



Sri Lanka Institute of Information Technology

IE2062-Web Security

IT Number	Name
IT22581402	C.D.Aluthge

Information gathering and reconnaissance phase

- a. Subdomain enumeration
 - I. Recon-ng
- b. Getting alive subdomains
 - I. Nslookup
- c. DNS enumeration
 - I. Dnsdumpster
 - II. Nikto
 - III. Dnsrecon
- d. Public devices enumeration
 - I. Whatweb
 - II. whois
- e. Find WAF (web application firewall) protection.
 - I. Wafwoof
- f. Find open ports.
 - I. Nmap
- g. Exploitation
 - I. sqlmap

vulnerability analysis phase

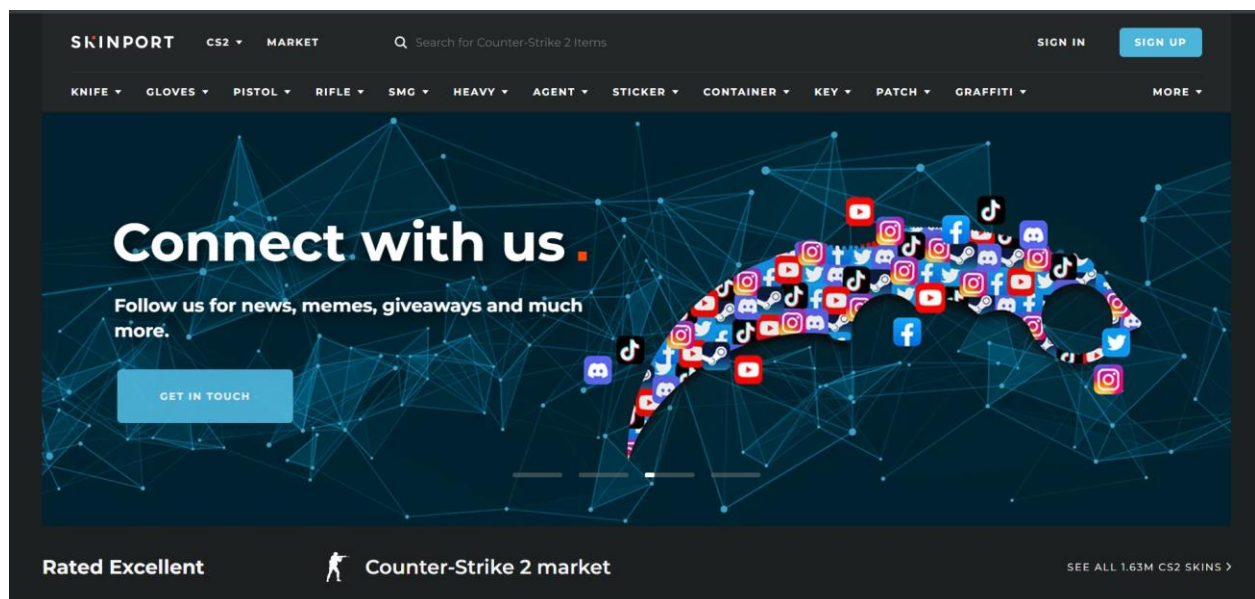
Target domain: <https://skinport.com>

- a. Weak Ciphers Enabled (Confirmed)
- b. Content Security policy (CSP) Not Implemented
- c. Expect-CT Not Enabled
- d. Email Address Disclosure
- e. Web Application Firewall Detected
- f. Generic Email Address Disclosure
- g. ExpressJS Identified
- h. Content Security policy (CSP) Contains Out of Scope report-Uri Domain
- i. Referrer-Policy Not Implemented

Conclusion

Scope:

A website called Skinport.com is devoted to virtual goods exchange in gaming, with a primary concentration on skins from well-known titles. It serves as a marketplace where players from different gaming platforms and games may purchase, sell, and exchange in-game things including weapon skins, character costumes, and other cosmetic items. Skinport.com offers a safe platform for gamers to transact virtual goods, guaranteeing fair pricing, authenticity, and dependable payment processing for both buyers and sellers.



In Scope

api.skinport.com Public REST API - Docs: https://docs.skinport.com Cloudflare DDOS Cloudflare WAF Express Heroku JavaScript PostgreSQL	Domain	In scope	Critical	Eligible	Feb 21, 2023
app.skinport.com Backend: app.skinport.com Important Note: Alias of skinport.com/api/ (to app.skinport.com/api/) Cloudflare DDOS Cloudflare WAF Express Heroku JavaScript PostgreSQL	Domain	In scope	Critical	Eligible	Feb 21, 2023
skinport.com skinport.com (without subdomains, e.g. screenshot.skinport.com, float.skinport.com and so on) Frontend: skinport.com Important Note: <ul style="list-style-type: none"> • skinport.com/api/ (redirected to app.skinport.com/api/) submissions, please use app.skinport.com scope! • skinport.com/support: If you are to test anything related to typing in the support ticket, please, send following message before that. <div>Hello. I'm a pentester from HackerOne. I'm going to test something in support ticket. Your developers are aware of that.</div> Cloudflare DDOS Cloudflare WAF Express Heroku JavaScript React	Domain	In scope	Critical	Eligible	Feb 21, 2023
http://skinport.com/blog/ Cloudflare DDOS Cloudflare WAF JavaScript MySQL	URL	In scope	Medium	Eligible	Feb 21, 2023

Out of scope

*.skinport.com	Wildcard	Out of scope	None	Ineligible	May 15, 2023
----------------	----------	--------------	------	------------	--------------

OWASP top 10 vulnerabilities

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration

- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery

Broken Access Control

When users are unable to adequately impose limitations on what they can access or do within a system, this is known as broken access control. This vulnerability makes it possible for unauthorized individuals to access private data or carry out tasks that shouldn't be permitted. Insecure references to objects, improperly configured permissions, and a lack of authentication checks are the causes of it. Because it can result in illegal data exposure, manipulation, or system penetration, it's a major problem.

Cryptographic Failures

Cryptographic collapses are the result of poor algorithms, incorrect implementations, or improper management of encryption keys, which compromise the security of information encrypted via encryption techniques. By undermining security safeguards and perhaps leading to data breaches, this can lead to unauthorized access to or exposure of sensitive data.

Injection

Injection: it is a type of security vulnerability in which untrusted data is sent to an interpreter as part of a command or query. Most often, attackers use this to inject malicious code into input fields, for example, login forms or search boxes. The interpreter then executes this code, which can give the attacker unauthorized access to data, alter the application's behavior, or gain full control over the system. There are many types of injections, such as SQL injection, where the attackers manipulate database queries, or cross-site scripting, where the malicious script is injected into a web page that other users view.

