Sri Lanka Institute of Information Technology

WEB SECURITY (IE2062)

BUG BOUNTY ASSIGNMENT

Submitted by:

Student Registration Number	Student Name
IT20613518	Madhusanka D.N.V

Acknowledgement

I would like to give my thank to Dr. Lakmal Rupasinghe, Ms. Chethana Liyanapathirana, and Ms. Menaka Moonamaldeniya for gave us guidance and knowledge during this bug bounty assignment.

Purpose

The main purpose of a bug bounty is to uncover vulnerabilities in products, systems, and websites and to help protect users by making products, systems, and websites more secure. In recent years, bug bounty programs have become a standard way to find vulnerabilities in products, systems, and websites. They have helped companies to find and fix vulnerabilities in their products, systems, and websites faster, reducing the impact of vulnerabilities on users, and have helped improve the security of their products, systems, and websites. Bug bounty programs have also helped companies build a more secure ecosystem by helping them build a closer relationship with their users and the broader security community.

Introduction

Information Security

Information security is one of the most difficult issues facing businesses today. Whether you're a tiny business or a major corporation, you need to know what information security means to you, where your existing procedures fall short, and how you may strengthen your security posture.

Web Security

For businesses of all sizes, web security is a constant concern thing. New attacks and weaknesses are found on a regular basis, and new technologies and approaches are employed to circumvent existing defenses. As attackers refine their strategies and employ new tools and methods to target your users and steal sensitive data, the threat landscape shifts. There has never been a more pressing need for a flexible and adaptable security program.

Web Audit

The process of examining a website's technical performance, quality, and design is known as a web audit. It is a best practice for locating, documenting, and resolving website issues. A web audit is a continuous process that includes the following steps: data collection, issue identification, and problem-solving recommendations. Data collection entails acquiring data from a range of sources, including analytics and user experience tests.

OWASP Top Ten Security Risks in 2021

1. Weak Access Control.
2. Cryptographic Errors
3. Injection.
4. Design that is insecure.
5. Misconfiguration of security.
6. Components that are vulnerable and out of date.
7. Failures in identification and authentication.
8. Failures in software and data integrity.
9. Breakdowns in security monitoring and logging.
10. Forgery on the server side is number ten.

Bug Bounty

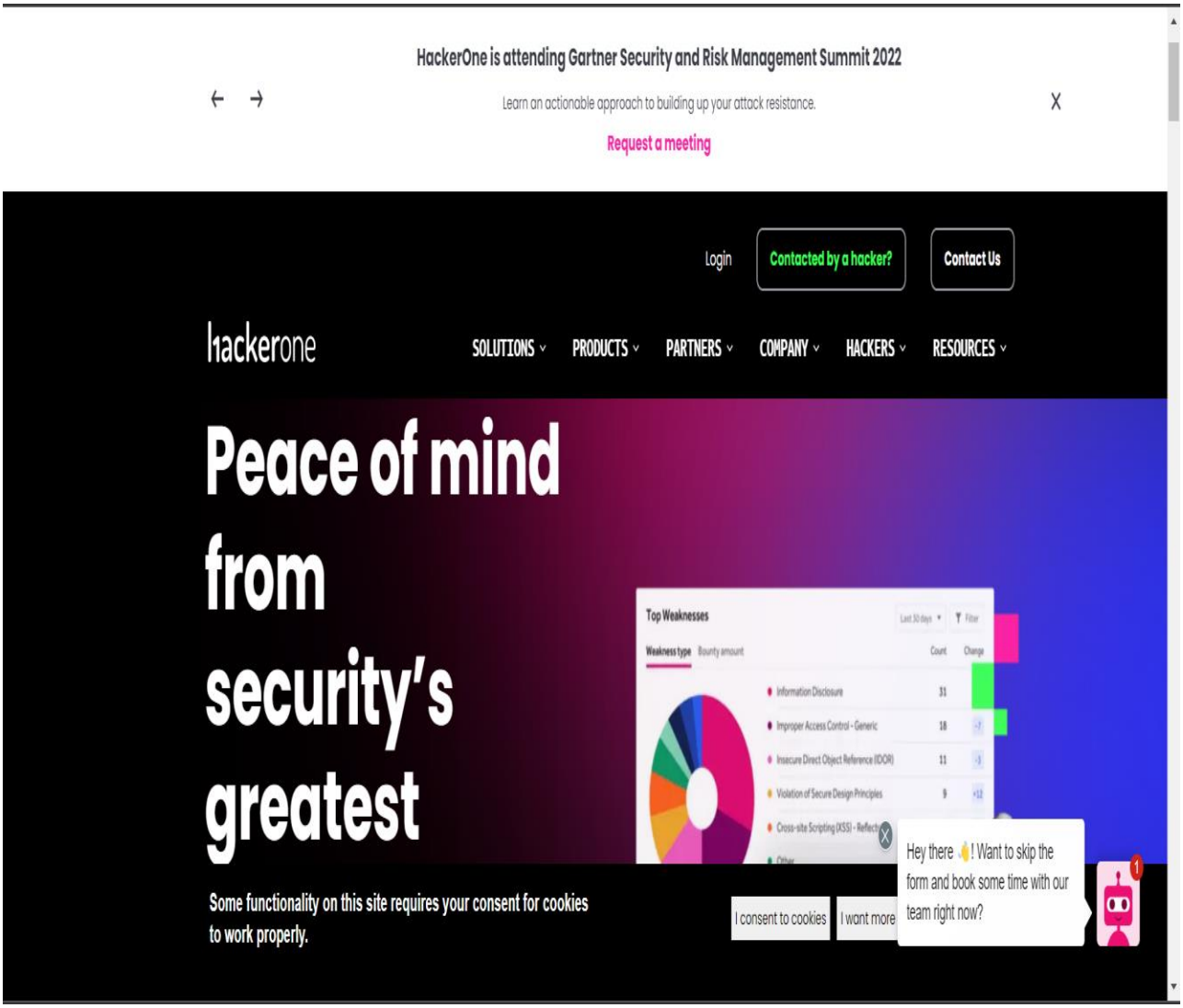
Bug bounty is a program designed to pay bug hunters for finding vulnerabilities in web products and services. The program is designed to help organizations to keep their users and their data safe, and it has been incredibly successful in bringing critical security improvements to web applications. Bug hunters who discover vulnerabilities in web products can earn bounty for reporting bugs with additional awards for complex and critical bugs.

Bug Bounty Platforms

To begin a site audit, we must first locate a bug bounty program. As a result, there are a plethora of well-known bug bounty sites. Hackerone, Bugcrowd, Facebook, SafeHats, Google, Yahoo, and others are among them. For my audit, I used programs from the Hackerone platform.

Hackerone

Hackerone is a tech firm that helps companies find bug bounty programs and hackers. It debuted in March of this year. Hackerone has helped many companies to secure their website. Bug bounty schemes are another area where Hackerone may help businesses. The company's creator and CEO, Jose Diaz-Gonzalez, has raised $2.5 million in funding.



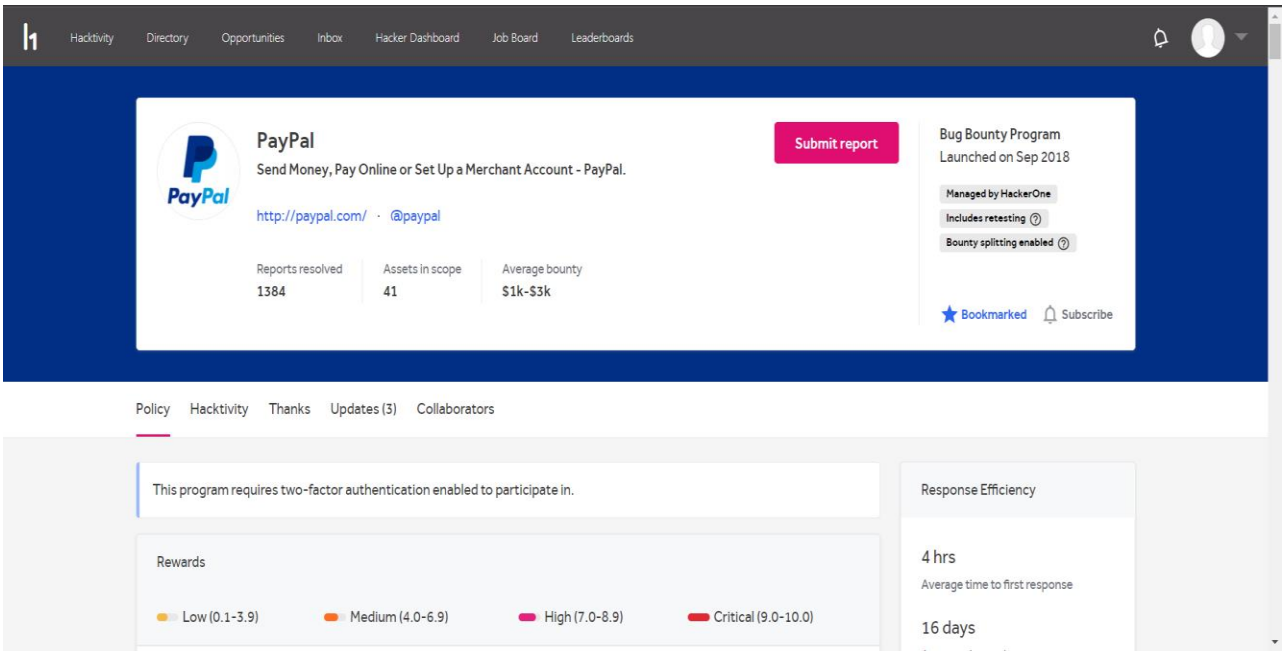
We need to create an account as a hacker and login to it. Then we can see programs in there.

Program selection

We need to choose a program that uses something that we are familiar with. Larger scope is better because the researchers will not concentrate on the same targets and some things might be overlooked.

I chose “PayPal” bug bounty program because this program has large scope with bounties. You can see the program in here.

https://hackerone.com/paypal?type=team



About “PayPal”

PayPal is a safe and secure e-commerce payment mechanism. PayPal is a safe and reliable payment network for online transactions, digital currency transactions, small businesses, and large corporations. They now handle payments for over 300,000 online businesses and 21 million online customers. PayPal is the most popular method of online payment, with 1.5 billion users and over 200 million active accounts. PayPal's success has been credited to its widespread use across several industries and millions of consumers worldwide.

Policy

Hackerone has disclosure guidelines for hackers about programs. You can refer it using disclosure guidelines link.

Scope

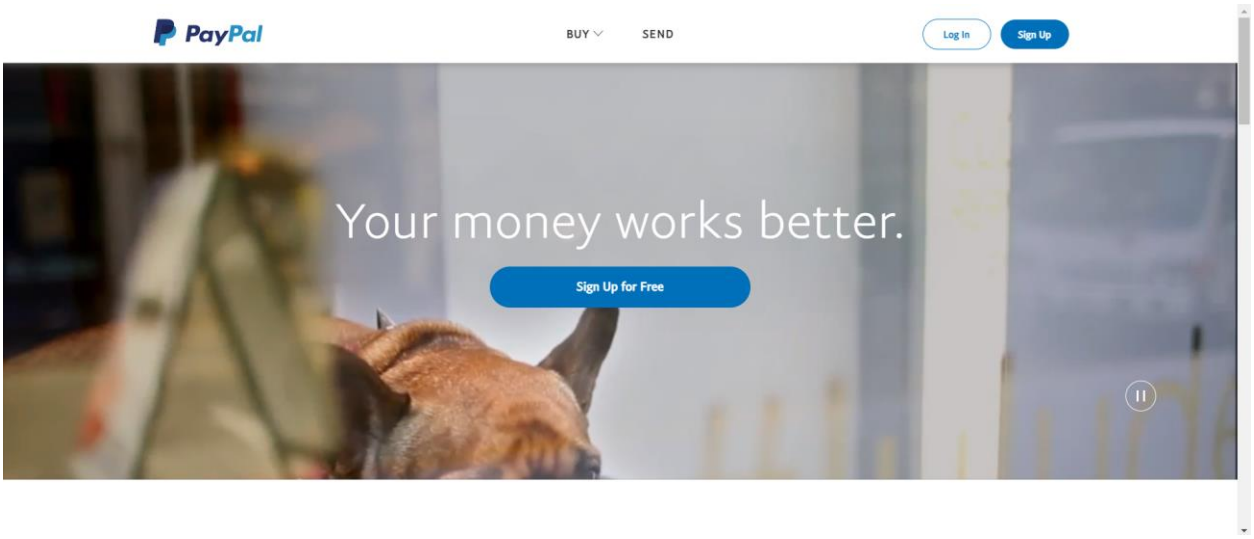
Scope is a collection of assets that hackers need to hack on. When assets are listed, hackers are required to select the applicable asset for each report.

Scopes			
In Scope			
Domain	**www.paypal-*.com** PayPal's Partner Sites (www.paypal-__.com) are mainly marketing based sites that are not part of the core PayPal customer domains (.paypal.com) and are managed by hosting vendor companies. They have variable timelines and are often decommissioned. A listing of these sites designated for deprecation will not be publically maintained due to frequent changes. When researching bugs on these sites, please keep this in mind as bug Submissions for sites on schedule for deprecation will not be honored. Submissions of bugs relating to services or domains not referenced above or for sites on schedule for deprecation are ineligible for the Bug Bounty Program and will not be eligible for a Bounty Payment.	Critical	Eligible
Domain	***.xoom.com**	Critical	Eligible
Domain	***.paypal.com**	Critical	Eligible
Domain	***.braintreegateway.com** For testing and account creation, please use *.sandbox.braintreegateway.com rather than production.	Critical	Eligible
Domain	***.paydiant.com**	Critical	Eligible
Domain	***.venmo.com**	Critical	Eligible
Domain	**paypalobjects.com**	Critical	Eligible
Domain	**paypal.me**	Critical	Eligible
Domain	**py.pl**	Critical	Eligible
Domain	***.braintreepayments.com** For testing and account creation, please use *.sand.braintreepayments.com rather than production.	Critical	Eligible
Domain	***.braintree-api.com** For testing and account creation, please use *.sandbox.braintree-api.com rather than production.	Critical	Eligible

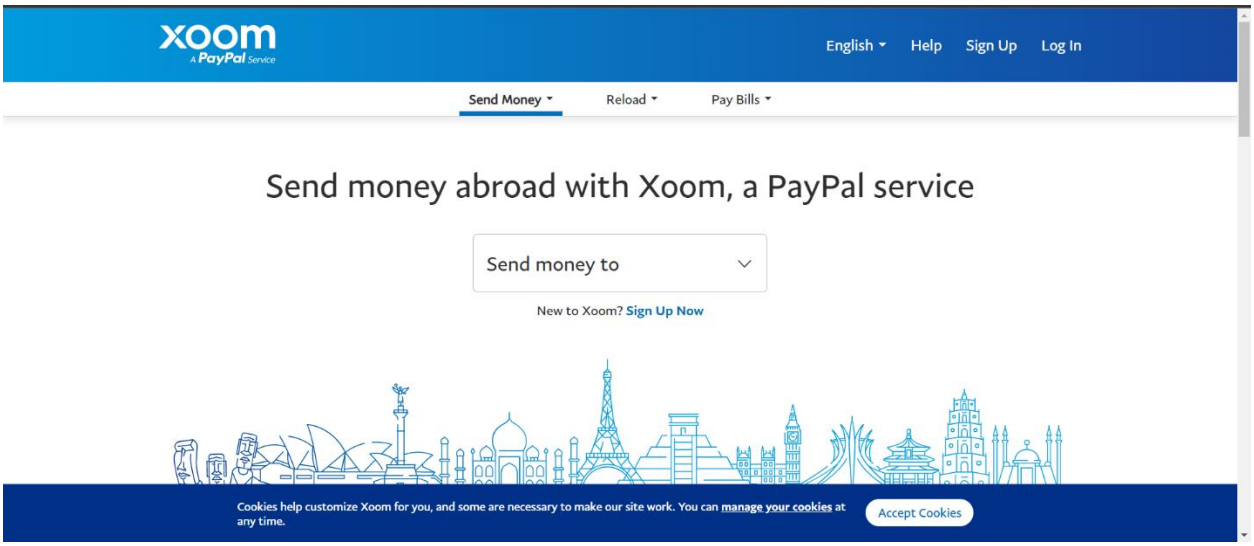
Domain	***.braintree-api.com** For testing and account creation, please use *.sandbox.braintree-api.com rather than production.	Critical	Eligible
Domain	***.braintree.tools** Please note, this is a development environment that is constantly in flux. Accordingly, vulnerabilities found on this asset will generally have lower impact and payouts.	Critical	Eligible
Domain	**prequal.swiftfinancial.com** We are aware that the root URL of this domain returns an error, the API is functioning correctly.	Critical	Eligible
Domain	**partner.swiftfinancial.com** We are aware that the root URL of this domain returns an error, the API is functioning correctly.	Critical	Eligible
Domain	**decision.swiftfinancial.com** We are aware that the root URL of this domain returns an error, the API is functioning correctly.	Critical	Eligible
Domain	**pigeon.swiftfinancial.com** We are aware that the root URL of this domain returns an error, the API is functioning correctly.	Critical	Eligible
Domain	**scrutiny.swiftfinancial.com** We are aware that the root URL of this domain returns an error, the API is functioning correctly.	Critical	Eligible
Domain	**www.swiftcapital.com**	Critical	Eligible
Domain	**www.loanbuilder.com**	Critical	Eligible
Domain	**www.swiftfinancial.com**	Critical	Eligible
Domain	**api.swiftfinancial.com**	Critical	Eligible
Domain	**my.swiftfinancial.com**	Critical	Eligible
Domain	**api.loanbuilder.com**	Critical	Eligible

I selected 5 domains out from here.

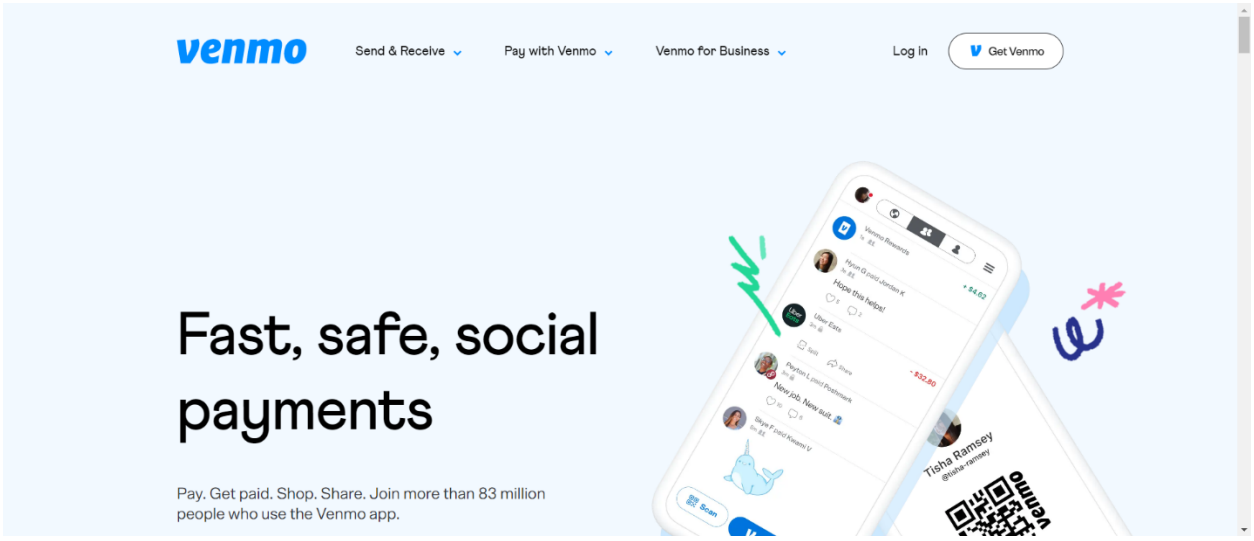
1) .paypal.com



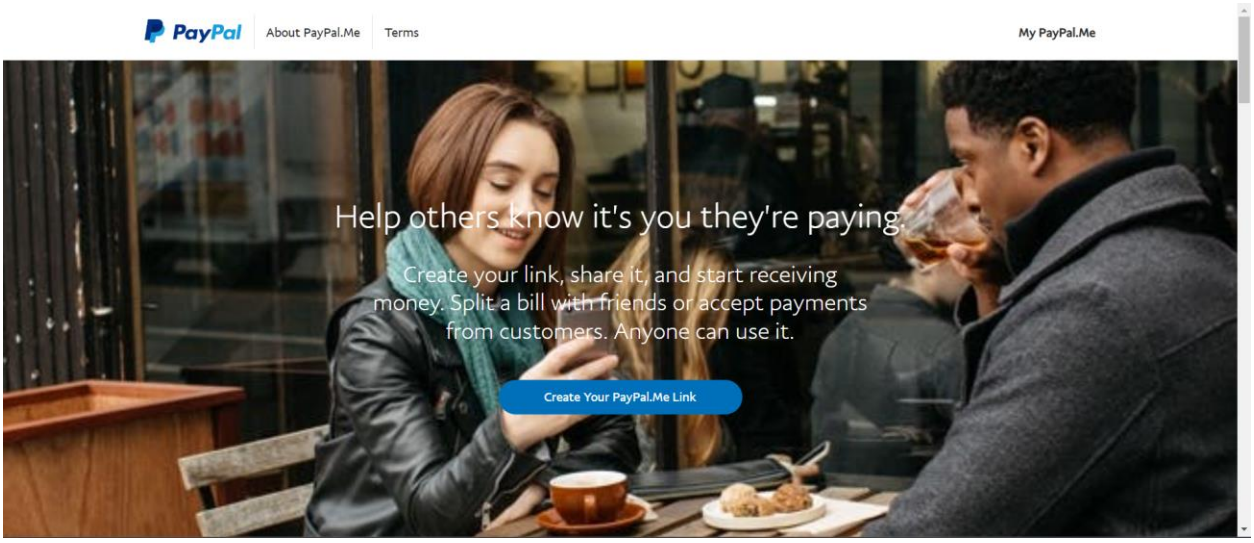
2) .xoom.com



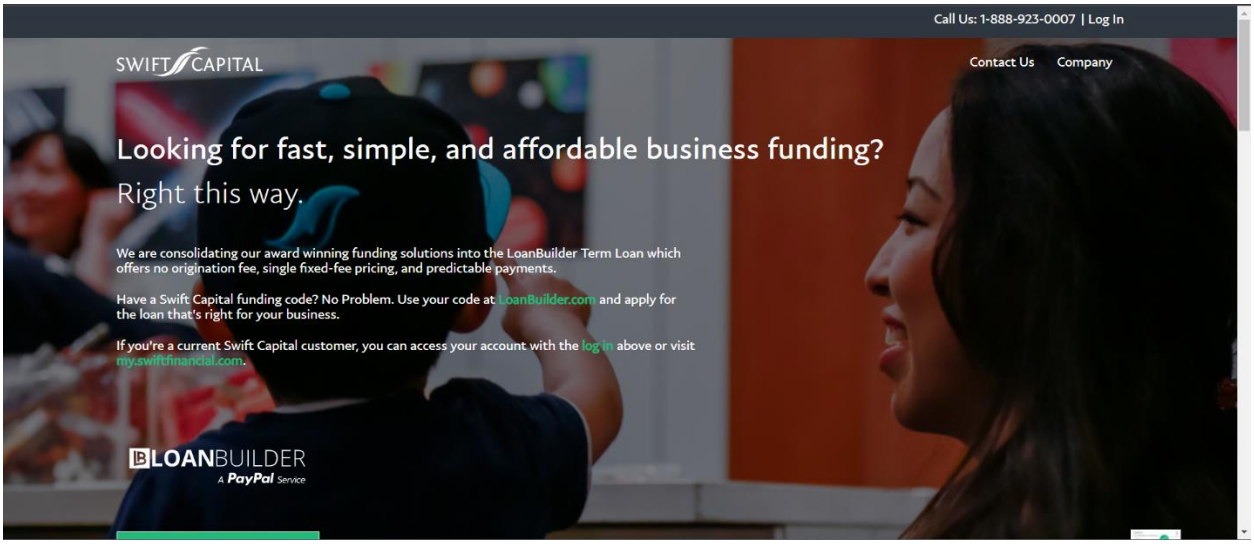
3) .venmo.com



4) paypal.me



5) www.swiftcapital.com



Out of Scope

Out of Scope	
Domain	*.paypal.cn Please note that we are unable to accept submissions on this domain due to China's Data Security Law.
Domain	braintree.com Please note braintree.com does not belong to PayPal, and as such is out of scope.

Information Gathering

We need to find information about our target domains. Because then we can understand the process of each domain. There are two types of Information Gathering.

- Active Information Gathering
- Passive Information Gathering

Information Gathering Tools

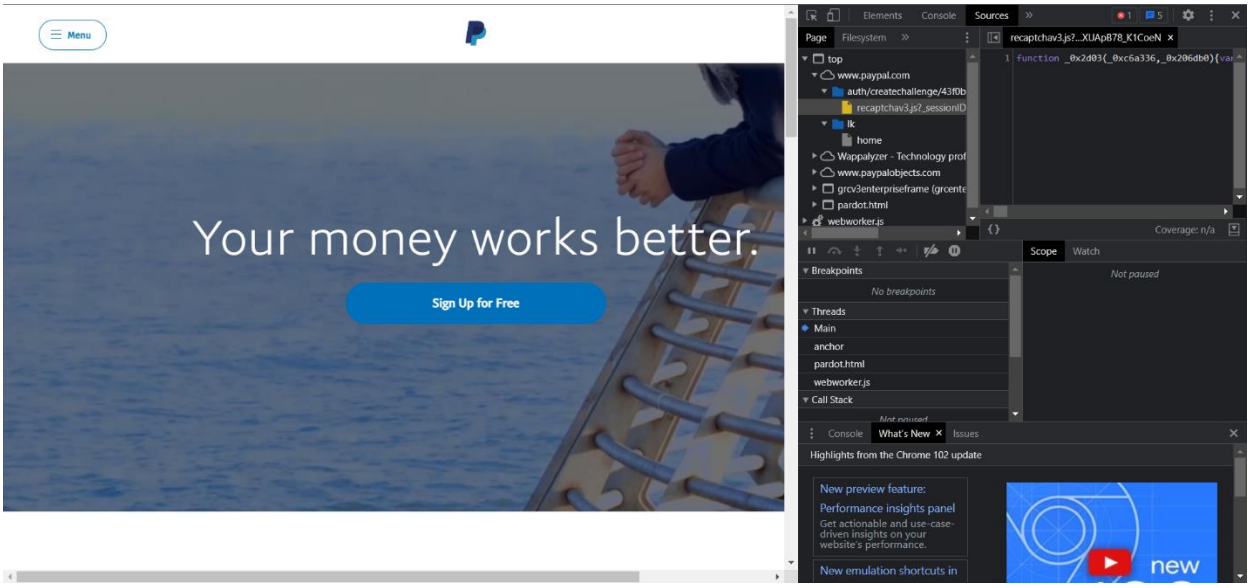
1) Web Browser

All operating systems have web browsers. With the use of an internet browser, you can get information on a target in a variety of methods.

