University of Guilan

Technical College

Title:

Discovering security vulnerabilities in the services and websites of Guilan University and testing its penetration

Supervisor:

Dr. Hamidreza Ahmadi Far

Student:

Adham Al-Saadi

1-1- Introduction

- A penetration test is a method of evaluating the security level of a computer (usually a server) or a network by simulating attacks by a penetration tester (which does not have access). In this method, all systems, programs and services installed on the network are tested to find security problems and then provide appropriate solutions to these problems.

1-2- Project objectives

- Examining the internal services and website of guilan.ac.ir and discovering security weaknesses, describing all its bugs and vulnerabilities, and proposing security solutions to fix the bugs.

1-3- Requirements

- High linux os proficiency
- penetration testing distribution (the distro used is kali)
- Familiarity with Web Application Analysis tools
+ Scripting in languages bash, html, javascript, Python, php and others
- Knowledge of security vulnerabilities

2-1- Test Summary Reports

- The penetration test began on 25/2/2021 using the Black Box method and ended on 3/2/2021.

- First we get comprehensive information from the website and determine the state of the ports. To do this we need special software, such as the Nmap tool.

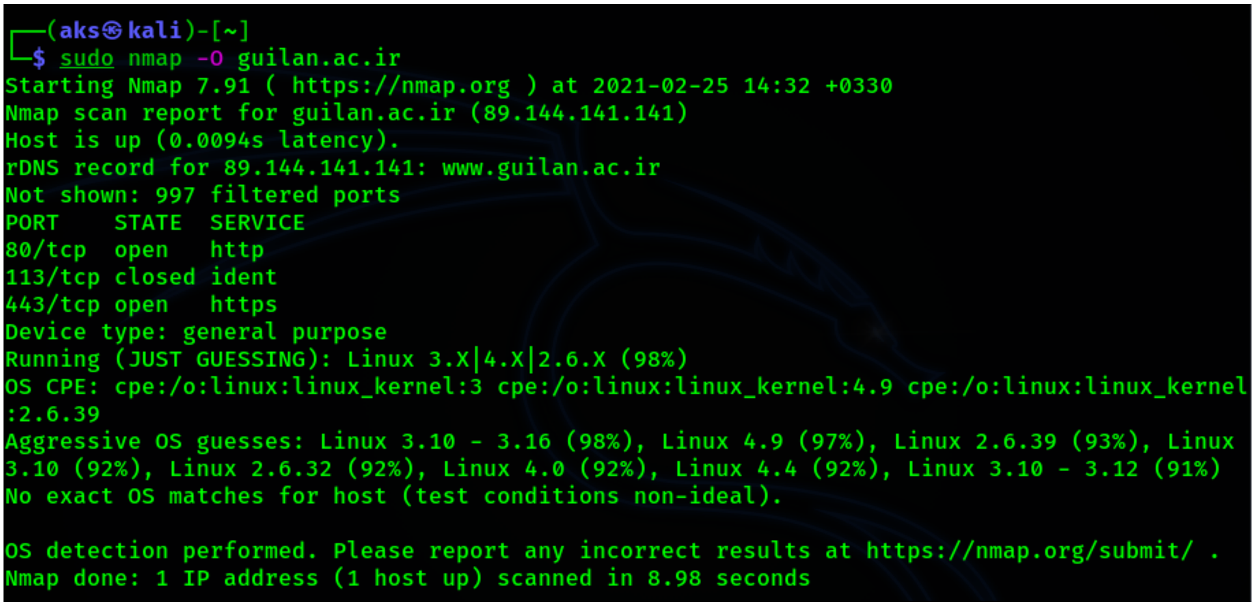
❖ Nmap - Network mapper software features :

- Host discovery – Identifying hosts on a network (based on a ping response or an open port)
- Port scanning
- Determine the version of software and services
- Operating system detection
- Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language.
- Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.

- First we collect the required information, this information includes server specifications, open ports (tcp & udp), services offered, installed software versions, etc.

- To detect the operating system, we can use the following command

$ sudo nmap -O guilan.ac.ir



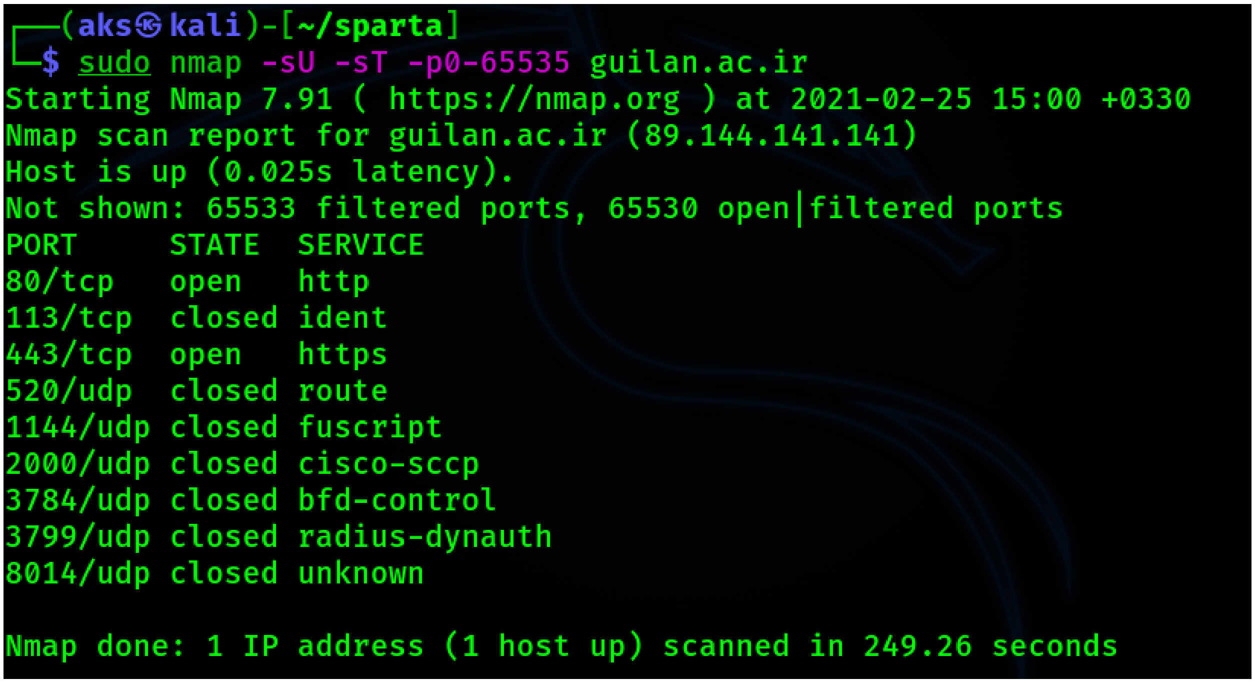
```
┌──(aks㉿kali)-[~]
└─$ sudo nmap -O guilan.ac.ir
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-25 14:32 +0330
Nmap scan report for guilan.ac.ir (89.144.141.141)
Host is up (0.0094s latency).
rDNS record for 89.144.141.141: www.guilan.ac.ir
Not shown: 997 filtered ports
PORT    STATE  SERVICE
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
```

result (1)

- To gather more information, we scan the target with external and internal IP addresses, and in the following results we will see the difference in the output.

- Installed ports and services are identified using these commands

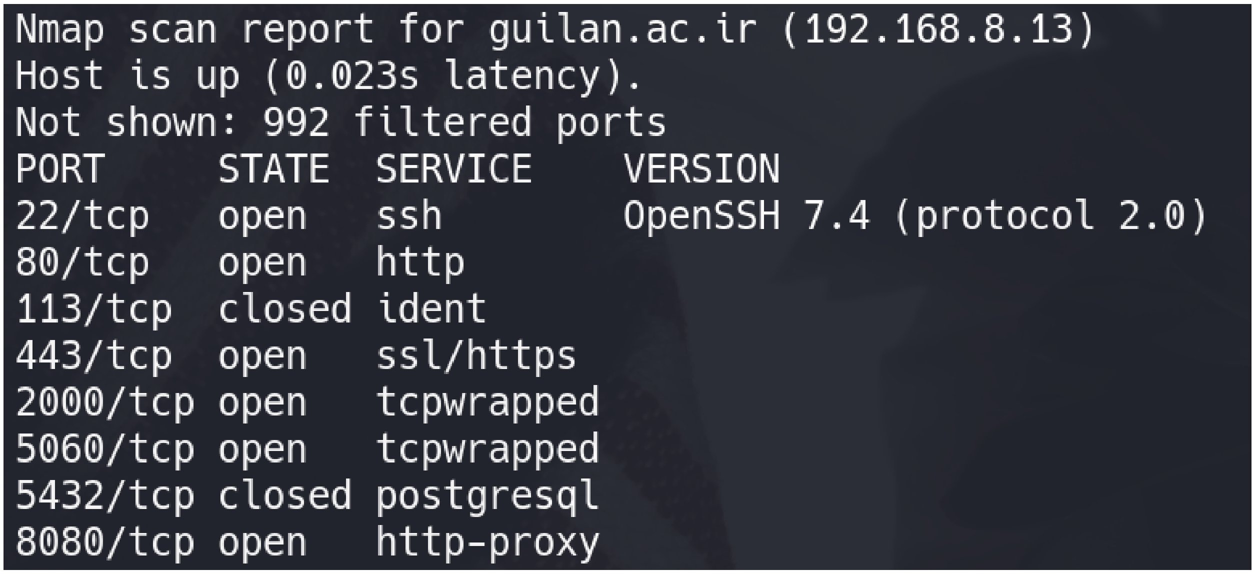
$ sudo nmap -sU -sT -p0-65535 guilan.ac.ir (by external ip)



```
┌──(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 fuscript
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
```

result (2)

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

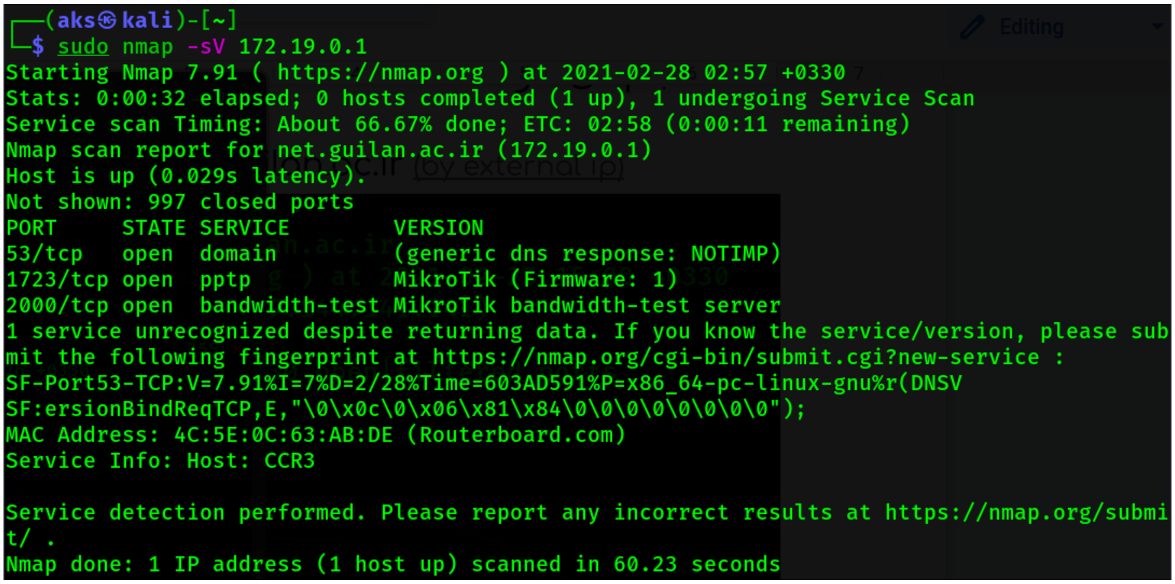


```
Nmap scan report for guilan.ac.ir (192.168.8.13)
Host is up (0.023s latency).
Not shown: 992 filtered ports
PORT     STATE  SERVICE     VERSION
22/tcp   open   ssh         OpenSSH 7.4 (protocol 2.0)
80/tcp   open   http
113/tcp  closed ident
443/tcp  open   ssl/https
2000/tcp open   tcpwrapped
5060/tcp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

result (3)

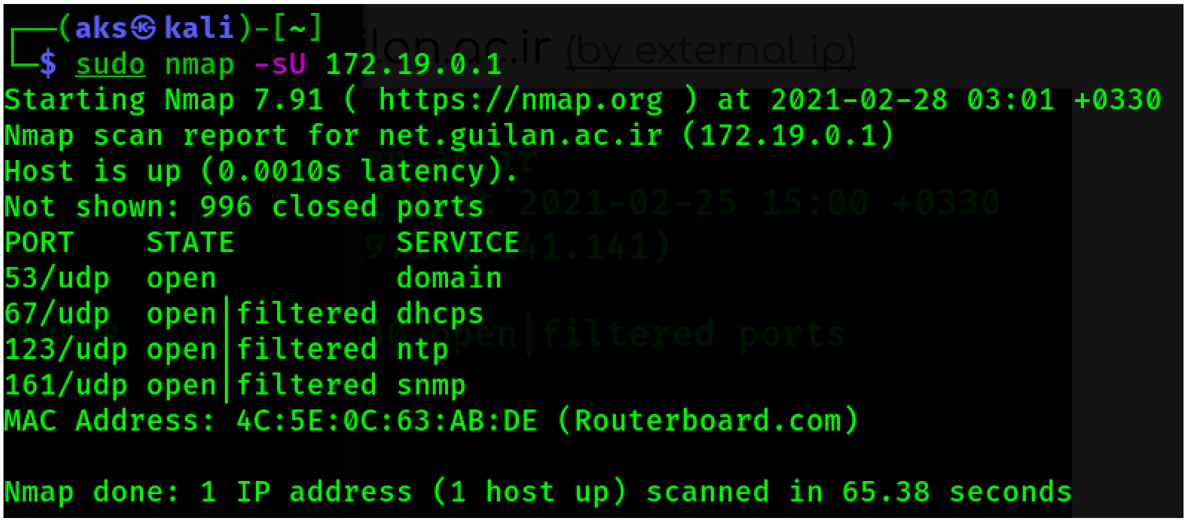
- Checking the university's Internet server net.guilan.ac.ir

tcp ports



