

**جامعة جيلان**

الكلية التقنية

العنوان:

**اكتشاف الثغرات الأمنية في الخدمات والمواقع الإلكترونية  
التابعة لجامعة جيلان واختبار الاختراق عليها**

الأستاذ المشرف:

**د. حميد رضا احمدى فر**

الطالب:

**أدهم السعدي**

## 1-1- المقدمة

- اختبار الاختراق (Penetration test) هو وسيلة لتقييم مستوى أمان جهاز الحاسوب (خادم عادةً) أو شبكة ما عن طريق محاكاة هجمات بواسطة مختبر اختراق (الذي لا يملك تصريح للوصول). في هذه الطريقة ، يتم اختبار جميع الأنظمة والبرامج والخدمات المثبتة على الشبكة للعثور على المشاكل الأمنية ومن ثم تقديم الحلول المناسبة لهذه المشاكل .

## 1-2- أهداف المشروع

- فحص الخدمات الداخلية و الموقع الالكتروني [guilan.ac.ir](http://guilan.ac.ir) ، واكتشاف الثغرات الأمنية وشرح جميع الأخطاء ونقاط الضعف الموجودة ، واقتراح حلولاً أمنية لإصلاح هذه الثغرات .

## 1-3- المتطلبات الأساسية

- إتقان عالي لنظام التشغيل لينكس
- نظام تشغيل لينكس توزيعه اختبار اختراق (التوزيعه المستخدمة kali linux)
- الإلمام بأدوات تحليل برامج الويب Web Application Analysis
- + لغات البرمجة النصية php , python , javascript , html , bash و غيره
- معرفة بالثغرات الأمنية

## 1-2- شرح الأنشطة المنجزة

- بدأ اختبار الاختراق بتاريخ 2021/2/25 على طريقة الصندوق الأسود (Black Box) وانتهى بتاريخ 2021/3/2 .
- أولاً نحصل على معلومات شاملة من الموقع ونحدد حالة المنافذ. للقيام بذلك نحتاج إلى برامج خاصة ، مثل أداة Nmap .

### ❖ خصائص أداة - Network mapper - Nmap :

- كشف المضيفين على الشبكة (بناءً على استجابة ping أو منفذ ما مفتوح)
- فحص المنافذ
- تحديد نسخة البرامج والخدمات
- تشخيص نظام التشغيل
- التفاعل البرمجي مع الهدف : باستخدام NSE<sup>1</sup> (المحرك البرمجي لـ Nmap) و لغة البرمجة Lua
- تستطيع Nmap توفير معلومات أكثر عن الأهداف ، تتضمن أسماء DNS<sup>2</sup> العكسية ، وأنواع الأجهزة، وعناوين MAC<sup>3</sup>

---

<sup>1</sup> Nmap Scripting Engine

<sup>2</sup> Domain Name System

<sup>3</sup> Media Access Control

- أولاً نقوم بجمع المعلومات المطلوبة ، وتشمل هذه المعلومات مواصفات الخادم ، والمنافذ المفتوحة (tcp & udp) ، والخدمات المقدمة ، وإصدارات البرامج المثبتة ، وما إلى ذلك .

- لتحديد نظام التشغيل يمكننا استخدام الأمر التالي:

**\$ sudo nmap -O guilan.ac.ir**

```
(aks@kali)-[~]
└─$ sudo nmap -O guilan.ac.ir
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-25 14:32 +0330
Nmap scan report for guilan.ac.ir (89.144.141.141)
Host is up (0.0094s latency).
rDNS record for 89.144.141.141: www.guilan.ac.ir
Not shown: 997 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
Device type: general purpose
Running (JUST GUESSING): Linux 3.X|4.X|2.6.X (98%)
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4.9 cpe:/o:linux:linux_kernel:2.6.39
Aggressive OS guesses: Linux 3.10 - 3.16 (98%), Linux 4.9 (97%), Linux 2.6.39 (93%), Linux 3.10 (92%), Linux 2.6.32 (92%), Linux 4.0 (92%), Linux 4.4 (92%), Linux 3.10 - 3.12 (91%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.98 seconds
```

نتيجة (١)

- لجمع المزيد من المعلومات ، نقوم بفحص الهدف بعناوين IP خارجية وداخلية ، وفي النتائج التالية سنرى الفرق في المخرجات .

- يتم تحديد المنافذ والخدمات المثبتة باستخدام هذه التعليمات

**\$ sudo nmap -sU -sT -p0-65535 guilan.ac.ir (by external ip)**

```
(aks@kali)-[~/sparta]
└─$ sudo nmap -sU -sT -p0-65535 guilan.ac.ir
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-25 15:00 +0330
Nmap scan report for guilan.ac.ir (89.144.141.141)
Host is up (0.025s latency).
Not shown: 65533 filtered ports, 65530 open|filtered ports
PORT      STATE SERVICE
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  https
520/udp   closed route
1144/udp  closed fuscrypt
2000/udp  closed cisco-sccp
3784/udp  closed bfd-control
3799/udp  closed radius-dynauth
8014/udp  closed unknown

Nmap done: 1 IP address (1 host up) scanned in 249.26 seconds
```

نتيجة (٢)

**\$ sudo nmap -sV guilan.ac.ir (by internal ip)**

```
Nmap scan report for guilan.ac.ir (192.168.8.13)
Host is up (0.023s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
80/tcp    open  http
113/tcp   closed ident
443/tcp   open  ssl/https
2000/tcp  open  tcpwrapped
5060/tcp  open  tcpwrapped
5432/tcp  closed postgresql
8080/tcp  open  http-proxy
```

نتيجة (٣)

- التحقق من مخدم الإنترنت الخاص بالجامعة net.guilan.ac.ir

### tcp منافذ

```
(aks@kali)-[~]
$ sudo nmap -sV 172.19.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-28 02:57 +0330
Stats: 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 66.67% done; ETC: 02:58 (0:00:11 remaining)
Nmap scan report for net.guilan.ac.ir (172.19.0.1)
Host is up (0.029s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE        VERSION
53/tcp    open  domain         (generic dns response: NOTIMP)
1723/tcp  open  pptp           MikroTik (Firmware: 1)
2000/tcp  open  bandwidth-test MikroTik bandwidth-test server
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.91%I=7%D=2/28%Time=603AD591P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,E,"%0\x0c\x06\x81\x84\x00\x00\x00\x00");
MAC Address: 4C:5E:0C:63:AB:DE (Routerboard.com)
Service Info: Host: CCR3

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 60.23 seconds
```

