

Sri Lanka Institute of Information Technology




WEB SECURITY (IE2062)

BUG BOUNTY REPORT 3

Thilakarathna S.T.D- IT22578914

B.Sc. (Hons) in Information Technology Specializing in cyber
security

Overview of the website



Yelp
Connecting people to great local businesses in communities around the world.
<https://www.yelp.com>

Reports resolved
381

Assets in scope
9

Average bounty
\$300-\$500

[Submit report](#)
[Give feedback](#)

Bug Bounty Program
Launched in Sep 2016

Includes retesting ⓘ
Collaboration enabled ⓘ

[★ Bookmarked](#) [🔔 Subscribe](#)

Overview **Scope** Hacktivity Thanks Updates (1) Collaborators

Rewards

Last updated on September 21, 2022. [View changes](#)

Low	Medium	High	Critical
Avg. bounty \$381 40.87% submissions	Avg. bounty \$688 36.52% submissions	Avg. bounty \$992 18.26% submissions	Avg. bounty \$2,517 4.35% submissions
\$500-\$1,250	\$1,500-\$4,000	\$4,500-\$6,000	\$7,000-\$10,000

Response Efficiency

1 day, 21 hours
Average time to first response



















5 days, 19 hours
Average time from triage to bounty

5 days, 19 hours













One well-known website that is completely changing the way consumers find and evaluate businesses is Yelp.com. Yelp offers consumers a plethora of information to help them make wise judgments by acting as a thorough directory for nearby establishments, eateries, retail stores, and service providers. The website allows users to browse a wide range of local businesses, read customer reviews, see images, and discover important information like contact details and operating hours. Users are empowered by Yelp's review system to share their thoughts and experiences, assisting others in navigating the local business scene. Apart from its features aimed at consumers, Yelp provides tools and resources to business owners so they can handle their web presence, interact with clients, and reply to reviews. Yelp.com has become a vital resource for both customers and companies due to its user-friendly interface, strong review system, and dedication to transparency.

Scope

• InScope

542767785 Restaurant Manager iOS app	iOS: App Store	In scope	 Critical	 Eligible	Feb 11, 2020	4 (1%)
936983378 Yelp for Business Owners	iOS: App Store	In scope	 Critical	 Eligible	Feb 11, 2020	6 (2%)
284910350 Yelp Mobile	iOS: App Store	In scope	 Critical	 Eligible	Feb 11, 2020	4 (1%)
com.yelp.android Yelp Mobile for Android	Android: Play Store	In scope	 Critical	 Eligible	Feb 12, 2020	5 (1%)
com.yelp.android.biz Yelp for Business Owners	Android: Play Store	In scope	 Critical	 Eligible	Feb 12, 2020	3 (1%)
*.yelp.com	Wildcard	In scope	 Critical	 Eligible	May 15, 2023	85 (22%)
*.yelp-support.com	Wildcard	In scope	 High	 Eligible	May 15, 2023	4 (1%)
*.yelpwifi.com	Wildcard	In scope	 Low	 Eligible	May 15, 2023	3 (1%)
yelptop100.com	Domain	In scope	 Low	 Eligible	Sep 30, 2022	0 (0%)

• OutScope

engineeringblog.yelp.com	Domain	Out of scope	 None	 Ineligible	Feb 14, 2020	0 (0%)
blog.yelp.com	Domain	Out of scope	 None	 Ineligible	Sep 20, 2022	0 (0%)
www.yelp-ir.com	Domain	Out of scope	 None	 Ineligible	Feb 14, 2020	0 (0%)
cloud.e.yelp-business.com This is a product provided by Salesforce. Please report bugs to the Salesforce Security Team https://www.salesforce.com/company/disclosure/	Domain	Out of scope	 None	 Ineligible	Feb 14, 2020	0 (0%)
yelp-press.com	Domain	Out of scope	 None	 Ineligible	Sep 20, 2022	0 (0%)
yelp.careers	Domain	Out of scope	 None	 Ineligible	Sep 20, 2022	0 (0%)

Information Gathering

Security researchers and ethical hackers must first gather data through bug bounty programs in order to identify vulnerabilities in a target system or application. This step's objective is to learn as much as you can about the target, including its technologies, architecture, known vulnerabilities, and potential weak points. Open-source intelligence gathering (OSINT), network scanning, fingerprinting, and asset enumeration are typically required to give a complete view of the target's attack surface.