```
┌──(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 sub
mit 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=603AD591%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,E,"\0\x0c\0\x06\x81\x84\0\0\0\0\0\0\0\0");
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/submi
t/ .
Nmap done: 1 IP address (1 host up) scanned in 60.23 seconds
```

udp ports



```
┌──(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 dhcps
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
```

result (4)

2-2- Identifying vulnerabilities in target sites :

- After the process of discovering the operating system, versions of software and services installed on the server, we move on to web tools. One of the most famous of these tools is Vega. It is a scanner used for penetration testing and can be useful for setting up the site by the administrator.

❖ Vega tool features :

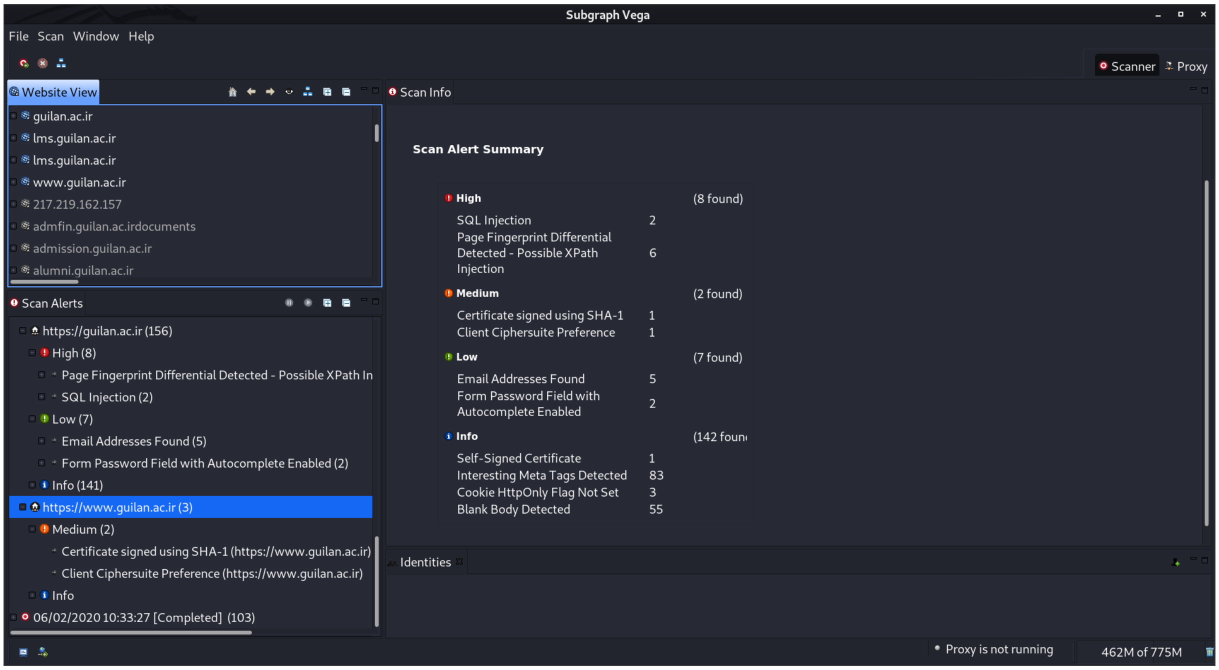
- Scan the GET entries of the desired website.
- Scan the POST entries of the desired website.
- Testing some attacks on the server side.
- Vulnerability scanning : sql injection, cross site scripting, directory check, remote file injection, HTTP headers, etc.
- Divide vulnerabilities into four levels :

  1-High 2-Medium 3-low 4-info
- To scan the desired site, it is enough to have the site address.

❖ Tool requirements :

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

Scan bugs on guilan.ac.ir

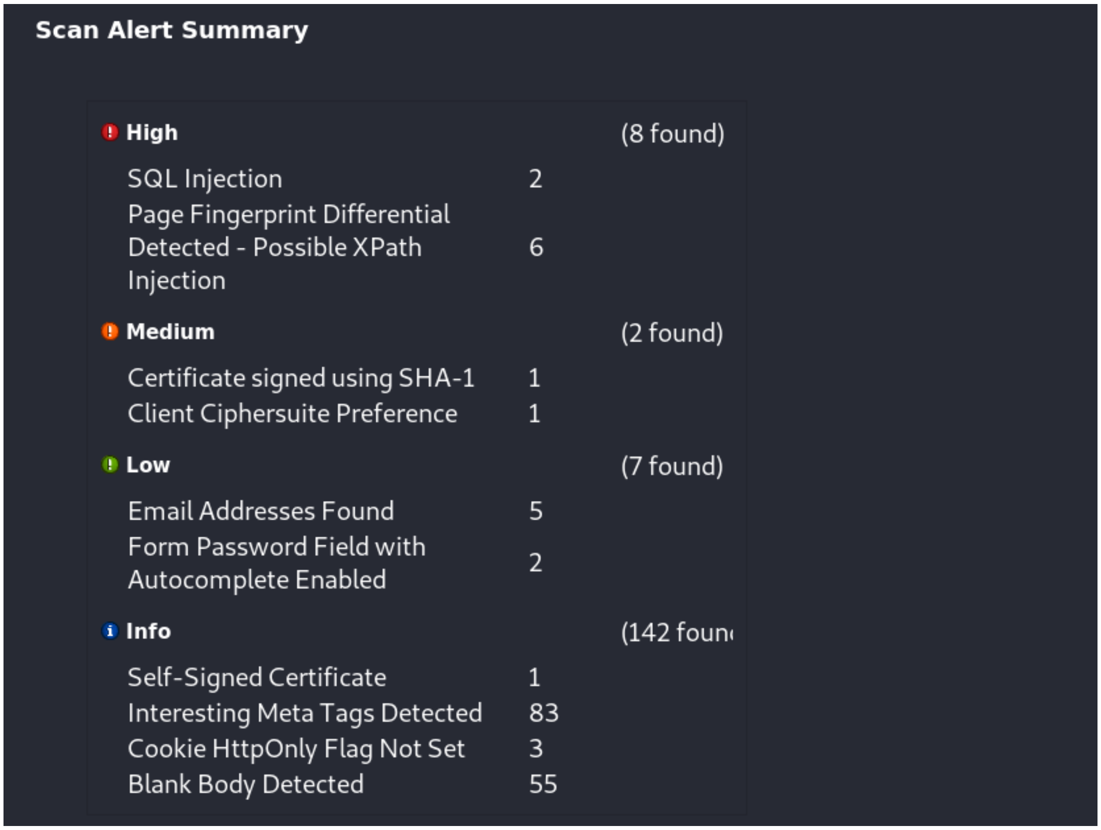


```
guilan.ac.ir
lms.guilan.ac.ir
lms.guilan.ac.ir
www.guilan.ac.ir
217.219.162.157
admfin.guilan.ac.irdocuments
admission.guilan.ac.ir
alumni.guilan.ac.ir
```

```
https://guilan.ac.ir (156)
  High (8)
    Page Fingerprint Differential Detected - Possible XPath In
    SQL Injection (2)
  Low (7)
    Email Addresses Found (5)
    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)
```

```
Scan Alert Summary

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

```
Proxy is not running    462M of 775M
```



```
Scan Alert Summary

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

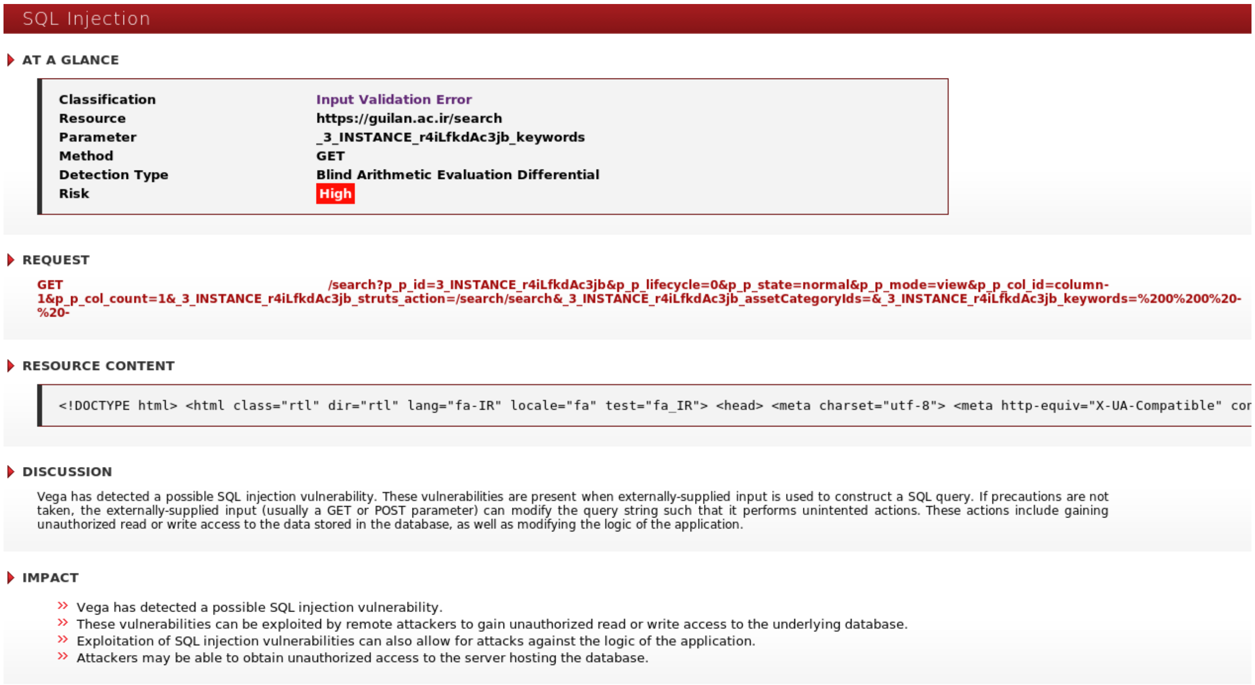
result (5)

2-3- Define the vulnerabilities that were found :

1. <u>SQL Injection bug (High)</u>

- This attack occurs by injecting SQL code into the database through input. The logic of this bug is that the database information is extracted by a malicious query. In this bug we can read database information by some methods (UNION SELECT). This bug exists in all databases such as MariaDB, Microsoft SQL, Oracle, Mysql, etc. This vulnerability has nothing to do with the weakness of these database, but is caused by programmer errors in PHP, ASP, and other web and server-side languages, and sometimes, If there are non-standard server configurations, this issue makes the website more vulnerable and allows the user to set and execute database commands through input.

- The purpose of this bug is different, once you can execute database commands via URL you can do almost anything. Such as access the username and password of admin and users, access and change of all site content, etc.



SQL Injection

AT A GLANCE

Classification	**Input Validation Error**
Resource	**https://guilan.ac.ir/search**
Parameter	**_3_INSTANCE_r4iLfkdAc3jb_keywords**
Method	**GET**
Detection Type	**Blind Arithmetic Evaluation Differential**
Risk	**High**

REQUEST

