internship
studio

ETHICAL HACKING INTERNSHIP

Name: Kartik Muley

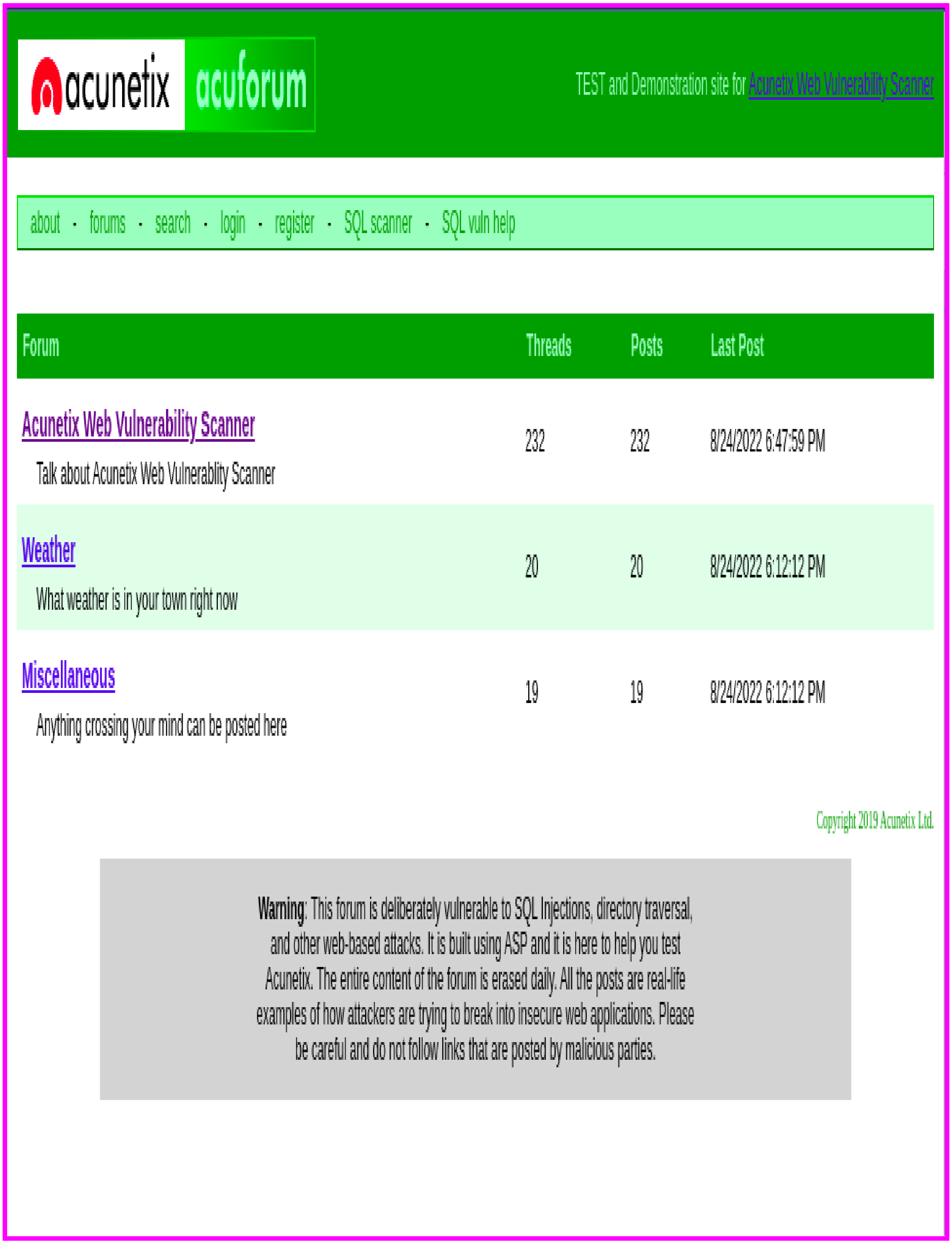
Institutional Affiliation: Internship Studio