While accessing an internet website, press 'Ctrl+Shift+I' on a PC or 'Option + Command + I' on a Mac to open the Developer Tools in Firefox. We might be able to get started using Google Chrome or Chromium by employing similar shortcuts. Developer Tools allows us to examine a large amount of data that our browser has collected and sent to a remote server. For example, we can examine or even edit the JavaScript (JS) files, examine the cookies that have been set on our device, and discover the web page content folder structure.

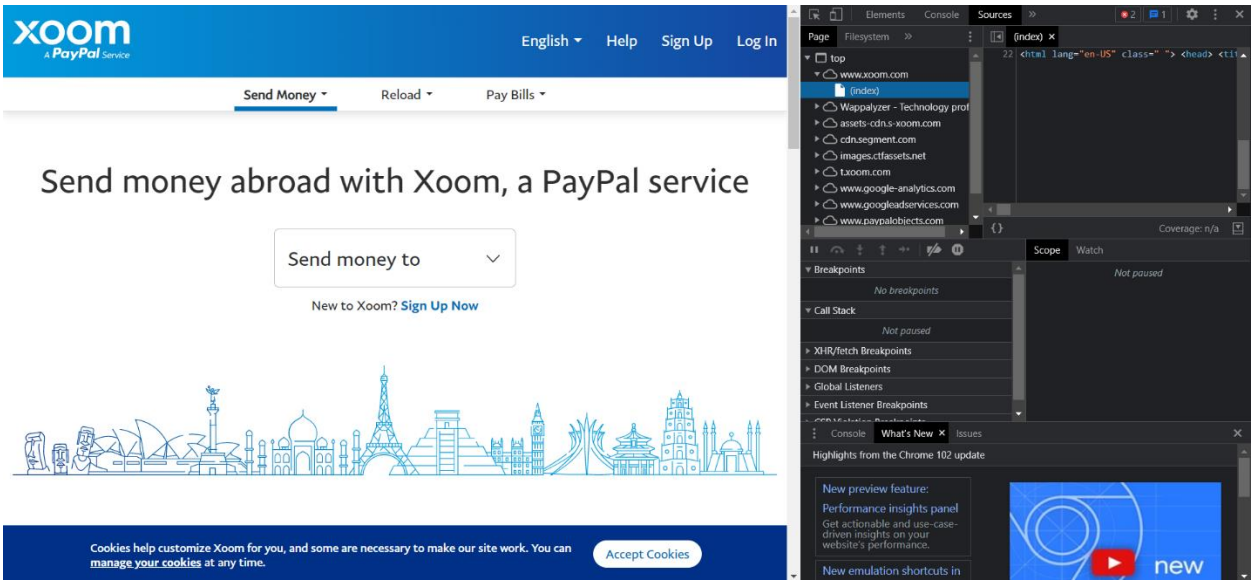
Results

- ✓ .paypal.com



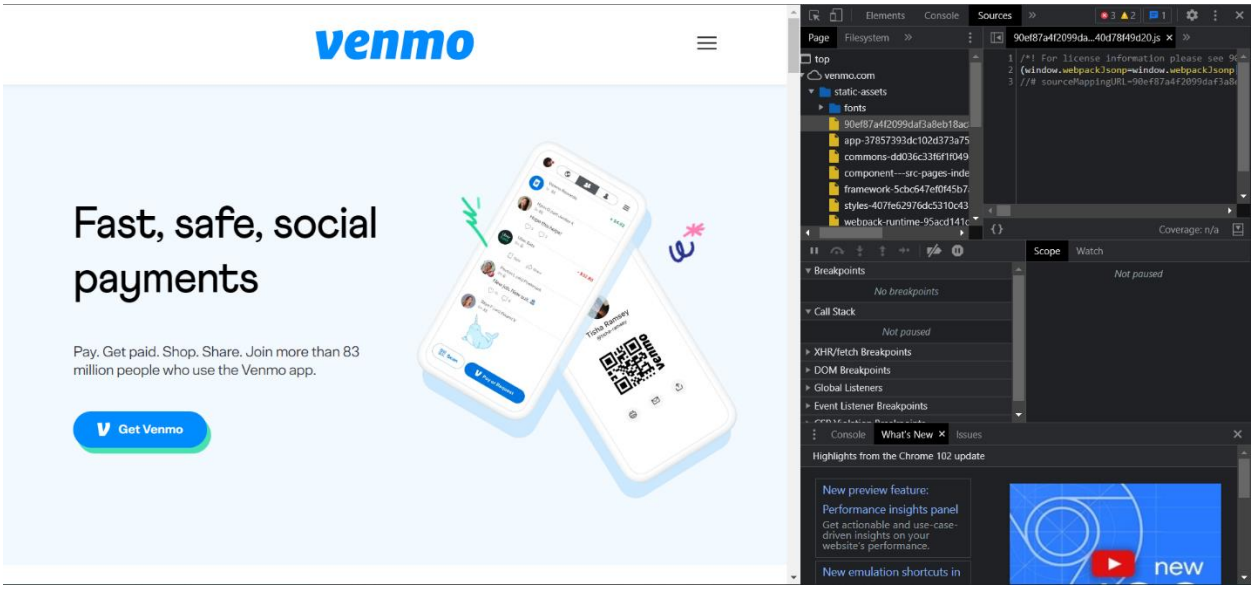
In here I found one JavaScript file called “recaptchav3.js”

- ✓ .xoom.com



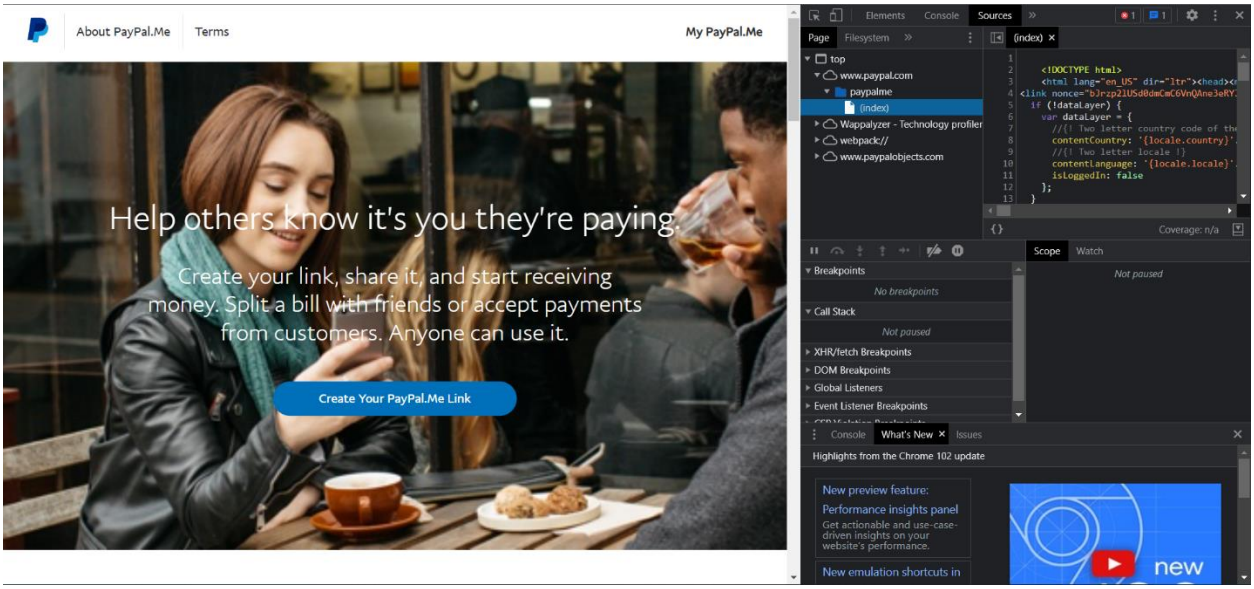
In here, I find only index file.

✓ .venmo.com



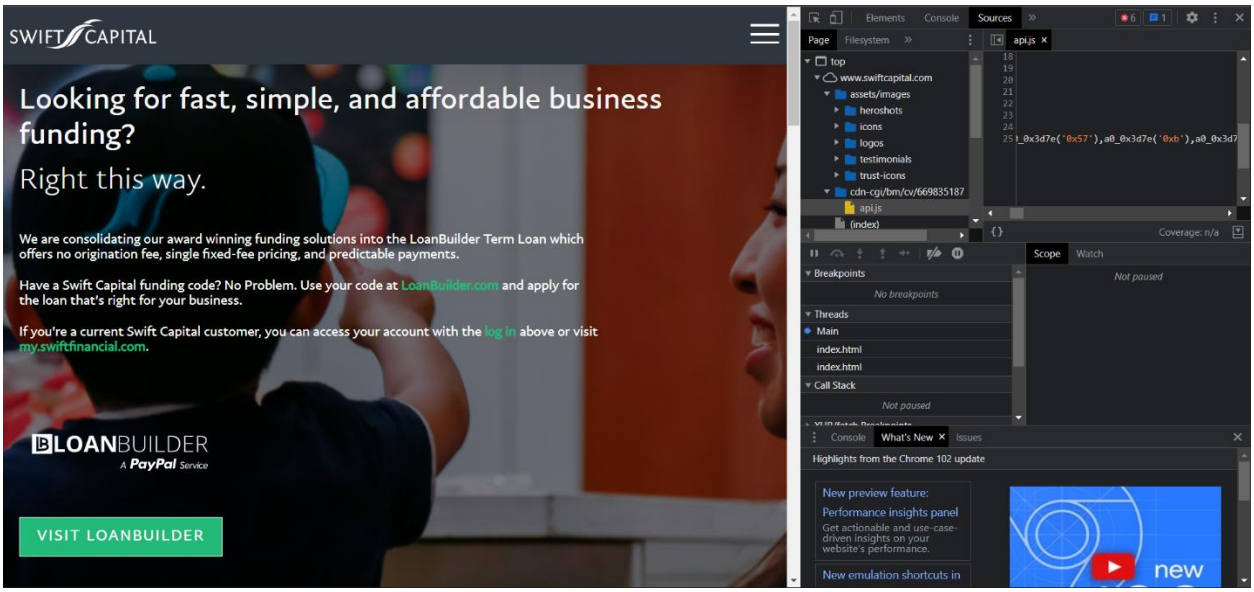
In here, I found seven JavaScript files and font.css in ‘fonts’ folder.

✓ paypal.me



In here also I found only index.html file.

- ✓ www.swiftcapital.com



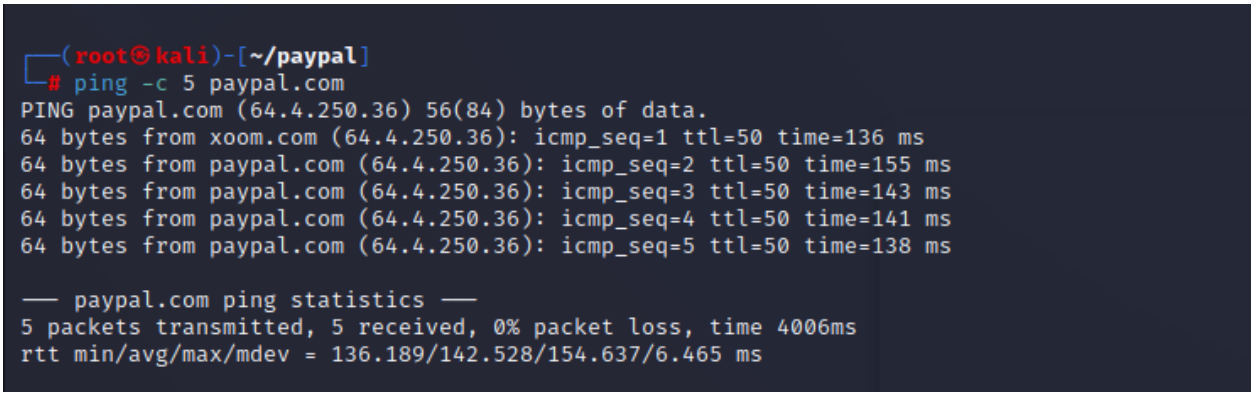
In here, I found two directories. One directory contained some images and other directory contained “api.js” file.

2) Ping

The ping is a command that sends an ICMP Echo packet to a remote machine. If the remote machine is online, and the ping packet become efficaciously routed and now no longer blocked via way of means of any firewall, the remote machine ought to send again an ICMP Echo Reply. Similarly, the ping respond ought to attain the first system if correctly routed and now no longer blocked by any firewall.

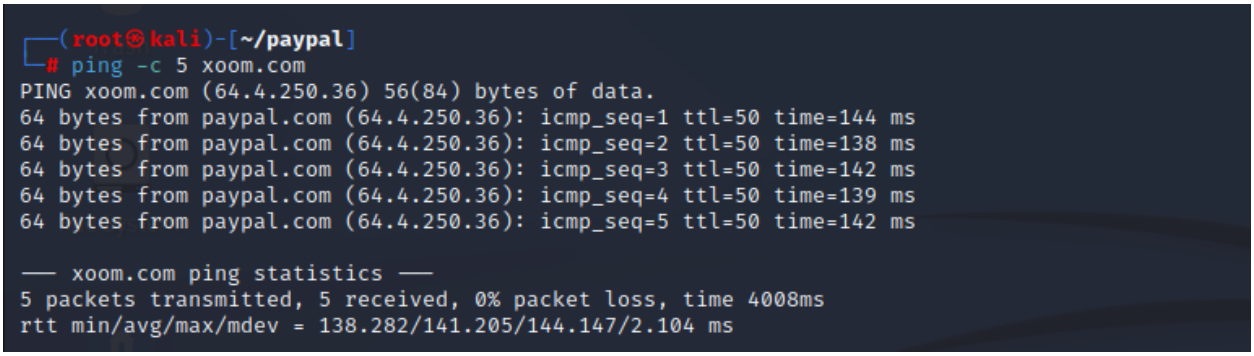
Results

- ✓ .paypal.com



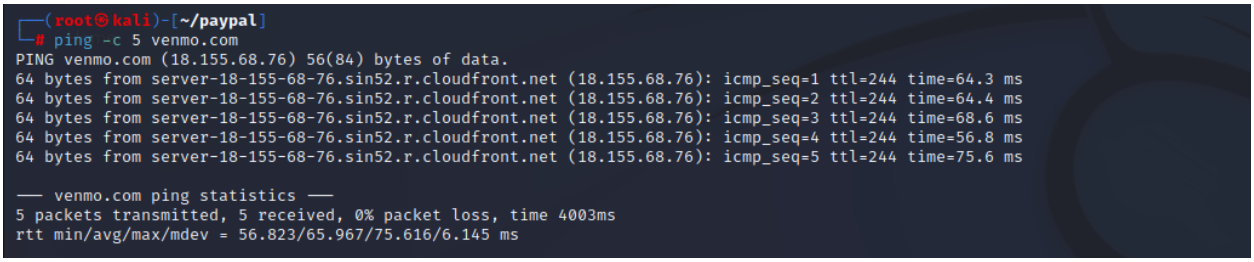
Ping work successfully for “paypal.com”. We can see Ip address of “paypal.com” as 64.4.250.36.

- ✓ .xoom.com



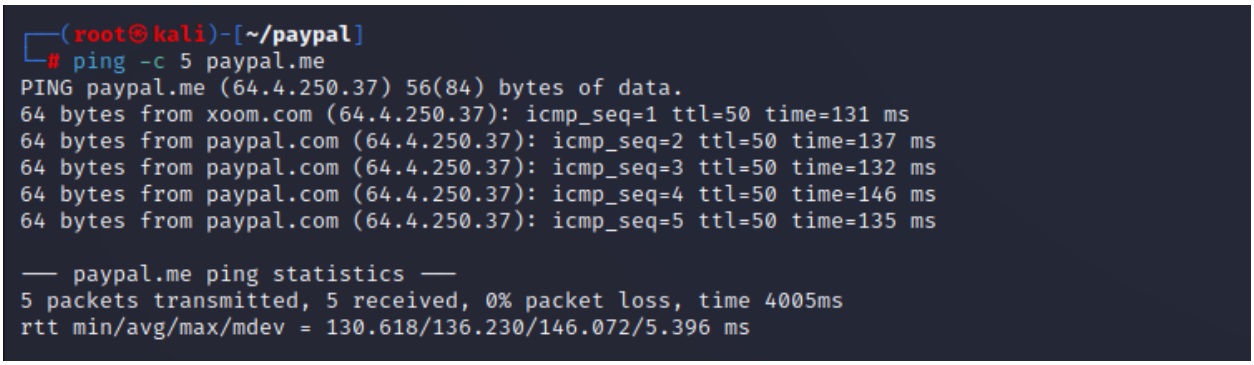
This also ping command successful. But Ip address is same as “paypal.com” because of “paypal.com” and “xoom.com” are hosted by single server.

✓ .venmo.com



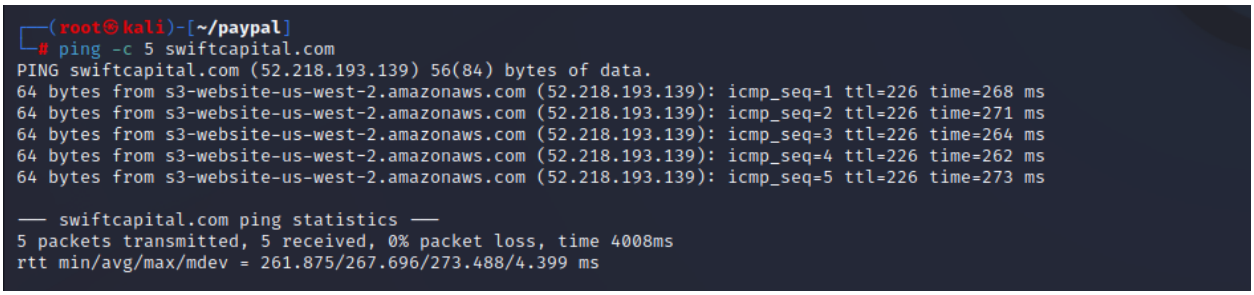
Ping command successful. Ip address is 18.155.68.76.

✓ paypal.me



Ping successful. Ip address is 64.4.250.37.

- ✓ .swiftcapital.com



Ping successful. Ip address is 52.218.193.139.

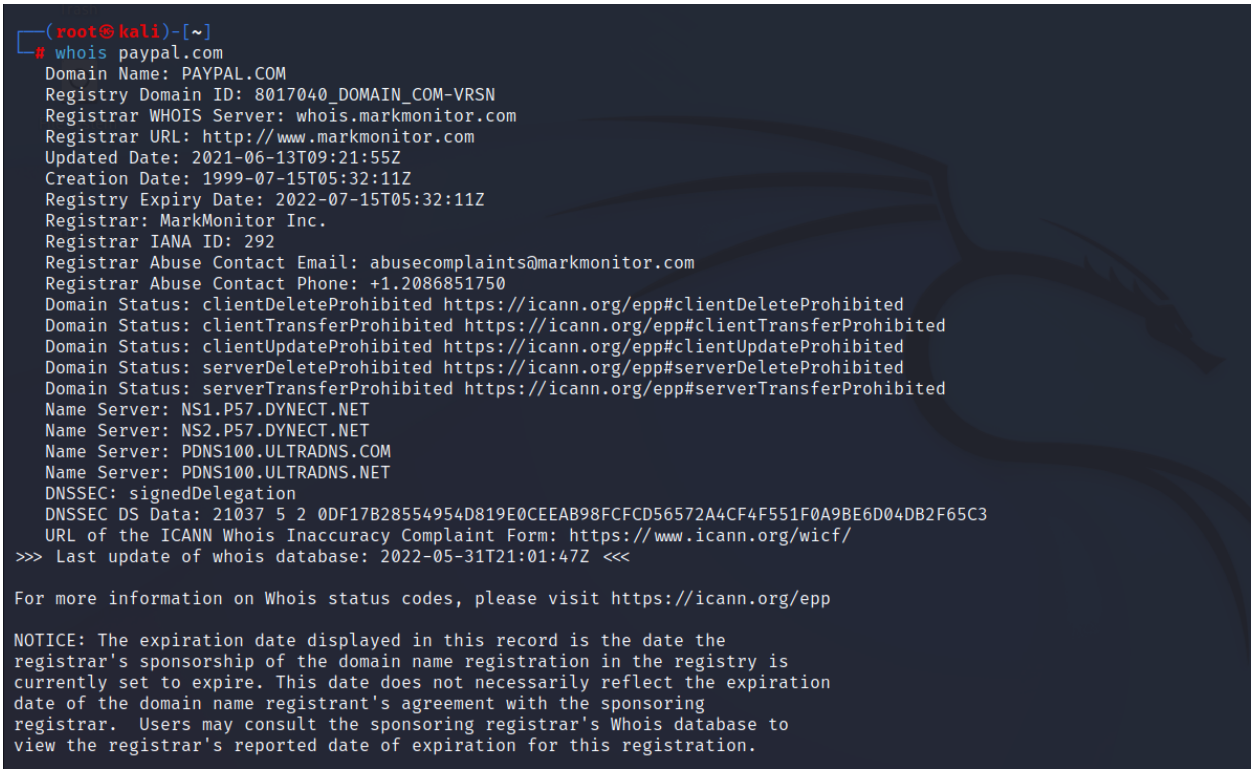
3) Whois

WHOIS is a protocol. A WHOIS server listens on TCP port forty three for incoming requests. The WHOIS server replies with diverse records associated with the area requested.

- ❖ Registrar
- ❖ Contact data of registrant
- ❖ Creation date , update date and expiration dates
- ❖ Name Server

Results

- ✓ .paypal.com



```
TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: paypal.com
Registry Domain ID: 8017040_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2021-06-13T09:21:55+0000
Creation Date: 1999-07-15T05:32:11+0000
Registrar Registration Expiration Date: 2022-07-14T07:00:00+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)
```

- ✓ .xoom.com

```
┌──(root㉿kali)-[~]
└─# whois xoom.com
   Domain Name: XOOM.COM
   Registry Domain ID: 2267723_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2021-10-31T09:41:14Z
   Creation Date: 1996-12-03T05:00:00Z
   Registry Expiry Date: 2022-12-02T05:00:00Z
   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
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.P134.DYNECT.NET
   Name Server: NS2.P134.DYNECT.NET
   Name Server: PDNS100.ULTRADNS.COM
   Name Server: PDNS100.ULTRADNS.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-05-31T20:20:45Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: xoom.com
Registry Domain ID: 2267723_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2021-10-31T09:41:14+0000
Creation Date: 1996-12-03T05:00:00+0000
Registrar Registration Expiration Date: 2022-12-02T00:00:00+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)
Domain Status: serverUpdateProhibited (https://www.icann.org/epp#serverUpdateProhibited)
Domain Status: serverTransferProhibited (https://www.icann.org/epp#serverTransferProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: PayPal Inc.
Registrant Street: 2211 North First Street,
Registrant City: San Jose
Registrant State/Province: CA
Registrant Postal Code: 95131
Registrant Country: US
Registrant Phone: +1.8882211161
Registrant Phone Ext:
Registrant Fax: +1.4025375774
Registrant Fax Ext:
Registrant Email: hostmaster@paypal.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: PayPal Inc.
Admin Street: 2211 North First Street,
Admin City: San Jose
Admin State/Province: CA
Admin Postal Code: 95131
```

✓ .venmo.com

```
┌──(root㉿kali)-[~]
└─# whois venmo.com
   Domain Name: VENMO.COM
   Registry Domain ID: 1534766363_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2021-11-24T09:19:33Z
   Creation Date: 2008-12-26T16:44:05Z
   Registry Expiry Date: 2022-12-26T16:44:05Z
   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
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS-1457.AWSDNS-54.ORG
   Name Server: NS-1599.AWSDNS-07.CO.UK
   Name Server: NS-304.AWSDNS-38.COM
   Name Server: NS-665.AWSDNS-19.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-05-31T20:23:30Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: venmo.com
Registry Domain ID: 1534766363_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2021-11-24T09:19:33+0000
Creation Date: 2008-12-26T16:44:05+0000
Registrar Registration Expiration Date: 2022-12-26T00:00:00+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)
```

✓ paypal.me

```
┌──(root㉿kali)-[~]
└─# whois paypal.me
Domain Name: PAYPAL.ME
Registry Domain ID: D108500000000010741-AGRS
Registrar WHOIS Server:
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-05-12T09:35:13Z
Creation Date: 2008-06-13T17:17:50Z
Registry Expiry Date: 2023-06-13T17:17:50Z
Registrar Registration Expiration Date:
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Reseller:
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Registrant Organization: PayPal PTE LTD.
Registrant State/Province: SG
Registrant Country: SG
Name Server: NS1.P57.DYNECT.NET
Name Server: NS2.P57.DYNECT.NET
Name Server: PDNS100.ULTRADNS.COM
Name Server: PDNS100.ULTRADNS.NET
DNSSEC: signedDelegation
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of WHOIS database: 2022-05-31T20:19:14Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

Access to WHOIS information is provided to assist persons in determining the contents of a domain name registration record in the registry database. The data in this record is provided by T
he Registry Operator for informational purposes only, and accuracy is not guaranteed.  This service is intended only for query-based access. You agree that you will use this data only for l
awful purposes and that, under no circumstances will you use this data to (a) allow, enable, or otherwise support the transmission by e-mail, telephone, or facsimile of mass unsolicited, co
mmercial advertising or solicitations to entities other than the data recipient's own existing customers; or (b) enable high volume, automated, electronic processes that send queries or dat
a to the systems of Registry Operator, a Registrar, or Afilias except as reasonably necessary to register domain names or modify existing registrations. All rights reserved. Registry Operat
or reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this policy.
The Registrar of Record identified in this output may have an RDDS service that can be queried for additional information on how to contact the Registrant, Admin, or Tech contact of the que
ried domain name.
```

✓ www.swiftcapital.com

```
┌──(root㉿kali)-[~]
└─# whois swiftcapital.com
   Domain Name: SWIFTCAPITAL.COM
   Registry Domain ID: 18616934_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2022-04-13T09:44:21Z
   Creation Date: 2000-01-28T17:44:20Z
   Registry Expiry Date: 2023-05-15T11:59:59Z
   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: NS-1187.AWSDNS-20.ORG
   Name Server: NS-1699.AWSDNS-20.CO.UK
   Name Server: NS-486.AWSDNS-60.COM
   Name Server: NS-581.AWSDNS-08.NET
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-05-31T20:33:07Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
```

```
TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining information
about or related to a domain name registration record. VeriSign does not
guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability.  VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.
Domain Name: swiftcapital.com
Registry Domain ID: 18616934_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2022-04-13T09:44:21+0000
Creation Date: 2000-01-28T17:44:20+0000
Registrar Registration Expiration Date: 2023-05-15T00:00:00+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)
```

4) Final Recon

Final Recon is a python-based project hosted on GitHub. Scanning, enumeration, and footprinting are some of the reconnaissance techniques utilized by Final Recon. This has many features. The commands below are used to access certain functionalities.