```
GET /search?p_p_id=3_INSTANCE_r4iLfkdAc3jb&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_r4iLfkdAc3jb_struts_action=/search/search&_3_INSTANCE_r4iLfkdAc3jb_assetCategoryIds=&_3_INSTANCE_r4iLfkdAc3jb_keywords=%200%200%20-
%20-
```

RESOURCE CONTENT

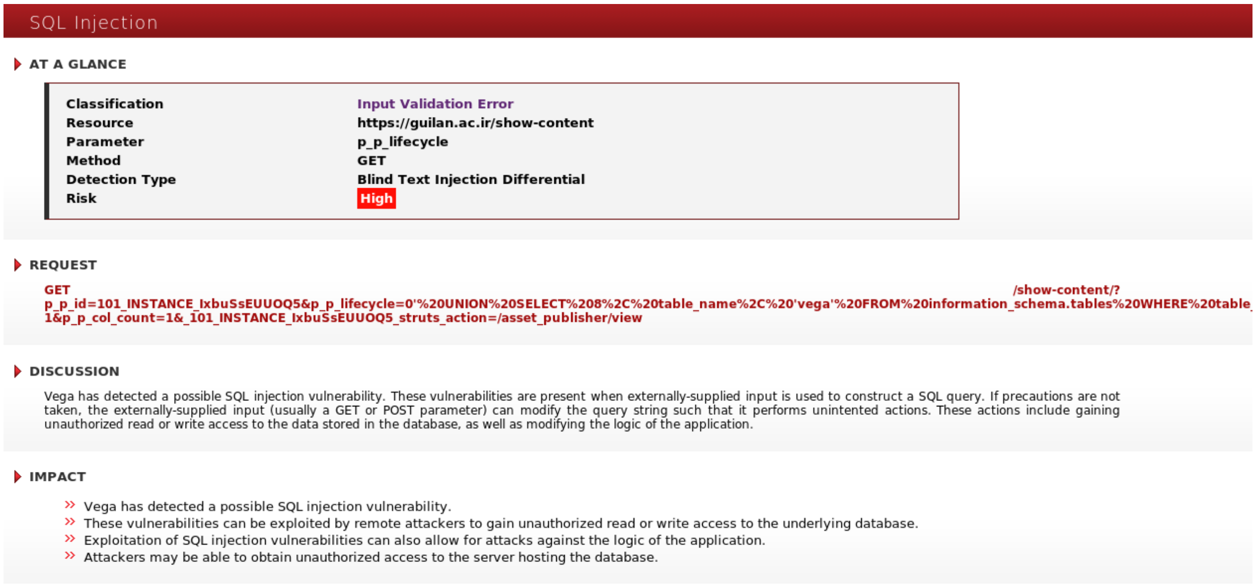
```
<!DOCTYPE html> <html class="rtl" dir="rtl" lang="fa-IR" locale="fa" test="fa_IR"> <head> <meta charset="utf-8"> <meta http-equiv="X-UA-Compatible" cor
```

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 unintented 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	**https://guilan.ac.ir/show-content**
Parameter	**p_p_lifecycle**
Method	**GET**
Detection Type	**Blind Text Injection Differential**
Risk	**High**

REQUEST

```
GET /show-content/?
p_p_id=101_INSTANCE_IxbuSsEUUOQ5&p_p_lifecycle=0'%20UNION%20SELECT%208%2C%20table_name%2C%20'vega'%20FROM%20information_schema.tables%20WHERE%20table_
1&p_p_col_count=1&_101_INSTANCE_IxbuSsEUUOQ5_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 unintented 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

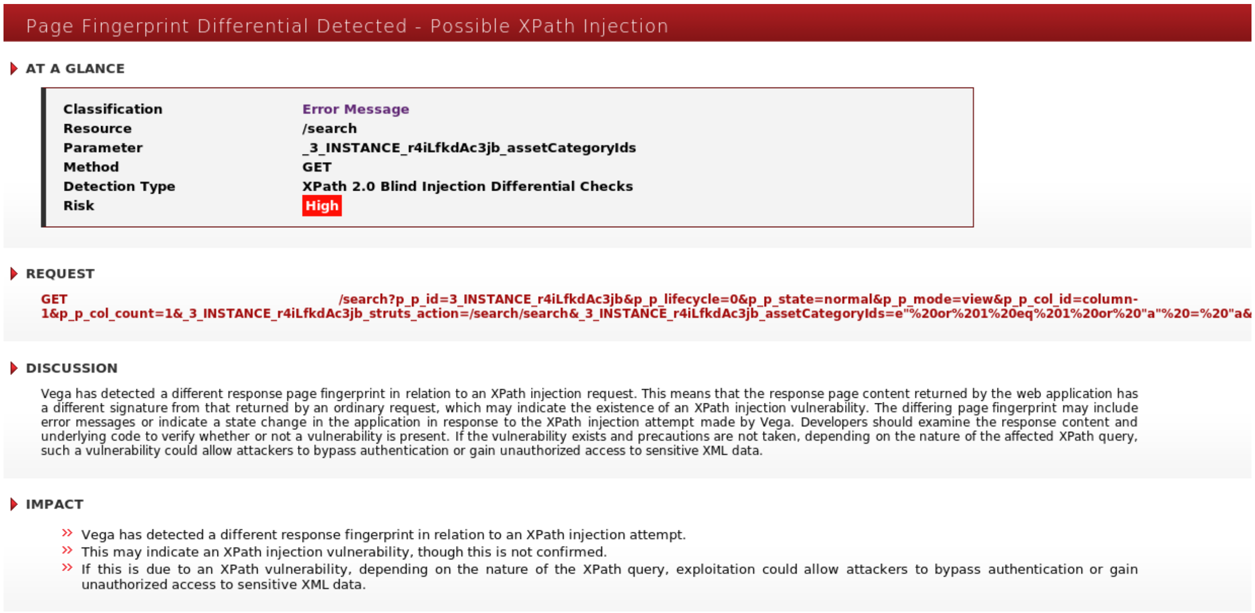
- Vega has detected a possible SQL injection vulnerability.
- These vulnerabilities can be exploited by remote attackers to gain unauthorized read or write access to the underlying database.
- Exploitation of SQL injection vulnerabilities can also allow for attacks against the logic of the application.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

result (6)

2. XPATH Injection bug (High)

- This attack is implemented on XML documents; The XPATH command is a command used in XML documents and is very widely used to search and find data in XML files. XPath Injection attacks, similar to SQL Injection, occur when a website uses user-supplied information to construct an XPath query for XML data.

- By submitting incorrect information to the website, the attacker can find out how the XML data is constructed or gain access to data that he might not normally have access to, even if the XML data is used for authentication, the attacker may be able to increase access level.



Page Fingerprint Differential Detected - Possible XPath Injection

AT A GLANCE

Classification	**Error Message**
Resource	**/search**
Parameter	**_3_INSTANCE_r4iLfkdAc3jb_assetCategoryIds**
Method	**GET**
Detection Type	**XPath 2.0 Blind Injection Differential Checks**
Risk	**High**

REQUEST

```
GET                                        /search?p_p_id=3_INSTANCE_r4iLfkdAc3jb&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_r4iLfkdAc3jb_struts_action=/search/search&_3_INSTANCE_r4iLfkdAc3jb_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.

result (7)

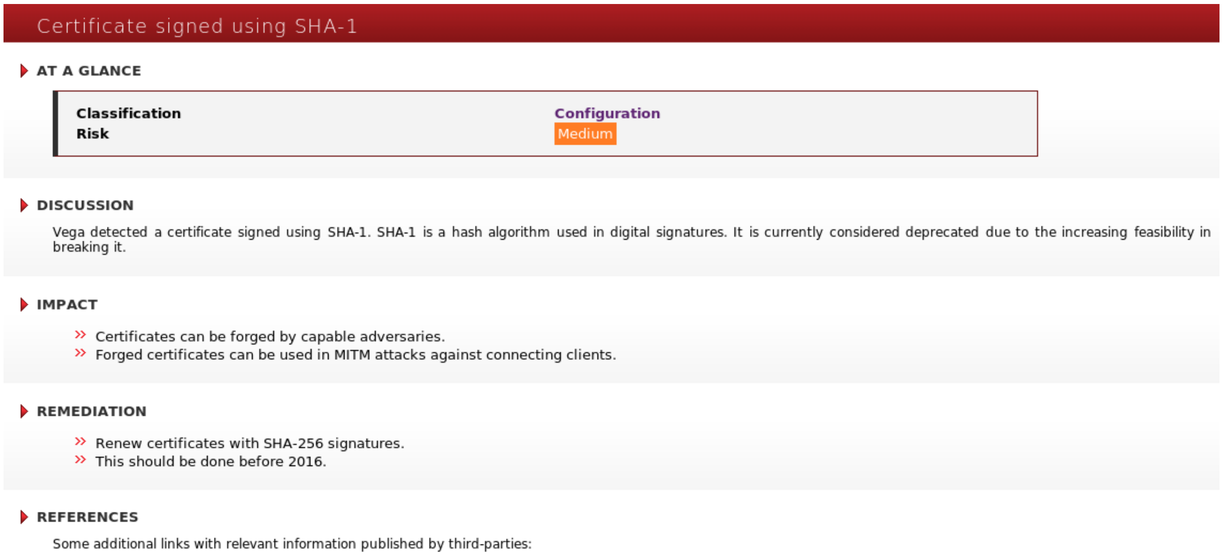
3. Certificate signed using SHA-1 bug (Medium)

- Git in its structures uses the SHA-1 synchronization function not for protection, but to ensure that the data is not changed. And of course, Git is so successful with this algorithm, for example, if you store data in it and after 5 years you want to look at your data, you will see that the data is guaranteed to be unchanged.

Encryption analysis and evaluation

- When we have a message digest of length L, in most cases we can attack the encrypted message with the same length with the complexity of 2 to the power of L by brute force and expose it, it is also called Preimage Attack, which even It can be independent of the message length or computational conditions of the attack.

- The second problem here is to find two different encryption algorithms that both produce the same message digest. In such cases, we say that a collision has occurred and the time required to discover it is from the order of 2 to the power of L/2.



Certificate signed using SHA-1

AT A GLANCE

Classification	Configuration
Risk	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.

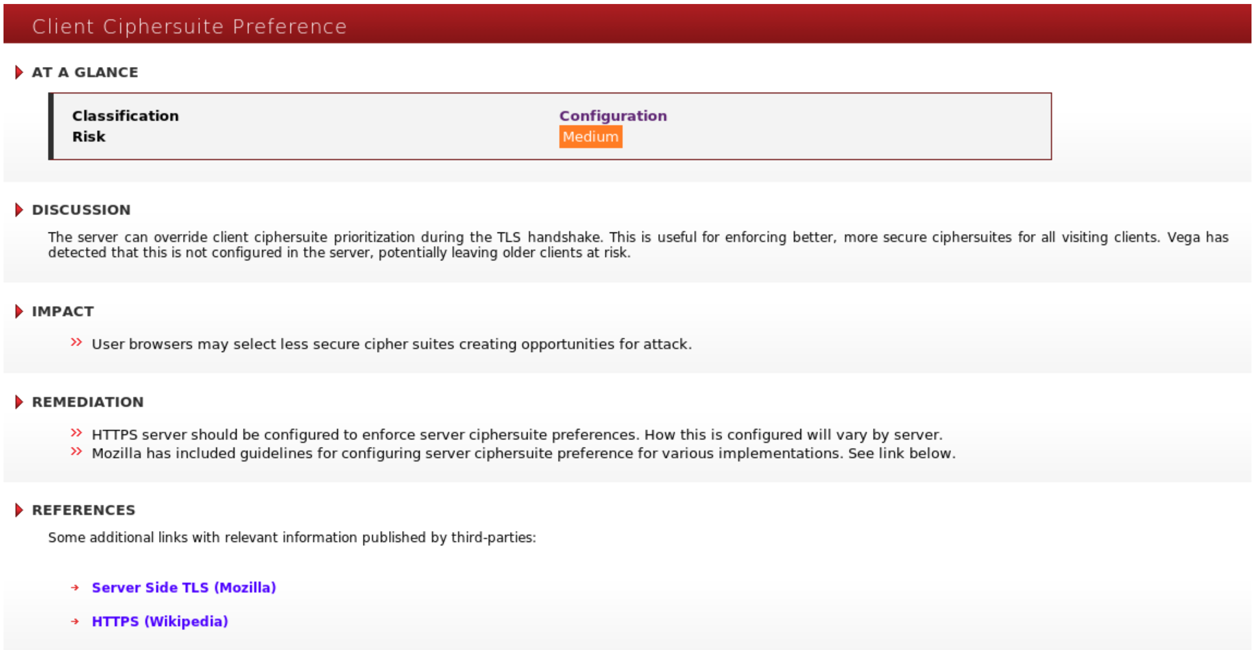
REFERENCES

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

result (8)

4. Client cipher suite preference bug (Medium)

- One of the most important parts of SSL/TLS configuration is to disable vulnerable algorithms and CipherSuites in a way that also enables forward secrecy to ensure security. User browsers may choose less secure cipher suites, which creates an opportunity for attack. User browsers may select less secure cipher suites creating opportunities for attack.



Client Ciphersuite Preference

AT A GLANCE

Classification	Configuration
Risk	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:

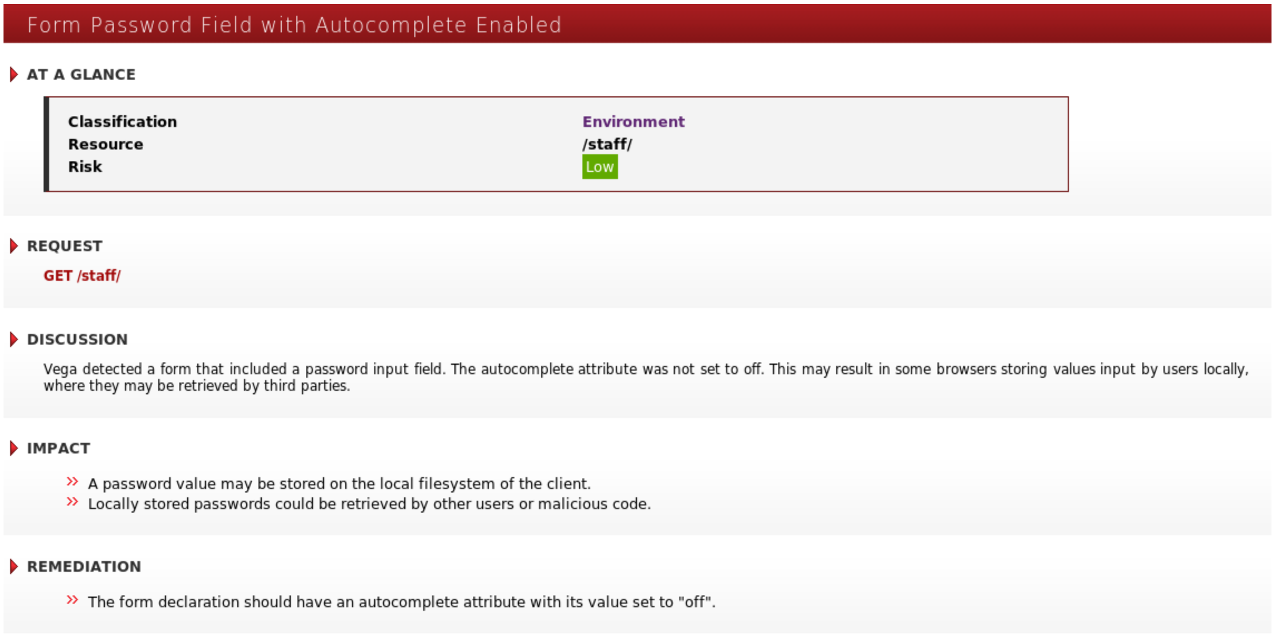
→ **Server Side TLS (Mozilla)**

→ **HTTPS (Wikipedia)**

result (9)

5. Form Password Field with Autocomplete Enabled bug (Low)

- 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.



Form Password Field with Autocomplete Enabled

AT A GLANCE

Classification	**Environment**
Resource	**/staff/**
Risk	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

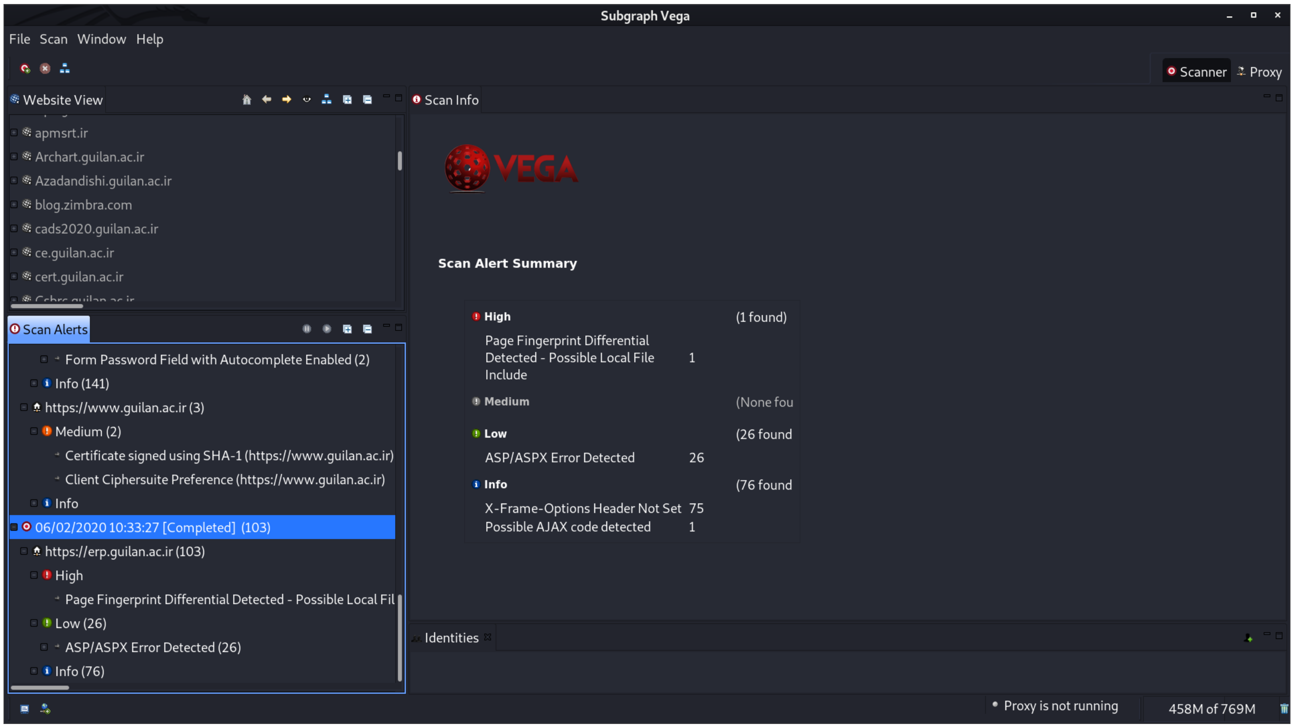
» A password value may be stored on the local filesystem of the client.
» Locally stored passwords could be retrieved by other users or malicious code.

REMEDIATION

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

result (10)

Scan bugs on erp.guilan.ac.ir