Email: kartikmuley28@gmail.com

Task : 3

Explore the website and try to find vulnerabilities in it

http://testasp.vulnweb.com/



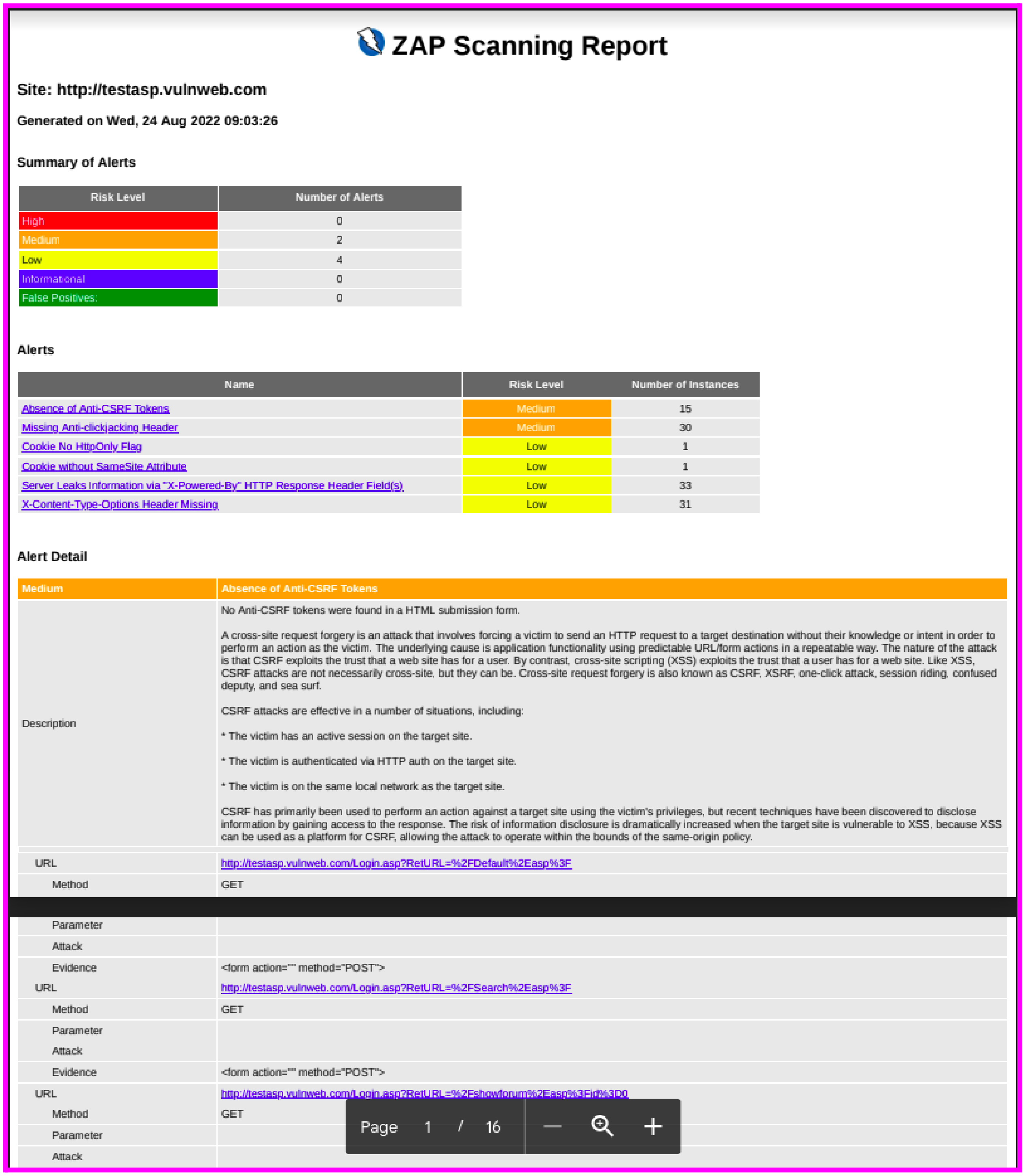
TEST and Demonstration site for Acunetix Web Vulnerability Scanner

about · forums · search · login · register · SQL scanner · SQL vuln help

Forum	Threads	Posts	Last Post
Acunetix Web Vulnerability Scanner Talk about Acunetix Web Vulnerablity Scanner	232	232	8/24/2022 6:47:59 PM
Weather What weather is in your town right now	20	20	8/24/2022 6:12:12 PM
Miscellaneous Anything crossing your mind can be posted here	19	19	8/24/2022 6:12:12 PM

Copyright 2019 Acunetix Ltd.