### udp منافذ

```
(aks@kali)-[~]
$ sudo nmap -sU 172.19.0.1
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-28 03:01 +0330
Nmap scan report for net.guilan.ac.ir (172.19.0.1)
Host is up (0.0010s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
53/udp    open  domain
67/udp    open|filtered dhcp
123/udp   open|filtered ntp
161/udp   open|filtered snmp
MAC Address: 4C:5E:0C:63:AB:DE (Routerboard.com)

Nmap done: 1 IP address (1 host up) scanned in 65.38 seconds
```

نتيجة (٤)

## 2-2- تحديد الثغرات في المواقع المستهدفة :

- بعد عملية اكتشاف نظام التشغيل و إصدارات البرامج والخدمات المثبتة على الخادم ، ننتقل إلى أدوات الويب ، ومن أشهرها أداة Vega . وهي عبارة عن ماسح يستخدم لاختبار الاختراق ويمكن أن يكون مفيدًا لإعداد الموقع من قبل المسؤول .

### ❖ مميزات أداة vega :

- فحص مدخلات GET من موقع الويب المطلوب.
- فحص مدخلات POST من موقع الويب المطلوب.
- اختبار بعض الهجمات التي تستهدف الServer.
- العثور على ثغرات مثل : Cross site scripting XSS directory ، sql injection ، HTTP Headers ، remote file injection ، check ، وغيره.
- تقسيم الثغرات الأمنية إلى أربعة مستويات :  
1-High      2-Medium      3-low      4-info
- لفحص الموقع المطلوب ، يكفي أن يكون لديك عنوان الموقع.

### ❖ المتطلبات الأساسية للأداة :

- Java jdk > 8.0
- Java jre > 8.0
- libwebkitgtk-1.0-0 (Web content engine library for GTK+)

## فحص ثغرات النطاق guilan.ac.ir

The screenshot shows the Subgraph Vega application interface. The 'Website View' pane on the left lists several domains including guilan.ac.ir, lms.guilan.ac.ir, www.guilan.ac.ir, and others. The 'Scan Alerts' pane shows a list of alerts for the selected domain, categorized by severity (High, Medium, Low, Info). The 'Scan Info' pane on the right displays a 'Scan Alert Summary' table.

Severity	Alert Type	Count	Total Found
High	SQL Injection	2	(8 found)
	Page Fingerprint Differential Detected - Possible XPath Injection	6	
Medium	Certificate signed using SHA-1 Client Ciphersuite Preference	1	(2 found)
		1	
Low	Email Addresses Found	5	(7 found)
	Form Password Field with Autocomplete Enabled	2	
Info	Self-Signed Certificate	1	(142 found)
	Interesting Meta Tags Detected	83	
	Cookie HttpOnly Flag Not Set	3	
	Blank Body Detected	55	

Scan Alert Summary			
High			(8 found)
SQL Injection	2		
Page Fingerprint Differential Detected - Possible XPath Injection	6		
Medium			(2 found)
Certificate signed using SHA-1 Client Ciphersuite Preference	1		
	1		
Low			(7 found)
Email Addresses Found	5		
Form Password Field with Autocomplete Enabled	2		
Info			(142 found)
Self-Signed Certificate	1		
Interesting Meta Tags Detected	83		
Cookie HttpOnly Flag Not Set	3		
Blank Body Detected	55		

نتيجة (٥)



## 3-2- تعريف الثغرات التي تم العثور عليها :

### 1. ثغرة (High) SQL Injection

- يحدث هذا الهجوم عن طريق إدخال كود SQL في قاعدة البيانات من خلال المدخلات . منطق هذا الخطأ هو أن يتم استخراج معلومات قاعدة البيانات بواسطة استعلام ضار . في هذا الخطأ يمكننا قراءة معلومات قاعدة البيانات عن طريق بعض أساليب (UNION SELECT). هذا الخطأ موجود في جميع قواعد البيانات مثل MariaDB و Microsoft SQL و Oracle و Mysql و غيرها ، وهذه الثغرة الأمنية لا علاقة لها بضعف قاعدة البيانات هذه ، ولكنها ناتجة عن أخطاء المبرمج في PHP و ASP و لغات الويب والخادم الأخرى ، وفي بعض الأحيان ، في حال وجود تكوينات غير قياسية للخادم تجعل هذه المشكلة موقع الويب أكثر عرضة للخطر وتسمح للمستخدم بتعيين مقادير قاعدة البيانات وتنفيذها من خلال الإدخال .
- أغراض هذه الثغرة مختلفة ، يمكنك فعل أي شيء تقريباً عندما يمكنك تنفيذ أوامر قاعدة البيانات عبر URL . مثل الوصول إلى أسماء المستخدمين وكلمات المرور الخاصة بالمسؤول والمستخدمين ، والوصول إلى محتوى الموقع وتعديله وما إلى ذلك .

## SQL Injection

### ▶ AT A GLANCE

Classification	Input Validation Error
Resource	<a href="https://guilan.ac.ir/search">https://guilan.ac.ir/search</a>
Parameter	_3_INSTANCE_r4iLfdAc3jb_keywords
Method	GET
Detection Type	Blind Arithmetic Evaluation Differential
Risk	High

### ▶ REQUEST

```
GET /search?p_p_id=3_INSTANCE_r4iLfdAc3jb&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=1&_3_INSTANCE_r4iLfdAc3jb_struts_action=/search/search&_3_INSTANCE_r4iLfdAc3jb_assetCategoryId=&_3_INSTANCE_r4iLfdAc3jb_keywords=%20%20%20-%20-
```

### ▶ RESOURCE CONTENT

```
<!DOCTYPE html> <html class="rtl" dir="rtl" lang="fa-IR" locale="fa" test="fa_IR"> <head> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" cor
```

### ▶ DISCUSSION

Vega has detected a possible SQL injection vulnerability. These vulnerabilities are present when externally-supplied input is used to construct a SQL query. If precautions are not taken, the externally-supplied input (usually a GET or POST parameter) can modify the query string such that it performs unintended actions. These actions include gaining unauthorized read or write access to the data stored in the database, as well as modifying the logic of the application.

