Project

Web Application Security Assessment

Members:

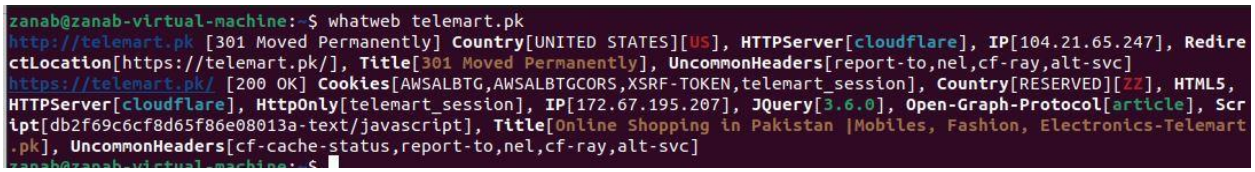
Muneeb Ur Rehman 21L-5424

Reconnaissance

Website 1

https://telemart.pk/

Command: whatweb (Getting information about target website)
-> whatweb telemart.pk



- **[301 Moved Permanently]:** This indicates that the URL has been permanently redirected to another location.
- **Country[UNITED STATES][US]:** The country where the server hosting the website is located.
- **HTTPServer[cloudflare]:** The web server software being used, in this case, Cloudflare.
- **IP[104.21.65.247]:** The IP address of the server hosting the website.
- **RedirectLocation[**https://telemart.pk/**]:** The new location to which the URL has been redirected.
- **Title[301 Moved Permanently]:** The title of the page returned by the server, indicating the HTTP status code.
- **UncommonHeaders[report-to,nel,cf-ray,alt-svc]:** Additional HTTP headers that are not commonly seen, such as reporting information, Network Error Logging (NEL), Cloudflare-specific headers, etc.

- **[200 OK]:** The HTTP status code indicating that the request was successful.
- **Cookies[AWSALBTG,AWSALBTGCORS,XSRF-TOKEN,telemart_session]:** Cookies set by the website, which may include session cookies and other tracking information.
- **Country[RESERVED][ZZ]:** Reserved or unspecified country code for the server location.
- **HTML5:** The version of HTML being used on the website.

- **HTTPServer[cloudflare]:** The web server software being used, in this case, Cloudflare.
- **HttpOnly[telemart_session]:** Indicates that the cookie is only accessible via HTTP and cannot be accessed by client-side scripts.
- **IP[172.67.195.207]:** The IP address of the server hosting the website.
- **JQuery[3.6.0]:** The version of jQuery being used on the website.
- **Open-Graph-Protocol[article]:** Indicates the use of Open Graph Protocol metadata, which can enhance the website's appearance when shared on social media platforms.
- **Script[db2f69c6cf8d65f86e08013a-text/javascript]:** A specific JavaScript script being loaded on the website.
- **Title[Online Shopping in Pakistan |Mobiles, Fashion, Electronics-Telemart.pk]:** The title of the webpage returned by the server.
- **UncommonHeaders[cf-cache-status,report-to,nel,cf-ray,alt-svc]:** Additional HTTP headers that are not commonly seen, such as cache status, reporting information, Network Error Logging (NEL), Cloudflare-specific headers, etc.

Getting technologies used: builtwith.com

- Analytics and Tracking
    - Alexa Certified Site Metrics
    - Cloudflare Rocket Loader
    - Facebook ConversionTracking
- Frameworks
    - PHP
    - Facebook Domain Verification
- Content Delivery Network
    - Cloud Front
    - Cloudflare
    - jsDelivr
    - CLoudflare JS
- JavaScript Libraries and Functions
    - JQuery
    - Facebook SDK
    - Bootstrap.js
    - Core-js
- Advertising
    - Bizo

- DoubleClick.Net

Website2

https://www.bigo.tv/

command: whatweb bigo.tv

1-

- http://bigo.tv**:** The URL of the website.
- **[301 Moved Permanently]:** The HTTP status code indicating that the URL has been permanently redirected.
- **Country[UNITED STATES][US]:** The country where the server hosting the website is located.
- **HTTPServer[nginx]:** The web server software being used, in this case, Nginx.
- **IP[169.136.79.151]:** The IP address of the server hosting the website.
- **RedirectLocation[**https://bigo.tv/**]:** The new location to which the URL has been redirected.
- **Title[301 Moved Permanently]:** The title of the page returned by the server, indicating the HTTP status code.
- **nginx:** Additional information confirming the use of the Nginx web server.

