



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**

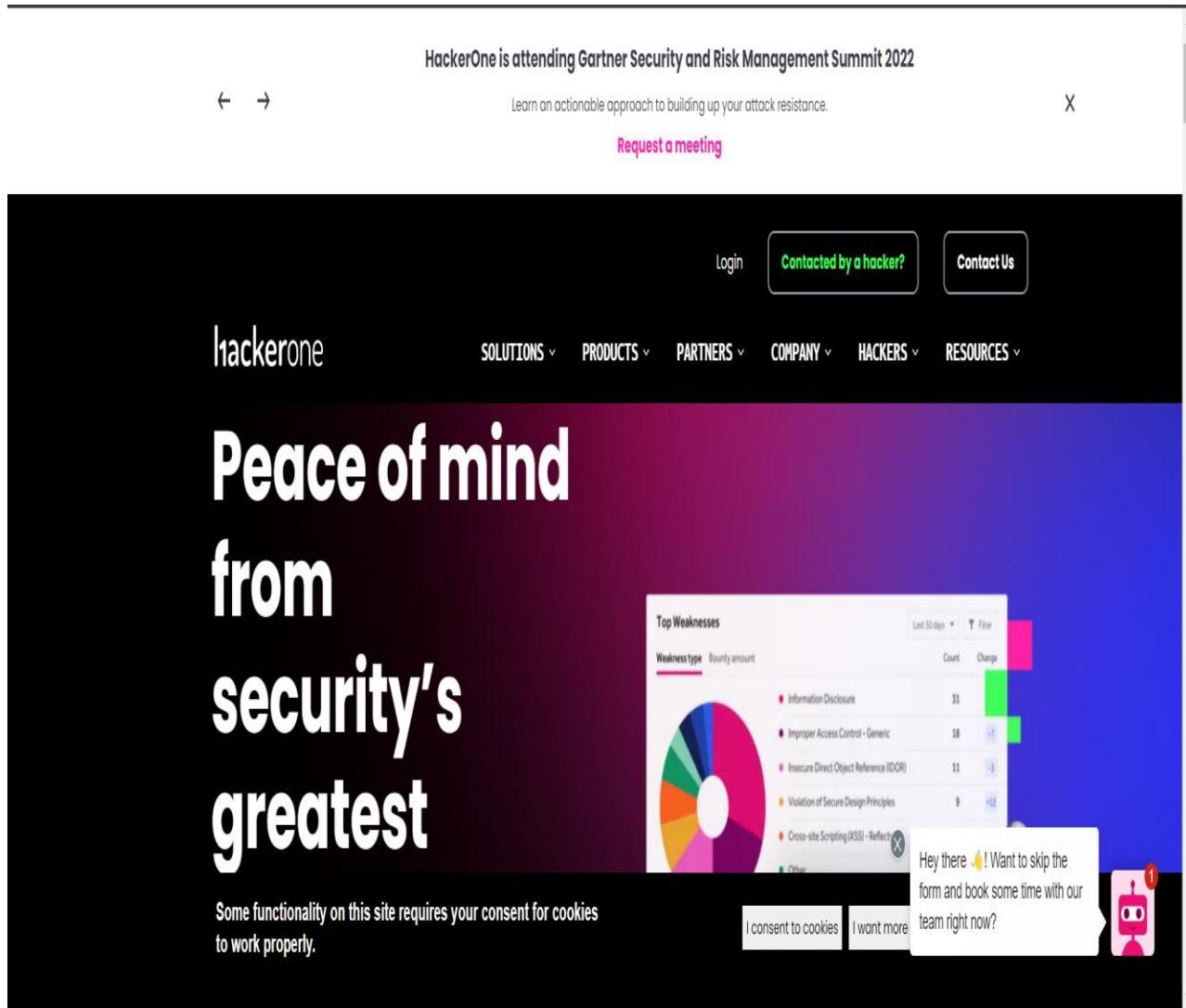
Bug bounty is a program designed to pay bug hunters for finding vulnerabilities in web products and services. The program is designed to help organizations to keep their users and their data safe, and it has been incredibly successful in bringing critical security improvements to web applications. Bug 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>

The screenshot shows the PayPal bug bounty program page on the HackerOne platform. At the top, there's a navigation bar with links to Hacktivity, Directory, Opportunities, Inbox, Hacker Dashboard, Job Board, and Leaderboards. Below the navigation is a main content area featuring the PayPal logo and the text "Send Money, Pay Online or Set Up a Merchant Account - PayPal." A "Submit report" button is prominently displayed. To the right, a sidebar provides details about the "Bug Bounty Program": "Launched on Sep 2018," "Managed by HackerOne," "Includes retesting," and "Bounty splitting enabled." Below the sidebar are "Bookmarked" and "Subscribe" buttons. In the center, there are three performance metrics: "Reports resolved" (1384), "Assets in scope" (41), and "Average bounty" (\$1k-\$3k). At the bottom of the main content area, there are links for "Policy," "Hacktivity," "Thanks," "Updates (3)," and "Collaborators". Below this, a note states "This program requires two-factor authentication enabled to participate in." There are also sections for "Rewards" (with a legend for Low, Medium, High, and Critical levels) and "Response Efficiency" (showing 4 hrs average time to first response and 16 days average time to resolution).

## 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

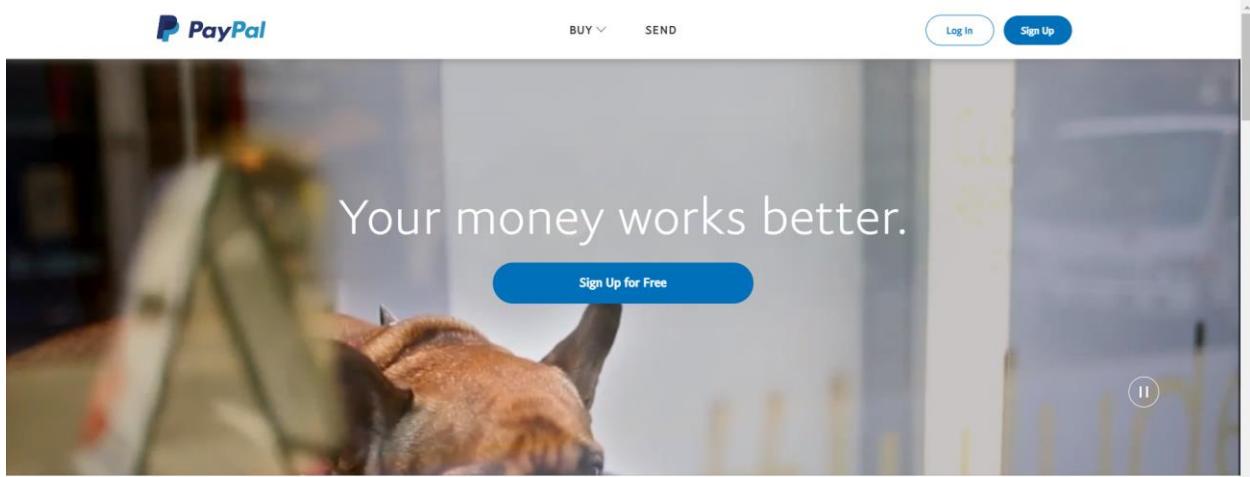
### In Scope

|        |   |   |  |
|--------|---|---|--|
| Domain | <b>www.paypal-* .com</b><br>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.<br>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. | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | * .xoom .com  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | * .paypal .com  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>* .braintreegateway .com</b><br>For testing and account creation, please use *.sandbox.braintreegateway.com rather than production.  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | * .paydiant .com  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | * .venmo .com   | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | paypalobjects .com  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | paypal .me  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | py .pl  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>* .braintreepayments .com</b><br>For testing and account creation, please use *.sand.braintreepayments.com rather than production.   | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>* .braintree-api .com</b><br>For testing and account creation, please use *.sandbox.braintree-api.com rather than production.  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |

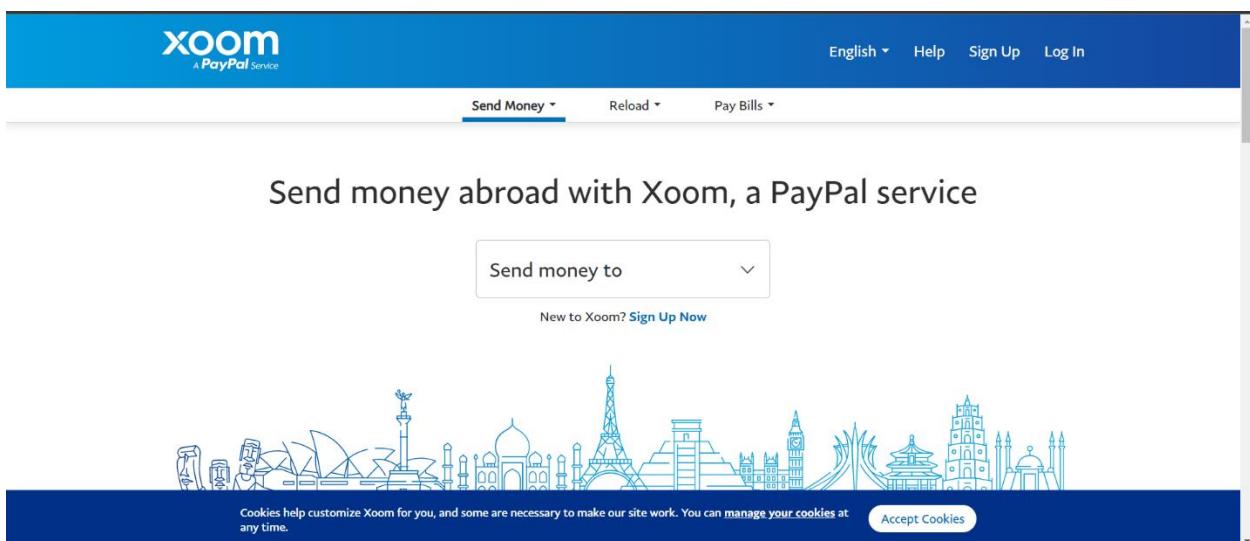
|        |   |   |  |
|--------|---|---|--|
| Domain | <b>*.braintree-api.com</b><br>For testing and account creation, please use *.sandbox.braintree-api.com rather than production.  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>*.braintree.tools</b><br>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. | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>prequal.swiftfinancial.com</b><br>We are aware that the root URL of this domain returns an error, the API is functioning correctly.  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>partner.swiftfinancial.com</b><br>We are aware that the root URL of this domain returns an error, the API is functioning correctly.  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>decision.swiftfinancial.com</b><br>We are aware that the root URL of this domain returns an error, the API is functioning correctly.   | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>pigeon.swiftfinancial.com</b><br>We are aware that the root URL of this domain returns an error, the API is functioning correctly.   | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>scrutiny.swiftfinancial.com</b><br>We are aware that the root URL of this domain returns an error, the API is functioning correctly.   | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>www.swiftcapital.com</b>   | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>www.loanbuilder.com</b>  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>www.swiftfinancial.com</b>   | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>api.swiftfinancial.com</b>   | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>my.swiftfinancial.com</b>  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |
| Domain | <b>api.loanbuilder.com</b>  | <span style="color: red;">■</span> Critical | <span style="color: green;">\$</span> Eligible |

I selected 5 domains out from here.

