Комерциялық емес акционерлік қоғамы

Ғұмарбек Дәукеев атындағы «АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»

Ақпараттық технологиялар институты

Ақпараттық жүйелері және киберқауіпсіздік кафедрасы

**№1 Лабораториялық жұмыс**

Пәні: Енуге тестілеу

Тақырыбы: «Burp suite community edition» плагинінің жұмыс принципін зерттеу

Білім беру бағдарламасы: 6В06102–«Ақпараттық Қауіпсіздік Жүйелері»

Орындаған: Касымов Даулет Тобы: СИБк-20-1

Тексерген: т.ғ.м, аға оқытушы Наубетов Д.\_\_\_\_\_\_\_

(ғылыми дәрежесі, лауазымы, аты-жөні)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(баға) (қолы)

Алматы 2023

Мазмұны

Кіріспе.......................................................................................................................3

Негізгі бөлім.............................................................................................................4

Қорытынды..............................................................................................................9

Қолданылған әдебиеттер тізімі.............................................................................10

**Кіріспе**

Қазіргі ақпараттық қауіпсіздік әлемінде цифрлық активтер мен деректердің құпиялылығын қорғауды қамтамасыз ету барған сайын маңызды бола түсуде. Өздеріңіз білетіндей, қауіпсіздік статикалық ұғым емес және қауіптер үнемі дамып отырады. Бұл тұрғыда ақпараттық қауіпсіздік мамандары арасында веб-қосымшалардың қауіпсіздігін талдауға және тексеруге арналған құралдар кеңінен танымал.

Киберқауіпсіздік мамандары назар аударатын осындай құралдардың бірі - "Burp Suite Community Edition". Бұл қуатты және икемді құрал шабуылдаушылар шабуылдар мен рұқсатсыз кіру үшін пайдалана алатын осалдықтарды анықтау үшін веб-қосымшаларды сканерлеуге және талдауға арналған.

Бұл зертханалық жұмыстың мақсаты-"Burp Suite Community Edition" плагинінің жұмыс принциптерін және оның веб-қосымшалардың қауіпсіздігін талдау саласындағы мүмкіндіктерін зерттеу. Жұмыстың бір бөлігі ретінде біз осы плагин ұсынатын негізгі функциялар мен құралдарды қарастырамыз, сонымен қатар оны веб-қосымшалардағы ықтимал осалдықтарды анықтау үшін қолдануды үйренеміз.

Бұл зертханалық жұмыс ақпараттық қауіпсіздік саласындағы студенттер мен мамандарға тиімді тестілеу және қазіргі цифрлық әлемде веб-қосымшалардың қауіпсіздігін қамтамасыз ету үшін қажетті практикалық дағдылар мен білім алуға мүмкіндік береді.

**Негізгі бөлім**

Burp Suite бағдарламасының негізгі құралдарымен танысу.

Target. Бұл құрал осалдықтарды тексеру процесін тиімдірек басқаруға мүмкіндік беретін қажет қосымшалар туралы егжей-тегжейлі деректерді қамтиды. Яғни, мұнда біздің жалпылама мақсаттарымыз бен олар туралы ақпараттарды көре аламыз.

Proxy. Веб-браузер пен мақсатты веб-қосымша арасында көпңр ретінде жұмыс істейтін веб-прокси. Толықпаған трафикті екі бағытта ұстап алуға, өзгертуге және тексеруге мүмкіндік береді. Бұл өзгелерінен қарағанда қажеттірік құрал. Сұраныс жүріп жатқан браузер мен сервер арасындағы трафикті ұстайды. Сондай-ақ трафикті тек ұстап қана қоймай, өзгерте де алады.

Intruder. Қосымшаға автоматтандырылған жеке шабуылдар жасауға арналған өте қуатты құрал. Конфигурациялауға жеңіл және көптеген тапсырмаларды орындау кезінде қолдануға қабілетті, бұл тестілеуді тезірек және тиімдірек етеді.

