SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY

WEB SECURITY (IE2062)

IT20059422 | WICKRAMASINGHE W A N

Vulnerability Analysis Report
GOLDMAN SACHS

By Wickramasinghe WAN| IT20059422

Sri Lanka Institute of Information Technology, Malabe, Sri Lanka

TERMS OF REFERENCE

THIS REPORT IS ABOUT BUG BOUNTY HUNTING. THIS WEB AUDIT FOCUSING ON SELECTED WEB DOMAIN SUB DOMAIN AND COMPLETE WEB SECURITY (IE2062) MODULE ASSIGNMENT. THIS PROJECT IS BEING CONDUCTED UNDER DEPARTMENT OF COMPUTER SYSTEMS ENGINEERING, SRI LANKA INSTITUTE OF INFORMATION TECHNOLOGY, MALABE, SRI LANKA.

ACKNOWLEDGMENT

I WOULD LIKE TO THANK DR.LANKAMAL RUPASINGHE HEAD OF WEB SECURITY (IE2026) FOR HIS CONTRIBUTIONS TO THE DEVELOPMENT OF PRACTICAL SKILLS AND MS. CHETHANA LIYANAPATHIRANA, MS. MENAKA MOONAMALDENIYA AND CHATHU UDAGEDARA FOR THEIR IMMEANSE SUPPORT AND GUIDANCE ON THIS WEB AUDIT.

ABSTRACT

BUG BOUNTY PROGRAMS PROVIDE ORGANIZATIONS THE ABILITY TO CROWDSOURCE SECURITY TESTING TO IDENTIFY AND REMEDIATE VULNERABILITIES. WHILE THE CONCEPT OF CROWDSOURCING SECURITY TESTING IS SOMEWHAT NEW, THE FOUNDATIONAL ROOTS CAN BE TRACED BACK TO PENETRATION TESTING ACTIVITIES. WITHIN THE LAST 10 YEARS, BUG BOUNTY PROGRAMS ARE STARTING TO GAIN TRACTION IN THE INFORMATION SECURITY INDUSTRY. AS BUG BOUNTY PROGRAMS CONTINUE TO BECOME MORE COMMONPLACE, THERE IS A NEED TO EVALUATE BOTH BUG BOUNTY PROGRAMS AND THE PLATFORMS THE PROGRAMS ARE HOSTED ON. THE PURPOSE OF THIS RESEARCH WAS TO EXAMINE HOW BUG BOUNTY PROGRAMS ARE ESTABLISHED, MAINTAINED, AND VIABLE. THERE IS ONLY A HANDFUL OF BUG BOUNTY PLATFORMS IN EXISTENCE THAT CONTROL MOST OF ALL BUG BOUNTY PROGRAMS. THESE PROGRAMS CAN BE CHALLENGING TO SET UP INITIALLY AND TO MAINTAIN BUT BRING SEVERAL SECURITY BENEFITS TO ANY ORGANIZATION WILLING TO ESTABLISH ONE. THE FINDINGS OF THIS RESEARCH ULTIMATELY REVEALED A NEED FOR A BUG BOUNTY OVERSIGHT COMMITTEE AND AN INCREASE IN PUBLIC VULNERABILITY DISCLOSURES. KEYWORDS: CYBERSECURITY, DR. CHRISTOPHER RIDDELL, BUG BOUNTY, VULNERABILITY DISCLOSURE, SECURITY RESEARCHER.

CONTENTS

WHAT IS WEB SECURITY

As technology changes, it becomes increasingly challenging for businesses of all types to keep their personal and customer's information on the web secure.

Web security is important to keeping hackers and cyber-thieves from accessing sensitive information. Without a proactive security strategy, businesses risk the spread and escalation of malware, attacks on other websites, networks, and other IT infrastructures. If a hacker is successful, attacks can spread from computer to computer, making it difficult to find the origin.

There are many ways to know if a website is secure, including implementing HTTPS on your website. In addition to HTTPS, you can tell if a website is trustworthy by asking yourself: [1]

- Is the website an established authority institution?
- Does the site provide expert value?
- Does the website look spammy, broken?
- When I hover over the links does the link look spammy?

Web security is also known as "Cybersecurity". It basically means protecting a website or web application by detecting, preventing, and responding to cyber threats.

Websites and web applications are just as prone to security breaches as physical homes, stores, and government locations. Unfortunately, cybercrime happens every day, and great web security measures are needed to protect websites and web applications from becoming compromised.

That's exactly what web security does – it is a system of protection measures and protocols that can protect your website or web application from being hacked or entered by unauthorized personnel. This integral division of Information Security is vital to the protection of websites,

web applications, and web services. Anything that is applied over the Internet should have some form of web security to protect it.

Details of Web Security

There are a lot of factors that go into web security and web protection. Any website or application that is secure is surely backed by different types of checkpoints and techniques for keeping it safe.

There are a variety of security standards that must be always followed, and these standards are implemented and highlighted by the OWASP. Most experienced web developers from **top cybersecurity companies** will follow the standards of the OWASP as well as keep a close eye on the Web Hacking Incident Database to see when, how, and why different people are hacking different websites and services.

Essential steps in protecting web apps from attacks include applying up-to-date encryption, setting proper authentication, continuously patching discovered vulnerabilities, avoiding data theft by having secure software development practices. The reality is that clever attackers may be competent enough to find flaws even in a robust secured environment, and so a holistic security strategy is advised.

Available Technology

There are different types of technologies available for maintaining the best security standards. Some popular technical solutions for testing, building, and preventing threats include:

- Black box testing tools
- Fuzzing tools
- White box testing tools
- Web application firewalls (WAF)
- Security or vulnerability scanners
- Password cracking tools

Your website or web application's security depends on the level of protection tools that have been equipped and tested on it. There are a few major threats to security which are the most common ways in which a website or web application becomes hacked. Some of the top vulnerabilities for all web-based services include:

- SQL injection
- Password breach
- Cross-site scripting
- Data breach
- Remote file inclusion
- Code injection

Preventing these common threats is the key to making sure that your web-based service is practicing the best methods of security.

The Best Strategies

There are two big defense strategies that a developer can use to protect their website or web application. The two main methods are as follows:

- **Resource assignment** – By assigning all necessary resources to causes that are dedicated to alerting the developer about new web security issues and threats, the developer can receive a constant and updated alert system that will help them detect and eradicate any threats before security is officially breached.
- **Web scanning** – There are several web scanning solutions already in existence that are available for purchase or download. These solutions, however, are only good for known vulnerability threats – seeking unknown threats can be much more complicated. This method can protect against many breaches, however, and is proven to keep websites safe in the long run.

Web Security also protects the visitors from the below-mentioned points –

- **Stolen Data:** Cyber-criminals frequently hacks visitor's data that is stored on a website like email addresses, payment information, and a few other details.
- **Phishing schemes:** This is not just related to email, but through phishing, hackers design a layout that looks exactly like the website to trick the user by compelling them to give their sensitive details.
- **Session hijacking:** Certain cyber attackers can take over a user's session and compel them to take undesired actions on a site.
- **Malicious redirects.** Sometimes the attacks can redirect visitors from the site they visited to a malicious website.
- **SEO Spam.** Unusual links, pages, and comments can be displayed on a site by the hackers to distract your visitors and drive traffic to malicious websites.

Thus, web security is easy to install, and it also helps the businesspeople to make their website safe and secure. A web application firewall prevents automated attacks that usually target small or lesser-known websites. These attacks are borne out by malicious bots or malware that automatically scan for vulnerabilities they can misuse, or cause DDoS attacks that slow down or crash your website.

Thus, Web security is extremely important, especially for websites or web applications that deal with confidential, private, or protected information. Security methods are evolving to match the different types of vulnerabilities that come into existence. [2]

WHAT IS A VULNERABILITY

A vulnerability, in information technology (IT), is a flaw in code or design that creates a potential point of security compromise for an endpoint or network. Vulnerabilities create possible attack vectors, through which an intruder could run code or access a target system's memory. The means by which vulnerabilities are exploited are varied and include code injection and buffer overruns; they may be conducted through hacking scripts, applications, and free hand coding. A zero-day exploit, for example, takes place as soon as a vulnerability becomes generally known.

The question of when to make a vulnerability disclosure public remains a contentious issue. Some security experts argue for full and immediate disclosure, including the specific information that could be used to exploit the vulnerability. Proponents of immediate disclosure maintain that it leads to more patching of vulnerabilities and more secure software. Those against vulnerability disclosure argue that information about vulnerabilities should not be published at all, because the information can be used by an intruder. To mitigate risk, many experts believe that limited information should be made available to a selected group after some specified amount of time has elapsed since detection.

Both black hats and white hats regularly search for vulnerabilities and test exploits. Some companies offer bug bounties to encourage white hat hackers to look for vulnerabilities. Typically, payment amounts are commensurate with the size of the organization, the difficulty in hacking the system and how much impact on users a bug might have. [3]

WHAT IS VULNERABILITY ANALYSIS

A vulnerability assessment is a risk management process used to identify, quantify and rank possible vulnerabilities to threats in a given system. It is not isolated to a single field and is applied to systems across different industries, such as:

- IT systems
- Energy and other utility systems
- Transportation
- Communication systems

The key component of a vulnerability assessment is the proper definition for impact loss rating and the system's vulnerability to that specific threat. Impact loss differs per system. For example, an assessed air traffic control tower may consider a few minutes of downtime as a serious impact loss, while for a local government office, those few minutes of impact loss may be negligible.

Vulnerability assessments are designed to yield a ranked or prioritized list of a system's vulnerabilities for various kinds of threats. Organizations that use these assessments are aware of security risks and understand they need help identifying and prioritizing potential issues. By understanding their vulnerabilities, an organization can formulate solutions and patches for those vulnerabilities for incorporation with their risk management system.

The perspective of a vulnerability may differ, depending on the system assessed. For example, a utility system, like power and water, may prioritize vulnerabilities to items that could disrupt services or damage facilities, like calamities, tampering and terrorist attacks. However, an information system (IS), like a website with databases, may require an assessment of its vulnerability to hackers and other forms of cyberattack. On the other hand, a data center may require an assessment of both physical and virtual vulnerabilities because it requires security for its physical facility and cyber presence. [4]

WEB SECURITY AUDITS

A Security Audit refers to the systematic evaluation of the security of an organization's information system. While performing a security assessment, how well the IT system confirms to a set of established criteria is also checked. Note that a thorough and in-depth audit usually analyses the security related to the physical configuration of the system. It also examines the software information handling processes and user practices. It is worth mentioning here that reliable security audit services can analyze your whole IT infrastructure along with its loopholes and vulnerabilities. Security audits can be broken down into two processes – Penetration testing and Vulnerability assessments. Let's take a glance at the significance of security audits and its varied types.

What is the primary purpose of a security audit?

A security audit is referred to as a high-level description of the variety of ways through which an organization can analyze their overall security posture. This also includes safe trading in the cybersecurity sphere. This also involves thorough scrutiny of the operating systems, applications, etc. Security audits are focused on vulnerability scans and penetration testing to discover potential flaws that can be exploited by attackers.

How do you perform a security audit?

To be frank, there exist innumerable ways that can help you perform a security audit. However, while performing a security audit, the workflow of the audit should be determined. For instance, you must define the assessment criteria clearly. While preparing the security audit, you must select the tools and methodologies to meet the goals. While carrying on with the security audit process, you must monitor the important data points for precision. So, let's look at the various ways with the help of which you can perform security audits.

1. Vulnerability scanners

To be precise, these tools are one of the most basic ways to discover your system's vulnerabilities and loopholes. There is a plethora of online vulnerability scanners available nowadays. For instance, Astra's Website Scanner is one of the most favored vulnerability scanners out there.

2. Manual Security Audits

You can perform a security audit manually by using your intelligence and analytical mind to weigh the seriousness of a particular threat. Interestingly, manual audits also require the help of automated tools to perform an audit successfully. However, manual audits are strictly prohibited to be performed by novices as there are certain security breaches that can easily pass their eye.

3. Automated security audits

Automated security audit**s** are the latest way of analyzing the vulnerability of your IT systems. Automated tools for security auditing are fast and take off a lot of stress from you. Moreover, most of them are available for free which is a great thing. However, there are certain downsides to automated security audits too. Automated auditing tools are quite limited in their reach. They may not uncover all types of security vulnerabilities that are present in your systems and IT infrastructure. In other words, it creates an illusion that you are safe, when in fact, you are not.

4. Security audit services from professionals

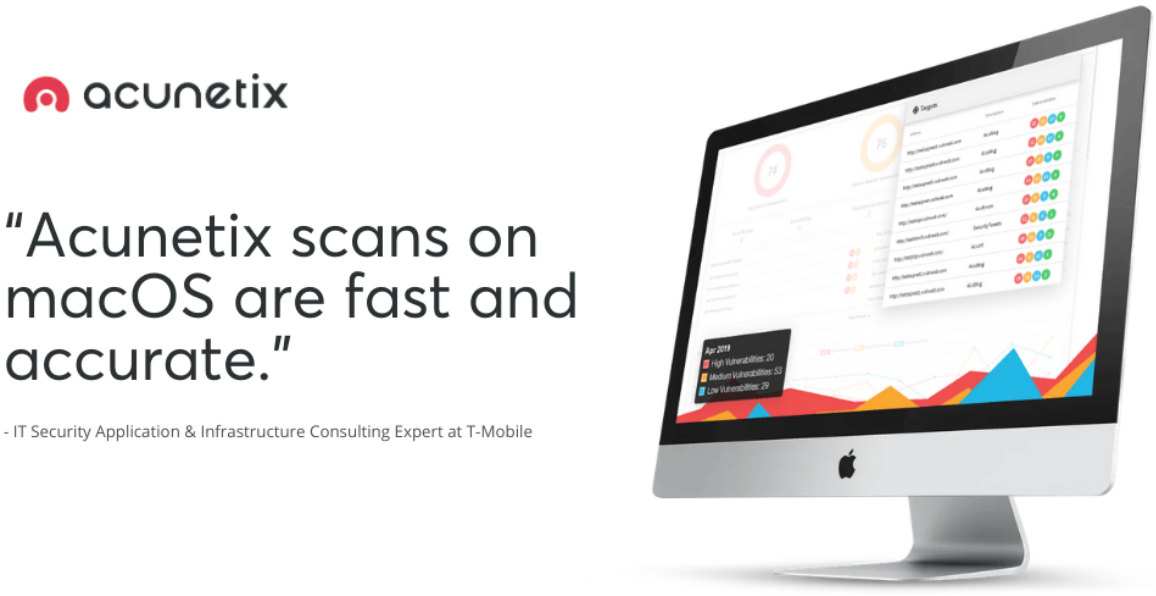
As a business owner, it is not always possible for you to carry out your organization's security audits. Moreover, if you have branches in various parts of the world, it is seemingly impossible for you to execute a security audit all by yourself. This is where the professional security audit services come to the fore. They follow a nuanced procedure of security scrutiny which ensures that none of the security breaches and vulnerabilities is missed. Professional security audit services also provide you with comprehensive reports highlighting the stronger and weaker areas of your IT infrastructure. [5]

TYPES OF WEB SECURITY AUDITS

Astra Security

Astra provides you with a wide range of benefits which you would find nowhere. The VAPT services provided by Astra come in various plans which depict practicality to the business owners. Astra provides a collaborative and intuitive dashboard with the help of which you can keep a real-time track on the proceedings. Post the audit, Astra security experts also go the extra way to assist your developers in fixing those vulnerabilities. Astra also performs a prompt rescan to make sure that there are no underlying security breaches.