```
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
Cshrc.guilan.ac.ir
```

```
      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 Fil
    Low (26)
      ASP/ASPX Error Detected (26)
    Info (76)
```

Scan Alert Summary

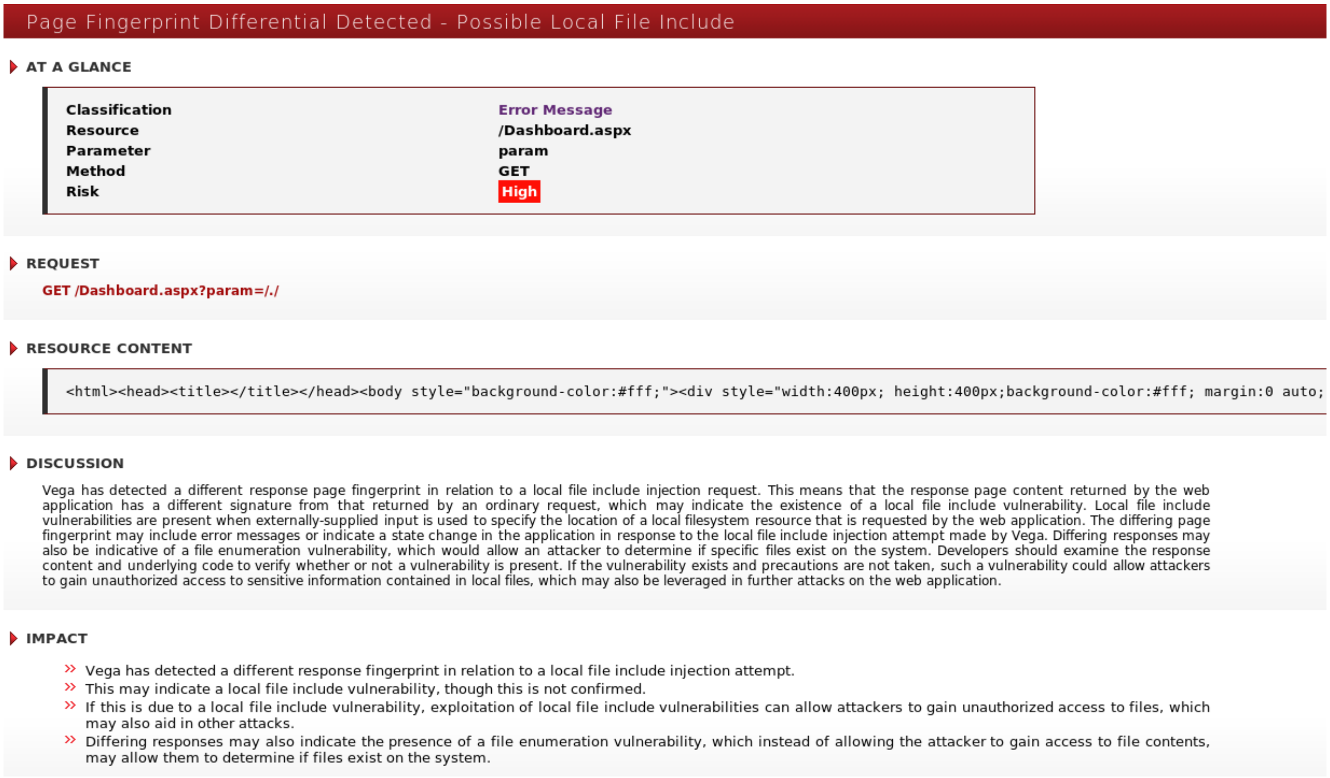
```
High                                          (1 found)
  Page Fingerprint Differential
  Detected - Possible Local File    1
  Include
Medium                                        (None fou
Low                                           (26 found
  ASP/ASPX Error Detected           26
Info                                          (76 found
  X-Frame-Options Header Not Set    75
  Possible AJAX code detected       1
```

```
Proxy is not running        458M of 769M
```

6. Local File Include bug (High)

- The LFI bug, which stands for local file inclusion, occurs when the site programmer has used functions such as include to call web pages and has not filtered illegal characters such as (.) and (/).

- In this case, the attacker can call an important file such as /etc/passwd/ which contains the site's username and passwords.



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.

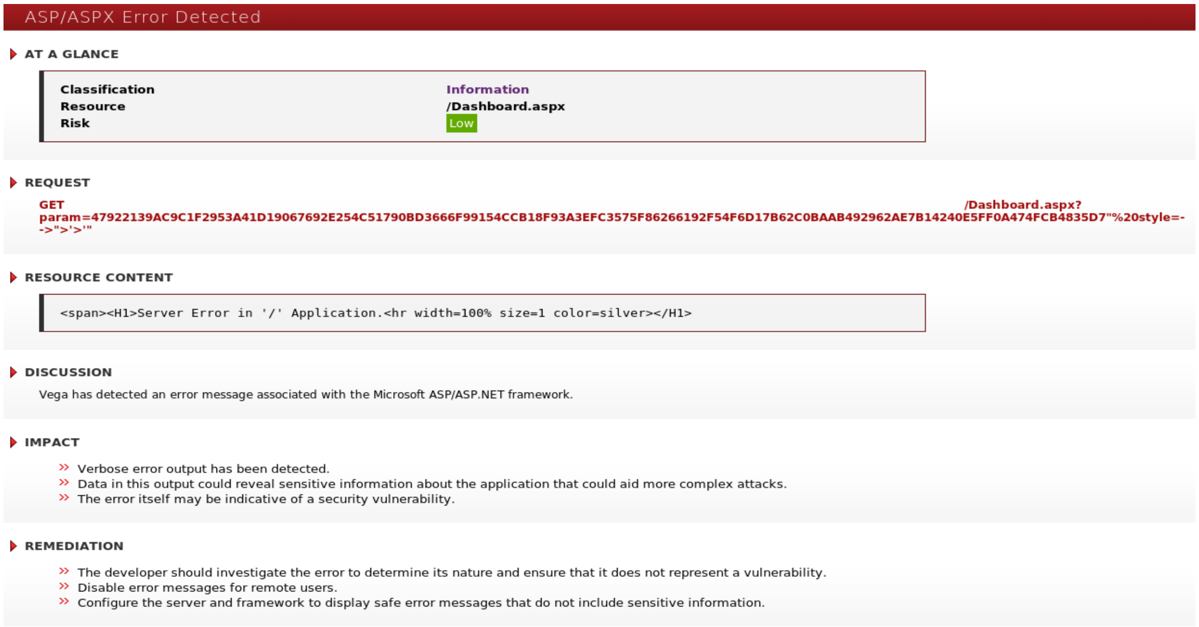
IMPACT

- 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.

result (11)

7. ASP/ASPX Error Detected bug (Low)

- Vega has detected an error message associated with the Microsoft ASP/ASP.NET framework.
- Data in this output could reveal sensitive information about the application that could aid more complex attacks.



ASP/ASPX Error Detected

AT A GLANCE

Classification	Information
Resource	/Dashboard.aspx
Risk	Low

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

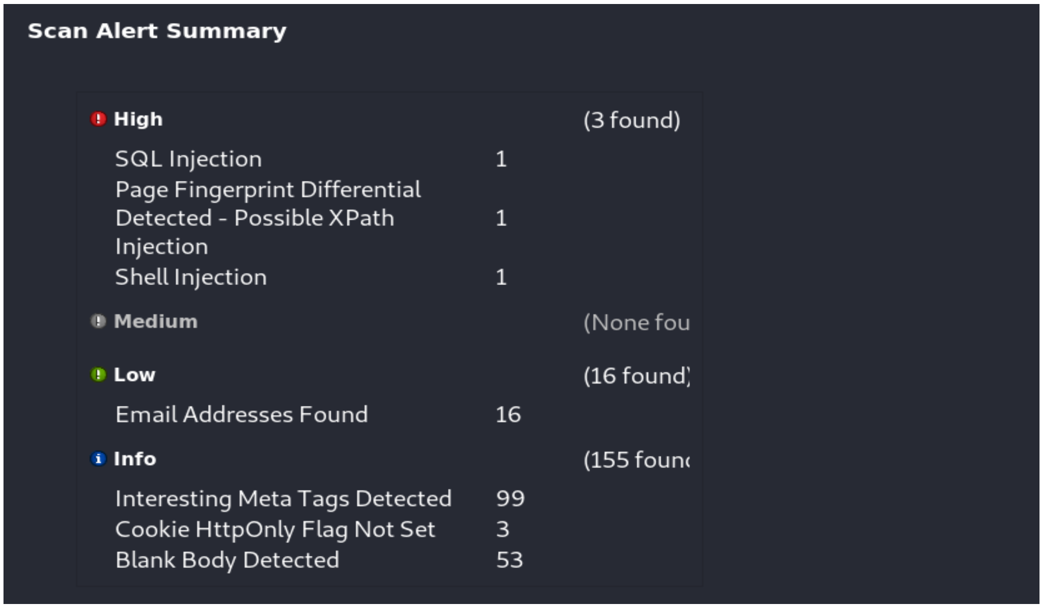
- Verbose error output has been detected.
- Data in this output could reveal sensitive information about the application that could aid more complex attacks.
- The error itself may be indicative of a security vulnerability.

REMEDIATION

- 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.

result (12)

Scan bugs on admfin.guilan.ac.ir

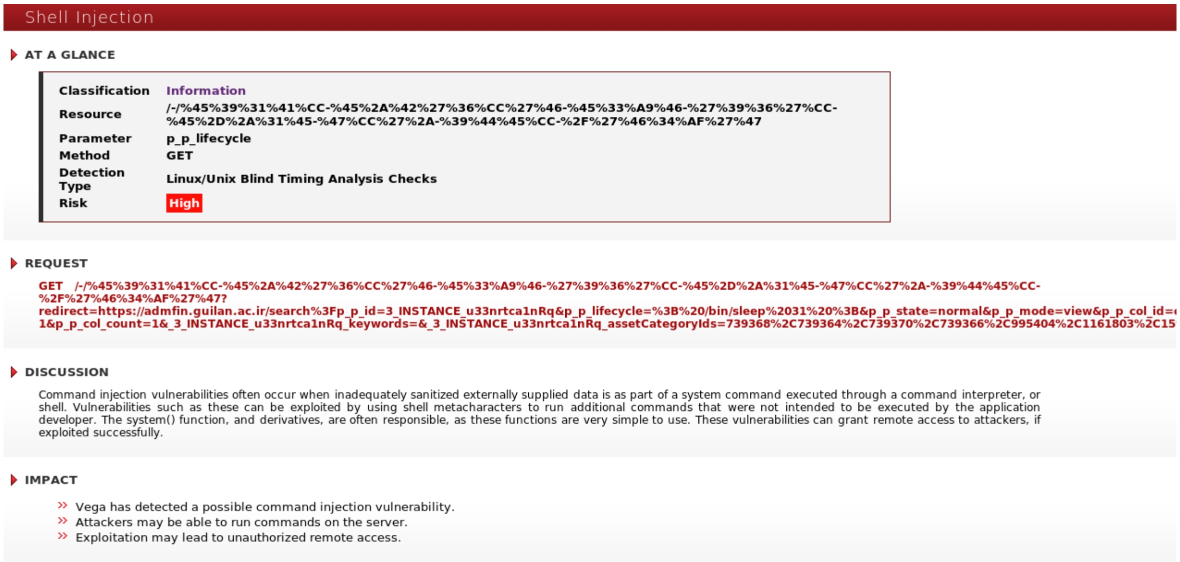


Scan Alert Summary

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

8. Shell Injection bug (High)

- Shell injection is the exploitation of bugs in a computer system that leads to the execution of unwanted commands in the system. By using injection attacks, the attacker can change the direction of the program in any direction he wants.



Shell Injection

AT A GLANCE

Classification	Information
Resource	/-/%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
Parameter	p_p_lifecycle
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://admfin.guilan.ac.ir/search%3Fp_p_id=3_INSTANCE_u33nrtca1nRq&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_u33nrtca1nRq_keywords=&_3_INSTANCE_u33nrtca1nRq_assetCategoryIds=739368%2C739364%2C739370%2C739366%2C995404%2C1161803%2C15
```

