آسیب‌پذیری رایج در سامانه‌های کشور

در گذشته

آسیب‌پذیری تزریق دستورات SQL

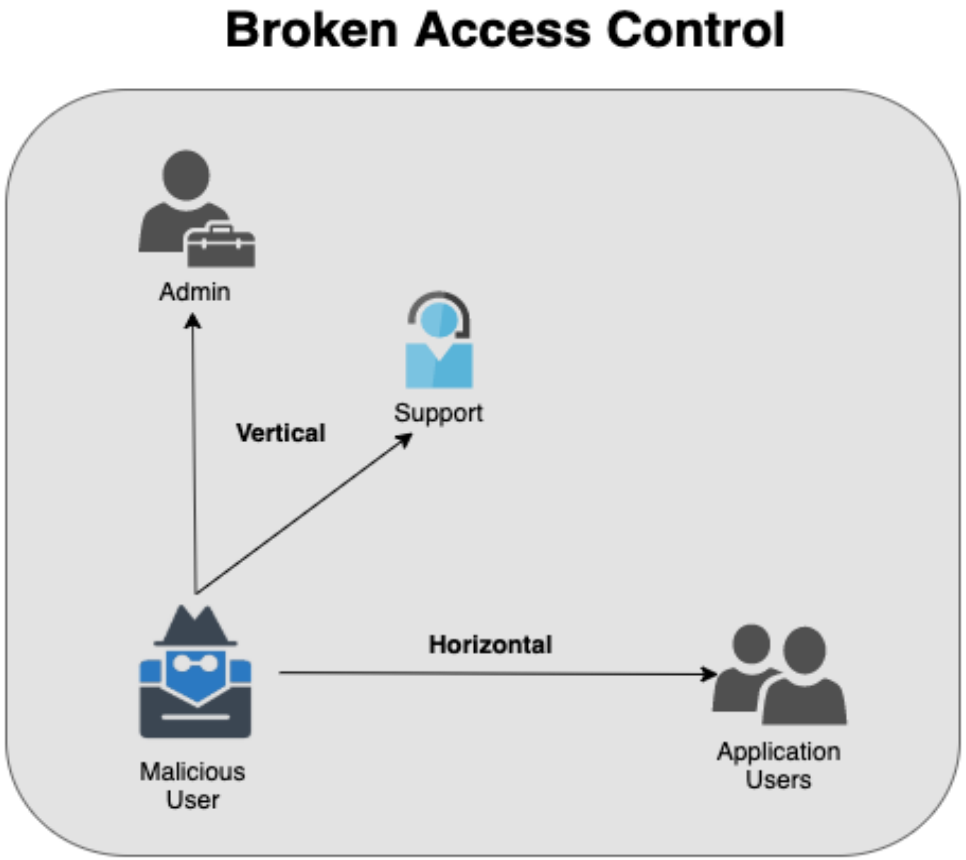
تزریق دستورات SQL

- مدیریت ضعیف در اعتبار سنجی کدها یا ورودیهای برنامه
- انجام عملیات مختلف در پایگاه داده (بسته به طراحی)

در حال حاضر

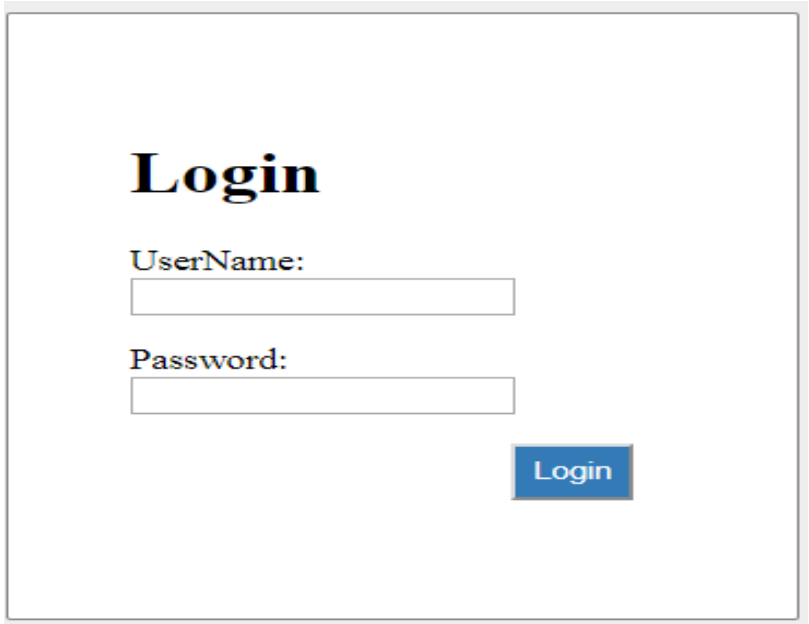
آسیب‌پذیری کنترل سطح دسترسی

کنترل سطح دسترسی



- اعمال محدودیت:
  - عملیات
  - منابع
- سطوح کنترل:
  - کنترل سطح دسترسی افقی
  - کنترل سطح دسترسی عمودی