Repeater. Веб-қосымшаның жауаптарын талдай отырып, жеке HTTP сұрауларын қолмен басқарудың және қайта жіберудің қарапайым құралы. Мұнда жіберілген сұраныстарды көруге, оларды қайта жіберуге және сұранысымызға алған жауапты көре аламыз.

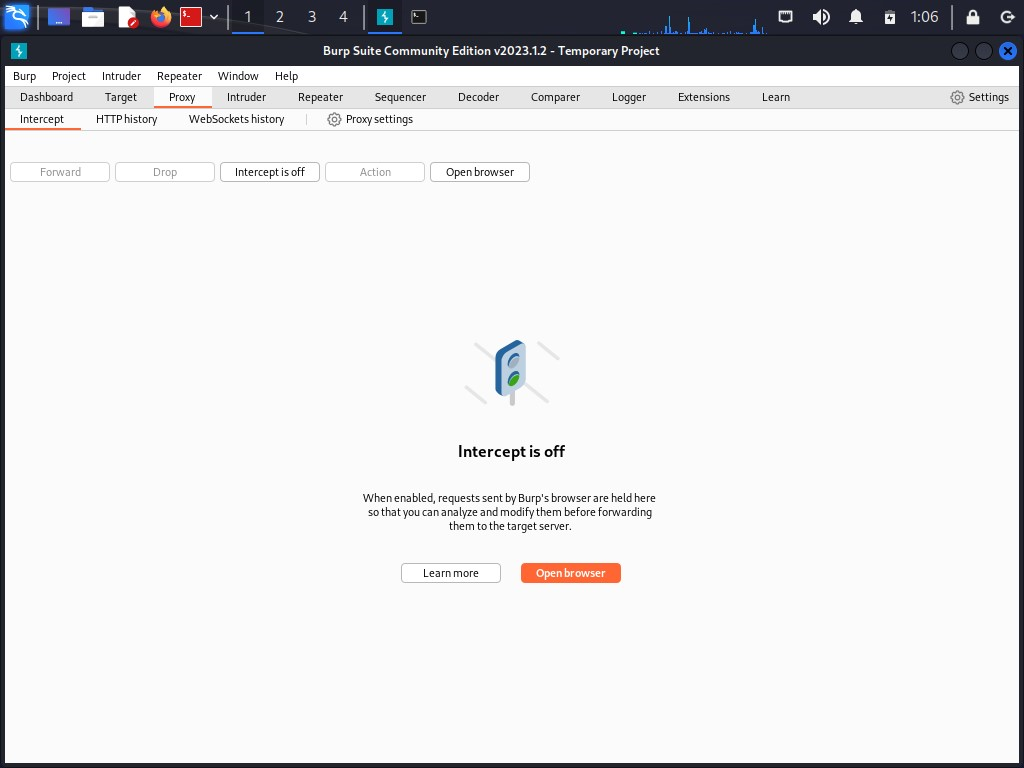
Sequencer. Веб-қосымшаның сеанс токендеріндегі кездейсоқтық қасиеттерін немесе болжауға болмайтын басқа да маңызды деректер элементтерін анализдейтін салыстырмалы түрде күрделі құрал.

Decoder. Қолмен немесе интелектуалды декодтау, сондай-ақ веб-қосымшаның деректерін кодтау үшін пайдалы нәрсе. Яғни, сұраныста кодталған элемент боса, осы құрал арқылы декодтай аламыз.

