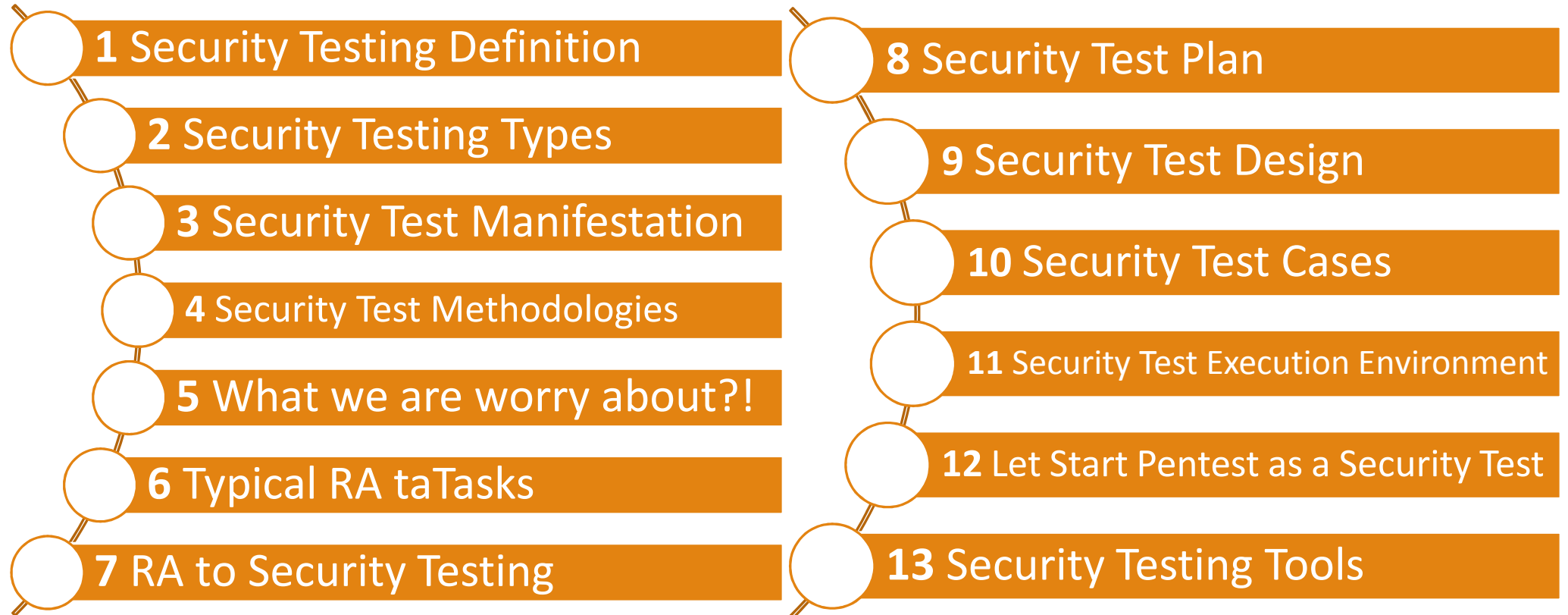


Software Security Testing

MAHDI SHABANI



Index

- 
- 1 Security Testing Definition
 - 2 Security Testing Types
 - 3 Security Test Manifestation
 - 4 Security Test Methodologies
 - 5 What we are worry about?!
 - 6 Typical RA taTasks
 - 7 RA to Security Testing
 - 8 Security Test Plan
 - 9 Security Test Design
 - 10 Security Test Cases
 - 11 Security Test Execution Environment
 - 12 Let Start Pentest as a Security Test
 - 13 Security Testing Tools

Security Testing Definition

- ❑ A process used to determine that the security features of a system **are implemented as designed** and that they are **adequate** for a proposed application environment.
- ❑ Verify and validate the **correctness** and **effectiveness** of security implementation

Security Testing Types

❑ Vulnerability scanning

- Various technics & tools
- Usually using automated tools
- Scan basic known vulnerabilities, known issues using known technics

❑ Security scanning

- Assessment manually
- Because tools are not 100% perfect
- Examining system responses, error messages, system logs

❑ Penetration scanning

- Real time simulation environment like mirror or images
- Black box, if white then im here, enter to where!!!