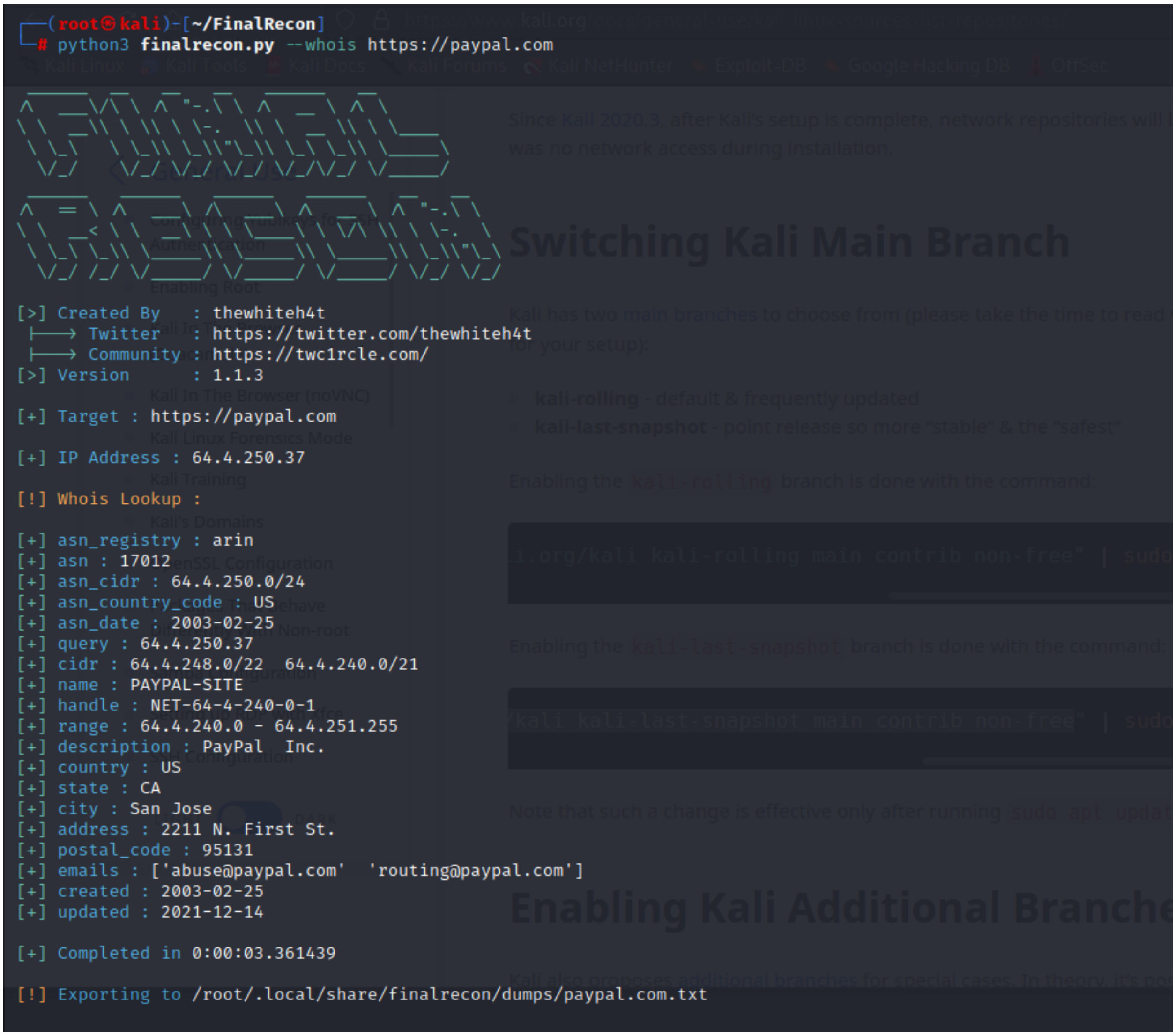
- Header - Check the server, content-type, and encoding methods in the headers.
- SSLinfo - Verify the site's security.
- Crawl - Gathering online pages or links from a website. WHOIS – lookup information about the domain.
- Dns - look up Dns A, AAA, and other records.
- Trace – can be used for troubleshooting purposes. Sub – find the subdomain
- Dir- Grab the hidden directory
- For port scanning, use Port Scan. For a full scan, use Full Scan.

Installation

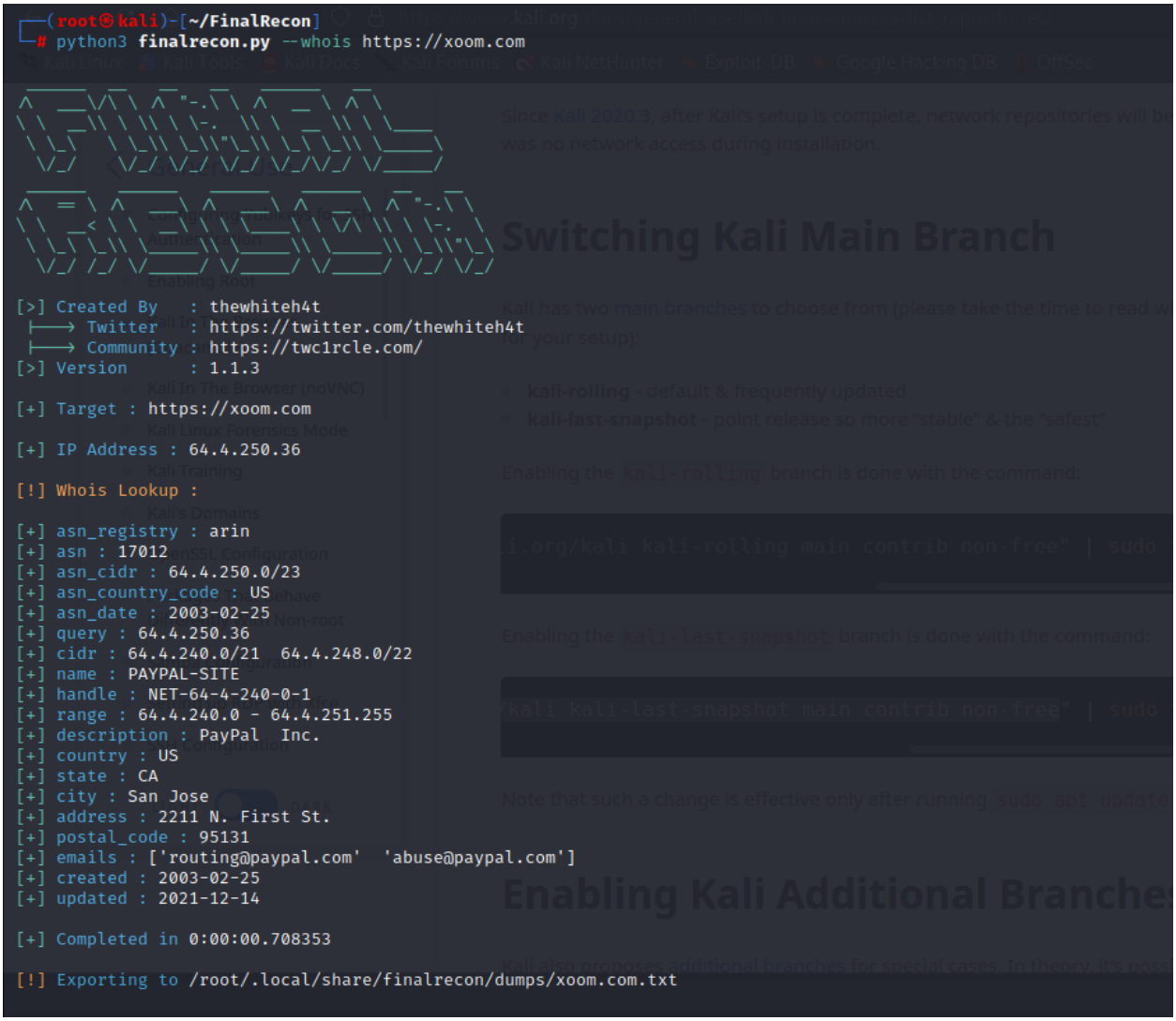
- git clone https://github.com/thewhiteh4t/FinalRecon.git
- cd FinalRecon
- pip3 install -r requirements.txt

Results

- ✓ .paypal.com


(root㉿kali)-[~/FinalRecon]
python3 finalrecon.py --whois https://paypal.com
[>] Created By : thewhiteh4t
Twitter : https://twitter.com/thewhiteh4t
Community : https://twc1rcle.com/
[>] Version : 1.1.3
[+] Target : https://paypal.com
[+] IP Address : 64.4.250.37
[!] Whois Lookup :
[+] asn_registry : arin
[+] asn : 17012
[+] asn_cidr : 64.4.250.0/24
[+] asn_country_code : US
[+] asn_date : 2003-02-25
[+] query : 64.4.250.37
[+] cidr : 64.4.248.0/22 64.4.240.0/21
[+] name : PAYPAL-SITE
[+] handle : NET-64-4-240-0-1
[+] range : 64.4.240.0 - 64.4.251.255
[+] description : PayPal Inc.
[+] country : US
[+] state : CA
[+] city : San Jose
[+] address : 2211 N. First St.
[+] postal_code : 95131
[+] emails : ['abuse@paypal.com' 'routing@paypal.com']
[+] created : 2003-02-25
[+] updated : 2021-12-14
[+] Completed in 0:00:03.361439
[!] Exporting to /root/.local/share/finalrecon/dumps/paypal.com.txt

✓ .xoom.com

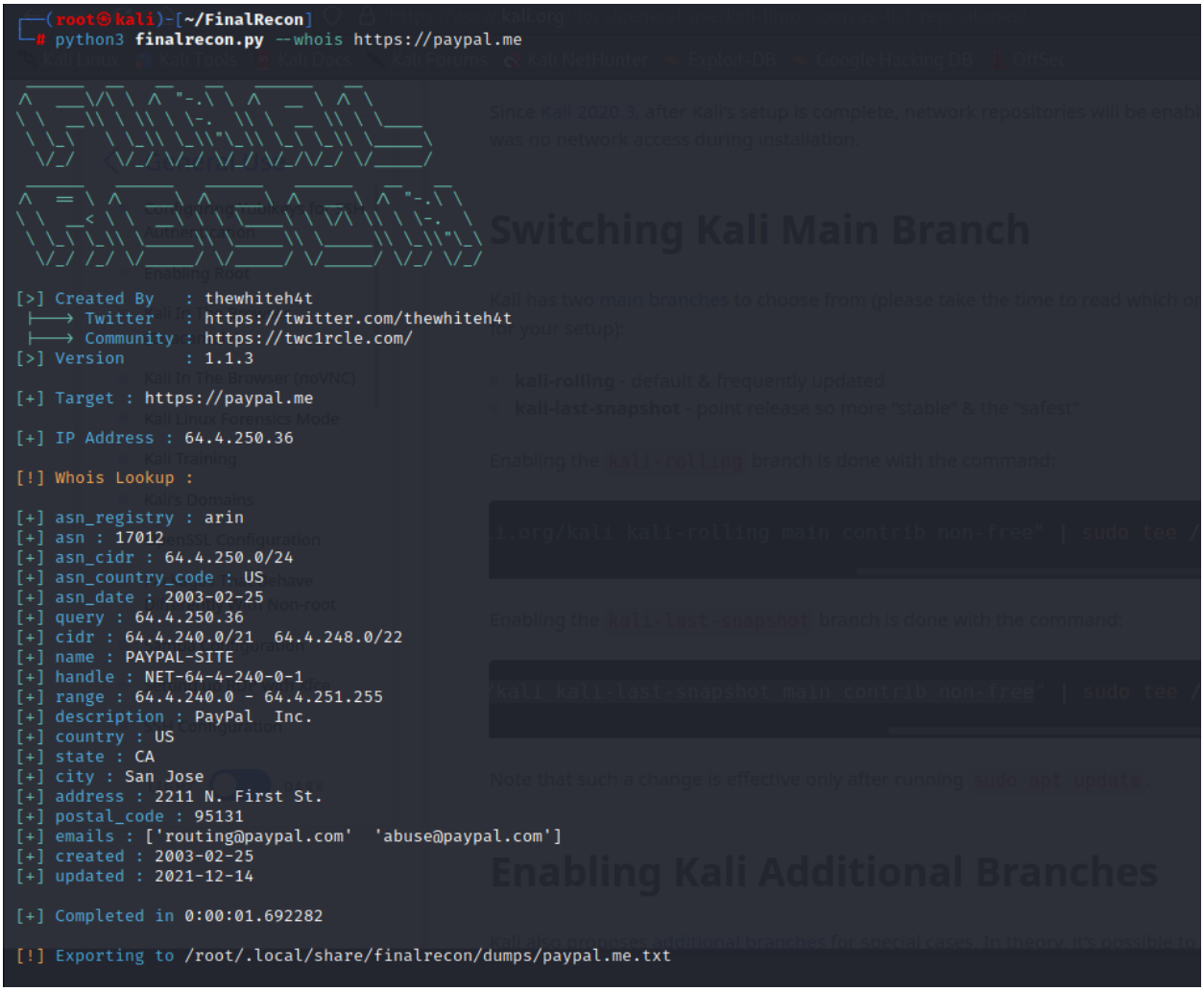

┌──(root㉿kali)-[~/FinalRecon]
└─# python3 finalrecon.py --whois https://xoom.com
[>] Created By : thewhiteh4t
[>] Version : 1.1.3
[+] Target : https://xoom.com
[+] IP Address : 64.4.250.36
[!] Whois Lookup :
[+] asn_registry : arin
[+] asn : 17012
[+] asn_cidr : 64.4.250.0/23
[+] asn_country_code : US
[+] asn_date : 2003-02-25
[+] query : 64.4.250.36
[+] cidr : 64.4.240.0/21 64.4.248.0/22
[+] name : PAYPAL-SITE
[+] handle : NET-64-4-240-0-1
[+] range : 64.4.240.0 - 64.4.251.255
[+] description : PayPal Inc.
[+] country : US
[+] state : CA
[+] city : San Jose
[+] address : 2211 N. First St.
[+] postal_code : 95131
[+] emails : ['routing@paypal.com' 'abuse@paypal.com']
[+] created : 2003-02-25
[+] updated : 2021-12-14
[+] Completed in 0:00:00.708353
[!] Exporting to /root/.local/share/finalrecon/dumps/xoom.com.txt

- ✓ .venmo.com

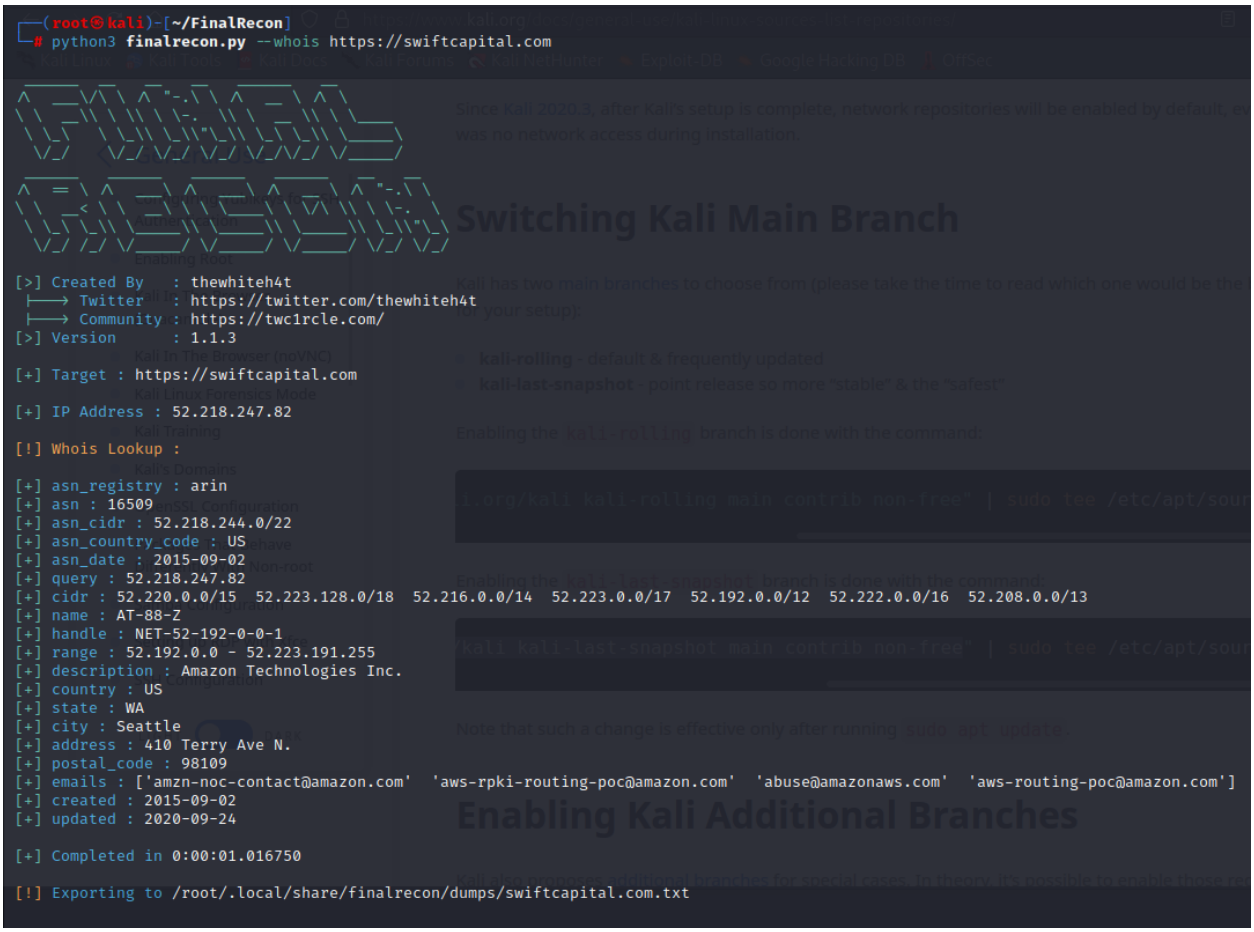
```
┌──(root㉿kali)-[~/FinalRecon]
└─# python3 finalrecon.py --whois https://venmo.com

 _____ __  __ __  __  _____  __
/\  __\/\ \ /\ "-.\ \/\  __ \/\ \
\ \  __\\ \ \\ \ \-.  \ \  __ \\ \ \____
 \ \_\   \ \_\\ \_\\"\_\\ \_\ \_\\ \_____\
  \/_/    \/_/ \/_/ \/_/ \/_/\/_/ \/_____/
 _____   _____   _____   _____   __  __
/\  == \ /\  __-. /\  __-. /\  __-. /\ "-./  \
\ \  __< \ \ \/\ \\ \ \/\ \\ \ \/\ \\ \ \-./\ \
 \ \_\ \_\\ \____- \ \____- \ \____- \ \_\ \ \_\
  \/_/ /_/ \/____/  \/____/  \/____/  \/_/  \/_/

[>] Created By    : thewhiteh4t
 |---> Twitter    : https://twitter.com/thewhiteh4t
 |---> Community  : https://twc1rcle.com/
[>] Version       : 1.1.3

[+] Target : https://venmo.com

[+] IP Address : 18.155.68.42

[!] Whois Lookup :

[+] asn_registry : arin
[+] asn : 16509
[+] asn_cidr : 18.155.64.0/21
[+] asn_country_code : US
[+] asn_date : 2019-10-07
[+] query : 18.155.68.42
[+] cidr : 18.128.0.0/9  18.64.0.0/10  18.32.0.0/11
[+] name : AT-88-Z
[+] handle : NET-18-32-0-0-1
[+] range : 18.32.0.0 - 18.255.255.255
[+] description : Amazon Technologies Inc.
[+] country : US
[+] state : WA
[+] city : Seattle
[+] address : 410 Terry Ave N.
[+] postal_code : 98109
[+] emails : ['abuse@amazonaws.com'  'amzn-noc-contact@amazon.com'  'aws-rpki-routing-poc@amazon.com'  'aws-routing-poc@amazon.com']
[+] created : 2019-10-07
[+] updated : 2021-02-10
[+] cidr : 18.154.0.0/15
[+] name : AMAZON-CF
[+] handle : NET-18-154-0-0-1
[+] description : Amazon.com  Inc.
[+] country : US
```

```
[+] state : WA
[+] city : SEATTLE
[+] address : 1918 8th Ave
[+] postal_code : 98101-1244
[+] emails : ['amzn-noc-contact@amazon.com'  'abuse@amazonaws.com'  'aws-routing-poc@amazon.com'  'aws-rpki-routing-poc@amazon.com']
[+] created : 2022-01-21
[+] updated : 2022-01-21

[+] Completed in 0:00:01.055501

[!] Exporting to /root/.local/share/finalrecon/dumps/venmo.com.txt
```

- ✓ paypal.me



- ✓ swiftcapital.com



DNS Enumeration

5) WhatWeb

The WhatWeb is a tool which used to discover specific internet technology utilized by the website. It is pre-hooked up device in kali linux.

