WHITEAB
سرویس ابری ارزیابی امنیتی

گزارش مقدماتی

سیستم بررسی امنیتی خودکار وایت‌لب

تست نفوذ برنامه تحت وب

ارائه شده توسط آزمایشگاه امنیت وایت‌لب

WhiteLab.ir | @WhiteLabir | info@WhiteLab.ir

بررسی امنیتی وب سایت 192.168.1.181

اطلاعات بررسی وب سایت

مشخصات پایه			
مدت زمان بررسی	26 دقیقه و 7 ثانیه	زمان شروع	10:15:48 ,08/03/2019
آدرس وب سایت	/http://example.com	هدف	example.com

مشخصات دیگر	
اطلاعات میزبان	Apache/2.4.29 (Ubuntu)

سطح آسیب پذیری

وضعیت وب‌سایت از نظر امنیتی خطرناک است

یک یا چند آسیب پذیری با اهمیت بالا توسط کاوشگر کشف شده اند

امکان سواستفاده توسط فرد مهاجم وجود دارد

هشدار های یافت شده 21	
خطرناک	5
ریسک پذیر	8
عادی	6
دیگر اطلاعات	2

WordPress 4.3 Multiple Vulnerabilities (0.7 - 4.3)

خطرناک

مسیر آسیب پذیر	/wordpress/
پارامتر آسیب پذیر	-

شرح

```
GET /wordpress/ HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

WordPress Cross-Site Scripting Vulnerability (0.70 - 4.1.1)

خطرناک

مسیر آسیب پذیر	/wordpress/
پارامتر آسیب پذیر	-

شرح

```
GET /wordpress/ HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

WordPress Cross-Site Scripting Vulnerability (3.9.3 - 4.2)

خطرناک

مسیر آسیب پذیر	/wordpress/
پارامتر آسیب پذیر	-

شرح

```
GET /wordpress/ HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

WordPress Directory Traversal (3.7 - 5.0.3)

خطرناک

مسیر آسیب پذیر	/wordpress/
پارامتر آسیب پذیر	-

شرح

```
GET /wordpress/ HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

WordPress Plugin Akismet Cross-Site Scripting (3.1.4)

خطرناک

مسیر آسیب پذیر	/wordpress/
پارامتر آسیب پذیر	-

شرح

```
GET /wordpress/wp-content/plugins/akismet/readme.txt HTTP/1.1
Connection: keep-alive
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
```

Directory listing	ریسک پذیر
میزبان	مسیر آسیب پذیر
-	پارامتر آسیب پذیر

شرح

```
GET / HTTP/1.1
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Directory listing	ریسک پذیر
/wordpress/wp-content/upgrade/	مسیر آسیب پذیر
-	پارامتر آسیب پذیر

شرح

```
GET /wordpress/wp-content/upgrade/ HTTP/1.1
Cookie:
comment_author_47a3a002389a2ff102883022698974c8=HfjNUlYZ;comment_author_email
_47a3a002389a2ff102883022698974c8=test%40whitelab.wlab;comment_author_url_47a
3a002389a2ff102883022698974c8=http%3A%2F%2Fcb.whitelab.ir;wordpress_47a3a0023
89a2ff102883022698974c8=+;wordpress_logged_in_47a3a002389a2ff102883022698974c
8=+;wordpress_sec_47a3a002389a2ff102883022698974c8=+;wordpress_test_cookie=WP
+Cookie+check;wordpresspass_47a3a002389a2ff102883022698974c8=+;wordpressuser_
47a3a002389a2ff102883022698974c8=+
Accept: */*
Accept-Encoding: gzip,deflate
```

```
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Directory listing	ریسک پذیر
/wordpress/wp-includes/ID3/	مسیر آسیب پذیر
-	پارامتر آسیب پذیر

شرح

```
GET /wordpress/wp-includes/ID3/ HTTP/1.1
Cookie:
comment_author_47a3a002389a2ff102883022698974c8=HfjNUlYZ;comment_author_email
_47a3a002389a2ff102883022698974c8=test%40whitelab.wlab;comment_author_url_47a
3a002389a2ff102883022698974c8=http%3A%2F%2Fcb.whitelab.ir;wordpress_47a3a0023
89a2ff102883022698974c8=+;wordpress_logged_in_47a3a002389a2ff102883022698974c
8=+;wordpress_sec_47a3a002389a2ff102883022698974c8=+;wordpress_test_cookie=WP
+Cookie+check;wordpresspass_47a3a002389a2ff102883022698974c8=+;wordpressuser_
47a3a002389a2ff102883022698974c8=+
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Directory listing	ریسک پذیر
/wordpress/wp-includes/SimplePie/	مسیر آسیب پذیر
-	پارامتر آسیب پذیر

شرح

```
GET /wordpress/wp-includes/SimplePie/ HTTP/1.1
Cookie:
comment_author_47a3a002389a2ff102883022698974c8=HfjNUlYZ;comment_author_email
_47a3a002389a2ff102883022698974c8=test%40whitelab.wlab;comment_author_url_47a
3a002389a2ff102883022698974c8=http%3A%2F%2Fcb.whitelab.ir;wordpress_47a3a0023
89a2ff102883022698974c8=+;wordpress_logged_in_47a3a002389a2ff102883022698974c
8=+;wordpress_sec_47a3a002389a2ff102883022698974c8=+;wordpress_test_cookie=WP
+Cookie+check;wordpresspass_47a3a002389a2ff102883022698974c8=+;wordpressuser_
```

