....	222
VT result	222
VT Hashes (22)	223
VT concerned entries / IP.....	224
ZoomEye	225
High-level ZE.....	279
ZE Vulnerabilities (11)	281
Nginx	281

BuiltWith	282
XXXX.COM Connected Websites (3)	293
Domains Redirecting to XXXX.COM (102 domains redirect to pages on XXXX.com).....	293
Domain Performance and Error Scan	297
1. IP-Addresses.....	297
2. DNSSEC.....	298
3. Name Servers	300
4. SOA-Entries	301
5. Screenshots.....	305
Mobile- and other Chrome-Checks.....	308
6. Url-Checks	308
7. Comments.....	310
8. Connections.....	319
9. Certificates	321
10. Last Certificates - Certificate Transparency Log Check	328
11. Html-Content - Entries	330
12. Nameserver - IP-Adresses	554
13. CAA - Entries.....	555
14. TXT - Entries	555
URL scan Results	557
IP/ASNs.....	557
Port 80 http Transactions	557
Redirect requests (79).....	566
JavaScript Global variables (29)	566
Security Headers	566
Indicators (89)	566
This is a term in the security industry to describe indicators such as IPs, Domains, Hashes, etc. This does not imply that any of these indicate malicious activity.....	566
DOM tree (Document Object Model)	568
Form Analysis (1 forms found in the DOM).....	610
Text Content.....	611
SSL Report	615
Server Key and Certificate #1.....	615
Additional Certificates (if supplied)	616
Certification Paths.....	617
Server Key and Certificate #1.....	617
Certification Paths.....	618
Configuration	619

Cipher Suites	619
Handshake Simulation	620
# Not simulated clients (Protocol mismatch).....	622
Protocol Details.....	623
HTTP Requests	625
Miscellaneous	625
Lampyre full Scan.....	626
Object attributes.....	627
Email: login.....	628
7 of 101	628
🔑 LinkedIn company ID	628
1 of 1	628
🔑 LinkedIn company screen name.....	628
1 of 1	628
🔑 LinkedIn company URL.....	628
1 of 1	628
👤 Credentials (20)	628
7 of 20	628
🕒 Date and time: day	629
7 of 7	629
🕒 Date and time: part.....	630
4 of 4	630
Objects and their links	630
Subdomains by domain via crt.sh - Search sub-domains	633
Company employees by domain - Company employees by domain (21 with prv. Adrs.).....	642
User Name - XXXX.com	643
Subdomains search by domain - Subdomains by domain	644
Threatcrowd search - Threatcrowd report	645
Mail Pwnd Report (788 pages).....	646
Hashes Analysis (216 pages)	647
L1 & L2 Domain analysis (2.993 pages).....	648