DISCUSSION

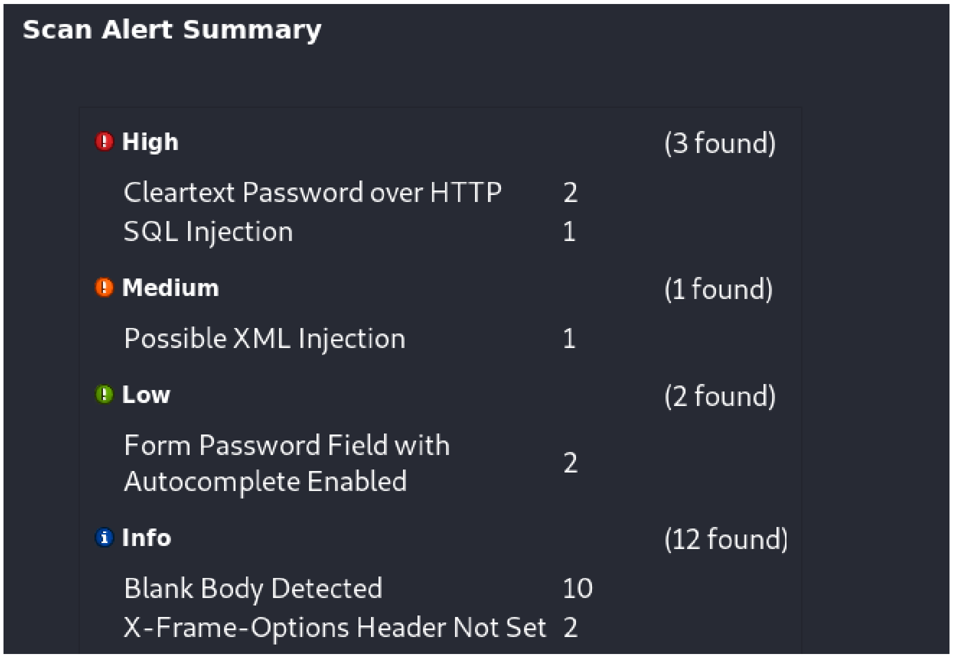
Command injection vulnerabilities often occur when inadequately sanitized externally supplied data is as part of a system command executed through a command interpreter, or shell. Vulnerabilities such as these can be exploited by using shell metacharacters to run additional commands that were not intended 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.

result (13)

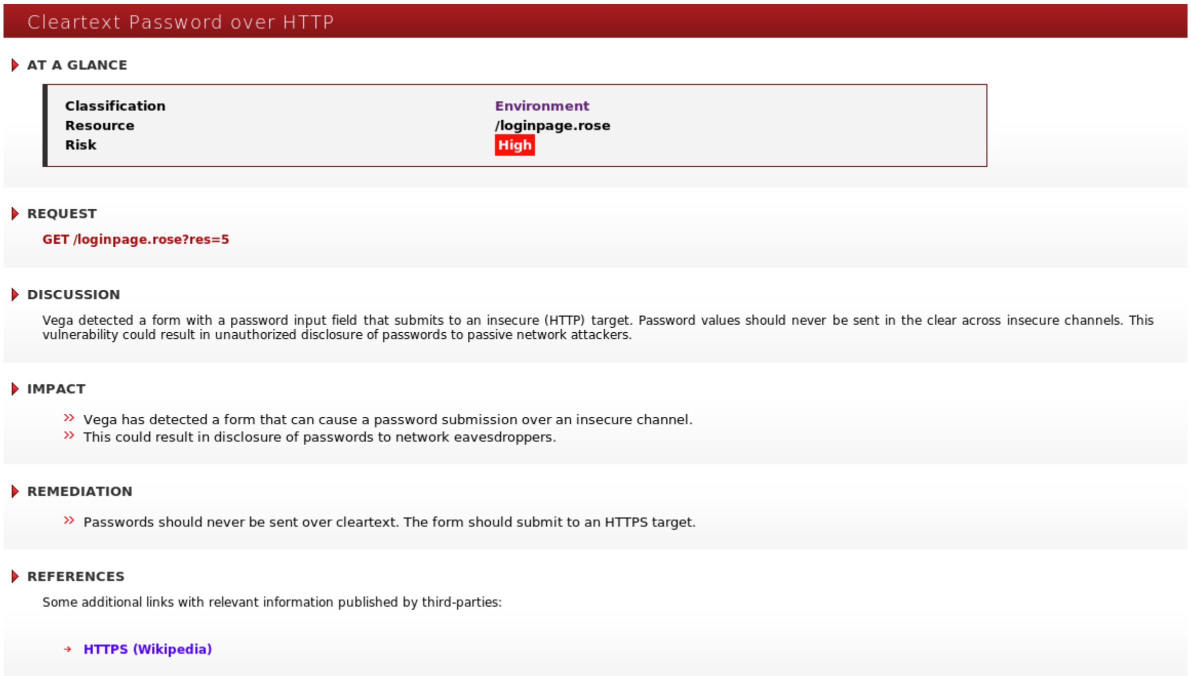
Scan bugs on food.guilan.ac.ir



```
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. Cleartext Password over HTTP bug (High)

- Vega has detected a form that can cause a password submission over an insecure channel.



Cleartext Password over HTTP

AT A GLANCE

Classification	Environment
Resource	/loginpage.rose
Risk	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

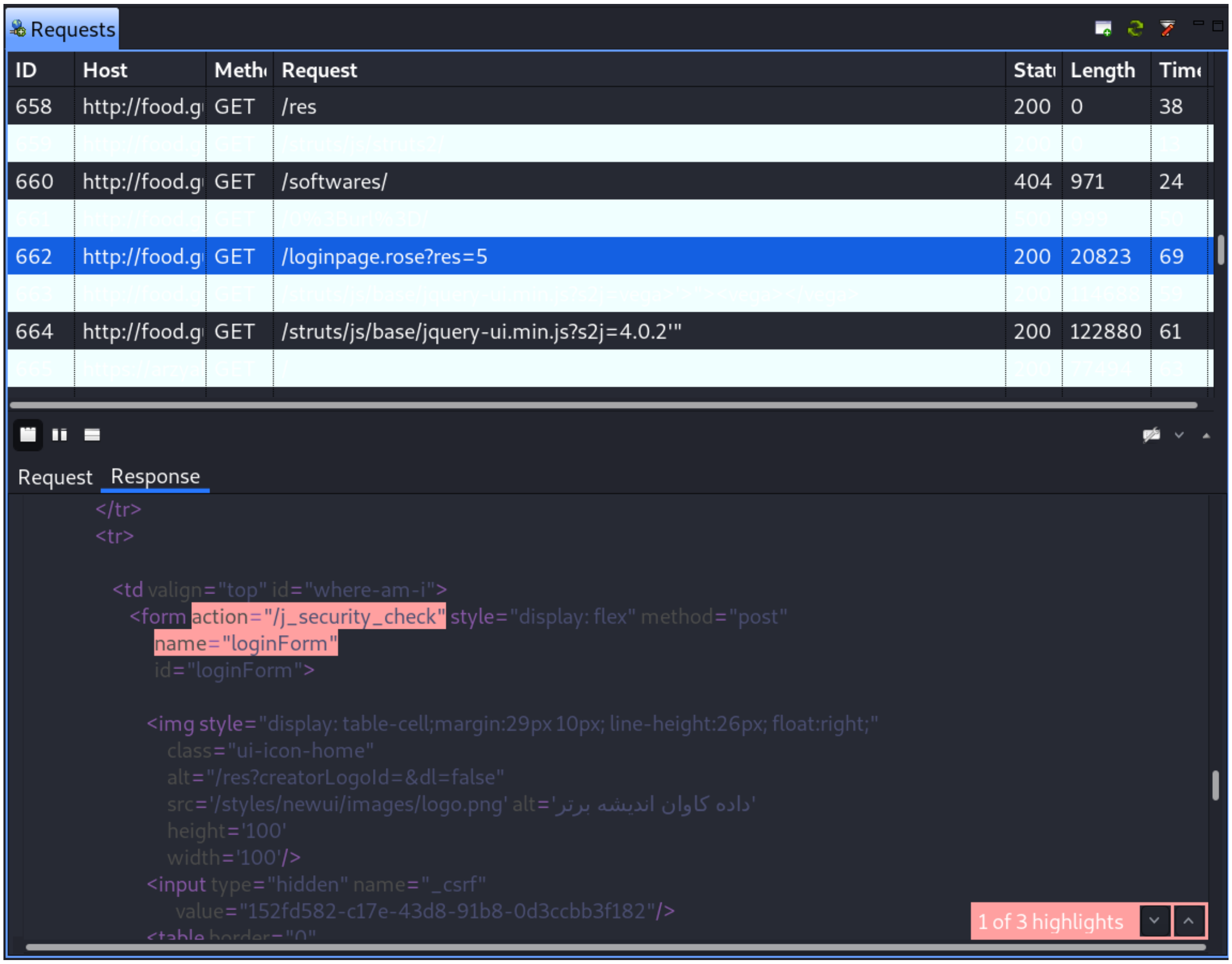
» Passwords should never be sent over cleartext. The form should submit to an HTTPS target.

REFERENCES

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

→ HTTPS (Wikipedia)

result (14)

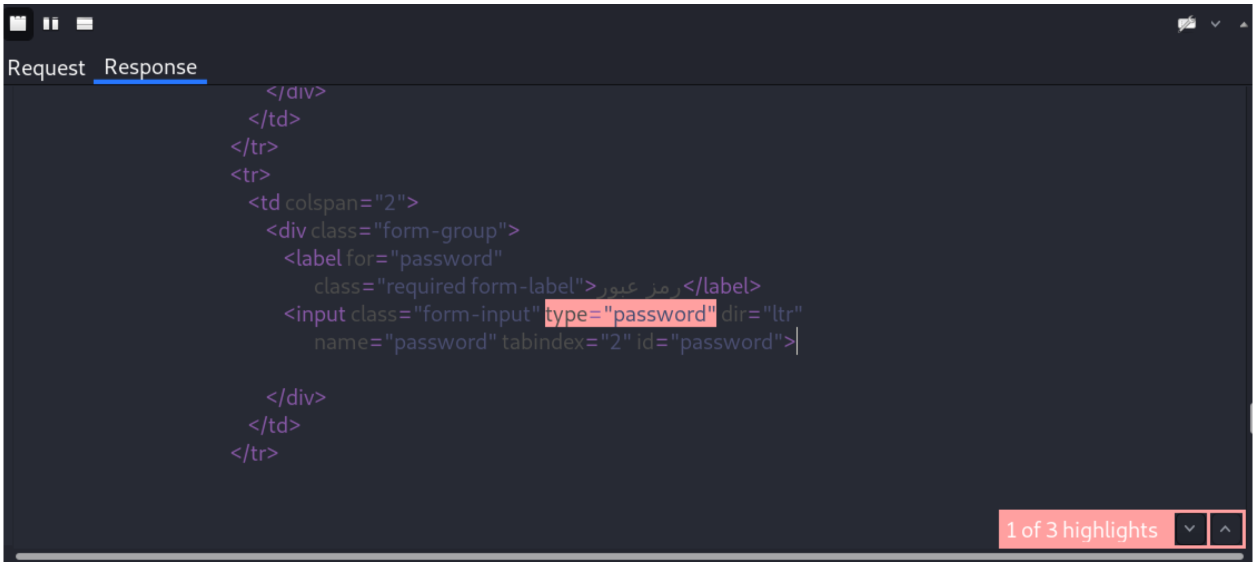


Requests

ID	Host	Meth	Request	Stat	Length	Time
658	http://food.g	GET	/res	200	0	38
659	http://food.g	GET	/struts/js/struts2/	200	0	13
660	http://food.g	GET	/softwares/	404	971	24
661	http://food.g	GET	/0%3Burl%3D/	500	999	50
662	http://food.g	GET	/loginpage.rose?res=5	200	20823	69
663	http://food.g	GET	/struts/js/base/jquery-ui.min.js?s2j=[illegible]	200	[illegible]	59
664	http://food.g	GET	/struts/js/base/jquery-ui.min.js?s2j=4.0.2'"	200	122880	61
665	https://arzyal	GET	/	200	77494	63

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">

              <img style="display: table-cell;margin:29px 10px; line-height:26px; float:right;"
                class="ui-icon-home"
                alt="/res?creatorLogoId=&dl=false"
                src='/styles/newui/images/logo.png' alt='داده کاوان اندیشه برتر'
                height='100'
                width='100'/>
              <input type="hidden" name="_csrf"
                value="152fd582-c17e-43d8-91b8-0d3ccbb3f182"/>
              <table border="0"
```