Results

- ✓ .paypal.com

```
┌──(root㉿kali)-[~]
└─# whatweb paypal.com
http://paypal.com [301 Moved Permanently] Country[UNITED STATES][US], IP[64.4.250.36], RedirectLocation[https://paypal.com/], Title[301 Moved Permanently]
https://paypal.com/ [302 Found] Country[UNITED STATES][US], IP[64.4.250.36], RedirectLocation[https://www.paypal.com/], Strict-Transport-Security[max-age=315
https://www.paypal.com/ [302 Found] Country[UNITED STATES][US], HTTPServer[Varnish], IP[151.101.129.21], RedirectLocation[https://www.paypal.com/lk/home], St
Headers[retry-after,x-served-by,x-cache-hits,server-timing], Varnish, Via-Proxy[1.1 varnish]
https://www.paypal.com/lk/home [200 OK] Cookies[LANG,cookie_check,enforce_policy,l7_az,nsid,ts,ts_c,tsrce,x-pp-s], Country[UNITED STATES][US], HTML5, HttpOnl
-Protocol[website], Script[application/ld+json], Strict-Transport-Security[max-age=63072000; includeSubDomains; preload], Title[Send Money, Pay Online or Set
l-debug-id,x-content-type-options,dc,x-served-by,x-cache-hits,x-timer,server-timing], Via-Proxy[1.1 varnish], X-UA-Compatible[IE=edge], X-XSS-Protection[1; m
```

✓ .xoom.com

```
┌──(root㉿kali)-[~]
└─# whatweb xoom.com
xoom.com [ Unassigned]

┌──(root㉿kali)-[~]
└─# whatweb xoom.com
xoom.com [ Unassigned]
```

✓ .venmo.com

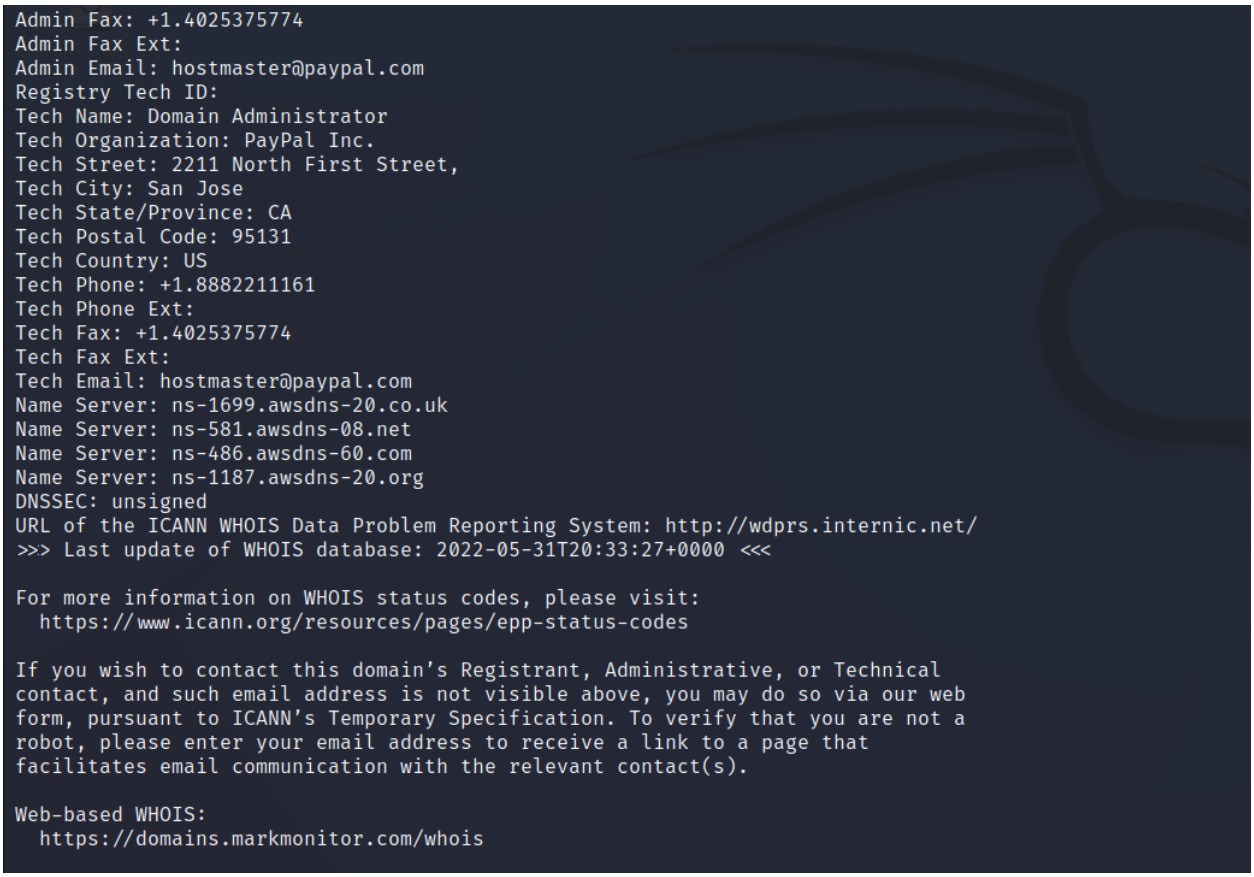
```
┌──(root㉿kali)-[~]
└─# whatweb venmo.com
http://venmo.com [301 Moved Permanently] CloudFront, Country[UNITED STATES][US], HTTPServer[CloudFront], IP[18.155.68.21], RedirectLocation[https://venmo.com
a-Proxy[1.1 0f2b81f417aa397d9ed9b32b2017aaca.cloudfront.net (CloudFront)]
https://venmo.com/ [200 OK] Country[UNITED STATES][US], Google-Analytics[Universal][UA-15492939-14,UA-15492939-15], HTML5, HTTPServer[nginx], IP[18.155.68.21
Transport-Security[max-age=31536000, max-age=31536000], UncommonHeaders[x-envoy-upstream-service-time,x-content-type-options,x-amz-cf-pop,x-amz-cf-id], Via-P
mpatible[ie=edge], X-XSS-Protection[1; mode=block], nginx
```

✓ paypal.me

```
┌──(root㉿kali)-[~]
└─# whatweb paypal.me
http://paypal.me [301 Moved Permanently] Country[UNITED STATES][US], IP[64.4.250.37], RedirectLocation[https://paypal.me/], Title[301 Moved Permanently]
https://paypal.me/ [302 Found] Country[UNITED STATES][US], IP[64.4.250.37], RedirectLocation[https://www.paypal.me/], Strict-Transport-Security[max-age=31536
https://www.paypal.me/ [301 Moved Permanently] Country[UNITED STATES][US], IP[151.101.193.21], RedirectLocation[https://www.paypal.com/paypalme/], Strict-Tra
paypal-debug-id,dc,x-served-by,x-cache-hits,x-timer,server-timing], Via-Proxy[1.1 varnish]
https://www.paypal.com/paypalme/ [200 OK] Country[UNITED STATES][US], HTML5, IP[151.101.193.21], Open-Graph-Protocol, Script[text/javascript], Strict-Transpo
commonHeaders[content-security-policy,paypal-debug-id,x-content-type-options,dc,x-served-by,x-cache-hits,x-timer,server-timing], Via-Proxy[1.1 varnish], X-Fr
```

✓ swiftcapital.com

```
┌──(root㉿kali)-[~]
└─# whatweb swiftcapital.com
http://swiftcapital.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[AmazonS3], IP[52.218.184.210], RedirectLocation[http://www.swiftcapita
http://www.swiftcapital.com/ [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[cloudflare], IP[104.16.83.73], RedirectLocation[https://www.swift
https://www.swiftcapital.com/ [200 OK] Bootstrap, CloudFront, Country[UNITED STATES][US], Email[ariel@mashraki.co.il,careers@swiftcapital.com,customerservice
A-23331527-1], HTML5, HTTPServer[cloudflare], IP[104.16.83.73], Open-Graph-Protocol[website], Script[text/javascript], Strict-Transport-Security[max-age=1555
 Swift Capital], UncommonHeaders[x-amz-cf-pop,x-amz-cf-id,cf-cache-status,expect-ct,x-content-type-options,cf-ray], Via-Proxy[1.1 759e09affff41285e9585e1a315
```

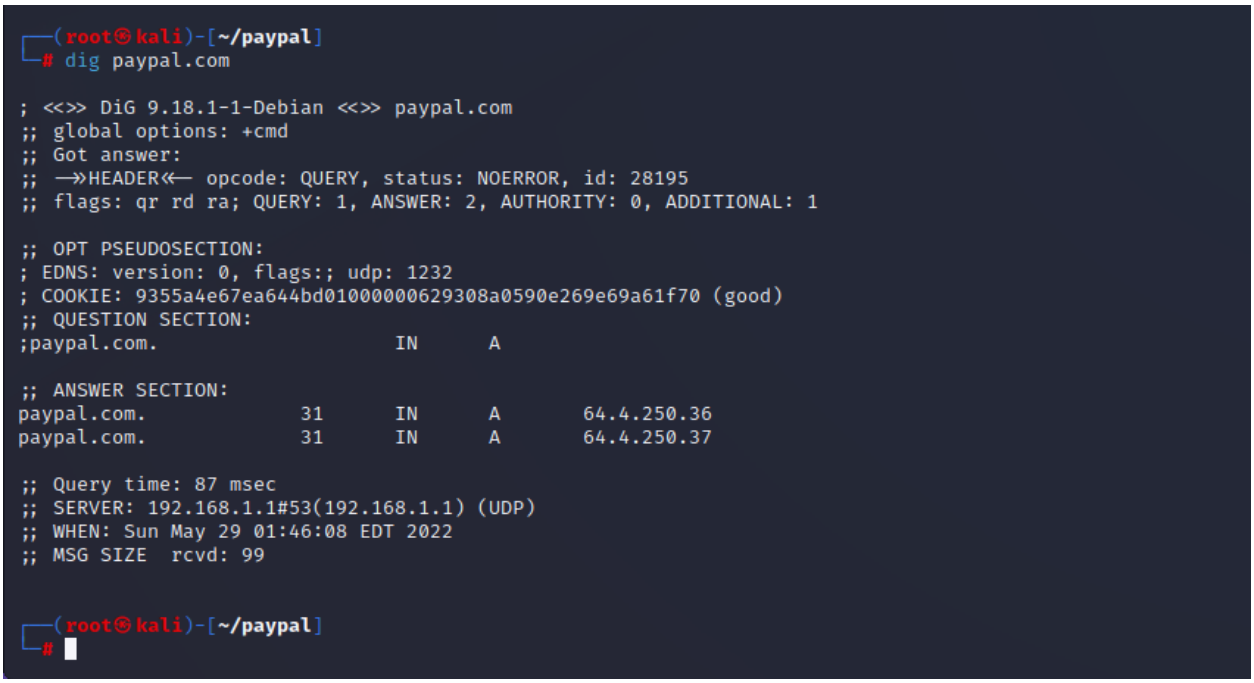


6) Dig

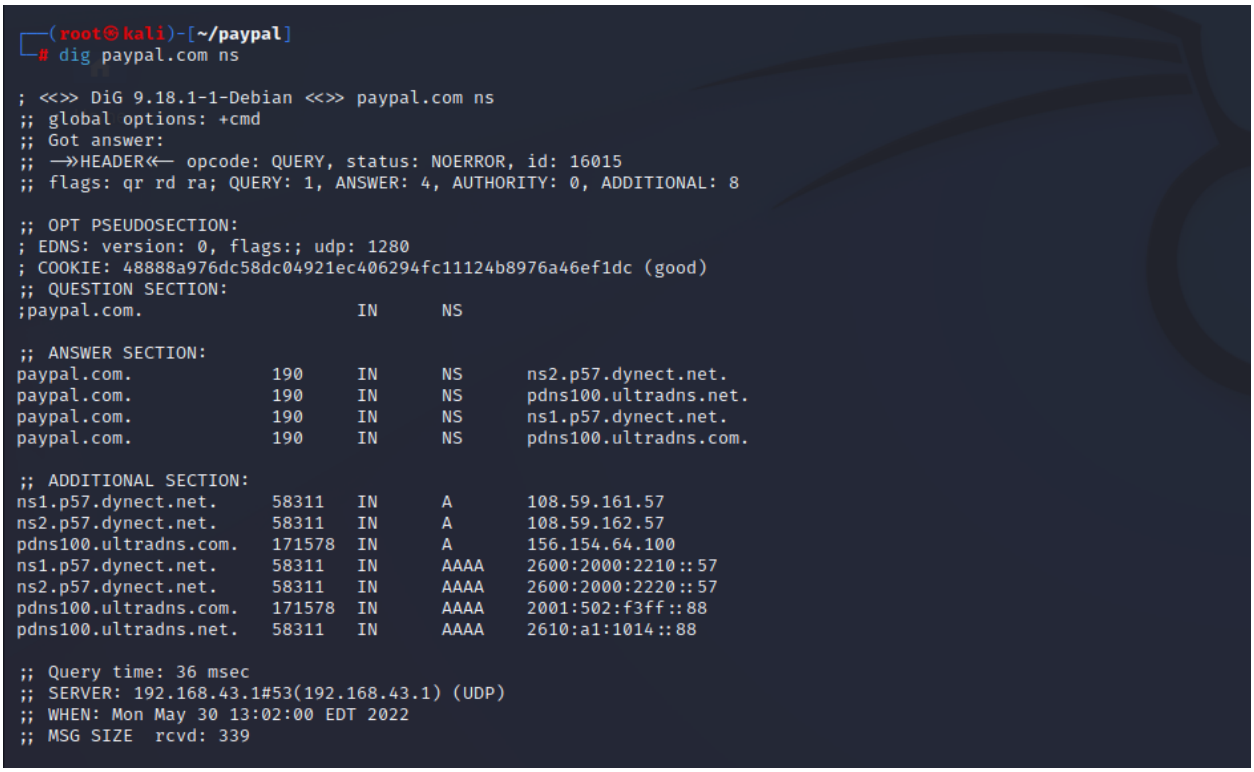
Dig is the abbreviation for 'Domain Information Groper.' Dig comes pre-installed in the Kali Linux operating system. It can be used to query the Domain Name System (DNS).

Results

- ✓ .paypal.com



In here, I found that the domain paypal.com point to the 64.4.250.36 and 64.4.250.37 IP addresses. ‘ns’ keyword use to find authoritative Dns servers information for given domain.

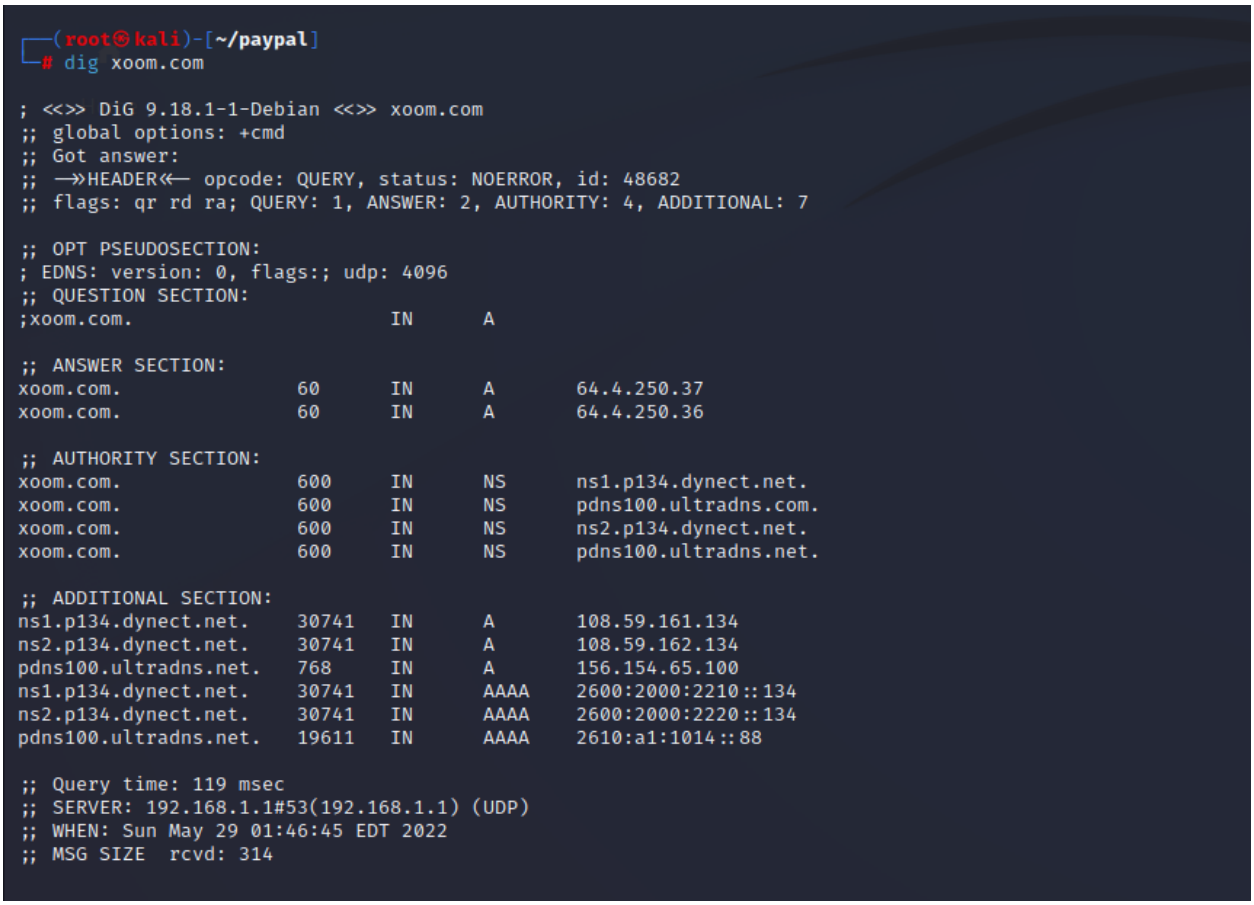


```
┌──(root㉿kali)-[~/paypal]
└─# dig paypal.com ns

; <<>> DiG 9.18.1-1-Debian <<>> paypal.com ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 16015
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 8

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: 48888a976dc58dc04921ec406294fc11124b8976a46ef1dc (good)
;; QUESTION SECTION:
;paypal.com.                    IN      NS

;; ANSWER SECTION:
paypal.com.             190     IN      NS      ns2.p57.dynect.net.
paypal.com.             190     IN      NS      pdns100.ultradns.net.
paypal.com.             190     IN      NS      ns1.p57.dynect.net.
paypal.com.             190     IN      NS      pdns100.ultradns.com.

;; ADDITIONAL SECTION:
ns1.p57.dynect.net.     58311   IN      A       108.59.161.57
ns2.p57.dynect.net.     58311   IN      A       108.59.162.57
pdns100.ultradns.com.   171578  IN      A       156.154.64.100
ns1.p57.dynect.net.     58311   IN      AAAA    2600:2000:2210::57
ns2.p57.dynect.net.     58311   IN      AAAA    2600:2000:2220::57
pdns100.ultradns.com.   171578  IN      AAAA    2001:502:f3ff::88
pdns100.ultradns.net.   58311   IN      AAAA    2610:a1:1014::88

;; Query time: 36 msec
;; SERVER: 192.168.43.1#53(192.168.43.1) (UDP)
;; WHEN: Mon May 30 13:02:00 EDT 2022
;; MSG SIZE  rcvd: 339
```

I found four authoritative Dns servers and their Ip addresses for ‘paypal.com’.

- ns2.p57.dynect.net.
- pdns100.ultradns.net.
- ns1.p57.dynect.net.
- pdns100.ultradns.com.

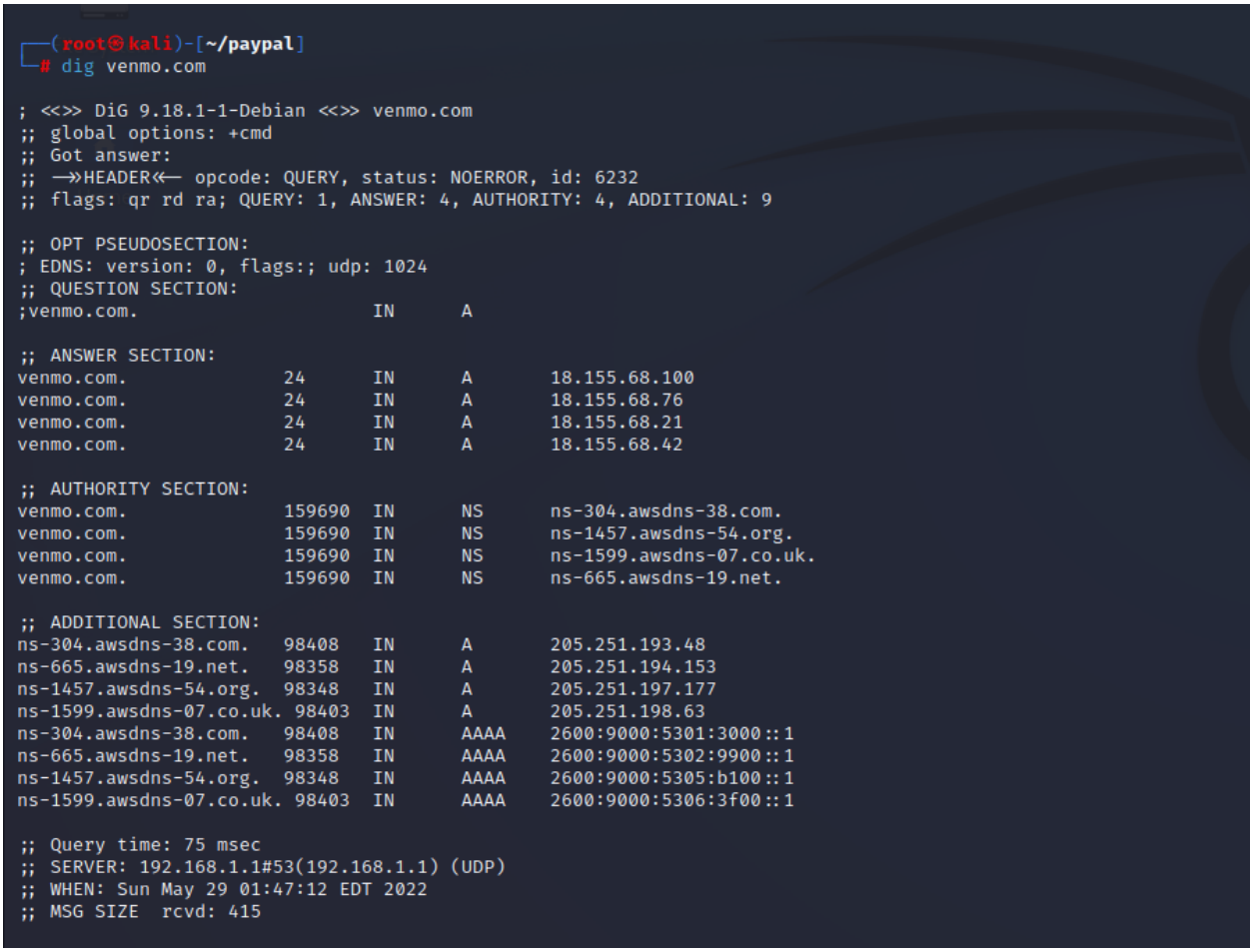
- ✓ .xoom.com



In here, I found Ip addresses of ‘xoom.com’ as 64.4.250.3 and 64.4.250.3. And also authority section we can see four authoritative Dns servers and additional section shows their Ip addresses.

- ❖ pdns100.ultradns.com.
- ❖ ns1.p134.dynect.net.
- ❖ pdns100.ultradns.net.
- ❖ ns2.p134.dynect.net.

- ✓ .venmo.com



```
┌──(root㉿kali)-[~/paypal]
└─# dig venmo.com

; <<>> DiG 9.18.1-1-Debian <<>> venmo.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6232
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1024
;; QUESTION SECTION:
;venmo.com.                     IN      A

;; ANSWER SECTION:
venmo.com.              24      IN      A       18.155.68.100
venmo.com.              24      IN      A       18.155.68.76
venmo.com.              24      IN      A       18.155.68.21
venmo.com.              24      IN      A       18.155.68.42

;; AUTHORITY SECTION:
venmo.com.              159690  IN      NS      ns-304.awsdns-38.com.
venmo.com.              159690  IN      NS      ns-1457.awsdns-54.org.
venmo.com.              159690  IN      NS      ns-1599.awsdns-07.co.uk.
venmo.com.              159690  IN      NS      ns-665.awsdns-19.net.

;; ADDITIONAL SECTION:
ns-304.awsdns-38.com.   98408   IN      A       205.251.193.48
ns-665.awsdns-19.net.   98358   IN      A       205.251.194.153
ns-1457.awsdns-54.org.  98348   IN      A       205.251.197.177
ns-1599.awsdns-07.co.uk. 98403  IN      A       205.251.198.63
ns-304.awsdns-38.com.   98408   IN      AAAA    2600:9000:5301:3000::1
ns-665.awsdns-19.net.   98358   IN      AAAA    2600:9000:5302:9900::1
ns-1457.awsdns-54.org.  98348   IN      AAAA    2600:9000:5305:b100::1
ns-1599.awsdns-07.co.uk. 98403  IN      AAAA    2600:9000:5306:3f00::1

;; Query time: 75 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun May 29 01:47:12 EDT 2022
;; MSG SIZE  rcvd: 415
```

In here, I found four Ip addresses for “venmo.com’ and four authoritative DNS servers.

Ip addresses: 13.224.250.26, 13.224.250.68, 13.224.250.83, 13.224.250.38

Dns servers:

- ns-1599.awsdns-07.co.uk.
- ns-304.awsdns-38.com.
- ns-1457.awsdns-54.org.
- ns-665.awsdns-19.net.

- ✓ paypal.me

```
┌──(root㉿kali)-[~/paypal]
└─# dig paypal.me

; <<>> DiG 9.18.1-1-Debian <<>> paypal.me
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 54728
;; flags: qr rd ra ad; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;paypal.me.                     IN      A

;; ANSWER SECTION:
paypal.me.              184     IN      A       64.4.250.36
paypal.me.              184     IN      A       64.4.250.37

;; Query time: 16 msec
;; SERVER: 192.168.43.1#53(192.168.43.1) (UDP)
;; WHEN: Mon May 30 12:44:46 EDT 2022
;; MSG SIZE  rcvd: 59
```

In here, 65.4.250.36 and 64.4.250.37 Ip addresses are pointed to “paypal.me”. This is same as “paypal.com” and “xoom.com” Ip addresses.

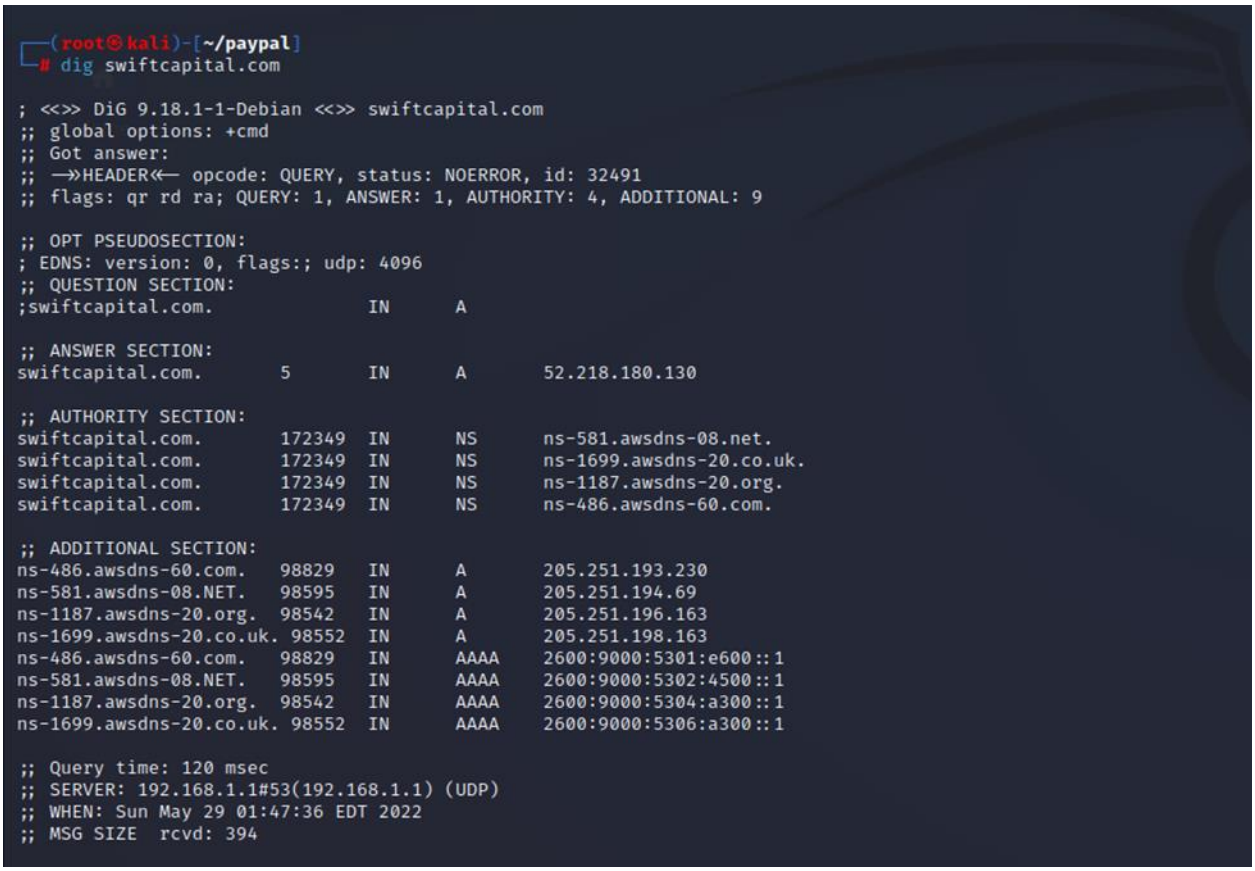
```
┌──(root㉿kali)-[~/paypal]
└─# dig paypal.me ns

; <<>> DiG 9.18.1-1-Debian <<>> paypal.me ns
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42718
;; flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1280
; COOKIE: d9f3293740c205b72cbcfdcd6295034451422fc7b94bdb9a (good)
;; QUESTION SECTION:
;paypal.me.                     IN      NS

;; ANSWER SECTION:
paypal.me.              300     IN      NS      pdns100.ultradns.com.
paypal.me.              300     IN      NS      ns1.p57.dynect.net.
paypal.me.              300     IN      NS      ns2.p57.dynect.net.
paypal.me.              300     IN      NS      pdns100.ultradns.net.

;; Query time: 99 msec
;; SERVER: 192.168.43.1#53(192.168.43.1) (UDP)
;; WHEN: Mon May 30 13:29:29 EDT 2022
;; MSG SIZE  rcvd: 181
```

“paypal.me” also has four authoritative DNS servers.