Acunetix



Quite impressively, Acunetix can recognize more than 7000 vulnerabilities in custom and open source apps. Its AcuSensor feature allows you to explore and test the hidden inputs which are not found during normal auditing. On the other hand, it comes with advanced authentication and crawling support which ensures you with the option to assess security breaches in JavaScript websites. With Acunetix, you can also track fixed issues to determine whether or not they are reappearing.

Netsparker

Netsparker is a fully scalable and integrated web application with built-in functionalities which makes the process of security audits easier. It is primarily associated with fortifying your web security processes. Interestingly, you can perform an automatic vulnerability assessment which would help you to prioritize your work on fixing several issues. It can automatically crawl and scan a wide range of modern web apps and sites. [5]

HOW TO STRAT BUG BOUNTY HUNTING

First of all, it doesn't matter, if you're not from the computer science field you can always learn and start from square one.
So if you're willing to learn how to become a bug bounty hunter, you'll enjoy the actionable steps in this definitive guide.
Without any further ado, let's dive right in the step-by-step process.
As you may already know all the websites, programs, software, and applications are created with writing codes using various programming languages.
But sometimes things go blue and the applications behave differently from their intended behavior.
The term, '**bug bounty hunting**' means finding technical errors in the coding scripts that can compromise the security of any application, validating and reporting the error to the concerned authority, and in return, you get a reward in monetary terms and recognition for your work. [6]

PLATFORMS

Now the next step is deciding a suitable platform for your first bug hunting. Since you are a fresher into this field, therefore you need to follow a different methodology to find a bug bounty platforms. You need to wisely decide your these platform. In order to do so, you should find those platforms which are less crowded and less competitive. And these platforms are the ones that don't offer monetary benefits rather they provide recognition, points, and reputations only and not exactly bounty. When you are just starting out, you **should not run for the money,** instead, you need to **focus on experience,** reputation points, and hall of fame.
Once you select a decent platform for bug hunting and decide a particular website or application to find bugs, now the next step is to decide what type of bug you will find, whether it's cross-site scripting, or injection, or any other. **You need to work systematically by focusing on one type of bug at a time.** Now once you select one specific type of bug, you need to do an exhaustive search and apply all the knowledge to find for the specific type of bug.
Finding a bug will not be straightforward, and even in case if you find something easily and report it. There are huge chances that it has already reported and then you will get a duplicate flag and will not receive the bounty. [6] [7]

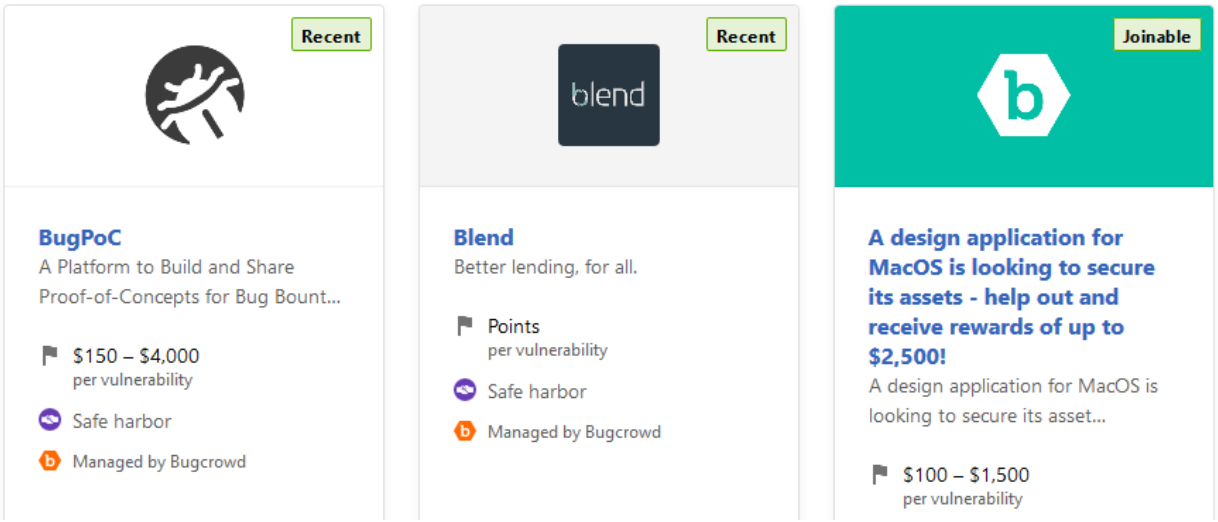
1. HackerOne

   HackerOne is undoubtedly the world's largest ethical hacking community. Experts from almost all countries participate and collaborate on this platform. They host some of the largest companies in their bug bounty programs.

   As an ethical hacker, you can join the community and participate in their bounty programs. Hackers have earned over $100 million in cash rewards for finding vulnerabilities and weaknesses in web apps. They also have a hacking class that allows you to learn the basic principles of web hacking.
   All you need to do is signup for an account and create your profile. To participate in the programs, you can browse through the list here. The rewards are mentioned against each program.

2. BugCrowd

BugCrowd is a similar platforms that allows you to join as a security researcher and help companies find weaknesses in their websites. They offer many public bounties that you can take part in and earn money.



Once you find a vulnerability, you can create a Bug report and submit it to the specific organization to which it belongs. Once they review your report and accept it, you will receive instant payments. You can browse through the available programs from this list. The platform supports payments via Paypal and Payoneer.
If you have good feedback rating and performance statistics, you might get invites to private programs that companies offer frequently.

3. Yogosha

Yogosha is a popular ethical hacking community that accepts applications from all over the world. It's a close community that offers private bounty programs to the successful candidates.

Getting into Yogosha is a bit harder than other platforms. They have a rigorous testing process that only 25 percent of candidates are able to pass on average. Before you start with the selection process, make sure that you have all the knowledge and skills required for website pen testing.

The company also evaluates you for your trustworthiness and reliability. So don't bother submitting the application unless you know what you're doing.

4. SafeHats

SafeHats is a globally managed bug bounty platform that hires the best of the best security researchers to join their team. They call it the "SafeHats Tiger Team".

As a researcher, you can apply to be a part of their elite team. You will be assessed for your experience, skills and intelligence. The getting in part is hard but once you do, you will enjoy some exclusive benefits.

As a Tiger team member, you will gain hands-on experience with the latest tools and equipment available in the market.You might also get access to some private exclusive programs. Additionally, you get a SafeHats Tiger badge that you can brag about.

5. Intigriti

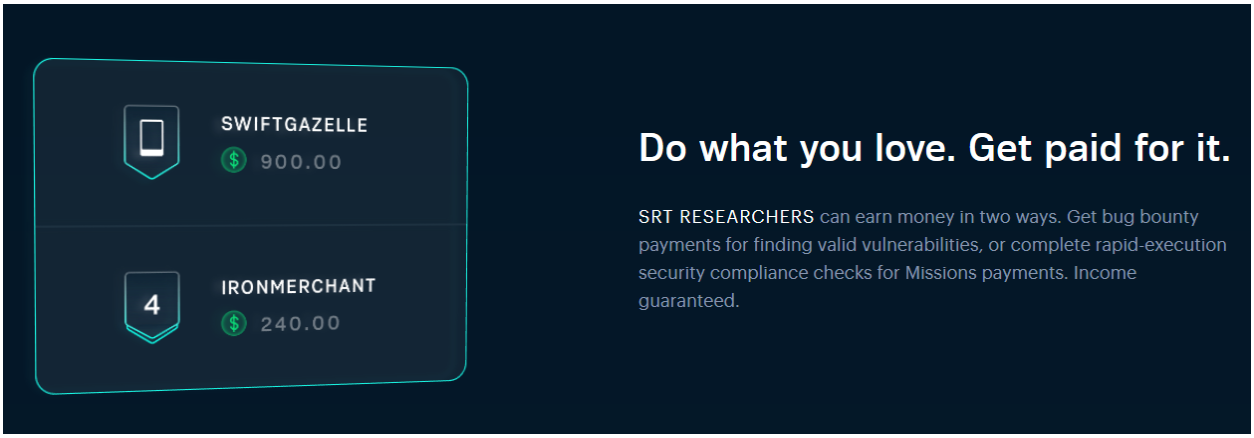
Intigriti is one of the biggest online communities for cyber security experts in Europe. They offer you complete flexibility to work according to your own schedule.

The best feature about the platform is the variety of industries you're able to work for. This includes Web hacking, Network hacking or IoT. They also have a ranking system that allows you to compete with other experts.

Their payment mechanism is exceptionally good. Once your report is accepted, you will be paid instantly via Wire Transfer, Paypal or Payoneer.

6. SynAck

SynAck is a renowned global penetration testing platform that works with clients all over the globe. As a security expert, you can join their "Red Team" which is an elite team of researchers from over 80 countries.

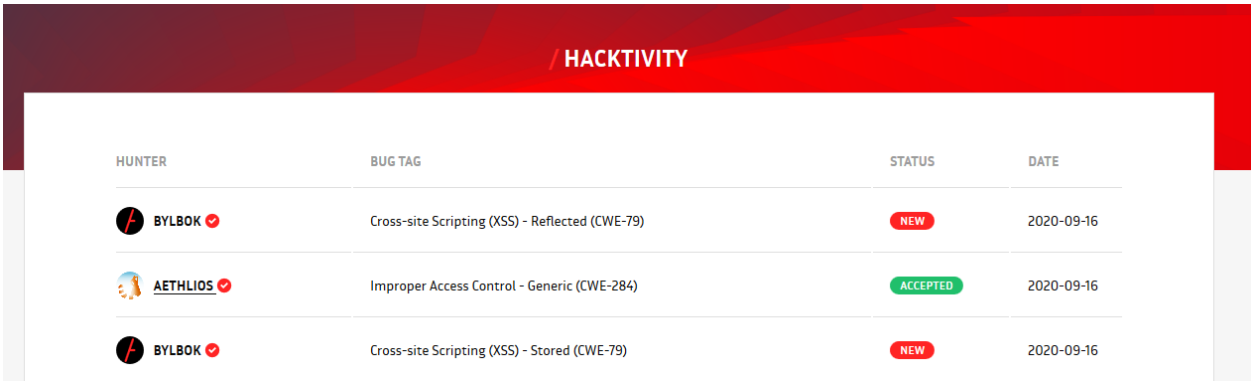


They have a detailed selection process after which you will get accepted into a recognized team of experts. As a member, you will be working with some of the largest brands to secure their systems and web apps.

As you progress on the platform, you will achieve new levels. You will receive instant payments as soon as your reported vulnerabilities get accepted.

7. YesWeHack

YesWeHack is a global bug bounty platform that hires hackers from all over the world. As a researcher, you will be working with global clients to secure their web applications. The amount you can earn as bounty depends on the severity of the vulnerability itself. If it's critical, you should expect a higher payout than usual.



Researchers are awarded points based on their experience. The interaction with clients also plays an important role in determining your level. The more points you have, the more money you can earn.

8. HackenProof

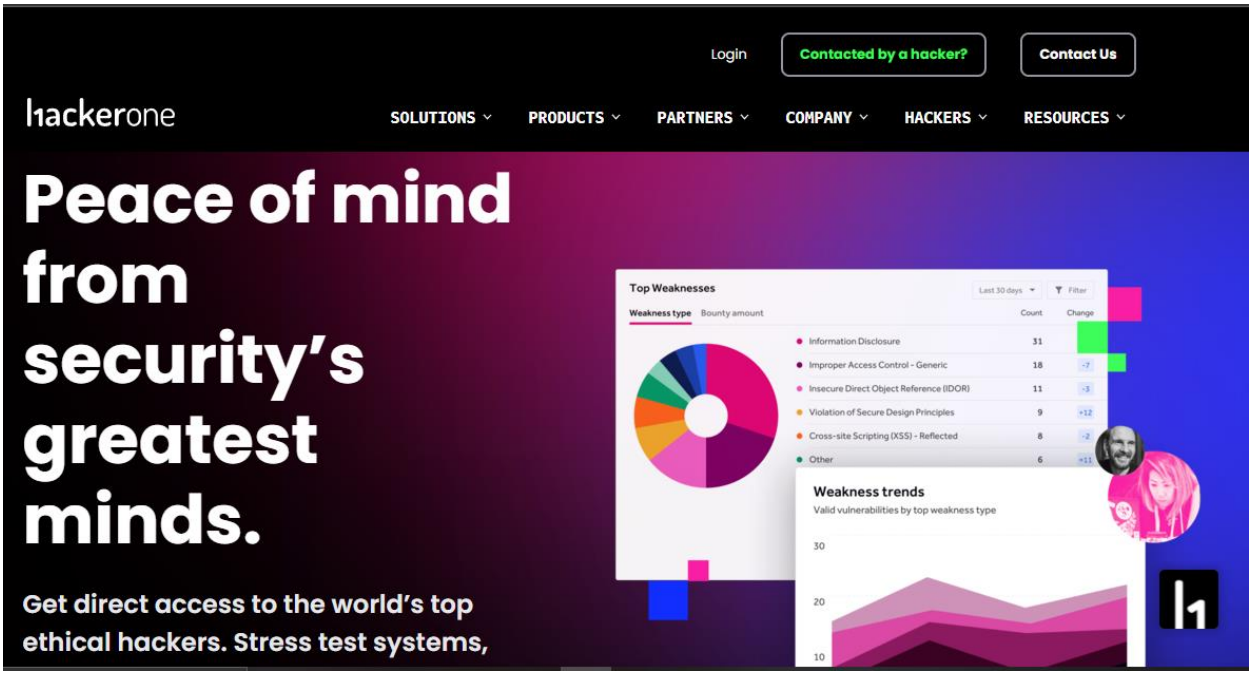
HackenProof is a cyber security coordination platforms that connect security researchers to work in bug bounty programs. As a hacker, you will be able to participate in multiple programs and submit reports for each vulnerability that you discover.