Insecure Design

Insecure design means the security flaws within the fundamental system or application design born out of insufficient attention to security at the design time. Consequently, systems have vulnerabilities that enable unauthorized system access or breaches. Examples are poor user authentication or no network segmentation. To fix insecure design, significant changes to the architecture are needed to develop the designs securely.

Security Misconfiguration

Imagine you accidentally leave your front door closed but not locked. That's what a security misconfiguration is like. Essentially, it's not properly securing your software systems, servers, or web applications. This can include default settings, shipped insecurely, or unnecessary features. Unauthorized users might target such vulnerabilities to access your info or disrupt the operation. Therefore, one should monitor and update security measures continuously to avoid misconfiguration.

Vulnerable and Outdated Components

Vulnerable components are software elements that are known to contain security flaws that could be exploited by hackers. However, software components that have not received an upgrade in a long time are known as outdated components, and they may not include important security updates and bug fixes. In order to maintain a secure system environment, both sorts of components present security concerns and should be routinely updated and monitored.

Identification and Authentication Failures

When systems are unable to accurately confirm user identities or authenticate their access credentials, identification and authentication failures take place. Whereas authentication failures are caused by an inability to verify user identities, identification failures are the consequence of incorrect user recognition. In order to identify and fix system vulnerabilities, strong authentication procedures and frequent security assessments are essential. These failures might result in unauthorized access and security breaches.

Software and Data Integrity Failures

Software code or data accuracy, consistency, and reliability are jeopardized in software and data integrity issues. Data integrity problems are caused by mistakes, unauthorized access, or cyberattacks, whereas programming errors, malicious code, or unauthorized alterations are the causes of software integrity problems. To reduce risks and guarantee system security and dependability, preventive measures include backups, data encryption, access controls, and regular updates.

Security Logging and Monitoring Failures

Failed security logging and monitoring systems result in delayed detection of security incidents and higher risks since they are unable to reliably capture and evaluate security-related events. Monitoring failures are caused by insufficient tools or response protocols, whereas logging failures are caused by misconfigurations or deactivated logging systems. Organizations should establish strong response protocols, use comprehensive logging practices, deploy efficient monitoring tools like SIEM tools, train security teams, and continuously improve logging and monitoring configurations in light of best practices and emerging threats in order to address these failures. By taking these steps, cybersecurity defenses are strengthened, and the effects of security events are lessened.

Server-Side Request Forgery

A security flaw known as server-side request forgery (SSRF) allows attackers to take control of a susceptible server and send unwanted requests, usually to external or internal systems. Unauthorized access, data loss, and more exploitation may result from this. Input validation, whitelisting authorized resources, network segmentation, and access controls are all part of prevention. Frequent security testing improves overall system security by assisting in the identification and mitigation of SSRF threats.

Information gathering and reconnaissance phase.

The objective is to gather as much pertinent data as you can about the intended system or organization. Understanding the target's infrastructure, seeing potential vulnerabilities, and organizing additional security testing operations are all made easier with the aid of this information.

Domain: <https://skinport.com>

Subdomain enumeration

Recon-ng

Recon-ng is an open-source reconnaissance tool with Python foundation that is used for penetration testing and security evaluations. It collects data from domains, IPs, emails, and social media platforms using a modular framework with different modules. The advantages of recon-ng are its flexibility for scripting and automation, integration with many data sources, and data enrichment capabilities. It is used by security experts to gather and evaluate intelligence, spot possible weaknesses, and improve overall security posture during the first reconnaissance phase. Its vibrant community guarantees continuous upgrades and support, which makes it an invaluable addition to cybersecurity toolkits.

```
(deshan@kali)-[~]
$ recon-ng
[*] Version check disabled.
```

Sponsored by ...

BLACK HILLS
www.blackhillinfosec.com more you are able to hear"

www.practisec.com

[recon-ng v5.1.2, Tim Tomes (@lanmaster53)]

```
[1] Recon modules

[recon-ng][default] > marketplace search googel
[*] Searching module index for 'googel'...
[!] No modules found.
Searches marketplace modules

Usage: marketplace search [<regex>]

[recon-ng][default] > marketplace search google
[*] Searching module index for 'google'...
```

Path	Version	Status	Updated	D	K
recon/domains-hosts/google_site_web	1.0	installed	2019-06-24		*

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

```
[recon-ng][default] > marketplace install recon/domains-hosts/google_site_web
[*] Module installed: recon/domains-hosts/google_site_web
[*] Reloading modules ...
```

```
$ recon-ng
```


—, —, —.

© 2011 Blackwell Publishing Ltd *Journal of Internal Medicine* 270: 105–114

111. **Recon. No.**

```
[*] Searching
```

```
[!] No modul
```

Searches mar

10

9-11-2000

```
[*] Searching
```

[*] Searching

K = Required

```
[*] Module i
```

```
[*] Reloading
```

100

Proof of concept:

```
[recon-ng][default] > show info
Shows various framework items

Usage: show <companies|contacts|credentials|domains|hosts|leaks|locations|netblocks|ports|profiles|pushpins|repositories|vulnerabilities>

[recon-ng][default] > marketplace search google
[*] Searching module index for 'google' ...

+-----+-----+-----+-----+-----+-----+
| Path | Version | Status | Updated | D | K |
+-----+-----+-----+-----+-----+
| recon/domains-hosts/google_site_web | 1.0 | installed | 2019-06-24 | | |
+-----+-----+-----+-----+-----+

D = Has dependencies. See info for details.
K = Requires keys. See info for details.

[recon-ng][default] > modules load recon/domains-hosts/google_site_web
[recon-ng][default][google_site_web] > info

Name: Google Hostname Enumerator
Author: Tim Tomes (@lanmaster53)
Version: 1.0
```

```
Description:
Harvests hosts from Google.com by using the 'site' search operator. Updates the 'hosts' table with the results.

Options:
  Name      Current Value  Required  Description
  -----
SOURCE     skinport.com    yes       source of input (see 'info' for details)

Source Options:
  default      SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>     string representing a single input
  <path>       path to a file containing a list of inputs
  query <sql>  database query returning one column of inputs

[recon-ng][default][google_site_web] > options set source skinport.com
SOURCE => skinport.com
[recon-ng][default][google_site_web] > run
```

Proof of concept:

```
[*] Searching Google for: site:skinport.com
[*] Country: None
[*] Host: status.skinport.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: docs.skinport.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*]
[*] Country: None
[*] Host: screenshot.skinport.com
[*] Ip_Address: None
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
```

SUMMARY

```
[*] 3 total (3 new) hosts found.
[recon-ng][default][google_site_web] > █
```

Getting alive subdomains

- Nslookup

A command-line utility called `nslookup` is used to query DNS (Domain Name System) servers and get DNS-related data. In addition to performing reverse DNS lookups and retrieving other DNS records like A, AAAA, MX, NS, PTR, and TXT records, it resolves domain names to IP addresses. It is flexible for diagnosing DNS problems, validating DNS configurations, and testing DNS servers because it may be used in both interactive and non-interactive modes. Network administrators and cybersecurity experts frequently utilize `nslookup`, which runs on several platforms, for DNS-related activities and diagnostics.