احراز هویت



آسیب‌پذیری کنترل سطح دسترسی افقی

- مشاهده پروفایل دیگران
- انجام هر عمل قابل دسترس برای کاربر

- https://insecure-website.com/acc=12
- Name: Ali
- Balance: 100,000,000

- https://insecure-website.com/Add/
- https://insecure-website.com/Edit/
- https://insecure-website.com/Delete/

آسیب‌پذیری کنترل سطح دسترسی عمودی

- مشاهده اطلاعات مهم
- انجام هر عمل قابل دسترس برای ادمین

- https://insecure-website.com/Info
- Info
  - Organization data
  - Application data

- https://insecure-website.com/Op
- Op
  - Add,
  - Update,
  - Edit,
  - Delete any data

مثال در دنیای واقعی

کنترل سطح دسترسی افقی

درخواست

Raw | Params | Headers | Hex

```
POST /internship/yd/callus/reply HTTP/1.1
Host: [redacted]ir
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:76.0) Gecko/20100101 Firefox/76.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: fa,en-US;q=0.7,en;q=0.3
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 11
Origin: [redacted].ir
DNT: 1
Connection: close
Referer: http://[redacted]internship/yd/mainpage/page?1591091713
Cookie: _ga=GA1.3.1029492134.1590487532;
ci_session=KTnyghmT4FOnAblAllyB3dkDAnaLomEQoeaTV57fGA9zR86cTNPJXOEwslfmF7TwC%2F783Hq4n7goAv
VxW3UPd31dUF%2FmBqlrwODXyxwnWmTlVqYHpvt5ua7CmEMOFXxE7gsTI7yJB6wSkCTUw60u5Iug9uUkWJvn6wXWXSC
ellRcfffvYCpQUOEnrSlinnkr0isfLMFl5bWKLGhfzy4hNlThfD6SKhbROKwylDI4P92IyZrIe4TmY9%2BxgIN%2BPw
AWJilpE67099tAaUhshmllm24ESpEsReP%2BiwzOxXaQ6Gtvzdjonaz25jaxICfsOGFXQiW6E6ZFNnrLv2AtUoXFfDE
76K6sHyBUE4ofwHgtrQcw8E6avAZ2INnzGNUxAB7K
Upgrade-Insecure-Requests: 1

ydq_id=1364
```

پاسخ

موضوع پیام

بازیابی نام کاربری و رمز عبور

متن پیام

با سلام احتراما شرکت تعاونی [redacted] خواست

بازیابی نام کاربری و رمز عبور دارد. خواهشمند است همکاری های لازم مبذول

فرمایید. با سپاس شماره ملی کارفرما بهادر [redacted] ۸۶۴۱ [redacted]

تعداد مشاهده شده

پاسخ کارشناس

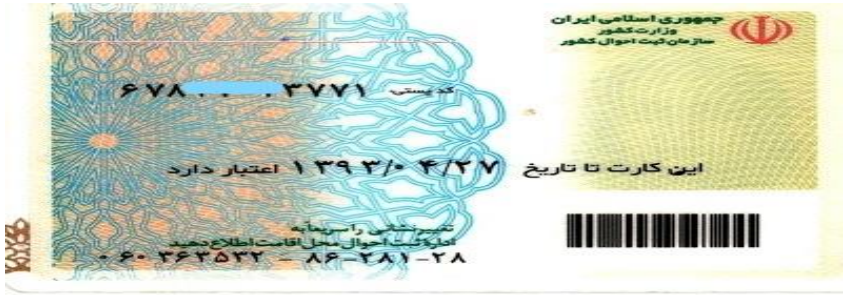
باسلام، نام کاربری: ۲۷ [redacted] رز عبور: ۲۷ [redacted] ۱۴