2-

- Similar to the previous section, but this time it shows the redirection from **https://bigo.tv/** to **https://www.bigo.tv/**.
- **Strict-Transport-Security[max-age=15768001]:** The Strict-Transport-Security header instructs browsers to access the website only over HTTPS for the specified duration (in seconds).

3-

- https://www.bigo.tv/**:** The URL of the website after redirection.
- **[200 OK]:** The HTTP status code indicating that the request was successful.
- **Country[UNITED STATES][US]:** The country where the server hosting the website is located.
- **Email[...]:** Email addresses associated with the website, likely for contact purposes.

- **Frame:** The website uses frames, a feature of HTML for displaying multiple web pages within a single window.
- **HTML5:** Indicates the use of HTML5 markup language.
- **HTTPServer[nginx]:** The web server software being used, in this case, Nginx.
- **IP[169.136.79.116]:** The IP address of the server hosting the website.
- **Open-Graph-Protocol[website]:** Indicates the presence of Open Graph Protocol metadata, which enhances the website's appearance when shared on social media platforms.
- **Script[application/ld+json]:** Indicates the presence of JSON-LD structured data, which provides additional context to search engines about the website's content.
- **Strict-Transport-Security[max-age=15768001]:** The Strict-Transport-Security header instructs browsers to access the website only over HTTPS for the specified duration (in seconds).
- **Title[BIGO LIVE - Live Stream, Live Games, Chat Rooms Online]:** The title of the webpage returned by the server.
- **X-Frame-Options[DENY]:** The X-Frame-Options header instructs browsers to prevent the website from being loaded in a frame or iframe on another site.
- **X-Powered-By[Express]:** Indicates that the website is powered by the Express framework.
- **nginx:** Additional information confirming the use of the Nginx web server.

Getting technologies used: builtwith.com

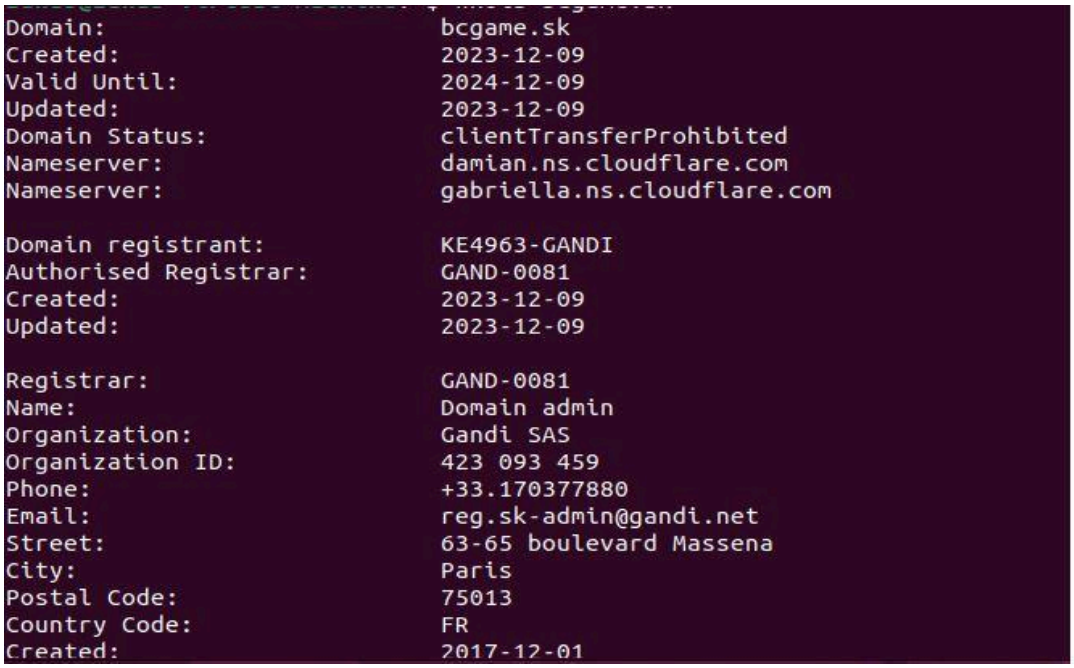
- Analytics and Tracking
    - WebTrends
    - Coremetrics
    - Mixpanel
- Frameworks
    - Nuxt.js
    - Express.js
- Languages
    - Arabic
    - German
    - English
    - Spanish
    - French
    - Hindi
    - Japanese

