nemasis

Nemasis DA Report (OWASP 2017)

http://php.testsparker.com/process.php

Result Overview:

A6 Security Misconfiguration

X-Frame-Options Header Not Set

Description:
X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.

Solution:
Most modern Web browsers support the X-Frame-Options HTTP header. Ensure it's set on all web pages returned by your site (if you expect the page to be framed only by pages on your server (e.g. it's part of a FRAMESET) then you'll want to use SAMEORIGIN, otherwise if you never expect the page to be framed, you should use DENY. ALLOW-FROM allows specific websites to frame the web page in supported web browsers).

References:
http://blogs.msdn.com/b/ieinternals/archive/2010/03/30/combating-clickjacking-with-x-frame-options.aspx

Url	Parameter	Evidence
/?file=Generics/index.nsp	X-Frame-Options	
/?file=Generics/contact.nsp	X-Frame-Options	
/?file=Generics/about.nsp	X-Frame-Options	
/	X-Frame-Options	

X-Content-Type-Options Header Missing

Description:
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.

Solution:
Ensure that the application/web server sets the Content-Type header appropriately, and that it sets the X-Content-Type-Options header to 'nosniff' for all web pages. If possible, ensure that the end user uses a standards-compliant and modern web browser that does not perform MIME-sniffing at all, or that can be directed by the web application/web server to not perform MIME-sniffing.

References:
http://msdn.microsoft.com/en-us/library/ie/gg622941%28v=vs.85%29.aspx
https://www.owasp.org/index.php/List_of_useful_HTTP_headers

Url	Parameter	Evidence
/?file=Generics/index.nsp	X-Content-Type-Options	
/?file=Generics/contact.nsp	X-Content-Type-Options	
/	X-Content-Type-Options	
/?file=Generics/about.nsp	X-Content-Type-Options	

Content Security Policy (CSP) Header Not Set

Description:
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.

Solution:
Ensure that your web server, application server, load balancer, etc. is configured to set the Content-Security-Policy header, to achieve optimal browser support: "Content-Security-Policy" for Chrome 25+, Firefox 23+ and Safari 7+, "X-Content-Security-Policy" for Firefox 4.0+ and Internet Explorer 10+, and "X-WebKit-CSP" for Chrome 14+ and Safari 6+.

References:
https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy
https://www.owasp.org/index.php/Content_Security_Policy
http://www.w3.org/TR/CSP/
http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html
http://www.html5rocks.com/en/tutorials/security/content-security-policy/
http://caniuse.com/#feat=contentsecuritypolicy
http://content-security-policy.com/

Url	Parameter	Evidence
/?file=Generics/index.nsp		
/		
/?file=Generics/contact.nsp		

/?file=Generics/about.nsp