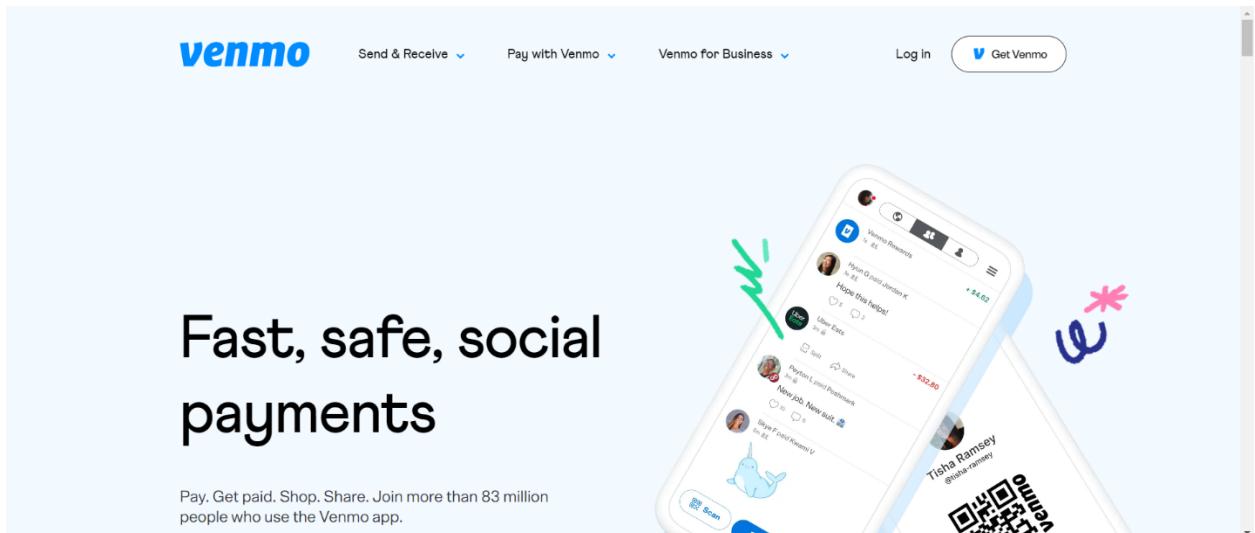
1) .paypal.com



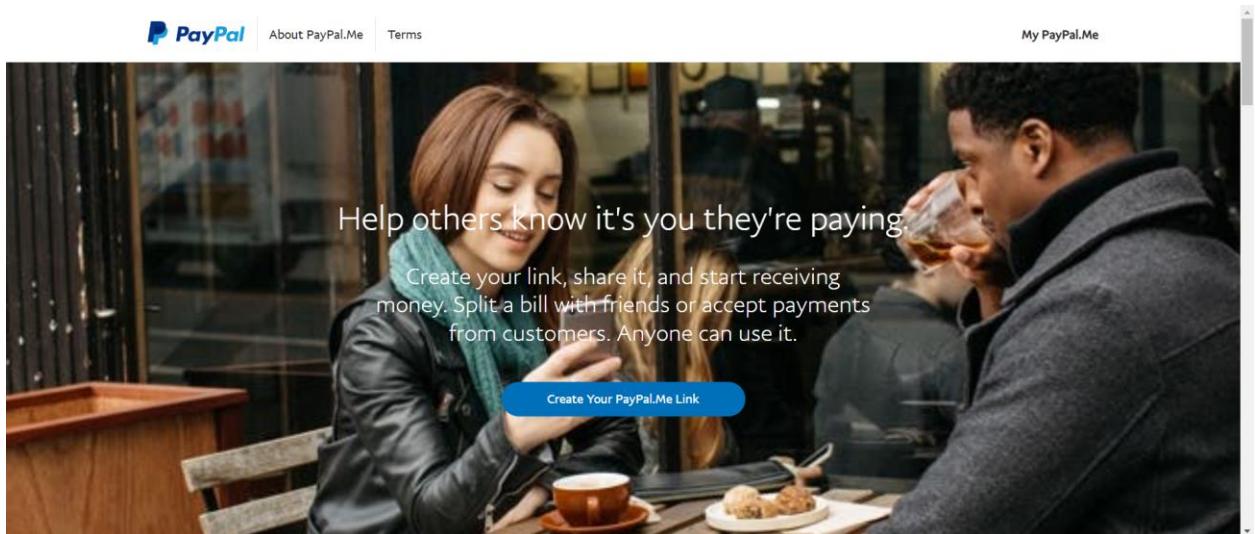
2) .xoom.com



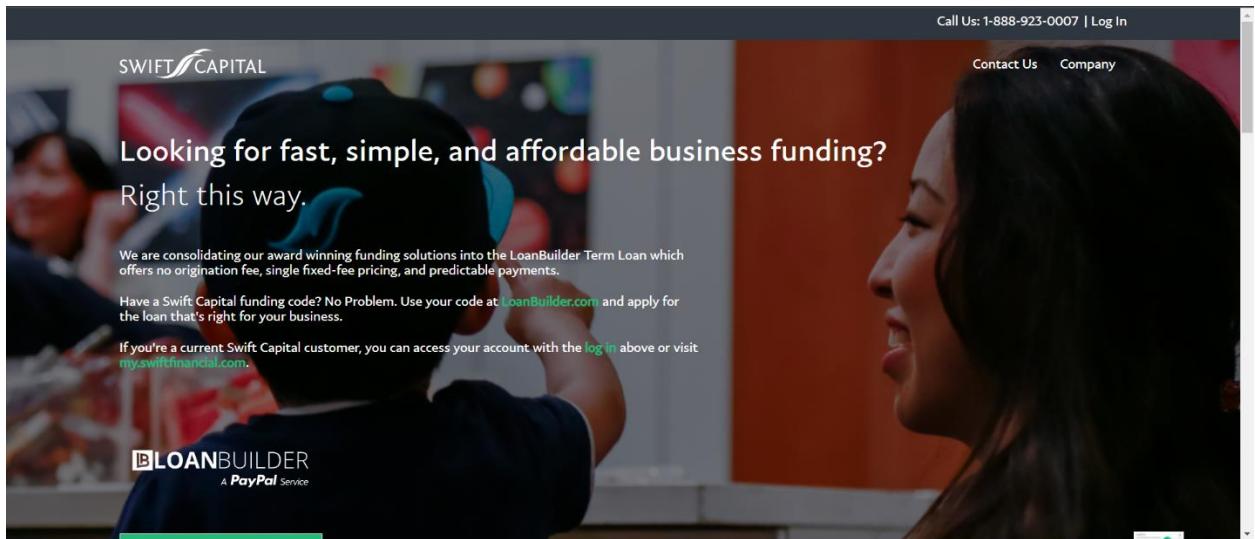
### 3) .venmo.com



### 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

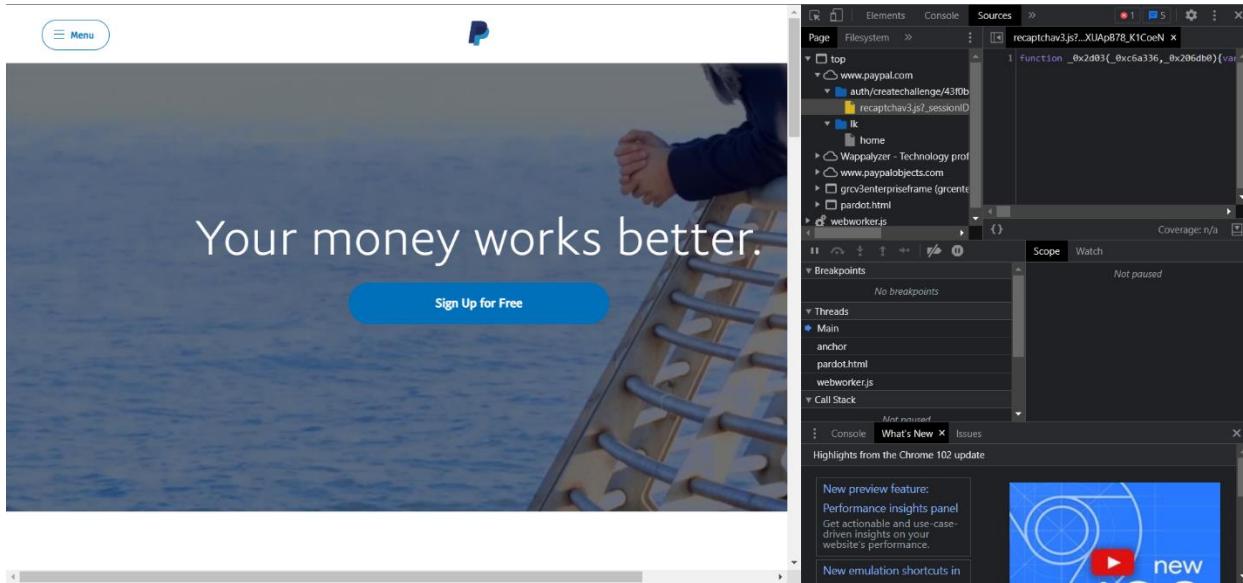
### 1) Web Browser

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.