### ▶ IMPACT

- » Vega has detected a possible SQL injection vulnerability.
- » These vulnerabilities can be exploited by remote attackers to gain unauthorized read or write access to the underlying database.
- » Exploitation of SQL injection vulnerabilities can also allow for attacks against the logic of the application.
- » Attackers may be able to obtain unauthorized access to the server hosting the database.

## SQL Injection

### ▶ AT A GLANCE

Classification	Input Validation Error
Resource	<a href="https://guilan.ac.ir/show-content">https://guilan.ac.ir/show-content</a>
Parameter	p_p_lifecycle
Method	GET
Detection Type	Blind Text Injection Differential
Risk	High

### ▶ REQUEST

```
GET /show-content/?p_p_id=101_INSTANCE_lxbuSsEUUOQ5&p_p_lifecycle=0"%20UNION%20SELECT%20%2C%20table_name%2C%20'vega"%20FROM%20information_schema.tables%20WHERE%20table_1&p_p_col_count=1&_101_INSTANCE_lxbuSsEUUOQ5_struts_action=/asset_publisher/view
```

### ▶ DISCUSSION

Vega has detected a possible SQL injection vulnerability. These vulnerabilities are present when externally-supplied input is used to construct a SQL query. If precautions are not taken, the externally-supplied input (usually a GET or POST parameter) can modify the query string such that it performs unintended actions. These actions include gaining unauthorized read or write access to the data stored in the database, as well as modifying the logic of the application.

### ▶ IMPACT

- » Vega has detected a possible SQL injection vulnerability.
- » These vulnerabilities can be exploited by remote attackers to gain unauthorized read or write access to the underlying database.
- » Exploitation of SQL injection vulnerabilities can also allow for attacks against the logic of the application.
- » Attackers may be able to obtain unauthorized access to the server hosting the database.

نتیجه (٦)

## 2. ثغرة (High) XPATH Injection

- يتم تنفيذ هذا الهجوم على مستندات XML ؛ أمر XPATH هو أمر مستخدم في مستندات XML وهو مفيد جدًا للبحث والعثور على البيانات في ملفات XML . تحدث هجمات XPath Injection المشابهة لـ SQL Injection عندما يستخدم موقع الويب المعلومات التي يحتاجها المستخدم لإنشاء استعلام XPath لبيانات XML .
- من خلال تقديم معلومات غير صحيحة إلى موقع الويب ، يمكن للمهاجم معرفة كيفية إنشاء بيانات XML أو الوصول إلى البيانات التي قد لا يكون لديه حق الوصول إليها عادةً ، حتى في حال استخدام بيانات XML للمصادقة يمكن للمهاجم زيادة مستوى الوصول إلى الموقع .

### Page Fingerprint Differential Detected - Possible XPath Injection

#### ▶ AT A GLANCE

Classification	Error Message
Resource	/search
Parameter	_3_INSTANCE_r4ilfkAc3jb_assetCategoryIds
Method	GET
Detection Type	XPath 2.0 Blind Injection Differential Checks
Risk	High

#### ▶ REQUEST

GET /search?p\_p\_id=3\_INSTANCE\_r4ilfkAc3jb&p\_p\_lifecycle=0&p\_p\_state=normal&p\_p\_mode=view&p\_p\_col\_id=column-1&p\_p\_col\_count=1&\_3\_INSTANCE\_r4ilfkAc3jb\_struts\_action=/search/search&\_3\_INSTANCE\_r4ilfkAc3jb\_assetCategoryIds=e"%20or%201%20eq%201%20or%20"a"%20=%20"a&

#### ▶ DISCUSSION

Vega has detected a different response page fingerprint in relation to an XPath injection request. This means that the response page content returned by the web application has a different signature from that returned by an ordinary request, which may indicate the existence of an XPath injection vulnerability. The differing page fingerprint may include error messages or indicate a state change in the application in response to the XPath injection attempt made by Vega. Developers should examine the response content and underlying code to verify whether or not a vulnerability is present. If the vulnerability exists and precautions are not taken, depending on the nature of the affected XPath query, such a vulnerability could allow attackers to bypass authentication or gain unauthorized access to sensitive XML data.

#### ▶ IMPACT

- » Vega has detected a different response fingerprint in relation to an XPath injection attempt.
- » This may indicate an XPath injection vulnerability, though this is not confirmed.
- » If this is due to an XPath vulnerability, depending on the nature of the XPath query, exploitation could allow attackers to bypass authentication or gain unauthorized access to sensitive XML data.

نتيجة (V)

### 3. ثغرة certificate signed using SHA-1 (Medium)

- تستخدم Git في هيكلها وظيفته تكامل SHA-1 ليس لأجل الحماية ، ولكن لضمان عدم تغيير البيانات. وبالطبع ، فإن Git ناجحة للغاية مع هذه الخوارزمية لدرجة أنه على سبيل المثال ، إذا قمت بتخزين البيانات فيها وبعد 5 سنوات أردت إلقاء نظرة على بياناتك ، فسترى أن البيانات مضمونة بأنها لم تتغير .

#### تحليل وتقييم التشفير

- عندما يكون لدينا ملخص لرسالة بطول  $L$  ، يمكننا في كثير من الأحيان مهاجمة وكشف الرسالة المشفرة من نفس الطول مع تعقيد  $2^L$  بواسطة هجوم Brute Force ، يسمى هذا الهجوم أيضاً بـ Attack Preimage ، والتي يمكن أن تكون مستقلة حتى عن طول الرسالة أو الظروف الحسابية للهجوم .
- المسألة الثانية المطروحة هنا هي العثور على خوارزميتي تشفير مختلفة ينتج عنهما ملخص رسالة . ونقول في مثل هذه الحالات ، أنه حدث تصادم والوقت المطلوب لاكتشافه من المرتبة  $2^{L/2}$  .

#### Certificate signed using SHA-1

AT A GLANCE

Classification  
Risk

Configuration  
Medium

DISCUSSION

Vega detected a certificate signed using SHA-1. SHA-1 is a hash algorithm used in digital signatures. It is currently considered deprecated due to the increasing feasibility in breaking it.