```
47a3a002389a2ff102883022698974c8=+
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Directory listing

ریسک پذیر

مسیر آسیب پذیر	/wordpress/wp-includes/js/
پارامتر آسیب پذیر	-

شرح

```
Cookie:
comment_author_47a3a002389a2ff102883022698974c8=HfjNUlYZ;comment_author_email
_47a3a002389a2ff102883022698974c8=test%40whitelab.wlab;comment_author_url_47a
3a002389a2ff102883022698974c8=http%3A%2F%2Fcb.whitelab.ir;wordpress_47a3a0023
89a2ff102883022698974c8=+;wordpress_logged_in_47a3a002389a2ff102883022698974c
8=+;wordpress_sec_47a3a002389a2ff102883022698974c8=+;wordpress_test_cookie=WP
+Cookie+check;wordpresspass_47a3a002389a2ff102883022698974c8=+;wordpressuser_
47a3a002389a2ff102883022698974c8=+
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Vulnerable Javascript library

ریسک پذیر

مسیر آسیب پذیر	/wordpress/wp-includes/js/jquery/jquery.js
پارامتر آسیب پذیر	-

شرح

```
GET /wordpress/wp-includes/js/jquery/jquery.js HTTP/1.1
Cookie:
comment_author_47a3a002389a2ff102883022698974c8=HfjNUlYZ;comment_author_email
_47a3a002389a2ff102883022698974c8=test%40whitelab.wlab;comment_author_url_47a
3a002389a2ff102883022698974c8=http%3A%2F%2Fcb.whitelab.ir;wordpress_47a3a0023
89a2ff102883022698974c8=+;wordpress_logged_in_47a3a002389a2ff102883022698974c
```

```
8=+;wordpress_sec_47a3a002389a2ff102883022698974c8=+;wordpress_test_cookie=WP
+Cookie+check;wordpresspass_47a3a002389a2ff102883022698974c8=+;wordpressuser_
47a3a002389a2ff102883022698974c8=+
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

WordPress XML-RPC authentication brute force

ریسک پذیر

مسیر آسیب پذیر	/wordpress/xmlrpc.php
پارامتر آسیب پذیر	-

شرح

```
POST /wordpress//xmlrpc.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Connection: keep-alive
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 264
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
<?xml version="1.0" encoding="iso-8859-1"?>
<methodCall>
<methodName>wp.getUsersBlogs</methodName>
<params>
<param><value><string>admin</string></value></param>
<param><value><string>8947589543789543753498 7</string></value>
</param>
</params>
</methodCall>
```

WordPress username enumeration

ریسک پذیر

مسیر آسیب پذیر	/wordpress/
پارامتر آسیب پذیر	-

شرح

```
POST /wordpress//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Connection: keep-alive
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 32
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
log=example&pwd=z&wp-submit=Login
```

Clickjacking: X-Frame-Options header missing

عادی

مسیر آسیب پذیر	میزبان
پارامتر آسیب پذیر	-

شرح

```
GET / HTTP/1.1
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
```

Cookie(s) without HttpOnly flag set

عادی

مسیر آسیب پذیر	میزبان
پارامتر آسیب پذیر	-

شرح

```
GET /wordpress/wp-login.php HTTP/1.1
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Documentation file	عادی
مسیر آسیب پذیر	میزبان
پارامتر آسیب پذیر	-

شرح

```
GET /wordpress/readme.html HTTP/1.1
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
```

Login page password-guessing attack	عادی
مسیر آسیب پذیر	/wordpress/wp-login.php
پارامتر آسیب پذیر	-

شرح

```
POST /wordpress/wp-login.php HTTP/1.1
Content-Type: application/x-www-form-urlencoded
Referer: http://example.com/
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 125
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
log=t7pyVDLA&pwd=fXEX1Ham&redirect_to=http://example.com/wordpress/wp-
admin/&rememberme=forever&testcookie=1&wp-submit=Log%20In
```

WordPress admin accessible without HTTP authentication

عادی

مسیر آسیب پذیر	میزبان
پارامتر آسیب پذیر	-

شرح

```
GET /wordpress/wp-admin/ HTTP/1.1
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
```

WordPress default administrator account

عادی

مسیر آسیب پذیر	/wordpress/wp-login.php
پارامتر آسیب پذیر	-

شرح

```
POST /wordpress//wp-login.php HTTP/1.1
Content-type: application/x-www-form-urlencoded
Connection: keep-alive
Cookie: wordpress_test_cookie=WP+Cookie+check
Accept: */*
Accept-Encoding: gzip,deflate
Content-Length: 42
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
log=admin&pwd=Whitelabtest&wp-submit=Login
```

Content Security Policy (CSP) not implemented

سایر اطلاعات

مسیر آسیب پذیر	میزبان
پارامتر آسیب پذیر	-

شرح

```
GET / HTTP/1.1
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
Connection: Keep-alive
```

Error page web server version disclosure	سایر اطلاعات
میزبان	مسیر آسیب پذیر
-	پارامتر آسیب پذیر

شرح

```
GET /suSY2ZTcfG HTTP/1.1
Connection: keep-alive
Accept: */*
Accept-Encoding: gzip,deflate
Host: example.com
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.21 (KHTML,
like Gecko) Chrome/41.0.2228.0 Safari/537.21
```