Security Testing Types

❑ Security auditing (to supplement security testing)

- Specific control for our compliance issues
- Usually compliance team are risk evaluating team
- procedural level and architectural level
- Often investigates areas that are difficult to test in a direct way, such as procedures, policies and controls

❑ Security review (to supplement security testing)

- Review standards, architecture diagrams
- Performing gap analysis

Security Test Manifestation

- ❑ Security requirement maturity
- ❑ Risk Assessment (Thread || Vulnerability || Cost)(output as input of...)
- ❑ Secure design review(Business Logic Testing)
- ❑ Application security test (SAST+DAST=IAST)

Security Test Methodologies

- ❑ Model-based security testing,(design model)
- ❑ Code-based testing and static analysis,(implementation)
- ❑ Penetration testing and dynamic analysis,(on running)
- ❑ Security regression testing (during maintenance)

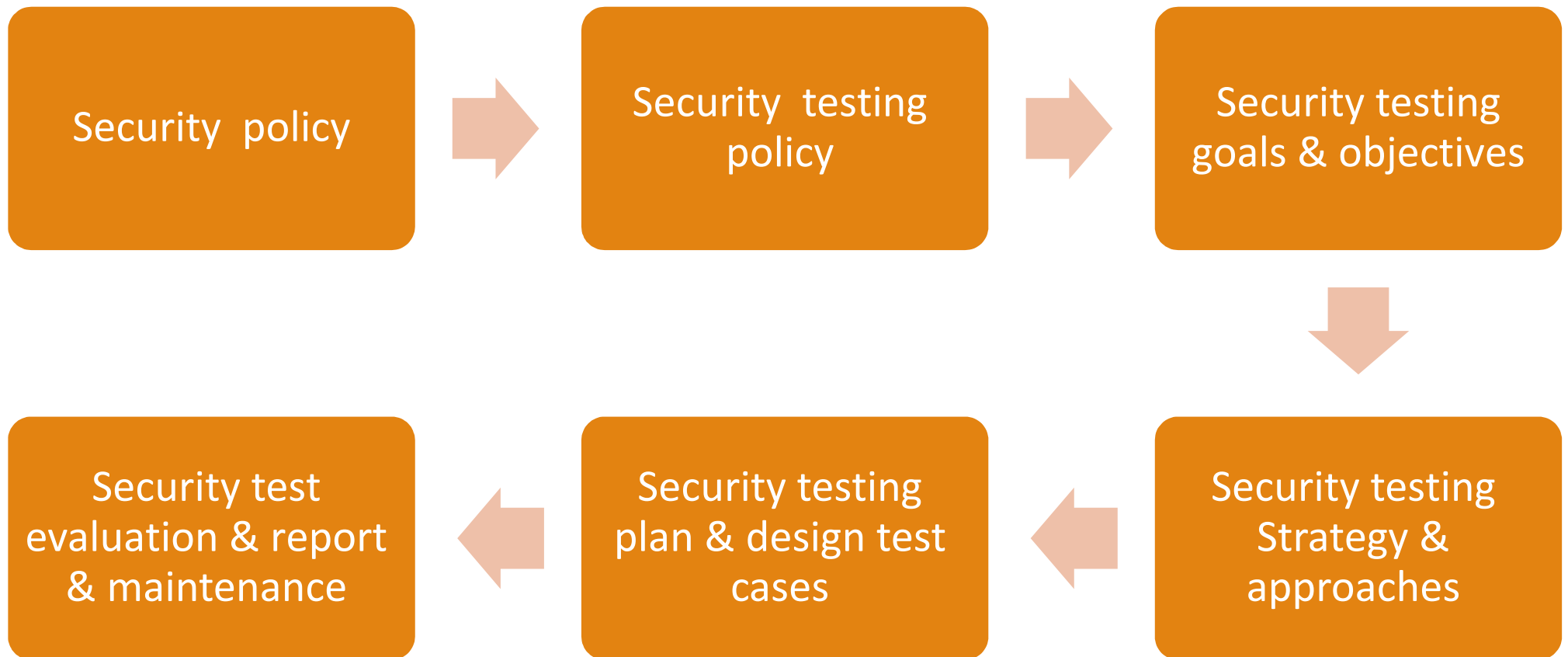
What we are worry about?!

- ❑ We need output of RA as input of Security test design
- ❑ We need output of asset assessment as input of RA through detect:
 - Assets
 - Value of assets
 - Location of assets
 - Access channel of assets
 - Assets protection controls (security establishment)
- ❑ We need security policy
- ❑ So we are worry about assets protection controls existence and efficiency and adequacy

Typical RA taTasks [NIST 88-30]

- ❑ Identify relevant threat sources
- ❑ Identify threat events from those sources
- ❑ Identify vulnerabilities could be exploited by those threat events
- ❑ Determine the likelihood successful threat events
- ❑ Determine the impacts and ranking process

RA to Security Testing



Security Test Plan

- ☐ Scope of the project
- ☐ Objectives
- ☐ Target market
- ☐ Assumptions
- ☐ Testing cycle start/end dates
- ☐ Major roles and responsibilities/overall resources
- ☐ Testing environment
- ☐ Deliverables
- ☐ Major risks and how to handle these risks
- ☐ Defect reporting and mitigation
- ☐ Testing end date
- ☐ To testing teams and other teams or stakeholders