- ❖ pdns100.ultradns.com.
- ❖ ns1.p57.dynect.net.

- ns2.p57.dynect.net.
- pdns100.ultradns.net.

- ✓ swiftcapital.com



Swiftcapital.com has point to the 52.218.180.130 Ip address. And also, there are four authoritative DNS servers.

- ns-1187.awsdns-20.org.
- ns-486.awsdns-60.com.
- ns-581.awsdns-08.net.
- ns-1699.awsdns-20.co.uk.

Subdomain Enumeration

The process of enumerating valid subdomains for a domain is known as subdomain enumeration. This is done to broaden our attack surface and find more potential sites of weakness.

7) Subfinder

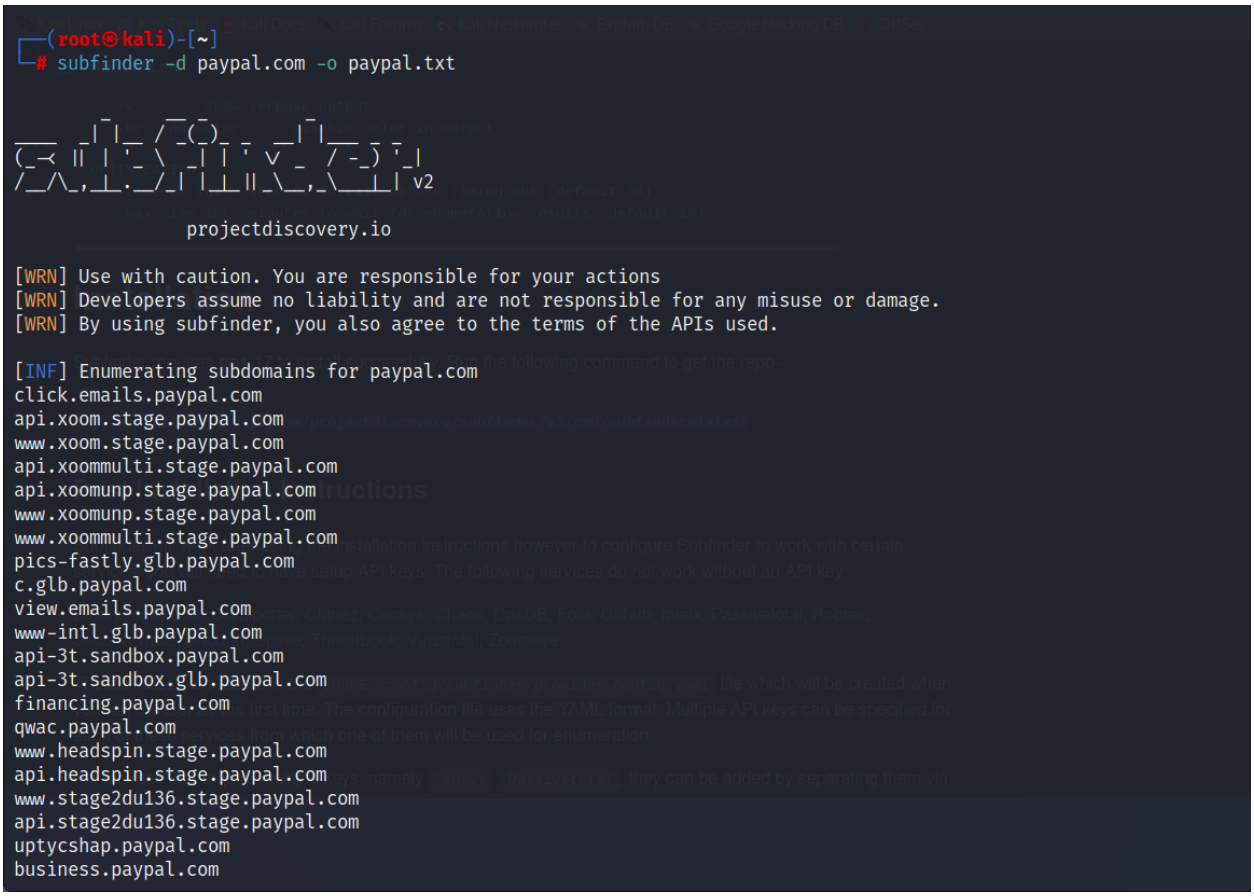
Subfinder is a subdomain enumeration tool that discovers valid subdomains for websites.

Installation

1. tar -xzvf subfinder-linux-amd64.tar.gz
2. mv Subfinder /usr/bin/subfinder
3. subfinder

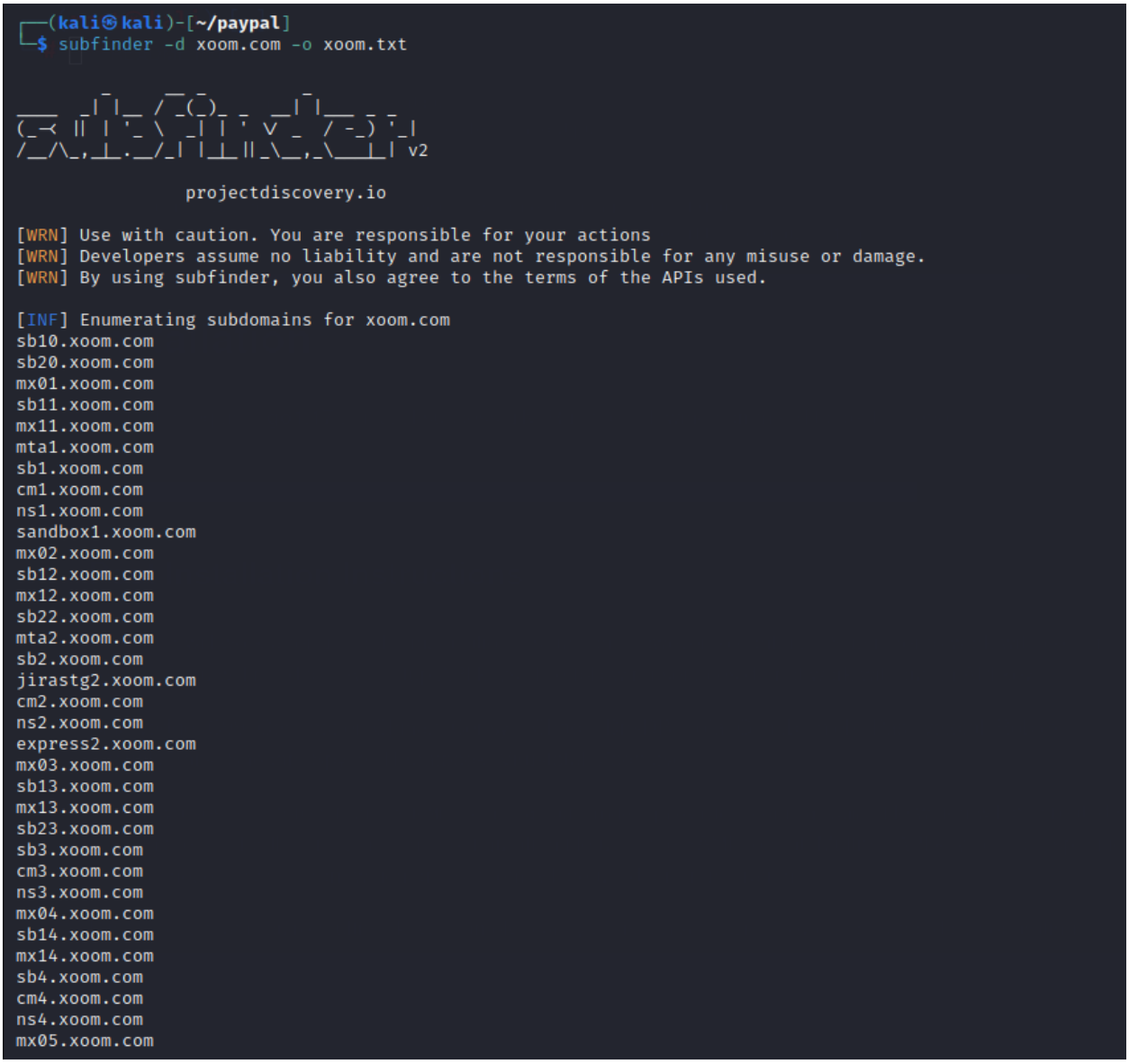
Results

- ✓ paypal.com



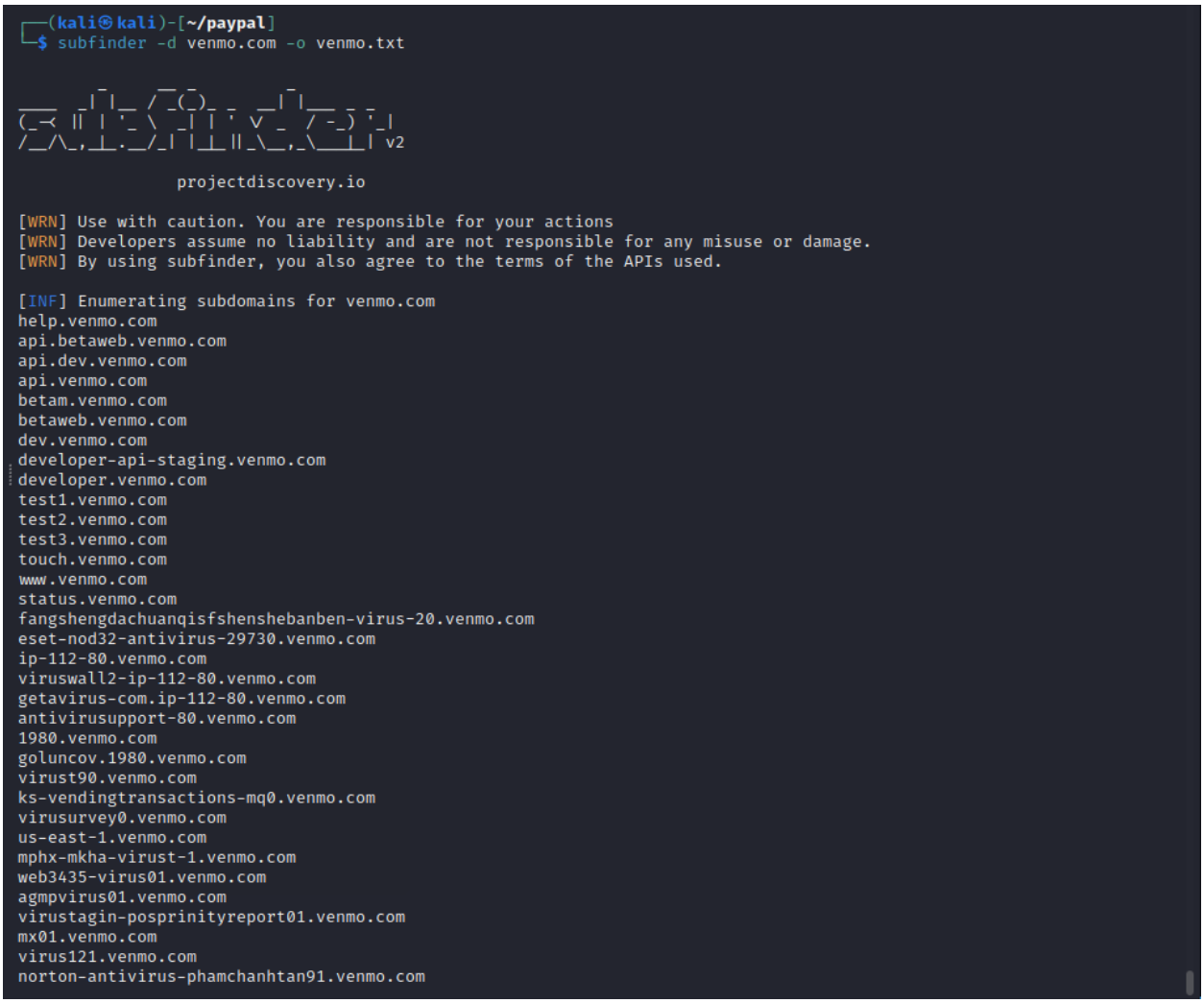
I found 3581 subdomains for “paypal.com”.

- ✓ xoom.com



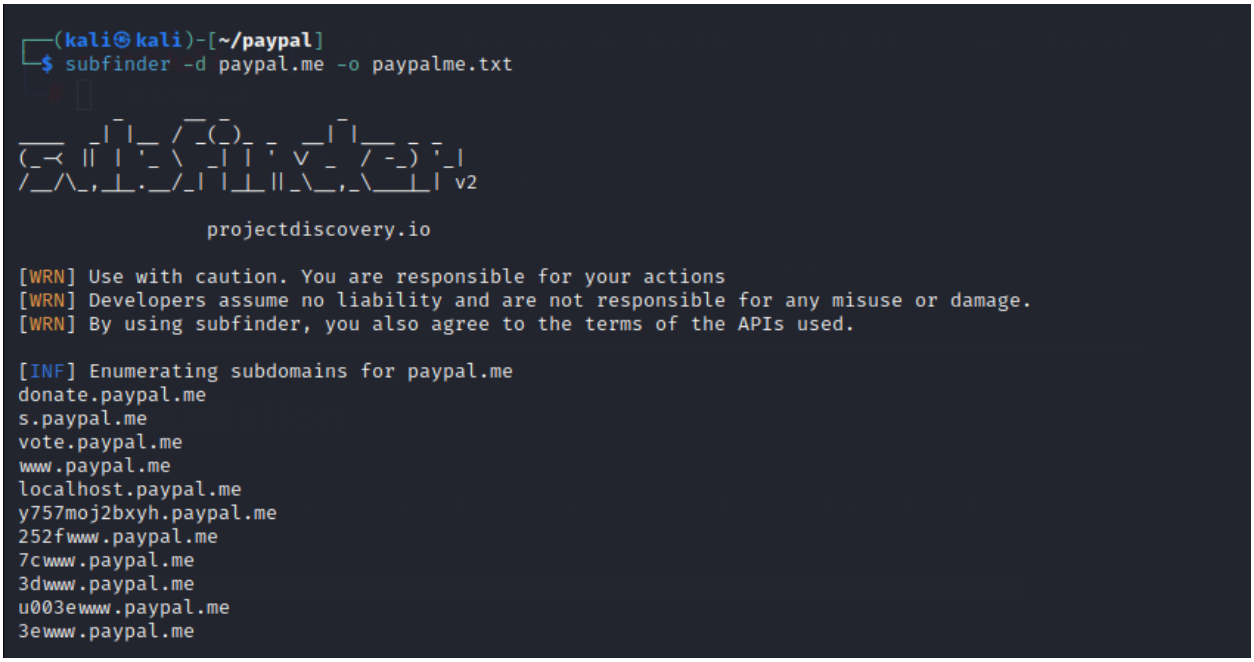
I found 1479 subdomains for “xoom.com”.

- ✓ venmo.com



I found 21703 subdomains for “venmo.com”.

✓ paypal.me



I found only 11 subdomains for “paypal.me”

✓ Swiftcapital.com

```
┌──(kali㉿kali)-[~/paypal]
└─$ subfinder -d swiftcapital.com -o swiftcapital.txt

               __    _____           __         
   _______  __/ /_  / __(_)___  ____/ /__  _____
  / ___/ / / / __ \/ /_/ / __ \/ __  / _ \/ ___/
 (__  ) /_/ / /_/ / __/ / / / / /_/ /  __/ /    
/____/\__,_/_.___/_/ /_/_/ /_/\__,_/\___/_/ v2

                projectdiscovery.io

[WRN] Use with caution. You are responsible for your actions
[WRN] Developers assume no liability and are not responsible for any misuse or damage.
[WRN] By using subfinder, you also agree to the terms of the APIs used.

[INF] Enumerating subdomains for swiftcapital.com
go.swiftcapital.com
sip.swiftcapital.com
autodiscover.swiftcapital.com
www.swiftcapital.com
mail.swiftcapital.com
customer.swiftcapital.com
dev.swiftcapital.com
info.swiftcapital.com
internal.swiftcapital.com
ist.swiftcapital.com
logging.swiftcapital.com
remote.swiftcapital.com
sandbox.swiftcapital.com
sbx.swiftcapital.com
secure.swiftcapital.com
swiftcapital.com
swiftowa.swiftcapital.com
szdev.swiftcapital.com
szist.swiftcapital.com
szuat.swiftcapital.com
szwww.swiftcapital.com
test.swiftcapital.com
test.webservices.swiftcapital.com
try.swiftcapital.com
uat.swiftcapital.com
webservices.swiftcapital.com
www.try.swiftcapital.com
content.swiftcapital.com
my.swiftcapital.com
vip.swiftcapital.com
msoid.swiftcapital.com
lyncdiscover.swiftcapital.com
enterpriseregistration.swiftcapital.com
enterpriseenrollment.swiftcapital.com
api.swiftcapital.com
```

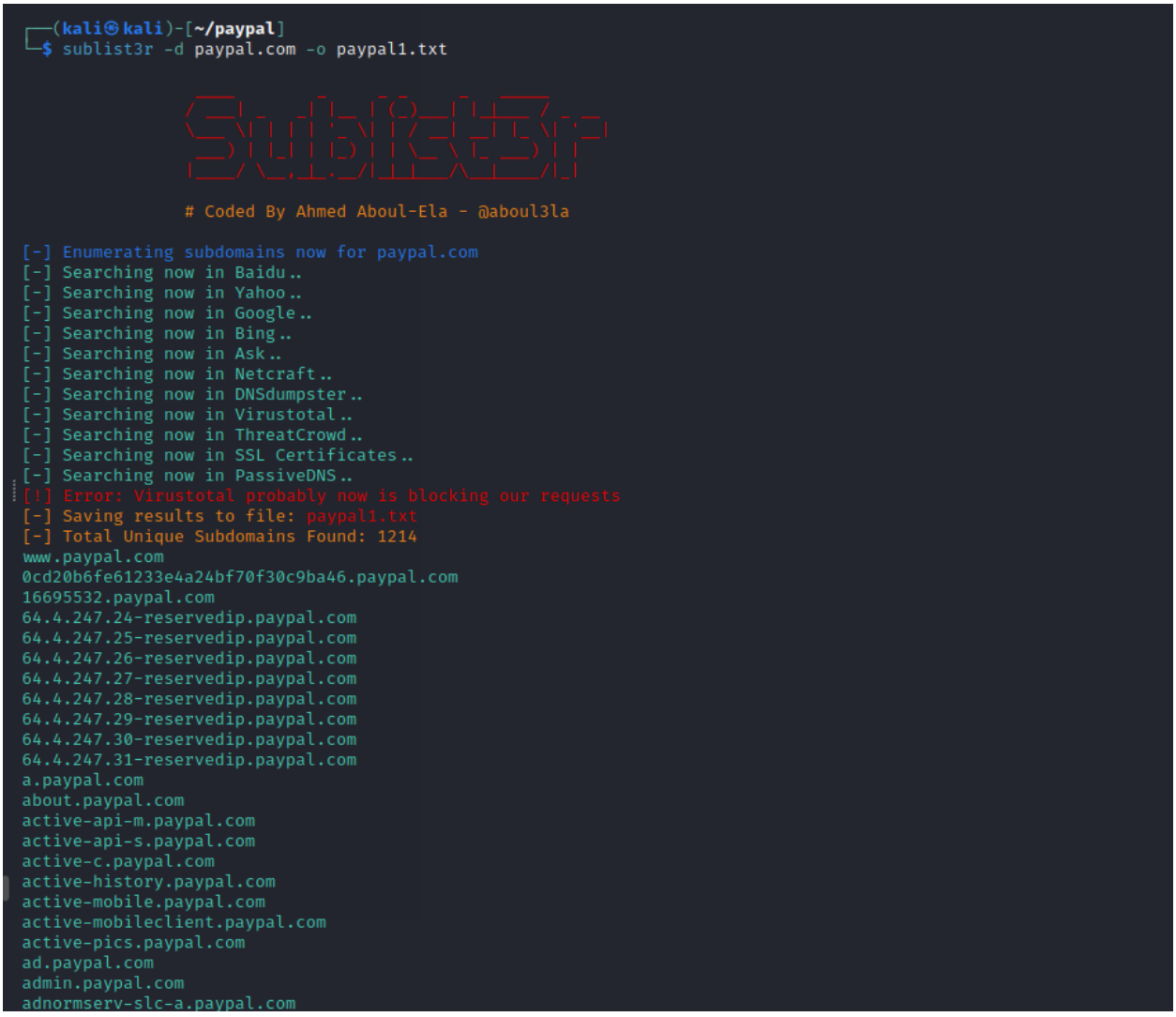
I found 40 subdomains for “swiftcapital.com”.

8) Sublist3r

Results

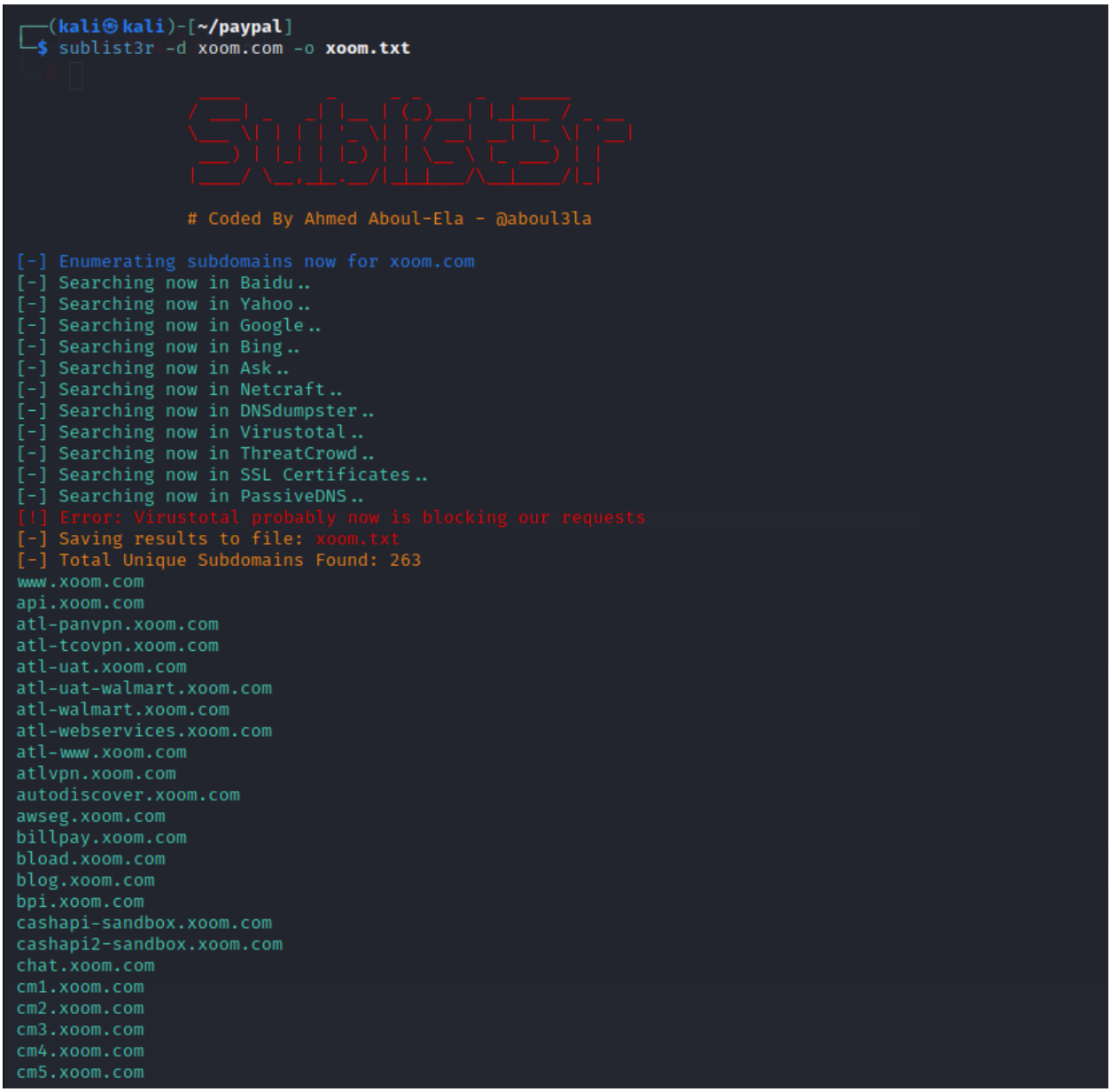
✓ Paypal.com

I got following result after scanning.



