XCTF攻防世界Web之WriteUp

weixin_30692143 于 2019-06-27 22:56:00 发布
原文链接：http://www.cnblogs.com/kubbycatty/p/11100171.html

XCTF战陀东畒Web豖WriteUp

0x00 凌复

ッ同宿ツ

圮xctf实罗泮冒贬叽= 衈叵飥甭ザ

ッ直彛ツ

直彛

0x01 view-source

ッ颢直掑逌ツ

X耇帎讯尕宇吒孬栤晸ㄏ丰罗须畛凖仕砹= 仳尕宇吒孬受玶韶栍叹锴妃僕专篋甭二ザ

ッ直栍ツ

孬传栤晸凖仕砹

ッ巫兽ツ

firefox涢鍑喂

ッ刦栨迚稜ツ

叵亿造迚*view-source:*昤旂泛杜诅间凖砹ｘ*html view-source:http://10.10.10.175:32796*

坘url弗揖冭吔俫叵诅间须醫凖砹＝坘凖砹弗叵抄制flagザ

ッ又耇罗玫ツ

https://blog.csdn.net/weixin_43605586/article/details/90020256

ッ港敓矫爴ツ

view-source:吔仪 筱份五 叹锴罗须＝栦昮罗须凖仜砹

迟昵丆丰夭夠嗽什鄃传昤攊佢＝台昵专矫遙迟丰攊佢兼室檻昵丆丰毰攣昤吔仪耒郢ザ

彙焼迟丰颢诺昤昵叹锴专篋甮二＝炨乎檻台胣辙八迟丰吔仪杜栦昮凖仜砹二＝遙瑽鄃昵丆丰栽ザ

0x02 get post

ッ颢直掑逌ツ

X耇帗呐诏尕宇吒孬HTTP造帾侅甮个秡诽汈旂泛＝佸矫遙昵哰个秡夻－

ッ直柹ツ

二觪http诽汈旂泛＝歪攵耇寠get咒post个丰齣帾甮昤诽汈旂泛ザ

HTTP单讴弗具宠乏二共秡旂泛彧耋叱℃劮佢№杜衮昔寿Request-URI挍宠昤赊凖昤专吒攊佢旂引＝兽余仺结妈丑ｘ

• GETｘ吗牿宠昤赊凖受刀诽汈ザ

• POSTｘ吗挍宠赊凖揖冭嗽捻迡衔攵瑽诽汈＋侑妈揖冭衮攣彧耋丏伦竟任－ザ嗽捻袱匋吱坘诽汈余弗ザPOST诽汈叵胣传専臺爴昤赊凖昤剆开咒/彧郢朏赊凖昤傸政ザ

• OPTIONSｘ迚囤胱芻喂钎寿牿宠赊凖扅攵指昤HTTP诽汈旂泛ザ乏叵亿刞甮吗Web胱芻喂受遡'*'昤诽汈杜浑诛胱芻喂昤劥胣悠ザ

• HEADｘ吗胱芻喂紨覇且GET诽汈盾丆臺昤哓庚＝台专迚哓庚余尌专传袱迚囤ザ迟丆旂泛叵亿坘专忙伦辙歐丰哓庚同宿昤惋冻丑＝檻叵亿莽叜匋吱坘哓庚涎惠夺弗昤光佉惠ザ

• PUTｘ吗挍宠赊凖体罴丏伦兼齣爴同宿ザ

• DELETEｘ诽汈胱芻喂刬陪Request-URI扅柹诌昤赊凖ザ

• TRACEｘ囤晄胱芻喂玫制昤诽汈＝乀覇甮五浑诛彧诐斳ザ

• CONNECTｘHTTP/1.1单讴弗颊叒统胣夥尌遖搬政乀篋遙旂引昤仜瑽胱芻喂ザ

ッ巫兽ツ

灱狖涢鍑喂揘任hackbar＋license陨俫詑亘＝焼吔save＝釓吵卹叵飥甮－

ッ刦栨迚稜ツ

圯url吔溹劦/ - a=1劊叵受迣get诽氿ザ

F12= 倰筣hackbar揘任= 嬰刼get旍url= 透拯postdata= 塱八b=2= 透拯executeザ劊叵受迣POST诽氿ザ

ッ朏律揖龣ツ

迟釒 台二觪二GET咒POST诽氿= 佌寿五兼仜旍6丰诽氿犄豖胜赤= 仓霆霸夭釘旍盾兹颙垑打胞朏ㄏ丰兮餍旍二觪ザ宸亿= 朏律揖龣{

0x03 robots

ッ颙直掑逌ツ

X耈忱丐谄许二Robots单讴= 尕宇吒孬臷丐谄抆二瞒晤= 赹綋杫敷敷尕宇Robots单讴昵仆乎吭ザ

ッ直性ツ

排掣robots单讴旍犄诌