Proof of concept:

```
(deshan@kali)-[~]  
$ nslookup skinport.com  
Server:          192.168.43.1  
Address:         192.168.43.1#53  
  
Non-authoritative answer:  
Name:   skinport.com  
Address: 104.18.16.19  
Name:   skinport.com  
Address: 104.18.17.19
```

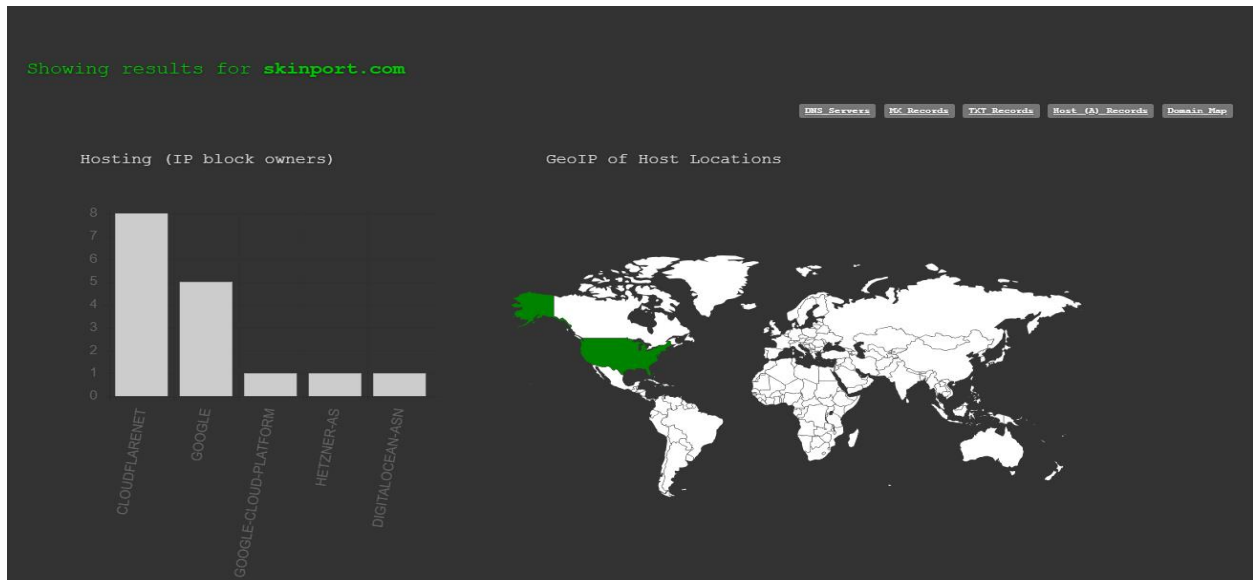
DNS enumeration

- dnsdumpster



































































DNSDumpster is an online tool focused on DNS information gathering for a target domain. It assists in discovering subdomains, viewing DNS records (A, AAAA, MX, NS, SOA, TXT), mapping domain names to IP addresses, and providing visual

representations of DNS-related data. Security professionals and penetration testers use DNSDumpster during reconnaissance to understand a domain's infrastructure, identify potential vulnerabilities, and aid in security assessments. While it offers valuable insights, users should supplement its findings with other tools for a comprehensive analysis, considering that its data may not always be the most current or complete.

Proof of concept:



Proof of concept:

DNS Servers		
edna.ns.cloudflare.com.     	172.64.32.109	CLOUDFLARENET United States
mark.ns.cloudflare.com.     	173.245.59.130	CLOUDFLARENET United States
MX Records ** This is where email for the domain goes...		
1 aspmx.l.google.com.    	142.251.163.27	GOOGLE United States
10 aspmx2.googlemail.com.    	209.85.202.27	GOOGLE United States
10 aspmx3.googlemail.com.    	64.233.184.26	GOOGLE United States
5 alt1.aspmx.l.google.com.    	209.85.202.27	GOOGLE United States
5 alt2.aspmx.l.google.com.    	64.233.184.26	GOOGLE United States
TXT Records ** Find more hosts in Sender Policy Framework (SPF) configurations		
"ahrefs-site-verification_ae2edc7266313f6def19087704c0f496d1619c1e88b44b6e231473b9d6d807e0"		
"facebook-domain-verification=hud44hmc0o6ul6x71sokjuampao5gq"		
"google-site-verification=_keDvfbxEOpLn7yrdIanbDDR0WP-t-On72IC_2XqFco"		
"v=spf1 include:_spf.google.com include:mail.zendesk.com include:amazonses.com -all"		
"yandex-verification: dac269d26167b890"		
Host Records (A) ** this data may not be current as it uses a static database (updated monthly)		
grafana.skinport.com    	34.117.214.84 84.214.117.34.bc.googleusercontent.com	GOOGLE-CLOUD-PLATFORM United States
blog.skinport.com     HTTP: cloudflare	104.18.17.19	CLOUDFLARENET unknown
cdn.skinport.com     HTTP: cloudflare	104.18.16.19	CLOUDFLARENET unknown
logs-drain.skinport.com     HTTP: nginx/1.22.0 HTTP TECH: nginx/1.22.0	78.47.196.118 static.118.196.47.78.clients.your-server.de	HETZNER-AS Germany
s.skinport.com     HTTP: cloudflare	104.18.16.19	CLOUDFLARENET unknown
docs.skinport.com     HTTP: cloudflare	104.18.16.19	CLOUDFLARENET unknown
status.skinport.com     HTTP: Caddy	68.183.43.169 status.ohdear.app	DIGITALOCEAN-ASN United Kingdom
float.skinport.com     HTTP: cloudflare	104.18.17.19	CLOUDFLARENET unknown
screenshot.skinport.com     HTTP: cloudflare	104.18.17.19	CLOUDFLARENET unknown

• Nikto

Nikto is an open-source web server scanner made to find possible security holes in applications and web servers. With its extensive scanning capabilities, it may identify problems including out-of-date software, unsafe configurations, weak scripts, and incorrect SSL/TLS settings. In addition to producing comprehensive results after scanning, Nikto may be customized and scripted, connects with

automated workflows, and receives community assistance and frequent database upgrades. For security experts performing web security assessments, it's a useful tool that helps with vulnerability discovery and mitigation to improve overall security posture.