Since it enables ethical hackers to identify potential points of entry and focus their search for system security flaws, efficient information gathering is the cornerstone of a successful bug hunting operation.

Subdomains for Hunting

The process of listing sub-domains for one or more domains is called sub-domain enumeration. This is a critical stage in the reconnaissance process. Finding vulnerabilities is made more likely by sub-domain enumeration, which can identify several domains and sub-domains that are part of a security assessment.

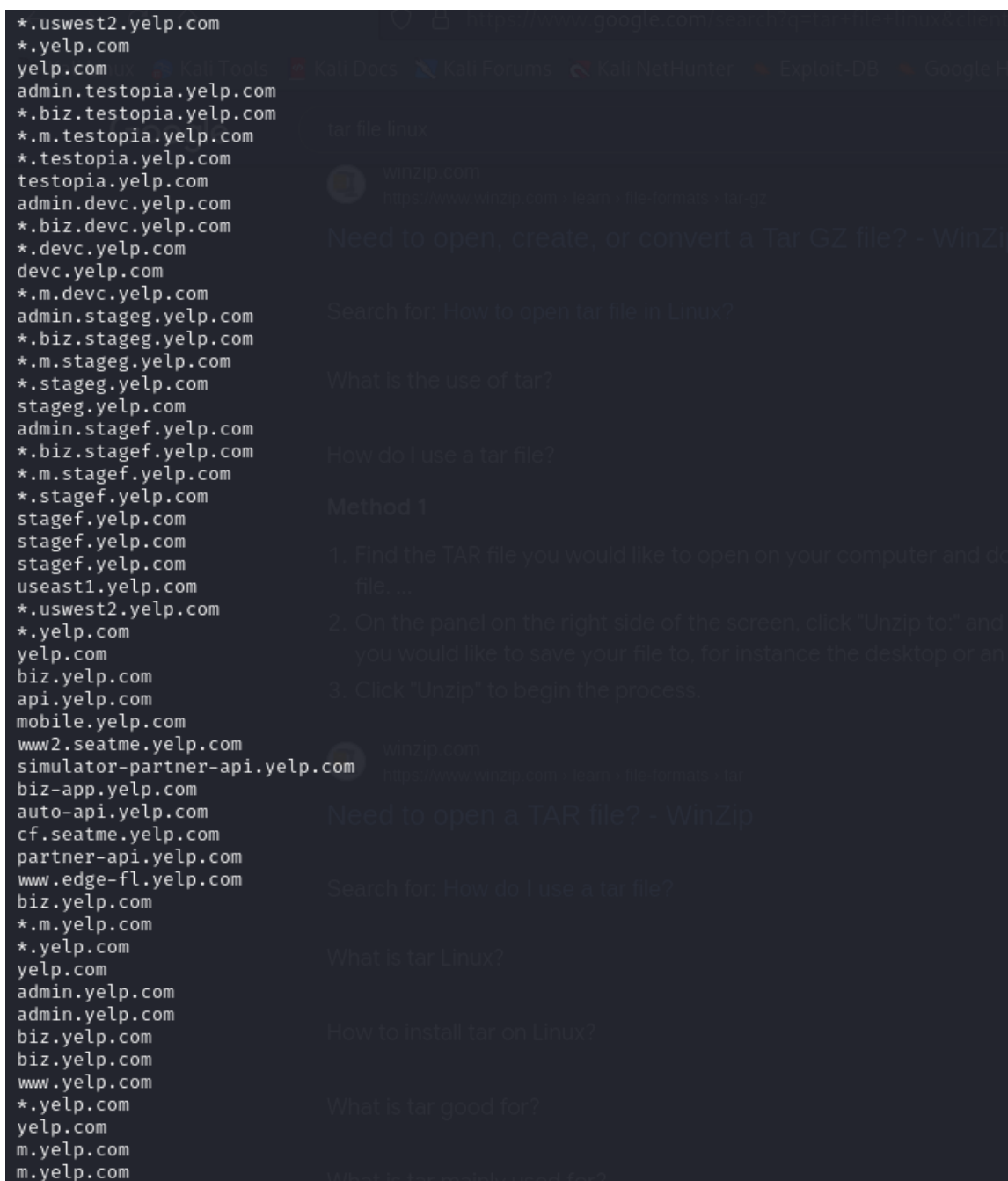
Seen through cryptic, abandoned sub-domains, programs may have dangerous bugs.

The same weaknesses are frequently found throughout numerous domains and applications within a single organization.