For each report that you submit, you will earn some points. Those points are in the form of "USDT". You can convert them to local currently via their exchanges. Here's the list of exchanges that they support.

9. UpSecurit

UpSecurit is a global platform that invites ethical hackers to join their team of researchers. As a member, you will enjoy exclusive features of their Bug hunter club. You can start earning money from day one by participating in the bounty programs. [8]

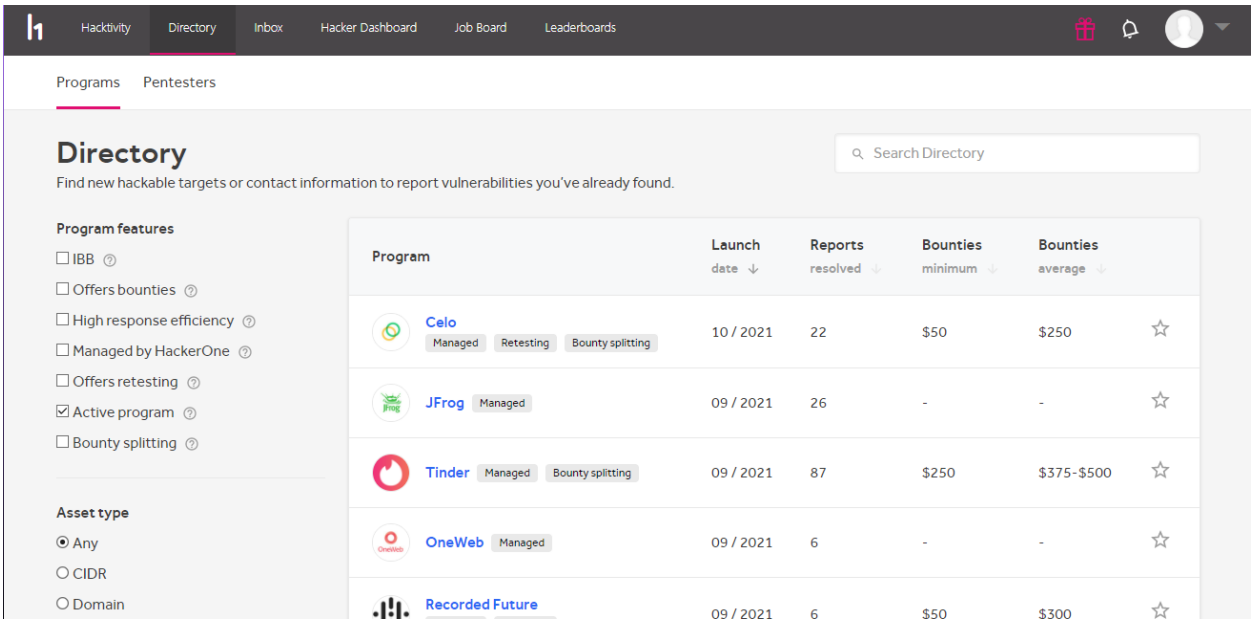
SELECTED PLATFORM – HACKERONE



HackerOne was founded by security experts and hackers who are passionate about making the internet a better place. In terms of hacker-powered security, our platform is the gold standard. We collaborate with the worldwide hacker community to identify our clients' most critical security problems before criminals can take advantage of them. HackerOne has offices in San Francisco, London, and the Netherlands. Benchmark, New Enterprise Associates, Dragoneer Investments, and EQT Ventures are among the companies that have invested.

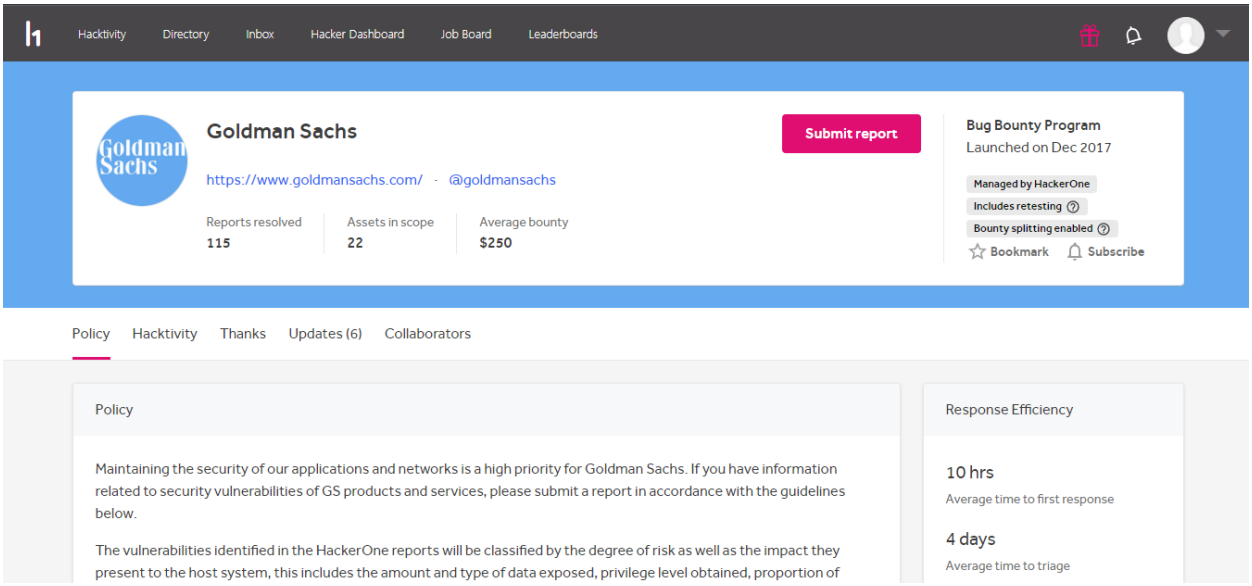
DOMAIN SELECTION

To begin, we must first establish a HackerOne account and log in. After logging in successfully, we are presented with a dashboard and a navigation bar; inside the navigation bar, there is a tab labeled "Directory," or we may reach it through this link. Programs may be found at https://hackerone.com/directory/programs. The number of listed domains for bug bounty scanning may be seen on the Directory page. We choose a domain from among those available. Below is a list of some of the domains that appear at the top of this page. After the specific involvement,



Always attempt to find a goal that covers all you're aiming to achieve. What technique will you use to track it down? By clicking on any of the listed programs and then scrolling down to the rules, as shown in the image below, you can find in-scope objects in the program rules. Because the scope item only has one domain, you only have to check for issues in one location. Because this program is now freely accessible, it will be utilized by a large number of other hunters, lowering your chances of success. Because there are so many people hunting on this program right now, we need a larger target. We need to come up with a bigger objective. Take a look at what's displayed in the diagram below.

SELECTED DOMAIN https://www.goldmansachs.com/



ABOUT GOLDMAN SACHS

The Goldman Sachs Group, Inc. is a leading global financial institution that provides a broad range of financial services to a large and diverse client base that includes corporations, financial institutions, governments, and individuals across investment banking, securities, investment management, and consumer banking.

The company, which was founded in 1869 and is headquartered in New York, has offices in all major financial cities around the globe.

POLICY ANALYZING

Maintaining the security of our applications and networks is a high priority for Goldman Sachs. If you have information related to security vulnerabilities of GS products and services, please submit a report in accordance with the guidelines below.

The vulnerabilities identified in the HackerOne reports will be classified by the degree of risk as well as the impact they present to the host system, this includes the amount and type of data exposed, privilege level obtained, proportion of systems or users affected.

Do not try to further pivot into the network by using a vulnerability. The rules around Remote Code Execution (RCE), SQL Injection (SQLi), vulnerabilities allowing you to access file/folder structure, defacement and file uploads are listed below.

Do not try to exploit service providers we use, prohibited actions include, but are not limited to bruteforcing login credentials of Domain Registrars, DNS Hosting Companies, Email Providers and/or others. The Firm does not authorize you to perform any actions to a non-GS owned property/system/service/data.

If you encounter Personally Identifiable Information (PII) contact us at bugbounty@gs.com immediately. Do not proceed with access and immediately purge any local information, if applicable.

Please limit any automated scanning to 60 requests per second. Aggressive testing that causes service degradation will be grounds for removal from the program.

SCOPE

Every bug bounty program has its own scope, and as a hunter, we must understand what is in-scope and what is out-of-scope. This section discusses how to report a problem and describes the program's disclosure policy, among other things. Because improper disclosure (for example, publicly disclosing a flaw without permission when authorization is required) may have unfavorable repercussions for both you and the client, it's essential that you understand the system's policy statement.

OUT-OF-SCOPE

When reporting vulnerabilities, please consider (1) attack scenario / exploitability, and (2) security impact of the bug. The following issues are considered out of scope:

- For the time being we are making all vulnerabilities in Flash files out of scope
- Reports from automated tools or scans
- Reports affecting outdated browsers
- Denial of Service Attacks
- Issues without clearly identified security impact (such as clickjacking on a static website) or speculative theoretical exploitability - for example using UXSS to steal the auth cookies, identifying Apache Tomcat 8.0.43 but not being able to perform any attack.
- Missing security best practices and controls (rate-limiting/throttling, lack of CSRF protection, lack of security headers, missing flags on cookies, descriptive errors, server/technology disclosure - without clear and working exploit)
- Lack of crossdomain.xml, p3p.xml, robots.txt or any other policy files and/or wildcard presence/misconfigurations in these.
- Use of a known-vulnerable libraries or frameworks - for example an outdated JQuery or AngularJS (without clear and working exploit)
- Self-exploitation (cookie reuse, self cookie-bomb, self denial-of-service etc.)
- Self Cross-site Scripting vulnerabilities without evidence on how the vulnerability can be used to attack another user
- Lack of HTTPS
- Reports about insecure SSL / TLS configuration
- Password complexity requirements, account/email enumeration, or any report that discusses how you can learn whether a given username or email address has a GS-related account
- Presence/Lack of autocomplete attribute on web forms/password managers.
- Server Banner Disclosure/Technology used Disclosure
- Full Path Disclosure
- IP Address Disclosure
- CSRF on logout or insignificant functionalities
- Publicly accessible login panels
- Clickjacking

- CSS Injection attacks. (Unless it gives you ability to read anti-CSRF tokens or other sensitive information)
- Tabnabbing
- Host Header Injection (Unless it gives you access to interim proxies)
- Cache Poisoning
- Reflective File Download
- Cross-Origin Resource Sharing (CORS) Access-Control-Allow-Origin: * or accepting of custom Origin header that do not specifically show a valid attack scenario
- PRSSI - Path-relative stylesheet import vulnerabilities (without a impactful exploitation scenario - for example stealing CSRF-tokens)
- OPTIONS/TRACE/DELETE/PUT/WEBDAV or any other HTTP Methods accepted by the server which do not specifically show a valid attack scenario
- Cookie scoped to parent domain or anything related to the path missconfiguration and improperly scoped
- Private IP/Hostname disclosures or real IP disclosures for services using CDN
- Open ports which do not lead directly to a vulnerability
- Our policies on presence/absence of SPF / DKIM / DMARC records
- Lack of DNS CAA and DNS-related configurations
- Weak Certificate Hash Algorithm
- Social engineering of GS employees or contractors
- Any physical/wireless attempt against GS property or data centers
- Do not try sending your commando-trained pigeons equipped with knowledge of RFC-2549 to sniff the traffic from our access points.

OUT-OF-SCOPE DOMAINS

Any SaaS or other service provider is not explicitly called out. If you think it's something owned by Goldman Sachs, you can send it along - we'll decide if it's out-of-scope.

IN SCOPE

- **goldmansachs.com**
- **gs.com**
  goldman.com
- **marcus.com**
- **honestdollar.com**
- **marcus.co.uk**
- **research.gs.com**
- **gsam.com**
- **gsselect.com**
- **mosaic.qa.gs.com**
- **mosaic.gs.com**
- **developer.gs.com**

INFORMATION GATHERING

Information collection is the process of obtaining different kinds of data about the target victim or system. Hackers may collect information using a variety of tools, techniques, and websites, including Whois and nslookup, among others.

Types of Information Gathering

There are two kinds of data collection.

1. Active Information Gathering

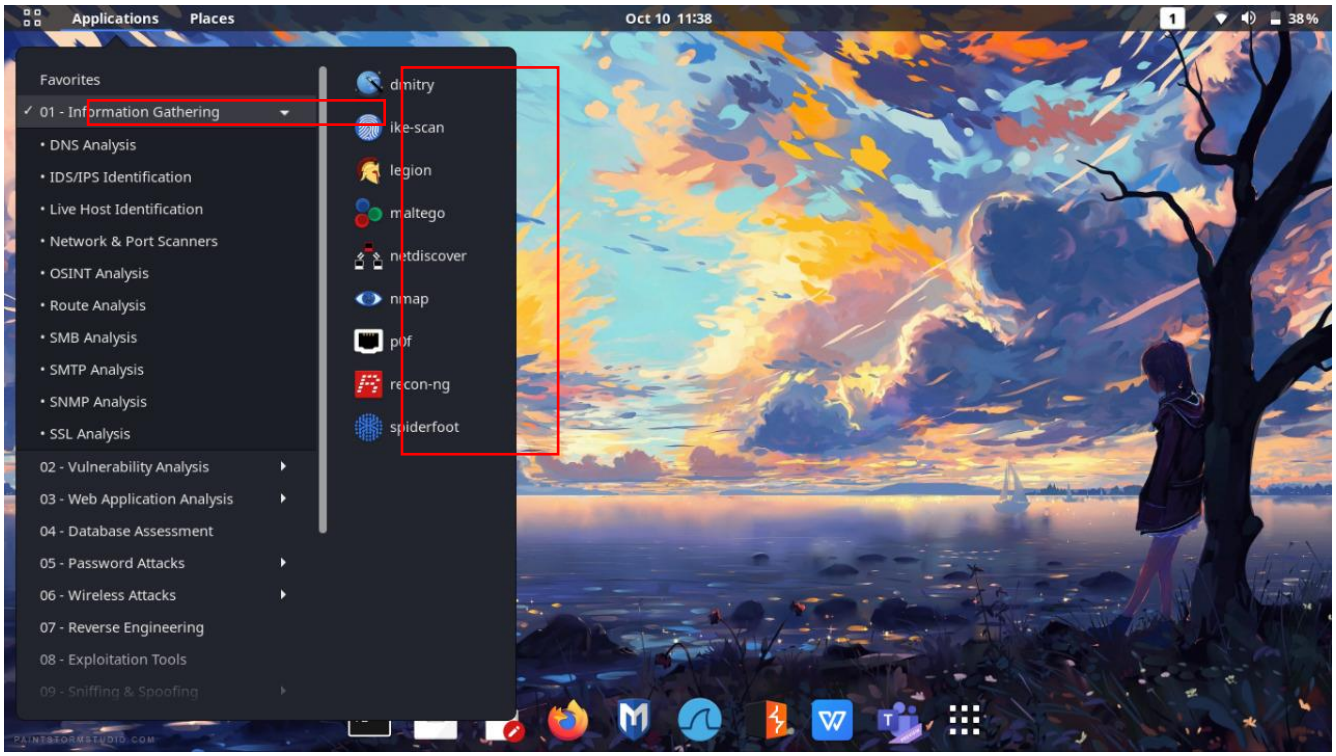
By actively interacting with these targets, we may learn more about them, which is known as passive information collection. In contrast to passive data collection, doing so without authorization may be a criminal offense in certain countries. DNS Enumeration, Port Scanning, and OS Fingerprinting are all possibilities. Active information gathering, like passive information gathering, seeks to obtain as much information as feasible.