IMPACT

- » Certificates can be forged by capable adversaries.
- » Forged certificates can be used in MITM attacks against connecting clients.

REMEDiation

- » Renew certificates with SHA-256 signatures.
- » This should be done before 2016.

REFERENCES

Some additional links with relevant information published by third-parties:

- » [SHA-1 \(Wikipedia\)](#)
- » [HTTPS \(Wikipedia\)](#)

نتيجة (٨)

## 4. ثغرة (Medium) client cipher suite preference

- يتمثل أحد أهم أجزاء تكوين SSL / TLS في تعطيل الخوارزميات الضعيفة و CipherSuites بطريقة تتيح أيضًا تمكين Forward secrecy لضمان توفير الأمان. إذ أن مستعرضات المستخدم قد تختار مجموعات تشفير أقل أمانًا مما يخلق فرصًا للهجوم .

### Client Ciphersuite Preference

AT A GLANCE

Classification  
Risk

Configuration  
Medium

DISCUSSION

The server can override client ciphersuite prioritization during the TLS handshake. This is useful for enforcing better, more secure ciphersuites for all visiting clients. Vega has detected that this is not configured in the server, potentially leaving older clients at risk.

IMPACT

» User browsers may select less secure cipher suites creating opportunities for attack.

REMEDIATION

» HTTPS server should be configured to enforce server ciphersuite preferences. How this is configured will vary by server.  
» Mozilla has included guidelines for configuring server ciphersuite preference for various implementations. See link below.

REFERENCES

Some additional links with relevant information published by third-parties:

→ [Server Side TLS \(Mozilla\)](#)

→ [HTTPS \(Wikipedia\)](#)

نتيجة (٩)

## 5. ثغرة (Low) Form Password Field with Autocomplete Enabled

- اكتشف Vega نموذجًا يتضمن حقل إدخال كلمة المرور . لم يتم ضبط سمة الإكمال التلقائي على وضع الإيقاف . قد يؤدي ذلك إلى قيام بعض المتصفحات بتخزين مدخلات القيم من قبل المستخدمين محليًا حيث يمكن استردادها بواسطة جهات خارجية .

### Form Password Field with Autocomplete Enabled

#### ▶ AT A GLANCE

Classification  
Resource  
Risk

Environment  
/staff/  
Low

#### ▶ REQUEST

GET /staff/

#### ▶ DISCUSSION

Vega detected a form that included a password input field. The autocomplete attribute was not set to off. This may result in some browsers storing values input by users locally, where they may be retrieved by third parties.

#### ▶ IMPACT

- » A password value may be stored on the local filesystem of the client.
- » Locally stored passwords could be retrieved by other users or malicious code.

#### ▶ REMEDIATION

- » The form declaration should have an autocomplete attribute with its value set to "off".

نتيجة (١٠)

# فحص النطاق الفرعي **erp.guilan.ac.ir**

Subgraph Vega

File Scan Window Help

Website View

- apmsrt.ir
- Archart.guilan.ac.ir
- Azadandishi.guilan.ac.ir
- blog.zimbra.com
- cads2020.guilan.ac.ir
- ce.guilan.ac.ir
- cert.guilan.ac.ir
- Cobze.guilan.ac.ir

Scan Alerts

- Form Password Field with Autocomplete Enabled (2)
- Info (141)
- https://www.guilan.ac.ir (3)
- Medium (2)
  - Certificate signed using SHA-1 (https://www.guilan.ac.ir)
  - Client Ciphersuite Preference (https://www.guilan.ac.ir)
- Info
- 06/02/2020 10:33:27 [Completed] (103)**
- https://erp.guilan.ac.ir (103)
  - High
    - Page Fingerprint Differential Detected - Possible Local File Include
  - Low (26)
    - ASP/ASPX Error Detected (26)
  - Info (76)

VEGA

Scan Alert Summary

Severity	Alert	Count
High	Page Fingerprint Differential Detected - Possible Local File Include	1
Medium		(None found)
Low	ASP/ASPX Error Detected	26
Info	X-Frame-Options Header Not Set	75
Info	Possible AJAX code detected	1

Identities

Proxy is not running 458M of 769M

## 6. ثغرة (High) Local File Include

- يحدث خطأ LFI ، والذي يرمز إلى local file inclusion ، عندما يستخدم مطور الموقع وظائف مثل include لاستدعاء صفحات الويب ولا يقوم بتصفية الأحرف غير المصرح بها مثل (.) و (/) .
- في هذه الحالة ، يمكن للمهاجم الوصول إلى ملف مهم مثل: / passwd / etc / والذي يحتوي على أسماء المستخدمين وكلمات المرور الخاصة بالموقع .

### Page Fingerprint Differential Detected - Possible Local File Include

#### ▶ AT A GLANCE

Classification	Error Message
Resource	/Dashboard.aspx
Parameter	param
Method	GET
Risk	High

#### ▶ REQUEST

GET /Dashboard.aspx?param=../

#### ▶ RESOURCE CONTENT

```
<html><head><title></title></head><body style="background-color:#fff;"><div style="width:400px; height:400px;background-color:#fff; margin:0 auto;
```

#### ▶ DISCUSSION

Vega has detected a different response page fingerprint in relation to a local file include injection request. This means that the response page content returned by the web application has a different signature from that returned by an ordinary request, which may indicate the existence of a local file include vulnerability. Local file include vulnerabilities are present when externally-supplied input is used to specify the location of a local filesystem resource that is requested by the web application. The differing page fingerprint may include error messages or indicate a state change in the application in response to the local file include injection attempt made by Vega. Differing responses may also be indicative of a file enumeration vulnerability, which would allow an attacker to determine if specific files exist on the system. Developers should examine the response content and underlying code to verify whether or not a vulnerability is present. If the vulnerability exists and precautions are not taken, such a vulnerability could allow attackers to gain unauthorized access to sensitive information contained in local files, which may also be leveraged in further attacks on the web application.