Security Test Design

□ Security test attributes would be considered:

- Prioritized by identified security risks and threat models
- Traced to defined security requirements
- Defined based on the intended audience (developers, functional testers, security testers)
- Defined based on security defect profiles
- Designed to be automated, if applicable

Security Test Design

□ Rings of security test design :

- The security test approach (project level)
- Security test risks, threat models and requirements (project level)
- Security test design techniques (based on risks, requirements and application)
- Security test cases and scenarios

Security Test Design

□ Common security risks and vulnerabilities:

- Functional Security Controls
- Functional Access Controls
- Structural Access Controls
- Secure Coding Practices
- Operating System Access
- Language Vulnerabilities
- Platform Vulnerabilities (OS)
- External Threats
- Internal Threats

Security Test Cases

- ☐ Test data
- ☐ Procedures/inputs
- ☐ Scenarios
- ☐ Descriptions
- ☐ Testing environment
- ☐ Expected results
- ☐ Actual results

Security Test Execution Environment

☐ Isolated

☐ Complete

- Operating system (exact version and configuration)
- Networking
- Middleware
- Desktop (hardware brand, processor, memory)
- Mobile device (manufacturer, processor, memory, power management)
- Database
- Access rights
- Browsers and plug-ins
- Co-existing applications
- Data (engineered test data or production data that has been obfuscated)

☐ Restorable



Let Start Pentest as a Security Test

Our sample process

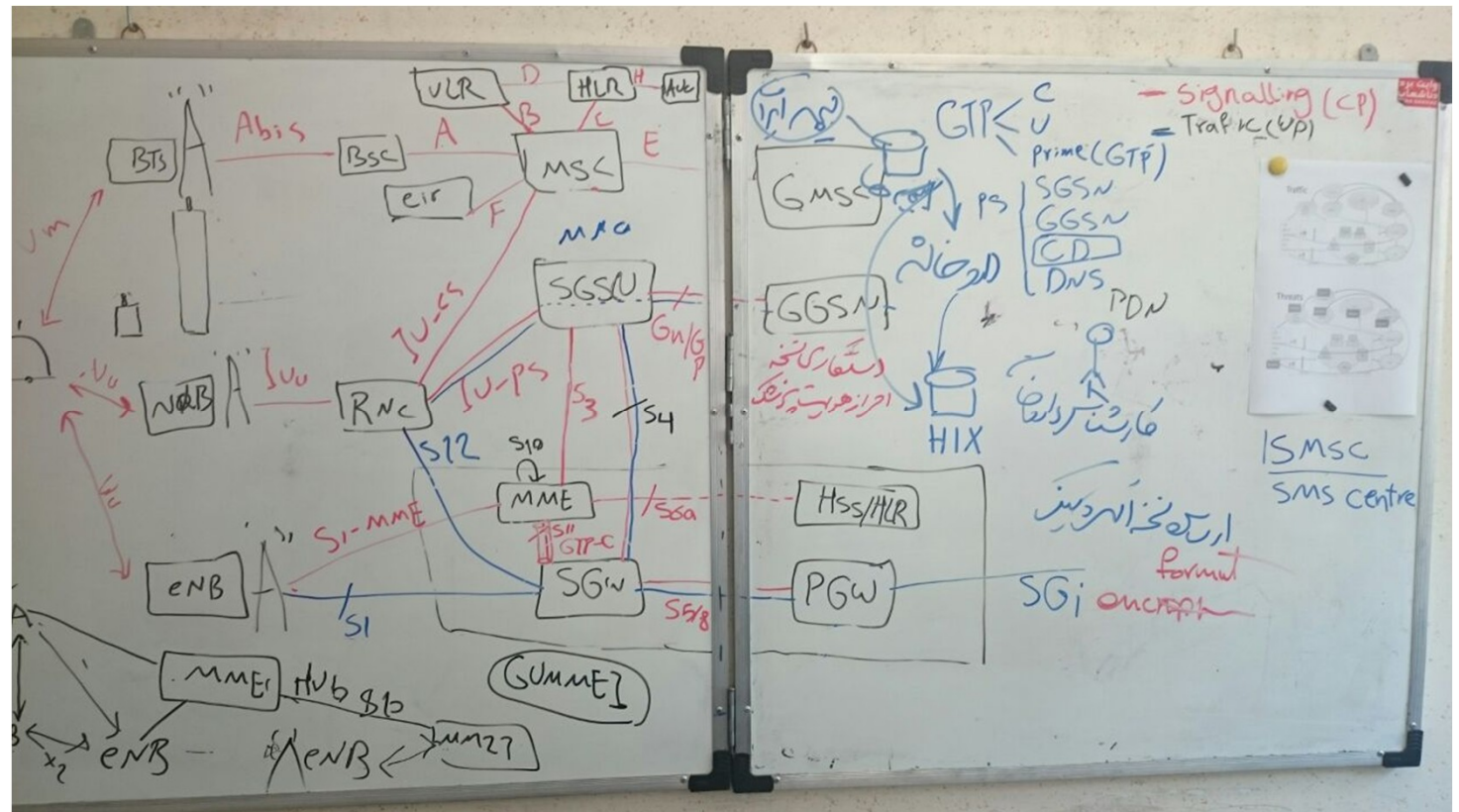
- ❑ Start sec test project and review meeting and taking brief
- ❑ Getting objective and goals and strategic view points
- ❑ Making security test plan
- ❑ Making security test design or choosing it from choices
 - Pre-engagement Interactions
 - Intelligence Gathering
 - Threat Modeling based on agile RA
 - Vulnerability Scanning & Analysis
 - Exploitation & Post Exploitation
 - Reporting
- ❑ Fire (Doing it in an isolated environment)