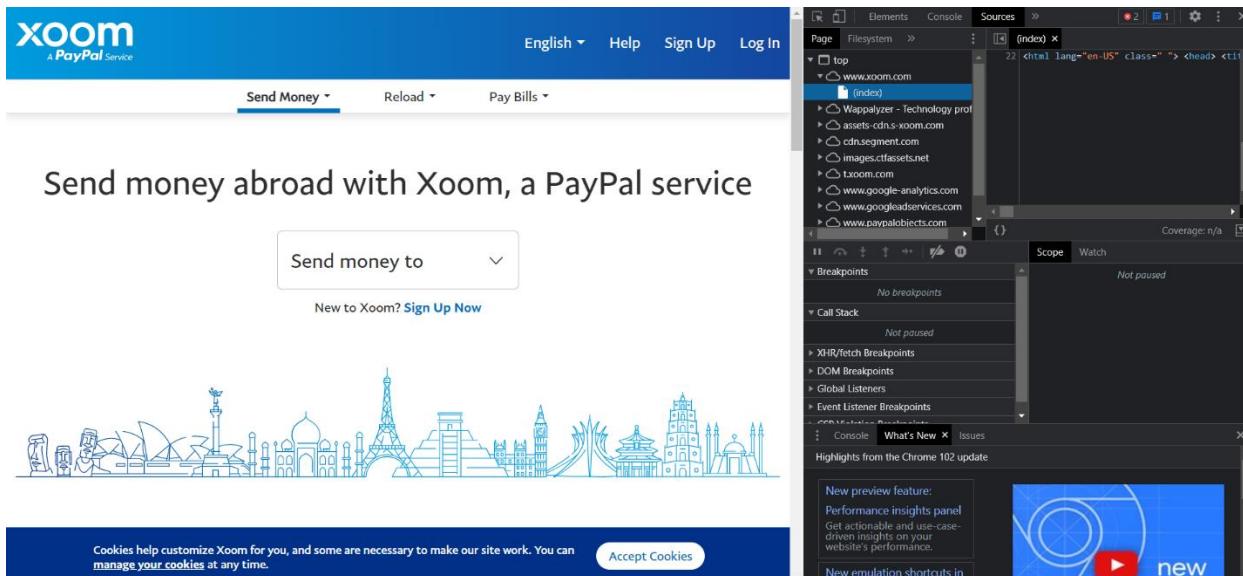
### Results

- ✓ .paypal.com



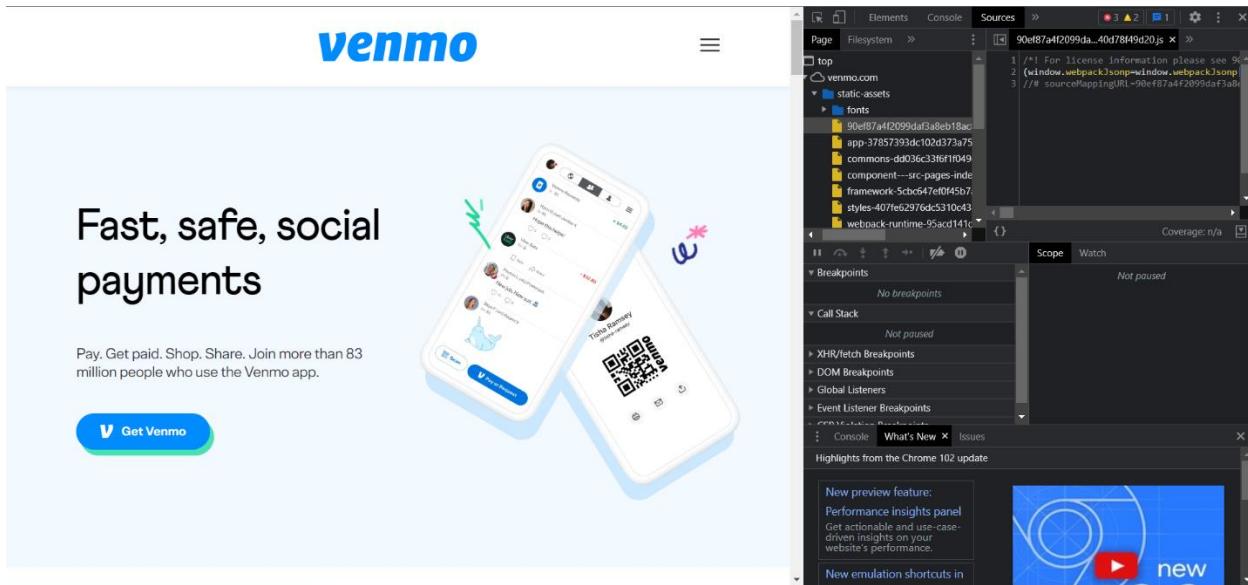
In here I found one JavaScript file called “recaptchav3.js”

✓ .xoom.com



In here, I find only index file.

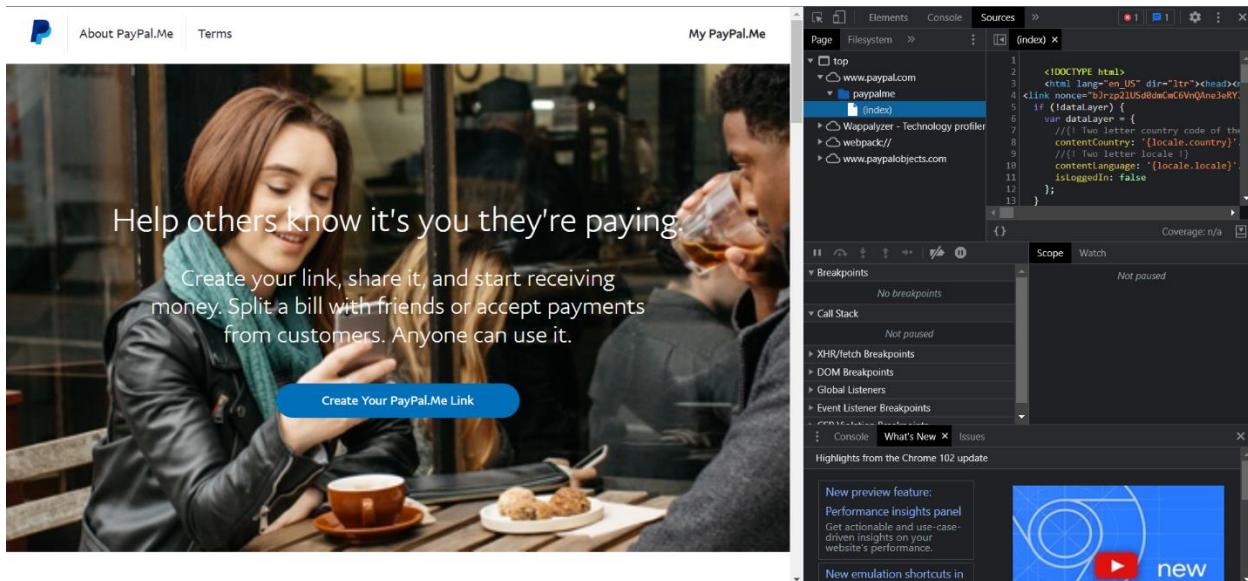
✓ .venmo.com



The screenshot shows the Venmo homepage with a large 'Fast, safe, social payments' headline and two phones displaying the app interface. The developer tools' Sources tab is open, showing a tree view of files. Under the 'static-assets' folder, there are seven JavaScript files (90ef87a412099da...), a 'font.css' file, and other assets like 'commons-6d03c336ff1049.js'. The 'fonts' folder contains '90ef87a412099da3a8eb18ac.css'.

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

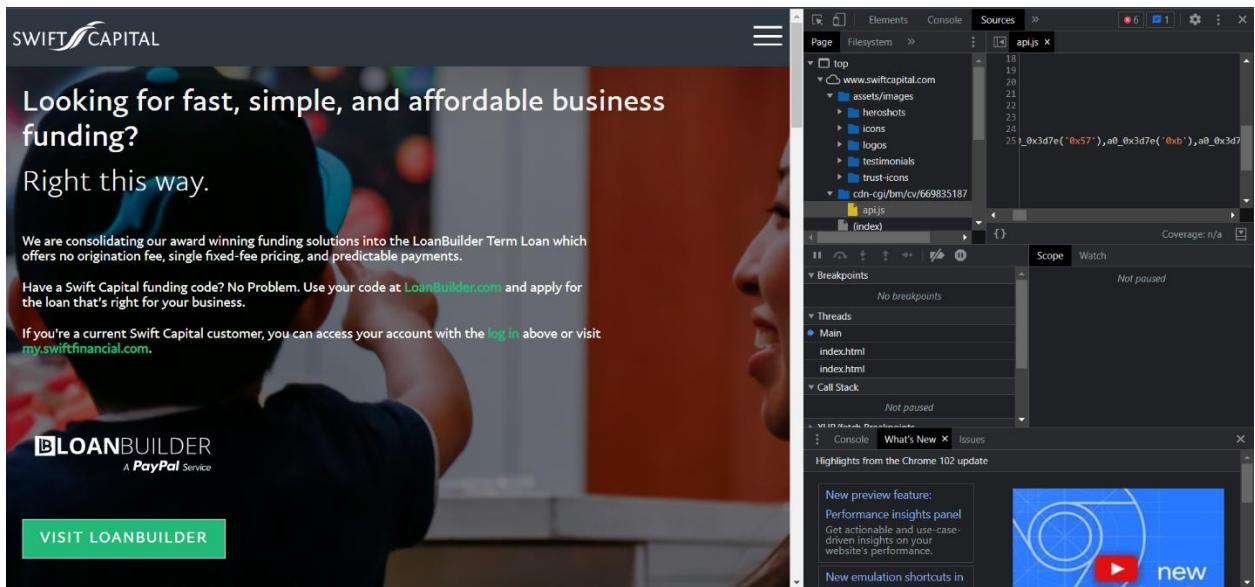
✓ paypal.me



The screenshot shows the PayPal.Me homepage with a woman at a cafe and a man drinking beer. The developer tools' Sources tab is open, showing a tree view of files. Under the 'paypalme' folder, there is an 'index.js' file. Other files listed include 'index.html', 'webpack://...', and 'www.paypalobjects.com'.

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

```
└──(root㉿kali)-[~/paypal]
# ping -c 5 paypal.com
PING paypal.com (64.4.250.36) 56(84) bytes of data.
64 bytes from xoom.com (64.4.250.36): icmp_seq=1 ttl=50 time=136 ms
64 bytes from paypal.com (64.4.250.36): icmp_seq=2 ttl=50 time=155 ms
64 bytes from paypal.com (64.4.250.36): icmp_seq=3 ttl=50 time=143 ms
64 bytes from paypal.com (64.4.250.36): icmp_seq=4 ttl=50 time=141 ms
64 bytes from paypal.com (64.4.250.36): icmp_seq=5 ttl=50 time=138 ms

--- paypal.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 136.189/142.528/154.637/6.465 ms
```

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

✓ .xoom.com

```
└──(root㉿kali)-[~/paypal]
# ping -c 5 xoom.com
PING xoom.com (64.4.250.36) 56(84) bytes of data.
64 bytes from paypal.com (64.4.250.36): icmp_seq=1 ttl=50 time=144 ms
64 bytes from paypal.com (64.4.250.36): icmp_seq=2 ttl=50 time=138 ms
64 bytes from paypal.com (64.4.250.36): icmp_seq=3 ttl=50 time=142 ms
64 bytes from paypal.com (64.4.250.36): icmp_seq=4 ttl=50 time=139 ms
64 bytes from paypal.com (64.4.250.36): icmp_seq=5 ttl=50 time=142 ms

--- xoom.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 138.282/141.205/144.147/2.104 ms
```

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

```
[root@kali:[~/paypal]
# ping -c 5 venmo.com
PING venmo.com (18.155.68.76) 56(84) bytes of data.
64 bytes from server-18-155-68-76.sin52.r.cloudfront.net (18.155.68.76): icmp_seq=1 ttl=244 time=64.3 ms
64 bytes from server-18-155-68-76.sin52.r.cloudfront.net (18.155.68.76): icmp_seq=2 ttl=244 time=64.4 ms
64 bytes from server-18-155-68-76.sin52.r.cloudfront.net (18.155.68.76): icmp_seq=3 ttl=244 time=68.6 ms
64 bytes from server-18-155-68-76.sin52.r.cloudfront.net (18.155.68.76): icmp_seq=4 ttl=244 time=56.8 ms
64 bytes from server-18-155-68-76.sin52.r.cloudfront.net (18.155.68.76): icmp_seq=5 ttl=244 time=75.6 ms

--- venmo.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 56.823/65.967/75.616/6.145 ms
```

Ping command successful. Ip address is 18.155.68.76.

✓ paypal.me

```
[root@kali:[~/paypal]
# ping -c 5 paypal.me
PING paypal.me (64.4.250.37) 56(84) bytes of data.
64 bytes from xoom.com (64.4.250.37): icmp_seq=1 ttl=50 time=131 ms
64 bytes from paypal.com (64.4.250.37): icmp_seq=2 ttl=50 time=137 ms
64 bytes from paypal.com (64.4.250.37): icmp_seq=3 ttl=50 time=132 ms
64 bytes from paypal.com (64.4.250.37): icmp_seq=4 ttl=50 time=146 ms
64 bytes from paypal.com (64.4.250.37): icmp_seq=5 ttl=50 time=135 ms

--- paypal.me ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4005ms
rtt min/avg/max/mdev = 130.618/136.230/146.072/5.396 ms
```

Ping successful. Ip address is 64.4.250.37.