- **Assetfinder**

A program called Assetfinder is mainly meant for penetration testers and cybersecurity experts to detect and count domains and subdomains connected to a certain target domain. Its primary purpose is to list subdomains, but that is not all that important. Each subdomain that is found may be an application, a component of an organization's infrastructure, or even unrecognized online assets that are open to intrusions.

```
(tharusha@kali)-[~]
$ assetfinder --subs-only yelp.com
www.yelp.com
m.yelp.com
docs.developer.yelp.com
yelp.com
business.yelp.com
tacotrailblazer.yelp.com
data.yelp.com
proze.yelp.com
brands-email.yelp.com
trust.yelp.com
cameraeatsfirst.yelp.com
static.px.yelp.com
status.developer.yelp.com
images.yelp.com
s.yelp.com
seatme.yelp.com
seatme.yelp.com
chiefpizzaofficer.yelp.com
terms.yelp.com
groove.yelp.com
clicks.yelp.com
static.seatme.yelp.com
info.biz.yelp.com
admin.yelp.com
admin.yelp.com
*.biz.yelp.com
*.m.yelp.com
*.yelp.com
yelp.com
blog.yelp.com
mail.yelp.com
yelp.com
imageoptbackend.yelp.com
snapscalebackend.yelp.com
admin.stageg.yelp.com
*.biz.stageg.yelp.com
*.business.stageg.yelp.com
*.m.stageg.yelp.com
*.stageg.yelp.com
stageg.yelp.com
admin.devc.yelp.com
*.biz.devc.yelp.com
*.business.devc.yelp.com
*.devc.yelp.com
devc.yelp.com
*.m.devc.yelp.com
admin.stagef.yelp.com
*.biz.stagef.yelp.com
*.business.stagef.yelp.com
*.m.stagef.yelp.com
```