Warning: This forum is deliberately vulnerable to SQL Injections, directory traversal, and other web-based attacks. It is built using ASP and it is here to help you test Acunetix. The entire content of the forum is erased daily. All the posts are real-life examples of how attackers are trying to break into insecure web applications. Please be careful and do not follow links that are posted by malicious parties.



ZAP Scanning Report

Site: http://testasp.vulnweb.com

Generated on Wed, 24 Aug 2022 09:03:26

Summary of Alerts

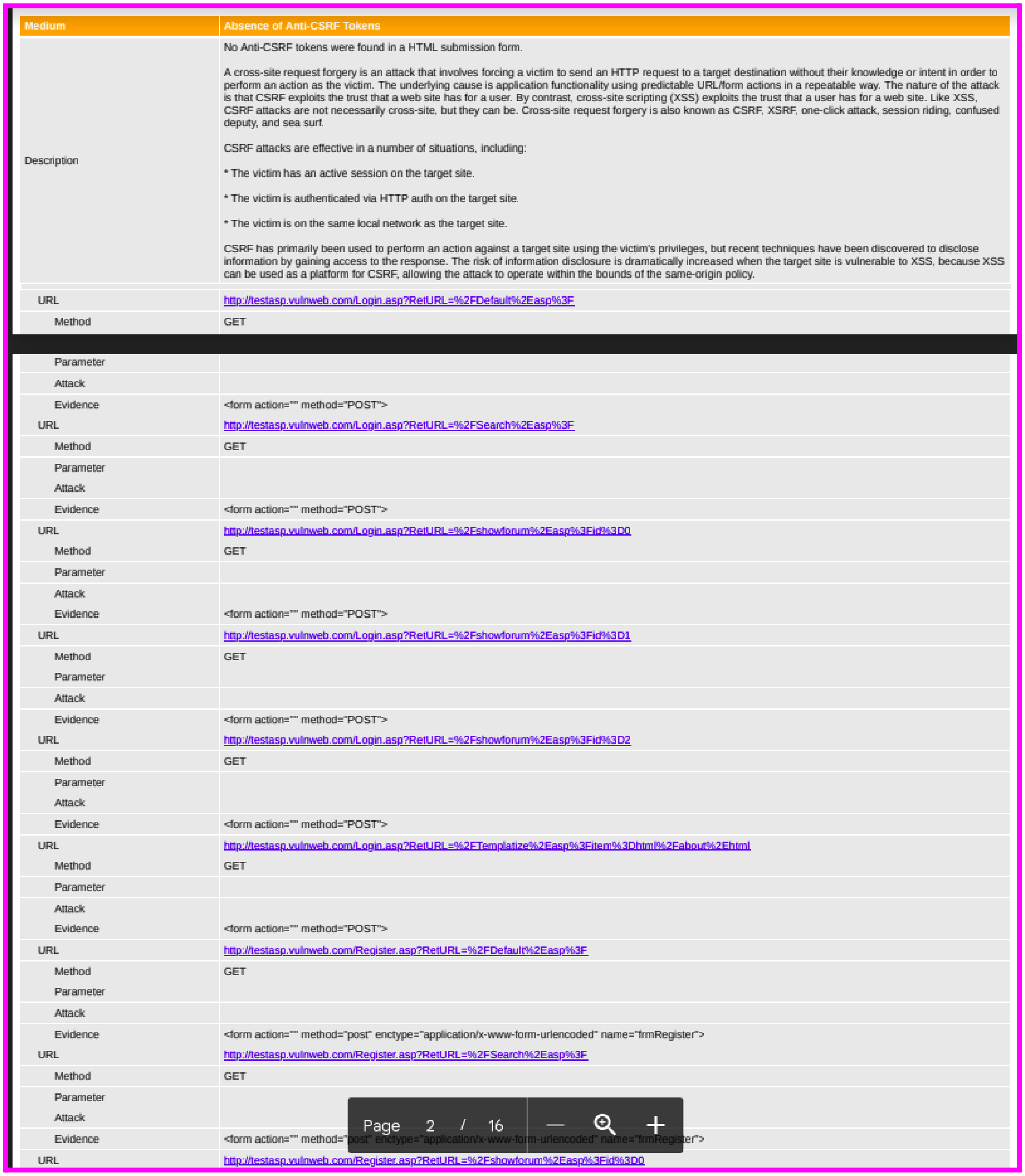
Risk Level	Number of Alerts
High	0
Medium	2
Low	4
Informational	0
False Positives:	0