✓ .swiftcapital.com

```
[root@kali:~/paypal]
# ping -c 5 swiftcapital.com
PING swiftcapital.com (52.218.193.139) 56(84) bytes of data.
64 bytes from s3-website-us-west-2.amazonaws.com (52.218.193.139): icmp_seq=1 ttl=226 time=268 ms
64 bytes from s3-website-us-west-2.amazonaws.com (52.218.193.139): icmp_seq=2 ttl=226 time=271 ms
64 bytes from s3-website-us-west-2.amazonaws.com (52.218.193.139): icmp_seq=3 ttl=226 time=264 ms
64 bytes from s3-website-us-west-2.amazonaws.com (52.218.193.139): icmp_seq=4 ttl=226 time=262 ms
64 bytes from s3-website-us-west-2.amazonaws.com (52.218.193.139): icmp_seq=5 ttl=226 time=273 ms

--- swiftcapital.com ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4008ms
rtt min/avg/max/mdev = 261.875/267.696/273.488/4.399 ms
```

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

```
[root@kali:~]# whois paypal.com
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: 2021-06-13T09:21:55Z
Creation Date: 1999-07-15T05:32:11Z
Registry Expiry Date: 2022-07-15T05:32:11Z
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
Name Server: NS1.P57.DYNECT.NET
Name Server: NS2.P57.DYNECT.NET
Name Server: PDNS100.ULTRADNS.COM
Name Server: PDNS100.ULTRADNS.NET
DNSSEC: signedDelegation
DNSSEC DS Data: 21037 5 2 0DF17B28554954D819E0CEEAB98FCFCD56572A4CF4F551F0A9BE6D04DB2F65C3
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-05-31T21:01:47Z <<

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: 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@sat1:~)
[root@sat1 ~]# 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
Seller:
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.NET
Name Server: PDNS100.ULTRADNS.COM
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 The 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 lawful 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, commercial 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 data 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 Operator 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 queried 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] $ https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories/
# python3 finalrecon.py --whois https://paypal.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Since Kali 2020.3, after Kali's setup is complete, network repositories will  
was no network access during installation.



## Switching Kali Main Branch



Kali has two main branches to choose from (please take the time to read  
your setup):



- kali-rolling - default & frequently updated
- kali-last-snapshot - point release so more "stable" & the "safest"



Enabling the kali-rolling branch is done with the command:



```
https://www.kali.org/kali/kali-rolling main contrib non-free" | sudo
```



Enabling the kali-last-snapshot branch is done with the command:



```
https://www.kali.org/kali/kali-last-snapshot main contrib non-free" | sudo
```



Note that such a change is effective only after running sudo apt update



## Enabling Kali Additional Branches



Kali also proposes additional branches for special cases. In theory, it's no



```
[+] Created By : thewhiteh4t
    Twitter : https://twitter.com/thewhiteh4t
    Community : https://twc1rcle.com/
[+] Version : 1.1.3
    Kali In The Browser (noVNC)
[+] Target : https://paypal.com
    Kali Linux Forensics Mode
[+] IP Address : 64.4.250.37
    Kali Training
[!] Whois Lookup :
    Kali's Domains
[+] asn_registry : arin
[+] asn : 17012_SnSSL Configuration
[+] asn_cidr : 64.4.250.0/24
[+] asn_country_code : US
    shave
[+] asn_date : 2003-02-25
    Non-root
[+] 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] https://www.kali.org/docs/general-use/kali-linux-sources-list-repositories
# python3 finalrecon.py --whois https://xoom.com
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec



Since Kali 2020.3, after Kali's setup is complete, network repositories will be enabled by default. This was not the case before, as there was no network access during installation.



## Switching Kali Main Branch



Kali has two main branches to choose from (please take the time to read what follows for your setup):



- kali-rolling - default & frequently updated
- kali-last-snapshot - point release so more "stable" & the "safest"



Enabling the kali-rolling branch is done with the command:



```
i.org/kali kali-rolling main contrib non-free" | sudo
```



Enabling the kali-last-snapshot branch is done with the command:



```
/kali kali-last-snapshot main contrib non-free" | sudo
```



Note that such a change is effective only after running sudo apt update.



## Enabling Kali Additional Branches



Kali also proposes additional branches for special cases. In theory, it's possible to enable them via the following command:



```
[+] 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
since Kali 2020.3, after Kali's setup is complete, network repositories will be enabled by default, even if there was no network access during installation.


Switching Kali Main Branch

Kali has two main branches to choose from (please take the time to read which one would be the best option for your setup):

[+] Created By : thewhiteh4t
[→] Twitter : https://twitter.com/thewhiteh4t
[→] Community : https://twcircle.com/
[+] Version Kali : 1.1.3 - Sics Mode
[+] Target : https://venmo.com
[+] IP Address: 18.155.68.42
[!] Whois Lookup: SSL Configuration

[+] 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

```

Enabling the `kali-rolling` branch is done with the command:

```
curl https://raw.githubusercontent.com/thewhiteh4t/kali-rolling/main/contrib/non-free | sudo tee /etc/apt/sources.list
```

Enabling the `kali-last-snapshot` branch is done with the command:

```
curl https://raw.githubusercontent.com/thewhiteh4t/kali-last-snapshot/main/contrib/non-free | sudo tee /etc/apt/sources.list
```

Note that such a change is effective only after running `sudo apt update`.

## Enabling Kali Additional Branches

Kali also proposes additional branches for special cases. In theory, it's possible to enable those regardless.

## Enabling Kali Additional Branches

Note that such a change is effective only after running `sudo apt update`.

```

[+] state : WA
[+] city : SEATTLE
[+] address : 1918 8th Ave DARK
[+] 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

```
(root@kali:[~/FinalRecon] # python3 finalrecon.py --whois https://paypal.me
# Kali Linux  Kali Tools  Kali Docs  Kali Forums  Kali-NetHunter  Exploit-DB  Google Hacking DB  OffSec

Since Kali 2020.3, after Kali's setup is complete, network repositories will be enabled by default. This means that you will have full access to the internet. If you were connected to a network during installation, you will be able to browse the web and download files. If you were not connected to a network during installation, you will not be able to browse the web or download files. This is because network repositories require an active connection to the internet in order to work correctly. If you are not connected to a network, you will need to manually enable network repositories in the Kali configuration files.

Switching Kali Main Branch

[+] Created By : thewhiteh4t
[+] Twitter : https://twitter.com/thewhiteh4t
[+] Community : https://twc1rcle.com/
[+] Version : 1.1.3
[+] Target : https://paypal.me
[+] IP Address : 64.4.250.36
[+] Whois Lookup :
[+] ASN Registry : ARIN
[+] ASN : 17012
[+] ASN CIDR : 64.4.250.0/24
[+] ASN Country Code : US
[+] ASN Date : 2003-02-25
[+] Query : 64.4.250.36
[+] 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.
[+] Configuration :
[+] 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 0:00:01.692282
[!] Exporting to /root/.local/share/finalrecon/dumps/paypal.me.txt

Kali has two main branches to choose from (please take the time to read which one is best for your setup):
  * kali-rolling - default & frequently updated
  * kali-last-snapshot - point release so more "stable" & the "safest"

Enabling the kali-rolling branch is done with the command:
curl https://www.kali.org/kali/kali-rolling/main/contrib/non-free | sudo tee /etc/apt/sources.list.d/kali-rolling.list

Enabling the kali-last-snapshot branch is done with the command:
curl https://www.kali.org/kali/kali-last-snapshot/main/contrib/non-free | sudo tee /etc/apt/sources.list.d/kali-last-snapshot.list

Note that such a change is effective only after running sudo apt update.

Enabling Kali Additional Branches

Kali also proposes additional branches for special cases. In theory, it's possible to enable them by adding their URLs to /etc/apt/sources.list.d/kali-additional.list. However, this is not recommended as it may cause conflicts with other packages. Instead, it's better to use the official Kali repositories.
```

✓ swiftcapital.com

```

└─(root㉿kali)-[~/FinalRecon] └─ A https://www.kali.org/general-use/kali-linux-sources-list-repositories
└─# python3 finalrecon.py --whois https://swiftcapital.com
└─ Kali Linux └─ Kali Tools └─ Kali Docs └─ Kali Forums └─ Kali NetHunter └─ Exploit-DB └─ Google Hacking DB └─ OffSec

Since Kali 2020.3, after Kali's setup is complete, network repositories will be enabled by default, even if there was no network access during installation.

Switching Kali Main Branch

[+] Created By : thewhiteh4t
[+] Twitter : https://twitter.com/thewhiteh4t
[+] Community : https://twc1rcle.com/
[+] Version : 1.3
[+] Kali In The Browser (noVNC)
[+] Target : https://swiftpcapital.com
[+] Kali Linux Forensics Mode
[+] IP Address : 52.218.247.82
[+] Kali Training
[!] Whois Lookup :
    Kali's Domains
[+] asn_registry : arin
[+] asn : 16509
[+] asn_cidr : 52.218.244.0/22
[+] asn_country_code : US
[+] asn_date : 2015-09-02
[+] query : 52.218.247.82
[+] cidr : 52.220.0.0/15 52.223.128.0/18 52.216.0/14 52.223.0.0/17 52.192.0.0/12 52.222.0.0/16 52.208.0.0/13
[+] name : AT-88-Z
[+] handle : NET-52-192-0-0-1
[+] range : 52.192.0.0 - 52.223.191.255
[+] description : Amazon Technologies Inc.
[+] country : US
[+] state : WA
[+] city : Seattle
[+] address : 410 Terry Ave N.
[+] postal_code : 98109
[+] emails : ['amzn-noc-contact@amazon.com' 'aws-rpki-routing-poc@amazon.com' 'abuse@amazonaws.com' 'aws-routing-poc@amazon.com']
[+] created : 2015-09-02
[+] updated : 2020-09-24
[+] Completed in 0:00:01.016750
[!] Exporting to /root/.local/share/finalrecon/dumps/swiftpcapital.com.txt

Kali has two main branches to choose from (please take the time to read which one would be the best for your setup):
  * kali-rolling - default & frequently updated
  * kali-last-snapshot - point release so more "stable" & the "safest"

Enabling the kali-rolling branch is done with the command:
curl https://raw.githubusercontent.com/kali/kali-rolling/main/contrib/non-free | sudo tee /etc/apt/sources.list.d/kali-rolling.list

Enabling the kali-last-snapshot branch is done with the command:
curl https://raw.githubusercontent.com/kali/kali-last-snapshot/main/contrib/non-free | sudo tee /etc/apt/sources.list.d/kali-last-snapshot.list

Note that such a change is effective only after running sudo apt update.