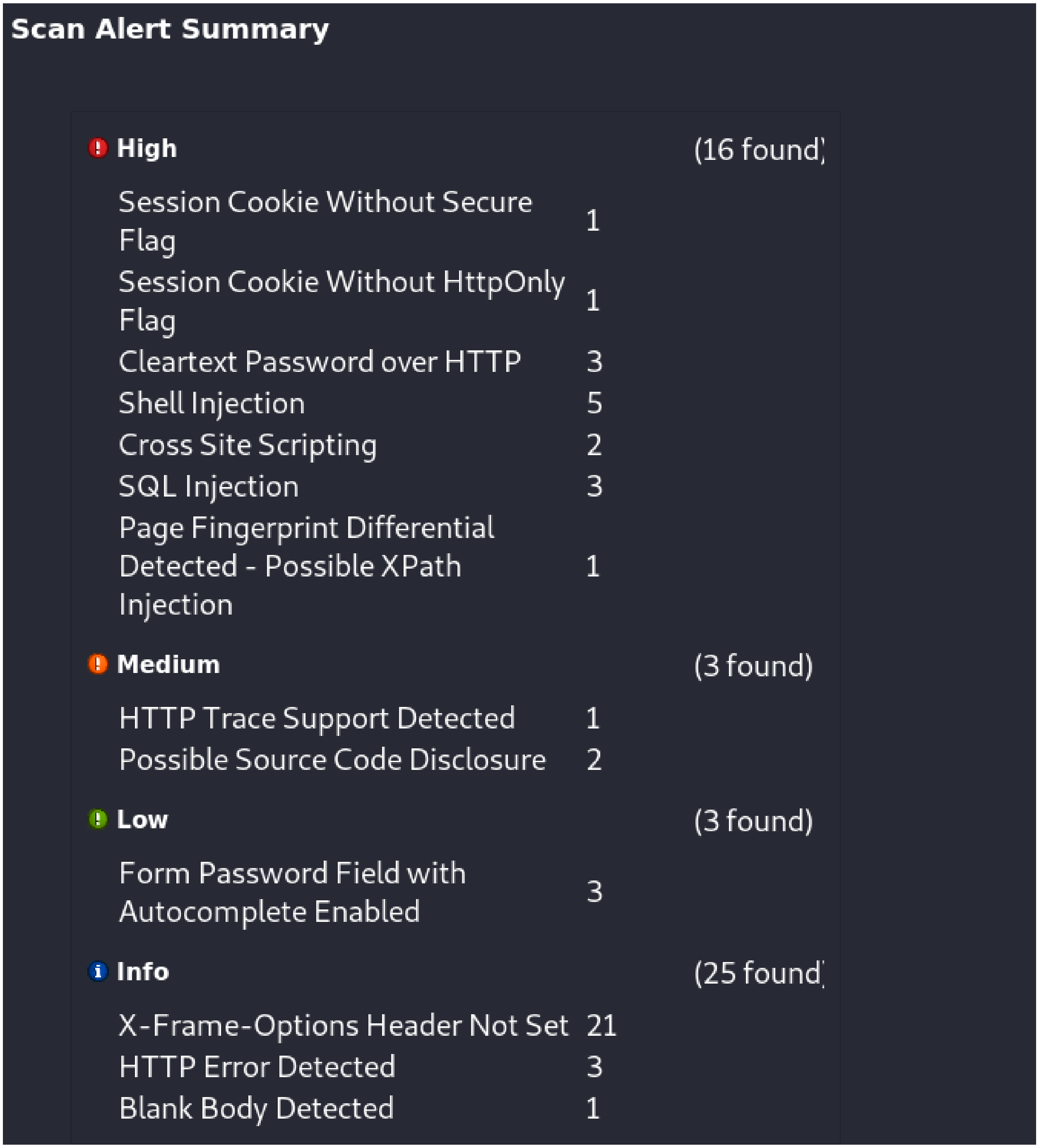


Request Response

```
                      </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>
```

result (15)

Scan bugs on courses.guilan.ac.ir

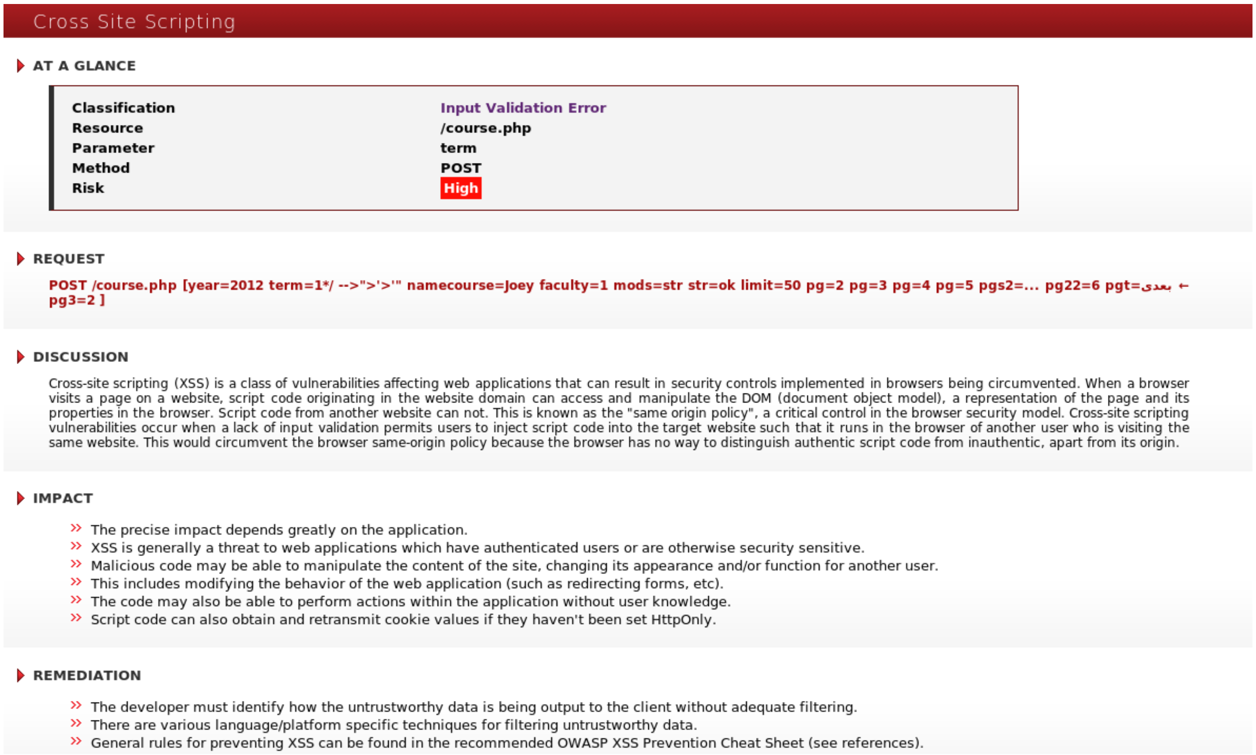


Scan Alert Summary

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	
Info		(25 found)
X-Frame-Options Header Not Set	21	
HTTP Error Detected	3	
Blank Body Detected	1	

10. Cross Site Scripting XSS bug (High)

- This bug allows the attacker to execute his own script on the website. These scripts can only be client-side languages, which means it is visible to the user.



Cross Site Scripting

AT A GLANCE

Classification	**Input Validation Error**
Resource	**/course.php**
Parameter	**term**
Method	**POST**
Risk	**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 pgt=بعدى ← pg3=2]

DISCUSSION

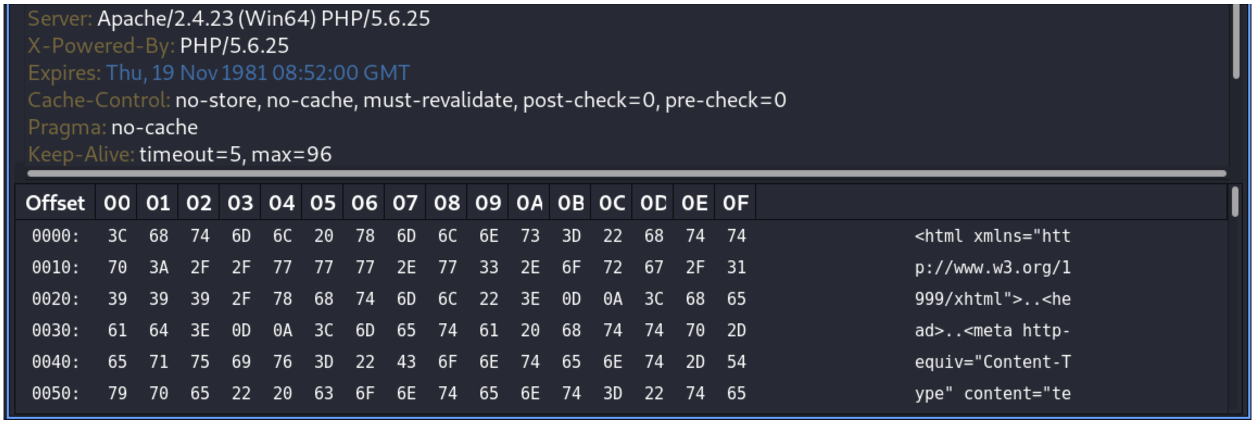
Cross-site scripting (XSS) is a class of vulnerabilities affecting web applications that can result in security controls implemented in browsers being circumvented. When a browser visits a page on a website, script code originating in the website domain can access and manipulate the DOM (document object 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).



