PENETRATION TEST DIGISIGNPLAY

Level : Expert
Time Taken : 1-2 days
Topic : NMAP, OWASP, OpenVAS, Information Gathering, Vulnerability, Cyber Security

---

1. NMAP Test

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
80	tcp	open	http	syn-ack			
443	tcp	open	https	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack			

Nmap 7.70 was initiated at Mon Aug 14 02:15:55 2023 with these arguments:

"nmap -v -oX=- --host-timeout=28800s -Pn -T4 -sT --webxml --max-retries=1 --open -p0-65355 apps.digisignplay.com"

Verbosity: 1; Debug level 0

Address : **43.218.69.157**
Hostname USER : **apps.digisignplay.com**
Hostname PTR : **ec2-43-218-69-157.ap-southeast-3.compute.amazonaws.com**

RESULTS :

1. The 65349 ports scanned but not shown below are in state : **FILTERED**
2. 65349 ports replied with : **no-responses**
3. The 4 ports scanned but not shown below are in state : **CLOSED**
4. 4 ports replied with : **conn-refused**

NOTE :

NMAP is short for Network Mapper. It is an open-source Linux command-line tool that is used to scan IP addresses and ports in a network and to detect installed applications.

Nmap allows network admins to find which devices are running on their network, discover open ports and services, and detect vulnerabilities.

2. OWASP ZAP Active

Risk Level	Number of Alerts
High	0
Medium	1
Low	0
Informational	1

Target All Scanned : **https://apps.digisignplay.com/login**
JavaScript included from : **https://unpkg.com &** **https://apps.digisignplay.com**
ZAP VERSION 2.12.0

METHOD GET

- https://apps.digisignplay.com/dist/style.bundle.min.js?rev&v=3.1.1
- https://apps.digisignplay.com/dist/style.bundle.min.js?rev=unavailable&v=3.1.1
- https://apps.digisignplay.com/dist/style.bundle.min.js?v=3.1.1&rev=unavailable
- https://apps.digisignplay.com/dist/vendor.bundle.min.js?rev&v=3.1.1
- https://apps.digisignplay.com/dist/vendor.bundle.min.js?rev=unavailable&v=3.1.1
- https://apps.digisignplay.com/dist/vendor.bundle.min.js?v=3.1.1&rev=unavailable

EVIDENCE FROM dist/vendor

.version="2.22.2",t=kt,r.fn=sn,r.min=function(){returnAt("isBefore",[].slice.call(arguments,0))},r.max=function(){return At("isAfter",[].slice.call(arguments,0))},r.now=function(){returnDate.now?Date.now():+newDate},r.utc=f,r.unix=function(e){return kt(1e3*e)},r.months=function(e,t){return un(e,t,"months")},r.isDate=c,r.locale=rt,r.invalid=_,r.duration=It,r.isMoment=

CONCLUSION :

WE WILL UPGRADE JQUERY SIMULTANEOUSLY WITH DIGISIGN PLAY CMS WITH PHP 8.2. NO WORRIES WITH JQUERY 3.1.1, YOUR DATA STILL SAFE WITH AWS ENCRYPTION. (see digisignPlay Architecture picture)

WHAT IS OWASP?

The Open Web Application Security Project (OWASP) is a worldwide not-for-profit organization focused on improving the security of software systems. OWASP's mission is to make software security visible, so that individuals and organizations worldwide can make informed decisions about software security risks.

CONFIGURATION SECURITY DIGISIGN PLAY

```
568   # Security Web added by rio@innograph.com
569
570   Header set X-XSS-Protection "1; mode=block"
571   Header always append X-Frame-Options SAMEORIGIN
572   Header set X-Content-Type-Options nosniff
573   Header edit Set-Cookie ^(.*)$ $1;HttpOnly;Secure;SameSite=Strict
574   Header always set Strict-Transport-Security "max-age=63072000; includeSubDomains"
575   ServerSignature Off
576   ServerTokens Prod
577   Header add Content-Security-Policy "default-src 'self';"
```

path : C:\xampp\apache\conf\httpd.ini

- **LINE 570 :**
  HTTP X-XSS-Protection response header is a feature of Internet Explorer, Chrome and Safari that stops pages from loading when they detect reflected cross-site scripting (XSS) attacks.

- **LINE 571 :**
  X-Frame-Options HTTP response header can be used to indicate whether or not a browser should be allowed to render a page in a <frame> , <iframe> , <embed> or <object> . Sites can use this to avoid click-jacking attacks, by ensuring that their content is not embedded into other sites.