Security Test Design and Execution

Pre-engagement Interactions

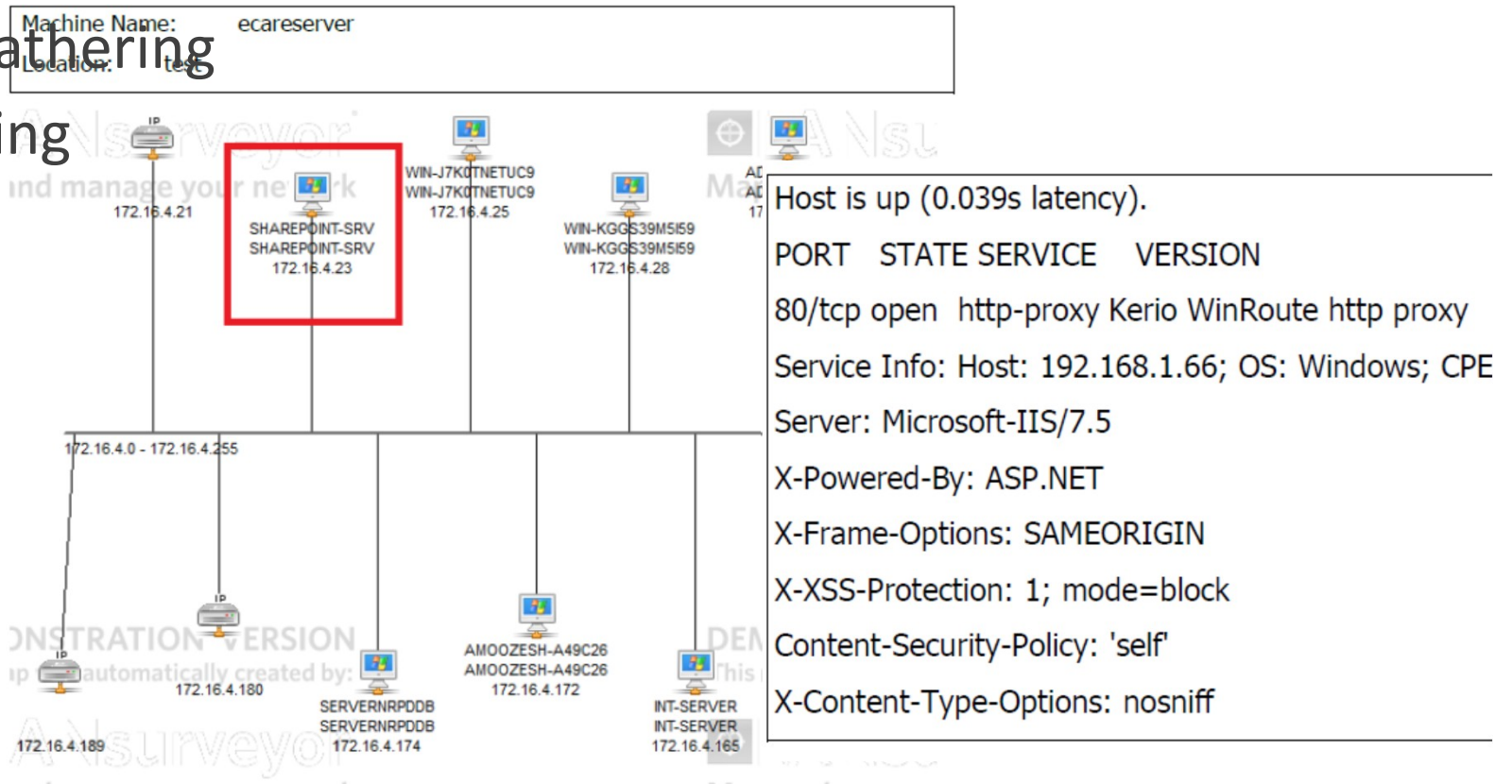
- Scope?
- Schedule?
- Blackbox or Whitebox?
- Contacts?