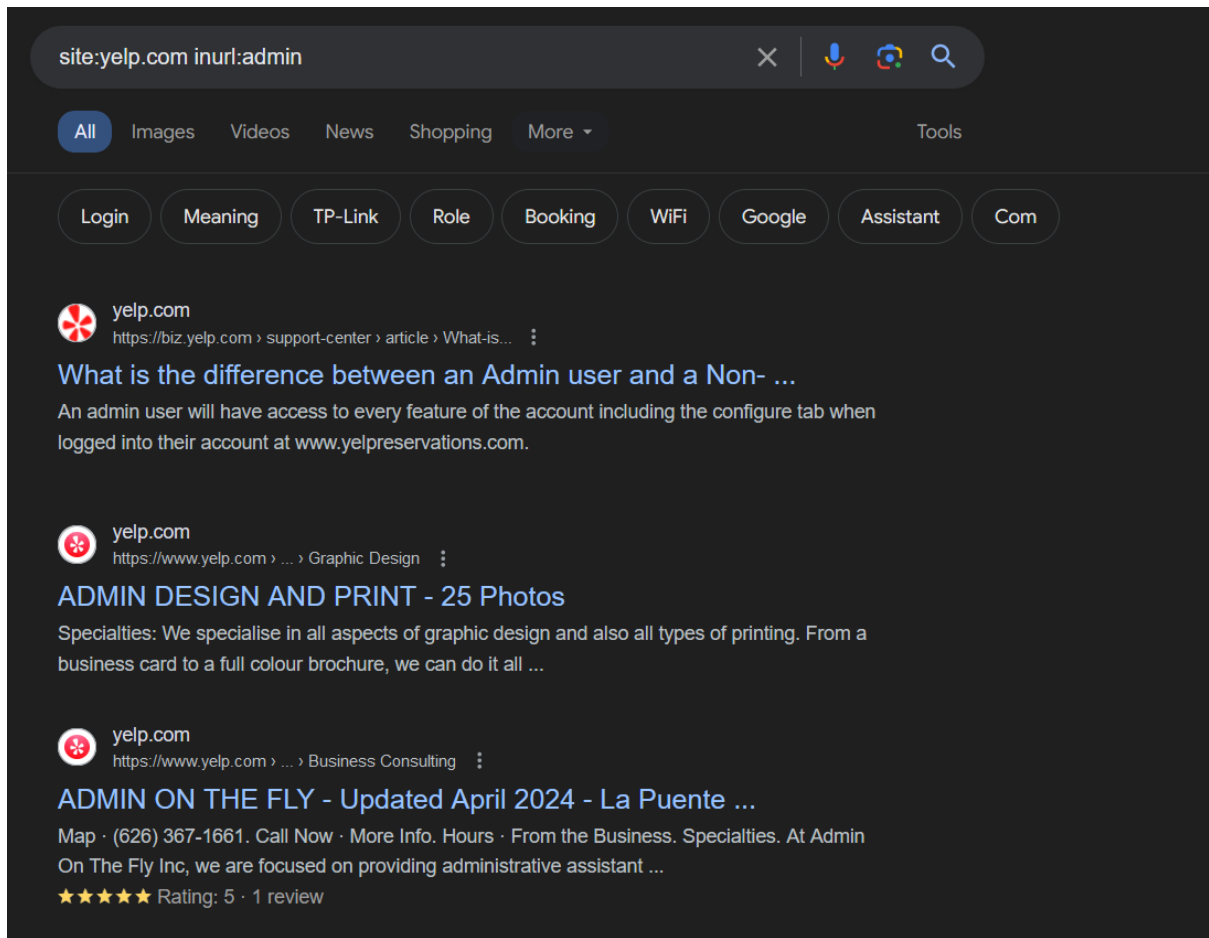


- **Google Dorking**

Use this search method to help the search engine find sensitive and significant website information.

Site refers to the request that Google show only results from a particular website. By doing this, you'll be able to find the most trustworthy source on the topic with ease.

Inurl: This is a good way to identify vulnerable pages on a particular domain. For example, we can look for login, admin, email, password, etc. It will provide us with sensitive data.











































- **Dnsdumpster**

Block addresses, emails, domain names, and other kinds of DNS-related data can be gathered using an online passive scanning tool called DNSdumpster.
















Result of yelp.com

dns recon & research, find & lookup dns records

DNS Servers

dns1.p06.nsonline.net.	198.51.44.6	NSONE United States	    
dns2.p06.nsonline.net.	198.51.45.6	NSONE United States	    
dns3.p06.nsonline.net.	198.51.44.70	NSONE United States	    
dns4.p06.nsonline.net.	198.51.45.70	NSONE United States	    
ns01.midtowndoornailns.com.	45.54.54.1	NETACTUATE-AS-AP NetActuate, Inc United States	    
ns02.midtowndoornailns.com.	45.54.54.65	NETACTUATE-AS-AP NetActuate, Inc United States	    
ns03.midtowndoornailns.com.	45.54.54.129	NETACTUATE-AS-AP NetActuate, Inc United States	    
ns04.midtowndoornailns.com.	45.54.54.193	NETACTUATE-AS-AP NetActuate, Inc United States	    

MX Records ** This is where email for the domain goes...

1 aspmx.l.google.com.	172.253.115.26	GOOGLE United States	  
10 alt4.aspmx.l.google.com.	142.250.153.26	GOOGLE United States	  
5 alt1.aspmx.l.google.com.	209.85.202.26	GOOGLE United States	  
5 alt2.aspmx.l.google.com.	64.233.184.27	GOOGLE United States	  
10 alt3.aspmx.l.google.com.	142.250.27.27	GOOGLE United States	  


```
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations

"pardot813133=a90e85640d4bb5a429d171325168640bb9463489071367d9615ebc73919f1bbb"
"citrix-verification-code=1dee59ff-c292-47a1-8faf-a0c7803c742a"
"v=spf1 include:yelp.com._nsfp.vali.email include:%{1}._ip.%{h}._ehlo.%{d}._spf.vali.email ~all"
"google-site-verification=40znISzbXHzmhzRM-NtpUcP1P6nIfsanNZdNI1G_EU8"
"google-site-verification=-Y773kzVn1DQ1VG-Ugprk7qDuZdk1_5cqljezw1daiU"
"status-page-domain-verification=kl0pq45qyb3d"
"gm36n17d8y8544hg7s3n5ptcjgzfb17f"
"status-page-domain-verification=z80f59yz1jkt"
"wrike-verification=NDA1MDgyNTp1MDcyYWNmMjgyYmEzOWFhNDE3NzA1YTE1NGFmYmYzYmU0Y2IxNGQwNTA5YzNkMDIyNWVhYmNhZDMwZmQ5ZTM1"
"apple-domain-verification=qa3GTY5z2ELxESie"
"mixpanel-domain-verify=277018fd-af0f-4112-bc98-ec0aa09c9e62"
"google-site-verification=6RQLNPjWLxGr_Ka6phLFqBXooCAZt35ZZz2ZV5JNsDQ"
"google-site-verification=-LX_luQh_Kq5PPMW-YLB6Ar22sLmB9uXTZDZYwWdWcc"
"_globalsign-domain-verification=P095qR5HARP3zbvcQ1WFBVylG8Uvgjmgc16ENjCtmy"
"google-site-verification=3lJN-zw-10jb4bLfMxSqFizDALMsnlhqZ-TPG-AjHWU"
"google-site-verification=NOSls2JfXI55tW5qFU89NY93kA8LB6YTHGBzCFz3cy8"
"google-site-verification=-RmG1SGbhN1-Y0wwdYV16f4DBPxThfIARwe8ZDVvbe"
"status-page-domain-verification=f3txhd81xn94"
"facebook-domain-verification=mdu6515tt8odq7akwzr4a036q6w3cz"
"atlassian-domain-verification=45ozypIxFMV4A0xxbgkqTjhHaKzj8CrxbzUxbakhomBdkM6bzt1170BkFPJl1bAX"
"_globalsign-domain-verification=_64UG15h1zSn86m51pRb3vaFMDTtUCsP2RBUJ7DAAM"
"onetrust-domain-verification=53afac8ba50845c3b7c8ba137d2349c0"
```