- **LINE 572 :**
  The Anti-MIME-Sniffing header X-Content-Type-Options was not set to 'nosniff'. This allows older versions of Internet Explorer and Chrome to perform MIME-sniffing on the response body, potentially causing the response body to be interpreted and displayed as a content type other than the declared content type. Current (early 2014) and legacy versions of Firefox will use the declared content type (if one is set), rather than performing MIME-sniffing.

- **LINE 573 :**
  If a cookie has been set without the secure flag, which means that the cookie can be accessed via unencrypted connections.

- **LINE 574 :**
  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 (i.e. HTTP layered over TLS/SSL). HSTS is an IETF standards track protocol and is specified in RFC 6797.

- **LINE 575 & 576:**
  The web/application server is leaking version information via the "Server" HTTP response header. Access to such information may facilitate attackers identifying other vulnerabilities your web/application server is subject to.

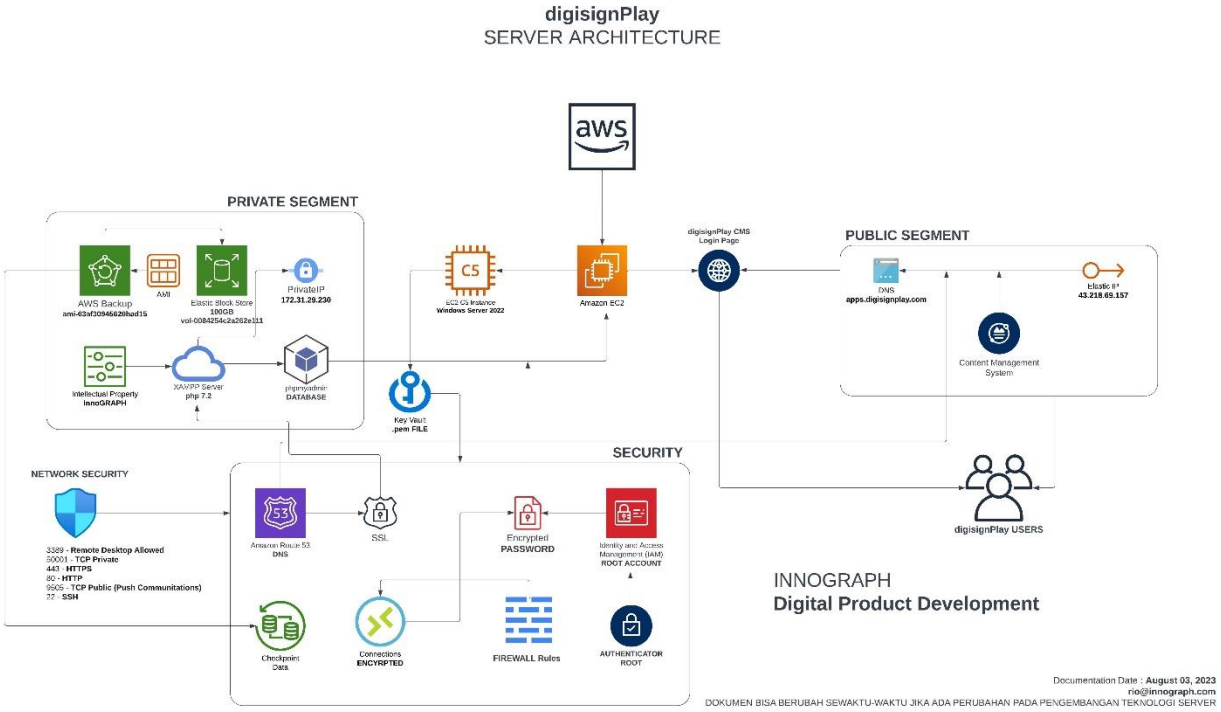
- **LINE 577 :**
  Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks. These attacks are used for everything from data theft to site defacement or distribution of malware. CSP provides a set of standard HTTP headers that allow website owners to declare approved sources of content that browsers should be allowed to load on that page — covered types are JavaScript, CSS, HTML frames, fonts, images and embeddable objects such as Java applets, ActiveX, audio and video files.

```
370    ; http://php.net/expose-php
371    ; Security Web added by rio@innograph.com
372    expose_php=Off
```

path : C:\xampp\php\php.ini

- **LINE 372 :**
  The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.

DIGISIGNPLAY ARCHITECTURE



PENETRATION TEST DATE : August 14-15, 2023
RESPONSIBLE : Rio Saroha Simamora
Cyber Security Certified List : https://linuxenic.com/mycert
Cyber Security Portfolio : https://tryhackme.com/p/linuxenic