2. Passive Information Gathering

We gather passive information on our goals using publicly available information (resources). The who-is information and search engine results may be useful. The goal must be met in order to get as much information about the topic as feasible.

INFORMATION GATHERING TOOLS

There are Number of tools to information gathering tools in Kali Linux.



WHOIS COMMAND

WHOIS is a standard query and response protocol developed on top of TCP for delivering information services to Internet users. The information provided by this service includes Name Servers, IP Address Blocks, and a wide range of additional information services. WHOIS is a client for connecting to a WHOIS server (or database server) on Linux through the well-known port 43, which stores and clearly communicates database information for humans.

Results

goldmansachs.com

```
┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ whois goldmansachs.com
   Domain Name: GOLDMANSACHS.COM
   Registry Domain ID: 1041012_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://cscdbs.com
   Updated Date: 2021-07-20T05:12:50Z
   Creation Date: 1995-07-25T04:00:00Z
   Registry Expiry Date: 2022-07-24T04:00:00Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   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.GOLDMANSACHS.BIZ
   Name Server: NS1.GOLDMANSACHS.INFO
   Name Server: NS1.GS.COM
   Name Server: NS1.GS360.NET
   Name Server: NS2.GS.COM
   Name Server: NS3.GS.COM
   Name Server: NS4.GS.COM
   Name Server: NS5.GS.COM
   Name Server: NS6.GS.COM
   Name Server: NS7.GS.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-10-16T07:00:45Z <<<

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
```

gs.com

```
┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ whois gs.com
   Domain Name: GS.COM
   Registry Domain ID: 1048026_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.corporatedomains.com
   Registrar URL: http://cscdbs.com
   Updated Date: 2021-10-13T13:59:51Z
   Creation Date: 1991-04-05T05:00:00Z
   Registry Expiry Date: 2022-04-06T04:00:00Z
   Registrar: CSC Corporate Domains, Inc.
   Registrar IANA ID: 299
   Registrar Abuse Contact Email: domainabuse@cscglobal.com
   Registrar Abuse Contact Phone: 8887802723
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   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.GOLDMANSACHS.BIZ
   Name Server: NS1.GOLDMANSACHS.INFO
   Name Server: NS1.GS.COM
   Name Server: NS1.GS360.NET
   Name Server: NS2.GS.COM
   Name Server: NS3.GS.COM
   Name Server: NS4.GS.COM
   Name Server: NS5.GS.COM
   Name Server: NS6.GS.COM
   Name Server: NS7.GS.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2021-10-16T07:00:45Z <<<

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
```

DMITRY TOOL

To gather information about Deepmagic, you may use DMitry (Deepmagic Information Gathering Tool), a UNIX/(GNU)Linux Command Line Application written in C. There are no limits to what DMitry may learn about a host. Several built-in features may help you find potential subdomains, emails, uptime statistics, tcp port scans, and even whois lookups.

Results

goldmansachs.com

```
┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ dmitry goldmansachs.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:204.74.99.100
HostName:goldmansachs.com

Gathered Inet-whois information for 204.74.99.100
---------------------------------


inetnum:        204.62.219.0 - 204.75.228.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
```

gs.com

```
┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ dmitry gs.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:204.74.99.100
HostName:gs.com

Gathered Inet-whois information for 204.74.99.100
---------------------------------


inetnum:        204.62.219.0 - 204.75.228.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        ------------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
remarks:
```

goldman.com

```
┌──(pasindu㉿kali)-[~/…/Year_2/Web security/TOOLS/Sublist3r]
└─$ dmitry goldman.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:204.74.99.100
HostName:goldman.com

Gathered Inet-whois information for 204.74.99.100
---------------------------------


inetnum:        204.62.219.0 - 204.75.228.255
netname:        NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:          IPv4 address block not managed by the RIPE NCC
remarks:        -----------------------------------------------------
remarks:
remarks:        For registration information,
remarks:        you can consult the following sources:
remarks:
remarks:        IANA
remarks:        http://www.iana.org/assignments/ipv4-address-space
remarks:        http://www.iana.org/assignments/iana-ipv4-special-registry
remarks:        http://www.iana.org/assignments/ipv4-recovered-address-space
remarks:
remarks:        AFRINIC (Africa)
remarks:        http://www.afrinic.net/ whois.afrinic.net
remarks:
remarks:        APNIC (Asia Pacific)
remarks:        http://www.apnic.net/ whois.apnic.net
remarks:
remarks:        ARIN (Northern America)
remarks:        http://www.arin.net/ whois.arin.net
remarks:
remarks:        LACNIC (Latin America and the Carribean)
remarks:        http://www.lacnic.net/ whois.lacnic.net
```

SUBLISTER TOOL

Sublist3r is a search and listing tool for subdomains that makes it simple to use. Virustotal and Netcraft are just a few of the search engines and databases that Sublist3r makes use of. DNSdumpster, ThreatCrowd, and ReverseDNS are some of the most well-known sources. Due to the integration of Sublist3r and subbrute, the option to use brute force has been introduced to Sublist3.

Sublisert Install & run

1. ***git clone https://github.com/aboul3la/Sublist3r.git***
2. ***cd Sublist3r/***
3. ***sudo pip install -r requirements.txt***
4. ***sudo apt-get install python-requests***
5. ***sudo apt-get install python-dnspython***
6. ***sudo apt-get install python-argparse***
7. ***python3 sublist3r.py -d reddit.com***

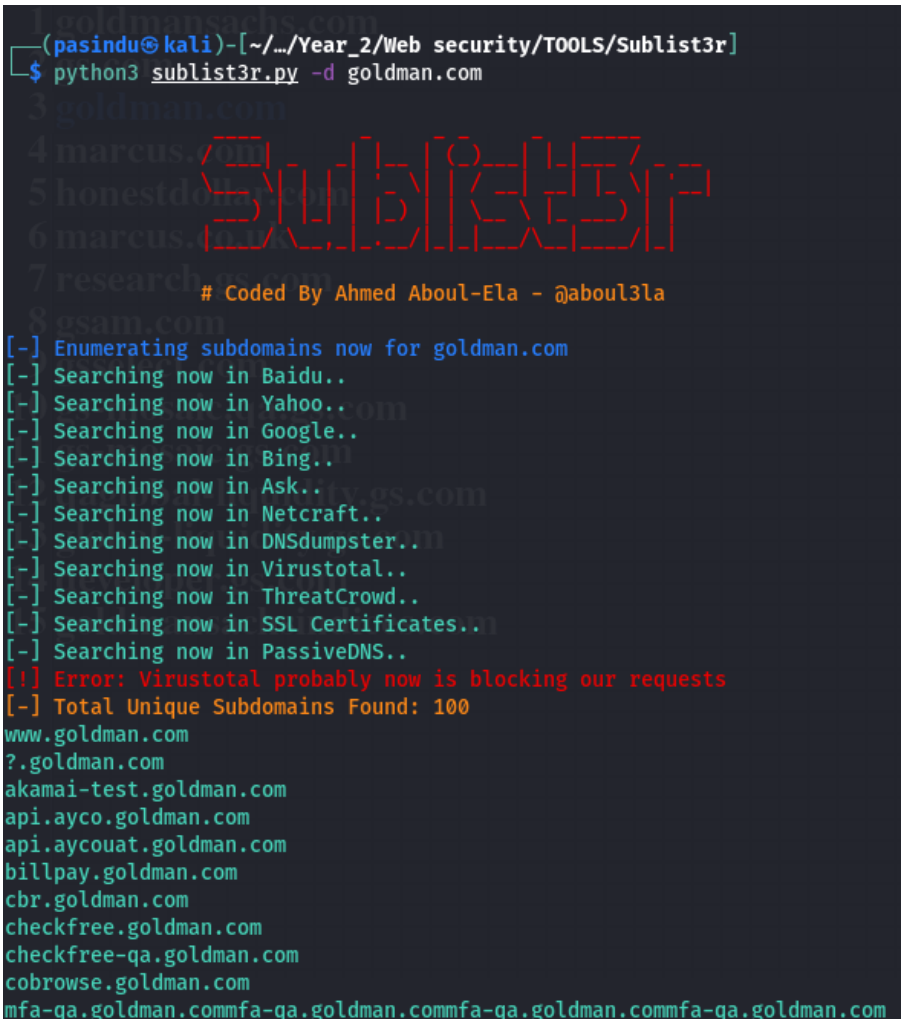
Results

goldmansachs.com

gs.com


(pasindu㉿kali)-[~/…/Year_2/Web security/TOOLS/Sublist3r]
$ python3 sublist3r.py -d gs.com
# Coded By Ahmed Aboul-Ela - @aboul3la
[-] Enumerating subdomains now for gs.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
[-] Total Unique Subdomains Found: 1033
www.gs.com
10000smallbusinessesme.gs.com
10000smallbusinessesmeqa.gs.com
10000womenme.gs.com
10000womenmeqa.gs.com
360.gs.com
www.360.gs.com
pre-prod.360.gs.com
360-b-qa.gs.com
360-qa.gs.com
origin.360-qa.gs.com

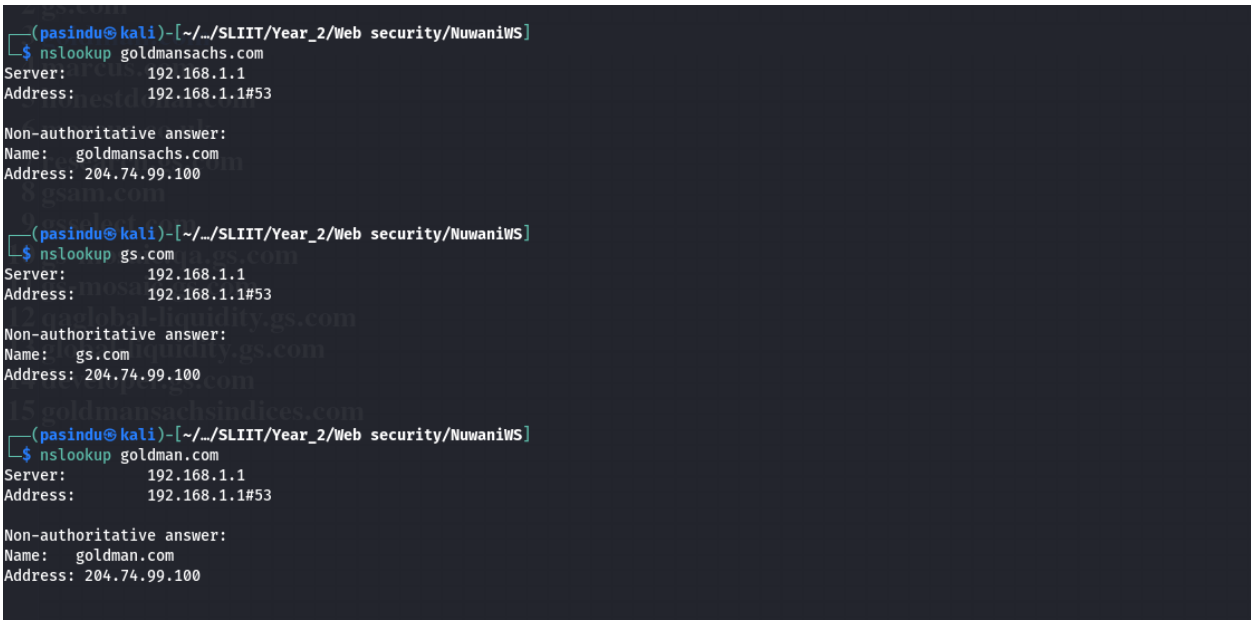
goldman.com



NSLOOKUP

Nslookup is a command-line tool for network management that is tiny in size but packs a big punch. This app has a basic user interface, but it is very helpful, nevertheless. There are several common computer operating systems that include the Nslookup command, including as Windows, Mac OS X, and many Linux distributions. Domain names and IP addresses, as well as any other DNS Records, may be obtained by running queries against the DNS server.