Alerts

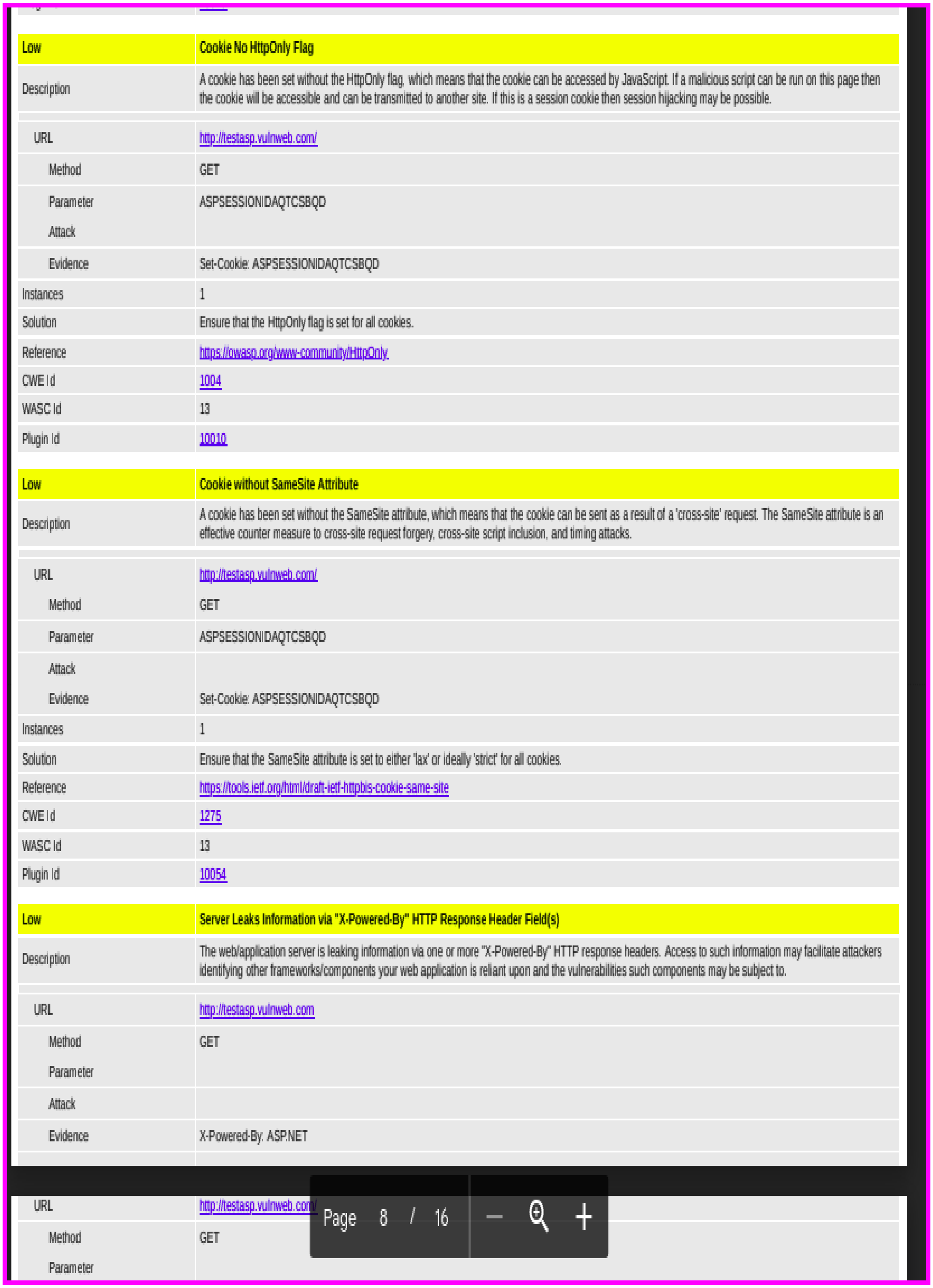
Name	Risk Level	Number of Instances
Absence of Anti-CSRF Tokens	Medium	15
Missing Anti-clickjacking Header	Medium	30
Cookie No HttpOnly Flag	Low	1
Cookie without SameSite Attribute	Low	1
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	33
X-Content-Type-Options Header Missing	Low	31