Security Test Design and Execution

☐ Intelligence Gathering

☐ Threat Modeling



Security Test Design and Execution

❑ Vulnerability Scanning & Analysis (Automated)

The screenshot displays the Subgraph Vega web security scanner interface. The main window is titled "VEGA" and "Open Source Web Security". The left sidebar shows a "Website View" and a "Scan Alerts" panel. The "Scan Alerts" panel lists various scan results, including a "High (4)" alert for "SQL Injection (http://172.16.4.141:8082/app/api/Shahr/GetData)". The main content area shows the details of this vulnerability, including a table with the following information:

AT A GLANCE	
Classification	SQL Injection
Resource	http://172.16.4.141:8082/app/api/Shahr/GetData
Parameter	
Method	GET
Detection Type	Blind Text Injection Differential
Risk	High

The "REQUEST" section shows the following GET request:

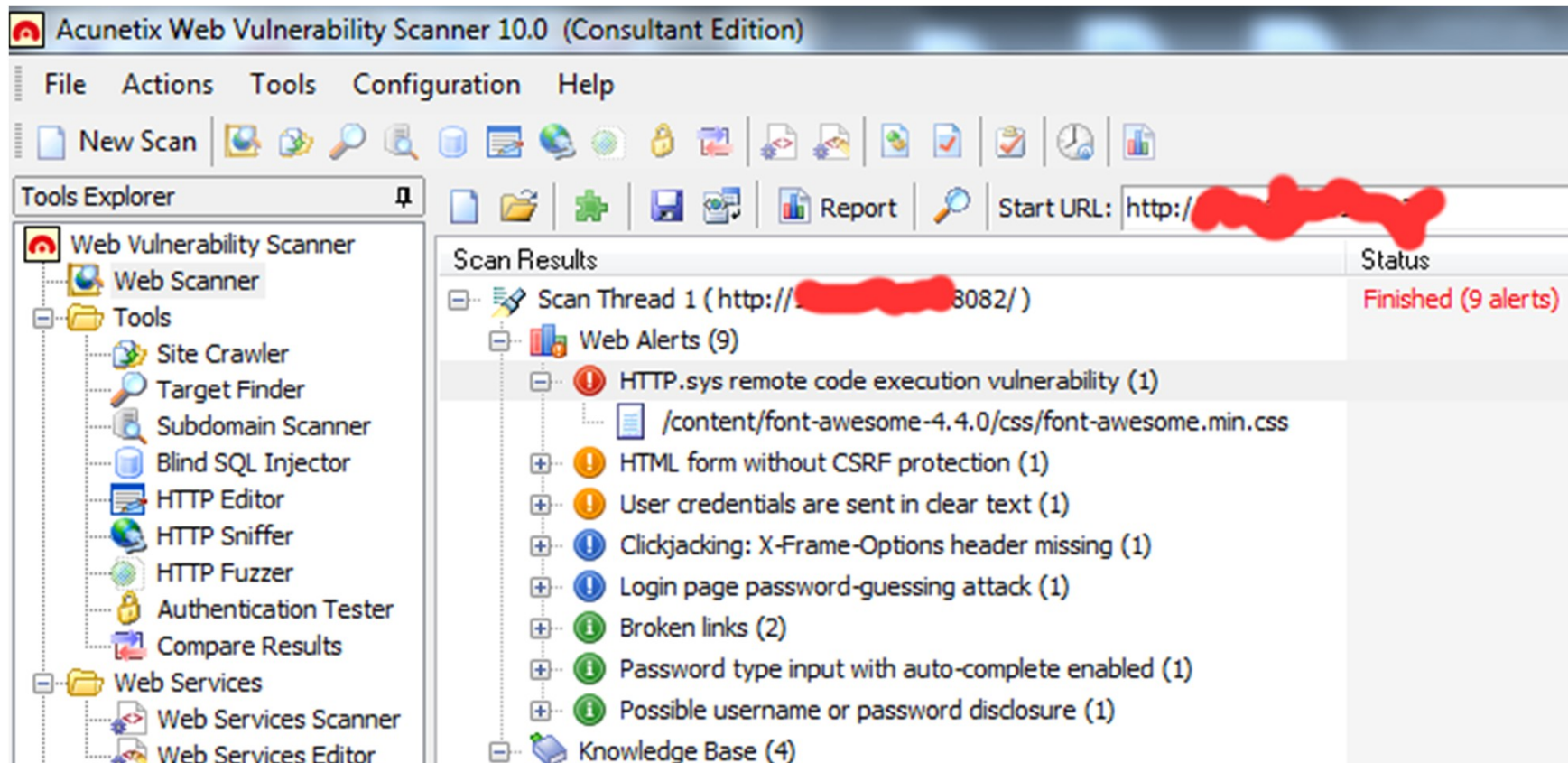
```
GET /app/api/Shahr/GetData?filter[logic]=and&filter[filters][0][field]=TaghsimatKeshvariId&filter[filters][0][operator]=eq""&filter[filters][0][value]=1088&OperationAccess[canView]=true&OperationAccess[canInsert]=true&OperationAccess[canUpdate]=true&OperationAccess[canDelete]=true&OperationAccess[canImport]=true&OperationAccess[canExport]=true&OperationAccess[canPrint]=true
```