✓ xoom.com

I got following result after scanning.



- ✓ venmo.com

I got following results after scanning “venmo.com”.

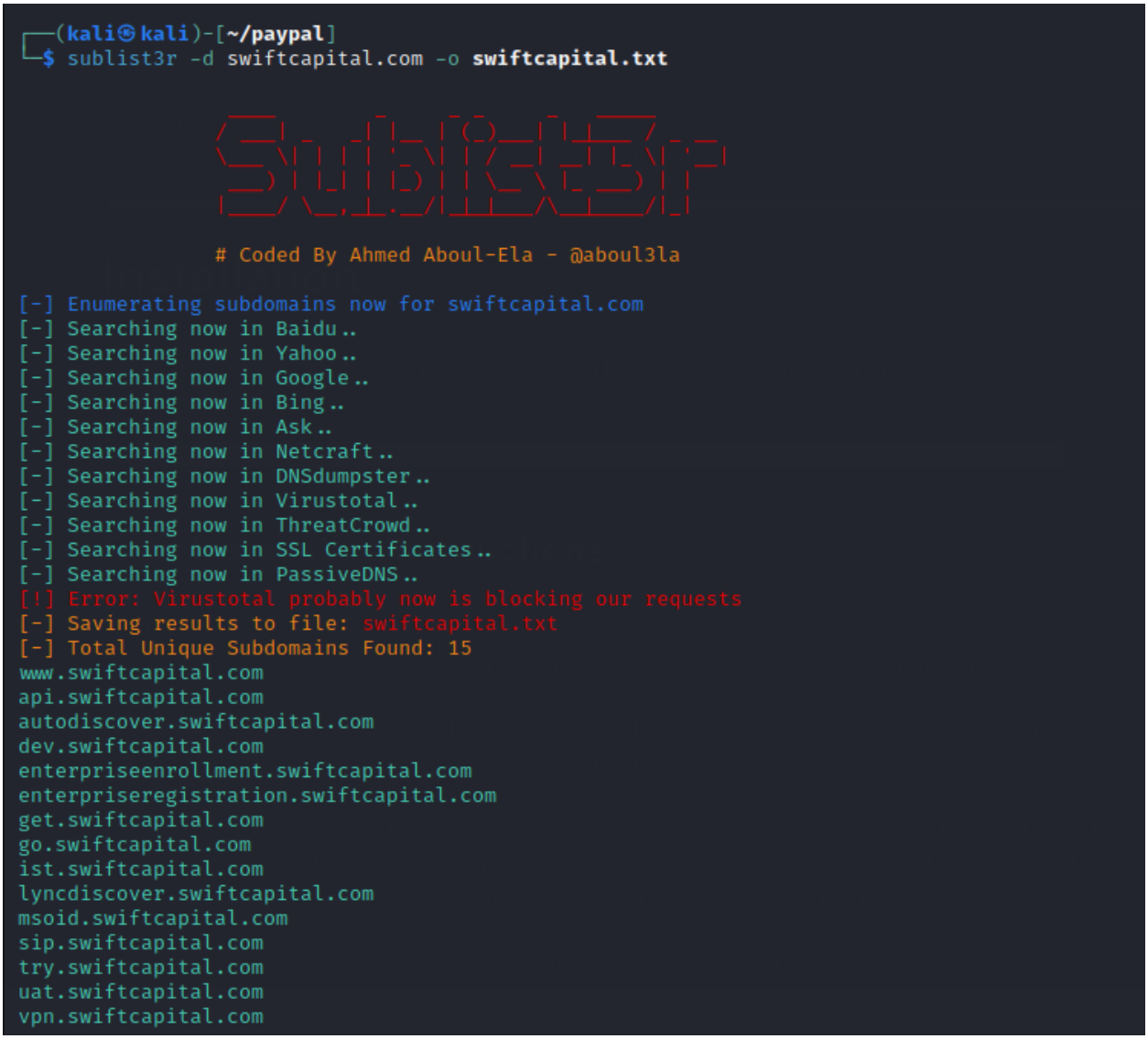
```
┌──(kali㉿kali)-[~/paypal]
└─$ sublist3r -d venmo.com -o venmo.txt
                 ____        _ _     _   _____
                / ___| _   _| | |__ | (_)___  / _ __
                \___ \| | | | | '_ \| | |  / / | '__|
                 ___) | |_| | | |_) | | | / /__| |_ \| '_|
                |____/ \__,_|_|_.__/|_|_|/____/\__|_| |_|

                # Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for venmo.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Saving results to file: venmo.txt
[-] Total Unique Subdomains Found: 5
o725.abmail.email.venmo.com
o726.abmail.email.venmo.com
o727.abmail.email.venmo.com
o728.abmail.email.venmo.com
o729.abmail.email.venmo.com
```

- ✓ paypal.me

I got following result after scanning “paypal.me”.

- ✓ swiftcapital.com

I got following result after scanning “swiftcapital.com”.

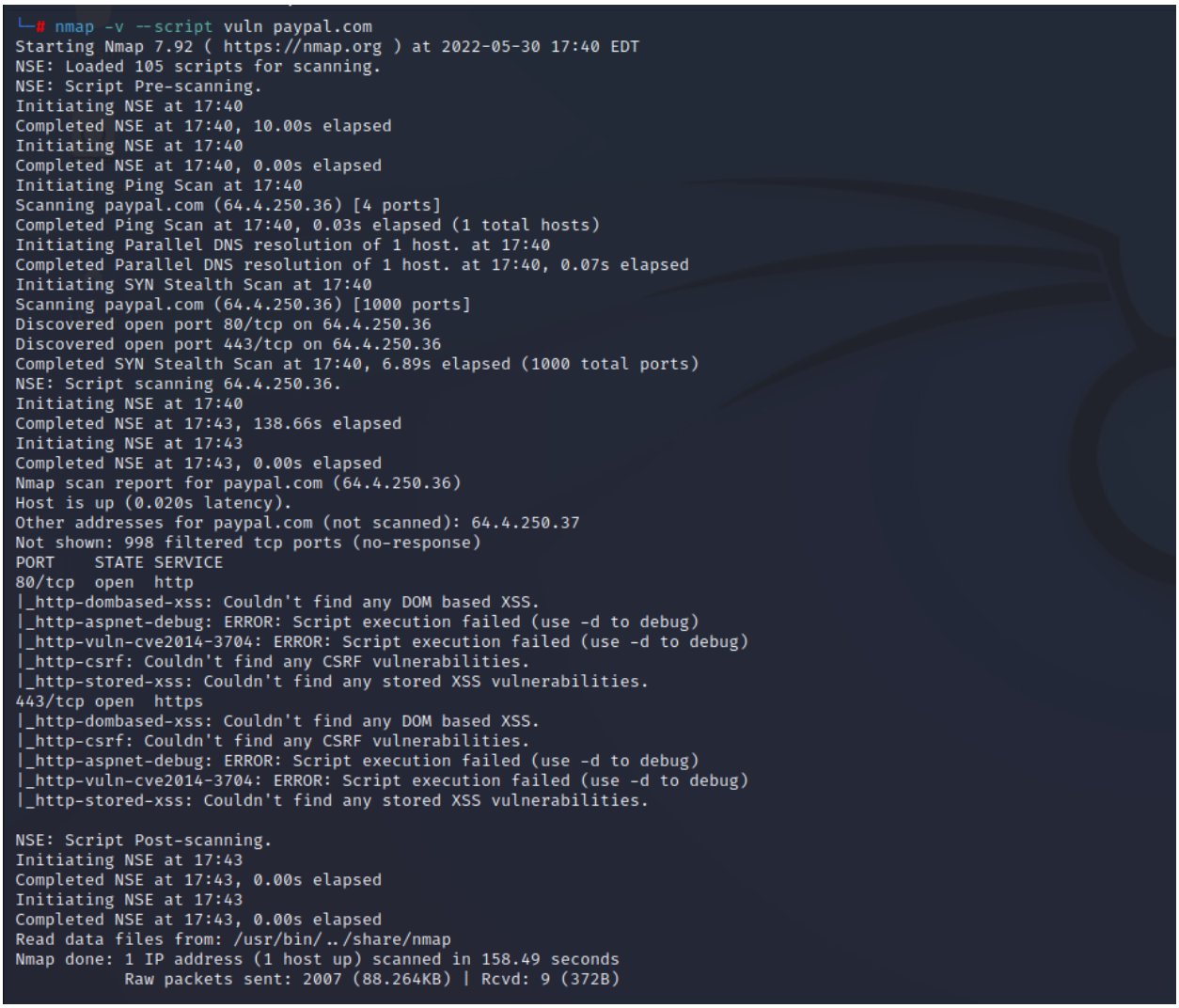


9) Nmap

Nmap is a tool which use to identify services, open ports, host name and vulnerabilities.

Results

- ✓ .paypal.com



```
└─# nmap -v --script vuln paypal.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 17:40 EDT
NSE: Loaded 105 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:40
Completed NSE at 17:40, 10.00s elapsed
Initiating NSE at 17:40
Completed NSE at 17:40, 0.00s elapsed
Initiating Ping Scan at 17:40
Scanning paypal.com (64.4.250.36) [4 ports]
Completed Ping Scan at 17:40, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:40
Completed Parallel DNS resolution of 1 host. at 17:40, 0.07s elapsed
Initiating SYN Stealth Scan at 17:40
Scanning paypal.com (64.4.250.36) [1000 ports]
Discovered open port 80/tcp on 64.4.250.36
Discovered open port 443/tcp on 64.4.250.36
Completed SYN Stealth Scan at 17:40, 6.89s elapsed (1000 total ports)
NSE: Script scanning 64.4.250.36.
Initiating NSE at 17:40
Completed NSE at 17:43, 138.66s elapsed
Initiating NSE at 17:43
Completed NSE at 17:43, 0.00s elapsed
Nmap scan report for paypal.com (64.4.250.36)
Host is up (0.020s latency).
Other addresses for paypal.com (not scanned): 64.4.250.37
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE
80/tcp  open  http
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
443/tcp open  https
|_http-dombased-xss: Couldn't find any DOM based XSS.
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-aspnet-debug: ERROR: Script execution failed (use -d to debug)
|_http-vuln-cve2014-3704: ERROR: Script execution failed (use -d to debug)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.

NSE: Script Post-scanning.
Initiating NSE at 17:43
Completed NSE at 17:43, 0.00s elapsed
Initiating NSE at 17:43
Completed NSE at 17:43, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 158.49 seconds
           Raw packets sent: 2007 (88.264KB) | Rcvd: 9 (372B)
```

This scan shows that http port 80 and https port 443 are open.

- ✓ .xoom.com

```
┌──(root㉿kali)-[~]
└─# nmap -sV xoom.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-30 23:57 EDT
Nmap scan report for xoom.com (64.4.250.37)
Host is up (0.029s latency).
Other addresses for xoom.com (not scanned): 64.4.250.36
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.96 seconds
```

This also port 80 and port 443 are open.

- ✓ .venmo.com

```
┌──(root㉿kali)-[~]
└─# nmap -sV venmo.com
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-31 00:12 EDT
Nmap scan report for venmo.com (18.155.68.76)
Host is up (0.014s latency).
Other addresses for venmo.com (not scanned): 18.155.68.100 18.155.68.42 18.155.68.21
rDNS record for 18.155.68.76: server-18-155-68-76.sin52.r.cloudfront.net
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE    VERSION
80/tcp  open  tcpwrapped
443/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

This also port 80 and port 443 are open.

- ✓ paypal.me

```
┌──(root㉿kali)-[~]
└─# nmap paypal.me -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-31 00:30 EDT
Nmap scan report for paypal.me (64.4.250.37)
Host is up (0.023s latency).
Other addresses for paypal.me (not scanned): 64.4.250.36
rDNS record for 64.4.250.37: xoom.com
Not shown: 998 filtered tcp ports (no-response)
PORT    STATE SERVICE   VERSION
80/tcp  open  http
443/tcp open  ssl/https
```

This also port 80 and 443 are open.

- ✓ www.swiftcapital.com

```
┌──(root㉿kali)-[~]
└─# nmap swiftcapital.com  -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2022-05-31 00:33 EDT
Nmap scan report for swiftcapital.com (52.218.212.211)
Host is up (0.049s latency).
rDNS record for 52.218.212.211: s3-website-us-west-2.amazonaws.com
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
80/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.52 seconds
```

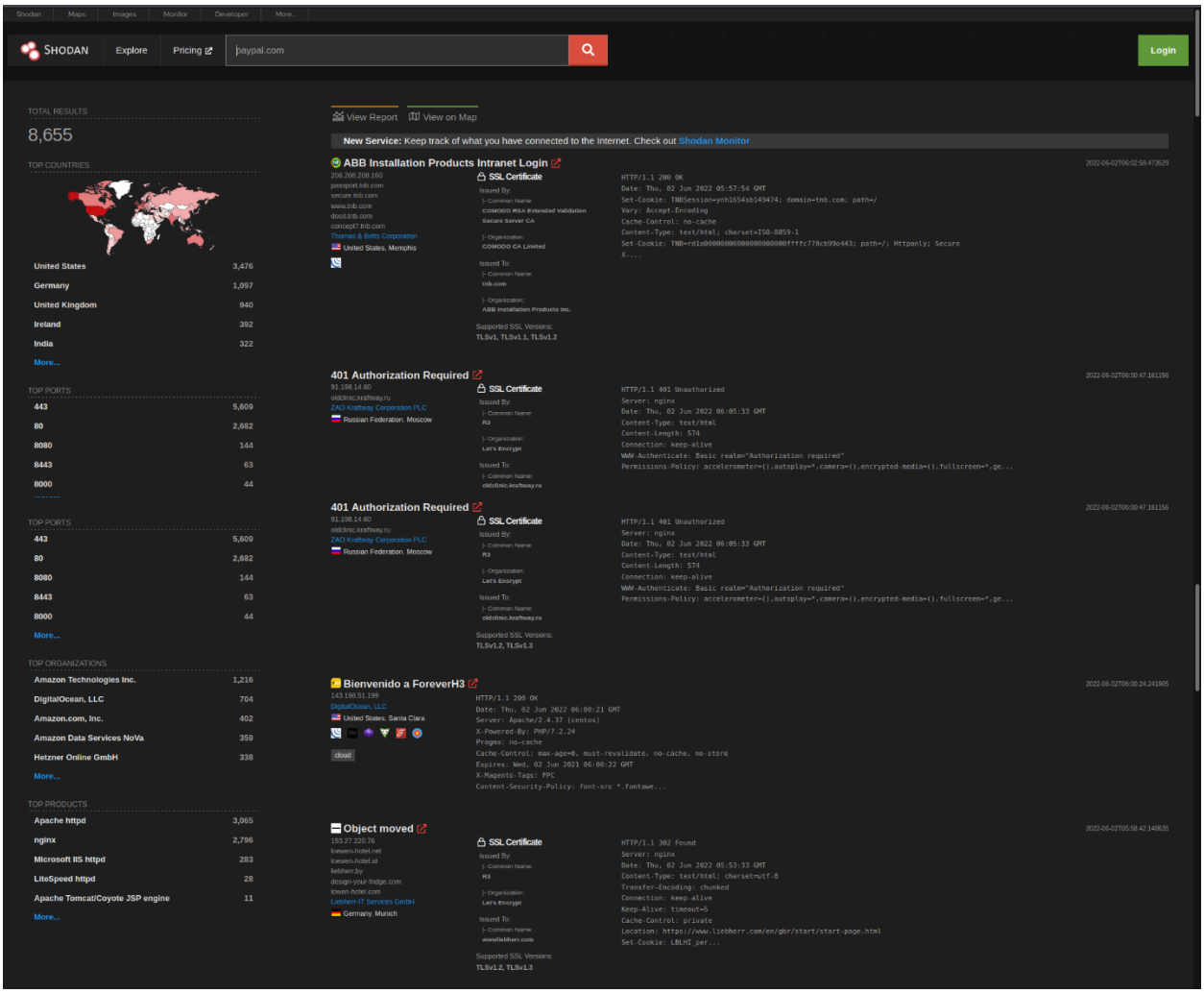
In here, only port 80 is open.

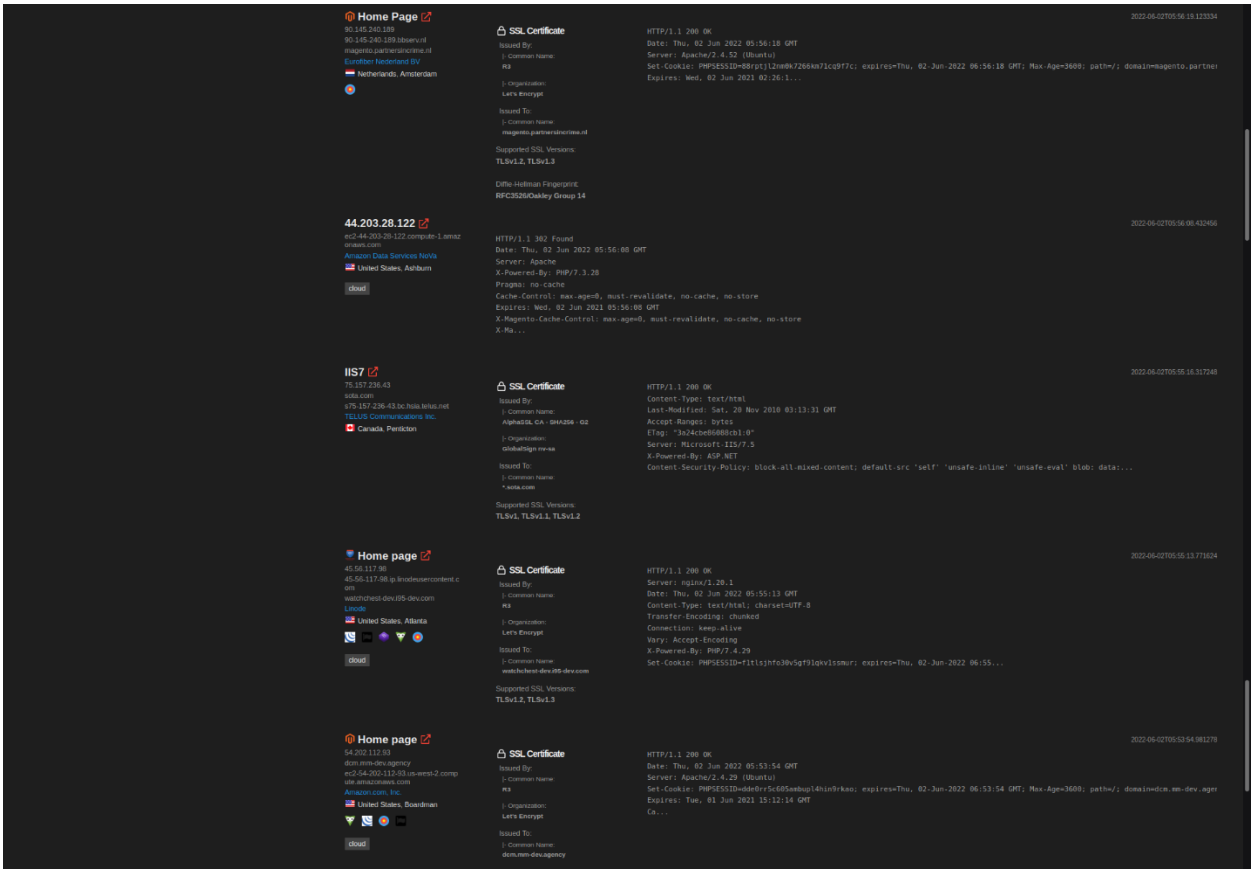
10) Shodan.io

Shodan is a websites scan engine. We can use it to locate different forms of computer systems related to the net the use of numerous filters. Shodan offers absolutely legal provider that collects facts that become already to be had to the public. The metadata for numerous IOT gadgets is already broadcast online, and Shodan definitely reviews what it finds.

Results:

Paypal.com





These are the results I got for “paypal.com”. I did scan for other 4 domains like this.

Vulnerability Scan

After find information about domains, we need to find vulnerabilities in that domains. So that we need to perform vulnerability scanning.

1. Netsparker

Netsparker is a fully automated and fully configurable web security scanning tool. It allows you to experiment websites, internet applications, services, and discover protection flaws. Netsparker can scan any kind of web applications.

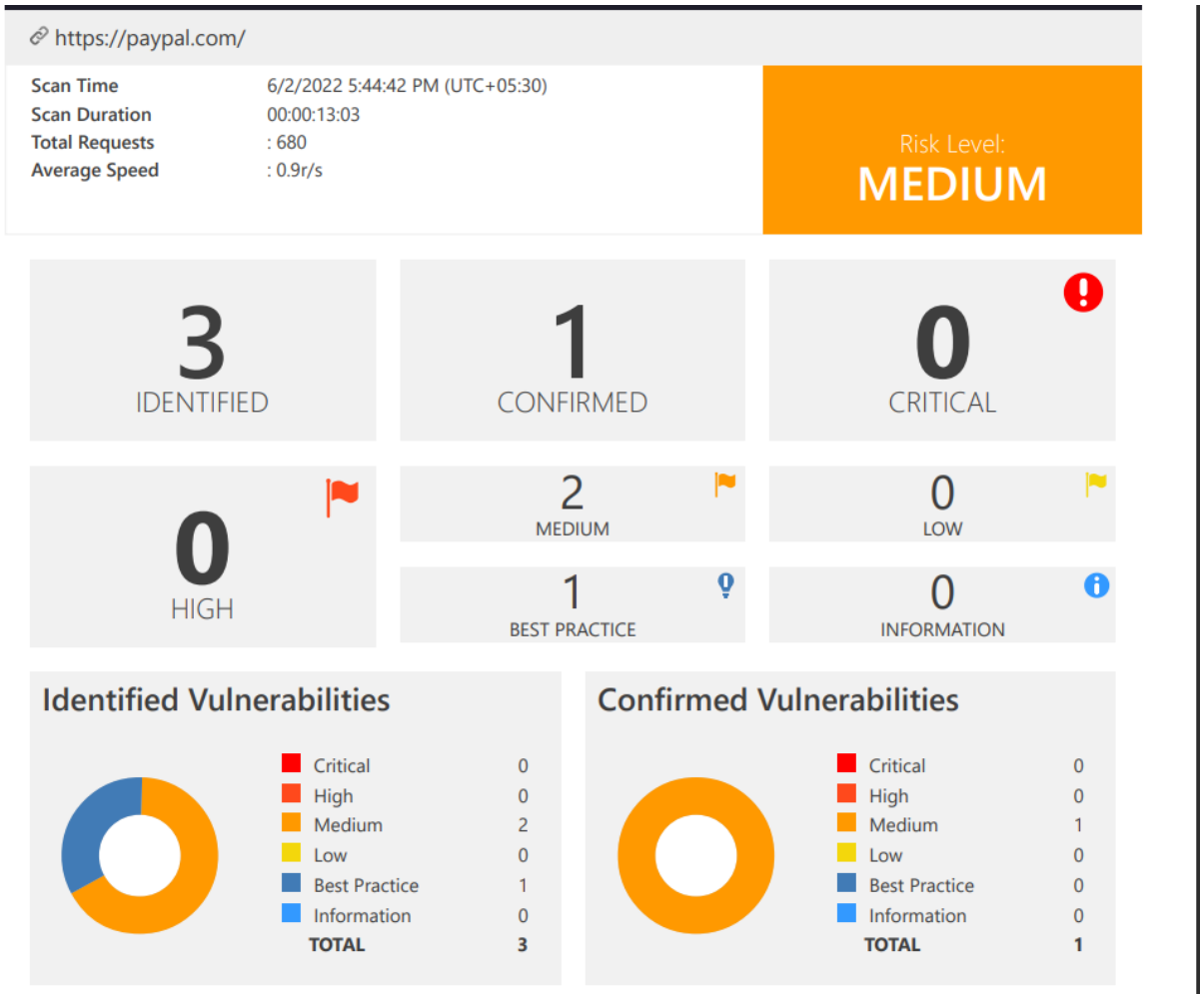
Netsparker is the only scanner that automatically exploits diagnosed vulnerabilities in a read-most effective and secure way, with a view to verify diagnosed issues.

Netsparker can identify following vulnerabilities.

- SQL Injection
- Boolean SQL Injection
- Blind SQL Injection
- Remote File Inclusion
- Command Injection
- Blind Command Injection
- XXE Injection
- Remote Code Evaluation
- Local File Inclusion
- Server-side Template Injection
- Remote Code Execution
- Injection through Local File Inclusion

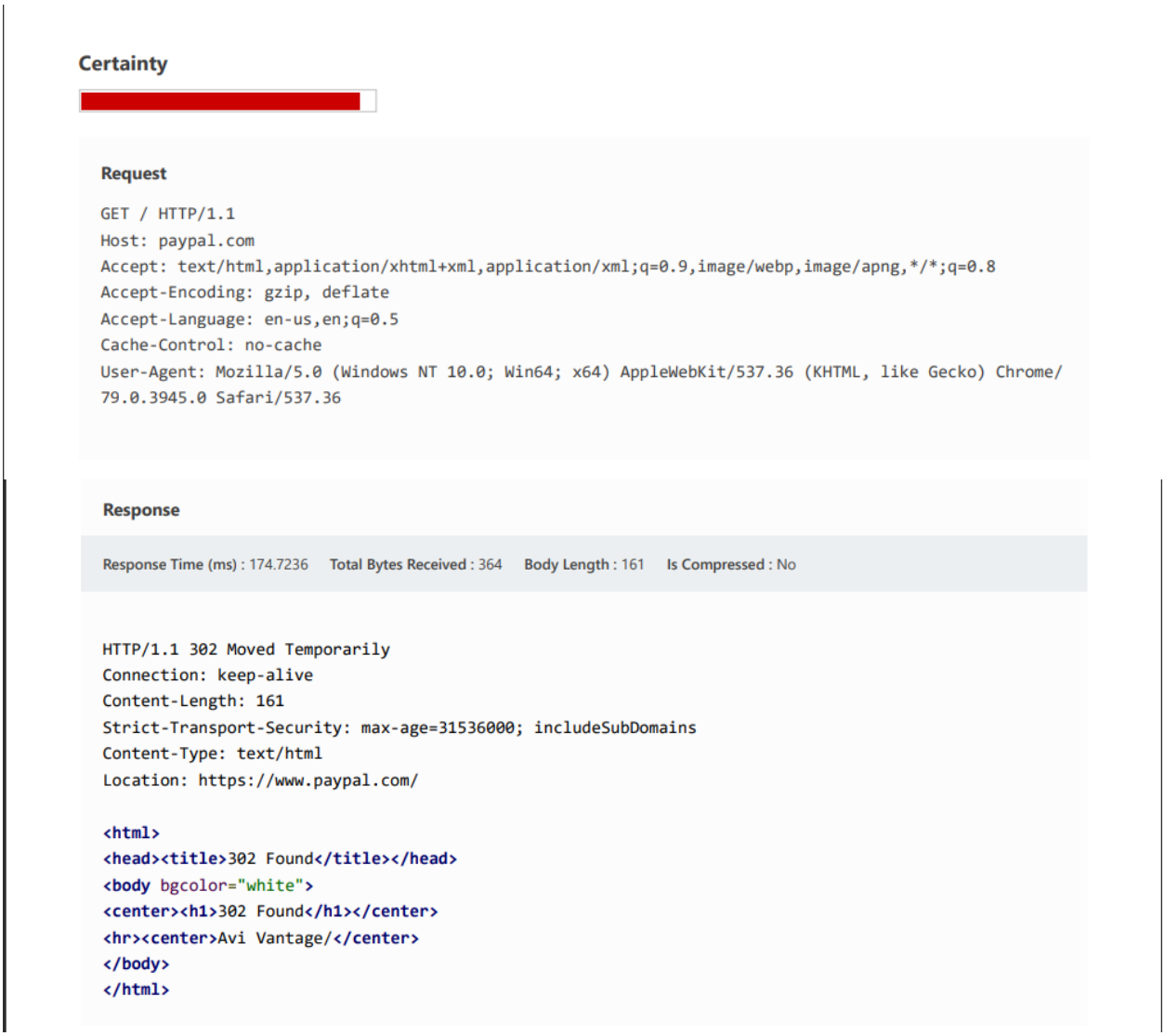
Results:

✓ Paypal.com



Netsparker found following vulnerabilities.

1. HTTP Strict Transport Security (HSTS) Errors and Warnings



Impact

The HSTS Warning and Error may allow attackers to avoid HSTS, allowing them to view and change your website communications.

How to prevent

You should take care of them as quickly as possible. You might want to rescan after you've done this to be sure they're gone.

2. Weak Ciphers Enabled

List of Supported Weak Ciphers

- TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
- TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
- TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
- TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
- TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009C)
- TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009D)

Impact

SSL traffic may be decrypted by attackers.

How to prevent

1) For Apache, you should modify the SSLCipherSuite directive in the httpd.conf.

