

## داکیومنت پروژه پایانی

عسل خوش قامت آزاد 9922762231

هما بدیعی 9912762278

- شناسایی دارایی ها: فایل اطلاعات کاربران، کلید های خصوصی کاربران، پیام های رد و بدل شده

بین کاربران

- ارزش گذاری دارایی ها:

○ فایل اطلاعات کاربران: زیاد

▪ علت: فایل دیتابیس شامل اطلاعاتی مثل ایمیل، نام کاربری، نقش، salt و پسورد هاش شده می

باشد، حملاتی مثل فیشینگ با استفاده از ایمیل شخص یا password guessing با استفاده

از نام کاربری شخص ممکن است.

○ کلید خصوصی: زیاد

▪ علت: در صورت فاش شدن کلید خصوصی، مهاجم به پیام های رمز شده ای که برای کاربر

victim فرستاده شده، دسترسی پیدا می کند.

○ پیام های رد و بدل شده: کم تا زیاد

▪ علت: بسته به محتوای پیام و سطح اهمیت و محرمانگی پیام، فاش شدن آن می تواند مشکل

ساز باشد.

## تشخیص آسیب پذیری ها:

- فایل اطلاعات کاربران:

○ عدم استفاده از مکانیزم های حفاظت از داده ها مانند رمزنگاری یا مجوزهای دسترسی دقیق.

○ فاش شدن ایمیل و نام کاربری و نقش کاربر

- کلیدهای خصوصی کاربران:

○ کلیدهای خصوصی ممکن است در فایل های متنی ساده یا مکان های ناامن ذخیره شوند.

○ در صورت عدم مدیریت درست چرخه عمر کلیدها، کلیدهای قدیمی ممکن است به روزرسانی یا بازنشانی

نشوند.

- پیام های رد و بدل شده بین کاربران:

○ در صورت عدم استفاده از رمزنگاری end to end پیام ها به صورت متن ساده منتقل می شوند و خطر

حمله Man-in-the-Middle وجود دارد.

○ پیام ها ممکن است در حین انتقال دستکاری شوند و یکپارچگی پیام ها حفظ نشود.

○ عدم استفاده از nonce

## تحلیل آسیب پذیری:

- ذخیره سازی ناامن اطلاعات کاربران:
  - تاثیر: دسترسی به اطلاعات حساس کاربران می تواند به نشت اطلاعات و خسارات مالی و اعتباری منجر شود. فایل دیتابیس شامل اطلاعاتی مثل ایمیل، نام کاربری، نقش، salt و پسورد هش شده می باشد، حملاتی مثل فیشینگ با استفاده از ایمیل شخص یا password guessing با استفاده از نام کاربری شخص ممکن است.
  - احتمال بهره برداری: بالا، در صورت عدم استفاده از روش های رمزنگاری و کنترل دسترسی مناسب.
  - اولویت اقدامات اصلاحی: بسیار بالا. استفاده از رمزنگاری و تنظیم مجوزهای دقیق دسترسی به فایل ها.
- دسترسی غیرمجاز به فایل ها:
  - تاثیر: دسترسی غیرمجاز به فایل های اطلاعات کاربران می تواند منجر به سوءاستفاده از اطلاعات شخصی شود.
  - احتمال بهره برداری: متوسط تا بالا، بسته به تنظیمات فعلی مجوزها.
  - اولویت اقدامات اصلاحی: بالا. تنظیم و بازبینی مجوزهای دسترسی به فایل ها.
- ذخیره سازی ناامن کلیدهای خصوصی:
  - تاثیر: دسترسی به کلیدهای خصوصی کاربران می تواند به شکستن رمزنگاری پیام ها و نقض حریم خصوصی منجر شود.
  - احتمال بهره برداری: بالا، در صورت عدم استفاده از روش های امن برای ذخیره سازی کلیدها.
  - اولویت اقدامات اصلاحی: بسیار بالا. استفاده از روش های مناسب.
- تولید ناامن کلیدها: (رفع شده)
  - تاثیر: استفاده از کلیدهای ضعیف یا غیرمعتبر می تواند امنیت کلی سیستم را به خطر بیندازد.
  - احتمال بهره برداری: متوسط، بسته به روش های تولید کلید.
  - اولویت اقدامات اصلاحی: متوسط. استفاده از الگوریتم ها و روش های استاندارد برای تولید کلیدها.
- عدم استفاده از رمزنگاری end to end: (رفع شده)
  - تاثیر: پیام های کاربران در معرض شنود و دستکاری قرار می گیرند.
  - احتمال بهره برداری: بالا، به خصوص در شبکه های ناامن.
  - اولویت اقدامات اصلاحی: بسیار بالا. پیاده سازی رمزنگاری end to end برای حفاظت از پیام ها.
- خطر حملات شنود (Man-in-the-Middle):
  - تاثیر: مهاجم می تواند پیام ها را شنود و دستکاری کند.
  - احتمال بهره برداری: بالا، در صورت عدم استفاده از پروتکل های امن.
  - اولویت اقدامات اصلاحی: بسیار بالا. استفاده از پروتکل های امن مانند TLS برای انتقال پیام ها یا رمزنگاری.
- عدم یکپارچگی پیام ها: (رفع شده)
  - تاثیر: پیام ها می توانند در حین انتقال دستکاری شوند.
  - احتمال بهره برداری: متوسط، بسته به روش های موجود برای بررسی یکپارچگی پیام ها.
  - اولویت اقدامات اصلاحی: متوسط. استفاده از امضای دیجیتال برای تضمین یکپارچگی پیام ها.