- Content Delivery Network
    - Cloud Front
    - Cloudflare
    - jsDelivr
    - CLoudflare JS
- JavaScript Libraries and Functions
    - JQuery
    - Sentry
    - CryptoJS
    - Core-js
    - Day.js
- Advertising
    - Facebook Custom Audiences
    - DoubleClick.Net
    - Bizo

Website3

https://bcgame.sk

command: whois bcgame.sk



```
Domain:                 bcgame.sk
Created:                2023-12-09
Valid Until:            2024-12-09
Updated:                2023-12-09
Domain Status:          clientTransferProhibited
Nameserver:             damian.ns.cloudflare.com
Nameserver:             gabriella.ns.cloudflare.com

Domain registrant:      KE4963-GANDI
Authorised Registrar:   GAND-0081
Created:                2023-12-09
Updated:                2023-12-09

Registrar:              GAND-0081
Name:                   Domain admin
Organization:           Gandi SAS
Organization ID:        423 093 459
Phone:                  +33.170377880
Email:                  reg.sk-admin@gandi.net
Street:                 63-65 boulevard Massena
City:                   Paris
Postal Code:            75013
Country Code:           FR
Created:                2017-12-01
```

Getting technologies used: builtwith.com

- Analytics and Tracking
  - Hotjar
  - Google Analytics
- Frameworks
  - Nuxt.js
  - Express.js
- Languages
  - Arabic
  - German
  - English
  - Spanish
  - French
  - Hindi
  - Japanese
- Content Dilevery Network
  - Cloudflare
  - GStatic Google Static Content

- JavaScript Libraries and Functions
    - JQuery
    - JSON3
    - React
    - Core-js
    - Socket.io
- Advertising
    - DoubleClick.Net
    - Bizo
    - AdMan Direct
    - Amazon Direct
    - AOL Direct

Website 4

https://24hours.pk

```
zanab@zanab-virtual-machine:~$ whatweb 24hours.pk
http://24hours.pk [301 Moved Permanently] Country[CANADA][CA], HTTPServer[cloudflare], IP[23.227.38.32], RedirectLocatio
n[https://24hours.pk/], UncommonHeaders[x-sorting-hat-podid,x-sorting-hat-shopid,x-storefront-renderer-rendered,x-redire
ct-reason,content-security-policy,x-shopid,x-shardid,powered-by,server-timing,x-dc,x-request-id,cf-cache-status,report-t
o,nel,x-content-type-options,x-permitted-cross-domain-policies,x-download-options,cf-ray,alt-svc], X-Frame-Options[DENY]
, X-XSS-Protection[1; mode=block]
https://24hours.pk/ [200 OK] Bootstrap, Content-Language[en], Cookies[_cmp_a,_landing_page,_orig_referrer,_shopify_s,_sh
opify_y,_tracking_consent,localization,secure_customer_sig], Country[CANADA][CA], Email[001_08adc0c1-eef8-4747-b8d7-f5d6
```

1-

- http://24hours.pk**:** The URL of the website.
- **[301 Moved Permanently]:** The HTTP status code indicating that the URL has been permanently redirected.
- **Country[CANADA][CA]:** The country where the server hosting the website is located.
- **HTTPServer[cloudflare]:** The web server software being used, in this case, Cloudflare.
- **IP[23.227.38.32]:** The IP address of the server hosting the website.
- **RedirectLocation[**https://24hours.pk/**]:** The new location to which the URL has been redirected.
- **UncommonHeaders[...]:** Various HTTP headers that are not commonly seen, including sorting hat-related headers, storefront rendering, cache status, reporting information, content type options, etc.
- **X-Frame-Options[DENY]:** The X-Frame-Options header instructs browsers to prevent the website from being loaded in a frame or iframe on another site.
- **X-XSS-Protection[1; mode=block]:** The X-XSS-Protection header enables the browser's Cross-Site Scripting (XSS) filter