- **DNSrecon**

For DNS enumeration and reconnaissance, an open-source tool named DNSRecon is utilized. The purpose of gathering information is to assist with penetration testing and security evaluations by providing details on DNS servers, domains, subdomains, and DNS records.

```
(tharusha@kali)-[~]
$ dnsrecon -d yelp.com
[*] std: Performing General Enumeration against: yelp.com...
[*] Wildcard resolution is enabled on this domain
[*] It is resolving to yelpcdn.map.fastly.net
[*] It is resolving to 199.232.44.116
[*] All queries will resolve to this list of addresses!!
[-] DNSSEC is not configured for yelp.com
[*] SOA dns1.p06.nsonone.net 198.51.44.6
[*] SOA dns1.p06.nsonone.net 2620:4d:4000:6259:7:6:0:1
[*] NS ns02.midtowndoornailns.com 45.54.54.65
[*] Bind Version for 45.54.54.65 "a0bd971e3"
[*] NS dns3.p06.nsonone.net 198.51.44.70
[*] Bind Version for 198.51.44.70 "a0bd971e3"
[*] NS dns3.p06.nsonone.net 2620:4d:4000:6259:7:6:0:3
[*] NS dns4.p06.nsonone.net 198.51.45.70
[*] Bind Version for 198.51.45.70 "a0bd971e3"
[*] NS dns4.p06.nsonone.net 2a00:edc0:6259:7:6::4
[*] NS ns03.midtowndoornailns.com 45.54.54.129
[*] Bind Version for 45.54.54.129 "a0bd971e3"
[*] NS dns1.p06.nsonone.net 198.51.44.6
[*] Bind Version for 198.51.44.6 "a0bd971e3"
[*] NS dns1.p06.nsonone.net 2620:4d:4000:6259:7:6:0:1
[*] NS dns2.p06.nsonone.net 198.51.45.6
[*] Bind Version for 198.51.45.6 "a0bd971e3"
[*] NS dns2.p06.nsonone.net 2a00:edc0:6259:7:6::2
[*] NS ns04.midtowndoornailns.com 45.54.54.193
[*] Bind Version for 45.54.54.193 "a0bd971e3"
[*] NS ns01.midtowndoornailns.com 45.54.54.1
[*] Bind Version for 45.54.54.1 "a0bd971e3"
[*] NS ns01.midtowndoornailns.com 64:ff9b::2d36:3601
[*] MX alt1.aspmx.l.google.com 173.194.202.27
[*] MX alt4.aspmx.l.google.com 64.233.171.27
[*] MX aspmx.l.google.com 142.251.12.26
[*] MX alt2.aspmx.l.google.com 142.250.141.26
[*] MX alt3.aspmx.l.google.com 142.250.115.26
[*] MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1b
[*] MX alt4.aspmx.l.google.com 2607:f8b0:4003:c15::1a
[*] MX aspmx.l.google.com 2404:6800:4003:c11::1b
[*] MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*] MX alt3.aspmx.l.google.com 2607:f8b0:4023:1004::1b
[*] A yelp.com 199.232.80.116
[*] TXT _dmarc.yelp.com v=DMARC1; p=reject; rua=mailto:dmarc_agg@vali.email,mailto:dmarc@yelp.com; ruf=mailto:dmarc_fr@yelp.com; ri=14400
[*] Enumerating SRV Records
[-] No SRV Records Found for yelp.com
```