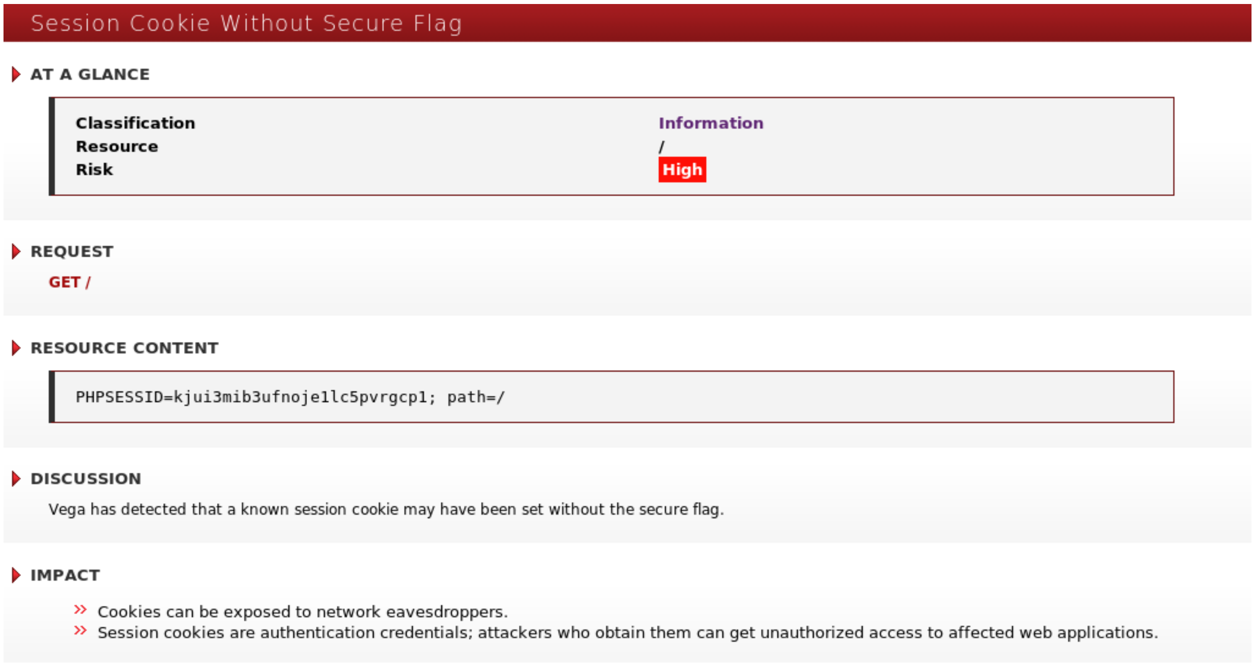
```
Server: Apache/2.4.23 (Win64) PHP/5.6.25
X-Powered-By: PHP/5.6.25
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, post-check=0, pre-check=0
Pragma: no-cache
Keep-Alive: timeout=5, max=96
```

```
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
```

result (16)

11. Session Cookie Without Secure Flag bug (High)

- A cookie is a client-side file that contains information, this information can be items in your shopping cart or your username and password. attackers who obtain them can get unauthorized access to affected web applications.



Session Cookie Without Secure Flag

AT A GLANCE

Classification	Information
Resource	/
Risk	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.

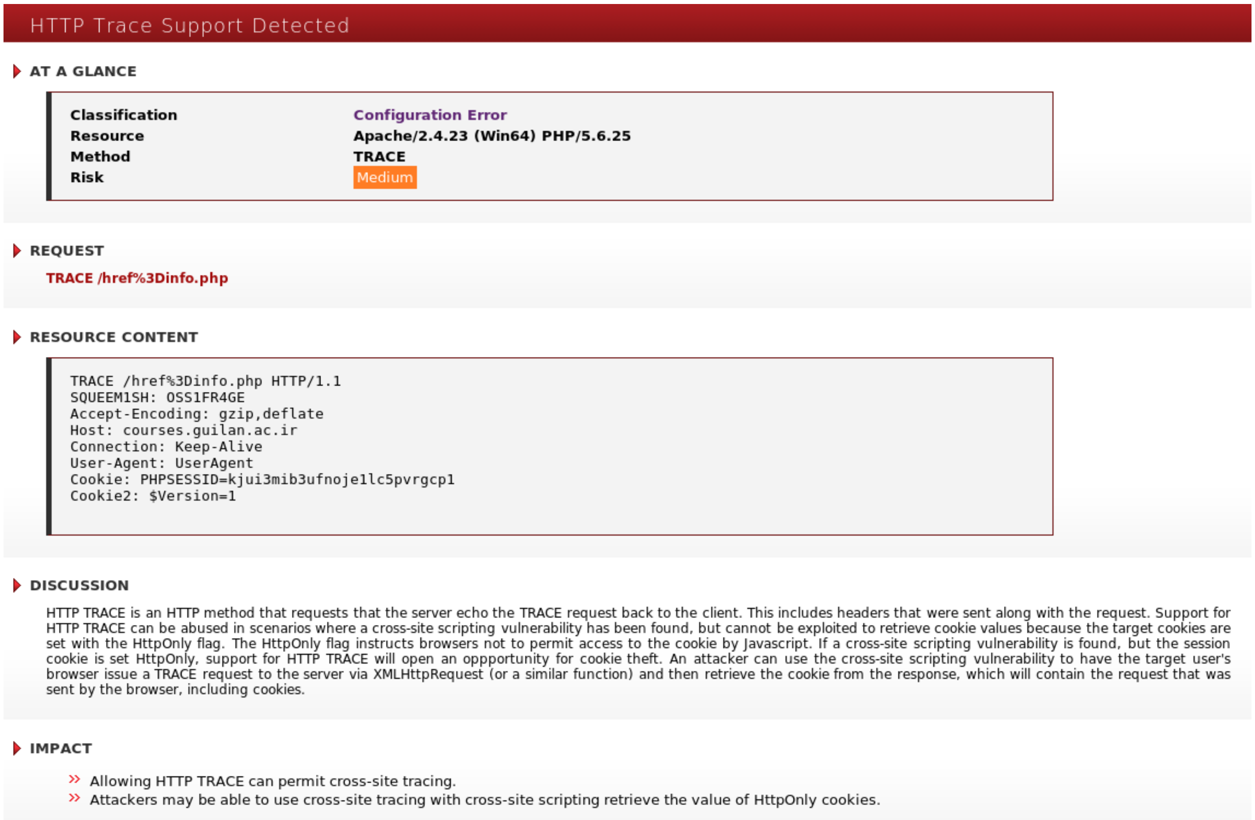
IMPACT

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

result (17)

12. HTTP Trace Support Detected bug (High)

- By this bug, attackers may be able to use cross-site tracing with cross-site scripting to retrieve the value of HttpOnly cookies.