Kali also proposes additional branches for special cases. In theory, it's possible to enable those re

```

## 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=31536000]
https://www.paypal.com/ [302 Found] Country[UNITED STATES][US], HTTPServer[varnish], IP[151.101.129.21], RedirectLocation[https://www.paypal.com/lk/home], Strict-Transport-Security[max-age=31536000]
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, HttpOnly, 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=0]
```

## ✓ .xoom.com

```
└─(root㉿kali)-[~]
  # whatweb xoom.com
xoom.com [ Unassigned]
  Kali In The Browser
└─(root㉿kali)-[~] hole
  # whatweb xoom.com
xoom.com [ Unassigned] rowser (noVNC)
```

Kali has two main branches to choose from (please choose for your setup):

- **kali-rolling** - default & frequently updated

## ✓ .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, HTTPS[nginx], IP[18.155.68.21]
Strict-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-Proxy[1.1 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=31536000]
https://www.paypal.me/ [301 Moved Permanently] Country[UNITED STATES][US], IP[151.101.193.21], RedirectLocation[https://www.paypal.com/paypalme/], Strict-Transport-Security[max-age=31536000]
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-Transport-Security[max-age=1555]
UncommonHeaders[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-Frame-Options[DENY]
```

## ✓ 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.swiftcapital.com/]
https://www.swiftcapital.com/ [301 Moved Permanently] Country[UNITED STATES][US], HTTPServer[cloudflare], IP[104.16.83.73], RedirectLocation[https://www.swiftcapital.com/]
https://www.swiftcapital.com/ [200 OK] Bootstrap, CloudFront, Country[UNITED STATES][US], Email[ariel@mashraki.co.il,careers@swiftcapital.com,customerservice@-23331527-1], HTML5, HTTPS[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]
```

```
Admin Fax: +1.4025375774
Admin Fax Ext:
Admin Email: hostmaster@paypal.com
Registry Tech ID:
Tech Name: Domain Administrator
Tech Organization: PayPal Inc.
Tech Street: 2211 North First Street,
Tech City: San Jose
Tech State/Province: CA
Tech Postal Code: 95131
Tech Country: US
Tech Phone: +1.8882211161
Tech Phone Ext:
Tech Fax: +1.4025375774
Tech Fax Ext:
Tech Email: hostmaster@paypal.com
Name Server: ns-1699.awsdns-20.co.uk
Name Server: ns-581.awsdns-08.net
Name Server: ns-486.awsdns-60.com
Name Server: ns-1187.awsdns-20.org
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2022-05-31T20:33:27+0000 <<<

For more information on WHOIS status codes, please visit:
https://www.icann.org/resources/pages/epp-status-codes
```

If you wish to contact this domain's Registrant, Administrative, or Technical contact, and such email address is not visible above, you may do so via our web form, pursuant to ICANN's Temporary Specification. To verify that you are not a robot, please enter your email address to receive a link to a page that facilitates email communication with the relevant contact(s).

Web-based WHOIS:  
<https://domains.markmonitor.com/whois>

## 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

```
[root@kali]~/.paypal]
# dig paypal.com

; <>> DiG 9.18.1-1-Debian <>> paypal.com
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 28195
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 9355a4e67ea644bd01000000629308a0590e269e69a61f70 (good)
;; QUESTION SECTION:
;paypal.com.           IN      A

;; ANSWER SECTION:
paypal.com.        31      IN      A      64.4.250.36
paypal.com.        31      IN      A      64.4.250.37

;; Query time: 87 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun May 29 01:46:08 EDT 2022
;; MSG SIZE rcvd: 99
```

```
[root@kali]~/.paypal]
#
```

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.dyne...net.
paypal.com.          190     IN      NS      pdns100.ultradns.net.
paypal.com.          190     IN      NS      ns1.p57.dyne...net.
paypal.com.          190     IN      NS      pdns100.ultradns.com.

;; ADDITIONAL SECTION:
ns1.p57.dyne...net.  58311   IN      A       108.59.161.57
ns2.p57.dyne...net.  58311   IN      A       108.59.162.57
pdns100.ultradns.com. 171578  IN      A       156.154.64.100
ns1.p57.dyne...net.  58311   IN      AAAA    2600:2000:2210::57
ns2.p57.dyne...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.dyne...net.
- ❖ pdns100.ultradns.net.
- ❖ ns1.p57.dyne...net.
- ❖ pdns100.ultradns.com.

✓ .xoom.com

```
(root㉿kali)-[~/paypal]
# dig xoom.com

; <>> DiG 9.18.1-1-Debian <>> xoom.com
;; global options: +cmd
;; Got answer:
;; →HEADER← opcode: QUERY, status: NOERROR, id: 48682
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 4, ADDITIONAL: 7

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;xoom.com.           IN      A

;; ANSWER SECTION:
xoom.com.        60      IN      A      64.4.250.37
xoom.com.        60      IN      A      64.4.250.36

;; AUTHORITY SECTION:
xoom.com.        600     IN      NS      ns1.p134.dynect.net.
xoom.com.        600     IN      NS      pdns100.ultradns.com.
xoom.com.        600     IN      NS      ns2.p134.dynect.net.
xoom.com.        600     IN      NS      pdns100.ultradns.net.

;; ADDITIONAL SECTION:
ns1.p134.dynect.net. 30741   IN      A      108.59.161.134
ns2.p134.dynect.net. 30741   IN      A      108.59.162.134
pdns100.ultradns.net. 768     IN      A      156.154.65.100
ns1.p134.dynect.net. 30741   IN      AAAA    2600:2000:2210::134
ns2.p134.dynect.net. 30741   IN      AAAA    2600:2000:2220::134
pdns100.ultradns.net. 19611   IN      AAAA    2610:a1:1014::88

;; Query time: 119 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun May 29 01:46:45 EDT 2022
;; MSG SIZE  rcvd: 314
```

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.dyneet.net.
- ❖ pdns100.ultradns.net.

- ✓ swiftcapital.com

```
(root㉿kali)-[~/paypal]
# dig swiftcapital.com

; <>> DiG 9.18.1-1-Debian <>> swiftcapital.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<- opcode: QUERY, status: NOERROR, id: 32491
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;swiftcapital.com.      IN      A

;; ANSWER SECTION:
swiftcapital.com.      5       IN      A      52.218.180.130

;; AUTHORITY SECTION:
swiftcapital.com.      172349  IN      NS      ns-581.awsdns-08.net.
swiftcapital.com.      172349  IN      NS      ns-1699.awsdns-20.co.uk.
swiftcapital.com.      172349  IN      NS      ns-1187.awsdns-20.org.
swiftcapital.com.      172349  IN      NS      ns-486.awsdns-60.com.

;; ADDITIONAL SECTION:
ns-486.awsdns-60.com.  98829   IN      A      205.251.193.230
ns-581.awsdns-08.NET.  98595   IN      A      205.251.194.69
ns-1187.awsdns-20.org. 98542   IN      A      205.251.196.163
ns-1699.awsdns-20.co.uk. 98552   IN      A      205.251.198.163
ns-486.awsdns-60.com.  98829   IN      AAAA    2600:9000:5301:e600::1
ns-581.awsdns-08.NET.  98595   IN      AAAA    2600:9000:5302:4500::1
ns-1187.awsdns-20.org. 98542   IN      AAAA    2600:9000:5304:a300::1
ns-1699.awsdns-20.co.uk. 98552   IN      AAAA    2600:9000:5306:a300::1

;; Query time: 120 msec
;; SERVER: 192.168.1.1#53(192.168.1.1) (UDP)
;; WHEN: Sun May 29 01:47:36 EDT 2022
;; MSG SIZE rcvd: 394
```

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

```

└─(root㉿kali)-[~]
└─# subfinder -d paypal.com -o paypal.txt

      V           show verbose output
      [ ]          show color in output
      ( )          enable color in output
      -           timing out (default 30)
      -           max time in minutes to wait for enumeration results (default 10)
      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 paypal.com
click.emailspaypal.com
api.xoom.stagepaypal.com
www.xoom.stagepaypal.com
api.xoommultistagepaypal.com
api.xoomunpstagepaypal.com
www.xoomunpstagepaypal.com
www.xoommultistagepaypal.com
pics-fastly.glbpaypal.com
c.glidepaypal.com
view.emailspaypal.com
www-intl.glidepaypal.com
api-3t.sandboxpaypal.com
api-3t.sandbox.glidepaypal.com
financing.paypal.com
qwac.paypal.com
www.headspin.stagepaypal.com
api.headspin.stagepaypal.com
www.stage2du136.stagepaypal.com
api.stage2du136.stagepaypal.com
uptycshappaypal.com
business.paypal.com

```

I found 3581 subdomains for “paypal.com”.

✓ xoom.com

```
(kali㉿kali)-[~/paypal]
$ subfinder -d xoom.com -o xoom.txt

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 xoom.com
sb10.xoom.com
sb20.xoom.com
mx01.xoom.com
sb11.xoom.com
mx11.xoom.com
mta1.xoom.com
sb1.xoom.com
cm1.xoom.com
ns1.xoom.com
sandbox1.xoom.com
mx02.xoom.com
sb12.xoom.com
mx12.xoom.com
sb22.xoom.com
mta2.xoom.com
sb2.xoom.com
jirastg2.xoom.com
cm2.xoom.com
ns2.xoom.com
express2.xoom.com
mx03.xoom.com
sb13.xoom.com
mx13.xoom.com
sb23.xoom.com
sb3.xoom.com
cm3.xoom.com
ns3.xoom.com
mx04.xoom.com
sb14.xoom.com
mx14.xoom.com
sb4.xoom.com
cm4.xoom.com
ns4.xoom.com
mx05.xoom.com
```

I found 1479 subdomains for “xoom.com”.

✓ venmo.com

```
(kali㉿kali)-[~/paypal]$ subfinder -d venmo.com -o venmo.txt
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 venmo.com
help.venmo.com
api.betaweb.venmo.com
api.dev.venmo.com
api.venmo.com
betam.venmo.com
betaweb.venmo.com
dev.venmo.com
developer-api-staging.venmo.com
developer.venmo.com
test1.venmo.com
test2.venmo.com
test3.venmo.com
touch.venmo.com
www.venmo.com
status.venmo.com
fangshengdachuanqisfshenshebanben-virus-20.venmo.com
eset-nod32-antivirus-29730.venmo.com
ip-112-80.venmo.com
viruswall2-ip-112-80.venmo.com
getavirus-com.ip-112-80.venmo.com
antivirussupport-80.venmo.com
1980.venmo.com
goluncov.1980.venmo.com
virust90.venmo.com
ks-vendingtransactions-mq0.venmo.com
virusurvey0.venmo.com
us-east-1.venmo.com
mphx-mkha-virust-1.venmo.com
web3435-virus01.venmo.com
agmpvirus01.venmo.com
virustagin-posprinityreport01.venmo.com
mx01.venmo.com
virus121.venmo.com
norton-antivirus-phamchanhtan91.venmo.com
```

I found 21703 subdomains for “venmo.com”.