Results



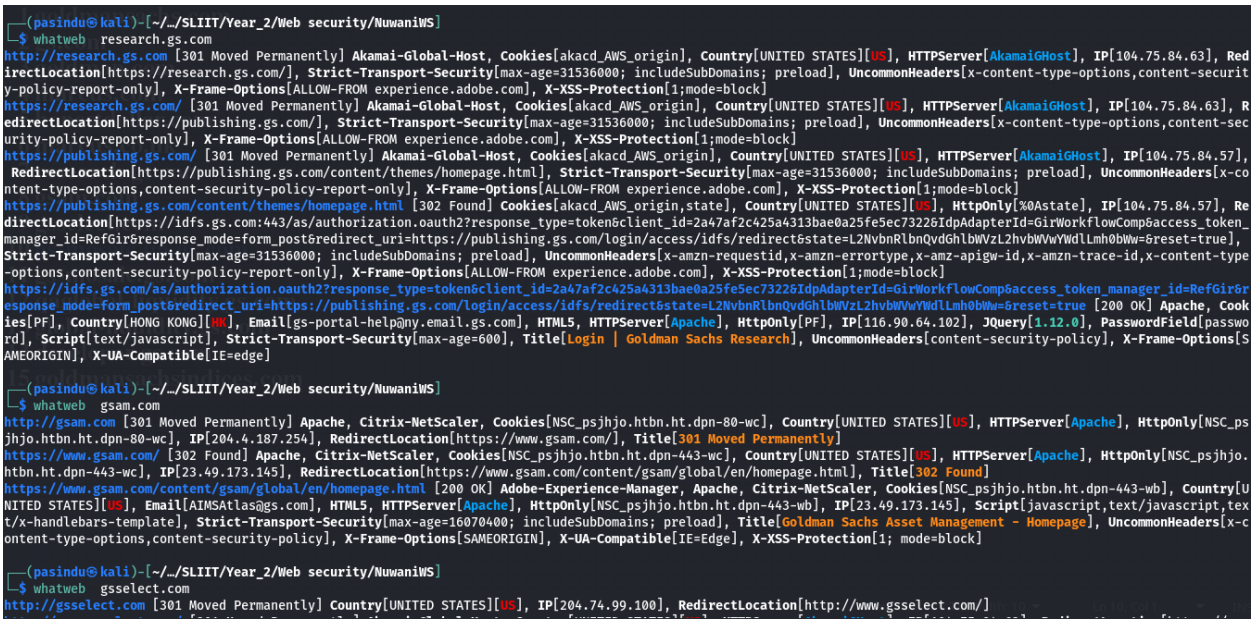
WHATWEB TOOL

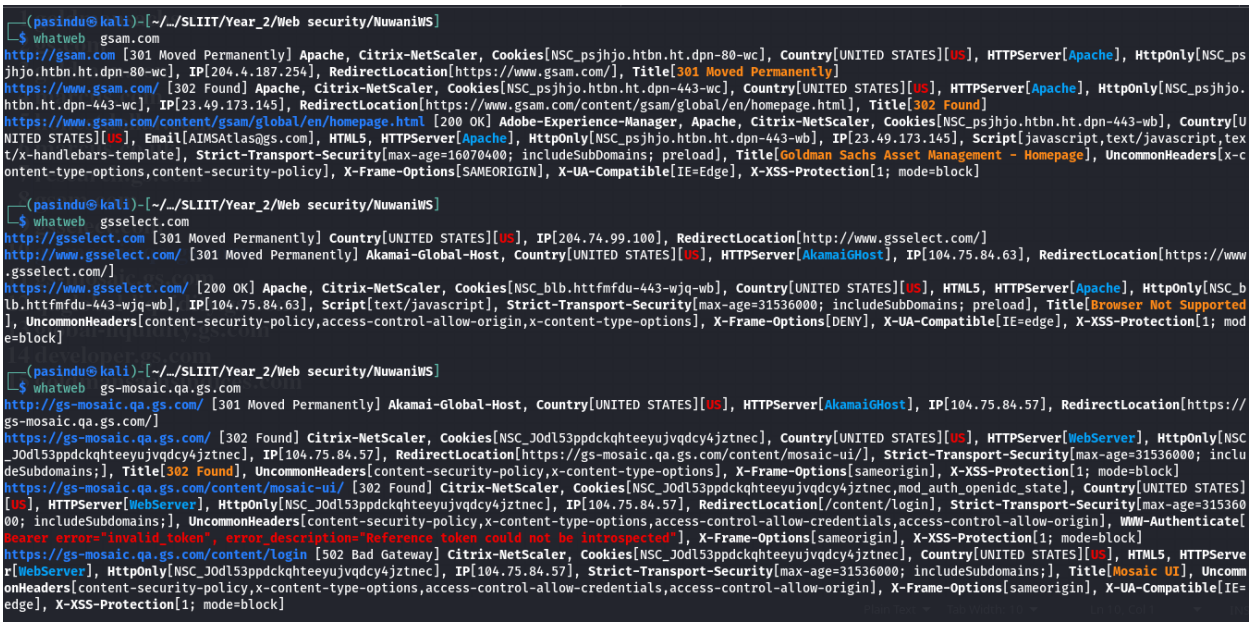
WhatWeb is a website that recognizes webpages. In addition to content management systems (CMS), blogging platforms, statistical and analytic packages, JavaScript libraries, web servers, and embedded devices are all recognized by the standards body. WhatWeb offers approximately 900 plugins, each of which is designed to recognize something specific. Other information that is identified includes version numbers, email addresses, account IDs, web framework modules, SQL problems, and other information about the application.

Results

```
┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ whatweb  goldmansachs.com
http://goldmansachs.com [301 Moved Permanently] Country[UNITED STATES][US], IP[204.74.99.100], RedirectLocation[http://www.goldmansachs.com/]
http://www.goldmansachs.com/ [301 Moved Permanently] Akamai-Global-Host, Country[SINGAPORE][SG], HTTPServer[AkamaiGHost], IP[118.214.57.112], RedirectLocation[https://w
ww.goldmansachs.com/], UncommonHeaders[viewport_width,viewport_initial_scale,resolution_width,resolution_height,physical_screen_width,physical_screen_height,mobile_brow
ser_version,mobile_browser,is_wireless_device,is_tablet,device_os_version,device_os,is_mobile,ajax_preferred_geoloc_api,x-akamai-device-characteristics,server-timing],
X-XSS-Protection[1; mode=block]
https://www.goldmansachs.com/ [200 OK] Country[SINGAPORE][SG], HTML5, HTTPServer[Webserver], IP[118.214.57.112], Open-Graph-Protocol, PoweredBy[partnership,], Script[ap
plication/ld+json,text/javascript], Title[Goldman Sachs], UncommonHeaders[server-timing,x-akamai-device-characteristics,ajax_preferred_geoloc_api,is_mobile,device_os,de
vice_os_version,is_tablet,is_wireless_device,mobile_browser,mobile_browser_version,physical_screen_height,physical_screen_width,resolution_height,resolution_width,viewp
ort_initial_scale,viewport_width,x-akamai-transformed], X-UA-Compatible[IE=Edge], X-XSS-Protection[1; mode=block]

┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ whatweb  gs.com
http://gs.com [301 Moved Permanently] Country[UNITED STATES][US], IP[204.74.99.100], RedirectLocation[http://www.goldmansachs.com/]
http://www.goldmansachs.com/ [301 Moved Permanently] Akamai-Global-Host, Country[SINGAPORE][SG], HTTPServer[AkamaiGHost], IP[118.214.57.112], RedirectLocation[https://w
ww.goldmansachs.com/], UncommonHeaders[viewport_width,viewport_initial_scale,resolution_width,resolution_height,physical_screen_width,physical_screen_height,mobile_brow
ser_version,mobile_browser,is_wireless_device,is_tablet,device_os_version,device_os,is_mobile,ajax_preferred_geoloc_api,x-akamai-device-characteristics,server-timing],
X-XSS-Protection[1; mode=block]
https://www.goldmansachs.com/ [200 OK] Country[SINGAPORE][SG], HTML5, HTTPServer[Webserver], IP[118.214.57.112], Open-Graph-Protocol, PoweredBy[partnership,], Script[ap
plication/ld+json,text/javascript], Title[Goldman Sachs], UncommonHeaders[server-timing,x-akamai-device-characteristics,ajax_preferred_geoloc_api,is_mobile,device_os,de
vice_os_version,is_tablet,is_wireless_device,mobile_browser,mobile_browser_version,physical_screen_height,physical_screen_width,resolution_height,resolution_width,viewp
ort_initial_scale,viewport_width,x-akamai-transformed], X-UA-Compatible[IE=Edge], X-XSS-Protection[1; mode=block]

┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ whatweb  goldman.com
http://goldman.com [301 Moved Permanently] Country[UNITED STATES][US], IP[204.74.99.100], RedirectLocation[http://www.goldman.com/]
http://www.goldman.com/ [301 Moved Permanently] Akamai-Global-Host, Cookies[_abck,bm_sz], Country[SINGAPORE][SG], HTTPServer[AkamaiGHost], HttpOnly[bm_sz], IP[118.214.5
3.33], RedirectLocation[https://www.goldman.com/]
https://www.goldman.com/ [302 Found] Cookies[_abck,bm_sz,dc], Country[SINGAPORE][SG], HTTPServer[webserver], HttpOnly[bm_sz], IP[118.214.53.33], RedirectLocation[https:
//www.goldman.com/service-redirector/v1/services/next], Strict-Transport-Security[max-age=31536000; includeSubDomains], Title[302 Found], UncommonHeaders[x-content-type
-options,content-security-policy], X-Frame-Options[SAMEORIGIN], X-XSS-Protection[1; mode=block]
https://www.goldman.com/service-redirector/v1/services/next [200 OK] Cookies[_abck,bm_sz,dc,mod_auth_openidc_state_eOkN6K77c5urujz1D8jCIW2Hjg0], Country[SINGAPORE][SG],
 HTTPServer[webserver], HttpOnly[bm_sz,mod_auth_openidc_state_eOkN6K77c5urujz1D8jCIW2Hjg0], IP[118.214.53.33], Script[text/javascript], Title[Submitting...], UncommonHe
aders[x-akamai-transformed]
```

```
┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ whatweb  marcus.com
http://marcus.com [301 Moved Permanently] Country[UNITED STATES][US], IP[204.74.99.100], RedirectLocation[https://www.marcus.com/]
https://www.marcus.com/ [403 Forbidden] CloudFlare, Cookies[__cf_bm], Country[UNITED STATES][US], HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[104.19.155.86], S
cript[text/javascript], Title[Marcus], UncommonHeaders[referrer-policy,expect-ct,cf-ray], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge]

┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ whatweb  honestdollar.com
http://honestdollar.com [302 Found] Country[UNITED STATES][US], IP[138.8.25.58], RedirectLocation[https://origin.honestdollar.com/]
https://origin.honestdollar.com/ [302 Found] Apache, Citrix-NetScaler, Cookies[NSC_psjhjo.ipoftuepmmbs.dpn-443-wb], Country[UNITED STATES][US], HTTPServer[Apache], Http
Only[NSC_psjhjo.ipoftuepmmbs.dpn-443-wb], IP[148.86.15.58], RedirectLocation[https://www.honestdollar.com/], Title[302 Found]
https://www.honestdollar.com/ [200 OK] Apache, Citrix-NetScaler, Cookies[NSC_psjhjo.ipoftuepmmbs.dpn-443-wb], Country[UNITED STATES][US], HTTPServer[Apache], HttpOnly[N
SC_psjhjo.ipoftuepmmbs.dpn-443-wb], IP[104.75.84.63], Strict-Transport-Security[max-age=31536000; includeSubdomains;], Title[Honest Dollar], UncommonHeaders[x-content-t
ype-options,content-security-policy,access-control-allow-credentials], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=Edge], X-XSS-Protection[1; mode=block]

┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ whatweb  honestdollar.com
http://honestdollar.com [302 Found] Country[UNITED STATES][US], IP[138.8.25.58], RedirectLocation[https://origin.honestdollar.com/]
https://origin.honestdollar.com/ [302 Found] Apache, Citrix-NetScaler, Cookies[NSC_psjhjo.ipoftuepmmbs.dpn-443-wb], Country[UNITED STATES][US], HTTPServer[Apache], Http
Only[NSC_psjhjo.ipoftuepmmbs.dpn-443-wb], IP[148.86.15.58], RedirectLocation[https://www.honestdollar.com/], Title[302 Found]
https://www.honestdollar.com/ [200 OK] Apache, Citrix-NetScaler, Cookies[NSC_psjhjo.ipoftuepmmbs.dpn-443-wb], Country[UNITED STATES][US], HTTPServer[Apache], HttpOnly[N
SC_psjhjo.ipoftuepmmbs.dpn-443-wb], IP[104.75.84.47], Strict-Transport-Security[max-age=31536000; includeSubdomains;], Title[Honest Dollar], UncommonHeaders[x-content-t
ype-options,content-security-policy,access-control-allow-credentials], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=Edge], X-XSS-Protection[1; mode=block]

┌──(pasindu㉿kali)-[~/…/SLIIT/Year_2/Web security/NuwaniWS]
└─$ whatweb  marcus.co.uk
http://marcus.co.uk [301 Moved Permanently] Country[UNITED STATES][US], IP[204.74.99.100], RedirectLocation[https://www.marcus.co.uk/]
https://www.marcus.co.uk/ [301 Moved Permanently] Cookies[__cf_bm], Country[UNITED STATES][US], HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[104.17.56.15], RedirectLoc
ation[https://www.marcus.co.uk/uk/en], Strict-Transport-Security[max-age=63072000; includeSubdomains], Title[301 Moved Permanently], UncommonHeaders[cf-ray,cf-cache-sta
tus,expect-ct]
https://www.marcus.co.uk/uk/en [200 OK] Adobe-Experience-Manager, Cookies[__cf_bm], Country[UNITED STATES][US], HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[104
.17.56.15], Open-Graph-Protocol[website], Script[text/javascript], Strict-Transport-Security[max-age=63072000; includeSubdomains, max-age=63072000; includeSubdomains;],
 Title[Marcus UK | Marcus by Goldman Sachs&reg;], UncommonHeaders[cf-ray,cf-cache-status,content-security-policy,expect-ct,x-content-type-options,x-dispatcher,x-request
-id,x-vhost], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[IE=edge], X-XSS-Protection[1; mode=block]
```





ANALYZE INFORMATION

According to the information, I gathered, hear I mention some important things that can be useful.

sublister

Total Unique Subdomains Found

- goldmansachs.com : 23
- gs.com : 1033
- goldman.com : 100

nslookup

Server: 192.168.1.1

Address: 192.168.1.1#53

Deepmagic Information Gathering Tool

HostIP:118.214.57.112
Hostname: www.goldmasachs.com
Gathered TCP Port information for 118.214.57.112