Alert Detail

Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="POST">
URL	http://testasp.vulnweb.com/Login.asp?RetURL=%2FSearch%2Easp%3F
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="POST">
URL	http://testasp.vulnweb.com/Login.asp?RetURL=%2Fshowforum%2Easp%3Fid%3D0
Method	GET
Parameter	
Attack	



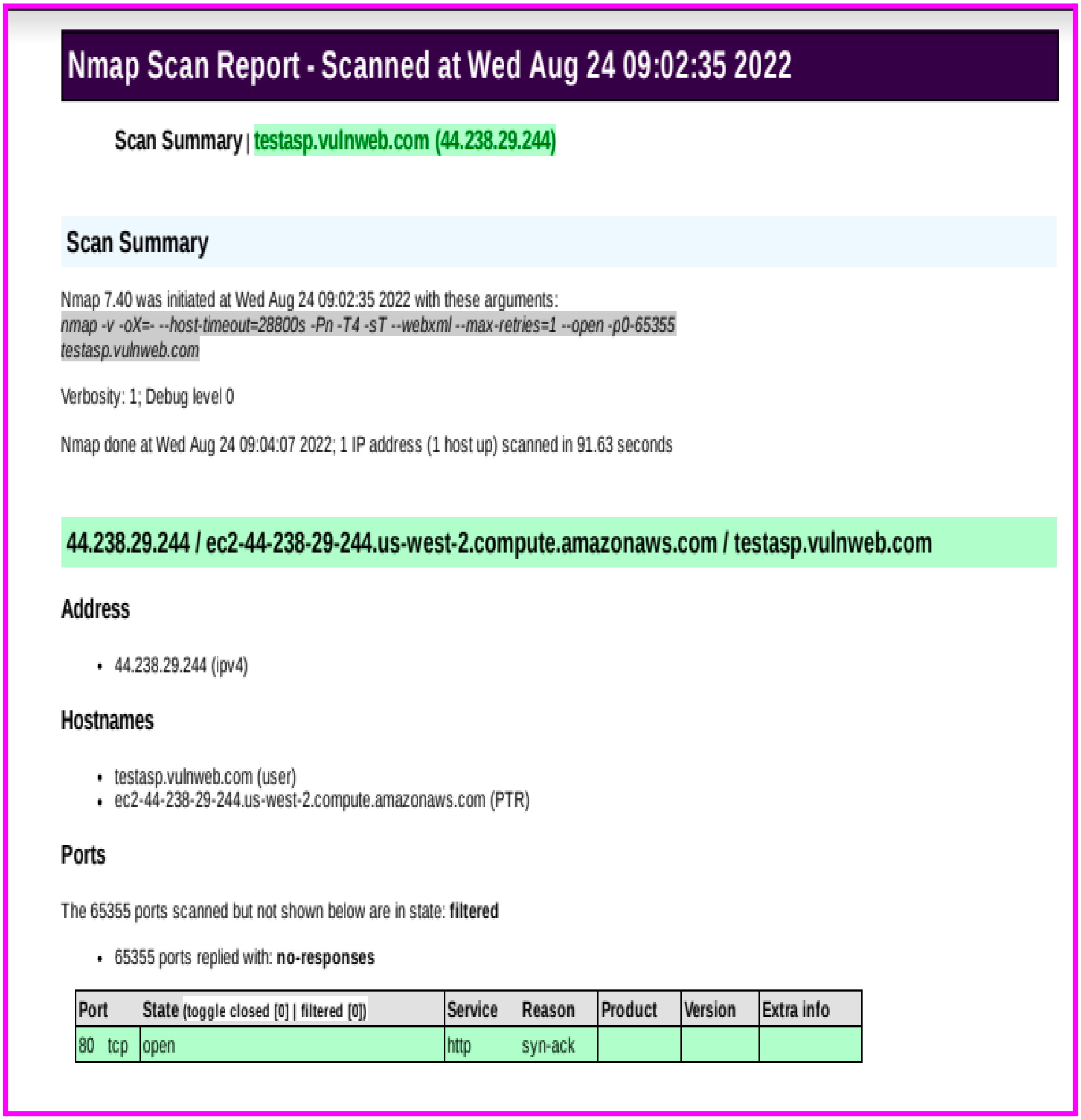
Medium	Absence of Anti-CSRF Tokens
Description	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://testasp.vulnweb.com/Login.asp?RetURL=%2FDefault%2Easp%3F
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="POST">
URL	http://testasp.vulnweb.com/Login.asp?RetURL=%2FSearch%2Easp%3F
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="POST">
URL	http://testasp.vulnweb.com/Login.asp?RetURL=%2Fshowforum%2Easp%3Fid%3D0
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="POST">
URL	http://testasp.vulnweb.com/Login.asp?RetURL=%2Fshowforum%2Easp%3Fid%3D1
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="POST">
URL	http://testasp.vulnweb.com/Login.asp?RetURL=%2Fshowforum%2Easp%3Fid%3D2
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="POST">
URL	http://testasp.vulnweb.com/Login.asp?RetURL=%2FTemplatize%2Easp%3Fitem%3Dhtml%2Fabout%2Ehtml
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="POST">
URL	http://testasp.vulnweb.com/Register.asp?RetURL=%2FDefault%2Easp%3F
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="post" enctype="application/x-www-form-urlencoded" name="frmRegister">
URL	http://testasp.vulnweb.com/Register.asp?RetURL=%2FSearch%2Easp%3F
Method	GET
Parameter	
Attack	
Evidence	<form action="" method="post" enctype="application/x-www-form-urlencoded" name="frmRegister">
URL	http://testasp.vulnweb.com/Register.asp?RetURL=%2Fshowforum%2Easp%3Fid%3D0