Proof of concept:

```
(root@kali)~[~]
# nikto -h skinport.com
- Nikto v2.5.0

+ Multiple IPs found: 104.18.16.19, 104.18.17.19
+ Target IP: 104.18.16.19
+ Target Hostname: skinport.com
+ Target Port: 80
+ Start Time: 2024-04-28 01:07:12 (GMT5.5)

+ Server: cloudflare
+ /: IP address found in the '__cf_bm' cookie. The IP is "1.0.1.1".
+ /: IP address found in the 'set-cookie' header. The IP is "1.0.1.1". See: https://portswigger.net/kb/issues/00600300_private-ip-addresses-disclosed
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options
+ Root page / redirects to: https://skinport.com/
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ /: The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/
+ /cdn-cgi/trace: Retrieved access-control-allow-origin header: *.
+ /cdn-cgi/trace: Cloudflare trace CGI found, which may leak some system information.
+ 7962 requests: 0 error(s) and 6 item(s) reported on remote host
+ End Time: 2024-04-28 01:20:46 (GMT5.5) (814 seconds)
```

```
+ 1 host(s) tested
```

Dnsrecon

For security evaluations and penetration tests, DNSRecon is a powerful open-source tool for DNS reconnaissance that finds and counts DNS information. It is particularly good at finding subdomains, enumerating DNS records (A, AAAA, MX, NS, SOA, TXT), transferring DNS zones, and it can handle wordlist-based and brute-force attacks. With its automation, customization, and integration features, it's a useful tool for figuring out possible attack points, comprehending target infrastructure, and raising security awareness in general. DNSRecon is still a dependable option for DNS reconnaissance operations because of its community support and frequent updates.

Proof of concept:

```
(deshan@kali)-[~]
$ dnsrecon -d skinport.com -D /user/share/wordlists/dnsmap.txt -t std --xml skinport.xml
[*] std: Performing General Enumeration against: skinport.com ...
[*] DNSSEC is configured for skinport.com
[*] DNSKEYs:
[*] NSEC KSK ECDSAP256SHA256 99db2cc14cabdc33d6d77da63a2f15f7 1112584f234e8d1dc428e39e8a4a97e1 aa271a555dc
90701e17e2a4c4b6f120b 7c32d44f4ac02bd894cf2d4be7778a19
[*] NSEC ZSK ECDSAP256SHA256 a09311112cf9138818cd2feae970ebbd 4d6a30f6088c25b325a39abbc5cd1197 aa098283e5a
af421177c2aa5d714992a 9957d1bcc18f98cd71f1f1806b65e148
[*] SOA edna.ns.cloudflare.com 173.245.58.109
[*] SOA edna.ns.cloudflare.com 172.64.32.109
[*] SOA edna.ns.cloudflare.com 108.162.192.109
[*] SOA edna.ns.cloudflare.com 2a06:98c1:50::ac40:206d
[*] SOA edna.ns.cloudflare.com 2606:4700:50::adf5:3a6d
[*] SOA edna.ns.cloudflare.com 2803:f800:50::6ca2:c06d
[*] NS mark.ns.cloudflare.com 172.64.33.130
[*] Bind Version for 172.64.33.130 "2024.4.1"
[*] NS mark.ns.cloudflare.com 173.245.59.130
[*] Bind Version for 173.245.59.130 "2024.4.1"
[*] NS mark.ns.cloudflare.com 108.162.193.130
[*] Bind Version for 108.162.193.130 "2024.4.1"
[*] NS mark.ns.cloudflare.com 2606:4700:58::adf5:3b82
[*] NS mark.ns.cloudflare.com 2803:f800:50::6ca2:c182
[*] NS mark.ns.cloudflare.com 2a06:98c1:50::ac40:2182
[*] NS edna.ns.cloudflare.com 108.162.192.109
```

Proof of concept:

```
[*] Bind Version for 108.162.192.109 "2024.4.1"
[*] NS edna.ns.cloudflare.com 172.64.32.109
[*] Bind Version for 172.64.32.109 "2024.4.1"
[*] NS edna.ns.cloudflare.com 173.245.58.109
[*] Bind Version for 173.245.58.109 "2024.4.1"
[*] NS edna.ns.cloudflare.com 2803:f800:50::6ca2:c06d
[*] NS edna.ns.cloudflare.com 2606:4700:50::adf5:3a6d
[*] NS edna.ns.cloudflare.com 2a06:98c1:50::ac40:206d
[*] MX aspmx.l.google.com 142.251.10.26
[*] MX aspmx2.googlemail.com 173.194.202.26
[*] MX alt2.aspmx.l.google.com 142.250.141.26
[*] MX alt1.aspmx.l.google.com 173.194.202.26
[*] MX aspmx3.googlemail.com 142.250.141.26
[*] MX aspmx.l.google.com 2404:6800:4003:c04::1a
[*] MX aspmx2.googlemail.com 2607:f8b0:400e:c00::1b
[*] MX alt2.aspmx.l.google.com 2607:f8b0:4023:c0b::1a
[*] MX alt1.aspmx.l.google.com 2607:f8b0:400e:c00::1a
[*] MX aspmx3.googlemail.com 2607:f8b0:4023:c0b::1a
[*] A skinport.com 104.18.17.19
[*] A skinport.com 104.18.16.19
[*] TXT skinport.com yandex-verification: dac269d26167b890
[*] TXT skinport.com ahrefs-site-verification_ae2edc7266313f6def19087704c0f496d1619c1e88b44b6e231473b9d6d
807e0
[*] TXT skinport.com facebook-domain-verification=hud44bmc0o6ul6x71sokjuampao5gq
```

```
[*] TXT skinport.com google-site-verification=_keDvfbxE0pLn7yrdIanbDDR0WP-t-On72IC_ZXqFco
[*] TXT skinport.com v=spf1 include:spf.google.com include:mail.zendesk.com include:amazonses.com -all
[*] TXT _dmarc.skinport.com v=DMARC1; p=reject; rua=mailto:83798c7fbfed40f084768eb4d85e7fa9@dmARC-report
s.cloudflare.net
[*] Enumerating SRV Records
[-] No SRV Records Found for skinport.com
[*] Saving records to XML file: skinport.xml
```

Public devices enumeration

- **Whatweb**

WhatWeb is a powerful open-source website scanner that specializes in identifying the technologies utilized by websites. It excels in detecting web servers, frameworks, content management systems (CMS), programming languages, and more through its fingerprinting and HTTP header analysis capabilities. Security professionals leverage WhatWeb during reconnaissance and vulnerability assessments to gather insights into target websites' technology stacks, assess security risks associated with detected technologies, and identify potential vulnerabilities or outdated components. Its scriptable and customizable nature, along with integration options, makes it a valuable tool for automating scanning workflows and enhancing security assessments.