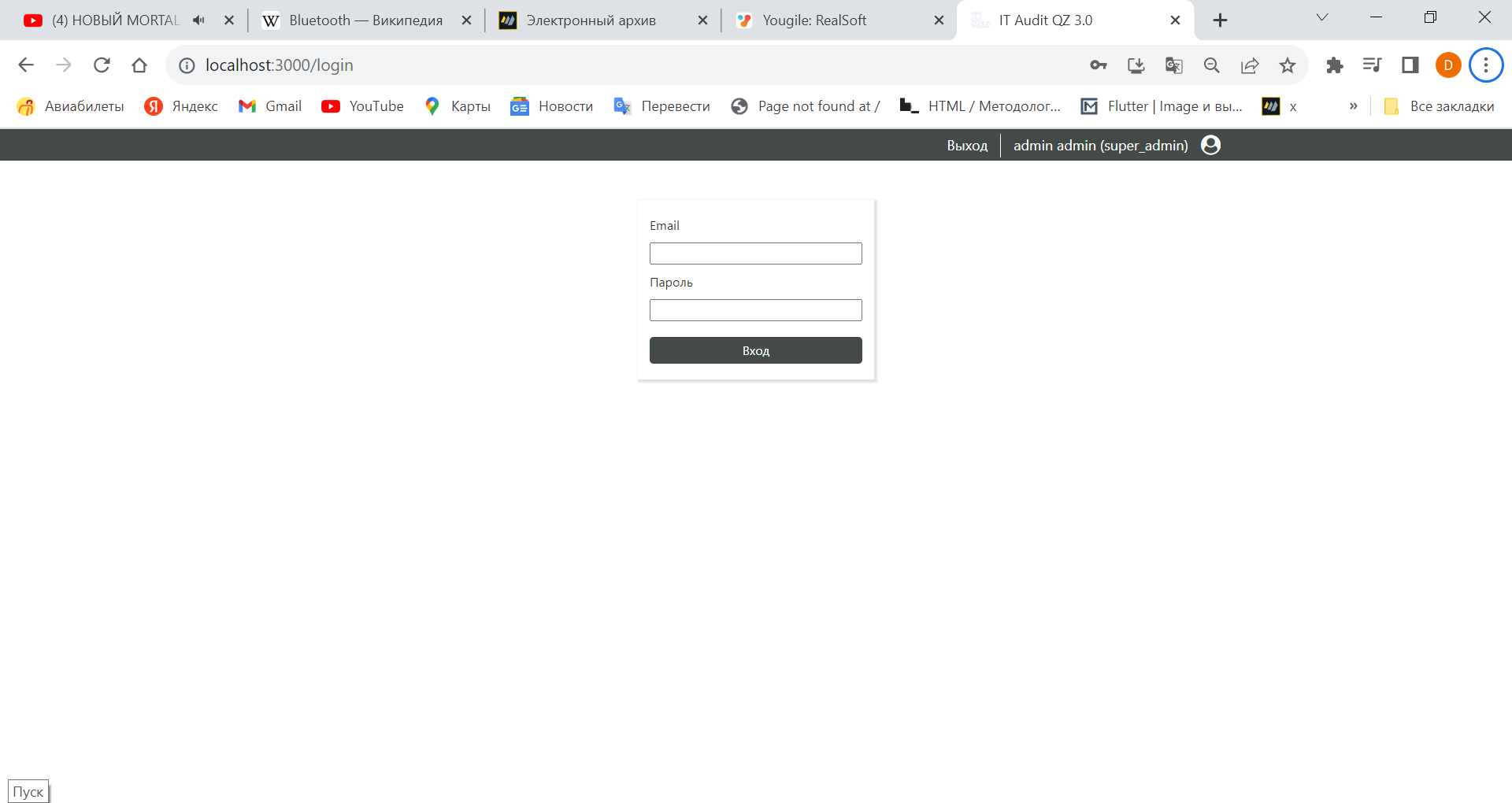
Comparer. «diff» пәрменін еске түсіретін ыңғайлы құрал. Бірақ кез келген 2 деректер элементі арасындағы айырмашылықтарды, мысалы, ұқсас HTTP хабарламаларының жұптарын визуализациялайды.

Мысалы, рұқсат етілген жүйенің авторизация бетіне өтеміз. Менің жағдайымда, ол: <https://portswigger.net/web-security/all-labs>.

Proxy құралы арқылы ұстап алуды орындаймыз. Ол үшін Intersept off батырмасын басамыз.