- **WHOIS**

Domain names, IP addresses, and autonomous system numbers (ASNs) can all be found via a database system or a protocol, respectively. It provides information, such as contact details, about the owner of a block of IP addresses or the person who registered a domain name.

```

(tharusha@kali)-[~]
$ whois yelp.com
Domain Name: YELP.COM
Registry Domain ID: 108150885_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-11-10T09:39:15Z
Creation Date: 2003-12-12T21:24:56Z
Registry Expiry Date: 2025-12-12T21:24:56Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Name Server: DNS1.P06.NSONE.NET
Name Server: DNS2.P06.NSONE.NET
Name Server: DNS3.P06.NSONE.NET
Name Server: DNS4.P06.NSONE.NET
Name Server: NS01.MIDTOWNDOORNAILNS.COM
Name Server: NS02.MIDTOWNDOORNAILNS.COM
Name Server: NS03.MIDTOWNDOORNAILNS.COM
Name Server: NS04.MIDTOWNDOORNAILNS.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: yelp.com
Registry Domain ID: 108150885_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2023-11-10T09:39:15+0000
Creation Date: 2003-12-12T21:24:56+0000
Registrar Registration Expiration Date: 2025-12-12T00:00:00+0000
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientUpdateProhibited (https://www.icann.org/epp#clientUpdateProhibited)
Domain Status: clientTransferProhibited (https://www.icann.org/epp#clientTransferProhibited)
Domain Status: clientDeleteProhibited (https://www.icann.org/epp#clientDeleteProhibited)
Registrant Organization: Yelp Inc.
Registrant State/Province: CA
Registrant Country: US
Registrant Email: Select Request Email Form at https://domains.markmonitor.com/whois/yelp.com
Admin Organization: Yelp Inc.
Admin State/Province: CA
Admin Country: US
Admin Email: Select Request Email Form at https://domains.markmonitor.com/whois/yelp.com
Tech Organization: Yelp Inc.
Tech State/Province: CA
Tech Country: US
Tech Email: Select Request Email Form at https://domains.markmonitor.com/whois/yelp.com
Name Server: ns02.midtowndoornailns.com
Name Server: ns01.midtowndoornailns.com
Name Server: dns2.p06.nsone.net
Name Server: dns1.p06.nsone.net
Name Server: ns03.midtowndoornailns.com
Name Server: dns3.p06.nsone.net
Name Server: dns4.p06.nsone.net
Name Server: ns04.midtowndoornailns.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-05-09T20:09:55+0000 <<<

```

- **Using nmap, open port enumeration**

Open port enumeration is a method for locating and classifying the open network ports on a target machine or network using the Nmap (Network Mapper) program. Nmap is an effective open-source tool for network scanning and host discovery that provides extensive information on the services and statuses that are running on various ports. This process involves sending specially made packets to a target system and analyzing the responses in order to determine which ports are open and what services are using them.

Nmap is a popular tool for network administrators and security specialists to assess system security, identify potential security flaws, and enhance network configurations due to its abundance of features and versatility. It's a helpful tool for enhancing security and computer network administration in general.

```
(tharusha@kali)~  
$ sudo nmap -sS yelp.com  
[sudo] password for tharusha:  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 16:22 EDT  
Nmap scan report for yelp.com (146.75.72.116)  
Host is up (0.022s latency).  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
25/tcp    open  smtp  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 9.03 seconds  
  
(tharusha@kali)~  
$ sudo nmap --script vuln yelp.com  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-09 16:23 EDT  
Nmap scan report for yelp.com (199.232.56.116)  
Host is up (0.026s latency).  
Other addresses for yelp.com (not scanned): 64:ff9b::c7e8:3874  
Not shown: 997 filtered tcp ports (no-response)  
PORT      STATE SERVICE  
25/tcp    open  smtp  
80/tcp    open  http  
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)  
|_http-csrf: Couldn't find any CSRF vulnerabilities.  
|_http-dombased-xss: Couldn't find any DOM based XSS.  
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)  
443/tcp   open  https  
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.  
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)  
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)  
|_http-dombased-xss: Couldn't find any DOM based XSS.  
|_http-csrf:  
| Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=yelp.com  
| Found the following possible CSRF vulnerabilities:  
|  
| Path: http://yelp.com:443/  
| Form id:  
|_ Form action: https://www.yelp.com/search  
  
Nmap done: 1 IP address (1 host up) scanned in 209.04 seconds
```

- **Using Nikto to scan for vulnerabilities**

One method to check for vulnerabilities in Kali Linux is to use the powerful open-source tool Nikto web scanner, which is part of the popular operating system for penetration testing and ethical hacking. Nikto is specifically designed to identify and assess server and web application vulnerabilities.