Proof of concept:

```
(root@kali)-[~]
└─# whatweb skinport.com
http://skinport.com [301 Moved Permanently] Cookies[__cf_bm], Country[UNITED STATES][US], HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[104.18.16.19], RedirectLocation[https://skinport.com/], Title[301 Moved Permanently], UncommonHeaders[x-content-type-options,cf-ray]
https://skinport.com/ [200 OK] Cookies[__cf_bm], Country[UNITED STATES][US], HTML5, HTTPServer[cloudflare], HttpOnly[__cf_bm], IP[104.18.16.19], Open-Graph-Protocol[website], Script, Strict-Transport-Security[max-age=31536000; includeSubDomains; preload], Title[Skinport], UncommonHeaders[cf-ray,cf-cache-status,content-security-policy,expect-ct,nel,origin-agent-cluster,referrer-policy,report-to,reporting-endpoints,x-content-type-options,x-dns-prefetch-control,x-download-options,x-permitted-cross-domain-policies], Via-Proxy[1.1 vegur], X-Frame-Options[SAMEORIGIN], X-UA-Compatible[ie=edge], X-XSS-Protection[0]
```

- **Whois**

A key networking tool and protocol, whois is used to query databases and obtain data on IP addresses, domain names, and autonomous system numbers (ASNs). It offers information about domain registration, owner contact details, DNS information, IP address allocation, and ASN ownership. Whois is frequently used for domain research, network problems, IP geolocation, abuse investigations, and domain registration questions by network administrators, cybersecurity experts, domain registrars, and law enforcement organizations. Due to privacy concerns,

registrars have started offering privacy services that conceal personal information from view in public Whois data. While Whois provides insightful information, users should be aware of potential limits across multiple Whois servers, privacy concerns, and data accuracy.

Proof of concept:

```
(root@kali)~[~] | for: site:https://skinport.com
# whois skinport.com found on the current page. Jumping to Result 3701.
Domain Name: SKINPORT.COM | https://skinport.com
Registry Domain ID: 2306485802_DOMAIN_COM-VRSN | Jumping to Result 3801.
Registrar WHOIS Server: whois.namecheap.com | com
Registrar URL: http://www.namecheap.com | Page: Jumping to Result 3901.
Updated Date: 2020-09-23T11:10:20Z | skinport.com
Creation Date: 2018-09-05T18:23:35Z | com | Page: Jumping to Result 4001.
Registry Expiry Date: 2026-09-05T18:23:35Z | com
Registrar: NameCheap, Inc. | the current page. Jumping to Result 4101.
Registrar IANA ID: 1068 | https://skinport.com
Registrar Abuse Contact Email: abuse@namecheap.com | ng to Result 4201.
Registrar Abuse Contact Phone: +1.6613102107 | com
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Name Server: EDNA.NS.CLOUDFLARE.COM | skinport.com
Name Server: MARK.NS.CLOUDFLARE.COM | nt Page. Jumping to Result 4401.
DNSSEC: signedDelegation | https://skinport.com
DNSSEC DS Data: 2371 13 2 49F728E1B59EE31AEDA9ADE3A92725C8022F9D446710F1C74667C4ADC8A999CB
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2024-04-22T09:30:01Z <<< Result 4601.
```


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

No New Subdomains Found on the Current Page. Jumping to Result 3701.

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.

Search by Google: <https://www.google.com>

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

Proof of concept:

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 1 3701.
Registrars. [site:https://skinport.com](https://skinport.com)
Domain name: skinport.com [und on the Current Page. Jumping to Result 3801.](#)
Registry Domain ID: 2306485802_DOMAIN_COM-VRSN [.com](#)
Registrar WHOIS Server: whois.namecheap.com [Page. Jumping to Result 3901.](#)
Registrar URL: <http://www.namecheap.com> [kinport.com](#)
Updated Date: 2020-09-23T11:10:20.42Z [rent Page. Jumping to Result 4001.](#)
Creation Date: 2018-09-05T18:23:35.00Z [skinport.com](#)
Registrar Registration Expiration Date: 2026-09-05T18:23:35.00Z [ilt 4101.](#)
Registrar: NAMECHEAP INC [site:https://skinport.com](https://skinport.com)
Registrar IANA ID: 1068 [und on the Current Page. Jumping to Result 4201.](#)
Registrar Abuse Contact Email: abuse@namecheap.com
Registrar Abuse Contact Phone: +1.9854014545 [ge. Jumping to Result 4301.](#)
Reseller: NAMECHEAP INC [site:https://skinport.com](https://skinport.com)
Domain Status: clientTransferProhibited <https://icann.org/epp#clientTransferProhibited>
Registry Registrant ID: [site:https://skinport.com](https://skinport.com)
Registrant Name: Redacted for Privacy [rent Page. Jumping to Result 4501.](#)
Registrant Organization: Privacy service provided by Withheld for Privacy ehf
Registrant Street: Kalkofnsvegur 2 [Current Page. Jumping to Result 4601.](#)
Registrant City: Reykjavik [site:https://skinport.com](https://skinport.com)
Registrant State/Province: Capital Region [Page. Jumping to Result 4701.](#)
Registrant Postal Code: 101 [ite:https://skinport.com](https://skinport.com)
Registrant Country: IS
Registrant Phone: +354.4212434 [web\] > \[](#)