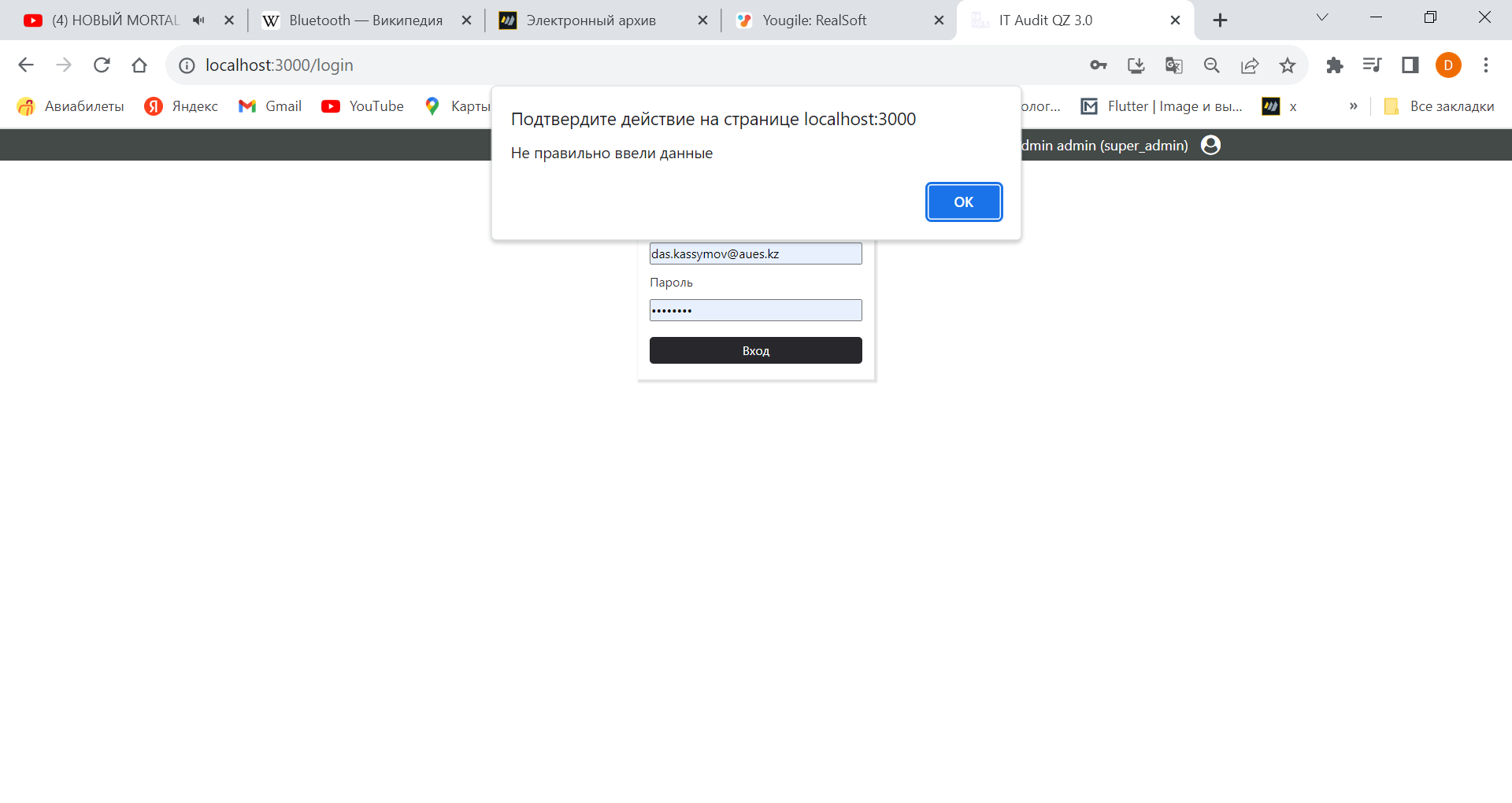


1-сурет – «Proxy»



2-сурет – «Авторизация»

Жүйеге администратор атынан кіруге болатыны белгілі. Алайды, құпия сөз біз үшін белгісіз. Бізге SQL-инъекцияны қолданып көреміз. Пайдаланушы атына ‘administrator’, ал құпия сөзге кездейсоқ символдарды жазып көреміз.