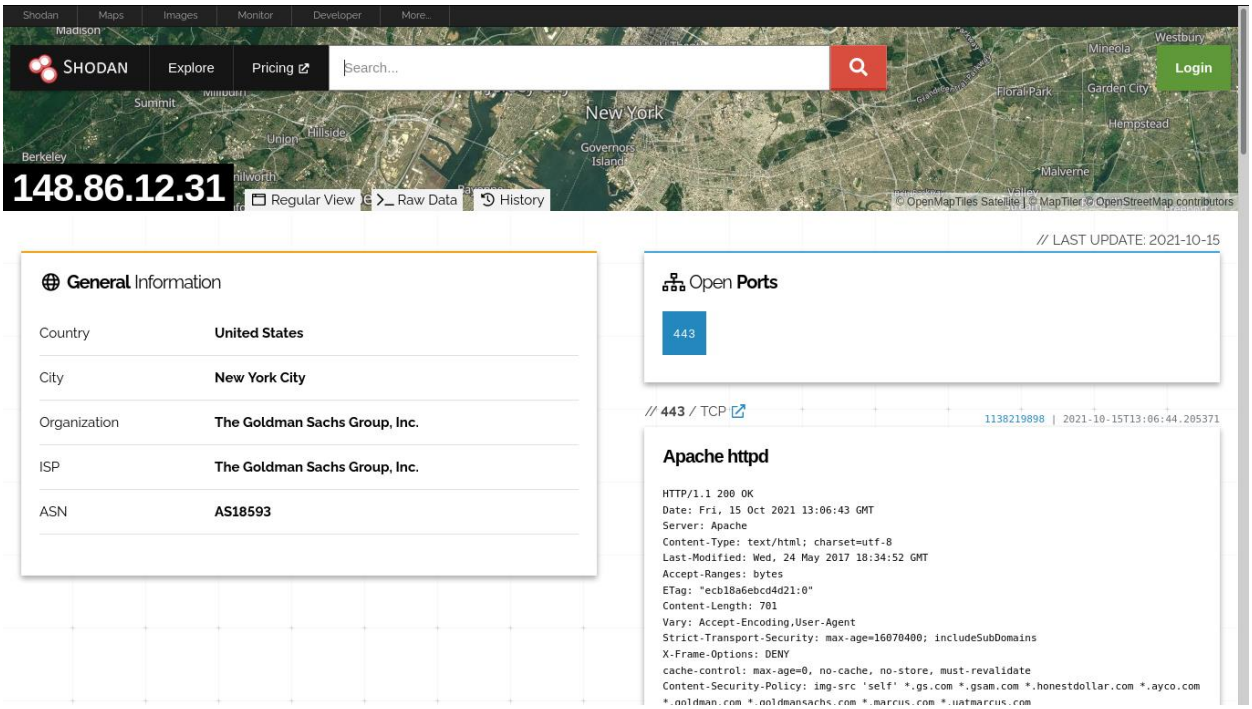
Port	State
25/tcp	open
80/tcp	open

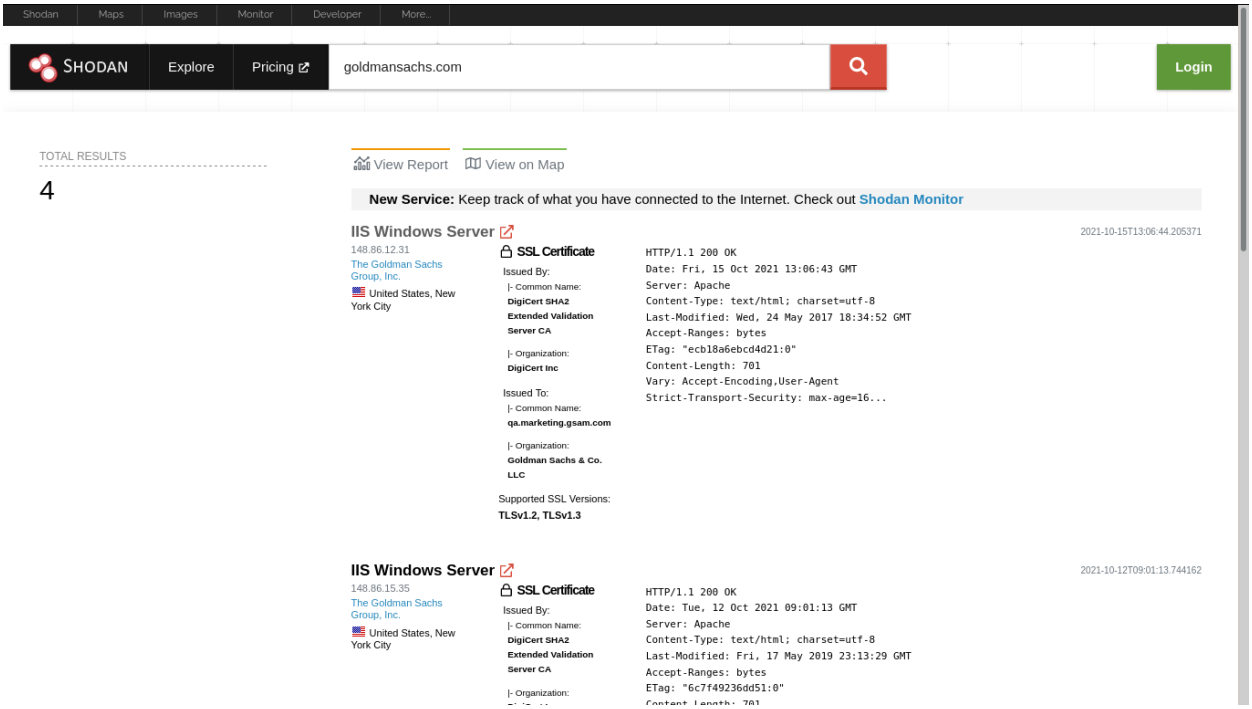
Port scan Finished: Scanned 150 ports, 0 ports were in state closed

SHODAN REPORT

The Internet is made up of many different components, including websites. Power plants, cell phones, refrigerators, and Minecraft servers may all be found with Shodan. Exposure to the Network should be monitored. Always be aware of which gadgets are connected to the Internet and which are not. Shodan helps you remain safe by giving you a complete picture of all exposed services.

Shodan is an online platform that allows users to utilize a number of criteria to find different kinds of internet-connected servers (such as cameras, routers, and servers). Information that the server provides back to the client has also been characterized as a search engine for service banners. A welcome message, server software information, or any other information that the client may discover before communicating with the server might be included in this section.


Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Pricing
Search...
Login
148.86.12.31
Regular View
Raw Data
History
© OpenMapTiles Satellite | © MapTiler © OpenStreetMap contributors
// LAST UPDATE: 2021-10-15
General Information
Country United States
City New York City
Organization The Goldman Sachs Group, Inc.
ISP The Goldman Sachs Group, Inc.
ASN AS18593
Open Ports
443
// 443 / TCP
1138219898 | 2021-10-15T13:06:44.205371
Apache httpd
HTTP/1.1 200 OK
Date: Fri, 15 Oct 2021 13:06:43 GMT
Server: Apache
Content-Type: text/html; charset=utf-8
Last-Modified: Wed, 24 May 2017 18:34:52 GMT
Accept-Ranges: bytes
ETag: "ecb18a6ebcd4d21:0"
Content-Length: 701
Vary: Accept-Encoding,User-Agent
Strict-Transport-Security: max-age=16070400; includeSubDomains
X-Frame-Options: DENY
cache-control: max-age=0, no-cache, no-store, must-revalidate
Content-Security-Policy: img-src 'self' *.gs.com *.gsam.com *.honestdollar.com *.ayco.com


Shodan
Maps
Images
Monitor
Developer
More...
SHODAN
Explore
Pricing
goldmansachs.com
Login
TOTAL RESULTS
4
View Report
View on Map
New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor
IIS Windows Server
148.86.12.31
The Goldman Sachs Group, Inc.
United States, New York City
SSL Certificate
Issued By:
|- Common Name:
DigiCert SHA2 Extended Validation Server CA
|- Organization:
DigiCert Inc
Issued To:
|- Common Name:
qa.marketing.gsam.com
|- Organization:
Goldman Sachs & Co. LLC
Supported SSL Versions:
TLSv1.2, TLSv1.3
2021-10-15T13:06:44.205371
HTTP/1.1 200 OK
Date: Fri, 15 Oct 2021 13:06:43 GMT
Server: Apache
Content-Type: text/html; charset=utf-8
Last-Modified: Wed, 24 May 2017 18:34:52 GMT
Accept-Ranges: bytes
ETag: "ecb18a6ebcd4d21:0"
Content-Length: 701
Vary: Accept-Encoding,User-Agent
Strict-Transport-Security: max-age=16...
IIS Windows Server
148.86.15.35
The Goldman Sachs Group, Inc.
United States, New York City
SSL Certificate
Issued By:
|- Common Name:
DigiCert SHA2 Extended Validation Server CA
|- Organization:
2021-10-12T09:01:13.744162
HTTP/1.1 200 OK
Date: Tue, 12 Oct 2021 09:01:13 GMT
Server: Apache
Content-Type: text/html; charset=utf-8
Last-Modified: Fri, 17 May 2019 23:13:29 GMT
Accept-Ranges: bytes
ETag: "6c7f49236dd51:0"

Organization	**The Goldman Sachs Group, Inc.**
ISP	**The Goldman Sachs Group, Inc.**
ASN	**AS18593**

Apache httpd

```
HTTP/1.1 200 OK
Date: Fri, 15 Oct 2021 13:06:43 GMT
Server: Apache
Content-Type: text/html; charset=utf-8
Last-Modified: Wed, 24 May 2017 18:34:52 GMT
Accept-Ranges: bytes
ETag: "ecb18a6ebcd4d21:0"
Content-Length: 701
Vary: Accept-Encoding,User-Agent
Strict-Transport-Security: max-age=16070400; includeSubDomains
X-Frame-Options: DENY
cache-control: max-age=0, no-cache, no-store, must-revalidate
Content-Security-Policy: img-src 'self' *.gs.com *.gsam.com *.honestdollar.com *.ayco.com
*.goldman.com *.goldmansachs.com *.marcus.com *.uatmarcus.com
Set-Cookie: NSC_rb.nbslfujoh.htbn.dpn-443-wc=14b5a3d9ac24df8fb7111b672b646ff4fc8e41f1a89c
e2e1953d4711790869edd5fd7a11;expires=Fri, 15-Oct-2021 13:08:43 GMT;path=/;secure;httponly
```