2-

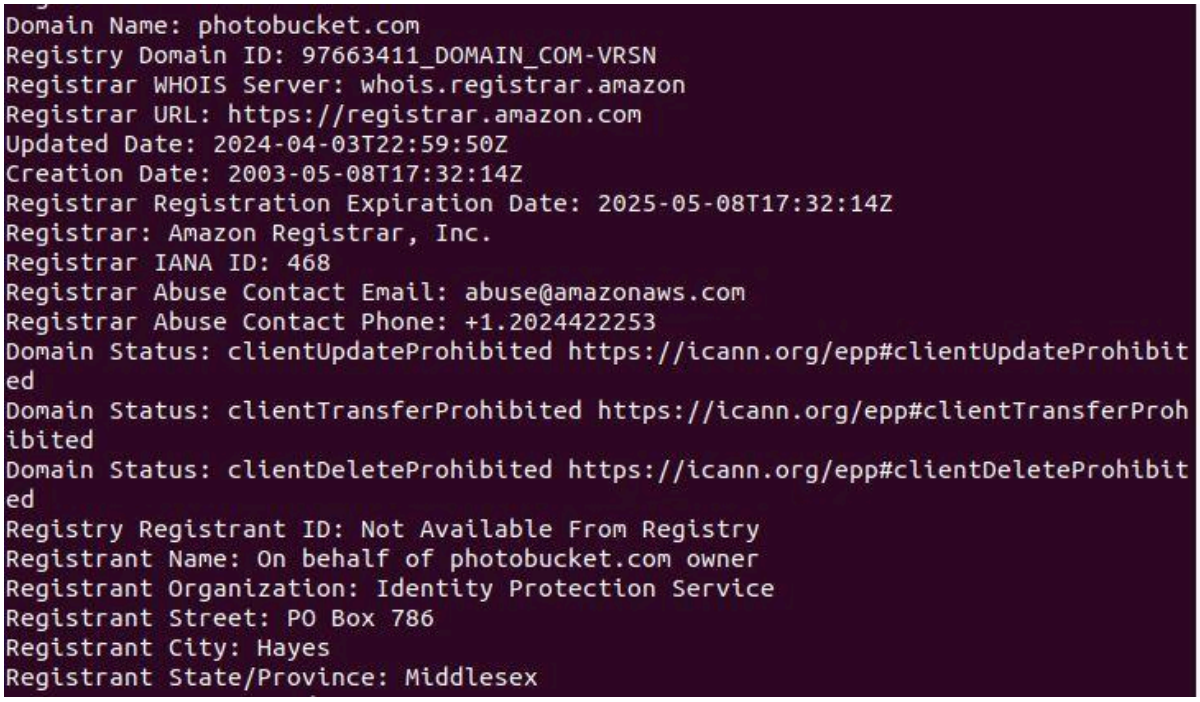
- https://24hours.pk/**:** The URL of the website after redirection.
- **[200 OK]:** The HTTP status code indicating that the request was successful.
- **Bootstrap:** Indicates the use of the Bootstrap framework for front-end development.
- **Content-Language[en]:** The language of the content on the website, in this case, English.
- **Cookies[...]:** Various cookies set by the website, likely for tracking and session management.
- **Country[CANADA][CA]:** The country where the server hosting the website is located.
- **Email[...]:** Email addresses associated with the website, possibly for contact purposes.