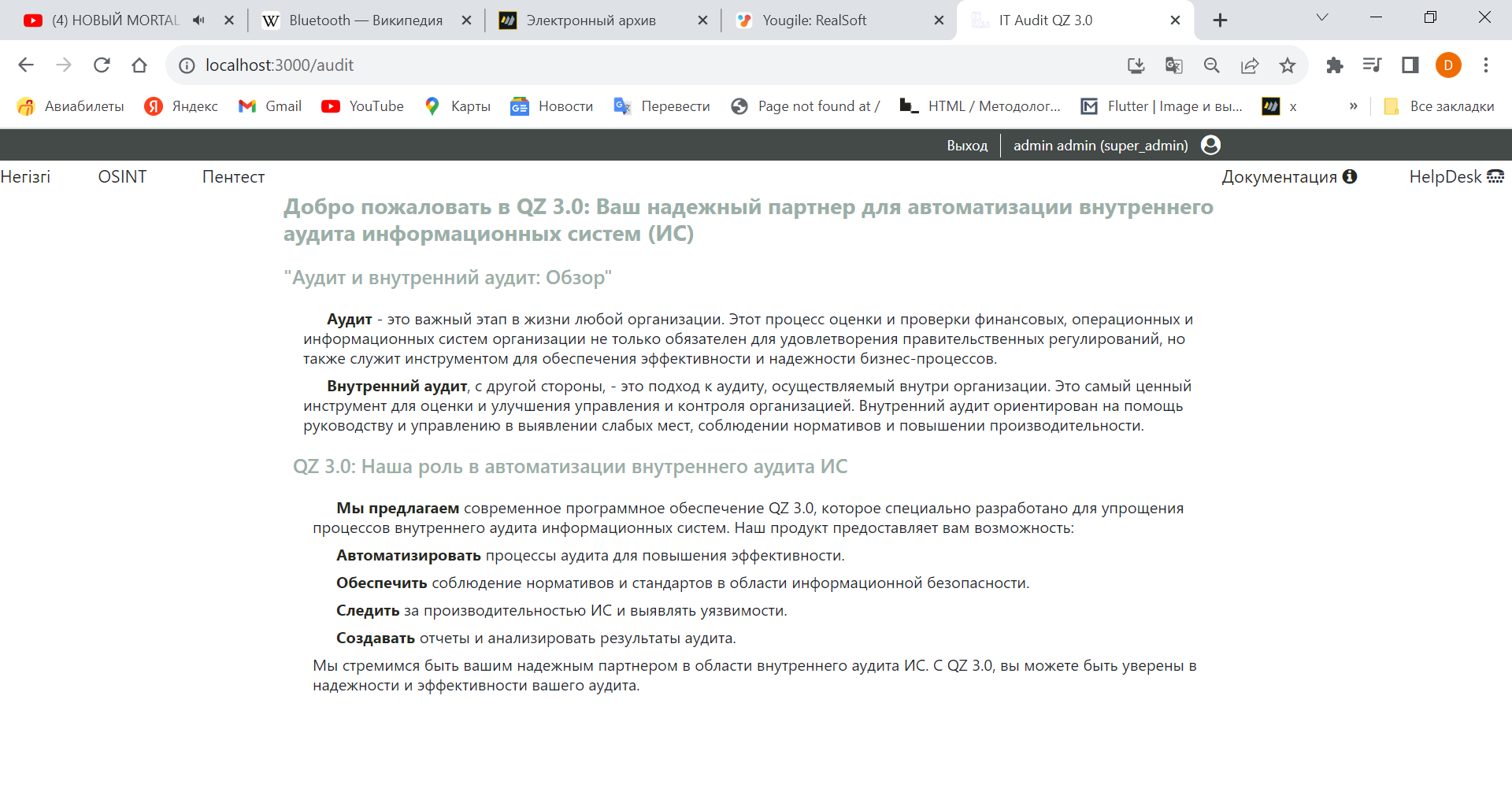


3-сурет – «Авторизациядағы қателік»

Сұраныс нәтижесі пайдаланушы атын немесе құпия сөзді қате жазғанымызды көрсетеді. Яғни, сервердегі SQL-кестесінде сұраныс төмендегідей болады.