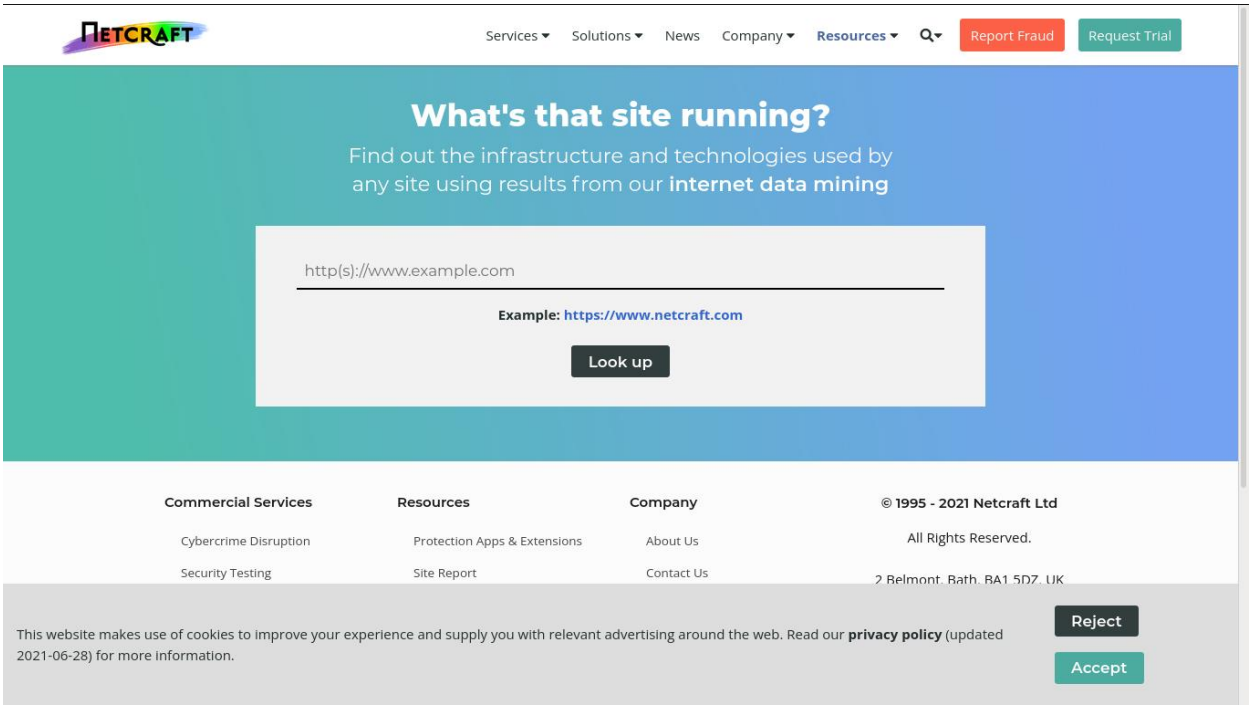
SSL Certificate

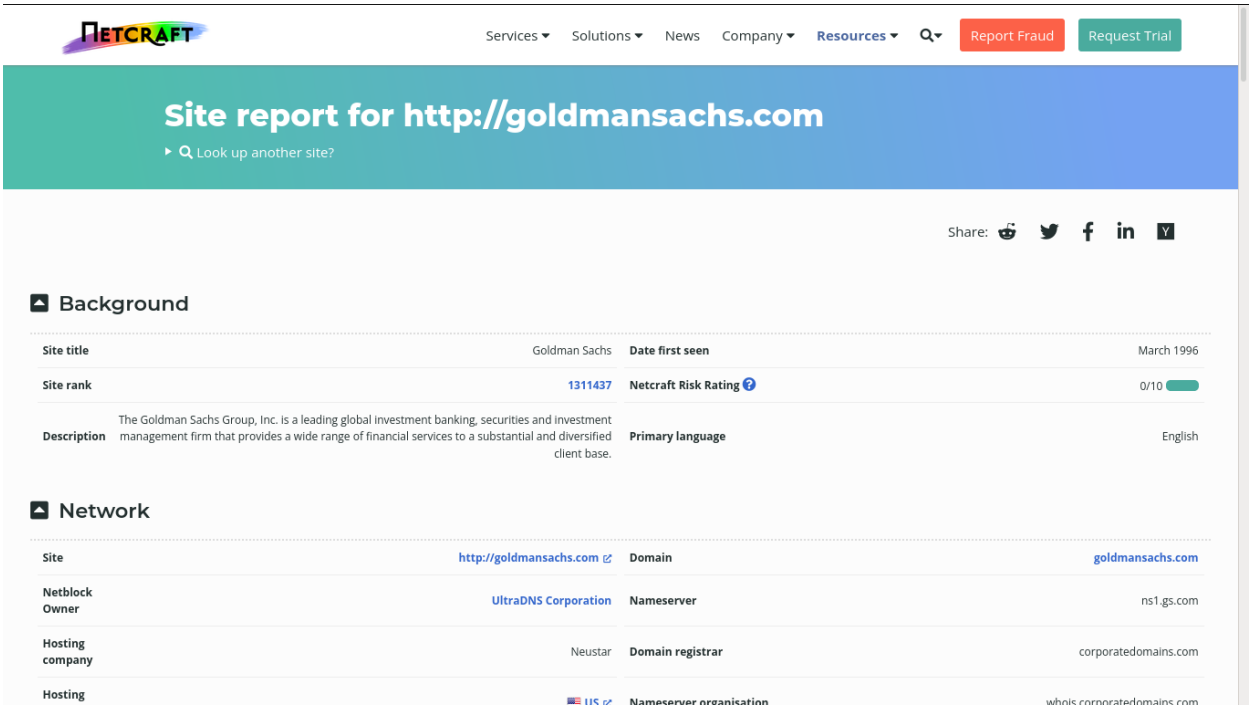
```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            07:5f:61:c2:ce:bc:8a:53:b8:5f:9b:d2:08:46:8b:7d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Vali
dation Server CA
        Validity
            Not Before: Jul  6 00:00:00 2021 GMT
            Not After : Jul 11 23:59:59 2022 GMT
        Subject: businessCategory=Private Organization/jurisdictionC=US/jurisdictionST=Ne
w York/serialNumber=1560743, C=US, ST=New York, L=New York, O=Goldman Sachs & Co. LLC, CN
=qa.marketing.gsam.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c9:e2:1b:86:15:29:83:9f:4c:55:10:34:bd:5f:
                    51:b6:3a:61:4d:a2:5d:e9:e2:be:82:a6:b6:bd:04:
                    da:93:80:44:37:14:10:08:72:b3:d6:86:5c:ca:8d:
```