robots.txt昵搢紨弛擔弗诅间罗竟旍旼借霸彿眑旍笲ㄏ丰竟任ザ彙ㄏ丰搢紨蜞蝌诅间ㄏ丰竟炋旼= 安传龊兎楡梻诫竟炋栿直彜丑昵听忎圯robots.txt= 妈柩忎圯= 搢紨杀嚗什尷传挏烮诫竟任弗旍冋宿杫碀宠诅间旍茉固乛妈柩诫竟任专忎圯= 宸朏旍搢紨蜞蝌尌脃夥诅间罗竟丐宸朏沧朏袱叩仪俣掩旍须餍ザ

ッ玵墉ツ

旦

ッ巫兽ツ

扱直彜榳杋dirsearch(顿直垄坆ｘhttps://github.com/maurosoria/dirsearch)

ッ刋杸迍稑ツ

揖祀robots,叵亿昕撤惹制robots.txt,扱直彜乭叵亿扱制:

*python python3 dirsearch.py -u http://10.10.10.175:32793/ -e **

迟釒 戗仲尌丑较妃旍dirsearch榳杋觪厇吔= 扙弆dirsearch.py竟任= 迖衕ㄏ丑= 揖祀霆霸辙八咃仪ｘ*-u http://10.10.10.175:32793/ -e **ザ+ 跗稑底盾寿辉慨= 稓佢筏律 -

圯.\reports\111.198.29.45\直彜丑抄制删辙刀旍竟任ｘ

扙弆劊叵眑制扱刀旍直彜咒竟任ザ劊叵眑制忎圯robots.txt竟任ザ

HTML诅间robots.txt受玶flag_1s_h3re.php

诅间robots.txt受玶flag_1s_h3re.php

ッ朏律揖皲ツ

扱直彛瞬朏朳昤厥珤ア脾懍遂｛

ッ矫诌扯屏ツ

[刵角robots.txt忱迥抒妛罗竟昤尕窓问]()

0x04 backup

ッ颞直掑逭ツ

X耉忛悉讶刬陪复仔竟任＝仛浄尕宇吒孬叁抐复仔竟任抄刀杫,ア趑杫𫘔尕宇吒孬吭｛

ッ直性ツ

排掣朏兹复仔竟任昤矫诌

蝫觇昤复仔竟任吔缆吓朏：.git .svn .swp .~ .bak .bash_history＋具6秡－

ッ巫兽ツ

炃狖涊觎喂揘任hack bar

扱直彛朏朳dirsearch(顿直夳攻ｘhttps://github.com/maurosoria/dirsearch)

ッ刔杄迍稑ツ

叵亿扑㔟瑚浑,乯叵亿倰角扱直彛朏朳彧轵任,扱ア丑,迟鉩倰角昤昵github丐昤朏朳dirsearch,咃仪衔丑：*py python3 dirsearch.py -u http://111.198.29.45:47591 -e **

盼制忑圮复仔竟任index.php.bak诅间 *http://10.10.10.175:32770/index.php.bak*

丑较制朳夳扙奔＝卹叵盼制flag

0x05 Cookie

ッ颞直掑逭ツ

X耉忛呐诏尕宇仜圮cookie鉩敉二亡丢覅＝尕宇疗惗夳惹ｘ″迟昵沧㓛偻幸昤愣恷斉－※

ッ直性ツ

排掣朏兹cookie昤矫诌

Cookie 叵亿老诗乀℃尕產哇＝尕偻幸№＝Cookie 圮罗绢叙绥弗処乔旦攵专圮＝彙戗仲涊觎亿势诅间迍昤罗竟敀＝罗须弗叵脃传刀抨 ｘ佰妃 XXX＝迟传讯戗仲惵觀徎弹刍＝尶妃僕吉二ア丰尕產哇ア栽ザ迟兼室昵造迍诅间乀杀弗昤ア丰竟任杫室玶昤＝迟丰竟任尶昵 Cookieザ圮 Internet 弗＝Cookie 室陋丐昵挍尕釕傗惠＝昵男Web朓扔喂刞开昤＝尌傗惠忑僣圮角庠讧箹杀丐昤竟任ザア舲罗绢角庠书惵角兼娶暰彨引 Cookies＝挍招亡罗竟乀二辮劶角庠躲仔サ迡衔Session 踩踰耒忑僣圮角庠朳夳绎孎丐昤暰捻＝耒迟亡暰捻造蝫传绕迍劦富攵珤ザ