## ✓ paypal.me

```
(kali㉿kali)-[~/paypal]
$ subfinder -d paypal.me -o paypalme.txt
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 paypal.me
donate.paypal.me
s.paypal.me
vote.paypal.me
www.paypal.me
localhost.paypal.me
y757moj2bxvh.paypal.me
252fwww.paypal.me
7cwww.paypal.me
3dwww.paypal.me
u003ewww.paypal.me
3ewww.paypal.me
```

I found only 11 subdomains for “paypal.me”

## ✓ Swiftcapital.com

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

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
lynccdiscover.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.

```
└─(kali㉿kali)-[~/paypal]
$ sublist3r -d paypal.com -o paypal1.txt

[!] Error: Virustotal probably now is blocking our requests
[-] Saving results to file: paypal1.txt
[-] Total Unique Subdomains Found: 1214

www.paypal.com
0cd20b6fe61233e4a24bf70f30c9ba46.paypal.com
16695532.paypal.com
64.4.247.24-reservedip.paypal.com
64.4.247.25-reservedip.paypal.com
64.4.247.26-reservedip.paypal.com
64.4.247.27-reservedip.paypal.com
64.4.247.28-reservedip.paypal.com
64.4.247.29-reservedip.paypal.com
64.4.247.30-reservedip.paypal.com
64.4.247.31-reservedip.paypal.com
a.paypal.com
about.paypal.com
active-api-m.paypal.com
active-api-s.paypal.com
active-c.paypal.com
active-history.paypal.com
active-mobile.paypal.com
active-mobileclient.paypal.com
active-pics.paypal.com
ad.paypal.com
admin.paypal.com
adnormserv-slc-a.paypal.com
```

## ✓ xoom.com

I got following result after scanning.

```
(kali㉿kali)-[~/paypal]
$ sublist3r -d xoom.com -o xoom.txt
# [REDACTED]
# Coded By Ahmed Aboul-Ela - @aboula3la

[-] Enumerating subdomains now for xoom.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: xoom.txt
[-] Total Unique Subdomains Found: 263
www.xoom.com
api.xoom.com
atl-panvpn.xoom.com
atl-tcovpn.xoom.com
atl-uat.xoom.com
atl-uat-walmart.xoom.com
atl-walmart.xoom.com
atl-webservices.xoom.com
atl-www.xoom.com
atlvpn.xoom.com
autodiscover.xoom.com
awseg.xoom.com
billpay.xoom.com
bload.xoom.com
blog.xoom.com
bpi.xoom.com
cashapi-sandbox.xoom.com
cashapi2-sandbox.xoom.com
chat.xoom.com
cm1.xoom.com
cm2.xoom.com
cm3.xoom.com
cm4.xoom.com
cm5.xoom.com
```

✓ 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 - @abou13la

[-] 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
0725.abmail.email.venmo.com
0726.abmail.email.venmo.com
0727.abmail.email.venmo.com
0728.abmail.email.venmo.com
0729.abmail.email.venmo.com
```

✓ paypal.me

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

```
(kali㉿kali)-[~/paypal]
$ sublist3r -d paypal.me -o paypalme1.txt

# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for paypal.me
[-] 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: paypalme1.txt
[-] Total Unique Subdomains Found: 3
www.paypal.me
donate.paypal.me
vote.paypal.me
```

✓ swiftcapital.com

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

```
└─(kali㉿kali)-[~/paypal]
└─$ sublist3r -d swiftcapital.com -o swiftcapital.txt


```

# Coded By Ahmed Aboul-Ela - @aboula3la

```
[–] Enumerating subdomains now for swiftcapital.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: swiftcapital.txt
[–] Total Unique Subdomains Found: 15
www.swiftcapital.com
api.swiftcapital.com
autodiscover.swiftcapital.com
dev.swiftcapital.com
enterpriseenrollment.swiftcapital.com
enterpriseregistration.swiftcapital.com
get.swiftcapital.com
go.swiftcapital.com
ist.swiftcapital.com
lyncrediscover.swiftcapital.com
msoid.swiftcapital.com
sip.swiftcapital.com
try.swiftcapital.com
uat.swiftcapital.com
vpn.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

**TOTAL RESULTS: 8,655**

**TOP COUNTRIES:**

- United States: 3,476
- Germany: 1,097
- United Kingdom: 940
- Ireland: 392
- India: 322

**TOP PORTS:**

| Port | Count |
|------|-------|
| 443  | 5,809 |
| 80   | 2,682 |
| 8080 | 144   |
| 8443 | 63    |
| 8000 | 44    |

**TOP ORGANIZATIONS:**

| Organization              | Count |
|---------------------------|-------|
| Amazon Technologies Inc.  | 1,216 |
| DigitalOcean, LLC         | 704   |
| Amazon.com, Inc.          | 402   |
| Amazon Data Services NoVa | 350   |
| Hetzner Online GmbH       | 338   |

**TOP PRODUCTS:**

| Product                         | Count |
|---------------------------------|-------|
| Apache httpd                    | 3,065 |
| nginx                           | 2,796 |
| Microsoft IIS httpd             | 283   |
| LiteSpeed httpd                 | 28    |
| Apache Tomcat/Coyote JSP engine | 11    |

**Findings:**

- ABB Installation Products Intranet Login**: SSL Certificate details, including Issuer (COMODO RSA Extended Validation Secure Server CA), Subject (Thomas A Betts Corporation, United States, Memphis), and supported SSL Versions (TLSv1, TLSv1.1, TLSv1.2).
- 401 Authorization Required**: SSL Certificate details, including Issuer (ZAO Krasnaya PLT, Russian Federation, Moscow) and supported SSL Versions (TLSv1.2, TLSv1.3).
- Bienvenido a ForeverH3**: SSL Certificate details, including Issuer (DigitalOcean, LLC, United States, Santa Clara) and supported SSL Versions (TLSv1.2, TLSv1.3).
- Object moved**: SSL Certificate details, including Issuer (LBBM IT Services GmbH, Germany, Munich) and supported SSL Versions (TLSv1.2, TLSv1.3).

**Logs:**

- HTTP/1.1 200 OK (2022-06-02T06:02:59.473629)
- HTTP/1.1 401 Unauthorized (2022-06-02T06:00:47.161156)
- HTTP/1.1 401 Unauthorized (2022-06-02T06:00:47.161156)
- HTTP/1.1 200 OK (2022-06-02T06:00:24.241805)
- HTTP/1.1 302 Found (2022-06-02T05:58:42.149835)

**Home Page**

90.145.240.189  
90.145.240.189.magento.partnerdevsite.nl  
magento.partnerdevsite.nl  
Europen Nederland BV  
Netherlands, Amsterdam

**SSL Certificate**

Issued By: Let's Encrypt

| Common Name: m  
| Organization: magento.partnerdevsite.nl

Supported SSL Versions: TLSv1.2, TLSv1.3

Diffe-Hellman Fingerprint: RFC3529Oakley Group 14

**44.203.28.122**

44.203.28.122.compmate-1.mozzis.com

Amazon Data Services Nova  
United States, Ashburn

**SSL Certificate**

HTTP/1.1 200 OK  
Date: Thu, 02 Jun 2022 05:56:18 GMT  
Server: Apache/2.4.52 (Ubuntu)  
Set-Cookie: PHPSESSID=0d8c126e097266ka71cq9f7c; expires=Thu, 02-Jun-2022 06:56:18 GMT; Max-Age=3600; path=/; domain=magento.partnerdevsite.nl; expires=Thu, 02-Jun-2023 02:56:18 GMT

**IIS7**

75.157.236.43  
soda.com  
75.157.236.43.soda.melus.net  
T-Mobile Communications Inc.  
Canada, Perinton

**SSL Certificate**

HTTP/1.1 200 OK  
Date: Thu, 02 Jun 2022 05:56:00 GMT  
Server: Apache  
X-Powered-By: PHP/7.3.28  
Pragms: no-cache  
Cache-Control: max-age=0, must-revalidate, no-cache, no-store  
Expires: Wed, 02 Jun 2022 05:56:00 GMT  
X-Magento-Cache-Control: max-age=0, must-revalidate, no-cache, no-store  
X-Ro...

**Home page**

45.54.117.96  
45.54.117.96.ip.ipaddresscontent.c  
t.co  
watched-test-dev.ip-dev.com  
Linode  
United States, Atlanta

**SSL Certificate**

HTTP/1.1 200 OK  
Date: Sat, 29 Nov 2018 03:13:31 GMT  
Last-Modified: Sat, 29 Nov 2018 03:13:31 GMT  
Accept-Ranges: bytes  
Content-Type: text/html; charset=UTF-8  
Server: Microsoft-IIS/7.5  
X-Powered-By: ASP.NET  
Content-Security-Policy: block-all-mixed-content; default-src 'self' 'unsafe-inline' 'unsafe-eval' blob: data:...

**Home page**

54.202.212.93  
dmn-mm-dev.agency  
ec2-54-202.212.93.us-west-2.compute.amazonaws.com  
Amazon.com, Inc.  
United States, Bodman

**SSL Certificate**

HTTP/1.1 200 OK  
Date: Thu, 02 Jun 2022 05:55:13 GMT  
Server: nginx/1.20.1  
Content-Type: text/html; charset=UTF-8  
Transfer-Encoding: chunked  
Connection: keep-alive  
Vary: Accept-Encoding  
X-Powered-By: PHP/4.2.9  
Set-Cookie: PHPSESSID=tltisinfo39vsgf9lakvlsmur; expires=Thu, 02-Jun-2022 06:55:13 GMT

**Home page**

54.202.212.93  
dmn-mm-dev.agency  
ec2-54-202.212.93.us-west-2.compute.amazonaws.com  
Amazon.com, Inc.  
United States, Bodman

**SSL Certificate**

HTTP/1.1 200 OK  
Date: Thu, 02 Jun 2022 05:53:54 GMT  
Server: Apache/2.4.29 (Ubuntu)  
Set-Cookie: PHPSESSID=ddde0rr5c695ewbup14nhirkeo; expires=Thu, 02-Jun-2022 06:53:54 GMT; Max-Age=3600; path=/; domain=dmn-mm-dev.agency

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.