```
SSLCipherSuite HIGH:MEDIUM:!MD5:!RC4
```

2) Lighttpd:

```
ssl.honor-cipher-order = "enable"

ssl.cipher-list = "EECDH+AESGCM:EDH+AESGCM"
```

Changes to the system registry are required for Microsoft IIS. The registry can be badly damaged if it is edited incorrectly. You should back up any important data on your computer before performing registry modifications.

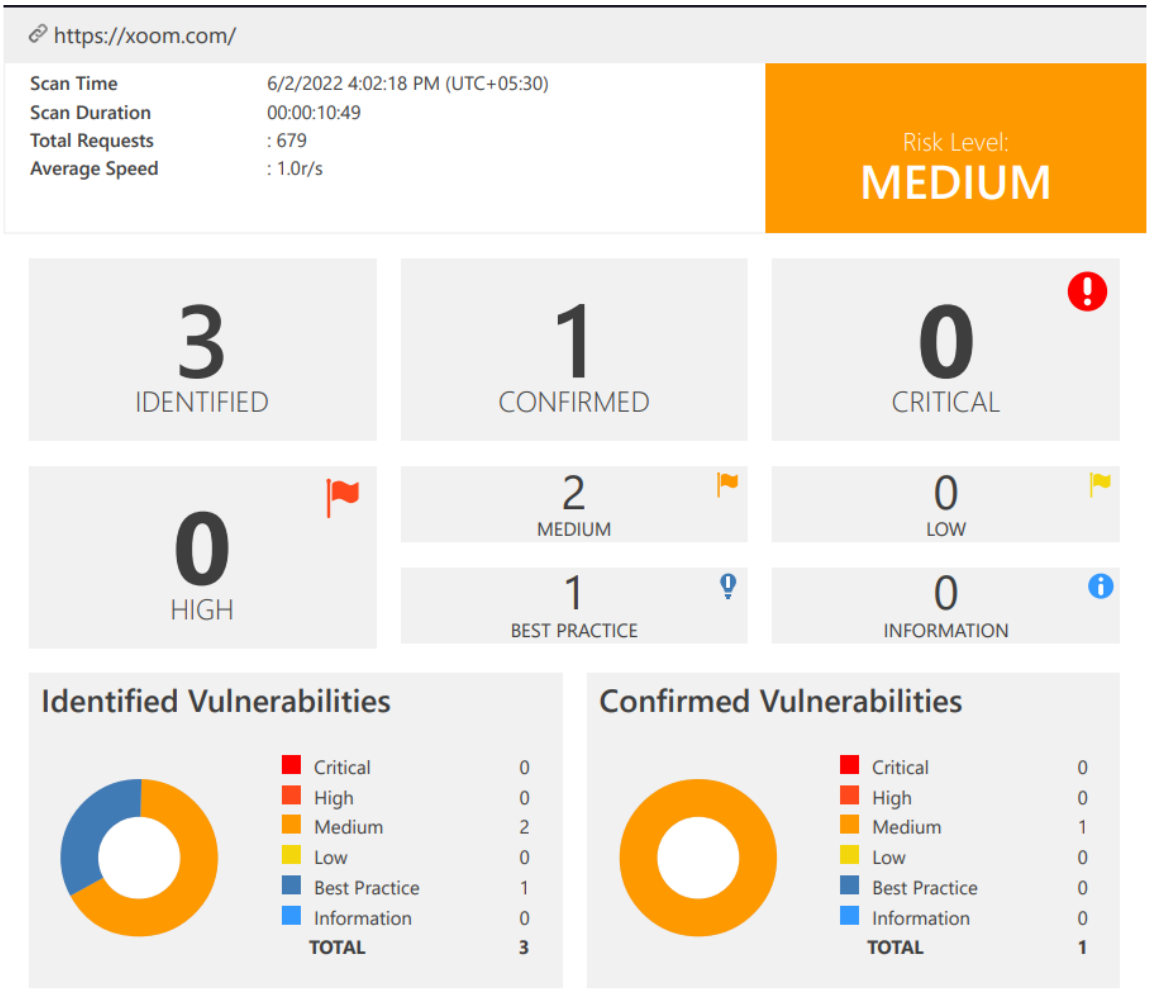
a.Click Start, click Run, type `regedt32`or type `regedit`, and then click OK.
b.In Registry Editor, locate the following registry key: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders`
c.Set "Enabled" DWORD to "0x0" for the following registry keys:

```
SCHANNEL\Ciphers\DES 56/56
SCHANNEL\Ciphers\RC4 64/128
SCHANNEL\Ciphers\RC4 40/128
SCHANNEL\Ciphers\RC2 56/128
SCHANNEL\Ciphers\RC2 40/128
SCHANNEL\Ciphers\NULL
SCHANNEL\Hashes\MD5
```

3. Expect-CT Not Enabled

CT stands for Certificate Transparency. CT is a technology that makes not possible for a certificates authority to give an SSL certificate for a website without the certificates being seen to the proprietor of that domain. Implementing these functions which might be supported through all foremost browsers is a great exercise and could offer a further layer of safety on your application.

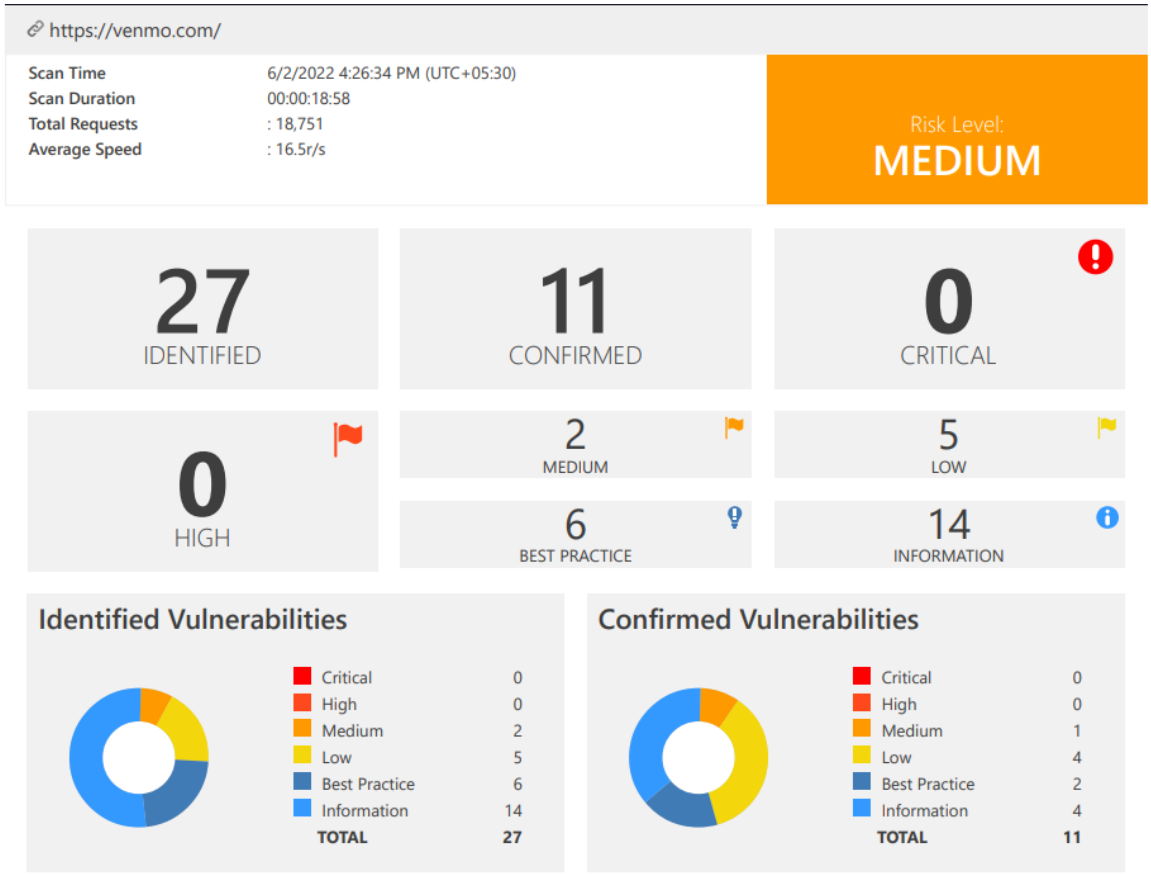
- ✓ Xoom.com



Netsparker found following vulnerabilities. These vulnerabilities same as "paypal.com" vulnerabilities.

- HTTP Strict Transport Security (HSTS) Errors and Warnings
- Weak Ciphers Enabled.
- Expect-CT Not Enabled.

✓ Venmo.com



Netsparker found following vulnerabilities.

Vulnerability Summary

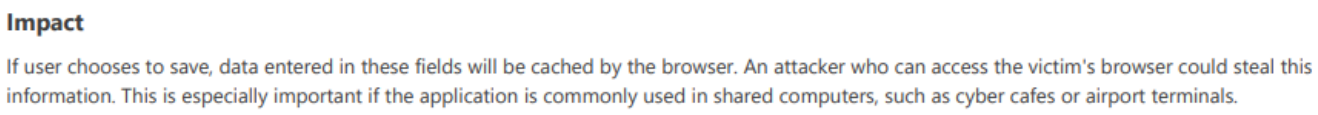
CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Errors and Warnings	GET	https://venmo.com/	No Parameters
	Weak Ciphers Enabled	GET	https://venmo.com/	No Parameters
	Missing X-Frame-Options Header	GET	https://venmo.com/	No Parameters
	Autocomplete is Enabled	GET	https://venmo.com/account/sign-in	No Parameters
	Cookie Not Marked as HttpOnly	GET	https://venmo.com/	No Parameters
	Cookie Not Marked as Secure	GET	https://venmo.com/	No Parameters
	Insecure Frame (External)	GET	https://venmo.com/about/crypto/	No Parameters
	Expect-CT Not Enabled	GET	https://venmo.com/	No Parameters
	Missing X-XSS-Protection Header	GET	https://venmo.com/static-assets/webpack-runtime-95acd141cdb6944ca139.js	No Parameters
	Referrer-Policy Not Implemented	GET	https://venmo.com/	No Parameters
	SameSite Cookie Not Implemented	GET	https://venmo.com/	No Parameters

Referrer-Policy Not Implemented	GET	https://venmo.com/	No Parameters
SameSite Cookie Not Implemented	GET	https://venmo.com/	No Parameters
Content Security Policy (CSP) Not Implemented	GET	https://venmo.com/	No Parameters
Subresource Integrity (SRI) Not Implemented	GET	https://venmo.com/	No Parameters
[Possible] Login Page Identified	GET	https://venmo.com/account/sign-in	No Parameters
Apple's App-Site Association (AASA) Detected	GET	https://venmo.com/.well-known/apple-app-site-association	No Parameters
Email Address Disclosure	GET	https://venmo.com/legal/us-user-agreement/	No Parameters
ExpressJS Identified	GET	https://venmo.com/(268409241-3136)	No Parameters
Generic Email Address Disclosure	GET	https://venmo.com/legal/us-privacy-policy/	No Parameters
Missing object-src in CSP Declaration	GET	https://venmo.com/static-assets/	No Parameters
Nginx Web Server Identified	GET	https://venmo.com/	No Parameters

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
Reverse Proxy Detected (Envoy)	GET	https://venmo.com/	No Parameters
Sitemap Detected	GET	https://venmo.com/sitemap.xml	No Parameters
Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://venmo.com/static-assets/	No Parameters
Autocomplete Enabled (Password Field)	GET	https://venmo.com/account/sign-in	No Parameters
Cross-site Referrer Leakage through usage of the origin keyword in Referrer-Policy	GET	https://venmo.com/account/sign-in	No Parameters
Forbidden Resource	GET	https://venmo.com/c:/boot.ini	No Parameters
Robots.txt Detected	GET	https://venmo.com/robots.txt	No Parameters

1) Autocomplete is Enabled

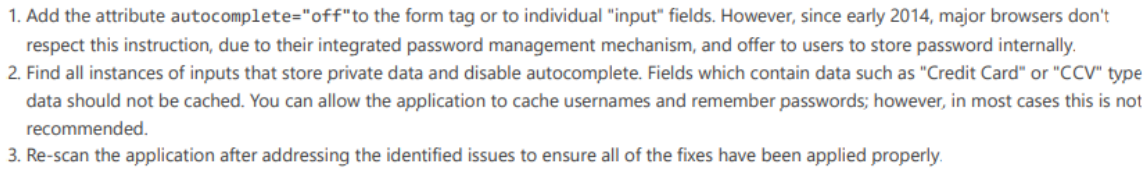
Impact:



Impact

If user chooses to save, data entered in these fields will be cached by the browser. An attacker who can access the victim's browser could steal this information. This is especially important if the application is commonly used in shared computers, such as cyber cafes or airport terminals.

How to prevent



1. Add the attribute `autocomplete="off"` to the form tag or to individual "input" fields. However, since early 2014, major browsers don't respect this instruction, due to their integrated password management mechanism, and offer to users to store password internally.
2. Find all instances of inputs that store private data and disable autocomplete. Fields which contain data such as "Credit Card" or "CCV" type data should not be cached. You can allow the application to cache usernames and remember passwords; however, in most cases this is not recommended.
3. Re-scan the application after addressing the identified issues to ensure all of the fixes have been applied properly.

2) Cookie Not Marked as HttpOnly and secure

Impact

During xss assaults, an attacker might simply access cookies and hijack the victim's session.

How to mitigate

Mark all of the cookies used by the application as HTTPOnly.

3) Insecure Frame (External)

Impact

IFrame sandboxing provides additional security for content inside a body, preventing potentially dangerous code from causing harm to the internet web page that embeds it.

The Same Origin Policy (SOP) prevents JavaScript code from one origin from accessing other sources' objects and functions, as well as HTTP replies from different origins. The access is best permitted if the protocol, port, and moreover the area are all identical.

Here is an example, the URLs below all belong to the same origin as *http://site.com*:

http://site.com
http://site.com/
http://site.com/my/page.html

Whereas the URLs mentioned below aren't from the same origin as *http://site.com*:

http://www.site.com (a sub domain)
http://site.org (different top level domain)
https://site.com (different protocol)
http://site.com:8080 (different port)

When the sandboxattribute is set, the iframe content is treated as being from a unique origin, even if its hostname, port and protocol match exactly. Additionally, sandboxed content is re-hosted in the browser with the following restrictions:

- Any kind of plugin, such as ActiveX, Flash, or Silverlight will be disabled for the iframe.
- Forms are disabled. The hosted content is not allowed to make forms post back to any target.
- Scripts are disabled. JavaScript is disabled and will not execute.
- Links to other browsing contexts are disabled. An anchor tag targeting different browser levels will not execute.
- Unique origin treatment. All content is treated under a unique origin. The content is not able to traverse the DOM or read cookie information.

When the sandboxattribute is not set or not configured correctly, your application might be at risk.

A compromised website that is loaded in such an insecure iframe might affect the parent web application. These are just a few examples of how such an insecure frame might affect its parent:

- It might trick the user into supplying a username and password to the site loaded inside the iframe.
- It might navigate the parent window to a phishing page.
- It might execute untrusted code.
- It could show a popup, appearing to come from the parent site.

Sandboxcontaining a value of :

- `allow-same-origin`will not treat it as a unique origin.
- `allow-top-navigation`will allow code in the iframe to navigate the parent somewhere else, e.g. by changing parent.location.
- `allow-forms`will allow form submissions from inside the iframe.
- `allow-popups`will allow popups.
- `allow-scripts`will allow malicious script execution however it won't allow to create popups.

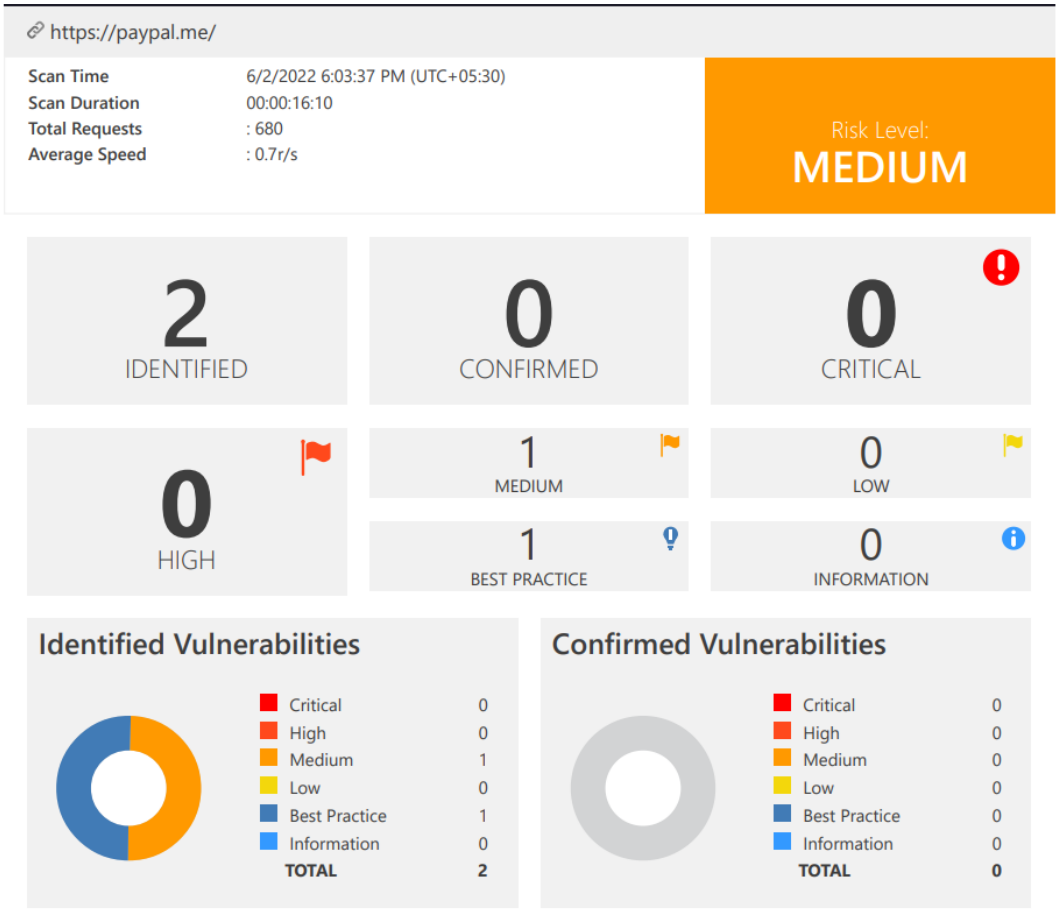
How to prevent

- Apply sandboxing in inline frame