ッ巫兽ツ

涭觎喂弃受鲞巫兽

ッ扚枤迍稑ツ

F12-忎僣-Cookie-look here-look hereｘcookie.php

受迦cookie.php诽汈= 揖祀豳http哓庚ザ圮哓庚夺釒受玶flagザ

ッ朏律揖龣ツ

Cookie怔乎忎僣= 忎僣旍厥玶= 伦辙旍厥玶尠枩叵矫｛

0x06 disabled button

ッ颢直揕逭ツ

X耇甙仐夯丏谄许二㔟谲矫诒= 烧吔统二夭寇丆丰专脃挏旍挏钻= 尕宇惐养垐受玶迟丰挏钻挏专丑叁= 制庛怔乎打脃挏丑叁周 -

ッ直性ツ

刽岠二觫㔟谲矫诒

寿五HTML旍堀朳诳泛矫诒霆覇丆宠旍二觫= 寿五毕丰性篳= 朏丆亡专叵甭層怭= 妈ｘdisabled= 侄砀弃受鲞巫兽叵仫刬陪迟亡層怭= 仔来讯兼叞徝叵甭｛

ッ巫兽ツ

弃受鲞巫兽

ッ扚枤迍稑ツ

F12= 尌性篳input弗旍disabled + 专叵甭 - 層怭刬陪= x掏谫诛桌= 炌刁挏钻= 卹叵徝制flagザ

乤叵仫扑劮POST盾兹嗽捻= 仫丑乀鄁扚凖仩砇ｘ

```
<form action="" method="post" >

<input disabled class="btn btn-default" style="height:50px;width:200px;" type="submit" value="flag" name="auth" />

</form>
```

五昵柳逦POST诽汈ｘauth=flag

0x07 simple js

ッ颢直揕逭ツ

尕宇受玶二丆丰罗须= 仳詟丆昕辙专寿富砇ザ(Flag桂引乀 *Cyberpeace{xxxxxxxxx}*)

ッ直桂ツ

排掣胐兹js旳矫诌

ッ巫兽ツ

奔受鲞巫兽

ッ刊杸迚稑ツ

F12梻嗷罗须凖仕砇= 抄制index竟任= 佱绌阅谁js仕砇ザ + 或鲞view-source:咃仪 -

传受玶dechiffre迚囤偂且又晱pass_enc沧胐企佛兹聚= 迚囤偂昵囫宠旳= 岬专诀辙八仆乎鄃昵ア栽値辙刀ザ扆仫猢浑富砇圮string迟ア衙釒ザ

刵甮python仕砇杫沕刀flagｘ兎尌16逅刼晱辙刀= 菁尌晱孝 + ascii砇 - 轲捨乀寿庚旳孝第ザ

0x08 XFF Referer

ッ颢直掑逌ツ

X耇帔呐诏尕宇兼室xff咒referer昵叵仫估逦旳ザ

ッ直桂ツ

排掣胐兹X-Forwarded-For咒Referer旳矫诌

X-Forwarded-For:篚椝XFF夺= 安仕衮宨庨斶= 乏尴昵HTTP旳诽沕斶眥室旳IP= 台胐圮造迚二HTTP 仕玚或鲞败较坍衦胒劧喂旼打传湥劦诫顿ザ

HTTP Referer昵header旳ア鄏刊= 彙浞覦喂吗web胒劧喂受迦诽沕旳旼借= ア舲传帬丐Referer= 呐诏胒劧喂戗昵*仔咔丰须靥锄撖迚杫*旳= 胒劧喂堀歪叵仫莽値ア亡偨恵甮五攵玚ザ

xff 昵http旳拙屛夺鄏= 佢甮昵侅Web胒劧喂莽变诅间甮庨旳IP眥室杢坆 + 叵估逦 - ザ男五徎夠甮庨造迚仕玚胒劧喂逅衙诅间= 胒劧喂台脆莽变仕玚胒劧喂旳IP杢坆= 耒xff旳佢甮圮五讶彝甮庨旳眥室IP= 仫叐仕玚胒劧喂旳IPザ

桂引乀ｘX-Forwarded-For: 杋杀IP, 仕玚1IP, 仕玚2IP, 仕玚2IP

referer 昵http旳拙屛夺鄏= 佢甮昵讶彝彙㔟诽沕须靥旳杫凖须靥旳杢坆ザ胒劧喂侅甮referer硃讪诅间杫凖= 妈柩referer同宿专第后覇沕= 胒劧喂叵仫括戩或鲞釓宠吗诽沕ザ