HTTP Trace Support Detected

AT A GLANCE

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

REQUEST

TRACE /href%3Dinfo.php

RESOURCE CONTENT

```
TRACE /href%3Dinfo.php HTTP/1.1
SQUEEM1SH: OSS1FR4GE
Accept-Encoding: gzip,deflate
Host: courses.guilan.ac.ir
Connection: Keep-Alive
User-Agent: UserAgent
Cookie: PHPSESSID=kjui3mib3ufnoje1lc5pvrgcp1
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 oppportunity 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.

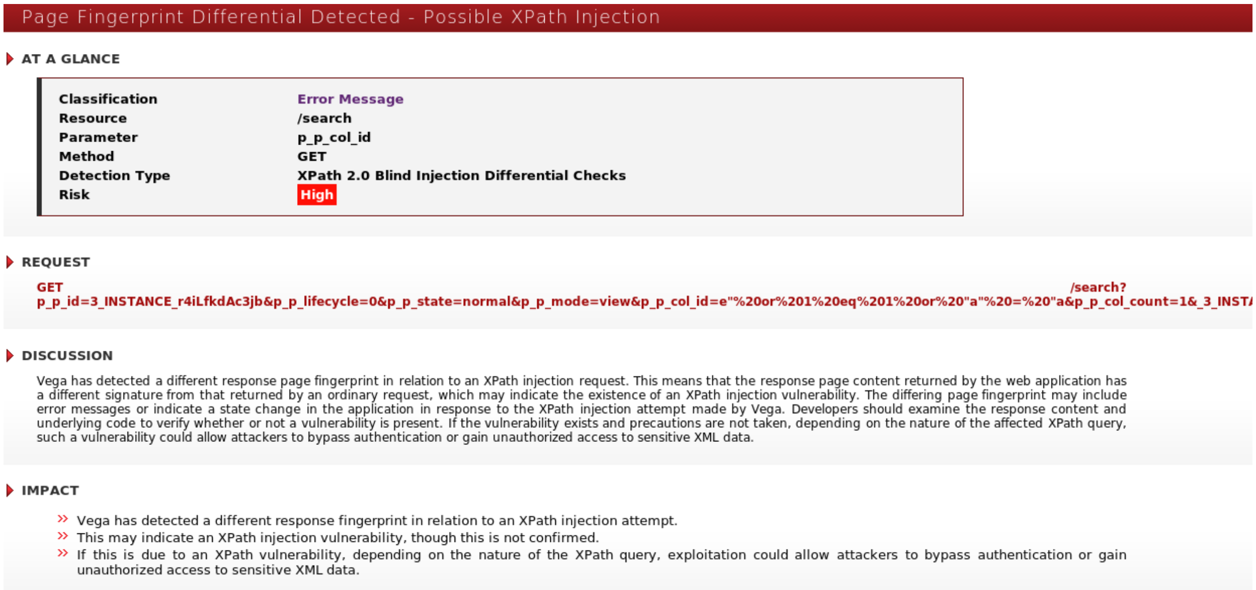
IMPACT

- 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.

result (18)

13. Session Cookie Without Secure Flag bug (High)

- With this bug, an attacker can obtain server source code from a web application, which may contain sensitive information such as database connection strings, usernames, and passwords.



Page Fingerprint Differential Detected - Possible XPath Injection

AT A GLANCE

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

REQUEST

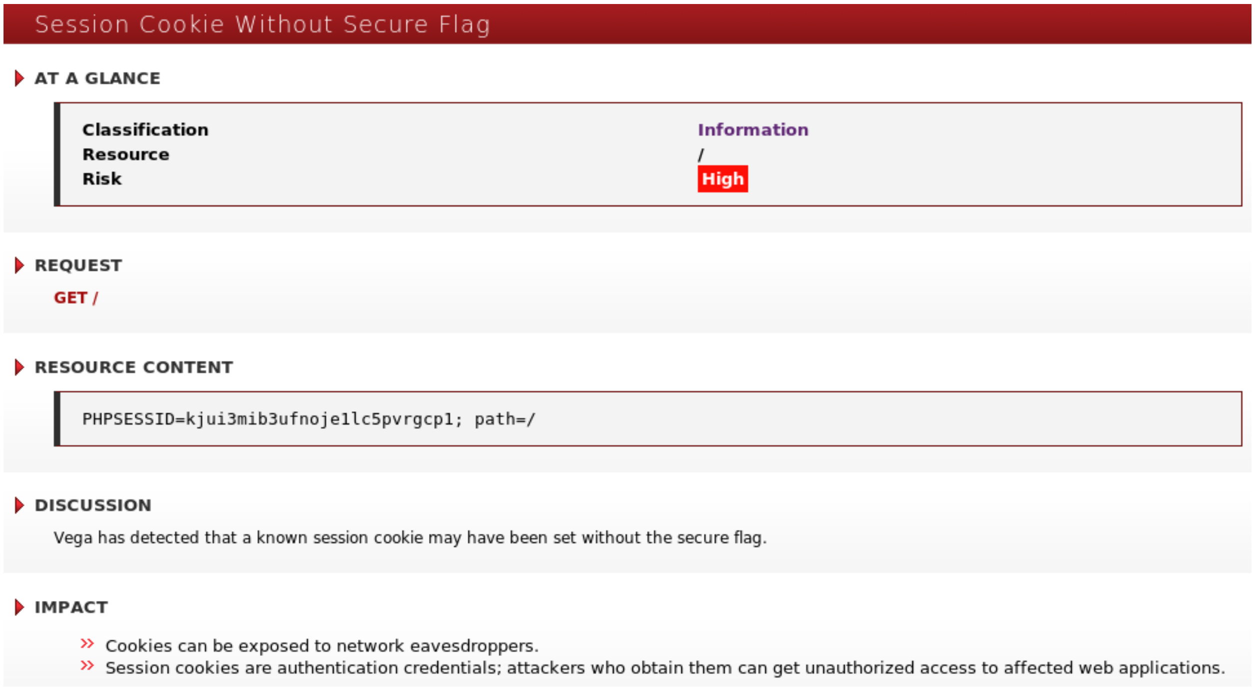
```
GET /search?
p_p_id=3_INSTANCE_r4iLfkdAc3jb&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=e"%20or%201%20eq%201%20or%20"a"%20=%20"a&p_p_col_count=1&_3_INST
```

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

Classification	Information
Resource	/
Risk	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

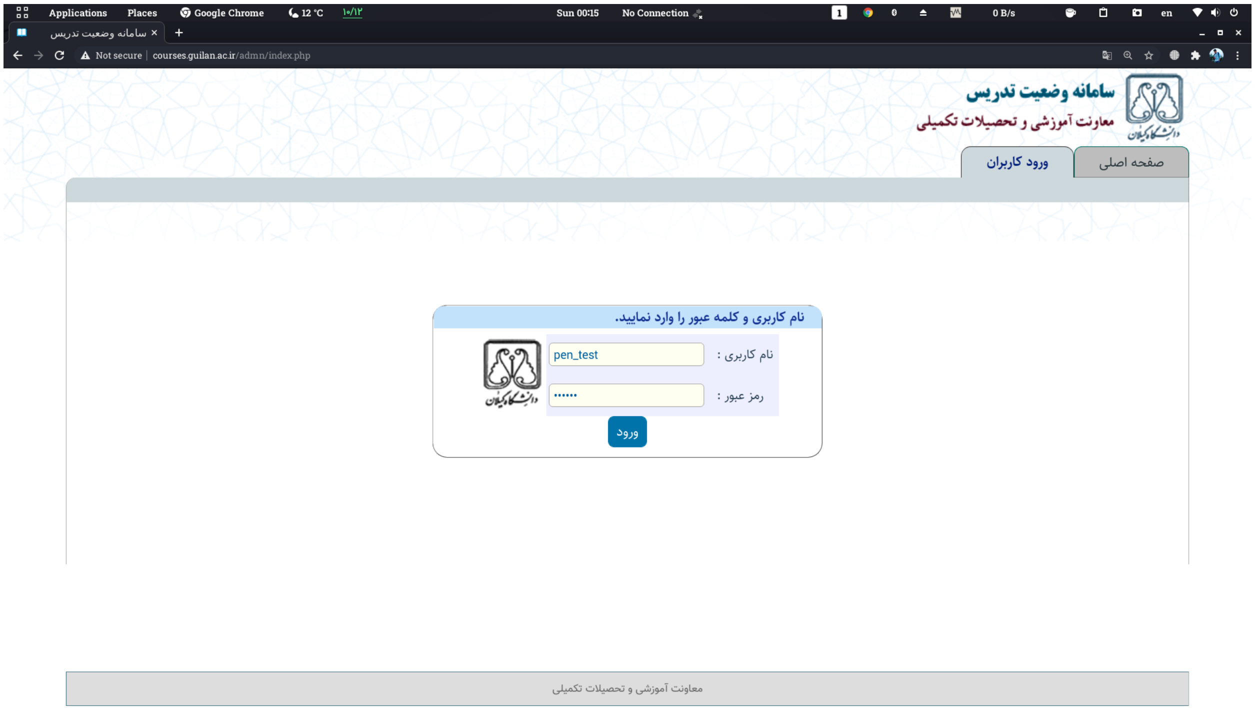
- Cookies can be exposed to network eavesdroppers.
- Session cookies are authentication credentials; attackers who obtain them can get unauthorized access to affected web applications.

result (19)

- As we can see, the last site has the most sensitive and largest number of security bugs. In this case, we can start the penetration test on the same site.

Exploitation of the bug Cleartext Password over HTTP

- One of the best penetration testing tools in this field is Wireshark. With this tool, we can obtain the data exchanged between the server and user, which in the following test, we can easily see the username and password in text form.
- First, we open the wireshark tool and start a new session, then we enter the target site with the desired browser, and go to the user login section, then enter the username and password.



نام کاربری و کلمه عبور را وارد نمایید.

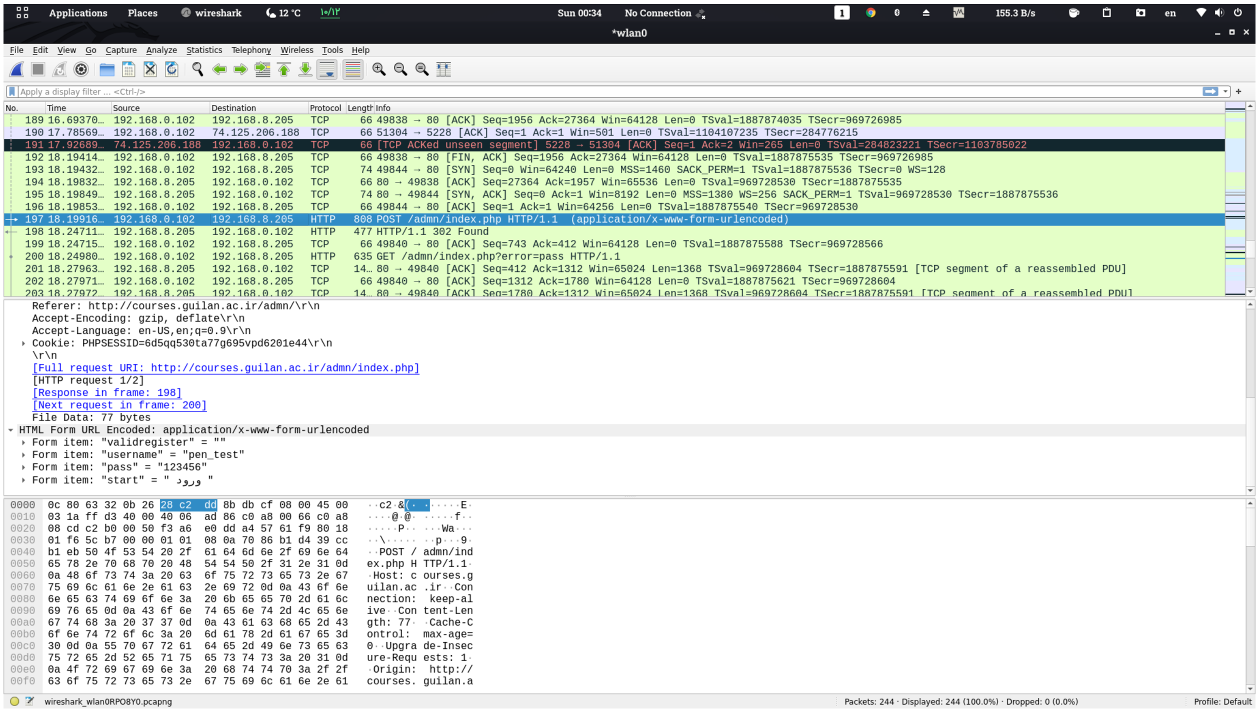
نام کاربری : pen_test

رمز عبور : ••••••

❖ in the image above, we used (pent_test) as username and (123456) as password

3-1- Conclusion

- As we can see, the wireshark tool showed us the targeted data, in the image below the package number 197 shows the information that we entered in the previous image using the Cleartext Password over HTTP vulnerability.

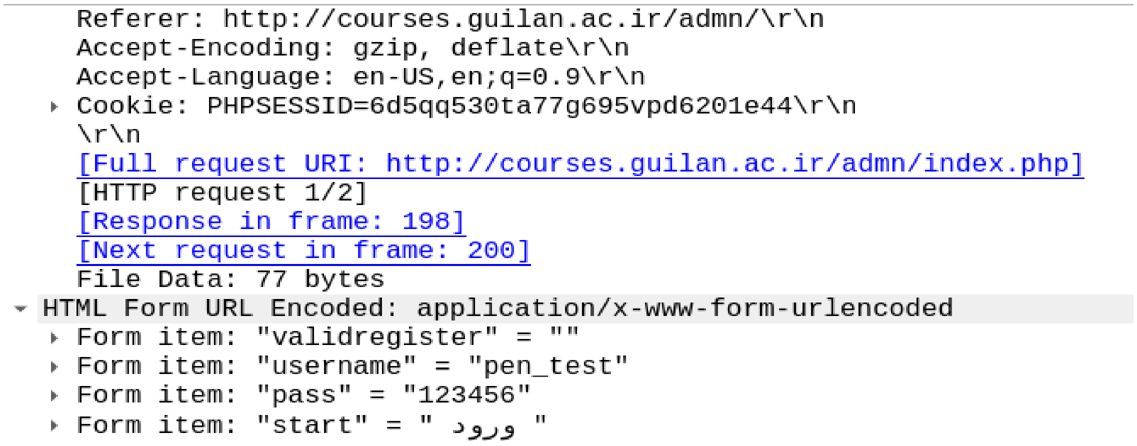


```
No.  Time         Source          Destination     Protocol Length Info
 189 16.69370…  192.168.0.102   192.168.8.205   TCP        66 49838 → 80 [ACK] Seq=1956 Ack=27364 Win=64128 Len=0 TSval=1887874035 TSecr=969726985
 190 17.78569…  192.168.0.102   74.125.206.188  TCP        66 51304 → 5228 [ACK] Seq=1 Ack=1 Win=501 Len=0 TSval=1104107235 TSecr=284776215
 191 17.92689…  74.125.206.188  192.168.0.102   TCP        66 [TCP ACKed unseen segment] 5228 → 51304 [ACK] Seq=1 Ack=2 Win=265 Len=0 TSval=284823221 TSecr=1103785022
 192 18.19414…  192.168.0.102   192.168.8.205   TCP        66 49838 → 80 [FIN, ACK] Seq=1956 Ack=27364 Win=64128 Len=0 TSval=1887875535 TSecr=969726985
 193 18.19432…  192.168.0.102   192.168.8.205   TCP        74 49844 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=1887875536 TSecr=0 WS=128
 194 18.19832…  192.168.8.205   192.168.0.102   TCP        66 80 → 49838 [ACK] Seq=27364 Ack=1957 Win=65536 Len=0 TSval=969728530 TSecr=1887875535
 195 18.19849…  192.168.8.205   192.168.0.102   TCP        74 80 → 49844 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1380 WS=256 SACK_PERM=1 TSval=969728530 TSecr=1887875536
 196 18.19853…  192.168.0.102   192.168.8.205   TCP        66 49844 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=1887875540 TSecr=969728530
 197 18.19916…  192.168.0.102   192.168.8.205   HTTP      808 POST /admn/index.php HTTP/1.1  (application/x-www-form-urlencoded)
 198 18.24711…  192.168.8.205   192.168.0.102   HTTP      477 HTTP/1.1 302 Found
 199 18.24715…  192.168.0.102   192.168.8.205   TCP        66 49840 → 80 [ACK] Seq=743 Ack=412 Win=64128 Len=0 TSval=1887875588 TSecr=969728566
 200 18.24980…  192.168.0.102   192.168.8.205   HTTP      635 GET /admn/index.php?error=pass HTTP/1.1
 201 18.27963…  192.168.8.205   192.168.0.102   TCP       14… 80 → 49840 [ACK] Seq=412 Ack=1312 Win=65024 Len=1368 TSval=969728604 TSecr=1887875591 [TCP segment of a reassembled PDU]
 202 18.27971…  192.168.0.102   192.168.8.205   TCP        66 49840 → 80 [ACK] Seq=1312 Ack=1780 Win=64128 Len=0 TSval=1887875621 TSecr=969728604
 203 18.27972…  192.168.8.205   192.168.0.102   TCP       14… 80 → 49840 [ACK] Seq=1780 Ack=1312 Win=65024 Len=1368 TSval=969728604 TSecr=1887875591 [TCP segment of a reassembled PDU]
```

```
    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 "
```

```
0000  0c 80 63 32 0b 26 28 c2  dd 8b db cf 08 00 45 00   ··c2·&(· ·····E·
0010  03 1a ff d3 40 00 40 06  ad 86 c0 a8 00 66 c0 a8   ····@·@· ·····f··
0020  08 cd c2 b0 00 50 f3 a6  e0 dd a4 57 61 f9 80 18   ·····P·· ···Wa···
0030  01 f6 5c b7 00 00 01 01  08 0a 70 86 b1 d4 39 cc   ··\····· ··p···9·
0040  b1 eb 50 4f 53 54 20 2f  61 64 6d 6e 2f 69 6e 64   ··POST / admn/ind
0050  65 78 2e 70 68 70 20 48  54 54 50 2f 31 2e 31 0d   ex.php H TTP/1.1·
0060  0a 48 6f 73 74 3a 20 63  6f 75 72 73 65 73 2e 67   ·Host: c ourses.g
0070  75 69 6c 61 6e 2e 61 63  2e 69 72 0d 0a 43 6f 6e   uilan.ac .ir··Con
0080  6e 65 63 74 69 6f 6e 3a  20 6b 65 65 70 2d 61 6c   nection:  keep-al
0090  69 76 65 0d 0a 43 6f 6e  74 65 6e 74 2d 4c 65 6e   ive··Con tent-Len
00a0  67 74 68 3a 20 37 37 0d  0a 43 61 63 68 65 2d 43   gth: 77· ·Cache-C
00b0  6f 6e 74 72 6f 6c 3a 20  6d 61 78 2d 61 67 65 3d   ontrol:  max-age=
00c0  30 0d 0a 55 70 67 72 61  64 65 2d 49 6e 73 65 63   0··Upgra de-Insec
00d0  75 72 65 2d 52 65 71 75  65 73 74 73 3a 20 31 0d   ure-Requ ests: 1·
00e0  0a 4f 72 69 67 69 6e 3a  20 68 74 74 70 3a 2f 2f   ·Origin:  http://
00f0  63 6f 75 72 73 65 73 2e  67 75 69 6c 61 6e 2e 61   courses. guilan.a
```

wireshark_wlan0RPO8Y0.pcapng   Packets: 244 · Displayed: 244 (100.0%) · Dropped: 0 (0.0%)   Profile: Default



```
    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 "
```

result (20)

The end