Low	Cookie No HttpOnly Flag
Description	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible.
URL	http://testasp.vulnweb.com/
Method	GET
Parameter	ASPSESSIONIDAQTCSBQD
Attack	
Evidence	Set-Cookie: ASPSESSIONIDAQTCSBQD
Instances	1
Solution	Ensure that the HttpOnly flag is set for all cookies.
Reference	https://owasp.org/www-community/HttpOnly
CWE Id	1004
WASC Id	13
Plugin Id	10010

Low	Cookie without SameSite Attribute
Description	A cookie has been set without the SameSite attribute, which means that the cookie can be sent as a result of a 'cross-site' request. The SameSite attribute is an effective counter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
URL	http://testasp.vulnweb.com/
Method	GET
Parameter	ASPSESSIONIDAQTCSBQD
Attack	
Evidence	Set-Cookie: ASPSESSIONIDAQTCSBQD
Instances	1
Solution	Ensure that the SameSite attribute is set to either 'lax' or ideally 'strict' for all cookies.
Reference	https://tools.ietf.org/html/draft-ietf-httpbis-cookie-same-site
CWE Id	1275
WASC Id	13
Plugin Id	10054

Low	Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)
Description	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.
URL	http://testasp.vulnweb.com
Method	GET
Parameter	
Attack	
Evidence	X-Powered-By: ASP.NET
URL	http://testasp.vulnweb.com/
Method	GET
Parameter	



Nmap Scan Report - Scanned at Wed Aug 24 09:02:35 2022

Scan Summary | testasp.vulnweb.com (44.238.29.244)

Scan Summary

Nmap 7.40 was initiated at Wed Aug 24 09:02:35 2022 with these arguments:
nmap -v -oX=- --host-timeout=28800s -Pn -T4 -sT --webxml --max-retries=1 --open -p0-65355 testasp.vulnweb.com

Verbosity: 1; Debug level 0

Nmap done at Wed Aug 24 09:04:07 2022; 1 IP address (1 host up) scanned in 91.63 seconds

44.238.29.244 / ec2-44-238-29-244.us-west-2.compute.amazonaws.com / testasp.vulnweb.com

Address

- 44.238.29.244 (ipv4)

Hostnames

- testasp.vulnweb.com (user)
- ec2-44-238-29-244.us-west-2.compute.amazonaws.com (PTR)

Ports

The 65355 ports scanned but not shown below are in state: **filtered**

- 65355 ports replied with: **no-responses**

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