					reconnaissance	Exploit			
area	**CPE**	**CVE**	**CVSS V2**	**Tool**	**Team Meml**	**target**	**exploit tried b**	**Exploitable**	**Comments**
		e.g. CVE-2020-1938		*e.g. Nessus*	*e.g. Freya*	*/app.php OR index.php*			*e.g. AWS firewall appears to drop this traffic.*
SQL injection		CWE-89	NA	SQLMAP	Jan	/add	Jan	No	No AWS firewall, however SQLi not possible
SQL injection		CWE-89	NA		Jan	CGI			no idea how to do that
CGI Generic Path Traversal		CWE-22	6.4	Nessus	Jan	CGI			no idea how to do that
jQuery 1.8.3	cpe:2.3:a:jquer	CVE-2020-7656	4.3	visual code i	Jan	main, ac	Jan	No	to exploit this the "load" method must be used, which isn't on this website
jQuery 1.8.3	cpe:2.3:a:jquer	CVE-2020-11022	4.3	visual code i	Jan	main, ac	Jan	No	the page doesn't load html from other sources, where we can inject our XSS
jQuery 1.8.3	cpe:2.3:a:jquer	CVE-2020-11023	4.3	visual code i	Jan	main, ac	Jan	No	the page doesn't load html from other sources, where we can inject our XSS
jQuery 1.8.3	cpe:2.3:a:jquer	CVE-2019-11358	4.3	visual code i	Jan	main, ac	Jan	No	to exploit this the "extend" method must be used, which isn't on this website
jQuery 1.8.3	cpe:2.3:a:jquer	CVE-2015-9251	4.3	visual code i	Jan	main, ac	Jan	No	no cross domain ajax requests are conducted, which are necessary to ecploit this
jQuery 1.8.3	cpe:2.3:a:jquer	CVE-2012-6708	4.3	visual code i	Jan	main, ac	Jan	No	likely prohibted by twig
OpenSSH 7.4	cpe:2.3:a:open	CVE - 2008-5161	NA	Nessus	Jan	NA	Jan	potentially	can be exploited, if there is traffic, you can sniff
OpenSSH 7.4	cpe:2.3:a:open	CVE-2020-15778	6.8	nmap + nvd	Jan	NA	Jan	No	can be exploited with SSH credentials or MITM, both very unlikely since SSH
OpenSSH 7.4	cpe:2.3:a:open	CVE-2020-14145	5.9	nmap + nvd	Jan	NA	Jan	potentially	can be exploited if you are in the same LAN as the victim.
OpenSSH 7.4	cpe:2.3:a:open	CVE-2019-6111	5.9	nmap + nvd	Jan	NA	Jan	No	can be exploited with SSH credentials or MITM, both very unlikely since SSH
OpenSSH 7.4	cpe:2.3:a:open	CVE-2019-6110	6.8	nmap + nvd	Jan	NA	Jan	No	can be exploited with SSH credentials or MITM, both very unlikely since SSH
OpenSSH 7.4	cpe:2.3:a:open	CVE-2019-6109	6.8	nmap + nvd	Jan	NA	Jan	No	MITM only, so you need to be in the same WLAN like the server. WLAN is AWS cloud,
OpenSSH 7.4	cpe:2.3:a:open	CVE-2018-20685	5.3	nmap + nvd	Jan	NA	Jan	No	can be exploited with SSH credentials or MITM, both very unlikely since SSH
OpenSSH 7.4	cpe:2.3:a:open	CVE-2018-15919	5.3	nmap + nvd	Jan	NA	Jan	No	since there are no usernames set up you can't guess them
OpenSSH 7.4	cpe:2.3:a:open	CVE-2018-15473	5.3	nmap + nvd	Jan	NA	Jan	No	since there are no usernames set up you can't guess them
OpenSSH 7.4	cpe:2.3:a:open	CVE-2017-15906	5.3	nmap + nvd	Jan	NA	Jan	No	can be exploited with SSH credentials or MITM, both very unlikely since SSH
OpenSSH 7.4	cpe:2.3:a:open	CVE-2008-3844	9.3	nmap + nvd	Jan	NA	Jan	No	not within our control at all and very unlikely that this happen to AWS
OpenSSH 7.4	cpe:2.3:a:open	CVE-2007-2768	4.3	nmap + nvd	Jan	NA	Jan	No	no OPIE used. can't be exploited
.DS_Store on server		CVE-2001-1446	5	Nessus	Jan	NA	Jan	Kinda	a DS_Store file is created by Apple PCs. It should not be on a server, but this happens
Clickjacking		CWE: 693	4.3	Nessus	Jan	NA	Jan	likely	
PHP 7.3	cpe:2.3:a:php	CVE-2021-21702	5	white box +	Jan	NA	Jan	No	no SOAP extensions are used in the app currently
PHP 7.3	cpe:2.3:a:php	CVE-2020-7071	5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2020-7070	5	white box +	Jan	NA	Jan	No	site doesn't use cookies currently, so exploit won't work
PHP 7.3	cpe:2.3:a:php	CVE-2020-7069	6.4	white box +	Jan	NA	Jan	No	decreasing AES-CCM isn't possible, since the site isn't encrypted at all (LOL)
PHP 7.3	cpe:2.3:a:php	CVE-2020-7068	3.3	white box +	Jan	NA	Jan	No	No phar files used
PHP 7.3	cpe:2.3:a:php	CVE-2019-11048	5	white box +	Jan	NA	Jan	No	no file upload possible currently
PHP 7.3	cpe:2.3:a:php	CVE-2020-7067	5	white box +	Jan	NA	Jan	No	vulnerable functions not used
PHP 7.3	cpe:2.3:a:php	CVE-2020-7066	4.3	white box +	Jan	NA	Jan	No	vulnerable function not used
PHP 7.3	cpe:2.3:a:php	CVE-2020-7065	6.8	white box +	Jan	NA	Jan	No	vulnerable function not used
