Page:

	VAPT LAB ASSIGNMENT
	6 05 25
	AVIOLE
	Company Name: Acme Retail Corp.
	2) not pries per enots
	Infrastructure: 3 web-apps
	Internal network with 25 systems
	Cloud-hosted assets on Aws
	2 mobile apps (android 2 103)
	VIN access for memote employees
	and rates of aread took artest of
	Business Priority: data security of customer transaction
	protect PII
	maintain 24 7 optime
	sovip to anni si more off some
1.	Scope of the state of
	a) Assets covered in VA;
	o all web-apps
	o Internal Intrastructure systems
	· cloud-hosted assets
	· both mobile apps
	· APLS
	b) Assets covered in 17:
	o same as above
	1912019 (8)
	c) OUT OF SCOPE
	a Testing VIN access which is
	there for external exmit employees
	o personal devices
	o social engineering

Page:
Date:

A Chia			
٥.	Tools FLATINGS DA DAS 19AV		
	6 08 08		
	5 For VA:		
	VA is mostly an automated process,		
	done by using tools		
	estate donn e loved undendal		
35	1 OWASP ZAP for web-apps		
	2 H & Have balond high		
	Fond Pros		
454	· easy to use		
	es tester just have to enter the		
	URL and it will automate the		
	scans		
	o teport-generation		
	s onces the scan is done, it gives		
	the choice to generate a sand	1	
	complete report		
	o Accurate results		
	it provides proof and palyonds for		
	all the alerts generated p		
	very less false positive		
	0194 *		
	2) 33 Scanner: for cloud assets on Aws		
	grado en amazo		
	3 Nuclei		
	les: 31,000 10 100 6		
3	· extremely tost scanning;		
220yeld	uses parallel scan		
	restant language o		

STAGE BISSUESESO

Page	1	
Date	6	

- · Templates police and and the first Soudei provides the feature to make ouston templates for specific needs / rumerobilities
- · uside coverage hookerabed es detents a wide range of eves, misconfigurations
- 1 Drozer, frida for mobile apps Stanger 19416 25 .

od of short county of bein stranger

- es explores exposed components privileage escalation Accommon Trans 100 100 10 10 1000 TEAMS
- is frida is a dynamic purpose toolkit analysis of suntime behavior
- (5) Android bebug lackage

1) Install (uniaBtall opps, access logs, file systems Sexprost sensitive files

Sused for manual testing and reconnaissance

6 for information gathering: ffuf, subfinder, httpx , subzy , on nmap

stored policy defects

Page:	
Date:	

	for Penetration Testing
mak	us a some of and and and a stranger out the
7.00117.4	It is mostly done manually, as the
	requests and responses needs to be
	Understood
Auga and Ang	in solve to some taken a state in
	1) BURPSUITE HAD
	es to capture requests mond
	is after requests
9 chol	wind standardor based samplereds from
V	D DWTF framework
	OWASP WSTG for web opp
	tistland asserted simpage a stabil &
-	& guide for testing Security of
	web - opp 2 services
30	TEST PLAN and TIMEUNE
	PLANNING
matous sie	egol seems ceddo Wordsired Votent
4	1 Information Gathering
nagosladao	· search for information leakage
	using google hacking
, valor	das 114 pairanting antimitant (3)
	" finger brint web server
	e numerate mep server
	· Identity entry points
	· most application architecture

ę

Page:	
Date :	

@ E Vulnerability Scanning

is using the bools mentioned is document every step

B Verification 201 1 most 1 m

solo a manual verification of the results from

& Penetrating Testing

4) Exploit assets that are in scope to demonstrate risk to be larged

used, proof of concept for each

es Assign CVSS score and rank the

3 Reporting

3 create an high-detailed overview and technical summary

6) Provide Remediation Support

5 resolve the 1880es found

5 Re-test to See it il is fixed

5 final Report

	Date:
	Different deams will be there for
	each asset:
	abandon alad bet saran eta
	O I team for web-app testing 2 APIS
	1 team for android app testing
	3 I team for los opp testing
	1 I team for cloud penterting
mon	3 5 teams for internal
	Intrastructe [I team each for
	5 systems)
*	antist prinning 1 A
	limeline
	adoss of sen toth doesn tiother of
	Day 1 to 7: Defining Scope, Objectives
- NO	Signing SLA
	Kules of engagement
	tay do
-	5 Information gathering and
	enumeration
	Meck 2 ' Valorative A
	Week 2: Vulnerability Assement for
Eu 9	and internal systems
	parelloly adapting
	harding
	and and a continuous continuous
	broof course the section from
	seed so to to one of the property
	moder logg to

Page:

			Date
	TIMBLIME		5/83/9/201
	Tools	2902 2003	8 -1 you
		694.103/110	
	Name	las la selles	CONS
		AJE DAINOIS	
0	owast ZAP	· very tem false tres	· can disrupt
		Report generation	web services due
		· Automated Scanning	to the huge amount
		seasy to use	of traffic generated
		il estrocu most was	O .
(3)	Nodei	o fast scanning	
		· custom templates	
	1312	Scanning and Volpera	8-F 400
•			0
3	Drozer	o explores exposed	
	(anobile abb)	components	
		elor betomeron aus	
9	fridation	provides real-time	
		code hooking	
	40	· analysis of funtime	
		behavio (100)	
(3)	Bulpsuite	· capture, modify	· No remediation
0	BOTPSON	HITTP 129UELS	· false bositives
	bood:13	o heat for web-app	
		papitopilina spodoid	
6	Astra lentest	o PUI-688, CIDER, HIRAA	· costly
6	Asma lenteur	180,8002	0
		compliance	
		o O fouse positives	
		o provides remediation	
		THE RESERVE OF THE PARTY OF THE	

Page:	1
Date:	

11		Date:	
	Timeline	Timesand formsomit	
	Day 1-3:		
	9. 0.		
	5	Objectives	
	2010	kules of engagement	
		Signing SLA	
*	oreit vos e	sour solo and profe of the leaster	0
165 K9 W	Day 4 - 6:	Reconnaissance and	
ma or	ad and d	Intelligence gothering	
2000	offord to	. 300 1 1100 6	
		o each team works in	
		parallel ma ten a laborta	
		actolyment minders of	10
	Day 7-8:		
	0	Scanning and Vulnerability	13
		Analysis	(8)
		of a maked 1 1	
		or on automated hols	
		o map out all the vulnerabilities	(4)
		o document them	
		o rank them on basis of	
		impact objects	
9040	Day-9-10:	Threat modeling.	0
7.9V	cional natal a	Alignosi TITH	
		odetermine risk impact a liklihood	
		· propose mitigations	
	o review the vulnerabilities		A
	U	· draw DADS	
		9200114000	
		Levelled sold 0 0	

and y	Page ; Date ;		
Day 11 - Exploitation			
0			
o manual expl	oitation takes time		
· document H	ne process, tools used,		
payloads u	sed, proof of		
concept			
Day 1s: Reporting and A	dvisory		
o oronte a dalated	reporting consisting		
- Lall Ambaga	reporting consisting		
P.O.C, and M			
1.0.0	7.77		
end			