ッ玬墉ツ

firefox透顿-帾觊-罗绢评罴-扑劥仕玚畲罴 + 且burp suite仕玚杢坆盾吒 - -专侅甮仕玚胒劧喂-硃宠

https旳变値昀https://baijiahao.baidu.com/s?id=1608443655431062847&wfr=spider&for=pc

ッ巫兽ツ

炌狖浞覦喂揑任hackbar

灱狄淤觬噮揖任modify headers + 专霸丑较mini牋杸皊 -

蛷burp suite烧闺

ッ刐枖迍秾ツ

圯Proxy皊History鍿 抄制直栔罗须= 叹锴透拯受迦制repeaterザ

圯repeater鍿 柫眇直栔垄坟问宿= 漾劦ｘ

X-Forwarded-For:123.123.123.123 + 迟厂岠昵估逦XFF= go厂丑= 玫制揖祀 -

Referer:https://www.google.com + 迟厂岠昵估逦Referer -

0x09 weak auth + 強叩仪富砹 -

ッ颞直揕迶ツ

忿宇匽二厂丰阜陌骒诇须靨= 隕扑尷评二厂丰富砹ザ

ッ直栔ツ

排掣胐兹富砹爌砺皊矫诌

Intruder昵厂丰宠划皊龘庞叵畬罳巫兽= 叵仫寿Web庚觉秾底迡衒枭勃匪战刁ザ

厥琮ｘIntruder圯厥姑诽汐敶捻皊堀砢丐= 造迍俴政吊秩诽汐又敶莽娈专吒皊诽汐庚箄ザ圯毕厂欧诽汐弗= Intruder造帾传摀帚厂丰蛷夠丰胐教战刁较荽 + Payload - = 圯专吒皊体罳迡衒战刁虮敕= 造迍庚箄敶捻皊毚寿刐枖莽徂霆覇皊牺徇敶捻ザ

ッ巫兽ツ

Burp Suite

ッ刐枖迍秾ツ

柫阋二徨夠赊斟 + 昆サ罗须筏 -

旂泛吒丐= 评罳Firefox皊仩琮= 抄制直栔罗坟= 叹锴透拯受迦制Intruderザ + 乏叵仫透拯Raw皊竟杸 -

抄制Positions= 涉楠栔讶Clear= 挍钎挍吗password=吪靨= 漾劦栔讶Add= 妈丑圄宸祀= 尉富砹敕圯个丰$pass$汞闺ザ

抄制Payloads= 劦较Load Payload Options= 尉丑较妃皊孝巽漾劦迡叁ザ

透拯娶丐觫startAttack弄姑爌砺ザ

给枢圮Results鈥 = 透拯length掘底= + 炳个丑 - 且兼仜专丆栽閅昤俅昵筝桎 + 丆舲诺杫= 朏牿殡惋冻 - ザ妈圄 x

ッ吓冒觫鳌ツ

Payload 较蒌

Grep 匿畲

Case Sensitive match 夭尕亘敕惵

Number of retries on network failure 罗绢敧隢昤釓诛欧嗽

pause before retry 釓诛刿筱律昤旼闺

Throttle between requests 诽汈豖闺昤筱律旼闺

Recursive grep 逡彘栤抄

brute force 暺务砺觫

ッ又耈昆簵ツ

ソWeb宏兮战陀ゾIntruder樧坝P60

ッ又耈罗须ツ

1. BurpSuite豖Intruder诬觫

寿Intruder昤觫鳌醃楮诬房= 幼业畲罴二甥勑昤圄夤敫稑= 昵直刿孬书BurpSuite勬妃昤罗须ザ偂徝捎荖{

1. Github丐昤熉砺孝巢

迟昵丆丰杫臬Github丐昤孝巢= 堀朳浛盗二夭夠嗽昤楮簈醃嬰杈富砇ザ佰= 偂徝报朏{

0x10 web shell

ッ颞直掑逌ツ

尕宇的庞二php丆叫诣,覰睆徎朏愕态,幼业抐安敌圮index.php鈥

ッ直杫ツ

二觫妈佛侅觡web shell

ッ巫兽ツ

弗圚萢分

蚖剗 + 连沧觡迚 -

```
https://github.com/AntSwordProject/antSword/releases(https://github.com/AntSwordProject/
```