SELECT \* FROM users WHERE username='administrator' and password='8v9$aXLZ'

Ендігі кезекте сайтта SQL-инъекция осалдығы бар не жоқ екенін тексереміз. Ол үшін пайдаланушы атын administrator', ал құпия сөзге кездейсоқ символдар жазамыз.

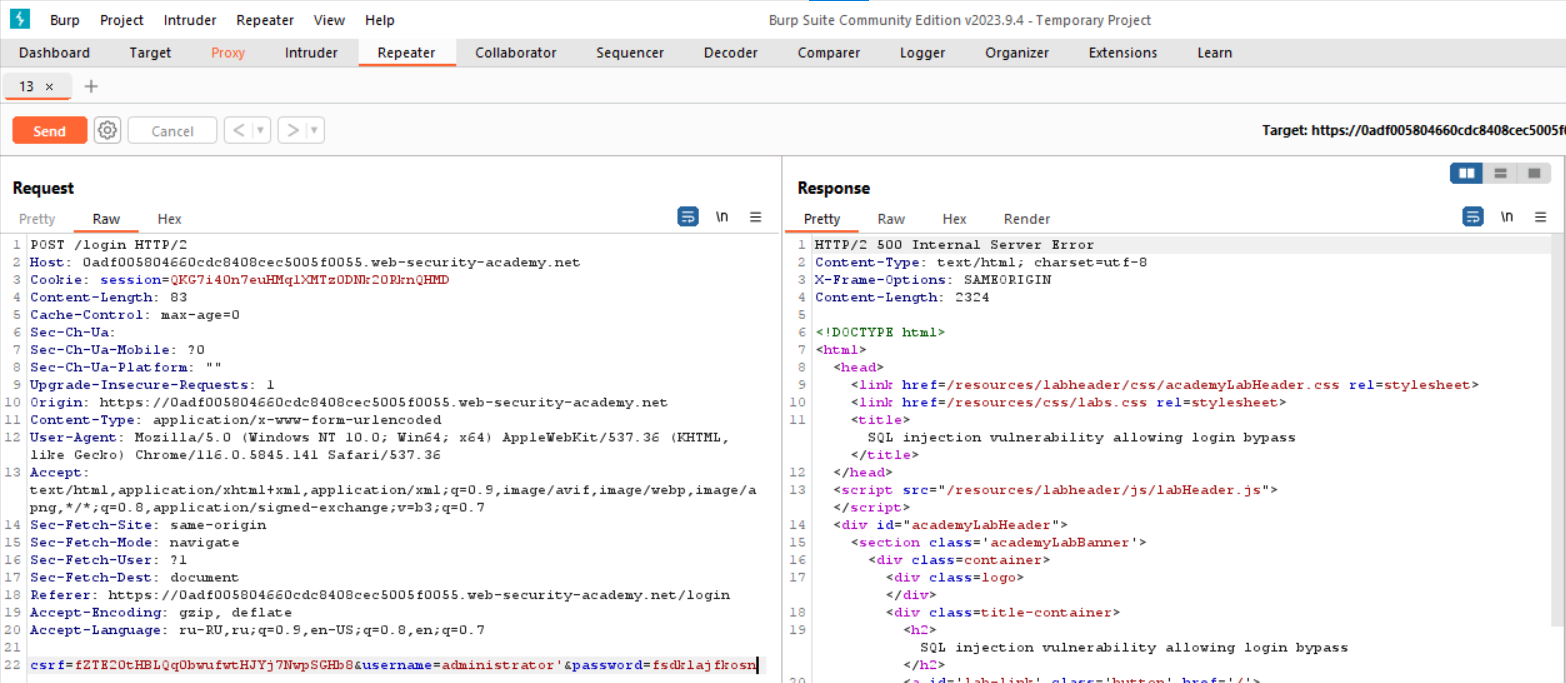


4-сурет – «Сервердің ішкі қателігі»

Көріп тұрғанымыздай біздің сұранысымыз сервердің ішкі қателігіне әкеп соқты. Яғни, сервердегі SQL-кестесінде сұраныс төмендегідей болады.