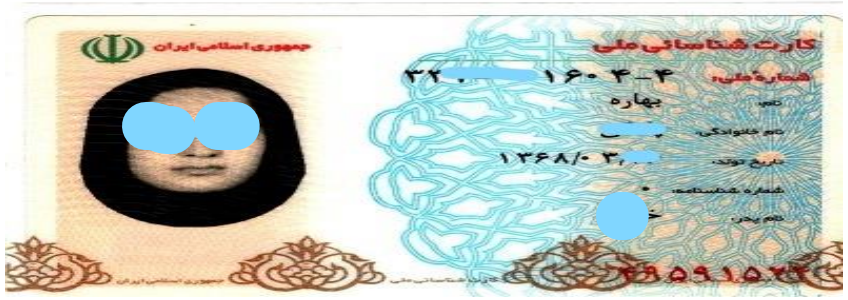
کنترل سطح دسترسی افقی

درخواست

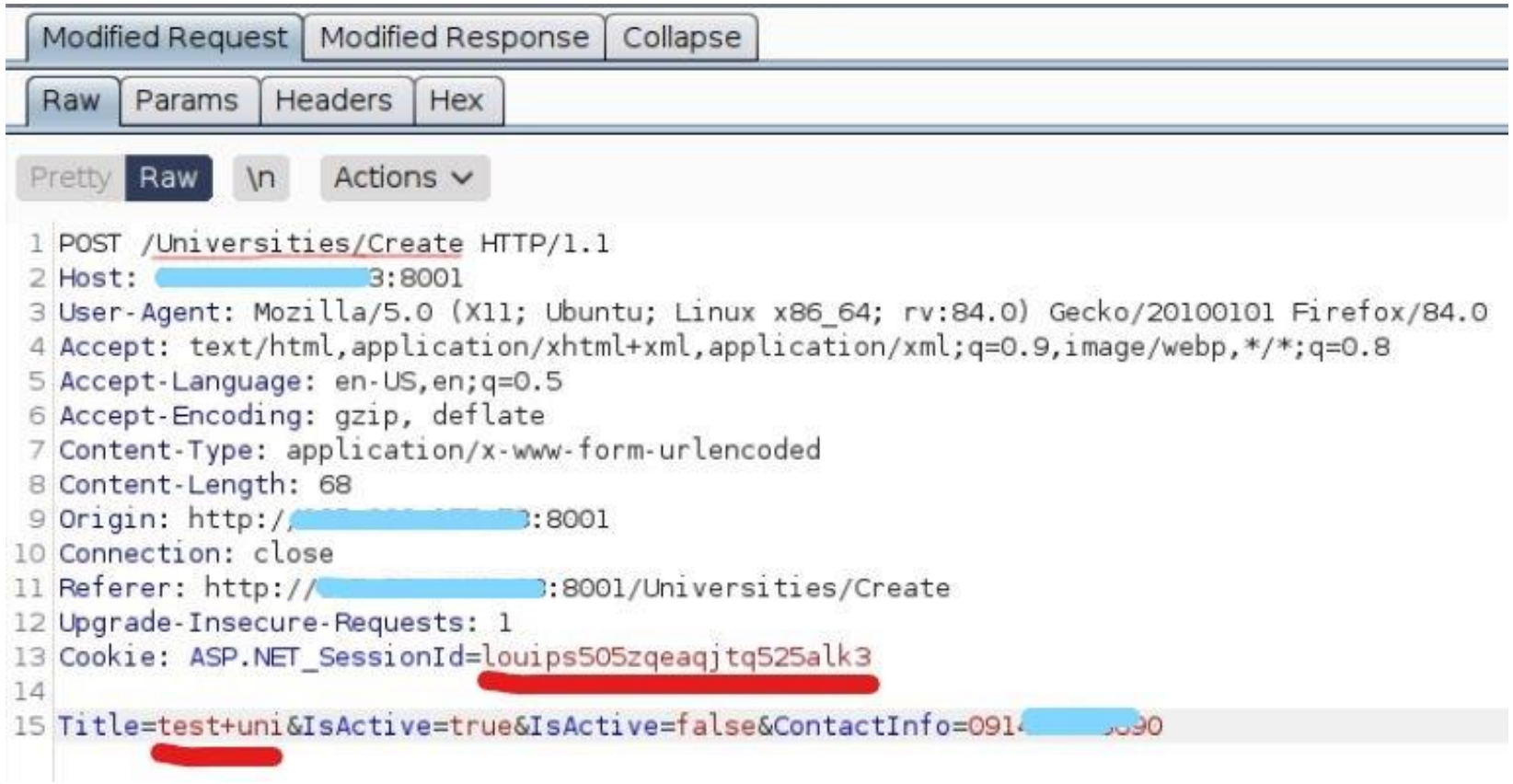
- http://***.****.gov.ir/imagesupload/karvarzi_document/nidstudent/13980917/1575835524.jpg

پاسخ





کنترل سطح دسترسی عمودی



نتیجه درخواست

ارتباط با ما

- از طریق اداره کل ارتباطات و فناوری اطلاعات استان
- وبسایت barootech.ir
- آدرس ایمیل cus@barootech.ir