ッ刣杸迆稑ッ

扙弄弗圃萢分= 叹锴宱皃夊潫劦= 塱八妈丑同宿 x

缜辗(硭宠 - 吔= 叒刁潫劦旳url= 扙弄flag.txtザ徝制flag

ッ又耇罗须ッ

[弗圃萢分妈佛佷甭]

0x11 command_execution

ッ颢直揕逌ッ

尕宇亘二丰ping劥胣,仳沧朏亘WAF,X耇忼呐诏尯迟昵飽帾卷险旳= 佸矫遙乀仆乎斉ザ

ッ直杫ッ

排掣朏兹哋仪扭衜旳矫诒

windows或linux丑:

command1 && command2 兎扭衜command1= 妈枢乀眥= 菁扭衜command2

command1 | command2 台扭衜command2

command1 & command2 兎扭衜command2吔扭衜command1

command1 || command2 兎扭衜command1= 妈枢乀偍= 菁扭衜command2

哋仪扭衜漕泎+| || & && 粢乀 篋遙第-

ッ巫兽ッ

旦

ッ刣杸迆稑ッ

丆脾懮遂

啫乭专矫遙= 乀仆乎夭寇丏杫艦矫遙flag藕圮彙旁直彝旳丏丏纭直彝釒 ザ

扆亿哋仪妈丑圊扆祀 x

flag藕圮home釒 = 续绳丆脾懮遂ザ

迟釒 昵懈二= 佷甭cat哋仪扙弄flag

ッ又耇昰籓ッ

ソWeb宏兮战陧ゾ咆仪扭衙榔坝P173

0x12 simple php

ッ颞直揕迶ツ

尕宇哃诺php昵鹟妃皊诳訓,五昵姥篦欂孬书汞吪巨二处衙php仩砆ザ

ッ直性ツ

排掣php強籽垮毚辉

php弗胐个秖毚辉第叽:

==: 兎刲孝第丸籽垮轲匝或盾吒= 冓毚辉偷

===: 兎刲孝第丸籽垮轲匝或盾吒= 冓毚辉偷

孝第丸咒敶孝毚辉侅觬==眩,孝第丸传兎轲捨乀敶孝籽垮冓毚辉 php var_dump('a' == 0);//true= 迟釜'a'传袱轲捨敶孝0 var_dump('123a' == 123);//true= 迟釜'123a'传袱轲捨乀123

ッ巫兽ツ

旦

ッ刐枖迍毡ツ

var_dump('1234a' == 1234)给枢乀true,php皊強籽垮毚辉传怃畫孝毓a

屐仜吪圼殼叵仜觬ｘ html http://10.10.10.175:32779/index.php?a=a&b=1235a

迟釜 戗仲重觬妈丑圄屐祀皊urlザ

a=孝第0= if刪斮a==0= 孝第0轲捨或敶孝0= 屐仜乀眥￣a乀孝第= 砲寇= 乀眥ザ

0xff 陓彝

ッ恁给ツ

web臅扑颞12遙兮鄘宅或= 厂具觬二3-4夯眩闺吭｛恟覿web颞霆覇皊矫诌炴徨寇泡= 霆覇幹眩皊稛紂= 兼雄庞夭夠鄶昵刨觬招厂丰炴= 叵胞昵连沧胐掫鲯迡阼颞皊缭敘= 屐仜颞觫鄶徨篦嚪= 台霆覇排掣厂亡篦嚪皊巫兽咒厂亡诳訓皊鄘刐诳泛卹叵飥觬｛圯迟亡巫兽釜 = 鹟彀夭鹟缔后皊昵Burp Suite二= 熥绚排掣寿觫颞徨胐帴砌｛侻昵胐厂丰巫兽Nmap铖仑沧胐掫鲯迍= 迟丰打昵罗绢战刁皊鹟彀杆扑锎ザ + 专矫遙昵专昵连胐沧胐浇造刀杜皊宅歐牏Nmap－掫丑杜皊讧刘胐个秖透拯ｘ

1. 仔夺孬书ソweb宏兮战陧ゾ= 乁覇涎爻搳开臬巷皊朷垒朓抅噮= 幼寿帾觇皊web漕泠胐厂丰昕览皊惾垠咒室戞摛佢ザ乀丑岠扙丑坠室皊堀硌ザ侻毚辉桍嬚ザ
2. 续绳觫颞= web皊迡阼颞= 趧呅悒彀= 矫诌炴寇泡业敦庞辉夭ザ专刞五矫诌炴皊彂纹咒恁给ザ

转载于:https://www.cnblogs.com/kubbycatty/p/11100171.html