Proof of concept:

```
Registrant Phone Ext: [redacted] site:https://skinport.com
Registrant Fax: [redacted] Found on the Current Page. Jumping to Result 3801.
Registrant Fax Ext: [redacted] site:https://skinport.com
Registrant Email: 1700f877b52643d8afd44d0b3f15962e.protect@withheldforprivacy.com
Registry Admin ID: [redacted] site:https://skinport.com
Admin Name: Redacted for Privacy [redacted] Current Page. Jumping to Result 4001.
Admin Organization: Privacy service provided by Withheld for Privacy ehf
Admin Street: Kalkofnsvegur 2 [redacted] Current Page. Jumping to Result 4101.
Admin City: Reykjavik [redacted] site:https://skinport.com
Admin State/Province: Capital Region [redacted] Current Page. Jumping to Result 4201.
Admin Postal Code: 101 [redacted] site:https://skinport.com
Admin Country: IS [redacted] Found on the Current Page. Jumping to Result 4301.
Admin Phone: +354.4212434 [redacted] site:https://skinport.com
Admin Phone Ext: [redacted] Found on the Current Page. Jumping to Result 4401.
Admin Fax: [redacted] Google for: site:https://skinport.com
Admin Fax Ext: [redacted] Found on the Current Page. Jumping to Result 4501.
Admin Email: 1700f877b52643d8afd44d0b3f15962e.protect@withheldforprivacy.com
Registry Tech ID: [redacted] Found on the Current Page. Jumping to Result 4601.
Tech Name: Redacted for Privacy [redacted] https://skinport.com
Tech Organization: Privacy service provided by Withheld for Privacy ehf
Tech Street: Kalkofnsvegur 2 [redacted] https://skinport.com
Tech City: Reykjavik
Tech State/Province: Capital Region [redacted]
```

```
Tech Postal Code: 101 [redacted] Found on the Current Page. Jumping to Result 4201.
Tech Country: IS [redacted] site:https://skinport.com
Tech Phone: +354.4212434 [redacted] Found on the Current Page. Jumping to Result 4301.
Tech Phone Ext: [redacted] Google for: site:https://skinport.com
Tech Fax: [redacted] Subdomains Found on the Current Page. Jumping to Result 4401.
Tech Fax Ext: [redacted] Google for: site:https://skinport.com
Tech Email: 1700f877b52643d8afd44d0b3f15962e.protect@withheldforprivacy.com
Name Server: edna.ns.cloudflare.com [redacted] https://skinport.com
Name Server: mark.ns.cloudflare.com [redacted] Current Page. Jumping to Result 4601.
DNSSEC: unsigned [redacted] site:https://skinport.com
URL of the ICANN WHOIS Data Problem Reporting System: http://wdprs.internic.net/
>>> Last update of WHOIS database: 2024-04-21T16:30:44.80Z <<<
For more information on Whois status codes, please visit https://icann.org/epp
```

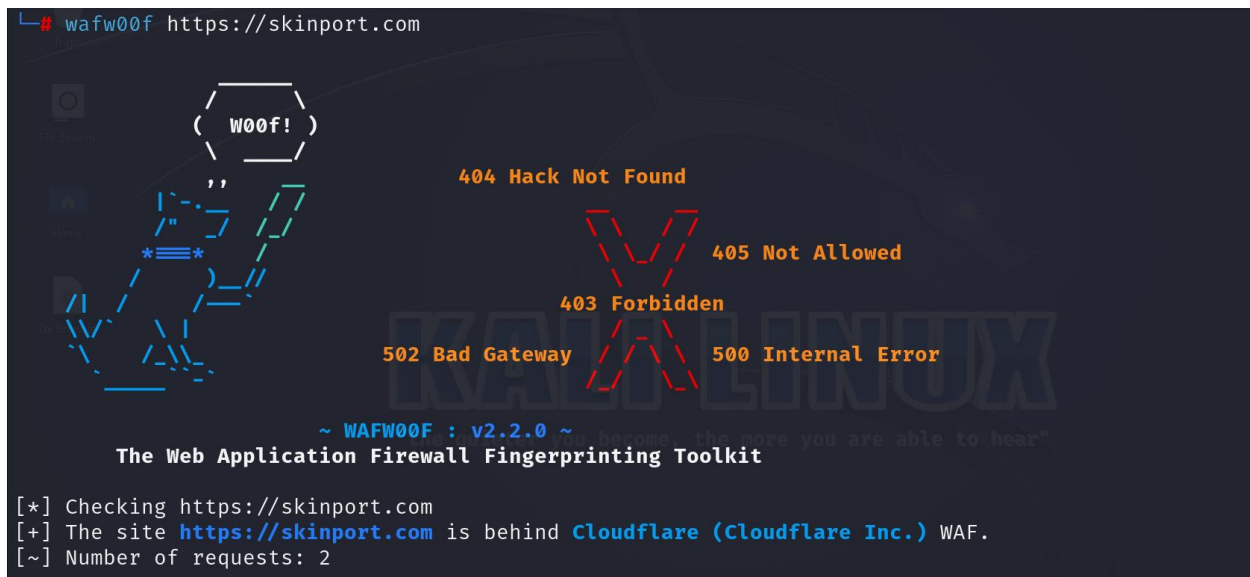
Find WAF (web application firewall) protection.

- Wafwoof

Wafw00f is an open-source program that uses content patterns, HTTP responses, and header analysis to detect and fingerprint web application firewalls (WAFs). It gives testers and security experts information about the particular WAF technology

or vendor being used as well as assists them in determining whether a web application is protected by a WAF. In addition to being user-friendly and seamlessly integrating with automated testing workflows, Wafw00f also keeps an updated database of WAF signatures and offers community support. It is a useful tool for security assessment and reconnaissance jobs, supporting the creation of efficient testing plans and workarounds.

Proof of concept:

The image is a screenshot of a terminal window with a dark background. At the top, a command is entered: `# wafw00f https://skinport.com`. Below the command, there is a large, stylized ASCII art graphic of a dog's head, with the text "(W00f!)" inside its snout. To the right of the dog, several HTTP status codes are listed in orange text: "404 Hack Not Found", "405 Not Allowed", "403 Forbidden", "502 Bad Gateway", and "500 Internal Error". Below these codes, the text "~ WAFW00F : v2.2.0 ~" is displayed, followed by the tagline "The Web Application Firewall Fingerprinting Toolkit". At the bottom of the terminal, there are three lines of output: "[*] Checking https://skinport.com", "[+] The site https://skinport.com is behind Cloudflare (Cloudflare Inc.) WAF.", and "[~] Number of requests: 2".

```
# wafw00f https://skinport.com

( W00f! )

404 Hack Not Found
405 Not Allowed
403 Forbidden
502 Bad Gateway
500 Internal Error

~ WAFW00F : v2.2.0 ~
The Web Application Firewall Fingerprinting Toolkit

[*] Checking https://skinport.com
[+] The site https://skinport.com is behind Cloudflare (Cloudflare Inc.) WAF.
[~] Number of requests: 2
```

Find open ports.