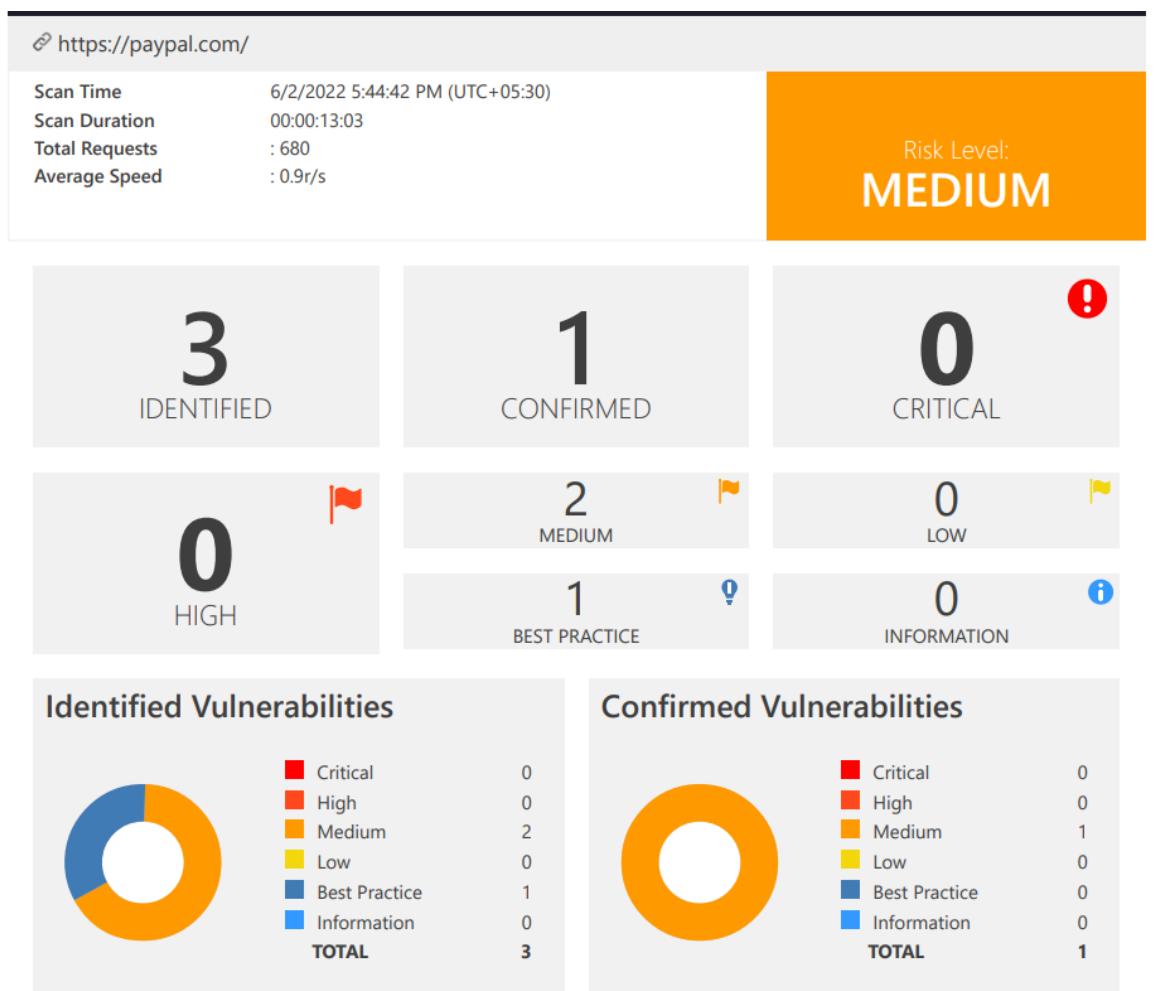
Netsparker is the only scanner that automatically exploits diagnosed vulnerabilities in a read-most effective and secure way, with a view to verify diagnosed issues.

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

## Certainty



## Request

```
GET / HTTP/1.1
Host: paypal.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8
Accept-Encoding: gzip, deflate
Accept-Language: en-us,en;q=0.5
Cache-Control: no-cache
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/79.0.3945.0 Safari/537.36
```

## Response

```
Response Time (ms) : 174.7236   Total Bytes Received : 364   Body Length : 161   Is Compressed : No
```

```
HTTP/1.1 302 Moved Temporarily
Connection: keep-alive
Content-Length: 161
Strict-Transport-Security: max-age=31536000; includeSubDomains
Content-Type: text/html
Location: https://www.paypal.com/

<html>
<head><title>302 Found</title></head>
<body bgcolor="white">
<center><h1>302 Found</h1></center>
<hr><center>Avi Vantage/<center>
</body>
</html>
```

## 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 `regedit32` 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 it impossible for a certificate 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

🔗 <https://xoom.com/>

|                |                                 |                              |
|----------------|---------------------------------|------------------------------|
| Scan Time      | 6/2/2022 4:02:18 PM (UTC+05:30) | Risk Level:<br><b>MEDIUM</b> |
| Scan Duration  | 00:00:10:49                     |                              |
| Total Requests | : 679                           |                              |
| Average Speed  | : 1.0r/s                        |                              |

**3**  
IDENTIFIED

**1**  
CONFIRMED

**0**  
CRITICAL !

**0**  
HIGH !

**2**  
MEDIUM !

**0**  
LOW !

**1**  
BEST PRACTICE !

**0**  
INFORMATION i

**Identified Vulnerabilities**



|               |          |
|---------------|----------|
| Critical      | 0        |
| High          | 0        |
| Medium        | 2        |
| Low           | 0        |
| Best Practice | 1        |
| Information   | 0        |
| <b>TOTAL</b>  | <b>3</b> |

**Confirmed Vulnerabilities**



|               |          |
|---------------|----------|
| Critical      | 0        |
| High          | 0        |
| Medium        | 1        |
| Low           | 0        |
| Best Practice | 0        |
| Information   | 0        |
| <b>TOTAL</b>  | <b>1</b> |

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

🔗 https://venmo.com/

Scan Time 6/2/2022 4:26:34 PM (UTC+05:30)  
Scan Duration 00:00:18:58  
Total Requests : 18,751  
Average Speed : 16.5r/s

Risk Level:  
**MEDIUM**

**27**  
IDENTIFIED

**11**  
CONFIRMED

**0**  
CRITICAL

**0**  
HIGH

**2**  
MEDIUM

**5**  
LOW

6 BEST PRACTICE

14 INFORMATION

#### Identified Vulnerabilities



|               |           |
|---------------|-----------|
| Critical      | 0         |
| High          | 0         |
| Medium        | 2         |
| Low           | 5         |
| Best Practice | 6         |
| Information   | 14        |
| <b>TOTAL</b>  | <b>27</b> |

#### Confirmed Vulnerabilities



|               |           |
|---------------|-----------|
| Critical      | 0         |
| High          | 0         |
| Medium        | 1         |
| Low           | 4         |
| Best Practice | 2         |
| Information   | 4         |
| <b>TOTAL</b>  | <b>11</b> |

Netsparker found following vulnerabilities.

# Vulnerability Summary

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

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

| CONFIRM | VULNERABILITY | METHOD   | URL | PARAMETER                         |
|---------|---------------|--|-----|-----------------------------------|
|         |               | <a href="#">Reverse Proxy Detected (Envoy)</a>   | GET | https://venmo.com/                |
|         |               | <a href="#">Sitemap Detected</a>   | GET | https://venmo.com/sitemap.xml     |
|         |               | <a href="#">Wildcard Detected in Domain Portion of Content Security Policy (CSP), Directive</a>    | GET | https://venmo.com/static-assets/  |
|         |               | <a href="#">Autocomplete Enabled (Password Field)</a>  | GET | https://venmo.com/account/sign-in |
|         |               | <a href="#">Cross-site Referrer Leakage through usage of the origin keyword in Referrer-Policy</a> | GET | https://venmo.com/account/sign-in |
|         |               | <a href="#">Forbidden Resource</a>   | GET | https://venmo.com/c/boot.ini      |
|         |               | <a href="#">Robots.txt Detected</a>  | GET | https://venmo.com/robots.txt      |

## 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 `sandbox`attribute 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 `sandbox`attribute 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-popupswill` allow popups.
- `allow-scripts`will allow malicious script execution however it won't allow to create popups.