Getting technologies used: builtwith.com

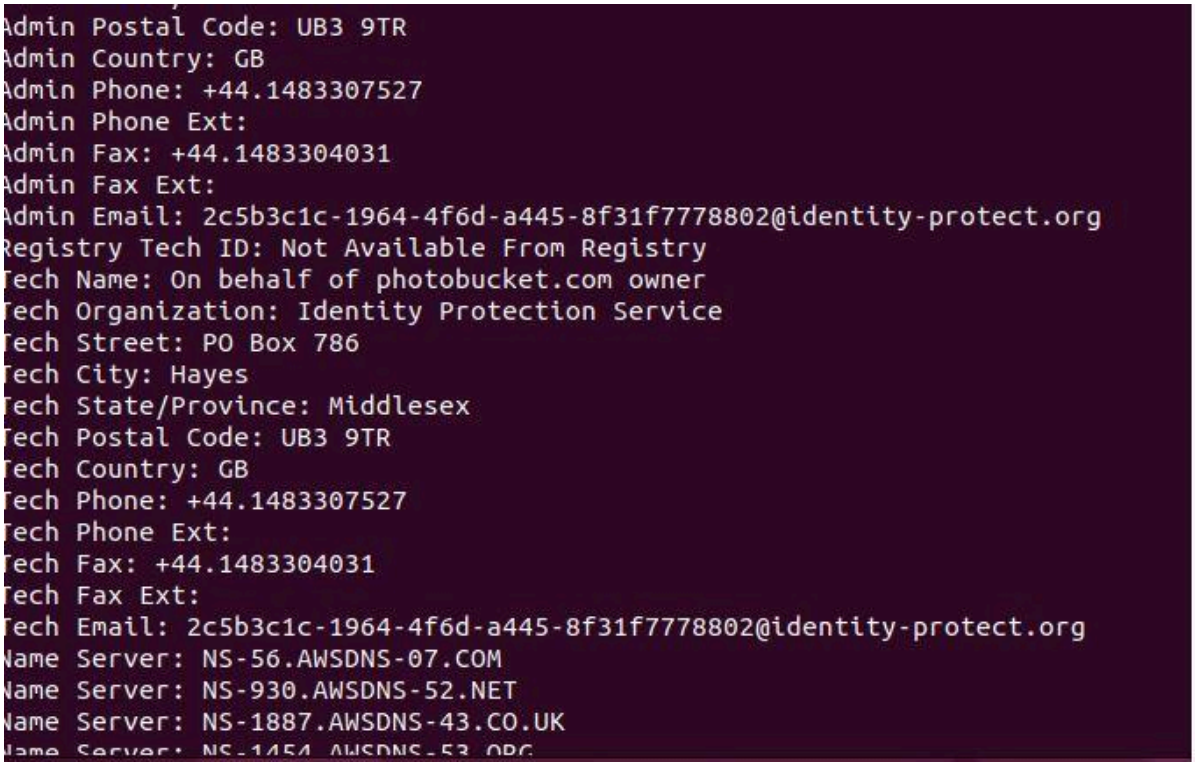
- Analytics and Tracking
    - WebTrends
    - Coremetrics
    - MIxpanel
- Frameworks
    - Organization Schema
- Content Delivery Network
    - Cloudflare
- JavaScript Libraries and Functions
    - JQuery
    - Modernizr
    - Facebook SDK
    - Core-js
    - JavaScript modules
- Advertising
    - Bizo
    - Facebook Custom Audiences

Website 5

https://www.photobucket.com



```
Domain Name: photobucket.com
Registry Domain ID: 97663411_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.registrar.amazon
Registrar URL: https://registrar.amazon.com
Updated Date: 2024-04-03T22:59:50Z
Creation Date: 2003-05-08T17:32:14Z
Registrar Registration Expiration Date: 2025-05-08T17:32:14Z
Registrar: Amazon Registrar, Inc.
Registrar IANA ID: 468
Registrar Abuse Contact Email: abuse@amazonaws.com
Registrar Abuse Contact Phone: +1.2024422253
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibit
ed
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProh
ibited
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibit
ed
Registry Registrant ID: Not Available From Registry
Registrant Name: On behalf of photobucket.com owner
Registrant Organization: Identity Protection Service
Registrant Street: PO Box 786
Registrant City: Hayes
Registrant State/Province: Middlesex
```



Getting technologies used: builtwith.com

- Analytics and Tracking
    - Raygun
- Frameworks
    - Organization Schema
- Document Encoding
    - UTF-8
- Document Standards
    - HTML5 DocType
    - Meta Description
    - Cascading Style Sheet
    - JavaScript