- عدم استفاده از nonce در پیام ها:
  - تاثیر: باعث حمله replay می شود.
  - احتمال بهره برداری: بالا، بسته به نحوه استفاده nonce ها.
  - اولویت اقدامات اصلاحی: بالا، استفاده از timestamp ها و nonce ها.

### اقدامات لازم برای رفع آسیب پذیری ها:

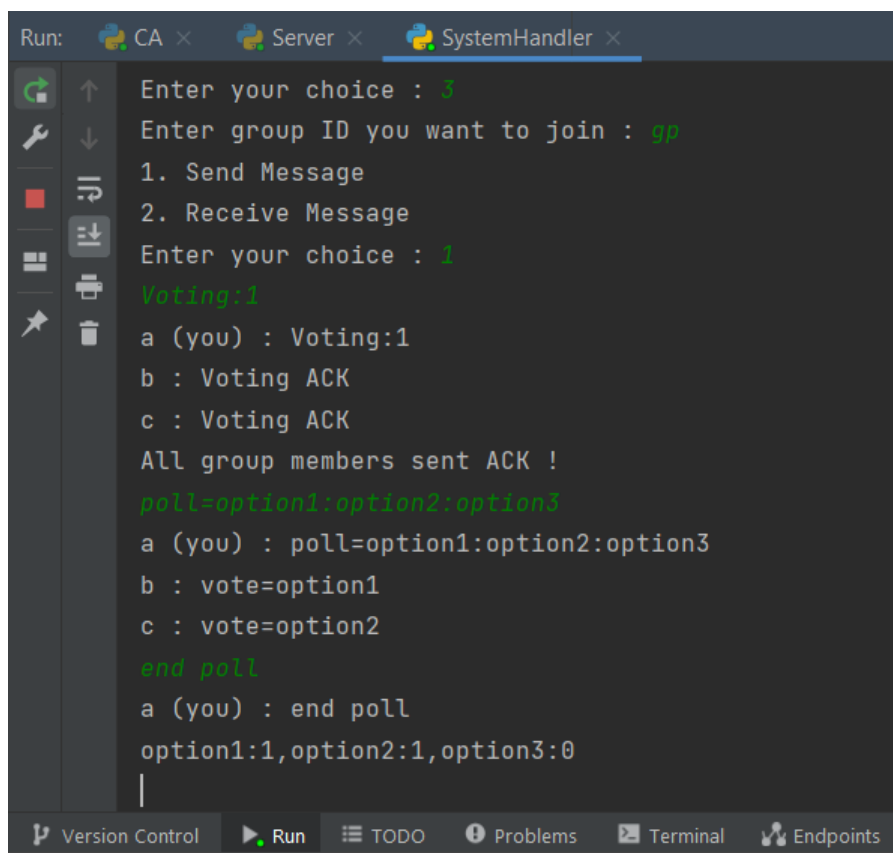
- ذخیره سازی ناامن اطلاعات کاربران: (پیاده سازی شده در فاز دوم)  
در این پروژه به منظور رفع این آسیب پذیری از رمزنگاری فایل دیتابیس اطلاعات کاربران استفاده کردیم. هر بار که نیاز به استفاده از این فایل داریم، با استفاده از پسورد آن را رمزگشایی کرده و در انتهای تغییرات فایل جدید را رمزنگاری کرده و فایل بدون رمز را حذف می کنیم.
- ذخیره سازی ناامن کلیدهای خصوصی: (پیاده سازی شده در فاز دوم)  
در این پروژه با استفاده از پسورد کاربران کلیدهای خصوصی هر کاربر را رمز می کنیم و در صورت نیاز به کلید خصوصی آن را رمزگشایی می کنیم و پس از رفع نیاز، کلید خصوصی رمز نشده را حذف می کنیم.
- دسترسی غیرمجاز به فایل ها:  
از پسورد ها برای دسترسی به فایل ها استفاده کردیم و در برخی موارد نیز برای دسترسی به یک فایل سطح دسترسی کاربر را بررسی می کنیم.
- خطر حملات شنود (Man-in-the-Middle):  
در این پروژه با استفاده از رمزنگاری پیام ها این آسیب پذیری را در چت خصوصی مدیریت کرده ایم.
- خطر حمله replay:  
می توانیم با استفاده از timestamp ها و nonce ها در پیام از این حمله جلوگیری کنیم.