SELECT \* FROM users WHERE username='administrator'' and password='8v9$aXLZ'

Жоғарыдағы қадамды Repeater құралы арқылы жасаймыз. Ол үшін Intercept экранында ұстап алған сұранысты тінтуірдің оң жағын басып, Send to Repeater батырмасын басамыз. Әрі қарай сұранысты өзгертіп, сұранысты қайталап жібереміз.



5-сурет – «Repeater»

Бұл сұраныстан жүйеде SQL-инъекция осалдығы бар екені анықталды. Әрі қарай SQL кодтарының ішінен пікірді (комментарий) пайдаланамыз. Демек, пайдаланушы атын administrator '-- , ал құпия сөзге кездейсоқ символдар жазамыз. “--”-бұл пікір символы өзінен кейінгі мәліметтерді ескермейді. Яғни, пайдаланушы аты бар, әрі қарай құпия сөздің дұрыс не бұрыс болуының еш мәні жоқ. Өйткені, ол SQL сұраныста пікірге (комментарий) айналып кетті.

**Қорытынды**

Осы зертханалық жұмысты орындау барысында біз жұмыс принципін және "Burp Suite Community Edition" плагинінің негізгі мүмкіндіктерін сәтті зерттедік. Бұл құрал веб-қосымшалардың қауіпсіздігін талдау және ықтимал осалдықтарды анықтау үшін қажет болды. Қорытындылай келе, біздің жұмыс барысында анықталған келесі негізгі ойларды атап өткім келеді:

Икемділік және бейімделу: "Burp Suite Community Edition" әртүрлі қауіпсіздік тестілеу сценарийлеріне бейімделетін көптеген құралдарды ұсынады. Бұл ақпараттық қауіпсіздік мамандарына үлкен және кіші веб-қосымшаларды тиімді талдауға мүмкіндік береді.

Осалдықтарды анықтаудың жоғары дәлдігі: құрал инъекция, буфердің толып кетуі, ақпараттың ағып кетуі және т.б. сияқты әртүрлі осалдықтарды анықтауға мүмкіндік береді. Оның күшті аналитикалық мүмкіндіктері осалдықтарды іздеу және талдау процесін тиімдірек етеді.

Интеграция және автоматтандыру:" Burp Suite Community Edition " басқа құралдармен оңай біріктіріледі және күнделікті тапсырмаларды орындау үшін автоматтандырылуы мүмкін, бұл уақытты үнемдейді және қауіпсіздікті талдау процесін жеңілдетеді.

Оқыту және дағдыларды дамыту: зертханалық жұмыс студенттерге веб-қосымшалардың қауіпсіздігін тексеру бойынша практикалық дағдыларды алуға мүмкіндік берді. "Burp Suite Community Edition" жұмыс принциптерін түсіну ақпараттық қауіпсіздік құралдарын тереңірек зерттеуге және қолдануға жол ашады.

Нәтижесінде, "Burp Suite Community Edition" ақпараттық қауіпсіздік мамандарының арсеналындағы маңызды құрал болып табылады және оны зерттеу қазіргі цифрлық әлемде веб-қосымшалардың қауіпсіздігін қамтамасыз ету үшін үлкен маңызға ие. Осы зертханалық жұмыстағы күш-жігеріміз бізге веб-қосымшалардың қауіпсіздігін қамтамасыз ету және цифрлық активтерді қорғау үшін қолдануға болатын практикалық дағдылар мен білім берді.

**Қолданылған әдебиеттер**

1. <https://portswigger.net/burp> - All labs of Web Security Academy.
2. <http://www.codenet.ru/webmast/php/HTTP-POST.php> - Генерация HTTP запросов.
3. <https://www.christophh.net/2012/07/24/php-socket-programming/> - Burp Suite Community Edition.