#### ▶ IMPACT

- » Vega has detected a different response fingerprint in relation to a local file include injection attempt.
- » This may indicate a local file include vulnerability, though this is not confirmed.
- » If this is due to a local file include vulnerability, exploitation of local file include vulnerabilities can allow attackers to gain unauthorized access to files, which may also aid in other attacks.
- » Differing responses may also indicate the presence of a file enumeration vulnerability, which instead of allowing the attacker to gain access to file contents, may allow them to determine if files exist on the system.

نتيجة (١١)



## 7. ثغرة (Low) ASP/ASPX Error Detected

- اكتشف Vega رسالة خطأ مرتبطة بـ Microsoft ASP/ASP.NET framework .
- قد تكشف البيانات الواردة في هذا المحتوى معلومات حساسة حول التطبيق يمكن أن تساعد في هجمات أكثر تعقيداً.

**ASP/ASPX Error Detected**

**AT A GLANCE**

<b>Classification</b> <b>Resource</b> <b>Risk</b>	<b>Information</b> <b>/Dashboard.aspx</b> <b>Low</b>
---	--

**REQUEST**

```
GET /Dashboard.aspx?param=47922139AC9C1F2953A41D19067692E254C51790BD3666F99154CCB18F93A3EFC3575F86266192F54F6D17B62C0BAAB492962AE7B14240E5FF0A474FCB4835D7~%20style=->">">"
```

**RESOURCE CONTENT**

```
<span><H1>Server Error in '/' Application.<hr width=100% size=1 color=silver></H1>
```

**DISCUSSION**

Vega has detected an error message associated with the Microsoft ASP/ASP.NET framework.

**IMPACT**

- >> Verbose error output has been detected.
- >> Data in this output could reveal sensitive information about the application that could aid more complex attacks.
- >> The error itself may be indicative of a security vulnerability.





**REMEDATION**

- >> The developer should investigate the error to determine its nature and ensure that it does not represent a vulnerability.
- >> Disable error messages for remote users.
- >> Configure the server and framework to display safe error messages that do not include sensitive information.

نتيجة (١٢)

**فحص النطاق الفرعي admfin.guilan.ac.ir**

## Scan Alert Summary

 <b>High</b>	(3 found)
SQL Injection	1
Page Fingerprint Differential Detected - Possible XPath Injection	1
Shell Injection	1
 <b>Medium</b>	(None found)
 <b>Low</b>	(16 found)
Email Addresses Found	16
 <b>Info</b>	(155 found)
Interesting Meta Tags Detected	99
Cookie HttpOnly Flag Not Set	3
Blank Body Detected	53

## 8. ثغرة (High) Shell Injection

- حقن الكود هو عبارة عن استغلال الأخطاء في نظام الكمبيوتر والذي يؤدي إلى تنفيذ تعليمات برمجية غير مرغوب فيها في النظام . ويمكن للمقرصن استخدام هجمات الحقن لتغيير اتجاه البرنامج في أي اتجاه يريد .

## Shell Injection

### ▶ AT A GLANCE

Classification	Information
Resource	<code>/-/%45%39%31%41%CC-%45%2A%42%27%36%CC%27%46-%45%33%A9%46-%27%39%36%27%CC-%45%2D%2A%31%45-%47%CC%27%2A-%39%44%45%CC-%2F%27%46%34%AF%27%47</code>
Parameter	<code>p_p_lifecycle</code>
Method	GET
Detection Type	Linux/Unix Blind Timing Analysis Checks
Risk	High

### ▶ REQUEST

```
GET /-/%45%39%31%41%CC-%45%2A%42%27%36%CC%27%46-%45%33%A9%46-%27%39%36%27%CC-%45%2D%2A%31%45-%47%CC%27%2A-%39%44%45%CC-%2F%27%46%34%AF%27%47?
redirect=https://admin.guilan.ac.ir/search%3Fp_p_id=3_INSTANCE_u33nrtcalnRq&p_p_lifecycle=%3B%20/bin/sleep%2031%20%3B&p_p_state=normal&p_p_mode=view&p_p_col_id=1&p_p_col_count=1&_3_INSTANCE_u33nrtcalnRq_keywords=&_3_INSTANCE_u33nrtcalnRq_assetCategoryId=739368%2C739364%2C739370%2C739366%2C995404%2C1161803%2C15
```

### ▶ DISCUSSION

Command injection vulnerabilities often occur when inadequately sanitized externally supplied data is as part of a system command executed through a command interpreter, or shell. Vulnerabilities such as these can be exploited by using shell metacharacters to run additional commands that were not intended to be executed by the application developer. The `system()` function, and derivatives, are often responsible, as these functions are very simple to use. These vulnerabilities can grant remote access to attackers, if exploited successfully.

### ▶ IMPACT

- ▶ Vega has detected a possible command injection vulnerability.
- ▶ Attackers may be able to run commands on the server.
- ▶ Exploitation may lead to unauthorized remote access.

نتيجة (١٣)

## فحص النطاق الفرعي food.guilan.ac.ir

Scan Alert Summary		
High		(3 found)
Cleartext Password over HTTP	2	
SQL Injection	1	
Medium		(1 found)
Possible XML Injection	1	
Low		(2 found)
Form Password Field with Autocomplete Enabled	2	
Info		(12 found)
Blank Body Detected	10	
X-Frame-Options Header Not Set	2	

### 9. ثغرة (High) Cleartext Password over HTTP

حدد فيجا نموذجًا يمكنه إرسال كلمة مرور عبر قناة غير آمنة. يمكن أن يؤدي هذا إلى الكشف عن كلمات المرور على الشبكة .

#### Cleartext Password over HTTP

AT A GLANCE

Classification Resource Risk	Environment /loginpage.rose High
------------------------------------	--

REQUEST

GET /loginpage.rose?res=5

DISCUSSION

Vega detected a form with a password input field that submits to an insecure (HTTP) target. Password values should never be sent in the clear across insecure channels. This vulnerability could result in unauthorized disclosure of passwords to passive network attackers.

IMPACT

- >> Vega has detected a form that can cause a password submission over an insecure channel.
- >> This could result in disclosure of passwords to network eavesdroppers.

REMEDIATION

- >> Passwords should never be sent over cleartext. The form should submit to an HTTPS target.