PHP 7.3	cpe:2.3:a:php	CVE-2020-7064	5.8	white box +	Jan	NA	Jan	No	no parsing of EXIF data
PHP 7.3	cpe:2.3:a:php	CVE-2020-7063	5	white box +	Jan	NA	Jan	No	no creation of PHAR archives
PHP 7.3	cpe:2.3:a:php	CVE-2020-7062	4.3	white box +	Jan	NA	Jan	No	no file upload possible currently
PHP 7.3	cpe:2.3:a:php	CVE-2020-7061	6.4	white box +	Jan	NA	Jan	No	No phar files used
PHP 7.3	cpe:2.3:a:php	CVE-2020-7060	6.4	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2020-7059	6.4	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2019-11050	6.4	white box +	Jan	NA	Jan	No	no parsing of EXIF data
PHP 7.3	cpe:2.3:a:php	CVE-2019-11049	7.5	white box +	Jan	NA	Jan	No	server not installed on Windows
PHP 7.3	cpe:2.3:a:php	CVE-2019-11047	6.4	white box +	Jan	NA	Jan	No	server not installed on Windows
PHP 7.3	cpe:2.3:a:php	CVE-2019-11046	5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2019-11045	4.3	white box +	Jan	NA	Jan	No	DirectoryIterator class not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2019-11044	5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2019-19246	5	white box +	Jan	NA	Jan	No	Oniguruma not used in the web app
PHP 7.3	cpe:2.3:a:php	CVE-2019-11043	7.5	white box +	Jan	NA	Jan	No	no FPM module used
PHP 7.3	cpe:2.3:a:php	CVE-2019-11042	5.8	white box +	Jan	NA	Jan	No	no FPM setup used
PHP 7.3	cpe:2.3:a:php	CVE-2019-11041	5.8	white box +	Jan	NA	Jan	No	no parsing of EXIF data

PHP 7.3	cpe:2.3:a:php	CVE-2019-11040	6.4	white box +	Jan	NA	Jan	No	no parsing of EXIF data
PHP 7.3	cpe:2.3:a:php	CVE-2019-11039	6.4	white box +	Jan	NA	Jan	No	no parsing of MIME headers
PHP 7.3	cpe:2.3:a:php	CVE-2019-11038	5	white box +	Jan	NA	Jan	No	no GD praphics library used
PHP 7.3	cpe:2.3:a:php	CVE-2019-11036	6.4	white box +	Jan	NA	Jan	No	no parsing of EXIF data
PHP 7.3	cpe:2.3:a:php	CVE-2019-11035	6.4	white box +	Jan	NA	Jan	No	no parsing of EXIF data
PHP 7.3	cpe:2.3:a:php	CVE-2019-11034	6.4	white box +	Jan	NA	Jan	No	no parsing of EXIF data
PHP 7.3	cpe:2.3:a:php	CVE-2019-9675	6.8	white box +	Jan	NA	Jan	No	element in dispute not even used at all
PHP 7.3	cpe:2.3:a:php	CVE-2019-9641	7.5	white box +	Jan	NA	Jan	No	no parsing of EXIF data
PHP 7.3	cpe:2.3:a:php	CVE-2019-9640	5	white box +	Jan	NA	Jan	No	no parsing of EXIF data
PHP 7.3	cpe:2.3:a:php	CVE-2019-9639	5	white box +	Jan	NA	Jan	No	no parsing of EXIF data
PHP 7.3	cpe:2.3:a:php	CVE-2019-9638	5	white box +	Jan	NA	Jan	No	no parsing of EXIF data
PHP 7.3	cpe:2.3:a:php	CVE-2019-9637	5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2019-9025	7.5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2019-9024	5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2019-9023	7.5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2019-9022	5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2019-9021	7.5	white box +	Jan	NA	Jan	No	no handling of PHAR archives
PHP 7.3	cpe:2.3:a:php	CVE-2019-9020	7.5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2019-6977	6.8	white box +	Jan	NA	Jan	No	GD Graphics Library not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2013-2220	7.5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
PHP 7.3	cpe:2.3:a:php	CVE-2007-3205	5	white box +	Jan	NA	Jan	No	vulnerable function not used currently
Bootstrap v.2.2.2	cpe:2.3:a:getb	CVE-2019-8331	4.3	visual code i	Jan	NA	Jan	No	no tooltip or popover data-template used currently
Bootstrap v.2.2.2	cpe:2.3:a:getb	CVE-2018-20677	4.3	visual code i	Jan	NA	Jan	No	affix property not used currently
Bootstrap v.2.2.2	cpe:2.3:a:getb	CVE-2018-20676	4.3	visual code i	Jan	NA	Jan	No	no tooltip data-viewport attribute used currently
Bootstrap v.2.2.2	cpe:2.3:a:getb	CVE-2018-14042	4.3	visual code i	Jan	NA	Jan	No	no tooltips used currently
Bootstrap v.2.2.2	cpe:2.3:a:getb	CVE-2018-14040	4.3	visual code i	Jan	NA	Jan	No	collapse data-parent attribute not used currently
twig 2.0 https://github.com	cpe:2.3:a:sym	https://nvd.nist.gov/vuln/de	4.3	Github + NV	Jan	NA	Jan	No	functions not used
twig 2.0 https://github.com	cpe:2.3:a:sym	https://nvd.nist.gov/vuln/de	9.8	Github + NV	Jan	NA	Jan	No	exploit blocked by code sanitization probably. https://www.exploit-db.com/exploits/44102