When checking target web servers for known vulnerabilities, common security issues, and misconfigurations, Nikto can be used from the Kali Linux command line. Nikto searches for issues including outdated software, possibly unsafe scripts, security headers, and other online vulnerabilities. It helps ethical hackers and security professionals understand and reduce such threats by providing comprehensive information on the vulnerabilities discovered.

```
(tharusha@kali)-[~]
└─$ sudo nikto -h yelp.com
- Nikto v2.5.0

+ Target IP: 199.232.80.116
+ Target Hostname: yelp.com
+ Target Port: 80
+ Start Time: 2024-05-09 16:27:36 (GMT-4)

+ Server: Varnish
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-mrs1050090-MRS.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Fastly CDN was identified by the x-timer header. See: https://www.fastly.com/
+ /: Uncommon header 'x-served-by' found, with contents: cache-mrs1050090-MRS.
+ /: An alt-svc header was found which is advertising HTTP/3. The endpoint is: ':443'. Nikto cannot test HTTP/3 over QUIC. See: https://developer.mozilla.org/
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
sing-content-type-header/
+ Root page / redirects to: https://yelp.com/
^C

(tharusha@kali)-[~]
└─$ sudo nikto -h 199.232.80.116
- Nikto v2.5.0

+ Target IP: 199.232.80.116
+ Target Hostname: 199.232.80.116
+ Target Port: 80
+ Start Time: 2024-05-09 16:28:02 (GMT-4)

+ Server: Varnish
+ /: Retrieved via header: 1.1 varnish.
+ /: Retrieved x-served-by header: cache-mrs10579-MRS.
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ /: Uncommon header 'x-served-by' found, with contents: cache-mrs10579-MRS.
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type.
sing-content-type-header/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
```

Exploitation

I employed SQLMAP tool to identify SQL injection vulnerabilities in the target web application for the exploitations.

- **SQLmap**

An open-source penetration testing tool called SQL Map automatically locates and takes advantage of SQL injection vulnerabilities to take over databases.

In an attempt to locate any web application injection points, I experimented with various payloads and parameters. I tested this application and discovered that it is not injectable.


```
(tharusha@kali)~/PwnXSS
$ sqlmap -u https://www.yelp.com/biz/kenneth-asire-plumbing-san-francisco-3?osq=Plumbers'

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws.
responsible for any misuse or damage caused by this program

[*] starting @ 06:59:26 /2024-05-10/

[06:59:27] [INFO] testing connection to the target URL
[06:59:27] [WARNING] the web server responded with an HTTP error code (503) which could interfere with the results of the tests
[06:59:27] [INFO] checking if the target URL is protected by some kind of WAF/IPS
[06:59:28] [INFO] testing if the target URL content is stable
[06:59:28] [INFO] target URL content is stable
[06:59:28] [INFO] testing if GET parameter 'osq' is dynamic
[06:59:29] [WARNING] GET parameter 'osq' does not appear to be dynamic
[06:59:29] [WARNING] heuristic (basic) test shows that GET parameter 'osq' might not be injectable
[06:59:30] [INFO] testing for SQL injection on GET parameter 'osq'
[06:59:30] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[06:59:32] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[06:59:32] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[06:59:34] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[06:59:36] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[06:59:37] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[06:59:39] [INFO] testing 'Generic inline queries'
[06:59:40] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[06:59:41] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[06:59:43] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[06:59:44] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[06:59:46] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[06:59:48] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[06:59:51] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[07:00:14] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[07:00:18] [WARNING] GET parameter 'osq' does not seem to be injectable
[07:00:18] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. Please retry with the swi
as this case looks like a perfect candidate (low textual content along with inability of comparison engine to detect at least one dynamic parameter). If you suspect that there is some kind
aybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[07:00:18] [WARNING] HTTP error codes detected during run:
503 (Service Unavailable) - 79 times


[*] ending @ 07:00:18 /2024-05-10/
```

Vulnerabilities detect when Scanning

In order to process and find problems and vulnerabilities that are based on the OWASP top 10, I used tool like OWASP ZAP.