REFERENCES

Some additional links with relevant information published by third-parties:

- [HTTPS \(Wikipedia\)](#)

نتيجة (١٤)

Requests

ID	Host	Method	Request	Status	Length	Time
658	http://food.g	GET	/res	200	0	38
659	http://food.g	GET	/styles/js/struts.js	200	1455	10
660	http://food.g	GET	/softwares/	404	971	24
661	http://food.g	GET	/res?creatorLogId=&dl=false	200	1455	10
662	http://food.g	GET	/loginpage.rose?res=5	200	20823	69
663	http://food.g	GET	/styles/js/newui/jquery-ui.min.js?res=5&creatorLogId=&dl=false	200	1455	10
664	http://food.g	GET	/struts/js/base/jquery-ui.min.js?s2j=4.0.2"	200	122880	61
665	http://food.g	GET	/res?creatorLogId=&dl=false	200	1455	10

Request
Response

```

</tr>
<tr>

<td valign="top" id="where-am-i">
<form action="/j_security_check" style="display: flex" method="post"
name="loginForm"
id="loginForm">


<input type="hidden" name="_csrf"
value="152fd582-c17e-43d8-91b8-0d3ccbb3f182"/>
<table border="0"

```

1 of 3 highlights

Request
Response

```

</div>
</td>
</tr>
<tr>
<td colspan="2">
<div class="form-group">
<label for="password"
class="required form-label">رمز عبور</label>
<input class="form-input" type="password" dir="ltr"
name="password" tabIndex="2" id="password">
</div>
</td>
</tr>

```

1 of 3 highlights

نتیجہ (۱۵)

## Scan Alert Summary

### ! High (16 found)

Session Cookie Without Secure Flag	1
Session Cookie Without HttpOnly Flag	1
Cleartext Password over HTTP	3
Shell Injection	5
Cross Site Scripting	2
SQL Injection	3
Page Fingerprint Differential Detected - Possible XPath Injection	1

### ! Medium (3 found)

HTTP Trace Support Detected	1
Possible Source Code Disclosure	2

### ! Low (3 found)

Form Password Field with Autocomplete Enabled	3
---	---

### i Info (25 found)

X-Frame-Options Header Not Set	21
HTTP Error Detected	3
Blank Body Detected	1

## 10. ثغرة Cross Site Scripting (High)

- تشير ثغرة XSS إلى ثلاث كلمات تعني تشغيل البرنامج النصي على الموقع . كما يوحي الاسم ، فإنه يسمح للمهاجم بتنفيذ البرنامج النصي الخاص به على موقع الويب . يمكن أن تكون هذه البرامج النصية من لغات client-side فقط ، أي أن تكون مرئية للمستخدم .

### Cross Site Scripting

▶ AT A GLANCE

<b>Classification</b>	<b>Input Validation Error</b>
<b>Resource</b>	/course.php
<b>Parameter</b>	term
<b>Method</b>	POST
<b>Risk</b>	High

▶ REQUEST

POST /course.php [year=2012 term=1/ -->">" namecourse=Joey faculty=1 mods=str str=ok limit=50 pg=2 pg=3 pg=4 pg=5 pgs2=... pg22=6 pgت=بدي pg3=2 ]

▶ DISCUSSION

Cross-site scripting (XSS) is a class of vulnerabilities affecting web applications that can result in security controls implemented in browsers being circumvented. When a browser visits a page on a website, script code originating in the website domain can access and manipulate the DOM (document object model), a representation of the page and its properties in the browser. Script code from another website can not. This is known as the "same origin policy", a critical control in the browser security model. Cross-site scripting vulnerabilities occur when a lack of input validation permits users to inject script code into the target website such that it runs in the browser of another user who is visiting the same website. This would circumvent the browser same-origin policy because the browser has no way to distinguish authentic script code from inauthentic, apart from its origin.

▶ IMPACT

- » The precise impact depends greatly on the application.
- » XSS is generally a threat to web applications which have authenticated users or are otherwise security sensitive.
- » Malicious code may be able to manipulate the content of the site, changing its appearance and/or function for another user.
- » This includes modifying the behavior of the web application (such as redirecting forms, etc).
- » The code may also be able to perform actions within the application without user knowledge.
- » Script code can also obtain and retransmit cookie values if they haven't been set HttpOnly.

▶ REMEDIATION

- » The developer must identify how the untrustworthy data is being output to the client without adequate filtering.
- » There are various language/platform specific techniques for filtering untrustworthy data.
- » General rules for preventing XSS can be found in the recommended OWASP XSS Prevention Cheat Sheet (see references).

```
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Keep-Alive: timeout=5, max=96

Offset 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
0000: 3C 68 74 6D 6C 20 78 6D 6C 6E 73 3D 22 68 74 74      <html xmlns="htt
0010: 70 3A 2F 2F 77 77 77 2E 77 33 2E 6F 72 67 2F 31      p://www.w3.org/1
0020: 39 39 39 2F 78 68 74 6D 6C 22 3E 0D 0A 3C 68 65      999/xhtml">..<he
0030: 61 64 3E 0D 0A 3C 6D 65 74 61 20 68 74 74 70 2D      ad>..<meta http-
0040: 65 71 75 69 76 3D 22 43 6F 6E 74 65 6E 74 2D 54      equiv="Content-T
0050: 79 70 65 22 20 63 6F 6E 74 65 6E 74 3D 22 74 65      ype" content="te
```

نتيجة (١٦)

## 11. ثغرة (High) Session Cookie Without Secure Flag

- الكوكي أو ملف تعريف الارتباط هو ملف من جانب العميل يحتوي على معلومات ، يمكن أن تكون هذه المعلومات عناصر في سلة التسوق أو اسم المستخدم وكلمة المرور . بالحصول عليهم يمكن للمهاجمين كسب الوصول غير المصرح به إلى تطبيقات الويب المتأثرة .

### Session Cookie Without Secure Flag

AT A GLANCE

Classification

Resource

Risk

Information

/

High

REQUEST

GET /

RESOURCE CONTENT

PHPSESSID=kjui3mib3ufnoje1lc5pvrgcpl; path=/

DISCUSSION

Vega has detected that a known session cookie may have been set without the secure flag.

IMPACT

>> Cookies can be exposed to network eavesdroppers.