The "RESOURCE CONTENT" section shows the following JSON response:

```
{"resultCode":0,"data":{"records":[{"ID":13018,"Onvan":"شهر ارطه","Noe":1,"Ta"}
```

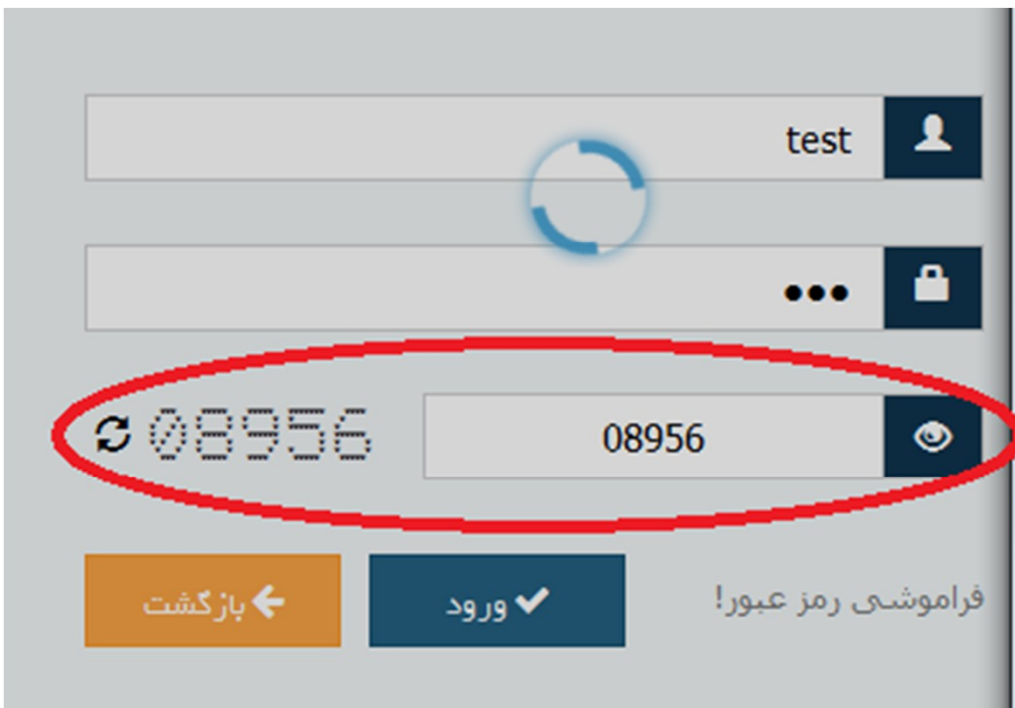

Security Test Design and Execution

❑ Vulnerability Scanning & Analysis (Automated)



Security Test Design and Execution

❑ Vulnerability Scanning & Analysis (Manualy)