```
<iframe sandbox src="framed-page-url"></iframe>
```

- For untrusted content, avoid the usage of `seamless`attribute and `allow-top-navigation`, `allow-popups`and `allow-scripts`in sandbox attribute.

✓ Paypal.me

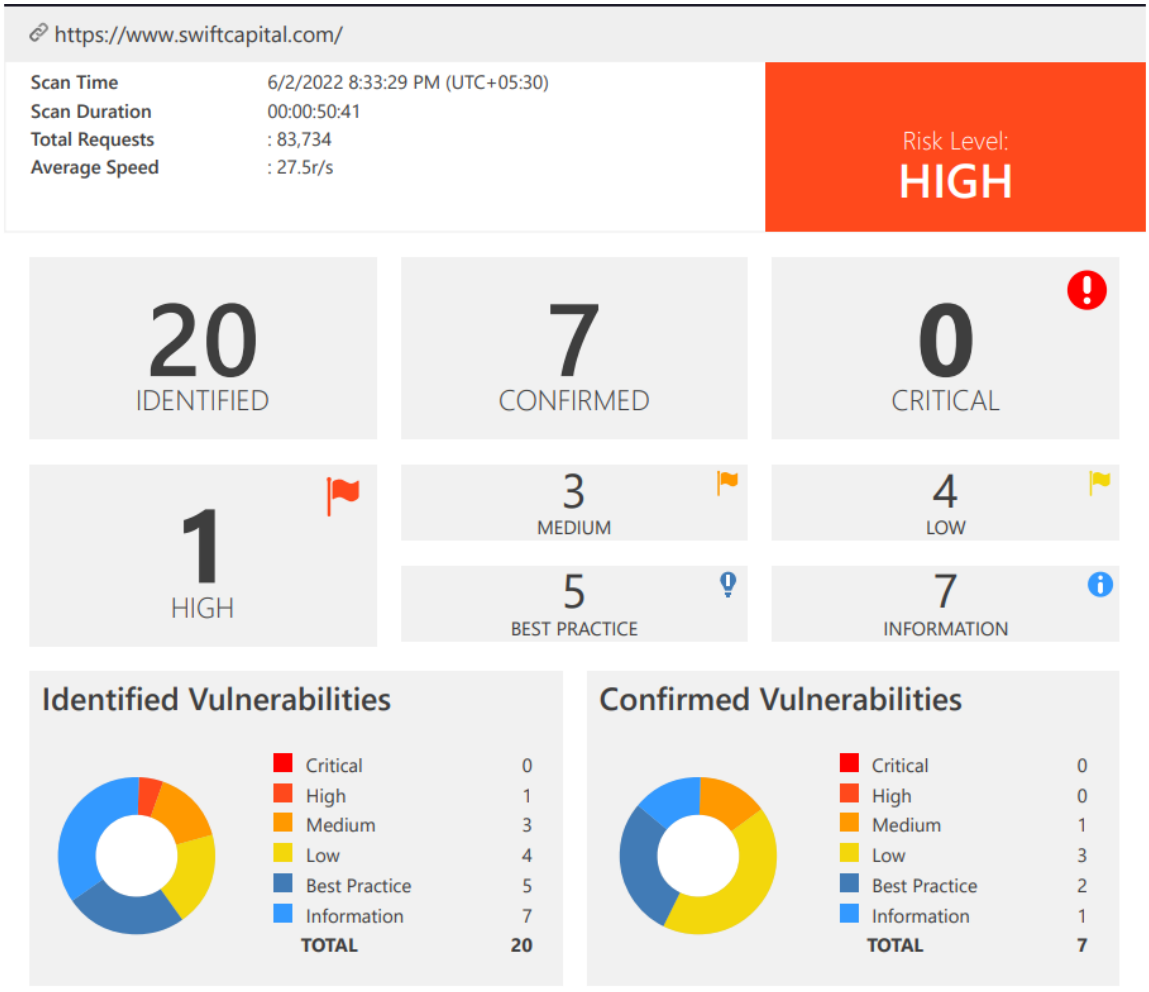


Netsparker detected only two vulnerabilities.

➢ HTTP Strict Transport Security (HSTS) Errors and Warnings.

➢ Expect-CT Not Enabled.

✓ www.swiftcapital.com



Netsparker identified 20 vulnerabilities.

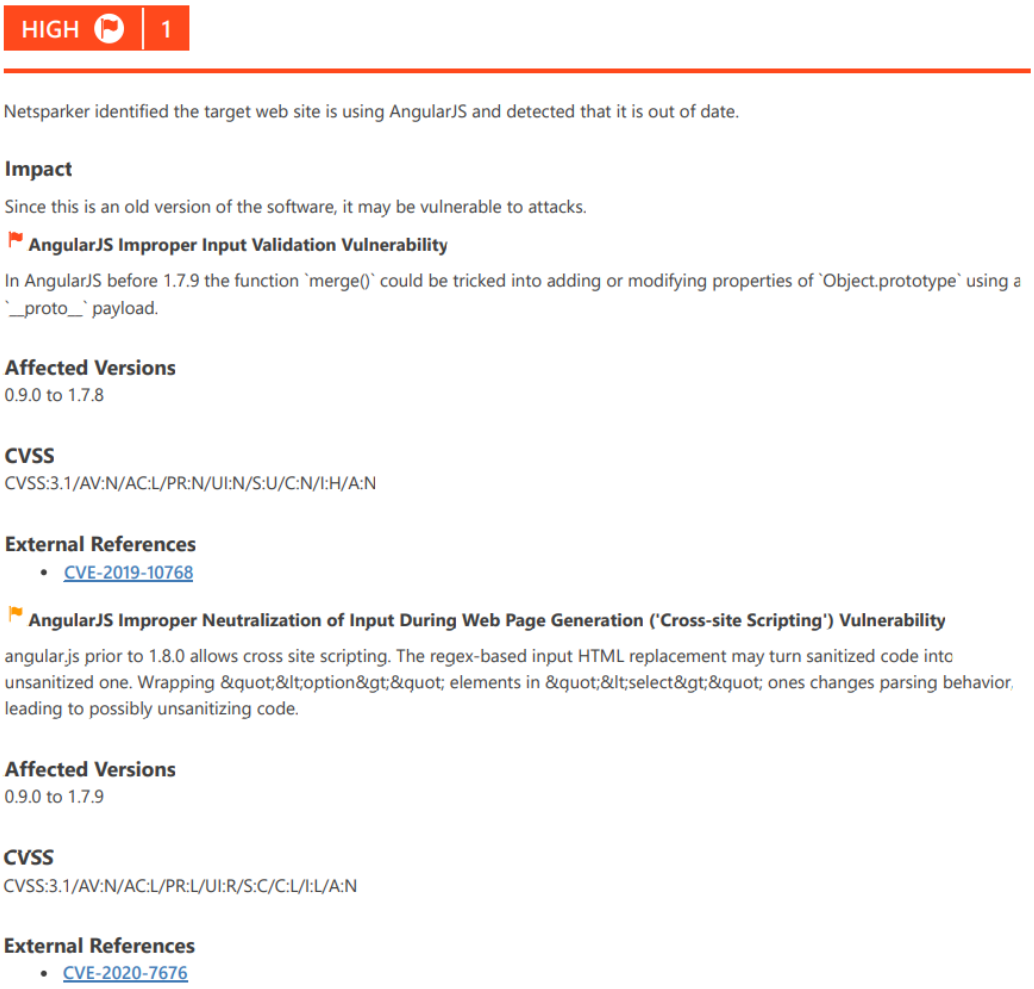
Vulnerability Summary

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	Out-of-date Version (AngularJS)	GET	https://www.swiftcapital.com/	No Parameters
	[Possible] Source Code Disclosure (Generic)	GET	https://www.swiftcapital.com/	No Parameters
	Out-of-date Version (jQuery)	GET	https://www.swiftcapital.com/Sizzle.js	No Parameters
	Weak Ciphers Enabled	GET	https://www.swiftcapital.com/	No Parameters
	Missing X-Frame-Options Header	GET	https://www.swiftcapital.com/	No Parameters
	Cookie Not Marked as HttpOnly	GET	https://www.swiftcapital.com/	No Parameters
	Cookie Not Marked as Secure	GET	https://www.swiftcapital.com/	No Parameters
	Insecure Frame (External)	GET	https://www.swiftcapital.com/	No Parameters
	Missing X-XSS-Protection Header	GET	https://www.swiftcapital.com/	No Parameters
	Referrer-Policy Not Implemented	GET	https://www.swiftcapital.com/	No Parameters
	SameSite Cookie Not Implemented	GET	https://www.swiftcapital.com/	No Parameters
	Content Security Policy (CSP) Not Implemented	GET	https://www.swiftcapital.com/	No Parameters
	Subresource Integrity (SRI) Not Implemented	GET	https://www.swiftcapital.com/	No Parameters
	[Possible] Internal Path Disclosure (Windows)	GET	https://www.swiftcapital.com/	No Parameters
	Email Address Disclosure	GET	https://www.swiftcapital.com/	No Parameters
	Expect-CT in Report Only Mode	GET	https://www.swiftcapital.com/	No Parameters

HTTP Strict Transport Security (HSTS) Max-Age Value Too Low	GET	https://www.swiftcapital.com/	No Parameters
Sitemap Detected	GET	https://www.swiftcapital.com/sitemap.xml	No Parameters
Web Application Firewall Detected	GET	https://www.swiftcapital.com/%3Cscript%3Ealert(0)%3C/script%3E	No Parameters
Forbidden Resource	GET	https://www.swiftcapital.com/	No Parameters

Out-of-date Version (AngularJS)

- Identified Version: 1.6.6
- Latest Version: 1.8.3



HIGH | 1

Netsparker identified the target web site is using AngularJS and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

AngularJS Improper Input Validation Vulnerability

In AngularJS before 1.7.9 the function `merge()` could be tricked into adding or modifying properties of `Object.prototype` using a `__proto__` payload.

Affected Versions

0.9.0 to 1.7.8

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

External References

- CVE-2019-10768

AngularJS Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

angular.js prior to 1.8.0 allows cross site scripting. The regex-based input HTML replacement may turn sanitized code into unsanitized one. Wrapping "<option>" elements in "<select>" ones changes parsing behavior, leading to possibly unsanitizing code.

Affected Versions

0.9.0 to 1.7.9

CVSS

CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2020-7676

How to prevent

Need to upgrade angular.js to latest version.

[Possible] Source Code Disclosure (Generic)

Identified Source Code

```
<%([\s\S]+?)%>
…
<%=([\s\S]+?)%>
…
<%-([\s\S]+?)%>
```

Certainty

Impact

The inside workings and business logic of the application may be revealed depending on the source code, database connection strings, usernames, and passwords. An attacker can launch the following attacks using this information:

- Use the database or other data resources to get information. It depends on the account's privileges as determined by the source code.
- It may be able to read, update, or delete data from the database without permission.
- Access password-protected administrative tools including dashboards, management consoles, and admin pages.
- As a result, you have complete control over the program.
- Investigate the source code for input validation issues and logic flaws to come up with new attacks.

How to mitigate

1. Confirm exactly what elements of the source code are actually exposed; because to the constraints of these types of vulnerabilities, this may not always be possible. Confirm that is not a planned feature.

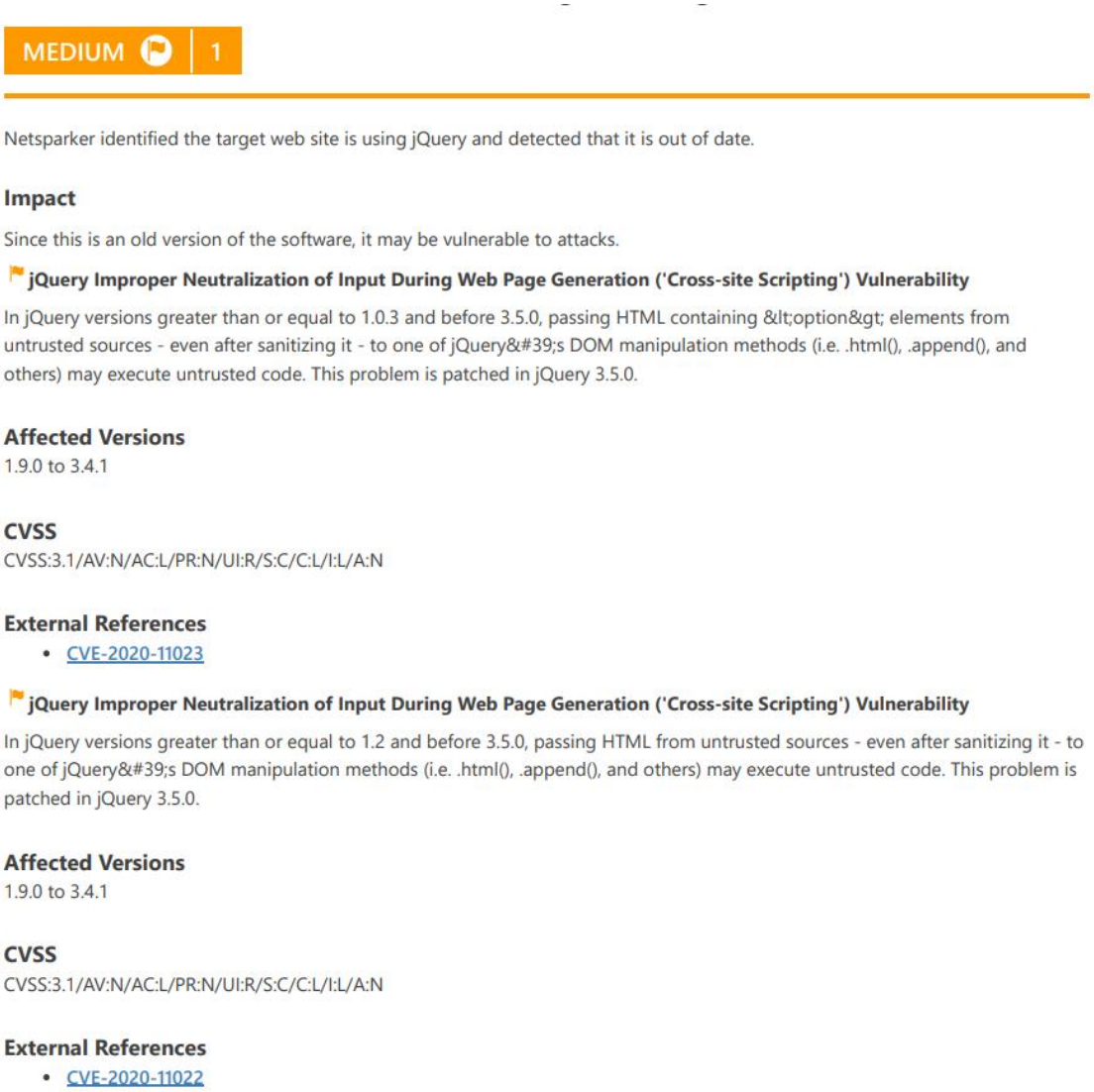
2. If the file is required by the application, alter its permissions to prevent it from being accessed by public users. Remove it from the web server if it isn't.

3. Check that the server is up to date on all security patches.

4. Delete the web server's temporary and backup files.

Out-of-date Version (jQuery)

- Identified Version: 3.2.1
- Latest Version: 3.6.0



MEDIUM 1

Netsparker identified the target web site is using jQuery and detected that it is out of date.

Impact

Since this is an old version of the software, it may be vulnerable to attacks.

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.9.0 to 3.4.1

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2020-11023

jQuery Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') Vulnerability

In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.

Affected Versions

1.9.0 to 3.4.1

CVSS

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

External References

- CVE-2020-11022

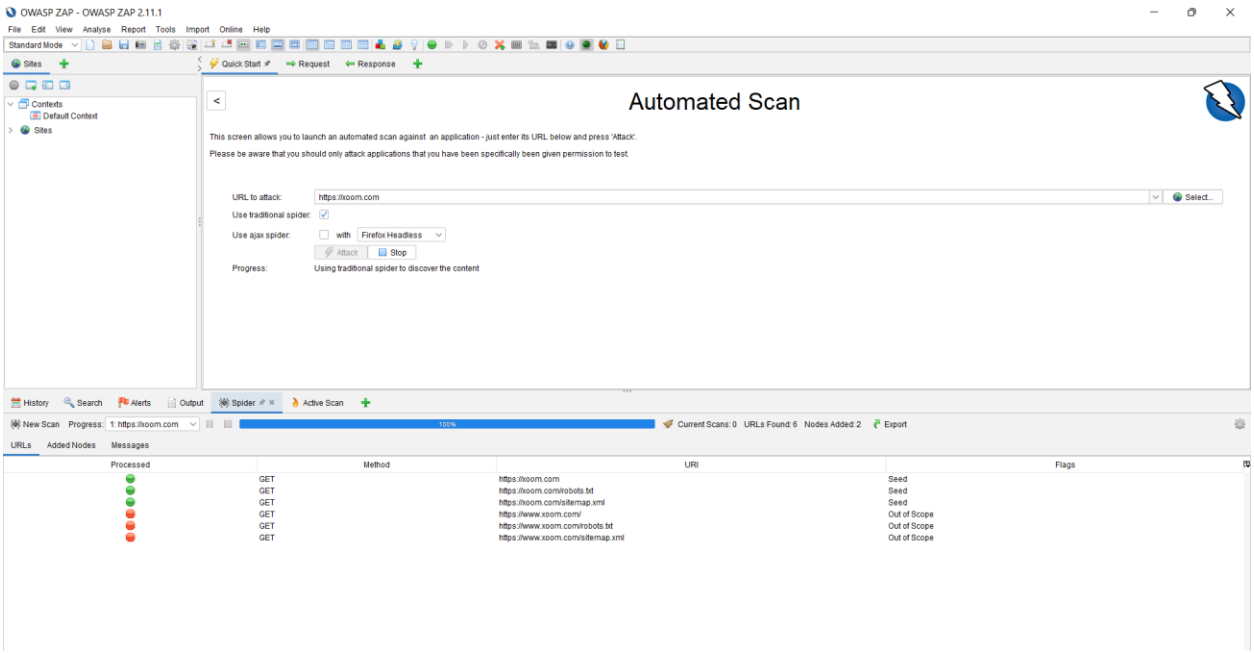
How to mitigate

Need to upgrade jQuery into latest version.

2) OWASP ZAP

OWASAP ZAP is an open-source penetration tool. It has been accorded Flagship status and is one of the most active Open Web Application Security Project (OWASP) projects. When used as a proxy server, it gives the user complete control over any traffic that flows through it, including https traffic. It can also run as a daemon and be controlled over a REST API.

Results:



These are the things I got from OWASP zap. These details are very similar to Netsparker scanning reports.

		Risk			
		High (= High)	Medium (>= Medium)	Low (>= Low)	Informational (>= Informational)
Site	https://www.swiftcapital.com	0 (0)	1 (1)	0 (1)	0 (1)
	https://venmo.com	0 (0)	4 (4)	2 (6)	1 (7)
	https://xoom.com	0 (0)	0 (0)	1 (1)	2 (3)
	https://paypal.com	0 (0)	2 (2)	5 (7)	0 (7)

Alert counts by alert type

This table shows the number of alerts of each alert type, together with the alert type's risk level.

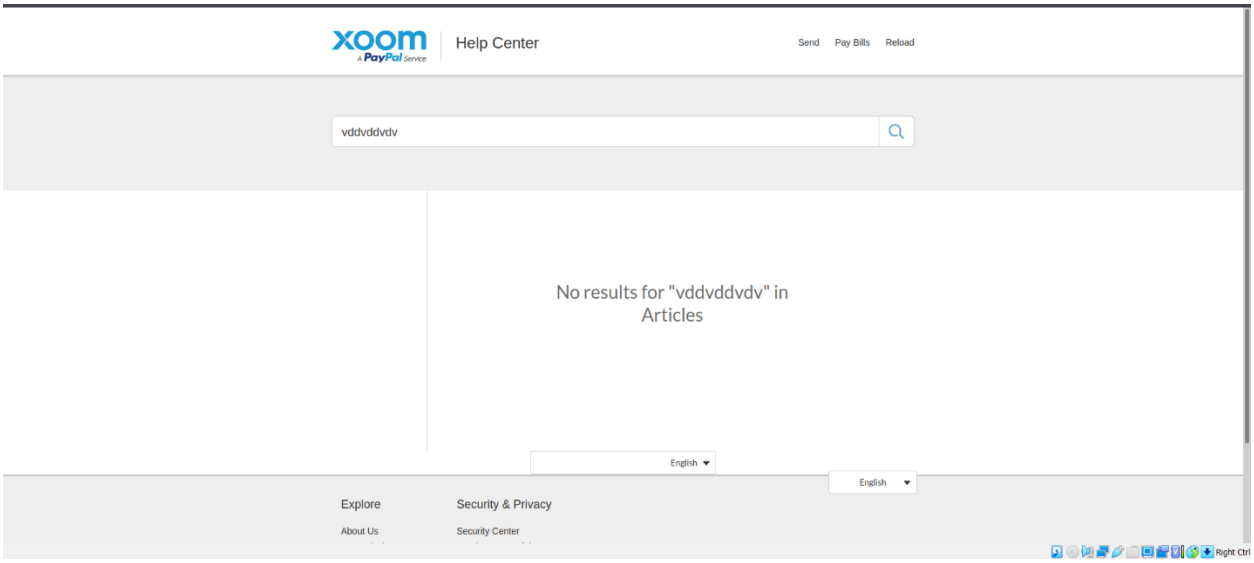
(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

Alert type	Risk	Count
Absence of Anti-CSRF Tokens	Medium	6 (33.3%)
CSP: Wildcard Directive	Medium	52 (288.9%)
CSP: script-src unsafe-inline	Medium	49 (272.2%)
CSP: style-src unsafe-inline	Medium	52 (288.9%)
Content Security Policy (CSP) Header Not Set	Medium	141 (783.3%)
Missing Anti-clickjacking Header	Medium	95 (527.8%)
Vulnerable JS Library	Medium	20 (111.1%)
CSP: Notices	Low	2 (11.1%)
Cookie No HttpOnly Flag	Low	43 (238.9%)
Cookie Without Secure Flag	Low	3 (16.7%)
Cookie without SameSite Attribute	Low	45 (250.0%)
Cross-Domain JavaScript Source File Inclusion	Low	289 (1,605.6%)
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	29 (161.1%)
Timestamp Disclosure - Unix	Low	1097 (6,094.4%)

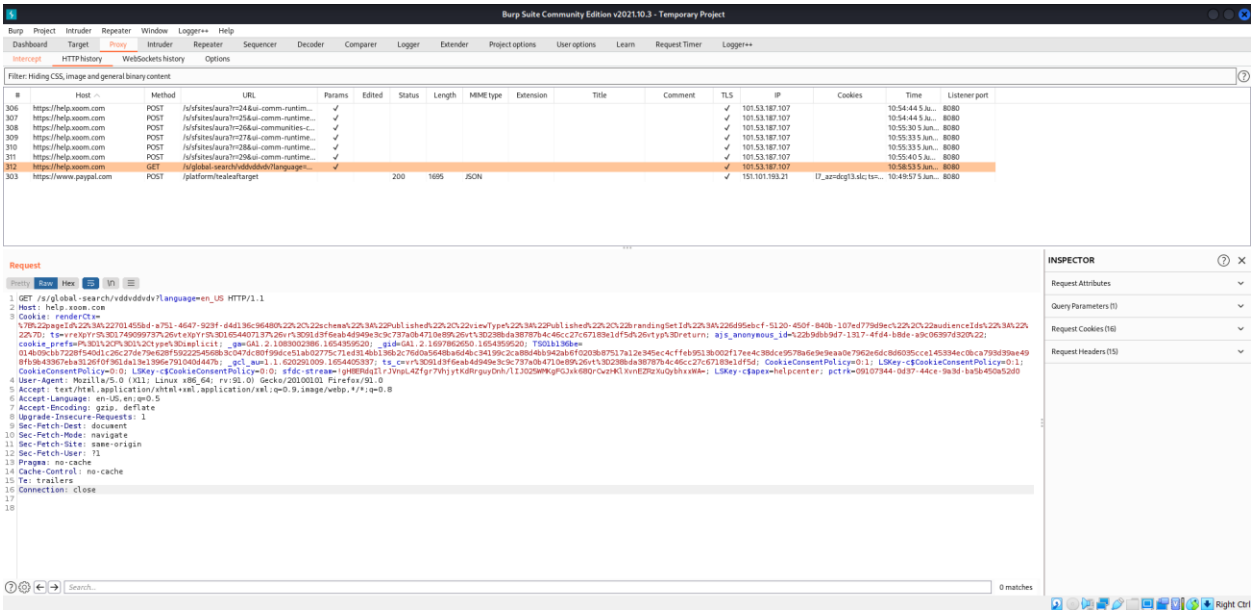
X-Content-Type-Options Header Missing	Low	133 (738.9%)
Information Disclosure - Sensitive Information in URL	Informational	2 (11.1%)
Information Disclosure - Suspicious Comments	Informational	61 (338.9%)
Re-examine Cache-control Directives	Informational	223 (1,238.9%)
Total		18

Try XSS Atttack on “xoom.com”

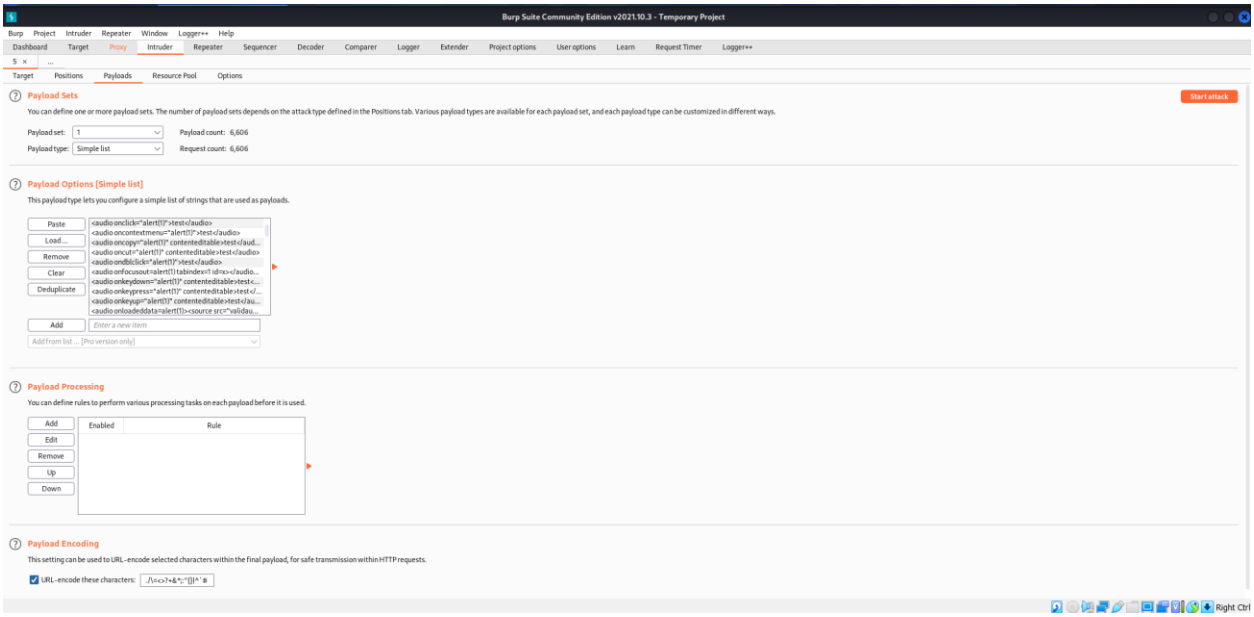
I tried cross site scripting attack on “xoom.com” using burp suit. I used “xoom.com” search bar to launch attack.



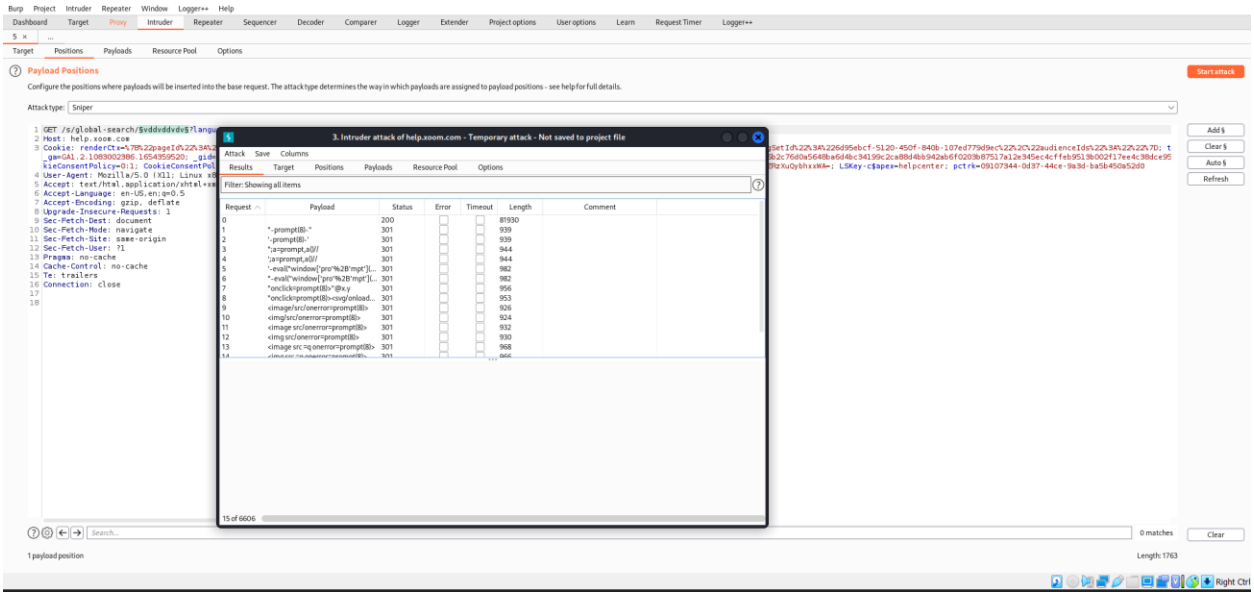
Then I capture request to burp suite.



Then I send request to intruder and try sniper attack. I use XSS wordlist for this. You can download it using https://github.com/payloadbox/xss-payload-list.git.



Then I launched attack.



After attack, I didn’t found any xss vulnerabilities in this search bar.

Conclusion

Web audit is a method of discovering vulnerabilities and weaknesses of web application. I chose Hackerone “paypal” bug bounty program for my web audit. First, I found information about domains and then find vulnerabilities using Netsparker and OWSAP zap. Then I found some medium and low vulnerabilities. That vulnerabilities are not highly risk to given domains. But Organization needs to use given prevention methods and practices to have better security in their web application.