## voting

ادمین گروه با ارسال کلمه **voting** یک رای گیری را آغاز می کند و منتظر می ماند تا همه اعضای گروه **voting ACK** را ارسال کنند در این حالت ادمین می تواند نظرسنجی را با فرمت **poll=option1:option2:...** قرار دهد. اعضا با **vote=...** می توانند در رای گیری شرکت کنند. بعد از اینکه اعضا در رای گیری شرکت کردند، ادمین با **end poll** رای گیری را متوقف می کند.

ادمین با وارد کردن **voting:1** مشخص می کند که رویکرد رای گیری شفافیت می باشد و با وارد کردن **voting:2** مشخص می کند که رویکرد رای گیری محرمانگی می باشد.

یک نمونه رای گیری با رویکرد شفافیت:



```
Run: CA x Server x SystemHandler x
Enter your choice : 3
Enter group ID you want to join : gp
1. Send Message
2. Receive Message
Enter your choice : 1
Voting:1
a (you) : Voting:1
b : Voting ACK
c : Voting ACK
All group members sent ACK !
poll=option1:option2:option3
a (you) : poll=option1:option2:option3
b : vote=option1
c : vote=option2
end poll
a (you) : end poll
option1:1,option2:1,option3:0
|
```

```
Run: SystemHandler x
Enter your choice : 3
Enter group ID you want to join : gp
1. Send Message
2. Receive Message
Enter your choice : 2
a : Voting:1
b : Voting ACK
Voting ACK
c (you) : Voting ACK
This poll is sent from admin !
a : poll=option1:option2:option3
b : vote=option1
vote=option2
c (you) : vote=option2
a : option1:1,option2:1,option3:0
|
```

Version Control Run TODO Problems Terminal Endpoints Python Packages

```
Run: SystemHandler x
Enter your choice : 3
Enter group ID you want to join : gp
1. Send Message
2. Receive Message
Enter your choice : 2
a : Voting:1
Voting ACK
b (you) : Voting ACK
c : Voting ACK
This poll is sent from admin !
a : poll=option1:option2:option3
vote=option1
b (you) : vote=option1
c : vote=option2
a : option1:1,option2:1,option3:0
|
```

Version Control Run TODO Problems Terminal Endpoints

یک نمونه رای گیری با رویکرد محرمانگی:

```
Run: SystemHandler x
Enter your choice : 3
Enter group ID you want to join : gp
1. Send Message
2. Receive Message
Enter your choice : 2
a : Voting:2
Voting ACK
b (you) : Voting ACK
c : Voting ACK
This poll is sent from admin !
a : poll=p1:p2:p3:p4
vote=p1
b (you) : vote=p1
a : p1:1,p2:0,p3:0,p4:1
```

```
Run: CA x Server x SystemHandler x
Enter your choice : 3
Enter group ID you want to join : gp
1. Send Message
2. Receive Message
Enter your choice : 1
Voting:2
a (you) : Voting:2
b : Voting ACK
c : Voting ACK
All group members sent ACK !
poll=p1:p2:p3:p4
a (you) : poll=p1:p2:p3:p4
b : vote=p1
c : vote=p4
end poll
a (you) : end poll
p1:1,p2:0,p3:0,p4:1
```

```
Run: SystemHandler x
Enter your choice : 3
Enter group ID you want to join : gp
1. Send Message
2. Receive Message
Enter your choice : 2
a : Voting:2
b : Voting ACK
Voting ACK
c (you) : Voting ACK
This poll is sent from admin !
a : poll=p1:p2:p3:p4
vote=p4
c (you) : vote=p4
a : p1:1,p2:0,p3:0,p4:1
|
```

Version Control Run TODO Problems Terminal Endp

## روند اجرا:

پیام voting با flag=6 فرستاده می شود و سرور با دریافت این پیام بررسی می کند که آیا فرستنده پیام ادمین گروه می باشد یا خیر. اگر ادمین گروه باشد، لیست تمام اعضای گروه را برای او ارسال می کند و پیام voting را برای سایر اعضای گروه نیز broadcast می کند.

پیام voting ACK با flag=1 توسط سایر اعضای گروه فرستاده می شود و هنگامیکه همه اعضای گروه این پیام را ارسال کردند رای گیری شروع می شود.

پیام poll با flag=7 از طرف ادمین ارسال می شود.

اگر رویکرد شفافیت باشد، رای ها با flag=1 برای همه اعضای گروه فرستاده می شوند و در غیر اینصورت رای ها با رویکرد محرمانگی با flag=8 فقط برای ادمین گروه ارسال می شوند.