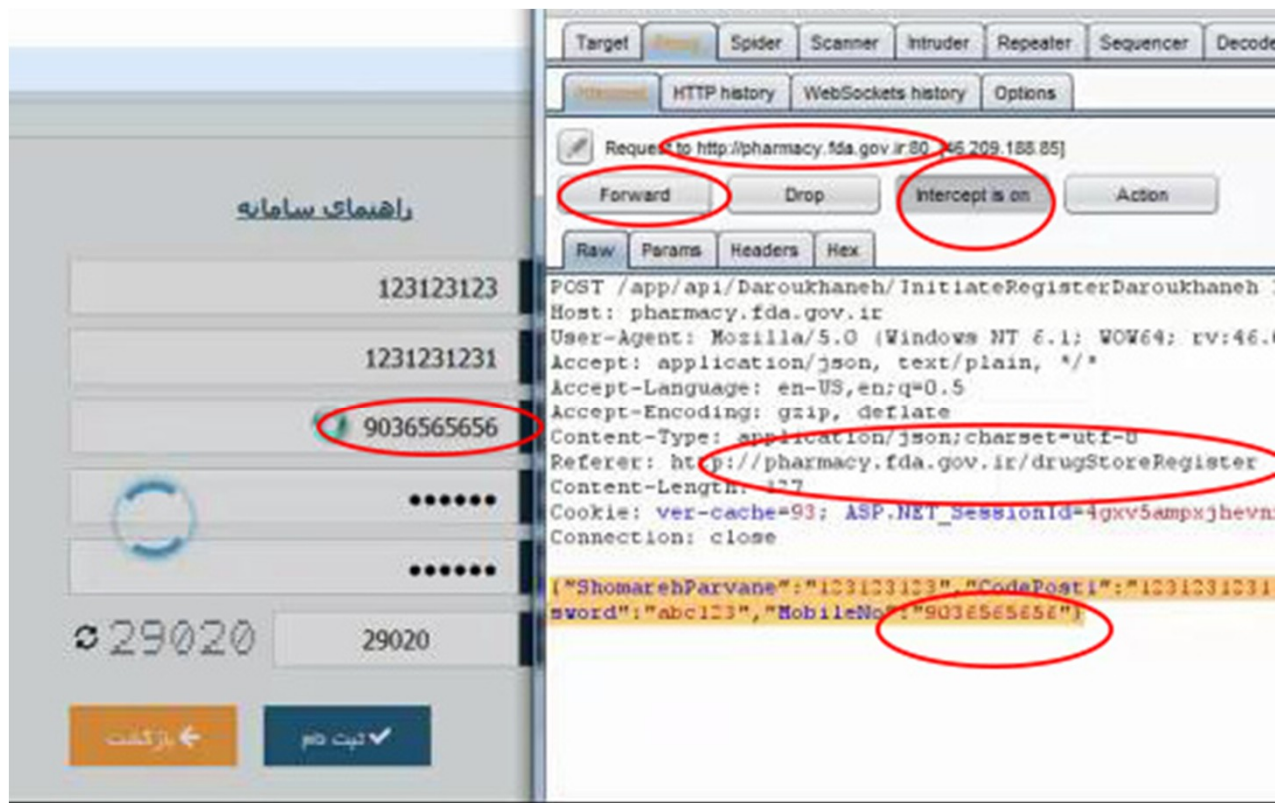


```
POST /app/api/Login/Login HTTP/1.1
Host: 172.16.4.141:8082
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; rv:46.0) G
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/json; charset=utf-8
Referer: http://172.16.4.141:8082/login
Content-Length: 36
Cookie: ver-cache=96; ver-cache=98; ASP.NET_SessionId=qakv
Connection: close
```

```
{"userName":"test","password":"123"}
```

Security Test Design and Execution

Exploitation



Security Test Design and Execution

Post Exploitation

The screenshot displays a web application response, likely from a REST client or browser's developer tools. The response is a JSON array of objects. Several fields and values are circled in red:

- `http://172.16.4.141:8082/dastourolamalArzeshyabiMain/196/2248/1065/1041`
- `Length: 1112`
- `ASP.NET_SessionId=x2nns`
- `SaatVoroud": "10:09", "SaatKhorouj": "12:22"`
- `"DarkhastID": "2248"`
- `"ID": "4290", "Porseshnameh": "یادداشت جدید"`
- `"ID": "4291", "Porseshnameh": "یادداشت جدید"`
- `"ID": "4292", "Porseshnameh": "یادداشت جدید"`
- `"ID": "4293", "Porseshnameh": "یادداشت جدید"`
- `"ID": "4294", "Porseshnameh": "یادداشت جدید"`
- `"ID": "4295", "Porseshnameh": "یادداشت جدید"`

The interface also shows tabs for "Response Data", "View Page", and "Structure Analysis". A search bar at the bottom right contains the text "Type a search term".

Security Test Design and Execution

Reporting

گزارش آزمون نفوذ پذیری سامانه ثبت الکترونیکی نسخه ها	
۴.۱.۴	آزمون متود های HTTP
۱۶	سایر آسیب پذیری های وب سرور و دیتابیس
۴.۱.۵	بررسی لاگ های سرور، پیامهای خطای سرور و ...
۴.۱.۵	بررسی سطح امتیازاتی که برنامه روی سرور با آن در حال اجرا است
۴.۱.۵	تلاش برای تحمیل بار اضافه به سرور جهت حملات منع سرویس
۴.۱.۵	تلاش برای ایلود فایل روی سرور
۴.۱.۵	بررسی امکان دسترسی به واسط مدیریتی وب سرور یا کاربران عادی
۴.۱.۷	آسیب پذیری های برنامه وب
۴.۱.۷	آزمون مدیریت هویت
۴.۲.۱	تعریف نقش ها
۴.۲.۱	فرایند ثبت کاربر
۴.۲.۱	مدیریت حساب های کاربری
۴.۲.۱	حدس پذیری حساب های کاربری
۴.۲.۱	گزاره ضعیف
۴.۲.۱	آزمون Authentication
۴.۲.۱	انتقال گواهی ها در کال رمز شده
۴.۲.۲	گواهی های پیشفرض
۴.۲.۲	مکانیزم مسدود کردن احراز هویت
۴.۲.۲	دور زدن اسکیمای احراز هویت
۴.۲.۲	یادآوری رمز عبور
۴.۲.۲	حفاظت پنهن مرورگر
۴.۲.۲	مکانیزم تغییر و فراموشی رمز عبور
۴.۲.۲	آزمون Authorization
۴.۲.۲	