>> Session cookies are authentication credentials; attackers who obtain them can get unauthorized access to affected web applications.

نتيجة (١٧)

## 12. ثغرة HTTP Trace Support Detected (High)

- مع هذه الثغرة يمكن للقراصنة استرداد ملفات تعريف الارتباط من المتصفحات الأخرى عن طريق كتابة نص XSS برمجي .

### HTTP Trace Support Detected

► AT A GLANCE

<b>Classification</b>	<b>Configuration Error</b>
<b>Resource</b>	<b>Apache/2.4.23 (Win64) PHP/5.6.25</b>
<b>Method</b>	<b>TRACE</b>
<b>Risk</b>	<b>Medium</b>

► REQUEST

**TRACE /href%3Dinfo.php**

► RESOURCE CONTENT

```
TRACE /href%3Dinfo.php HTTP/1.1
SQUEEMISH: OSS1FR4GE
Accept-Encoding: gzip,deflate
Host: courses.guilan.ac.ir
Connection: Keep-Alive
User-Agent: UserAgent
Cookie: PHPSESSID=kjui3mib3ufnojellcSpvrgcp1
Cookie2: $Version=1
```

► DISCUSSION

HTTP TRACE is an HTTP method that requests that the server echo the TRACE request back to the client. This includes headers that were sent along with the request. Support for HTTP TRACE can be abused in scenarios where a cross-site scripting vulnerability has been found, but cannot be exploited to retrieve cookie values because the target cookies are set with the HttpOnly flag. The HttpOnly flag instructs browsers not to permit access to the cookie by Javascript. If a cross-site scripting vulnerability is found, but the session cookie is set HttpOnly, support for HTTP TRACE will open an opportunity for cookie theft. An attacker can use the cross-site scripting vulnerability to have the target user's browser issue a TRACE request to the server via XMLHttpRequest (or a similar function) and then retrieve the cookie from the response, which will contain the request that was sent by the browser, including cookies.

► IMPACT

- » Allowing HTTP TRACE can permit cross-site tracing.
- » Attackers may be able to use cross-site tracing with cross-site scripting retrieve the value of HttpOnly cookies.

نتيجة (١٨)

## 13. ثغرة Session Cookie Without Secure Flag (High)

- باستخدام هذه الثغرة يمكن للمهاجم الحصول على النص البرمجي المصدر للخادم من خلال تطبيق الويب ، والتي يمكن أن تحتوي على معلومات حساسة مثل سلاسل اتصال قاعدة البيانات واسم المستخدم وكلمة المرور.



## Page Fingerprint Differential Detected - Possible XPath Injection

### ▶ AT A GLANCE

<b>Classification</b>	<b>Error Message</b>
<b>Resource</b>	/search
<b>Parameter</b>	p_p_col_id
<b>Method</b>	GET
<b>Detection Type</b>	XPath 2.0 Blind Injection Differential Checks
<b>Risk</b>	High

### ▶ REQUEST

GET /search? p\_p\_id=3\_INSTANCE\_r4ilfdAc3jb&p\_p\_lifecycle=0&p\_p\_state=normal&p\_p\_mode=view&p\_p\_col\_id=e"%20or%201%20eq%201%20or%20"a"%20=%20"a&p\_p\_col\_count=1&\_3\_INST/

### ▶ DISCUSSION

Vega has detected a different response page fingerprint in relation to an XPath injection request. This means that the response page content returned by the web application has a different signature from that returned by an ordinary request, which may indicate the existence of an XPath injection vulnerability. The differing page fingerprint may include error messages or indicate a state change in the application in response to the XPath injection attempt made by Vega. Developers should examine the response content and underlying code to verify whether or not a vulnerability is present. If the vulnerability exists and precautions are not taken, depending on the nature of the affected XPath query, such a vulnerability could allow attackers to bypass authentication or gain unauthorized access to sensitive XML data.

### ▶ IMPACT

- » Vega has detected a different response fingerprint in relation to an XPath injection attempt.
- » This may indicate an XPath injection vulnerability, though this is not confirmed.
- » If this is due to an XPath vulnerability, depending on the nature of the XPath query, exploitation could allow attackers to bypass authentication or gain unauthorized access to sensitive XML data.

## Session Cookie Without Secure Flag

### ▶ AT A GLANCE

<b>Classification</b>	<b>Information</b>
<b>Resource</b>	/
<b>Risk</b>	High

### ▶ REQUEST

GET /

### ▶ RESOURCE CONTENT

PHPSESSID=kjui3mib3ufnoje1lc5pvrgcp1; path=/

### ▶ DISCUSSION

Vega has detected that a known session cookie may have been set without the secure flag.

### ▶ IMPACT

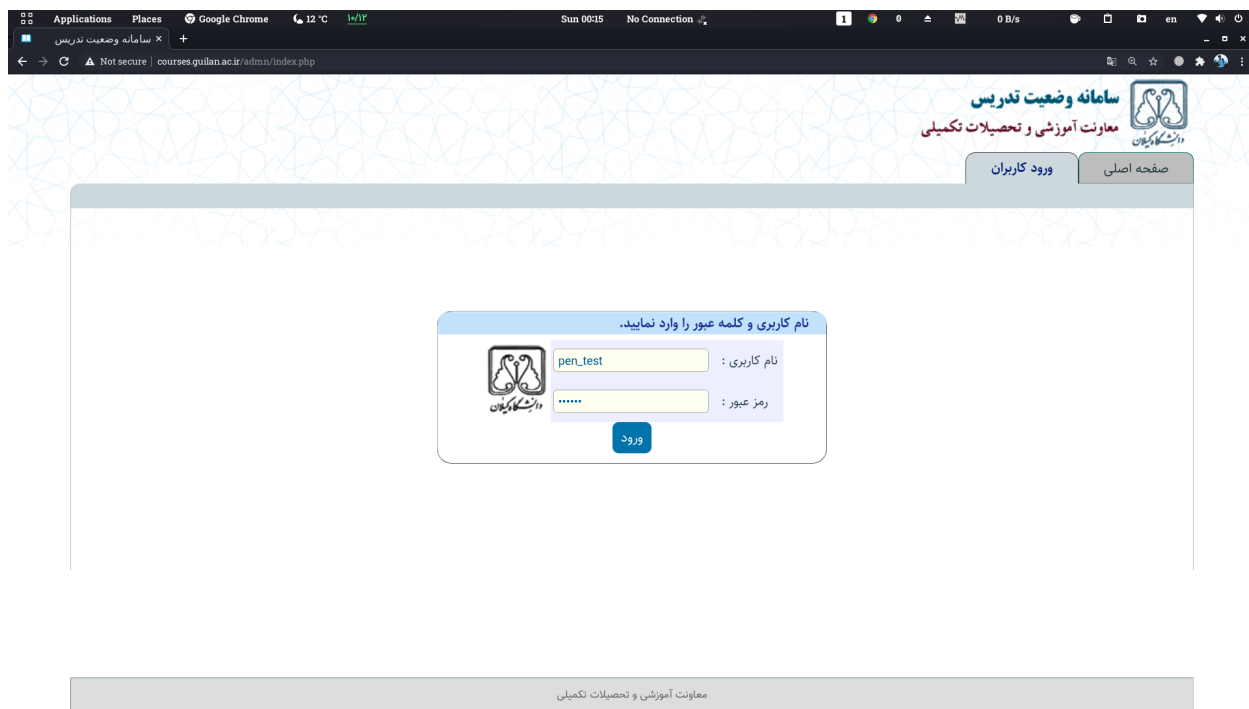
- » Cookies can be exposed to network eavesdroppers.
- » Session cookies are authentication credentials; attackers who obtain them can get unauthorized access to affected web applications.