- Nmap

Nmap, sometimes known as "Network Mapper," is a potent open-source network scanning program used for vulnerability analysis, security audits, and network discovery. It is particularly good at operating system detection, host discovery, port scanning, and service version detection. Because it supports custom scripting and automation, Nmap's scripting engine (NSE) is adaptable to a wide range of security activities and integration requirements. Because of its dependability, adaptability, and large feature set, network administrators, security experts, and penetration

testers frequently use it for network reconnaissance, security audits, and network monitoring.

Proof of concept:

```
(root@kali)-[~]
└─# nmap -sV -A -T4 skinport.com
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-22 15:14 +0530
Nmap scan report for skinport.com (104.18.17.19)
Host is up (0.0026s latency).
Other addresses for skinport.com (not scanned): 104.18.16.19
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
25/tcp    open  tcpwrapped
|_smtp-commands: Couldn't establish connection on port 25
80/tcp    open  tcpwrapped
|_http-server-header: cloudflare
443/tcp   open  tcpwrapped
|_http-server-header: cloudflare
|_ssl-cert: Subject: commonName=skinport.com
| Subject Alternative Name: DNS:*.skinport.com, DNS:skinport.com
| Not valid before: 2024-03-26T03:31:53
|_Not valid after: 2024-06-24T03:31:52
|_http-title: 400 The plain HTTP request was sent to HTTPS port
8080/tcp  open  tcpwrapped
|_http-server-header: cloudflare
|_http-title: Did not follow redirect to https://skinport.com/
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
No OS matches for host
Network Distance: 1 hop

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.30 ms  104.18.17.19
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 66.71 seconds
```

Exploitation

- Sqlmap

Web applications with SQL injection vulnerabilities can be automatically found and exploited with SQLMap, an open-source penetration testing tool. It employs a number of detecting methods, supports a number of database management systems, and provides customization choices. Security experts and penetration testers find SQLMap useful as it automates testing, enumeration, data extraction, and reporting procedures during security assessments. It should, therefore, be utilized sensibly, morally, and with the appropriate authorization to test programs and systems.

Proof of concept:

```
(root@kali)~[~]
# sqlmap -u skinport.com

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
end user's responsibility to obey all applicable local, state and federal laws. Developers assume no liability
y and are not responsible for any misuse or damage caused by this program

[*] starting @ 15:49:50 /2024-04-22/

[15:49:51] [INFO] testing connection to the target URL
[15:49:51] [WARNING] potential permission problems detected ('Access denied')
[15:49:51] [WARNING] the web server responded with an HTTP error code (403) which could interfere with the res
ults of the tests
you have not declared cookie(s), while server wants to set its own ('__cf_bm=.DEKRe7f8um ... U_ic8q7w_w'). Do yo
u want to use those [Y/n] Y
[15:49:54] [INFO] checking if the target is protected by some kind of WAF/IPS
[15:49:54] [CRITICAL] WAF/IPS identified as 'CloudFlare'
[15:49:54] [INFO] testing if the target URL content is stable
[15:49:54] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page compar
ison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results,
refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] C
[15:50:00] [CRITICAL] no parameter(s) found for testing in the provided data (e.g. GET parameter 'id' in 'www.
site.com/index.php?id=1'). You are advised to rerun with '--crawl=2'
[15:50:00] [WARNING] HTTP error codes detected during run:
403 (Forbidden) - 3 times
[15:50:00] [WARNING] your sqlmap version is outdated

[*] ending @ 15:50:00 /2024-04-22/
```

Vulnerability analysis phase

I used tool like netsparker to process and catch bugs and vulnerabilities are based on OWASP top 10.

Targeted Domain: - <https://skinport.com>

- Netsparker

An automated web application security scanner known for its precision and extensive vulnerability finding capabilities is called Netsparker. It simplifies the procedure for examining online applications and finds many security flaws, such as SQL injection, XSS, and misconfigurations. With its ability to provide comprehensive reports for compliance audits and vulnerability monitoring, Netsparker seamlessly interacts with development workflows. Because of its intuitive interface, sophisticated features like support for continuous monitoring and authentication, and free support and upgrades, it's a great resource for security experts and companies looking to effectively strengthen their web application security posture.

Vulnerability title

- **Weak cipher enabled (confirmed).**

Vulnerability description

The "Weak Ciphers Enabled" vulnerability stems from the use of outdated or insecure cryptographic ciphers in SSL/TLS configurations, exposing systems to cryptographic attacks. Weak ciphers like DES, RC4, and MD5 lack the necessary security standards and are prone to exploitation. You should allow only strong ciphers on your web server to protect secure communication with your visitors.

Impact assessment

- Attackers might decrypt SSL traffic between your server and your visitors.

Affected components

When HTTP Strict Transport Security (HSTS) is not there, there are security vulnerabilities associated with different parts of a web application and its infrastructure. The web server configuration, network traffic, user sessions, data integrity while in transit, adherence to compliance standards, and user trust and experience are among the components that are impacted.

How to mitigate?

Some changes must be made to the system registry. Editing the registry incorrectly can cause serious damage to your system. Before making changes to the registry, you should back up any valuable data on your computer. Configure your web server to disallow the use of weak ciphers.

Proof of concept:

Weak Ciphers Enabled

CONFIRMED

MEDIUM

URL : <https://skinport.com/>

List of Supported Weak Ciphers :

```
TLS_RSA_WITH_AES_128_CBC_SHA (0x002F)
TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x003C)
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x003D)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA (0xC009)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA (0xC00A)
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 (0xC023)
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 (0xC024)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xC013)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xC014)
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xC027)
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xC028)
```



Other vulnerabilities were identified during the scan

- Content Security policy (CSP) Not Implemented

Content Security Policy (CSP) Not Implemented

BEST PRACTICE

URL : <https://skinport.com/cdn-cgi/styles/>

Vulnerability Details

CSP is an added layer of security that helps to mitigate mainly Cross-site Scripting attacks.

CSP can be enabled instructing the browser with a Content-Security-Policy directive in a response header;

Impact

There is no direct impact of not implementing CSP on your website. However, if your website is vulnerable to a Cross-site Scripting attack CSP can prevent successful exploitation of that vulnerability. By not implementing CSP you'll be missing out this extra layer of security.

Actions to Take

Enable CSP on your website by sending the Content-Security-Policy in HTTP response headers that instruct the browser to apply the policies you specified.