گزارش آزمون نفوذ پذیری سامانه ثبت الکترونیکی نسخه ها		
بررسی آسیب پذیری ها در مدیریت حساب های کاربری		
شرح وضعیت	نوع آزمون	میزان مخاطره
سیستم قادر به دسترسی به بخش مدیریت نقش ها می باشد.	دستی	فاقد مخاطره
امکان تغییر نقش کاربر مانند سایر درخواست های مدیریتی تنها برای قابل دسترس خواهند بود و این موضوع در هر درخواست چک می	دستی	فاقد مخاطره
نظام قادر به ویرایش نقش خود و ارتقای آن نمی باشند و در صورت تغییر نقش خود توسط یک کاربر عادی پاسخ زیر برمی گردد: User: شما به منبع با نام نقشها و کد: "serviceResponse:{success:false,message:View}} (دسترسی نداریدView	دستی	فاقد مخاطره
مدیر سیستم می تواند به کاربران دیگر مانند کاربران داروخانه نیز عطا نماید.	دستی	کم
نقش مدیر می تواند نقش دیگر کاربران مدیر را نیز ویرایش نماید.	دستی	کم
سیستم می تواند نقش خود را به کاربر عادی تغییر دهد.	دستی	کم
مدیر کاربر اطلاعات حساب وی حذف شده و منتقل نمی شود.	دستی	متوسط
بروج کاربر مدیر سیستم از سامانه و قبل از ورود جدید درخواست کاربر برای یک کاربر محدود توسط مهاجم قبل از ابطال شناسه ت گیرد از تقای نقش کاربر با موفقیت انجام می شود. serviceResponse:{success:true}}	دستی	کم

گزارش آزمون نفوذ پذیری سامانه ثبت الکترونیکی نسخه ها		
۴.۲.۳.۴ دسترسی مستقیم غیر امن به منابع		
آزمون Authorization بررسی آسیب پذیری ها در دسترسی مستقیم غیر امن به منابع		
شرح وضعیت	نوع آزمون	میزان مخاطره
در برنامه لینک دسترسی به اکثر صفحات و منو ها مشابه هم است و تنها در یک پارامتر با هم متفاوت است. با این حال در صورت درخواست لینکی که کاربر مشاخر با نقش خود به آن دسترسی ندارد، صفحه لاگین نمایش داده می شود. (جدول یک)	دستی	فاقد مخاطره
پارامتر مورد اشاره برای هر یک از بخش های سایت در جدول زیر آمده است.	دستی	فاقد مخاطره
یک کاربر با نقش مدیر سیستم می تواند نقش کلیه کاربران از جمله دیگر کاربران مدیر سیستم و گروه مدیریت را تغییر دهد.	دستی	متوسط
کاربران گروه مدیریت با فراخوانی url مدیریت سامانه و امنیت، امکان تغییر نقش خود و دیگران به مدیر سیستم را دارند. در این حالت منوهایی که تا پیش از این برایشان نمایش داده نمی شد نشان داده می شود.	دستی	متوسط

جدول یک

منو	زیرمنو	لینک
	بیمه های طرف قرارداد	http://pharmanet.ava-salamat.ir/fw/extlist.aspx?entity=DepartmentInsurers
	اطلاعات بیماران	Patient
	اطلاعات پزشکان	Doctor

Security Testing Tools

❑ Vulnerability Scanning

- ISS, Foundscan, Nessus, Nikto

❑ Penetration Testing (Black Box Testing)

- Webinspect, Appscan, Hailstorm, Paros, Peach

❑ Binary Analysis/Reverse Engineering

- IDA Pro, @stake SmartRisk

❑ Source Code Analysis

- Fortify, Klockworks, Parasoft, Free Tools (e.g. FindBugs)

❑ Threat Modeling

- MS TAM, TRIKE, PTA Technologies

❑ Rootkit BackDoor Analysis

- rootkits.org and rootkit.nl

Q & A

Mh.shaabani@gmail.com