نتيجة (١٩)

- كما نرى ، إن آخر موقع تم فحصه لديه أكبر عدد من الثغرات الأمنية وأكثرها حساسية . في هذه الحالة ، يمكننا بدء اختبار الاختراق على نفس الموقع .

### استغلال ثغرة Cleartext Password over HTTP

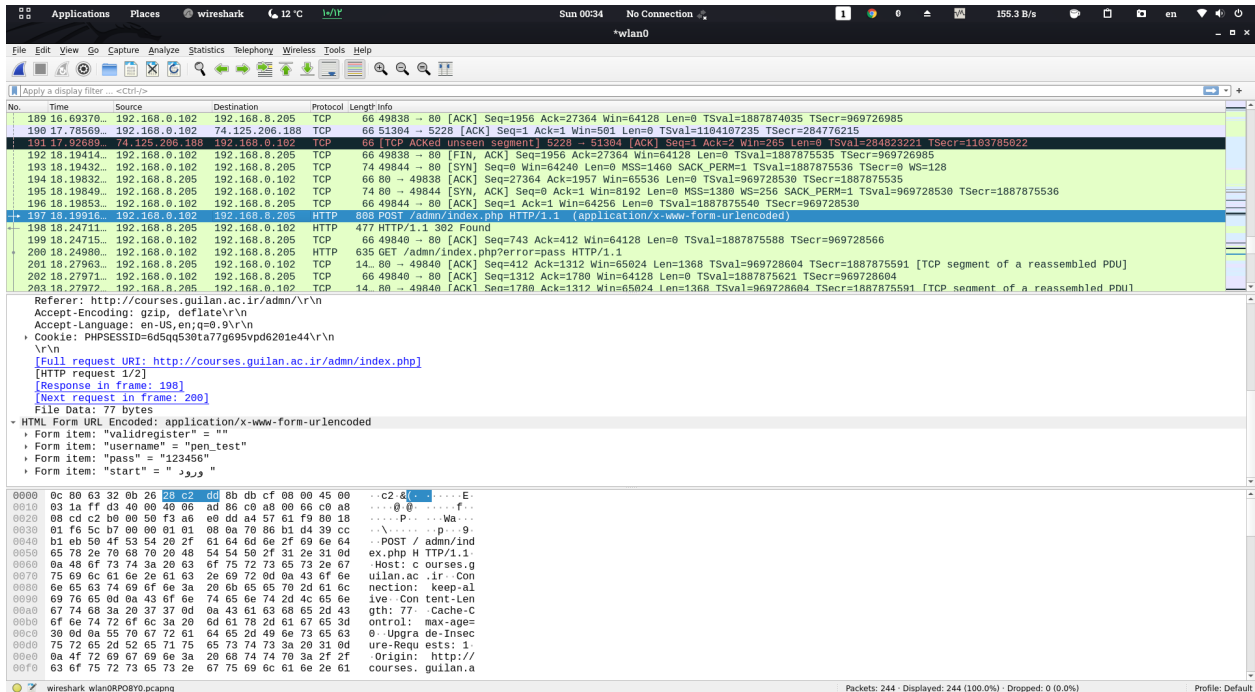
- واحدة من أفضل أدوات اختبار الاختراق في هذا المجال هي أداة Wireshark . باستخدام هذه الأداة ، يمكننا الحصول على البيانات المتبادلة بين الخادم والمستخدم . و في الاختبار التالي ، يمكننا بسهولة رؤية اسم المستخدم وكلمة المرور على شكل Text .
- في البداية نفتح أداة wireshark ونبدأ جلسة جديدة ، ثم ندخل إلى الموقع عبر المتصفح المرغوب ، ونذهب إلى قسم تسجيل دخول المستخدمين ، ثم ندخل اسم المستخدم وكلمة المرور .



❖ في الصورة أعلاه ، تم استخدام اسم المستخدم pent\_test وكلمة المرور 123456

## 3-1- النتائج

- كما نرى ، أظهرت لنا أداة wireshark البيانات المستهدفة ، وفي الصورة أدناه يظهر رقم الحزمة 197 المعلومات التي ادخلناها في الصورة السابقة باستخدام ثغرة ClearText Password over HTTP .



```
Referer: http://courses.guilan.ac.ir/admn/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: en-US,en;q=0.9\r\n
Cookie: PHPSESSID=6d5qq530ta77g695vpd6201e44\r\n
\r\n
[Full request URI: http://courses.guilan.ac.ir/admn/index.php]
[HTTP request 1/2]
[Response in frame: 198]
[Next request in frame: 200]
File Data: 77 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "validregister" = ""
Form item: "username" = "pen_test"
Form item: "pass" = "123456"
Form item: "start" = "ورود"
```

نتيجة (٢٠)

النهاية