OWASP ZAP is a testing tool that may be used to identify potential security gaps in internet applications. OWASP ZAP can be used to find common vulnerabilities such as SQL injection and cross-site scripting (XSS).

1. Vulnerability Title

 Edit Alert

PII Disclosure

URL: https://www.yelp.com/search?find_desc=Phone+Repair&find_loc=San+Francisco%2C+CA

Risk: High

Confidence: High

Parameter:

Attack:

Evidence: 560574010212922

CWE ID: 359

WASC ID: 13

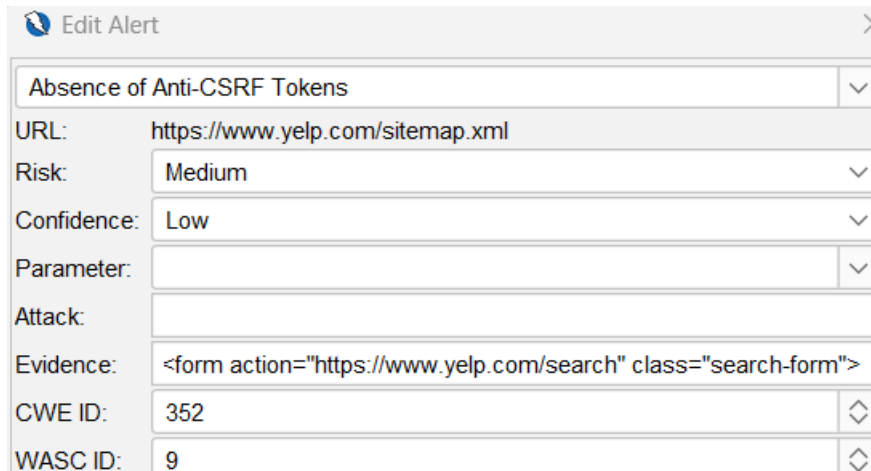
Vulnerability Description

The response contains Personally Identifiable Information, such as CC number, SSN and similar sensitive data.

How to mitigate

Check the response for the potential presence of personally identifiable information (PII), ensure nothing sensitive is leaked by the application.

2. Vulnerability Title



Edit Alert	
Absence of Anti-CSRF Tokens	
URL:	https://www.yelp.com/sitemap.xml
Risk:	Medium
Confidence:	Low
Parameter:	
Attack:	
Evidence:	<form action="https://www.yelp.com/search" class="search-form">
CWE ID:	352
WASC ID:	9

Vulnerability Description

No Anti-CSRF tokens were found in a HTML submission form.

A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf.

CSRF attacks are effective in a number of situations, including:

- * The victim has an active session on the target site.
- * The victim is authenticated via HTTP auth on the target site.
- * The victim is on the same local network as the target site.

CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the

target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.

How to mitigate

Phase: Architecture and Design

- Use a vetted library or framework that does not allow this weakness to occur or provides constructs that make this weakness easier to avoid.

For example, use anti-CSRF packages such as the OWASP CSRFGuard.

Phase: Architecture and Design

- Generate a unique nonce for each form, place the nonce into the form, and verify the nonce upon receipt of the form. Be sure that the nonce is not predictable (CWE-330). Note that this can be bypassed using XSS.
- Identify especially dangerous operations. When the user performs a dangerous operation, send a separate confirmation request to ensure that the user intended to perform that operation. Note that this can be bypassed using XSS.
- Use the ESAPI Session Management control. This control includes a component for CSRF.
- Do not use the GET method for any request that triggers a state change.

Phase: Implementation

- Ensure that your application is free of cross-site scripting issues, because most CSRF defenses can be bypassed using attacker-controlled script.
- Check the HTTP Referer header to see if the request originated from an expected page. This could break legitimate functionality, because users or proxies may have disabled sending the Referer for privacy reasons.

3. Vulnerability Title

Edit Alert		✕
Content Security Policy (CSP) Header Not Set		
URL:	https://www.yelp.com/sitemap.xml	
Risk:	Medium	
Confidence:	High	
Parameter:		
Attack:		
Evidence:		
CWE ID:	693	⬇
WASC ID:	15	⬇

Vulnerability Description

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

How to mitigate

Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header.