Web Application Development

SQL Injection Attacks…

Charlie Garrod
School of Computer Science
Carnegie Mellon University

SQL and the Django ORM

1. Write a SQL injection attack against today's in-class example (http://localhost:8000/) Hint: http://xkcd.com/327/
2. Write SQL queries equivalent to:
   a. `Student.objects.all()`
   b. `Student.objects.filter(first_name__iexact='Charlie')`
   c. `Student.objects.filter(first_name__istartswith='C')`
   d. `Student.objects.filter(first_name__startswith='C')`
   e. `Student.objects.filter(first_name__contains='har')`
   f. `Student.objects.filter(first_name__exact='Charlie').exclude(last_name__exact='Garrod')`
   g. `Course.objects.filter(students__first_name__exact='Charlie')`
3. Write a Django query and SQL query for:
   a. "Select all students who are classmates with a student named Charlie."