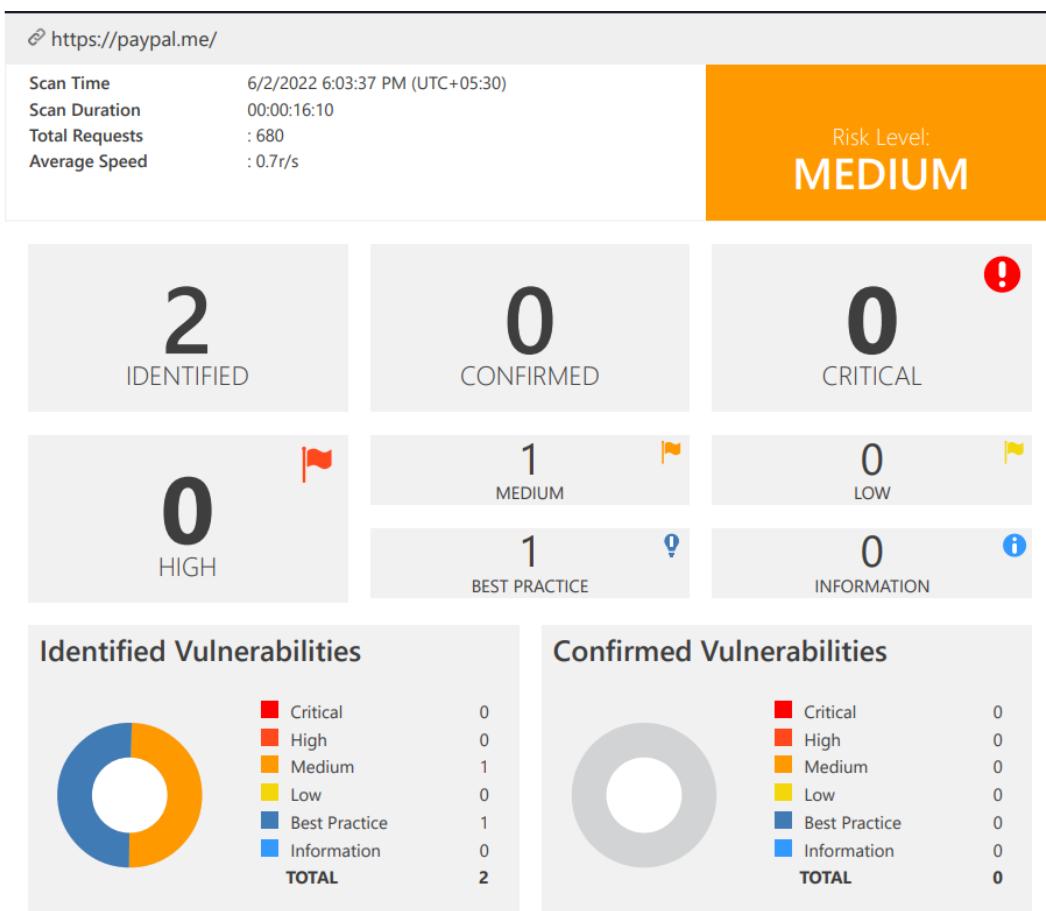
## How to prevent

- 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

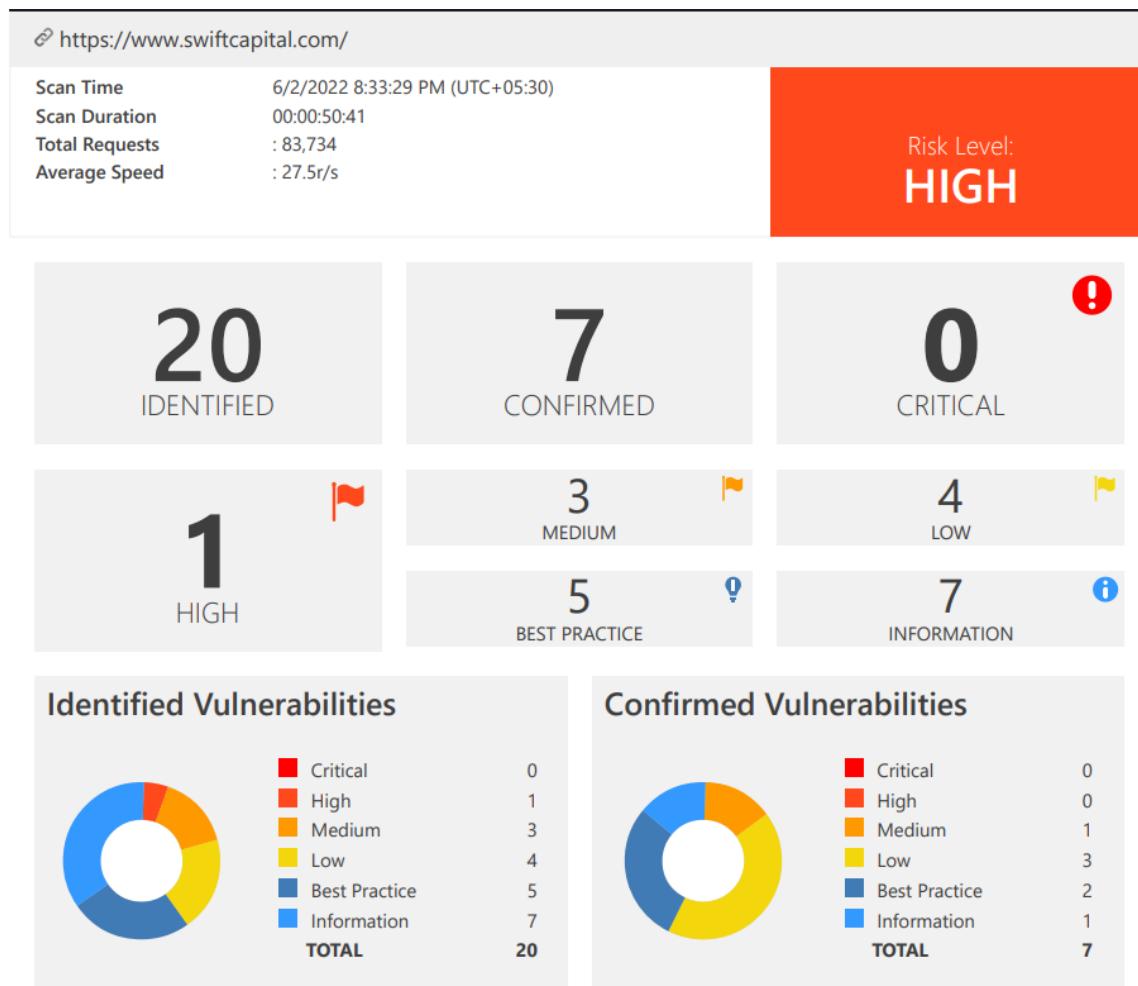


Netsparker detected only two vulnerabilities.

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

- Expect-CT Not Enabled.

✓ [www.swiftcapital.com](https://www.swiftcapital.com/)



Netsparker identified 20 vulnerabilities.

# Vulnerability Summary

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

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

## Out-of-date Version (AngularJS)

- Identified Version: 1.6.6
- Latest Version: 1.8.3

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 &quot;&lt;option&gt;&quot; elements in &quot;&lt;select&gt;&quot; 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 &lt;option&gt; 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:

The screenshot shows the OWASP ZAP 2.11.1 interface. In the top center, it says "Automated Scan". Below that, there's a note: "This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'. Please be aware that you should only attack applications that you have been specifically given permission to test." A text input field contains "https://zoom.com". Underneath, there are checkboxes for "Use traditional spider" (which is checked), "Use ajax spider", and "with Firefox Headless". Buttons for "Attack" and "Stop" are present. To the right is a progress bar at 100% completion. At the bottom, a table titled "Spider" lists the following data:

| Processed | Method | URI                              | Flags        |
|-----------|--------|----------------------------------|--------------|
| GET       | GET    | https://zoom.com/robots.txt      | Seed         |
| GET       | GET    | https://zoom.com/sitemap.xml     | Seed         |
| GET       | GET    | https://www.zoom.com/            | Out of Scope |
| GET       | GET    | https://www.zoom.com/robots.txt  | Out of Scope |
| GET       | GET    | https://www.zoom.com/sitemap.xml | Out of Scope |

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

| Site   | Risk             |                       |              |                      | Informational<br>al) |
|--|------------------|-----------------------|--------------|----------------------|----------------------|
|  | High<br>(= High) | Medium<br>(>= Medium) | Low (>= Low) | Information<br>ation |                      |
|  | 0<br>(0)         | 1<br>(1)              | 0<br>(1)     | 0<br>(1)             |                      |
| <a href="https://www.swiftcapital.com">https://www.swiftcapital.co<br/>m</a> | 0<br>(0)         | 1<br>(1)              | 0<br>(1)     | 0<br>(1)             | 0<br>(1)             |
| <a href="https://venmo.com">https://venmo.com</a>                            | 0<br>(0)         | 4<br>(4)              | 2<br>(6)     | 1<br>(7)             | 1<br>(7)             |
| <a href="https://xoom.com">https://xoom.com</a>                              | 0<br>(0)         | 0<br>(0)              | 1<br>(1)     | 2<br>(3)             | 2<br>(3)             |
| <a href="https://paypal.com">https://paypal.com</a>                          | 0<br>(0)         | 2<br>(2)              | 5<br>(7)     | 0<br>(7)             | 0<br>(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.

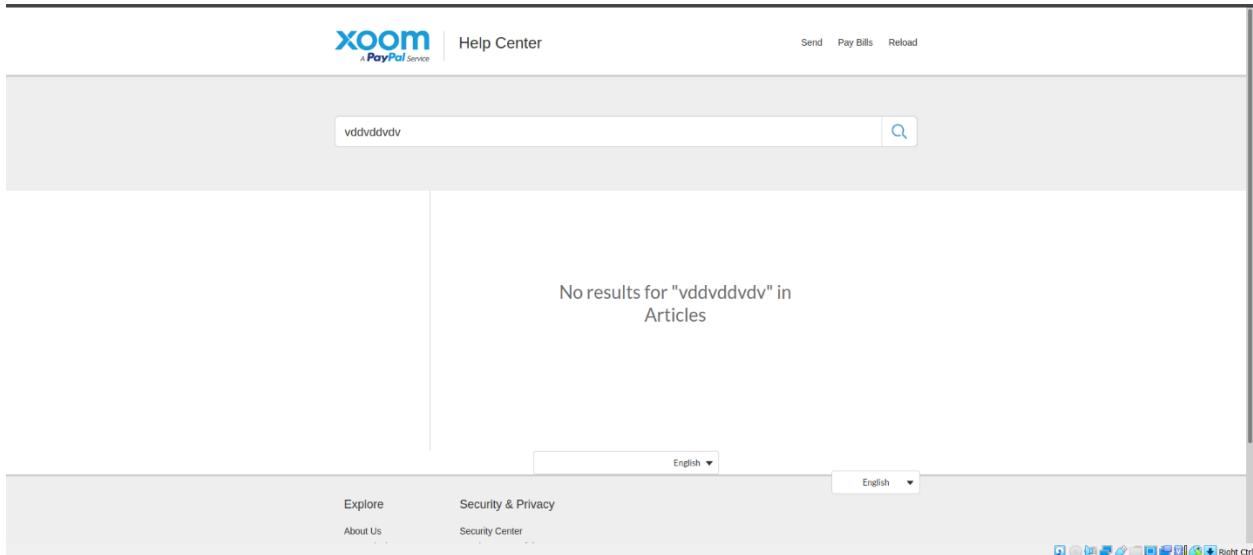
(The percentages in brackets represent each count as a percentage, rounded to one decimal place, of the total number of alerts included in this report.)

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

|  |               |                   |
|--|---------------|-------------------|
| <a href="#"><u>X-Content-Type-Options Header Missing</u></a>                 | Low           | 133<br>(738.9%)   |
| <a href="#"><u>Information Disclosure - Sensitive Information in URL</u></a> | Informational | 2<br>(11.1%)      |
| <a href="#"><u>Information Disclosure - Suspicious Comments</u></a>          | Informational | 61<br>(338.9%)    |
| <a href="#"><u>Re-examine Cache-control Directives</u></a>                   | Informational | 223<br>(1,238.9%) |
| <b>Total</b>   |               | <b>18</b>         |

## Try XSS Attack 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.

The screenshot shows the Burp Suite interface with several captured requests listed in the main pane. One specific request is highlighted in orange, which corresponds to the one shown in expanded detail in the lower half of the screen. The expanded view shows the raw request payload, which includes a complex URL with parameters like 'language=en\_US' and 'id=1'. The request is sent via GET to the URL `/global-search/individual/language=...`. The expanded view also includes tabs for Request, Response, Hex, and ASCII, along with an Inspector panel on the right containing detailed information about the request attributes, query parameters, cookies, and headers.

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>.

The screenshot shows the Burp Suite interface with the 'Proxy' tab selected. Under 'Payload Sets', there is a dropdown for 'Payload set' (set to 1) and 'Request count' (set to 6,606). Below it, 'Payload type' is set to 'Simple list'. A note says 'You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.' A 'Start attack' button is visible in the top right.

**Payload Options [Simple list]**  
This payload type lets you configure a simple list of strings that are used as payloads.

A list of payload items is shown, including:  
- <audio><script><alert></script></audio>  
- <audio><content><menu><alert></menu></content></table></audio>  
- <audio><script><alert></script></audio>  
- <audio><script><table><tbody><tr><td><script><alert></script></td></tr></tbody></table></audio>  
- <audio><onfocus><alert()></audio>  
- <audio><onkeydown><alert()></audio>  
- <audio><onkeydown><alert()></audio>  
- <audio><onkeyup><alert()></audio>  
- <audio><onload><alert()></audio>

**Add** Enter a new item  
Add from list... [Pro version only]

**Payload Processing**  
You can define rules to perform various processing tasks on each payload before it is used.

Enabled Rule

Add Edit Remove Up Down

**Payload Encoding**  
This setting can be used to URL-encode selected characters within the final payload, for safe transmission within HTTP requests.

URL-encode these characters: /%c>%4-%||^#

Then I launched attack.

The screenshot shows the Burp Suite interface with the 'Intruder' tab selected. The 'Attack type' is set to 'Splicer'. The 'Payload Positions' section indicates there are 6606 payload positions. The 'Results' tab shows a table of attack results:

| Request | Payload                        | Status | Error | Timeout | Length | Comment |
|---------|--------------------------------|--------|-------|---------|--------|---------|
| 1       | " prompt(); "                  | 200    | ✓     | ✓       | 81930  |         |
| 2       | " prompt(); "                  | 301    | ✓     | ✓       | 839    |         |
| 3       | " prompt(); "                  | 301    | ✓     | ✓       | 939    |         |
| 4       | " xprompt(); "                 | 301    | ✓     | ✓       | 944    |         |
| 5       | " eval(window['prompt']); "    | 301    | ✓     | ✓       | 944    |         |
| 6       | " eval(window['prompt2']); "   | 301    | ✓     | ✓       | 982    |         |
| 7       | " onclick=prompt(); " onload=" | 301    | ✓     | ✓       | 996    |         |
| 8       | " onclick=prompt(); " onload=" | 301    | ✓     | ✓       | 953    |         |
| 9       |          | 301    | ✓     | ✓       | 926    |         |
| 10      |          | 301    | ✓     | ✓       | 924    |         |
| 11      |          | 301    | ✓     | ✓       | 932    |         |
| 12      |          | 301    | ✓     | ✓       | 930    |         |
| 13      |          | 301    | ✓     | ✓       | 968    |         |
| 14      |          | 301    | ✓     | ✓       | 946    |         |

0 matches Clear Refresh

payload position

After attack, I didn't find 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. Those 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.