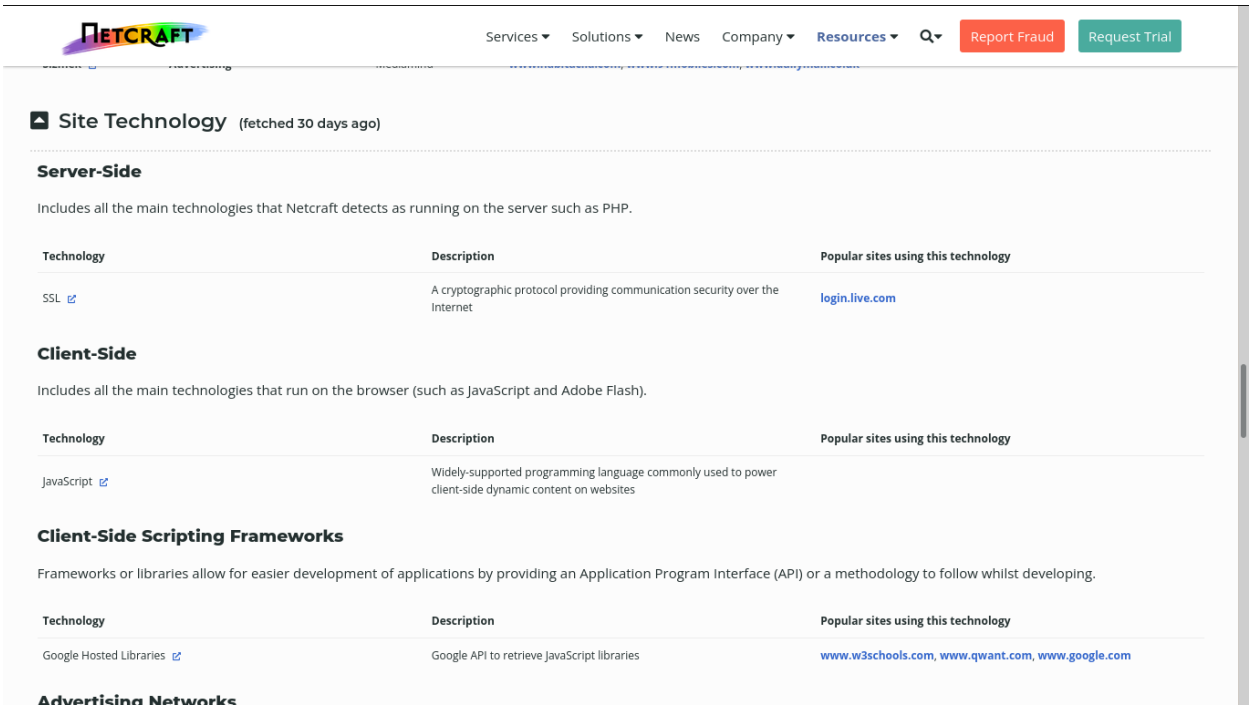

SSL Certificate

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            07:5f:61:c2:ce:bc:8a:53:b8:5f:9b:d2:08:46:8b:7d
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, O=DigiCert Inc, OU=www.digicert.com, CN=DigiCert SHA2 Extended Vali
dation Server CA
        Validity
            Not Before: Jul  6 00:00:00 2021 GMT
            Not After : Jul 11 23:59:59 2022 GMT
        Subject: businessCategory=Private Organization/jurisdictionC=US/jurisdictionST=Ne
w York/serialNumber=1560743, C=US, ST=New York, L=New York, O=Goldman Sachs & Co. LLC, CN
=qa.marketing.gsam.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:c9:e2:1b:86:15:29:83:9f:4c:55:10:34:bd:5f:
                    51:b6:3a:61:4d:a2:5d:e9:e2:be:82:a6:b6:bd:04:
                    da:93:80:44:37:14:10:08:72:b3:d6:86:5c:ca:8d:
                    fa:fd:01:64:9e:cd:b9:23:d4:ce:d0:1c:0b:32:9e:
                    17:f3:32:9d:dd:d7:67:c1:8e:1a:f0:e9:7c:f5:87:
                    ca:53:de:07:a2:9e:63:fe:a3:23:60:35:3a:40:72:
                    b6:74:31:f6:8b:0e:01:1e:e3:dd:24:f9:24:a7:6f:
                    0d:b1:ce:8e:ee:6c:80:8a:7d:c4:78:9e:3b:c3:05:
                    ae:f5:f0:0b:b6:4e:7d:1a:28:a9:d0:95:c2:3d:8f:
                    3a:9d:63:bb:b7:a5:e5:10:ea:d7:c8:f9:b1:c9:66:
                    d8:b0:59:03:71:be:5a:0d:7d:13:9b:0b:7f:aa:16:
                    9c:5e:8d:66:2e:b4:db:94:10:cd:4c:bb:0b:81:6d:
                    59:8d:2a:ea:04:00:5e:9d:bd:f2:d1:70:1c:51:0f:
                    d0:28:29:1a:e2:e3:3a:1c:39:b2:3e:15:ab:1e:23:
                    b0:e4:8d:97:44:ab:70:20:71:61:0f:d8:18:00:b9:
                    7e:c8:ca:0c:90:33:cc:ca:ae:18:46:29:b3:74:95:
                    8b:4d:a5:3a:c7:3e:06:65:e7:70:9e:be:ee:20:45:
                    aa:c3
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Authority Key Identifier:
                keyid:3D:D3:50:A5:D6:A0:AD:EE:F3:4A:60:0A:65:D3:21:D4:F8:F8:D6:0F
```

NETCRAFT REPORT







VULNERABILITY ASSESSMENT

Security vulnerabilities and flaws are found when a system or piece of software that operates on it is submitted to vulnerability scanning. Vulnerability management is a critical component of the entire strategy for safeguarding the company against data breaches and leaks. Vulnerability scanners scan the attack surface from the person who is looking at it. The program compares the attack surface information to a database of known security vulnerabilities in services and ports, packet construction anomalies, and probable pathways to susceptible apps or scripts. The scanning tool takes every attempt to exploit any hole it discovers.

Vulnerability scanning is essentially intrusive on the target computer's operating code, and as a result, it has its own set of risks. As a result, issues such as failures and reboots may occur during the scan, lowering productivity.

There are two types of vulnerability scanning: authenticated and unauthenticated. Because the tester does not have access to the network, the unauthenticated approach employs an intruder-style scan. Vulnerabilities discovered by such an audit may be accessed without logging in from outside the network. When the tester logs in as a network user, an authorized scan identifies vulnerabilities that might be exploited by a trusted user or an invader who has gained access as a trusted user.

TOOLS FOR VULNERABILITY SCANNING

Web application vulnerability Scanning software comes in a variety of forms. Scanners look for security flaws like XSS, SQL Injection, CGI-Binding, and Path Traversal in web applications from the outside.

There are number of tools

1. Netsparker
2. Rapid7 insightAppSec
3. Acunetix Web Vulnerability Scanner
4. PortSwigger Burp Suite
5. HCL AppScan
6. Qualys Web Application Scanner
7. Tenable Nessus
8. Mister Scanner
9. Zap
10. Legion
11. nmap

Among those number of tools, I focused on Netspaker, Zap, nmap Legion etc.

SCAN USING NMAP

Nmap stands for Network Mapper and is abbreviated as Nmap. As an open-source project, a Linux command-line application that analyzes IP addresses and ports in a network and discovers installed programs is available. Nmap is a network management program that determines which devices are connected to a network, which ports and services are open, and if security problems exist. Gordon Lyon (a.k.a. Fyodor) designed Nmap as a tool to aid in the mapping of a network's whole topology and the discovery of open ports and services. Nmap has become well-known as a result of its appearances in films and television series such as The Matrix and Mr. Robot.

For a multitude of reasons, security pros use Nmap as their scanning tool. Nmap allows you to quickly map a network since it doesn't need any sophisticated instructions or configurations. Simple commands (such as checking whether a host is up) and advanced programming utilizing the Nmap scripting engine are also available.

Nmap 7.91 scan initiated Sat Oct 16 17:03:50 2021 as: nmap -sS -iL Goldmansachs.txt -oN NmapScanResult.txt www.goldmansachs.com
Nmap scan report for goldmansachs.com (204.74.99.100)
Host is up (0.0086s latency).
rDNS record for 204.74.99.100: crs.ultradns.net
Not shown: 998 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http

Nmap scan report for honestdollar.com (138.8.25.58)
Host is up (0.019s latency).
Other addresses for honestdollar.com (not scanned): 148.86.15.58
Not shown: 997 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for research.gs.com (104.75.84.63)
Host is up (0.0073s latency).
Other addresses for research.gs.com (not scanned): 104.75.84.57
rDNS record for 104.75.84.63: a104-75-84-63.deploy.static.akamaitechnologies.com
Not shown: 996 filtered ports
PORT STATE SERVICE
25/tcp open smtp
53/tcp closed domain
80/tcp open http
443/tcp open https

Nmap scan report for gsam.com (204.4.187.254)
Host is up (0.019s latency).
Other addresses for gsam.com (not scanned): 207.17.33.254
Not shown: 997 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for gs-mosaic.qa.gs.com (104.75.84.57)
Host is up (0.0075s latency).
Other addresses for gs-mosaic.qa.gs.com (not scanned): 104.75.84.62 2402:d000:130:1::684b:543e 2402:d000:130:1::684b:5439

rDNS record for 104.75.84.57: a104-75-84-57.deploy.static.akamaitechnologies.com
Not shown: 996 filtered ports
PORT STATE SERVICE
25/tcp open smtp
53/tcp closed domain
80/tcp open http
443/tcp open https

Nmap scan report for gs-mosaic.gs.com (104.75.84.47)
Host is up (0.0073s latency).
Other addresses for gs-mosaic.gs.com (not scanned): 104.75.84.63
rDNS record for 104.75.84.47: a104-75-84-47.deploy.static.akamaitechnologies.com
Not shown: 997 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http
443/tcp open https

Nmap scan report for developer.gs.com (104.75.84.62)
Host is up (0.0070s latency).
Other addresses for developer.gs.com (not scanned): 104.75.84.63
rDNS record for 104.75.84.62: a104-75-84-62.deploy.static.akamaitechnologies.com
Not shown: 996 filtered ports
PORT STATE SERVICE
25/tcp open smtp
53/tcp closed domain
80/tcp open http
443/tcp open https

Nmap scan report for gs.com (204.74.99.100)
Host is up (0.011s latency).
rDNS record for 204.74.99.100: crs.ultradns.net
Not shown: 998 filtered ports
PORT STATE SERVICE
25/tcp open smtp
80/tcp open http

Nmap scan report for qaglobal-liquidity.gs.com (104.75.84.57)
Host is up (0.0077s latency).
Other addresses for qaglobal-liquidity.gs.com (not scanned): 104.75.84.62
rDNS record for 104.75.84.57: a104-75-84-57.deploy.static.akamaitechnologies.com
Not shown: 996 filtered ports
PORT STATE SERVICE

25/tcp open   smtp
53/tcp closed domain
80/tcp open   http
443/tcp open   https

Nmap scan report for global-liquidity.gs.com (104.75.84.63)
Host is up (0.0078s latency).
Other addresses for global-liquidity.gs.com (not scanned): 104.75.84.47
rDNS record for 104.75.84.63: a104-75-84-63.deploy.static.akamaitechnologies.com
Not shown: 996 filtered ports
PORT   STATE SERVICE
25/tcp open   smtp
53/tcp closed domain
80/tcp open   http
443/tcp open   https

Nmap scan report for goldman.com (204.74.99.100)
Host is up (0.011s latency).
rDNS record for 204.74.99.100: crs.ultradns.net
Not shown: 998 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http

Nmap scan report for marcus.com (204.74.99.100)
Host is up (0.011s latency).
rDNS record for 204.74.99.100: crs.ultradns.net
Not shown: 998 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http

Nmap scan report for marcus.co.uk (204.74.99.100)
Host is up (0.012s latency).
rDNS record for 204.74.99.100: crs.ultradns.net
Not shown: 998 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http

Nmap scan report for gsselect.com (204.74.99.100)
Host is up (0.013s latency).
rDNS record for 204.74.99.100: crs.ultradns.net

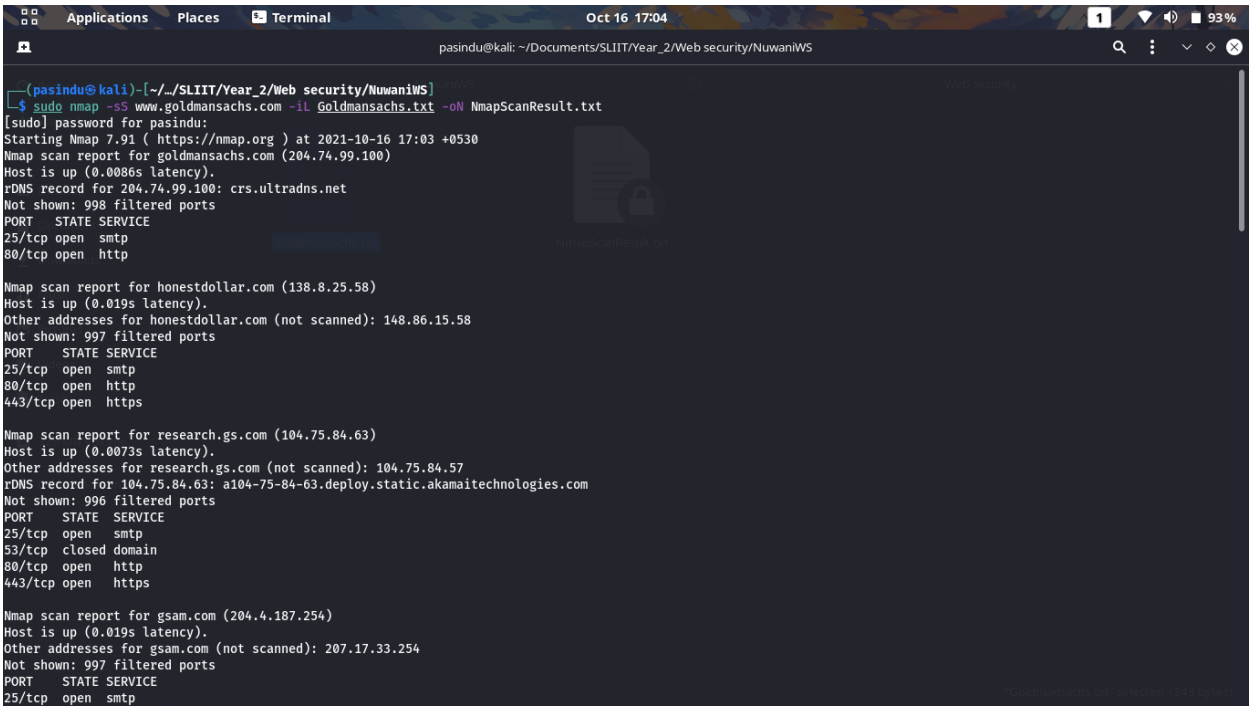
Not shown: 998 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http

Nmap scan report for goldmansachsindices.com (204.74.99.100)
Host is up (0.012s latency).
rDNS record for 204.74.99.100: crs.ultradns.net
Not shown: 998 filtered ports
PORT   STATE SERVICE
25/tcp open smtp
80/tcp open http

Nmap done at Sat Oct 16 17:04:47 2021 -- 15 IP addresses (15 hosts up) scanned in 56.55 seconds

Hear, I scan 15 Domains in my scope, and I identified 25, 80 are opened. I input all domains at ones with using this command,

nmap -sS www.goldmansachs.com -iL inscopedomain.txt -oN nampresult.txt



NETSPARKER

netsparker

10/27/2021 7:27:18 AM (UTC+05:30)
Detailed Scan Report

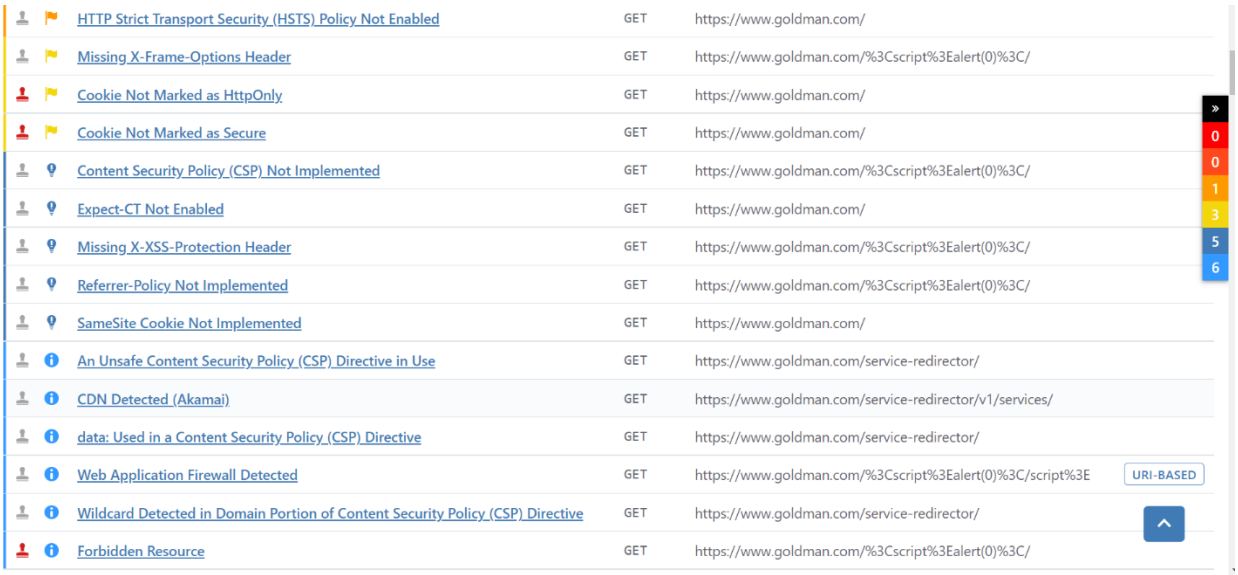
Netsparker is known as **a web application security scanner.** Netsparker is software that is widely used to detect existing vulnerabilities in web applications and reports to you in full detail, including solution suggestions.

goldman.com

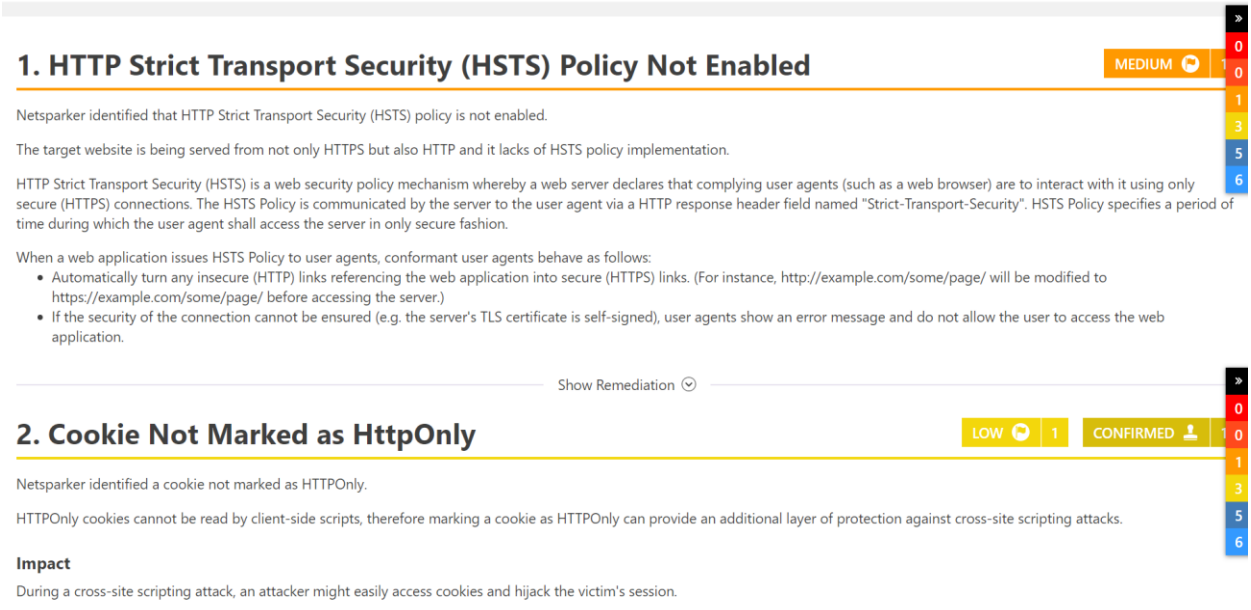
Vulnerability Summary

SEVERITY FILTER : CRITICAL HIGH MEDIUM LOW BEST PRACTICE INFORMATION

CONFIRM	VULNERABILITY	METHOD	URL	PARAMETER
	HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://www.goldman.com/	
	Missing X-Frame-Options Header	GET	https://www.goldman.com/%3Cscript%3Ealert(0)%3C/	
	Cookie Not Marked as HttpOnly	GET	https://www.goldman.com/	
	Cookie Not Marked as Secure	GET	https://www.goldman.com/	
	Content Security Policy (CSP) Not Implemented	GET	https://www.goldman.com/%3Cscript%3Ealert(0)%3C/	
	Expect-CT Not Enabled	GET	https://www.goldman.com/	
	Missing X-XSS-Protection Header	GET	https://www.goldman.com/%3Cscript%3Ealert(0)%3C/	
	Referrer-Policy Not Implemented	GET	https://www.goldman.com/%3Cscript%3Ealert(0)%3C/	
	SameSite Cookie Not Implemented	GET	https://www.goldman.com/	
	An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://www.goldman.com/service-redirector/	
	CDN Detected (Akamai)	GET	https://www.goldman.com/service-redirector/v1/services/	
	data: Used in a Content Security Policy (CSP) Directive	GET	https://www.goldman.com/service-redirector/	



HTTP Strict Transport Security (HSTS) Policy Not Enabled	GET	https://www.goldman.com/
Missing X-Frame-Options Header	GET	https://www.goldman.com/%3Cscript%3Ealert(0)%3C/
Cookie Not Marked as HttpOnly	GET	https://www.goldman.com/
Cookie Not Marked as Secure	GET	https://www.goldman.com/
Content Security Policy (CSP) Not Implemented	GET	https://www.goldman.com/%3Cscript%3Ealert(0)%3C/
Expect-CT Not Enabled	GET	https://www.goldman.com/
Missing X-XSS-Protection Header	GET	https://www.goldman.com/%3Cscript%3Ealert(0)%3C/
Referrer-Policy Not Implemented	GET	https://www.goldman.com/%3Cscript%3Ealert(0)%3C/
SameSite Cookie Not Implemented	GET	https://www.goldman.com/
An Unsafe Content Security Policy (CSP) Directive in Use	GET	https://www.goldman.com/service-redirector/
CDN Detected (Akamai)	GET	https://www.goldman.com/service-redirector/v1/services/
data: Used in a Content Security Policy (CSP) Directive	GET	https://www.goldman.com/service-redirector/
Web Application Firewall Detected	GET	https://www.goldman.com/%3Cscript%3Ealert(0)%3C/script%3E URI-BASED
Wildcard Detected in Domain Portion of Content Security Policy (CSP) Directive	GET	https://www.goldman.com/service-redirector/
Forbidden Resource	GET	https://www.goldman.com/%3Cscript%3Ealert(0)%3C/



1. HTTP Strict Transport Security (HSTS) Policy Not Enabled

MEDIUM

Netsparker identified that HTTP Strict Transport Security (HSTS) policy is not enabled.

The target website is being served from not only HTTPS but also HTTP and it lacks of HSTS policy implementation.

HTTP Strict Transport Security (HSTS) is a web security policy mechanism whereby a web server declares that complying user agents (such as a web browser) are to interact with it using only secure (HTTPS) connections. The HSTS Policy is communicated by the server to the user agent via a HTTP response header field named "Strict-Transport-Security". HSTS Policy specifies a period of time during which the user agent shall access the server in only secure fashion.

When a web application issues HSTS Policy to user agents, conformant user agents behave as follows:

- Automatically turn any insecure (HTTP) links referencing the web application into secure (HTTPS) links. (For instance, http://example.com/some/page/ will be modified to https://example.com/some/page/ before accessing the server.)
- If the security of the connection cannot be ensured (e.g. the server's TLS certificate is self-signed), user agents show an error message and do not allow the user to access the web application.

Show Remediation

2. Cookie Not Marked as HttpOnly

LOW 1 CONFIRMED

Netsparker identified a cookie not marked as HTTPOnly.

HTTPOnly cookies cannot be read by client-side scripts, therefore marking a cookie as HTTPOnly can provide an additional layer of protection against cross-site scripting attacks.

Impact

During a cross-site scripting attack, an attacker might easily access cookies and hijack the victim's session.

FINAL ASSESSMENT

Totally GOLDMANSACHS is in good security level and HTTP strict transport security Policy not enabled only medium level Risk I could find.

CONCLUSION

Vulnerability assessment provides deep insights on security deficiencies in an environment and helps to evaluate a system's vulnerability to a specific threat and the evolving ones. Simply put, an organization can fully understand the security flaws, overall risk, and assets that are vulnerable to cybersecurity breaches. To stay protected and to counter surprise attacks, a thorough vulnerability assessment can fix the unattended security issues.

Types of Vulnerability Assessments

- Basically, a vulnerability assessment applies various methods, tools, and scanners to find out grey areas, threats, and risks. Everything depends on how well the weakness in the given systems is discovered to attend to that specific need. Find below different types of vulnerability assessment scans:
- **Network-based scans**
  Going by the name, it helps identify possible network security attacks. The scan helps zero-in the vulnerable systems on wired or wireless networks.

- **Host-based scans**
  Server workstations or other network hosts vulnerabilities are easily identified using these scans. In the process, ports and services are examined vigorously. It also provides excellent visibility into the configuration settings and patch history of scanned systems.

- **Wireless network scans**
  Wireless network infrastructure is scanned to identify vulnerabilities; it helps in validating a company's network.

- **Application Scans**
  It is used to test websites to discover all known software vulnerabilities.

- **Database Scans**
  Database Scans aid in identifying grey areas in a database to prevent vicious attacks by cybercriminals.

So here to analyze the vulnerabilities of GOLDMAN SACHS I used many kinds of automated scanning tolls and information gathering tools. Then what I was taken from this was over roll I selected domains are operated under good security level.