Apply the whitelist and policies as strict as possible.

Rescan your application to see if Netsparker identifies any weaknesses in your policies.

Remedy

Enable CSP on your website by sending the Content-Security-Policy in HTTP response headers that instruct the browser to apply the policies you specified.

- Expect-CT Not Enabled

Expect-CT Not Enabled

BEST PRACTICE

Certainty : 
URL : <https://skinport.com/cdn-cgi/>

Vulnerability Details

Netsparker identified that Expect-CT is not enabled.

Certificate Transparency is a technology that makes impossible (or at least very difficult) for a CA to issue an SSL certificate for a domain without the certificate being visible to the owner of that domain.

Google announced that, starting with April 2018, if it runs into a certificate that is not seen in Certificate Transparency (CT) Log, it will consider that certificate invalid and reject the connection. Thus sites should serve certificate that takes place in CT Logs. While handshaking, sites should serve a valid Signed Certificate Timestamp (SCT) along with the certificate itself.

Expect-CT can also be used for detecting the compatibility of the certificates that are issued before the April 2018 deadline. For instance, a certificate that was signed before April 2018, for 10 years it will be still posing a risk and can be ignored by the certificate transparency policy of the browser. By setting Expect-CT header, you can prevent misissued certificates to be used.

CLASSIFICATION

CWE	16
WASC	15
ISO27001	A.14.1.2

Remedy

Configure your web server to respond with Expect-CT header.

Expect-CT: enforce, max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"

Note: We strongly suggest you to use Expect-CT header in **report-only mode** first. If everything goes well and your certificate is ready, go with the Expect-CT enforce mode. To use **report-only mode** first, omit **enforce** flag and see the browser's behavior with your deployed certificate.

Expect-CT: max-age=7776000, report-uri="https://ABSOLUTE_REPORT_URL"

- Email Address Disclosure

Email Address Disclosure

INFORMATION

Certainty : [REDACTED]
URL : <https://skinport.com/static/main.ceb72ef4003400ce.js>
Email Address(es) : affiliate@skinport.com
hello@skinport.com
jobs@skinport.com
98577efcbca24e6daef4a099b6611076@o298045.ingest.sentry.io

Vulnerability Details

Netsparker identified an Email Address Disclosure.

Impact

Email addresses discovered within the application can be used by both spam email engines and also brute-force tools. Furthermore, valid email addresses may lead to social engineering attacks.

Remedy

Use generic email addresses such as contact@ or info@ for general communications and remove user/people-specific email addresses from the website; should this be required, use submission forms for this purpose.

• Web Application Firewall Detected

Web Application Firewall Detected

INFORMATION

Certainty : [REDACTED]
URL : [https://skinport.com/<script>alert\(0\)</script>](https://skinport.com/<script>alert(0)</script>)
WAF Name : [Cloudflare](#)
Parameter Name : URI-BASED
Parameter Type : Full URL
Attack Pattern : %3cscript%3ealert(0)%3c%2fscript%3e

Vulnerability Details

Netsparker detected that the target website is using a Web Application Firewall (WAF).

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.


CLASSIFICATION

OWASP PC [C7](#)
ISO27001 [A.18.1.3](#)

• Generic Email Address Disclosure

Generic Email Address Disclosure

INFORMATION

Certainty : 
URL : <https://skinport.com/static/main.ceb72ef4003400ce.js>
Email Address(es) : info@skinport.com
support@skinport.com

Vulnerability Details

Netsparker identified a Generic Email Address Disclosure.

Impact

Generic email addresses discovered within the application.

Remedy

This is reported for informational purposes only.

You can use submission forms for this purpose to avoid automated email address harvesting tools.


CLASSIFICATION

OWASP PC	C7
CWE	200
CAPEC	118
WASC	13
ISO27001	A.18.1.4

- ExpressJS Identified

ExpressJS Identified

INFORMATION

Certainty : 
URL : <https://skinport.com/.well-known/>

Vulnerability Details

Netsparker identified that the target website is using ExpressJS as its web application framework.

This issue is reported as extra information only.

Impact

This issue is reported as additional information only. There is no direct impact arising from this issue.

- Content Security policy (CSP) Contains Out of Scope report-Uri Domain

Content Security Policy (CSP) Contains Out of Scope report-uri Domain

INFORMATION

Certainty : ☐
URL : <https://skinport.com/>
Report Uri With Different Host : https://o298045.ingest.sentry.io/api/5193335/security/?sentry_key=98577efcbca24e6daef4a099b6611076

Vulnerability Details

Netsparker detected that your CSP declaration contains `report-uri` value that points to an out of scope external domain. This domain will be aware of the CSP violation occurs on your website and some sensitive data will be disclosed to this site.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
ISO27001	A.14.2.5

Remedy

If you trust this domain you can ignore this issue. However if you do not trust this external domain, remove it from `report-uri` directive.

• Referrer-Policy Not Implemented

Referrer-Policy Not Implemented

BEST PRACTICE

Certainty : ☐
URL : <https://skinport.com/cdn-cgi/styles/>

Vulnerability Details

Netsparker detected that no Referrer-Policy header implemented.
Referrer-Policy is a security header designed to prevent cross-domain Referer leakage.

CLASSIFICATION

OWASP 2013	A6
OWASP 2017	A3
CWE	200
ISO27001	A.14.2.5

Impact

Referer header is a request header that indicates the site which the traffic originated from. If there is no adequate prevention in place, the URL itself, and even sensitive information contained in the URL will be leaked to the cross-site.

The lack of Referrer-Policy header might affect privacy of the users and site's itself

Actions to Take

In a response header:

```
Referrer-Policy: no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading
```

In a META tag

```
<meta name="Referrer-Policy" value="no-referrer | same-origin"/>
```

In an element attribute

```
<a href="http://crosssite.example.com" rel="noreferrer"></a>
```

or

```
<a href="http://crosssite.example.com" referrerpolicy="no-referrer | same-origin | origin | strict-origin | no-origin-when-downgrading"></a>
```

Remedy

Please implement a Referrer-Policy by using the Referrer-Policy response header or by declaring it in the meta tags. It's also possible to control referrer information over an HTML-element by using the `rel` attribute.

Conclusion

The security posture of Skinport.com has been comprehensively assessed by MY evaluation, which has highlighted serious vulnerabilities like weak ciphers, non-implementation of the Content Security Policy (CSP), and email disclosure concerns.

According to these results, security measures must be prioritized to safeguard sensitive data and maintain user confidence.